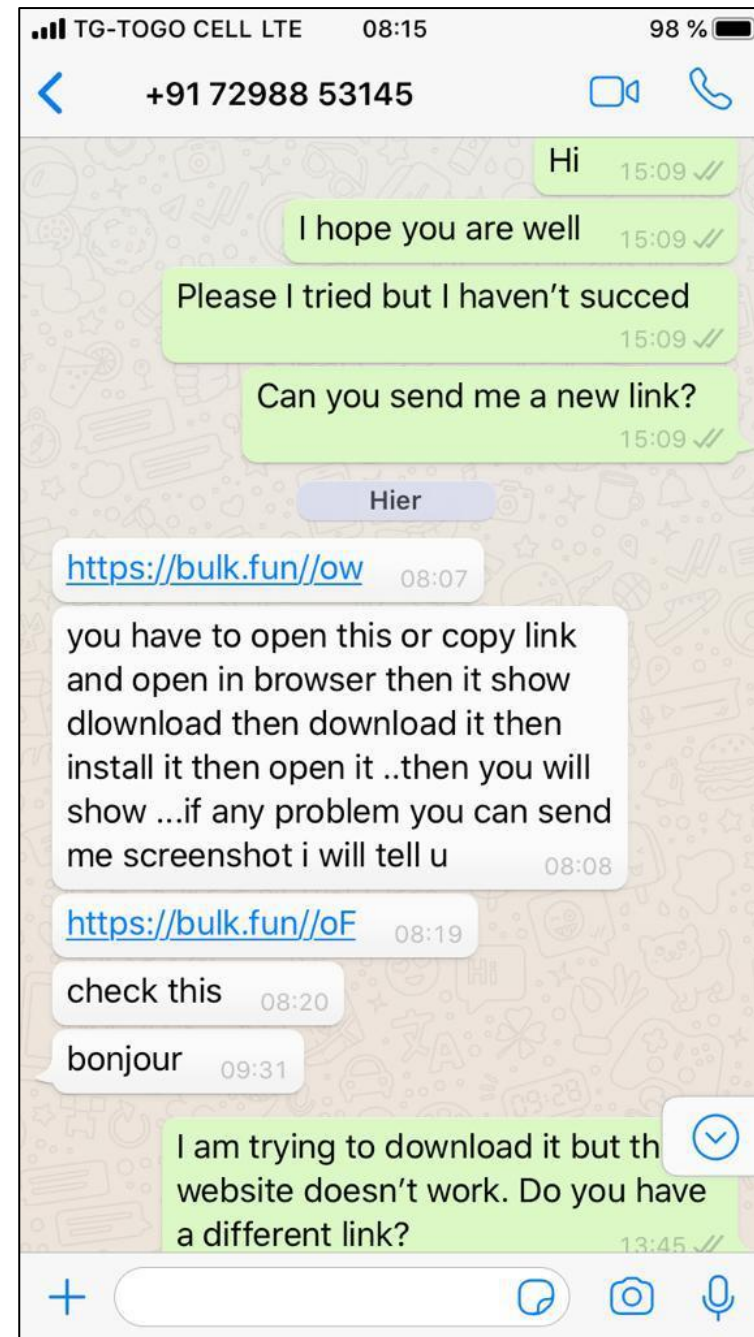
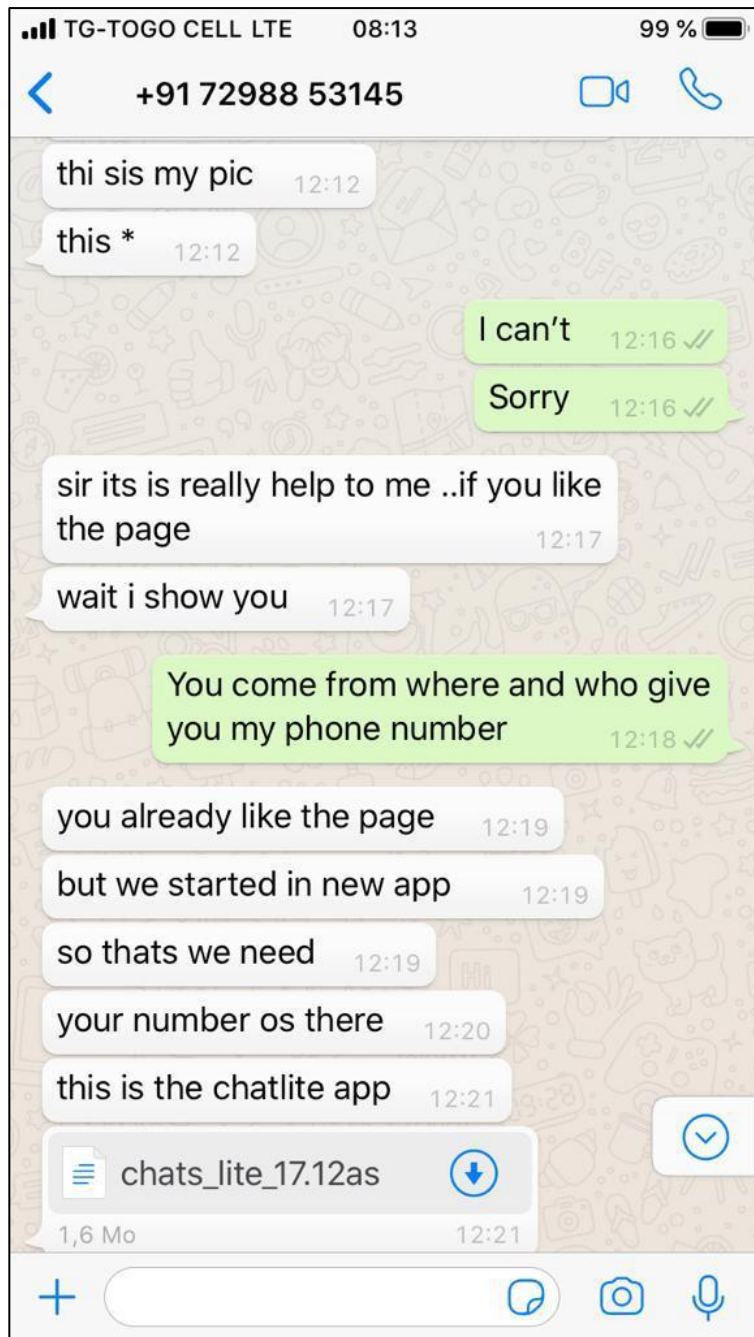


HACKERS-FOR-HIRE IN WEST AFRICA

A threat actor spreads its wings

Donncha Ó Cearbhaill
Amnesty International

Suspicious messages over WhatsApp



33

/ 64

ⓧ

Community Score

✓

ⓘ 33 security vendors flagged this file as malicious

46df9b77f5adbe03ed252248e5961408f8208827f4964e167356768a1fdd1b41
46df9b77f5adbe03ed252248e5961408f8208827f4964e167356768a1fdd1b41.bin

android apk malware reflection

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 1

AhnLab-V3

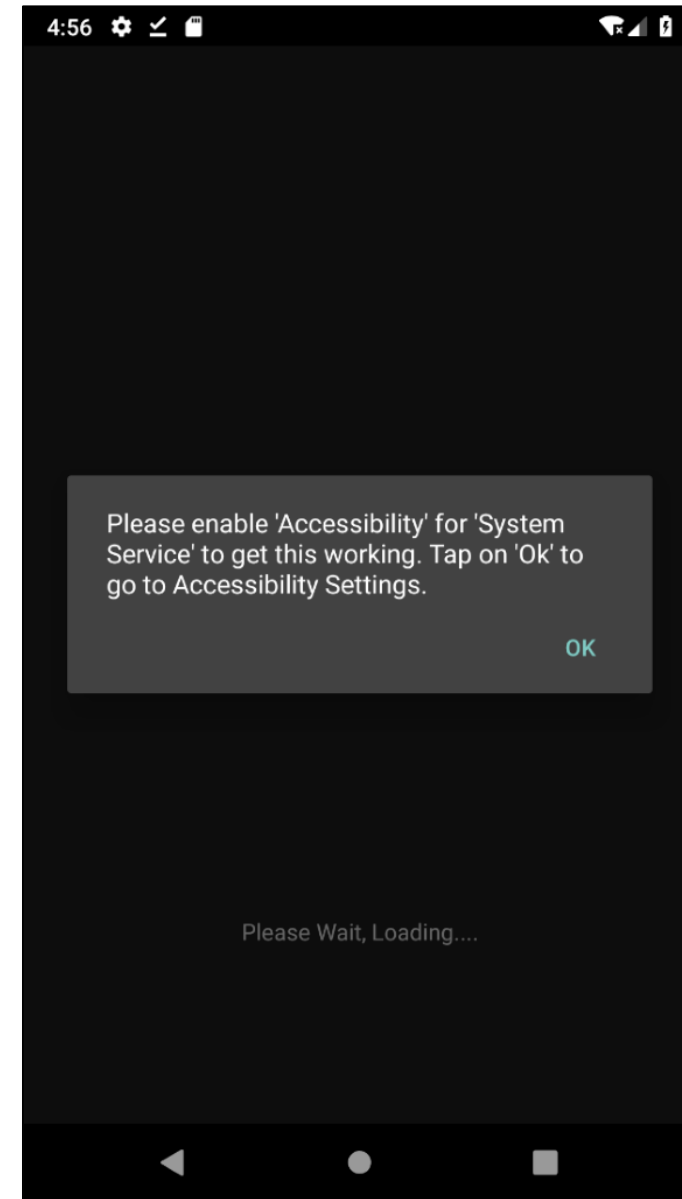
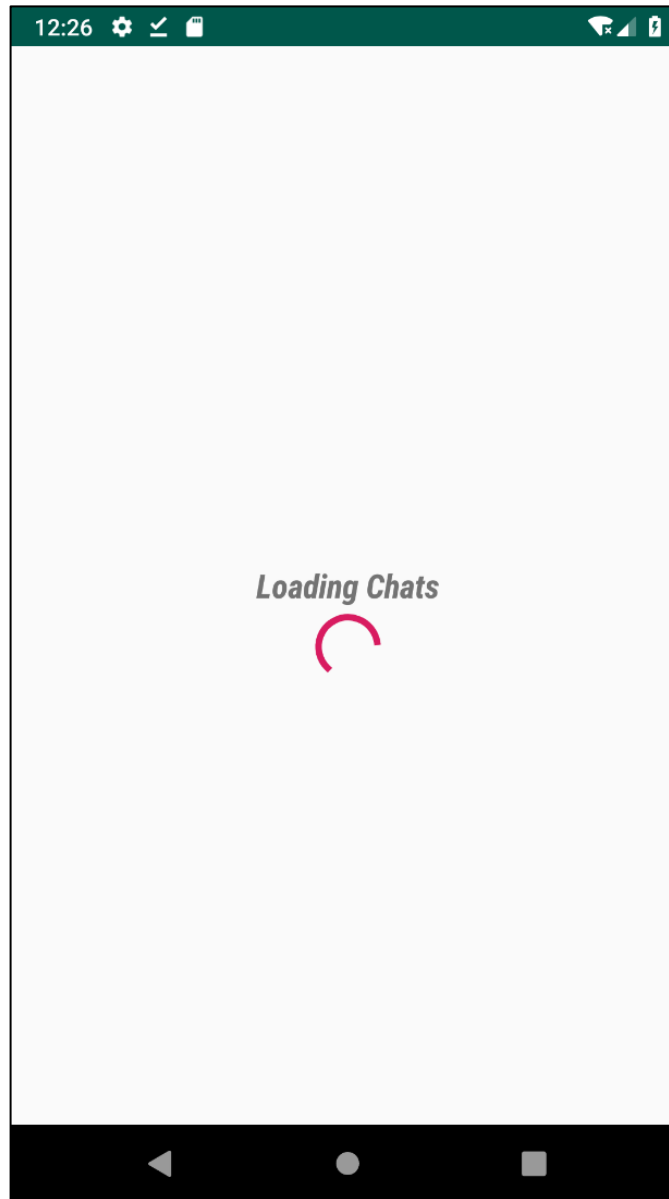
ⓘ Trojan/Android.SpyAgent.907760

Alibaba

Alibaba	ⓘ TrojanSpy:Android/Donot.bc693a13
Avast	ⓘ Android:Donot-A [Spy]
AVG	ⓘ Android:Donot-A [Spy]
BitDefenderFalx	ⓘ Android.Trojan.Donot.A
ClamAV	ⓘ Andr.Trojan.Donot-9778202-0

Stealjob/KNSpy Android
spyware linked to Donot Team

Connected to server
at **mimestyle[.]xyz**



Email received with malicious RTF file

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

Malicious RTF exploiting CVE-2017-0199

- RTF loaded an additional remote template containing the exploit payload from **`http://getelements[.]xyz/AN/AM`**
- Payload loads initial components of the Donot Team YTY framework and drops them on disk.
- Dropped YTY DLL (commit.dll) loaded by JS file and connects back to YTY C&C server at **`image.loadingmessage[.]info`**

```
var obl = new ActiveXObject("WScript.shell");  
obl.run('rundll32 "C:\\Windows\\Tasks\\commit.dll", solar');
```

Who are Donot Team

- APT group active in South Asia. Target focus includes Pakistan, India and Kashmir.
- First named by NetScout in 2018. Suspected continuation of EHDevel activity.
- Similarities to Operation Hangover (possible hacker-for hire operation).
- Uses StealJob/KNSpy against Android users, YTY framework on Windows.
- Clustered based on a **shared toolset**.

Multiple organisations or actors may be **sharing** tools, infrastructure and targeting.

NETSCOUT.

Donot Team Leverages New Framework

Donot Team Leverages New Modular Malware Framework in South Asia



产品中心 ▾ 解决方案 ▾ 合作伙伴 威胁研究 更多 ▾

威胁研究 > 正文

Donot team 组织(APT-C-35)移动端攻击活动分析



TALOS

Software Vulnerability Information Reputation Center Library Support

THURSDAY, OCTOBER 29, 2020

DoNot's Firestarter abuses Google Firebase Cloud Messaging to spread

AMNESTY
INTERNATIONAL

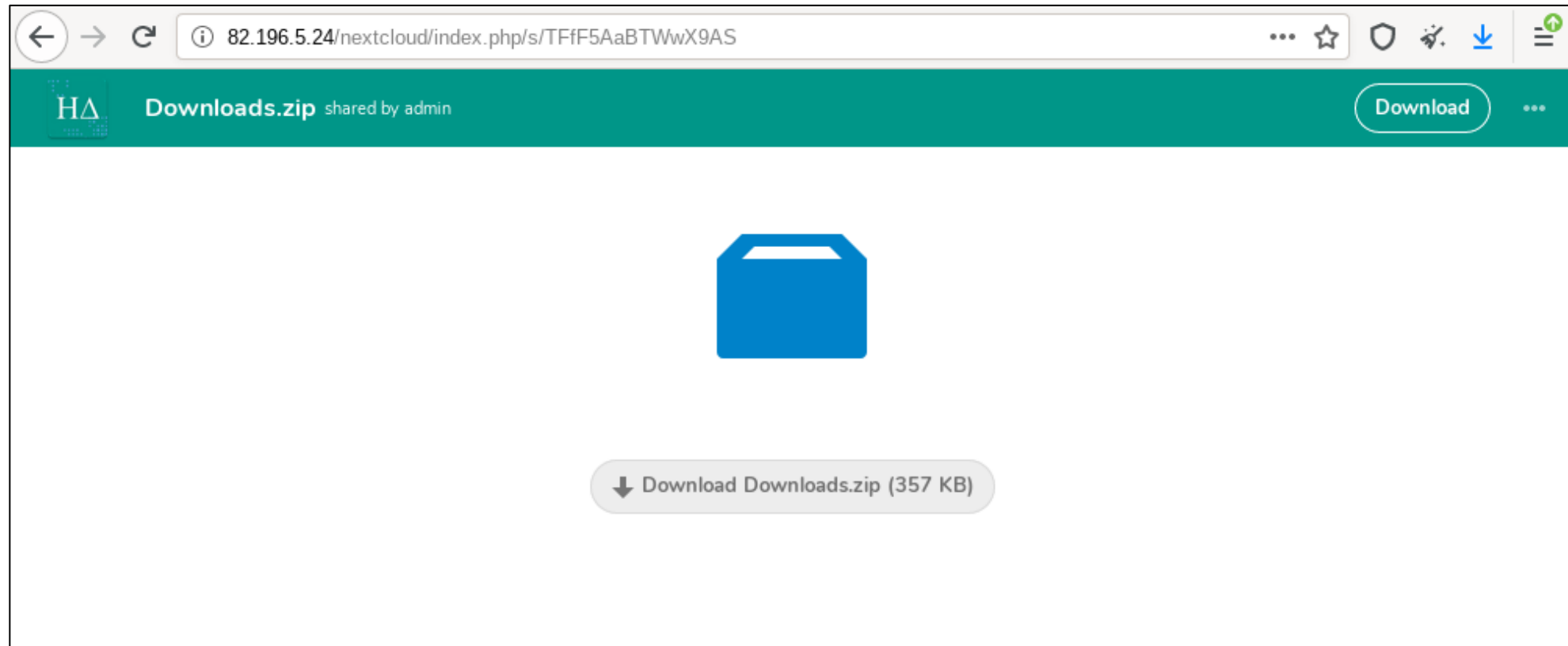


Digging deeper..

- Enumerated the (very) short URL shortener links which were included in the initial WhatsApp messages.
- Found links to spyware samples but also to potentially internal URLs
- Internal URLs pointing to **82.196.5.25**. Same server as **bulk.fun**.

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

Looking behind the curtain

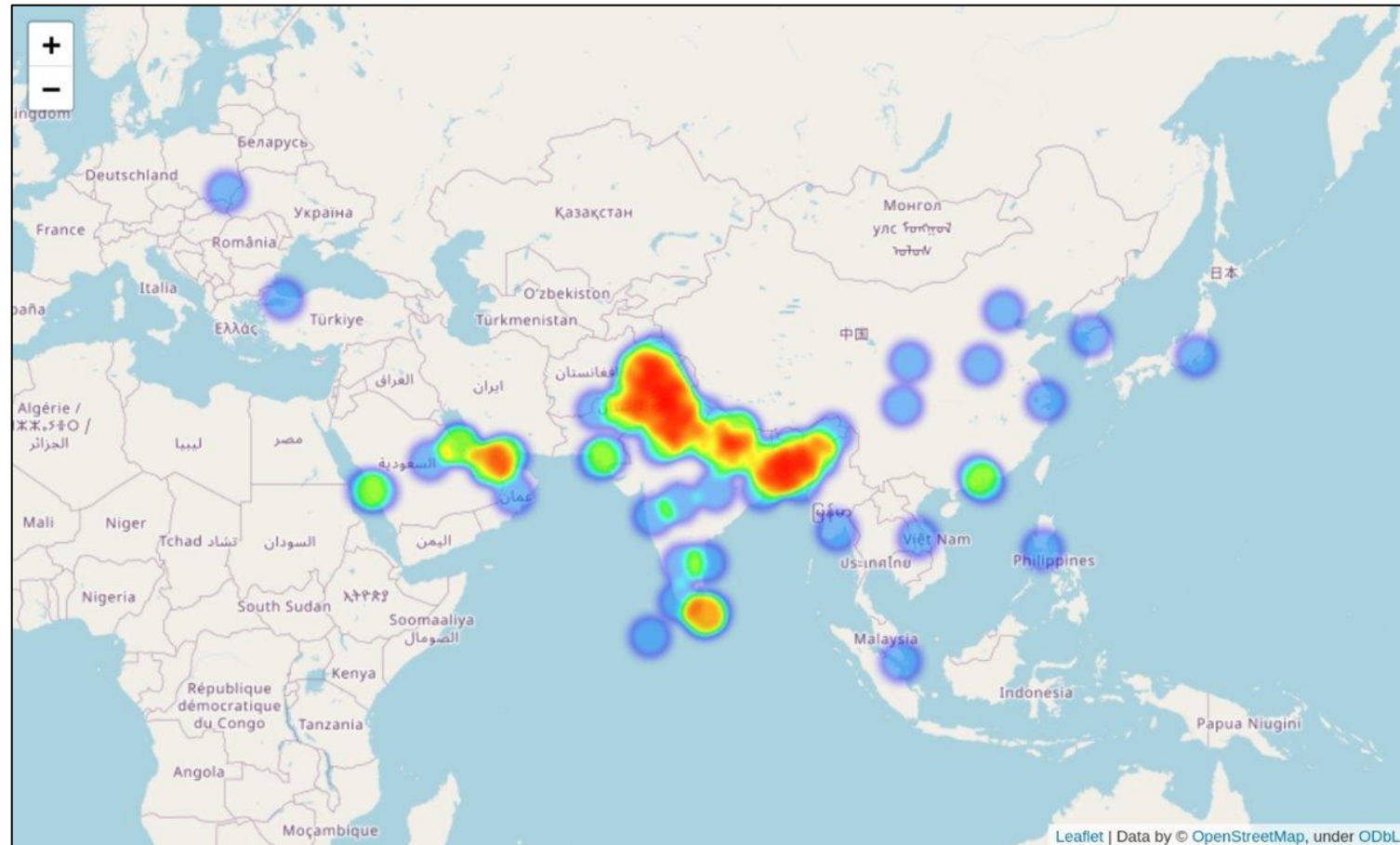


Looking behind the curtain

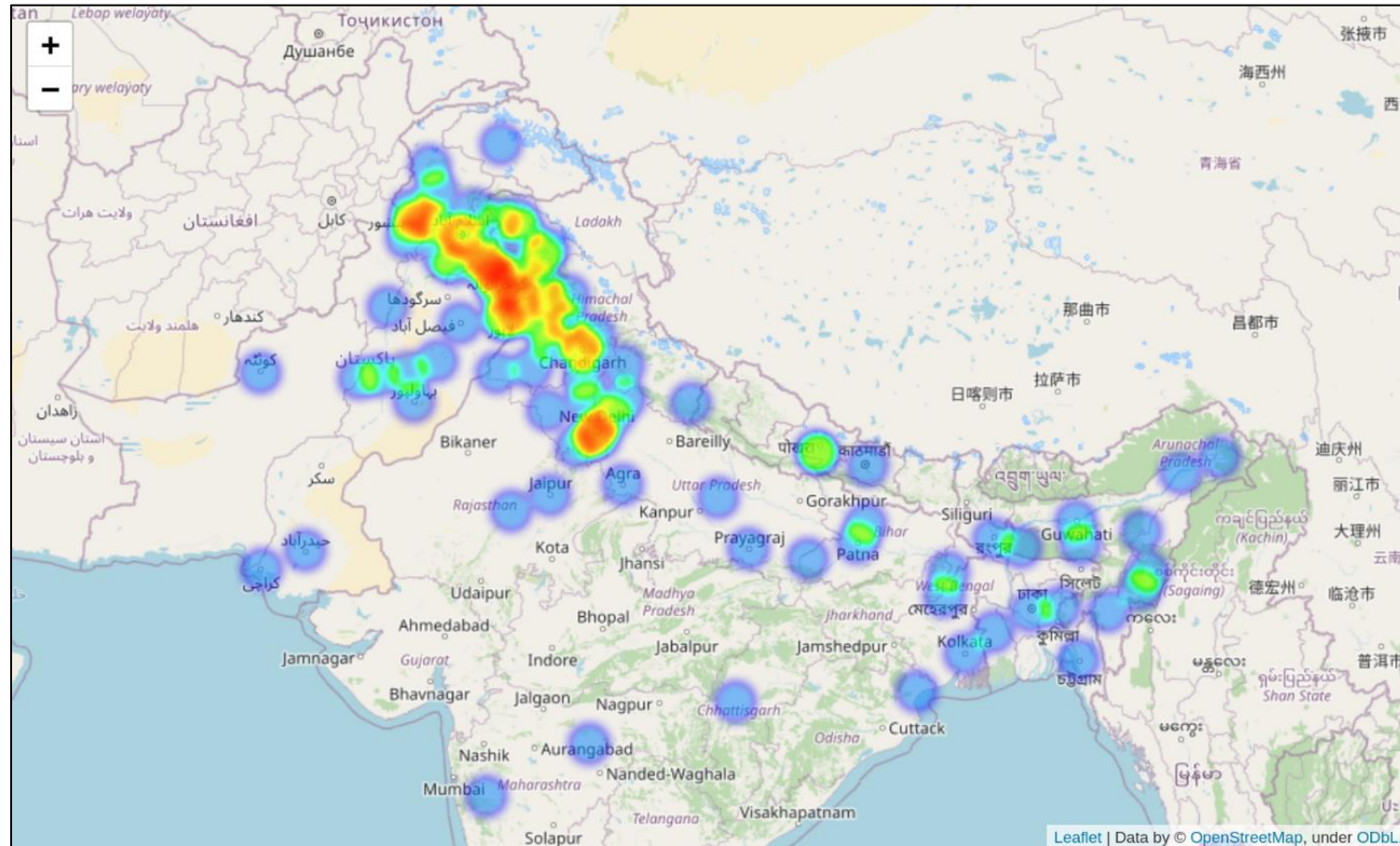
```
INSERT INTO `filex_downloads` (`id`, `fileid`, `date`, `ip`, `ua`) VALUES
(10553, 951, '2019-10-29 11:36:20', '192.168.1.1', 'Mozilla/5.0 (iPhone; CPU iPhone OS 13_1_3 like Mac OS X) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3989.93 Mobile Safari/537.36', '192.168.1.1'),
(10554, 950, '2019-10-29 11:36:32', '192.168.1.1', 'Mozilla/5.0 (Linux; Android 9; ANE-LX1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3989.93 Mobile Safari/537.36', '192.168.1.1'),
(10555, 950, '2019-10-29 11:39:48', '192.168.1.1', 'Mozilla/5.0 (Linux; Android 7.0; Lenovo K33a42) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3989.93 Mobile Safari/537.36', '192.168.1.1'),
(10556, 951, '2019-10-29 11:40:07', '192.168.1.1', 'Mozilla/5.0 (iPhone; CPU iPhone OS 11_1_2 like Mac OS X) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3989.93 Mobile Safari/537.36', '192.168.1.1'),
(10557, 950, '2019-10-29 11:45:22', '192.168.1.1', 'Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-J810F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3989.93 Mobile Safari/537.36', '192.168.1.1'),
(10558, 951, '2019-10-29 11:46:57', '192.168.1.1', 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3989.93 Safari/537.36', '192.168.1.1'),
(10559, 950, '2019-10-29 11:49:53', '192.168.1.1', 'Mozilla/5.0 (Linux; Android 9; ANE-LX1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3989.93 Mobile Safari/537.36', '192.168.1.1'),
(10560, 950, '2019-10-29 11:53:57', '192.168.1.1', 'Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-J810F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3989.93 Mobile Safari/537.36', '192.168.1.1'),
(10561, 917, '2019-10-29 11:56:01', '192.168.1.1', 'Dalvik/2.1.0 (Linux; U; Android 8.0.0; LDN-L21 Build/HUAWEILDN-L21)', '192.168.1.1')
```

- The Downloads.zip file contained two SQL database files of the Donot Team URL shortener and their spyware upload systems.
- Both database dumps were created in October 2019, two months before our investigation started.

Looking behind the curtain



Looking behind the curtain



What we know so far

- Human rights defender from Togo targeted with Android and Windows spyware.
- Both Windows and Android spyware are part of custom frameworks previously linked to the Donot Team APT group.
- Public Donot Team attacks have primarily targeted South Asia. Most of the IP addresses connecting to the spyware download server were from India, Pakistan and Bangladesh.

Internet scan for Android spyware server

```
SELECT
  ip,
  s.port_number,
  SAFE_CAST(s.banner AS String) AS banner,
FROM
  `censys-io.ipv4_banners_public.current`,
  UNNEST(services) AS s
WHERE
  SAFE_CAST(s.banner AS String) LIKE '%Starting'
```

```
SELECT
  ip,
  s.port_number,
  SAFE_CAST(s.banner AS String) AS banner,
  s.banner
FROM
  `censys-io.ipv4_banners_public.current`,
  UNNEST(services) AS s
WHERE
  SAFE_CAST(s.banner AS String) LIKE 'NSMVeY%'
```

The Donot Team Android spyware (StealJob) uses multiple distinct C&C protocols.

Return either:

- Base64 encoded public key beginning with **"NSMVeY..."**
- A "Starting" banner
\x00\x00\x00\x08Starting

Both useful for internet scanning

Internet scanning

```
SELECT
  ip,
  s.port_number,
  SAFE_CAST(s.banner AS String) AS banner,
FROM
  `censys-io.ipv4_banners_public.current`,
  UNNEST(services) AS s
WHERE
  SAFE_CAST(s.banner AS String) LIKE '%Starting'
```

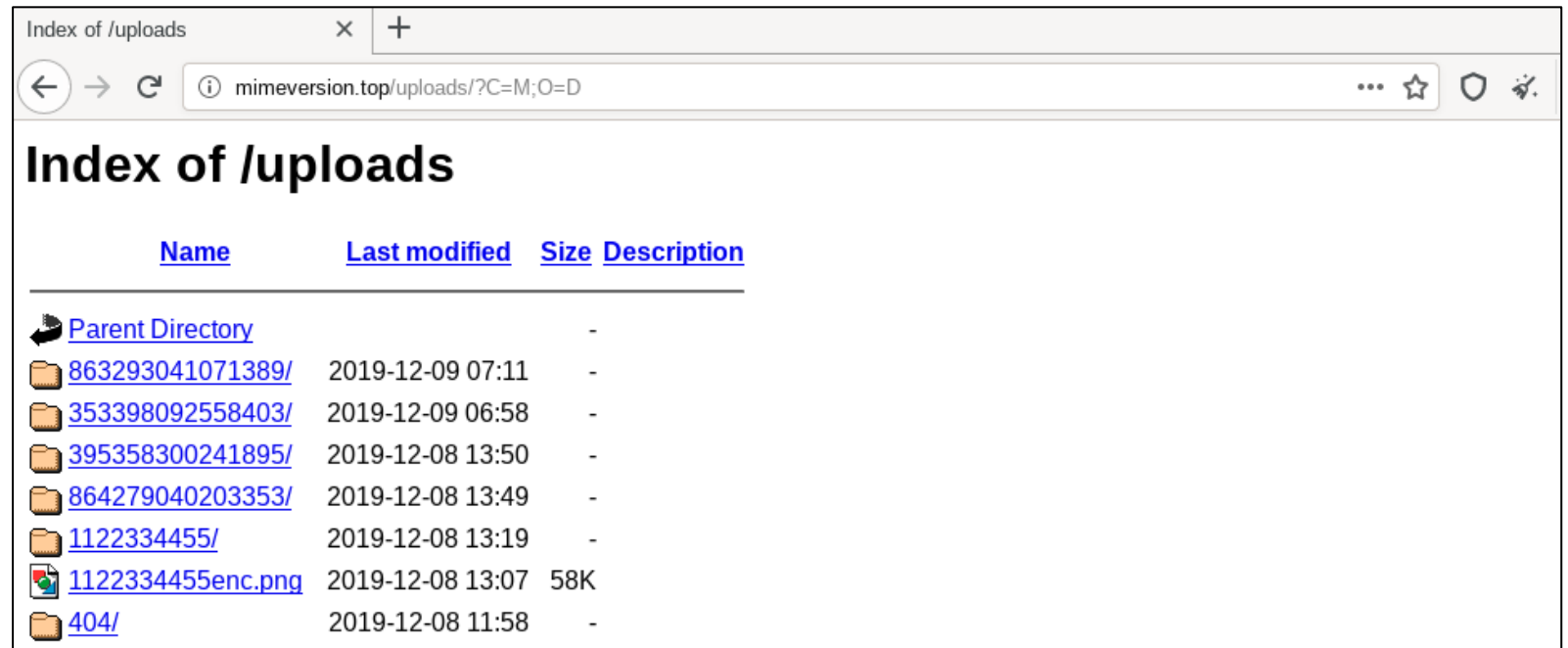
```
SELECT
  ip,
  s.port_number,
  SAFE_CAST(s.banner AS String) AS banner,
  s.banner
FROM
  `censys-io.ipv4_banners_public.current`,
  UNNEST(services) AS s
WHERE
  SAFE_CAST(s.banner AS String) LIKE 'NSMVeY%'
```









The Donot Team Android spyware (StealJob) uses multiple distinct C&C protocols.

Return either:

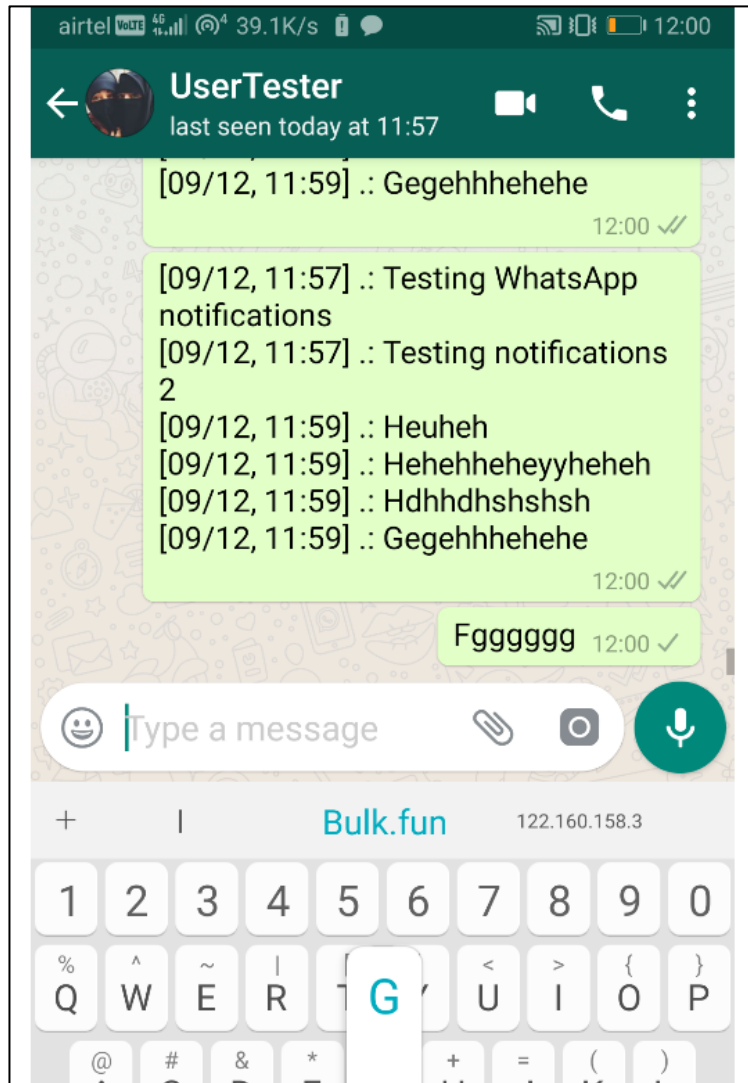
- Base64 encoded public key beginning with **"NSMVeY..."**
- A "Starting" banner
\x00\x00\x00\x08Starting

Both useful for internet scanning

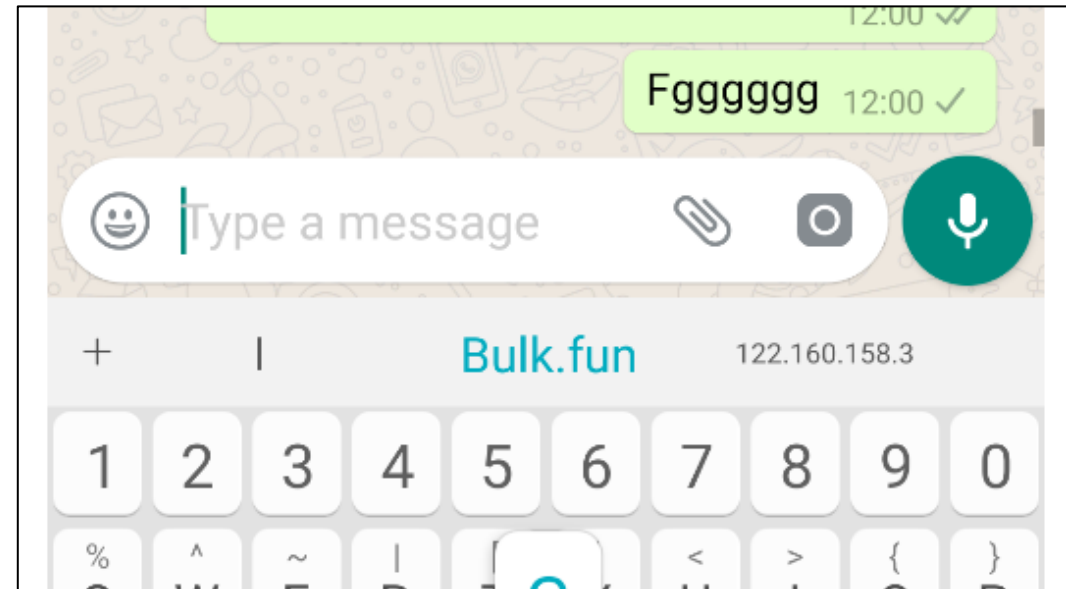
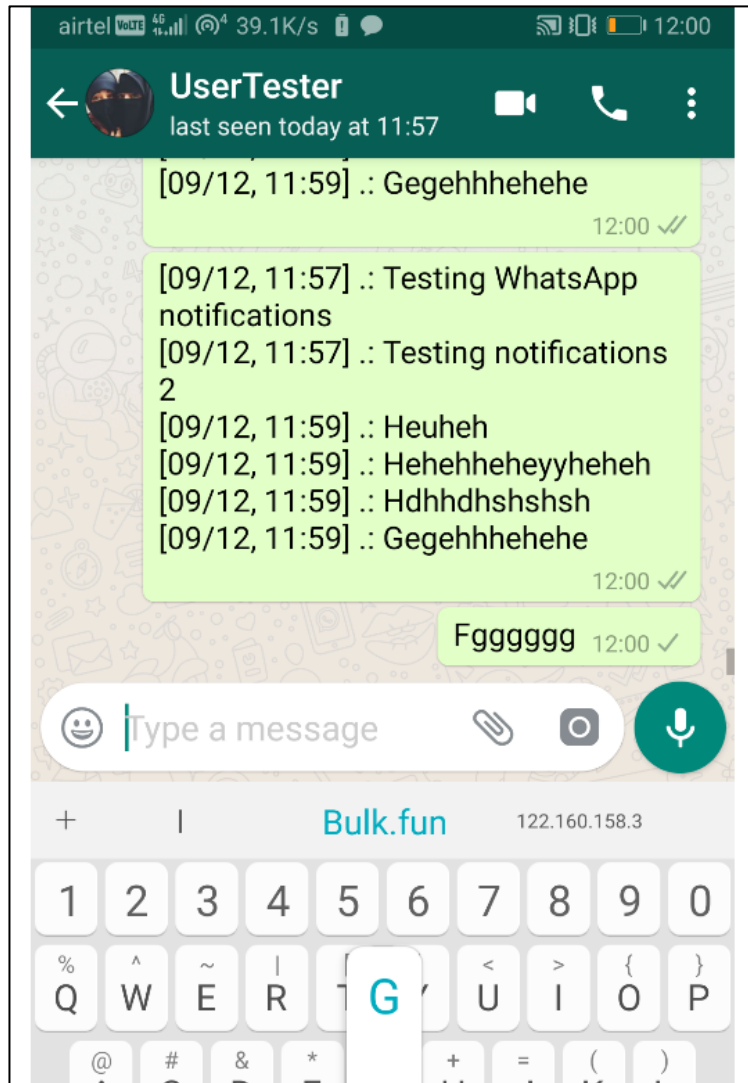


<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 863293041071389/	2019-12-09 07:11	-	
 353398092558403/	2019-12-09 06:58	-	
 395358300241895/	2019-12-08 13:50	-	
 864279040203353/	2019-12-08 13:49	-	
 1122334455/	2019-12-08 13:19	-	
 1122334455enc.png	2019-12-08 13:07	58K	
 404/	2019-12-08 11:58	-	

A fortuitous discovery



A fortuitous discovery

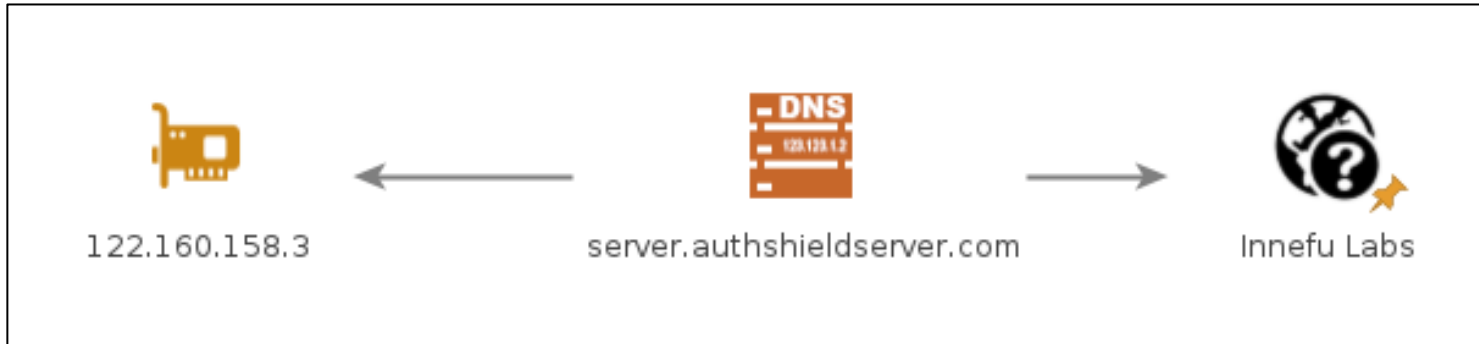


Keyboard auto-suggesting two URLs:

bulk.fun - URL shortener sent to Togo activist

122.160.158.3 - IP address located in India

Innefu Labs



- Passive DNS records show that the domain name **server.authshieldserver.com** has pointed to the Indian 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 Pvt.**

Who are Innefu Labs?



Innefu Labs



INNOVATING FUTURE

Innefu is a AI driven company developing cutting edge technology to carry out Predictive Intelligence and Cyber Security solution.



Innefu Labs



- Innefu claims its customers include “*some of the most sensitive and critical organizations in Government of India*”. Innefu also claims customers in “*Middle East / Africa / Bangladesh / India*”.
- The company does not publicly advertise offensive cyber services

Spyware development at Innefu Labs



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 maintenance of these builds.

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

[see less](#)

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

Response from Innefu Labs

- Amnesty International offered Innefu Labs a right to reply to the findings of this research.

- 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.

Conclusion

- Android and Windows spyware linked to Donot Team was sent to a prominent human rights defender in Togo.
- Discovered technical evidence connecting Innefu Labs, their IP address 122.160.158.3, and the bulk.fun attack infrastructure.
- Multiple former employees claimed to have developed spyware while working at Innefu Labs.

Conclusion

Confirmed additional links between Innefu Labs and the Operation Hangover attacks.

Note: Technical evidence is not sufficient to determine who carried out the targeting of the activist from Togo.

Tools and infrastructure may be shared by multiple operators and customers. Innefu Labs may only be involved in some aspects of the spyware development and not the full targeting process.

Thanks!

Donncha Ó Cearbhaill

donncha.ocearbhaill@amnesty.org

@DonnchaC

Samples or leads to
share@amnesty.tech

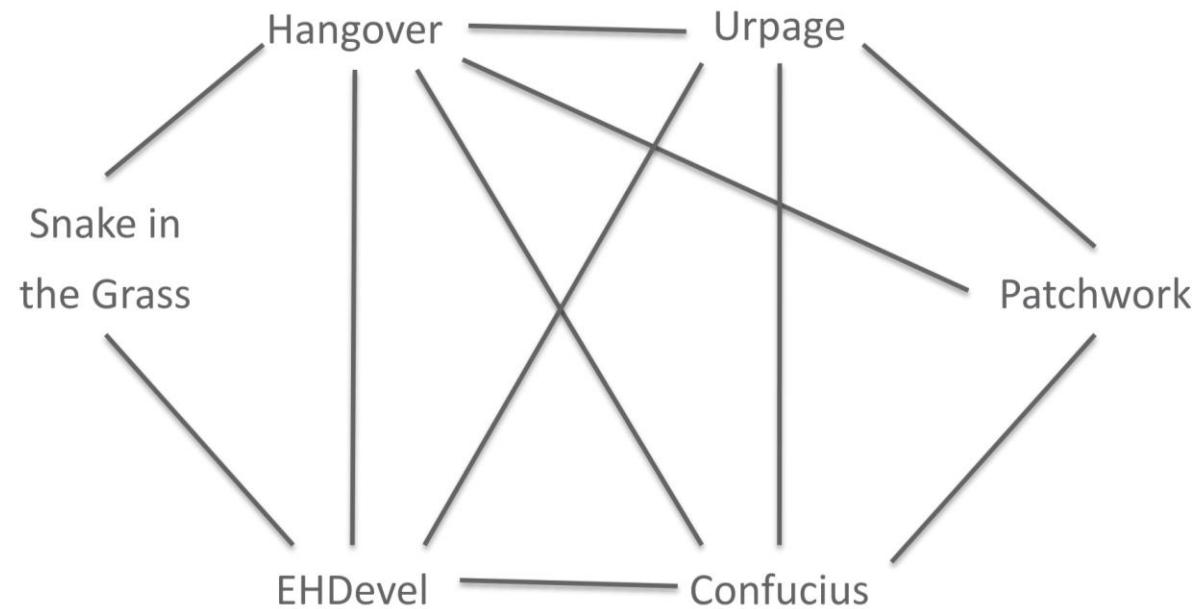
Additional slides

Indian IP address recorded in SQL database

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	
510	2019-02-19 11:11:11	193.169.244.74 (Deltahost)	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
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

Connections from Innefu Labs IP using XiaoMI Redmi 5A phone. The same browser user-agent made multiple connections from a Deltahost VPN IP. This Deltahost IP address is recorded as the uploader for hundreds of spyware samples and other files.

Trend Micro: Linking cyberespionage groups targeting victims in South Asia



Source:

https://www.first.org/resources/papers/tallinn2019/Linking_South_Asian_cyber_espionage_groups-to-publish.pdf

