Tracking Mobile Spyware during the Telegram blocking in Iran
Table of Contents

1 Executive Summary .................................................................................................................................... 1
2 Timeline .................................................................................................................................................. 2
3 Distribution channels ............................................................................................................................. 3
   3.1 Malware #1 (VPN Secure) ............................................................................................................. 3
   3.2 Malware #2 (Psiphon6) ................................................................................................................ 4
4 Functional analysis of the malware applications ................................................................................. 6
   4.1 VPN-Secure ..................................................................................................................................... 6
   4.2 Psiphon6-breacker .......................................................................................................................... 7
5 Attribution ................................................................................................................................................ 10
   5.1 Psiphon6-breacker ......................................................................................................................... 10
      5.1.1 The serverclient12.tk domain ............................................................................................... 12
      5.1.2 Ad-venture.ML and Amir Parsa Dehfuli (apd_1379) ............................................................. 13
      5.1.3 Ad-Venture.IR and Amir Parsa Dehfuli ................................................................................. 15
6 Detailed Analysis ..................................................................................................................................... 16
   6.1 VPN Secure ..................................................................................................................................... 16
      6.1.1 General Description ................................................................................................................ 16
      6.1.2 Permissions .............................................................................................................................. 17
      6.1.3 Files ......................................................................................................................................... 17
      6.1.4 Main activity ............................................................................................................................ 17
      6.1.5 Interesting details .................................................................................................................... 19
   6.2 Psiphon6 - Breacker ....................................................................................................................... 20
      6.2.1 General information ................................................................................................................ 20
      6.2.2 Permissions .............................................................................................................................. 20
      6.2.3 Files and Main Activities ....................................................................................................... 21
7 External Links .......................................................................................................................................... 24
8 Acknowledgements ............................................................................................................................... 25
1 Executive Summary

During the first of week of January 2018, we received numerous reports from Iran concerning the massive distribution of links promoting the download of fake VPN applications.

The fake Android mobile applications were distributed by SMS links, taking advantage of the blocking of Telegram in Iran, to deceive users to install the applications.

The first fake application used the name فیلترشکن آمدنهوز (Amadnews Filtershekan) and was hosted in the Amazon Storage, and the second sample impersonated the software “psiphon6” and was initially hosted at Backstory.com cloud service and later on at serverclient12.tk.

Our detailed analysis of the collected samples shows the privacy intrusive capabilities of the fake Android applications and how the attacker(s) behind the fake psiphon6 software can access all personal information of infected devices.

The malware, remotely controlled via the Iranian mobile notification service “pushe.co”, has the ability to snoop the SMS involved in two factor authentication. Additionally, the attacker can also gain access to location information and contact details.

Based on open source intelligence, we have managed to trace back the source code of the malware to a persona with the name “Amir Parsa Dehfoli”, who is working, or has been working with the Iranian startup company Ad Venture (ad-venture.ir).
2 Timeline

30 December 2017: The “Amadnews” channel is closed by Telegram as the channel includes messages promoting violence. The request was placed by Mohammad-Javad Azari Jahromi (@azarijahromi¹), Minister of Information and Communications Technology. After the closing of the channel, a new channel named “SadaieMardom” was created by the same administrators. The administrators promised Telegram’s co-founder Pavel Durov (@durov) to keep the channel free of information promoting violence.

31 December 2017: The Iranian authorities block access to Telegram and Instagram for the majority of Iranians after the refusal of Telegram to shutdown https://t.me/sedaiemardom and other peacefully protesting channels.

3 January 2018: A fake VPN software for Android is promoted to Iranians under the name “VPN Secure”. The fake software is spreading via SMS using the contacts of the affected phones and deletes all Phone Contacts on the victims devices.

6-7 January 2018: A second VPN software for Android is promoted by SMS under the name “Psiphon6”. The software is controlled using the Iranian “Mobile Notification Service” pushe.co and contains a wide range of functionalities to compromise the privacy of the affected phones. The malware is distributed using a free account of an Iranian cloud service (backtory.com) and later from the server serverclient12.tk.

13 January 2018: Iranian authorities lift the blocking of Telegram and Instagram.

17 January 2018: Iran CERTCC, the Iran Computer Emergency Response Team Coordination Center, releases a forensic report about the malware “VPN Secure”.

30 January 2018: Forensic Report released

---

¹ Twitter: https://twitter.com/azarijahromi?lang=en
² Telegram https://t.me/sadaiemardom
3 Distribution channels

3.1 Malware #1 (VPN Secure)

*Image 1: VPN Secure App SMS message*

*Image 2: Twitter report about the sample (9th January 2018)*
3.2 Malware #2 (Psiphon6)

The fake #فیلترشکن SMS again advertise. Please no don't download #فیلترشکن via SMS to your friends as well. #تظاهرات_سرازی #IranProtests

Image 3: A second fake app spreads (impersonating psiphon6)
Image 4: Short URL services were used to distribute the “psiphon6” fake Android mobile App.
4 Functional analysis of the malware applications

In order to find out the capabilities of the two fake Mobile applications, we have conducted static and dynamic analysis of the code samples. The static analysis was performed by “decompiling the binary code of the applications”, and the dynamic analysis was performed by running the applications in a “sandbox” with an Android software emulator.

The next section provides an overall description of the capabilities of the malware. For more technical details, please see Section 6.

4.1 VPN-Secure

Our first sample of VPN-Secure is dated January 3rd 2018. The first message that the user receives after installing the application is:

“Error 505 - Sorry your Device is not compatible with this Application.”
After that initial message, the “VPN Secure” application wipes out all contacts and starts sending the “spreading” message to each phone contact at a ratio of one SMS every 15 seconds. When all SMS has been sent, the phone will vibrate for 60 seconds.

4.2 Psiphon6-breacker

This second malware appeared just a few days (January 6th 2018) after the “VPN Secure” was distributed.

The second application contains much more functionality and we believe that the attacker had this code already written before the January events.

The malware is activated when the victim receives a SMS with the text:

"سلام - این فیلترشکن رو دانلود کن باهاش میتونی خیلی راحت به تلگرام وصل بشی"  
(Persian)
“Hi - Download this cracker with it, you can easily connect to the Telegram!.”  (English translation)

Once the victim clicks on the link, a URL shortening service (qqt.ir) will redirect the user to the site http://serverclient12.tk/dlvpn/vpn.apk

This application has intentionally been named “psiphon6”, to fool the user that the well-known circumvention tool Psiphon (https://psiphon.ca) will be downloaded.

After the installation, three fake error messages are displayed:

1. Please connect to the Internet
2. To enable the program to work properly, please turn on the Internet and try again
3. Proxy not working in your phone!, PSIPHON deleted successfully

The software states that the fake app is not compatible with the phone and has been deleted. However, the software is still running without the user’s knowledge.

The main mechanism implemented to control the trojan software (acting as a command and control) is the use of the Mobile notification service pushe.co.

The attacker uses the Iranian pushe.co notification service\(^3\) to send commands (JSON) to all compromised the devices.

For example, if the malware receives the command “spamsms”, it will send SMS to all the phone numbers of the phone book with the hardcoded message:

\(^3\) Pushe.co API: https://github.com/pusheco
"سلام - این فیلت شکن رو دانلود کن باید مبتنی خیلی راحت به تلگرام وصل بشی"

"Hi - Download this cracker with it! You can easily connect to the telegram. " (English translation)

This “spamsms” functionality is also triggered when the phone is infected without the need of the external command.

Other interesting commands that the malware can receive include:

1. The ability to download and upgrade the fake application
2. To capture received SMS for two factor authentication
3. View Instagram accounts
4. Exfiltrate (leak) contacts

Another important feature of this malware is the ability to download and install new Apps (including new malware) over the Internet.

The Trojan also contains code pointing to the bank service shaparak.ir. The code seems to be recycled from other malicious applications written in the past.

A quick look at the permissions requested by the App, shows that 32 of them include reading the device position, send and receive SMSs, read the contacts, and read and write in the external storage.

The Trojan can receive the two factor authentication confirmation codes for Telegram. The software can also access the network status, Wi-Fi name and service provider.

The Trojan also includes a reference to a php script hosted at elicharge.ir, which is a domain registered by Mohammad Dehfoli with the email address rilufeapd@gmail.com (note the “apd”). This service (elicharge.ir) has been used in previous malware campaigns as a fake Satellite App.

---

4 URL: https://bpm.shaparak.ir/pgwchannel/msuccessReceipt.mellat
5 PHP script: http://elicharge.ir/mp20ibest.php

Image 8: Fake Satellite App logo
5 Attribution

We have focused our efforts in attributing the second malware (Psiphon6-breacker).

5.1 Psiphon6-breacker

The 6\textsuperscript{th} of January a malware sample was distributed using the Iranian cloud service Backstory.com. The day after, the software was distributed from the server serverclient12.tk\textsuperscript{7}

Image 9: 120.000 downloads from backtory.com the release day

\textsuperscript{7} Source: http://serverclient12.tk/dlvpn/vpn.apk
This App aims to trick users making them think it is the official “Psiphon”\textsuperscript{8} App, using its name and logo.

\textbf{Image 10: Fake psiphon6 app from “ir.ops.breacker”}

\textbf{Image 11: Urlquery.net Crawl of the 1o2.ir short URL. Tracking the short URL code, links with serverclient12.tk.}

\footnotesize{8} https://play.google.com/store/apps/details?id=com.psiphon3.subscription
5.1.1 The serverclient12.tk domain

After backstory.com shut down the attacker’s free account in the system (redfox), he used the short URL service, qqt.ir aka 1o2.ir. This service allows the creation of short URLs that are rewritten to other websites, so the links can be shared easily by SMS. During the malware campaign, this Iranian shortening service was hidden behind Cloudflare. Currently it is hosted with OVH at the IP address 178.32.126.181.

One interesting feature of the qqt.ir service is the ability of the attacker to monitor the number of hits that the shorting service receives. The distributed link qqt.ir/psvpn pointed to the server serverclient12.tk. The domain was registered the middle of November 2016 by harvest68@gmail.com also known as “Harvest Moon” (h-moon.ir). This email is associated with Sina Motlagh (harvest.moon829@gmail.com), who publishes code to write Telegram bots in Github.

The domain name server ns1.serverclient12.tk hosted on the IP address 94.130.144.253 shares hosting with the domain name namazhe.net. Namazhe.net is linked to the email address apd_1379@yahoo.com, which is associated with Amir Parsa Dehfoli.

The following table shows the domains associated to Amir Parsa Dehfoli
<table>
<thead>
<tr>
<th>Domain name</th>
<th>Email</th>
<th>Phone</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>namazhe.net</td>
<td>Sina Motlagh</td>
<td>9712569854756</td>
<td>NetafrozCo</td>
</tr>
<tr>
<td></td>
<td>Harvast68</td>
<td></td>
<td>Used as Telegram channel associated with Elipay</td>
</tr>
<tr>
<td></td>
<td>gmail.com (SOA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:apd_1379@yahoo.com">apd_1379@yahoo.com</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>elipay.net</td>
<td><a href="mailto:apd_1379@yahoo.com">apd_1379@yahoo.com</a></td>
<td>982144529244</td>
<td>امیر پارسا دمفولی</td>
</tr>
<tr>
<td>eligeraam.net</td>
<td><a href="mailto:apd_1379@yahoo.com">apd_1379@yahoo.com</a></td>
<td>982144529244</td>
<td>امیر بارسا جهفولی</td>
</tr>
<tr>
<td>amirparsa.xyz</td>
<td><a href="mailto:apd_1379@yahoo.com">apd_1379@yahoo.com</a></td>
<td></td>
<td>AMIR PARSA DEHFUL</td>
</tr>
<tr>
<td>clashtour.ir</td>
<td><a href="mailto:apd_1379@yahoo.com">apd_1379@yahoo.com</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dominet.ir</td>
<td><a href="mailto:apd_1379@yahoo.com">apd_1379@yahoo.com</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>hamzad.net</td>
<td><a href="mailto:apd_1379@yahoo.com">apd_1379@yahoo.com</a></td>
<td></td>
<td>امیر بارسا جهفولی</td>
</tr>
<tr>
<td>elicharge.ir</td>
<td><a href="mailto:rilufcajd@gmail.com">rilufcajd@gmail.com</a></td>
<td>+9892144529244</td>
<td>Mohammad Dehfuli</td>
</tr>
</tbody>
</table>

Image 13: RiskIQ analysis of apd_1379@yahoo.com

5.1.2 Ad-venture.ML and Amir Parsa Dehfuli (apd_1379)

Historical data of elipay.net pointed us to the address 185.86.181.93 where the following sites have shared hosting:

1. ns1.elipay.net, ns2.elipay.net, elipay.net
2. botpay.ml
3. ad-venture.ml
4. hamzad.net, ftp.hamzad.net.
5. eligeraam.net
A few months ago, the domain ad-venture.ml shared hosting at the IP address 46.165.240.233 with advn.ir, ad-venture.ir, adlinker.info.

Thanks to Google Cache, we discovered that a “Amir Parsa Dehfuli” was previously working as Business Intelligence (BI) for the company ad-venture.ir.

Image 14: Cached LinkedIn of Amir Parsa Dehfuli (BI Consultant – Ad-Venture)

Image 15: Maltego Graph linking Amir Parsa Dehfuli with Ad-Venture
5.1.3 Ad-Venture.IR and Amir Parsa Dehfuli

We reached out to Ad Venture, a company based in Iran specialized in Telegram advertisement. Ad Venture’s CEO Alireza Aghasi (AlirezaAghasi@gmail.com) confirmed that Amir Parsa Dehfuli was a previous employee helping in the development of the site (ad-venture.ml).

Aghasi also stated that Amir Parsa Dehfuli is not on the company payroll. Alireza Aghasi, who calls himself a “telegrampreneur” has been critical against the shutdown of Telegram in Iran⁹.

According to historical records, the domain ad-venture.ml was registered in late August 2017 and ad-venture.ir went live in early December 2017. This information suggests that the persona “Amir Parsa Dehfuli” was helping Ad-Venture recently.

The domain ad-venture.ml vanished the 10th of January 2018, just a few days after “psiphon6-breacker” was released.

---

Image 16: Alireza Aghasi.

Image 17: CEO Ad-Venture
6 Detailed Analysis

6.1 VPN Secure

6.1.1 General Description

Package: android.com.ui
Checksum: 562e02130fcbea7cc0d2a527ace6c05
Min supported API: 9 (Gingerbread, 2.3)
Target API Android: 21 (Lollipop, 5.0)
Size: 344033 bytes
Distribution: https://s3.us-east-2.amazonaws.com/vpnsecure/vpn.apk
Spread: SMS using Phone Contacts

Image 18: VPN-Secure Logo.
6.1.2 Permissions

- android.permission.INTernet
- android.permission.RECEIVE_BOOT_COMPLETED
- android.permission.SEND_SMS
- android.permission.READ_CONTACTS
- android.permission.WRITE_CONTACTS
- android.permission.VIBRATE
- android.permission.FLASHLIGHT

6.1.3 Files

- android.com.ui.MainActivity: Main
- android.com.ui.receiver.MyBroadcastReceiver: Listener with permissions to track when the device is turned on and to start the service automatically.
- android.com.ui.service.MyService: Service that runs the main tasks of the app (See follow sections)

6.1.4 Main activity

The application is abfuscated using Pro Guard. The first message that a victim receives when launching the App is the message:

"Error 505 - Sorry your Device is not compatible with this Application."

The message is always sent without any checks.

protected void onCreate(Bundle bundle) {
    super.onCreate(bundle);
    setContentView(R.layout.activity_main);
    m488c();
    m487b();
    m486a();
}

private void m486a() {
    final AlertDialog create = new Builder(this).create();
    create.setCancelable(false);
    create.setTitle("Error 505");
    create.setMessage("Sorry your Device is not compatible with this Application.");
    /* SNIP */
    create.show();
}

The call m488c(), opens a new thread and is responsible of two tasks:

1. Hide the application so the user can not uninstall it easily.
   PackageManager.COMPONENT_ENABLED_STATE_DISABLED
2. Set the application as “unkillable” so the application runs permanetly
   PackageManager.DONT_KILL_APP
private void m488c() {
    new Thread(new C01272(this)).start();
}

class C01272 implements Runnable {
    /* SNIP */
    public void run() {
        this.f289a.getPackageManager().setComponentEnabledSetting(new ComponentName(this.f289a, MainActivity.class), PackageManager.COMPONENT_ENABLED_STATE_DISABLED, PackageManager.DONT_KILL_APP);
    }
}

Finally, m487b() calls the service (MyService):

private void m487b() {
    startService(new Intent(this, MyService.class));
}

The user will only see the following screen view.

![Image 19: Main pop-up of VPN-Secure.](image)
**MyService** is the main service of the application and is responsible of the following tasks:

1. Fetches all contacts from the device
2. Saves all contacts in “SharedPreferences” of the application into a simple XML format that is saved inside of the installation folder of the application with the key “Contacts”.
3. Deletes all contacts of the device.
4. Crawls all contacts in SharedPreferences and sends a SMS every 15 seconds including a SMS with a link to download the App.
5. Vibrates 60 seconds, launch the Activity: AdActivity and waits 10 seconds before returning to point 1.

### 6.1.5 Interesting details

1. The name of the package is “com.android.ui”, clearly trying to confuse users.
2. The screen shows real details of amadnews.org and PayPal link [https://goo.gl/tkzn4D](https://amadnews.org/archives/18258)
3. There is no evidence of data exfiltration to a server.
4. The application keeps track of contacts not to resend SMSs.
5. If the infected user adds a new contact, it will also receive the SMS
6. Users with “root” access to the device can recover their contacts.
7. How to uninstall the app:

   - `adb shell pm uninstall com.android.ui`
6.2Psiphon6 - Breacker

6.2.1 General information

Package: ir.ops.breacker
Checksum: 1371a4fb7baafa9af3aafcf7fd26da/90ff1a3fac150bd9482a7da0bca99b
Minimum SDK: 15 (Ice Cream Sandwich, 4.0.3)
Target SDK: 22 (Lollipop, 5.1.1)
Size: 1945380 bytes
Distribution: Backstory Cloud Service
Spread: SMS using Phone Contacts

6.2.2 Permissions

- android.permission.CALL_PHONE
- android.permissionINTERNET
- android.permission.READ_PHONE_STATE
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.READ_EXTERNAL_STORAGE
- android.permission.READ_CONTACTS
- android.permission.RECEIVE_SMS
- android.permission.ACCESS_NETWORK_STATE
- android.permission.SEND_SMS
- android.permission.WAKE_LOCK
- android.permission.VIBRATE
- android.permission.RECEIVE_BOOT_COMPLETED
- android.permission.READ_APP_BADGE
- android.permission.ACCESS_COARSE_LOCATION
- android.permission.ACCESS_WIFI_STATE
- ir.ops.breacker.permission.C2D_MESSAGE
- com.google.android.c2dm.permission.RECEIVE
- com.sec.android.provider.badge.permission.READ
- com.sec.android.provider.badge.permission.WRITE
- com.htc.launcher.permission.READ_SETTINGS
- com.htc.launcher.permission.UPDATE_SHORTCUT
- com.sonyericsson.home.permission.BROADCAST_BADGE
- com.sonymobile.home.permission.PROVIDER_INSERT_BADGE
- com.anddoes.launcher.permission.UPDATE_COUNT
- com.majeur.launcher.permission.UPDATE_BADGE
- com.huawei.android.launcher.permission.CHANGE_BADGE
- com.huawei.android.launcher.permission.READ_SETTINGS
- com.huawei.android.launcher.permission.WRITE_SETTINGS
- com.oppo.launcher.permission.READ_SETTINGS
6.2.3 Files and Main Activities

- **ir.ops.breacker.MainActivity**

Entry point of the App. When the user first opens the App, a screen similar to the official “Psiphon” app will appear. If the user presses the “START” button, the App will prompt:

“Proxy not Working in your phone!, PSIPHON deleted successfully”.

The App becomes hidden from the user as if it had been uninstalled\(^{10}\). In reality, the malware is NOT uninstalled, and starts to work: The App starts to send SMSs to the user's contacts asking to download the App\(^{11}\).

\(^{10}\) `getPackageManager().setComponentEnabledSetting(new ComponentName(this, MainActivity.class), PackageManager.COMPONENT_ENABLED_STATE_DISABLED, PackageManager.DONT_KILL_APP);`

\(^{11}\) سلام - این فیلتر شکن روح دانلود گن باهمش میتونی خیلی راحت به تلگرام وصل بنشی http://qqt.ir/psvpn
• `ir.ops.breacker.Main2Activity`: If some criteria is matched at MyPushListener, this Activity is called to send an SMS with data sent by a push notification.

• `ir.ops.breacker.buy`: This Activity is **NOT used** in the app. It seems to do some kind of interaction with various websites\(^{12}\). Perhaps a sign of recycled code.

• `ir.ops.breacker.C1347a`: Used in SmsListener to check if a phone number is equal to another phone number saved in SharedPreferences with key “numberforme”.

• `ir.ops.breacker.C1348b`: Used to subscribe to some topics in the Pushe service.

• `ir.ops.breacker.C1352c`: This class seems to **exfiltrate user data**. It appears to send user’s contact info to an URL sent by a push notification.

• `ir.ops.breacker.C1353g`: Application class. Initiates OneSignal services and has a method to get the DeviceId.

• `ir.ops.breacker.Dialog`: Shows a dialog with text sent by a push notification and does one of two things:
  - Opens a com.farsitel.bazaar page.
  - Sends an SMS.

• `ir.ops.breacker.MyPushListener`: Listens for push notifications and can run:
  - Opens a com.farsitel.bazaar page.
  - Sends an intent with VIEW action to open any app which listens to the criteria sent by the push notification.
  - Opens Dialog class.
  - Opens Main2Activity.
  - Opens MainActivity again.
  - Sends an SMS with data sent by a push notification.
  - Opens WebViewJ to load a website sent by a push notification.
  - Sends an intent with DELETE action to prompt the user a dialog to delete the app sent by a push notification (the user still needs to accept it).
  - Downloads a file specified by a push notification to the Downloads folder.
  - Calls a phone number.
  - Opens a Instagram profile.
  - Sets the current device as “blocked” in SharedPreferences to stop doing everything listed in this class (kill switch).
  - Opens C1348b class.
  - Opens C1352c class.
  - Opens a Telegram profile.

• `ir.ops.breacker.MYreceiver`: Listens to BOOT_COMPLETED action to start the MainActivity when the phone reboots.

• **ir.ops.breacker.NotificationExtenderBareBonesExample**: Does the same things as MyPushListener but using OneSignal services. Also, it can be used to download an APK and install it. It seems to be used to auto-update the app, although it can be used to install any apk.

• **ir.ops.breacker.SmsListener**: Listens to incoming SMS. It seems to send an SMS to a push notification-specified number containing info about two-step verification services.

• **ir.ops.breacker.VideoViewActivity**: Plays a video streaming\(^{13}\).

• **ir.ops.breacker.WebViewJ**: Loads sent websites.

---

\(^{13}\) [http://iptvir.ddns.me:8080/live/3100d95566f1a3e5/3100d95566f1a3e5/3994.m3u8](http://iptvir.ddns.me:8080/live/3100d95566f1a3e5/3100d95566f1a3e5/3994.m3u8)
7 External Links

Psiphon6 Infection
https://urlscan.io/result/3f58299b-02e3-4150-87aa-221f7cbc7722/jsonview/

Psiphon6 Infection and redirect
https://urlquery.net/report/0f6b4c68-3f0e-430d-8068-631c6be3c97b
https://storage.backtory.com/redfox/app-release.apk

VPN Secure APK Distribution
https://s3.us-east-2.amazonaws.com/vpnsecure/vpn.apk

Psiphon6 Distribution
http://serverclient12.tk/dlvpn/vpn.apk

CERTCC Report VPN Secure (Persian)
https://www.certcc.ir/ow_userfiles/plugins/base/attachments/5a606068391bd_5a6060683 8ac5.pdf

Koodous Sample
https://koodous.com/apks/fe91bb6258ddaf63760f69d7b2f48f9561e6f1734023c19e34c5c695bc 95d6d2

Sina Motlagh Code Repository
https://github.com/SinaXhpm

Psiphon6 Breacker sample
https://www.hybrid-analysis.com/sample/2d6bea3fe3b3488310e8b5cb2dab80fac6da1869e8ba793602e8a745ef7fa4 95

Mahware APK (Satellite Fake App)
https://www.hybrid-analysis.com/sample/53cc97ea897d90e3eed43007460944b0df1de9aed3e23029b35c825afd1479 ec
8 Acknowledgements

This research could not be possible without the support of the community. We want to thanks civicert.org for reporting the case and @hooshmandk who provided an early analysis of the events.