UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Research Brief
March 2014

Maliciously Repackaged Psiphon Found

Author: John Scott-Railton

SUMMARY

The Citizen Lab developed the original design of Psiphon, a censorship circumvention software, which was spun out of the lab into a private Canadian corporation (Psiphon Inc.) in 2008. In the past 24 hours, we have identified a **malicious repackaging of the Psiphon 3** circumvention tool. The malware contains both a functioning copy of Psiphon, and the njRAT trojan. When executed, the implant communicates with a Syrian Command and Control server. **This is likely part of a targeted attack against the Syrian opposition by a known actor, not all users of Psiphon**.

Interestingly, this is not the first time we identified a malicious repackaging of circumvention programs in the context of the Syrian conflict. For example, in June 2013 we published a report describing how attackers had maliciously modified the proxy software Freegate.

This brief note describes the implant's appearance and behavior, then explains how to obtain and verify genuine copies of Psiphon 3. The Psiphon team is monitoring the attack, and Karl Kathuria (Psiphon's VP) encourages all new users of Psiphon to check the validity of their client. If in doubt, visit psiphon.ca to download a new copy.

DETAILS AND APPEARANCE OF THE MALWARE

The file name and icon are intended to appear identical to a genuine Psiphon 3 executable file. The malware is believed to be part of an active campaign.

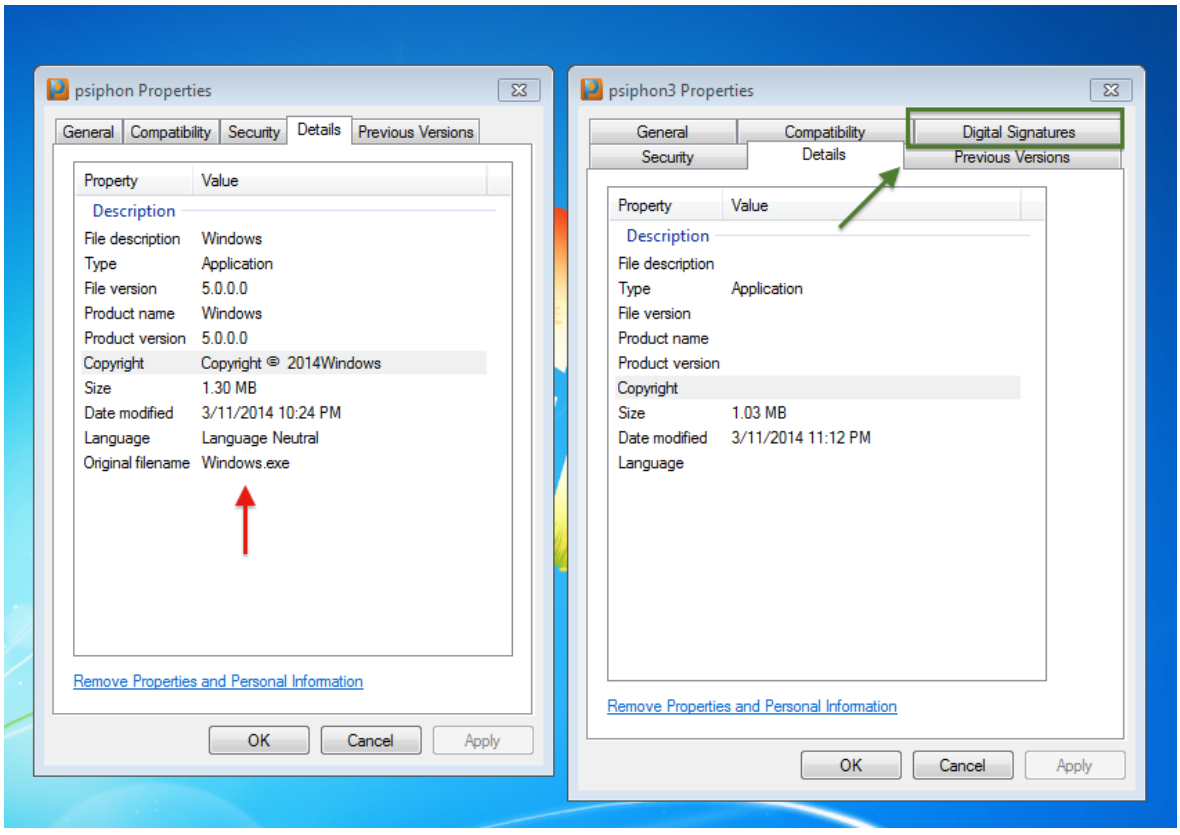
Malicious (left) and genuine (right) Psiphon 3 icons

File Properties

Filename: psiphon.exe
MD5: 28bf01f67db4a5e8e6174b066775eae0

The malware was first observed on the night of 11 March 2014 (Pacific Time): Virus Total has the binary with detection of 3/50 at time of writing.

Examination of the properties of a malicious and genuine Psiphon 3 provides the first clue that the file may not be what it seems. The malicious packaging is unsigned, whereas Psiphon 3 is always signed.



Malicious file (left) and **genuine Psiphon 3 (right)**. Note the original "Windows.exe" file name and the absence of a digital signature in the fake.

The file appears to have been written in Visual Studio, and the PE is .NET dependent. Examination of strings in the binary indicate limited operational security (or deliberate misinformation) on the part of the attackers.

For example:

c:\users\allosh hacker\documents\visual studio 2012\Projects\allosh\allosh\obj\Debug\Windows.pdb

INFECTION & PERSISTENCE

Once executed, the user sees the Psiphon 3 GUI. The malware has, in fact, dropped and executed a *working copy of Psiphon 3* alongside the implant.

Psiphon 3 GUI shown to the victim while the implant is dropped.

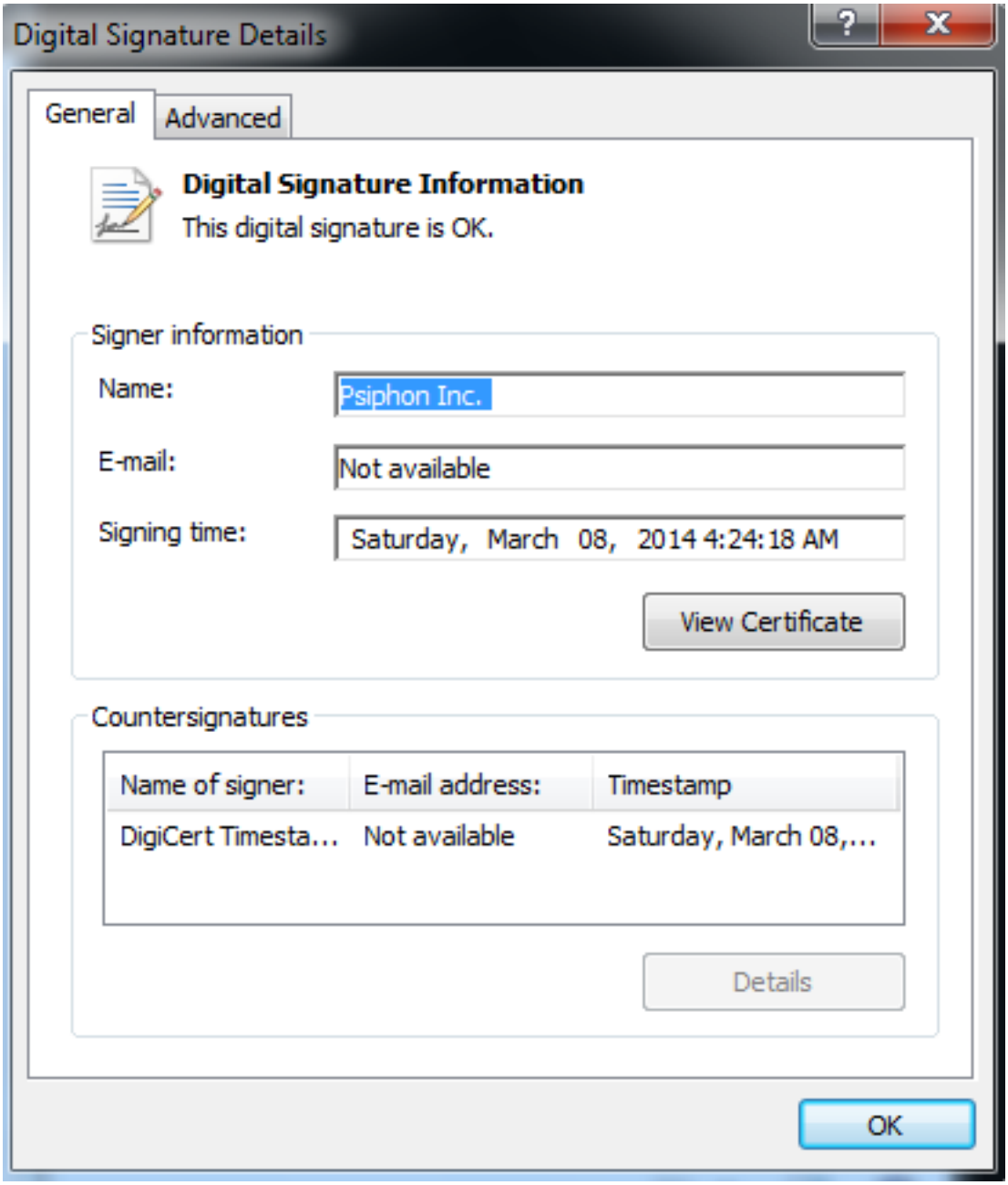
A malicious file is dropped by psiphon.exe into the User's AppData\Local folder:

C:\Users\[USER]\AppData\Local\Tempserver.exe
MD5: e1f2b15ec9f9a282065c931ec32a44b0

Psiphon 3 is dropped and run from the same directory:

C:\Users\[USER]\AppData\Local\Temppsiphon3.exe
MD5: 81287134d7aa541beae4b000d4ab3f19

The Psiphon 3 binary is functional, and is digitally signed by Psiphon. The attacker appears to have used a very recent copy of Psiphon 3.



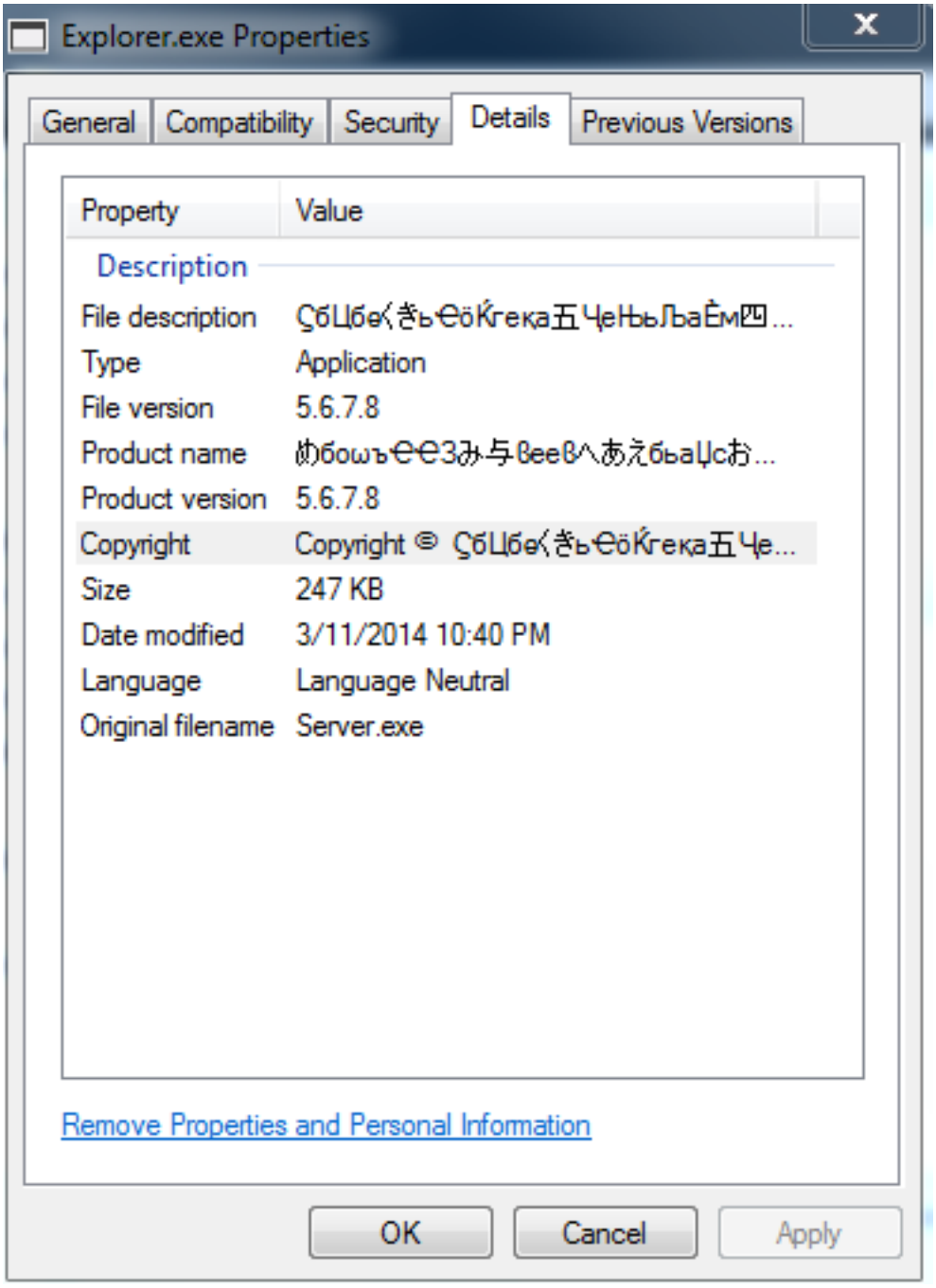
Meanwhile, Tempserver.exe makes the infection permanent by adding a copy of itself to the Windows Startup folder named "chrome.exe."

C:\Users\[User]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\chrome.exe
MD5: e1f2b15ec9f9a282065c931ec32a44b0

Tempserver.exe also copies itself as explorer.exe, and executes the newly created PE implant.

C:\Users\[User]\AppData\Roaming\Explorer.exe
MD5: e1f2b15ec9f9a282065c931ec32a44b0

This file is, in fact, the trojan njRAT.



Properties of explorer.exe (njRAT).

SOME OTHER BEHAVIOR

The implant, explorer.exe, begins collecting keystrokes, and writing the output to a file in the directory it was created in.

C:\Users\[USER]\AppData\Roaming\Explorer.exe.tmp

Here we see the keylogger capturing credentials as the victim enters credentials into Gmail.com via Internet Explorer and writing them to Explorer.exe.tmp.

14/03/12 iexplore Gmail – Windows Internet Explorer
dummy.login[TAP]
dummy.password

Interestingly, the keylogger records "TAB" as "TAP," a behavior that may help in identification.

Among other activities, the implant modifies the Windows Firewall to allow itself access to the network by issuing the following command line to netsh.exe

netsh firewall add allowedprogram "C:\Users\[User]\AppData\Roaming\Explorer.exe" "Explorer.exe" ENABLE

COMMAND & CONTROL

The implant initiates a TCP connection with 31.9.48.141 from port 49189 to the C2 on port 1960. Whois records for this IP address indicate that it is in Syria.

inetnum: 31.9.0.0 – 31.9.127.255
netname: SY-ISP-TARASSUL
descr: Tarassul inetnet Service Provider
country: SY

ANALYSIS

Psiphon 3 is a widely used and trusted circumvention product. It is unsurprising that it, along with other security and communications tools used by Syrian opposition groups, should be maliciously re-purposed. We do not believe this indicates a broader attack against Psiphon 3 users throughout the globe. Instead we suspect this was developed for yet another targeted attack against the opposition. Similarly, njRAT has been widely used by attackers in Syria, and is frequently packaged with dummy or functional programs. The continued targeting of security and communications is insidious: it reflects a well-informed approach to targeting the Syrian opposition with social engineering.

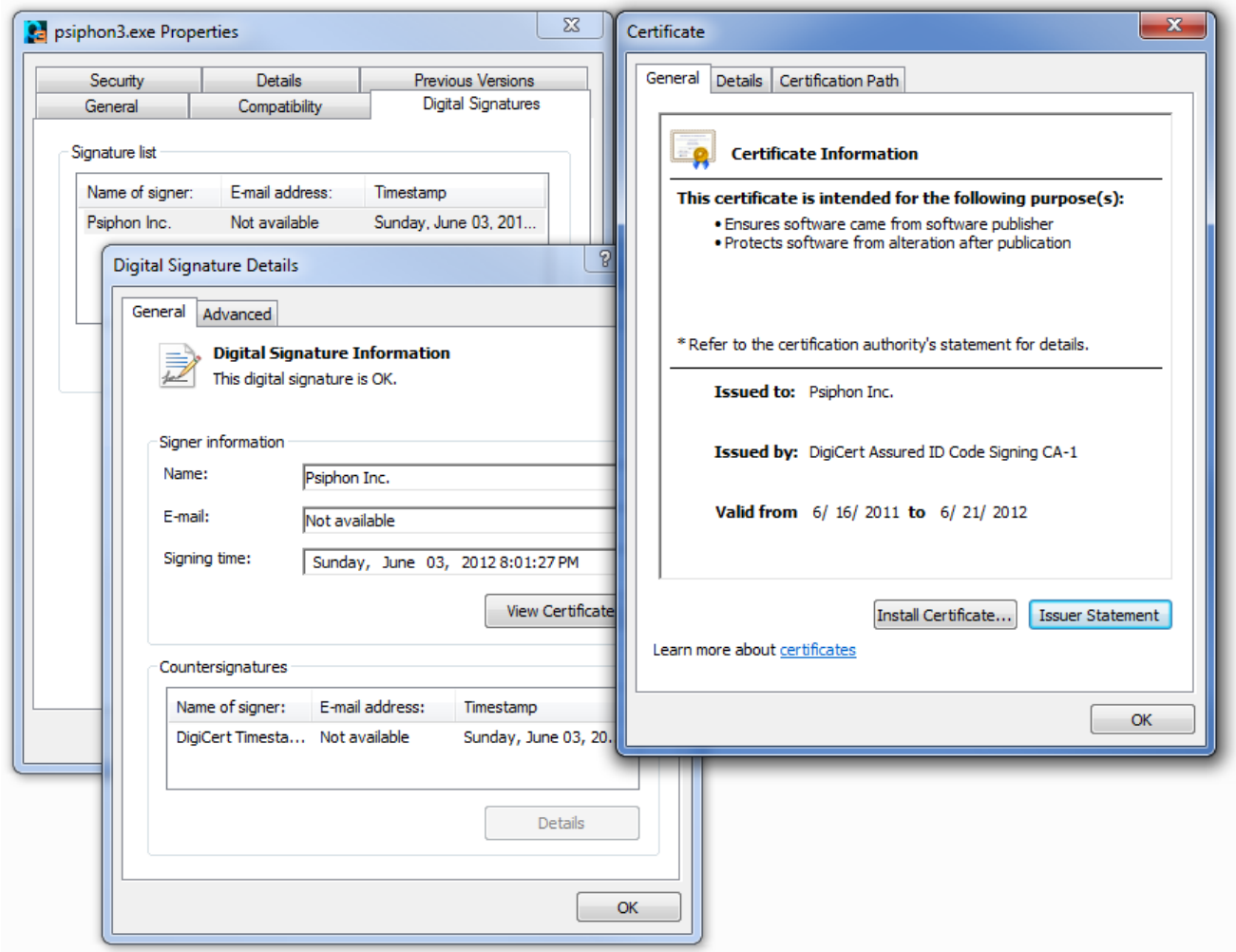
Attacks similar to this are complemented by others using intriguing political or religious content, and other forms of social engineering. Such attacks have been extensively analyzed by my Citizen Lab colleague Morgan Marquis-Boire and reported by Eva Galperin of the EFF, as well as many other researchers. The most recent joint Citizen Lab and EFF report (December 2013) can be found here.

ACTIONS TO TAKE

The developers of Psiphon were notified of the malware and suggest concerned users take the following steps (content adapted from their website).

1. Check your copy of Psiphon for windows by following these simple steps outlined by Psiphon on their website:
2. Right click on the Psiphon icon and select "Properties"
3. You should see a "Digital Signatures" tab. Click it. **If you do not see this tab, you may be looking at malware.**

4. Examine the Digital Signatures Tab. Does it look like the image below? (Click for larger image)



5. Psiphon's website states:"The SHA1 thumbprint for the Psiphon Inc. certificate public key is displayed in the Certificate dialog Details tab. For the certificate valid for the period June 16, 2011 to June 21, 2012 the SHA1 thumbprint is:8f:b7:ef:bd:20:a9:20:3a:38:37:08:a2:1e:0a:1d:2e:ad:7b:ee:6dThe certificate valid for the for the period May 21, 2011 to July 30, 2014 the SHA1 thumbprint is:84:c5:13:5b:13:d1:53:96:7e:88:c9:13:86:0e:83:ee:ef:48:8e:91Psiphon for Windows auto-updates itself, and this process automatically verifies that each update is authentic."
6. Note: while the malware does drop a working copy of Psiphon 3 (with a digital signature), it will be in a different directory than the one you executed Psiphon from (C:\Users\[USER]\AppData\Local\Temppsiphon3.exe)
7. The developers of Psiphon encourage anyone interested in Psiphon 3 to take these steps to ensure their copy of Psiphon is genuine. If in doubt, send a blank email to get@psiphon3.com to receive a new copy. Any questions for Psiphon's developer team can be sent to info@psiphon.ca.

In addition, while the malicious packaging results in a working copy of Psiphon and has a visually indistinguishable icon, the malware also leaves a number of files, any of which should be considered strong evidence of an infection. Here are several to watch out for:

C:\Users\[Your Username]\AppData\Local\Tempserver.exe
C:\Users\[Your Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\chrome.exe
C:\Users\[Your Username]\AppData\Roaming\Explorer.exe
C:\Users\[Your Username]\AppData\Roaming\Explorer.exe.tmp

If these files are found, Machines should be disconnected from the internet and reformatted. Additionally, users should take immediate steps to secure their accounts, as well as contacting others whose sensitive information may have been incidentally exposed.

In addition to these recommendations, we also suggest that, when possible, users make use of 2 factor authentication.

- To learn more about how to enable 2-Factor Authentication, see the links below for guides on how to do this on Facebook, Gmail and Twitter.

2 Factor Tutorial for Facebook
Enable 2 Factor for Gmail
Enable 2 Factor for Twitter

We note, however, that it is difficult for users in Syria to implement 2 factor authentication. The Google Play store is blocked for Syrian users by Google because of current Sanctions and Export Control regulations. This makes it difficult to obtain the 2-factor authentication app. Use of SMS messages as an alternative may present an unacceptable risk of exposure to surveillance. This remains an unresolved problem.

ACKNOWLEDGMENTS

Psiphon Team and Karl Kathuria, Nart Villeneuve (FireEye) for first conclusively identifying this as njRAT, Morgan Marquis-Boire (Citizen Lab), Seth Hardy (Citizen Lab) and Irene Poetranto (Citizen Lab).