Writing Malware

By Aadhithya Kannan
@aadhi0319

disclaimer

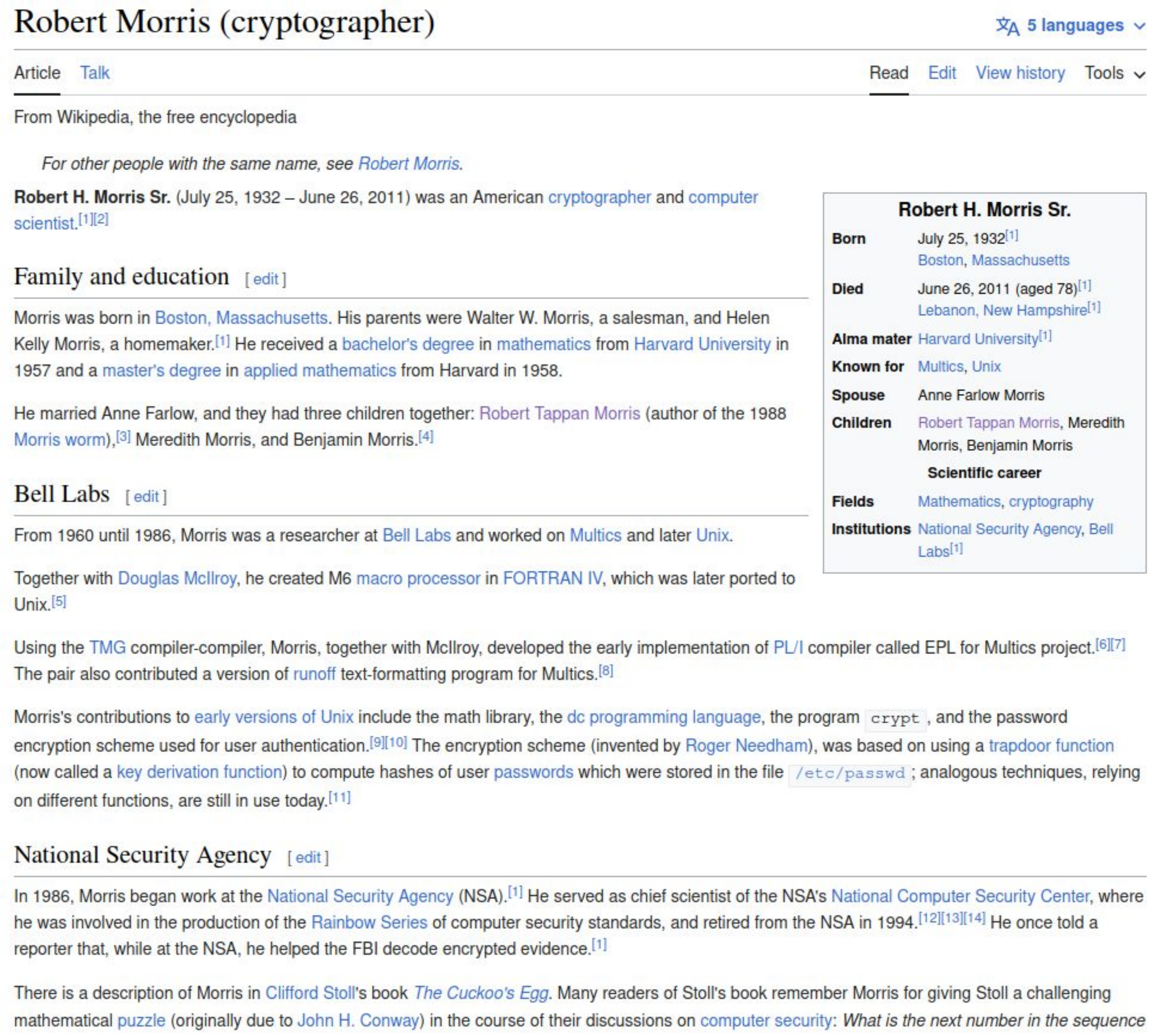
Please don't be malicious. The following information is for educational purposes only.

Origi

1966 - The i
was first pu

1971 - Creep

1988 - Morr



Robert Morris (cryptographer)

From Wikipedia, the free encyclopedia

For other people with the same name, see Robert Morris.

Robert H. Morris Sr. (July 25, 1932 – June 26, 2011) was an American cryptographer and computer scientist.[1][2]

Robert H. Morris Sr.	
Born	July 25, 1932[1] Boston, Massachusetts
Died	June 26, 2011 (aged 78)[1] Lebanon, New Hampshire[1]
Alma mater	Harvard University[1]
Known for	Multics, Unix
Spouse	Anne Farlow Morris
Children	Robert Tappan Morris, Meredith Morris, Benjamin Morris
Scientific career	
Fields	Mathematics, cryptography
Institutions	National Security Agency, Bell Labs[1]

Family and education [edit]

Morris was born in Boston, Massachusetts. His parents were Walter W. Morris, a salesman, and Helen Kelly Morris, a homemaker.[1] He received a bachelor's degree in mathematics from Harvard University in 1957 and a master's degree in applied mathematics from Harvard in 1958.

He married Anne Farlow, and they had three children together: Robert Tappan Morris (author of the 1988 Morris worm),[3] Meredith Morris, and Benjamin Morris.[4]

Bell Labs [edit]

From 1960 until 1986, Morris was a researcher at Bell Labs and worked on Multics and later Unix.

Together with Douglas McIlroy, he created M6 macro processor in FORTRAN IV, which was later ported to Unix.[5]

Using the TMG compiler-compiler, Morris, together with McIlroy, developed the early implementation of PL/I compiler called EPL for Multics project.[6][7] The pair also contributed a version of runoff text-formatting program for Multics.[8]

Morris's contributions to early versions of Unix include the math library, the dc programming language, the program `crypt`, and the password encryption scheme used for user authentication.[9][10] The encryption scheme (invented by Roger Needham), was based on using a trapdoor function (now called a key derivation function) to compute hashes of user passwords which were stored in the file `/etc/passwd`; analogous techniques, relying on different functions, are still in use today.[11]

National Security Agency [edit]

In 1986, Morris began work at the National Security Agency (NSA).[1] He served as chief scientist of the NSA's National Computer Security Center, where he was involved in the production of the Rainbow Series of computer security standards, and retired from the NSA in 1994.[12][13][14] He once told a reporter that, while at the NSA, he helped the FBI decode encrypted evidence.[1]

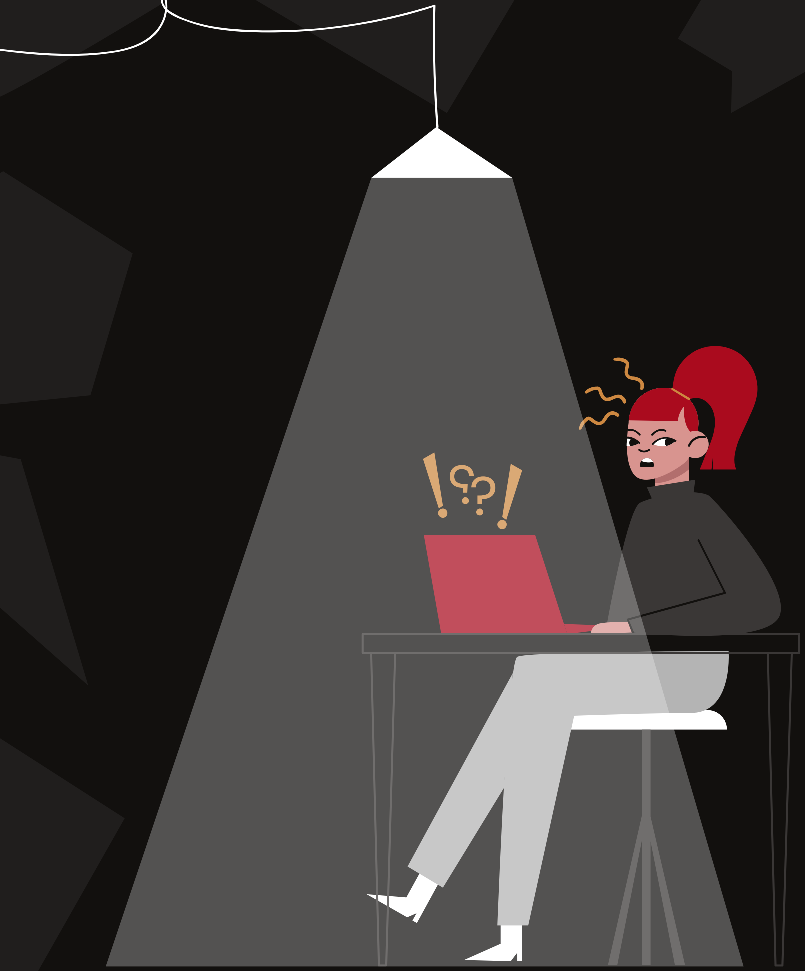
There is a description of Morris in Clifford Stoll's book *The Cuckoo's Egg*. Many readers of Stoll's book remember Morris for giving Stoll a challenging mathematical puzzle (originally due to John H. Conway) in the course of their discussions on computer security: *What is the next number in the sequence*

disclaimer

Please don't be malicious. The following information is for educational purposes only...unless your dad works for the NSA :)

*for all legal purposes, this is a joke

exploits vs malware

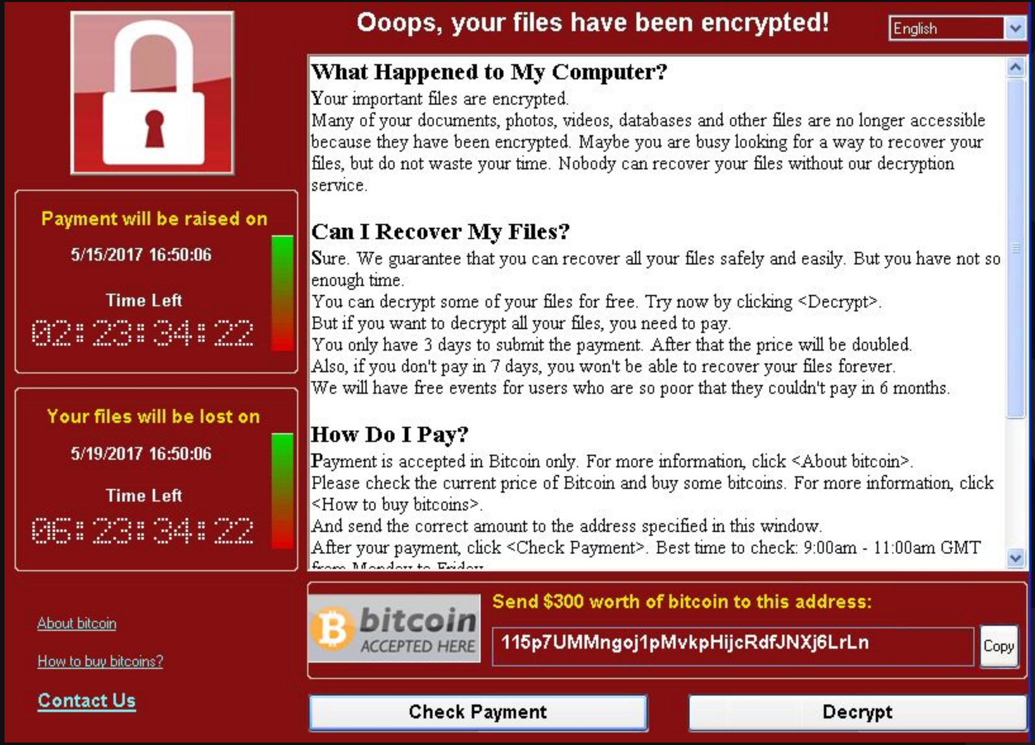


02.

strains

strains

- Ransomware
- Fileless Malware
- Spyware
- Adware
- Trojans
- Worms
- Rootkits
- Keyloggers
- Bots
- Mobile Malware
- Wiper Malware



Payment will be raised on

5/15/2017 16:50:06

Time Left

02:23:34:22

Your files will be lost on

5/19/2017 16:50:06

Time Left

06:23:34:22

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

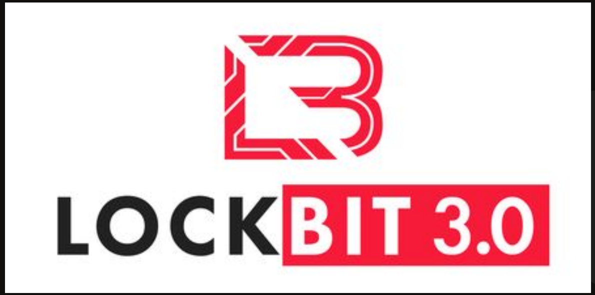
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/

Types of Attackers

Hacktivists

Nation States

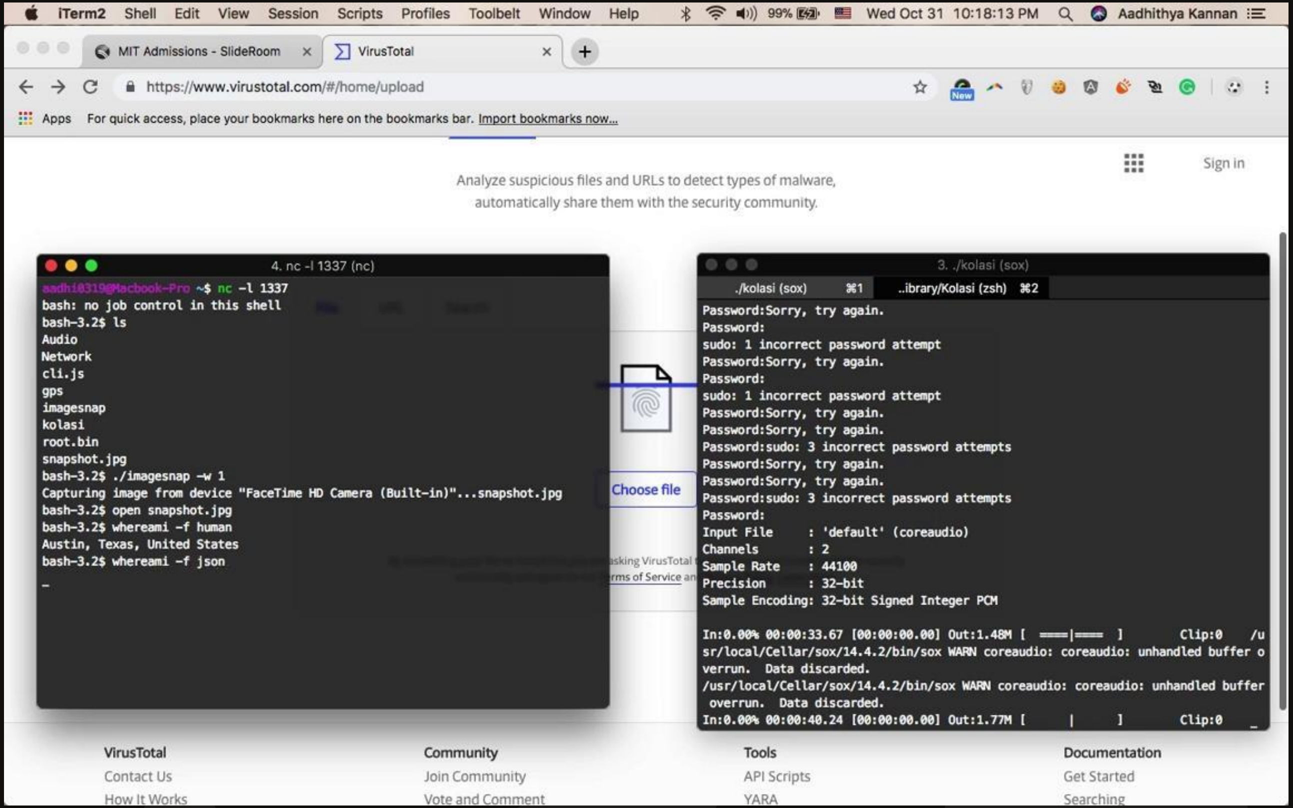


Organized Crime

03.

Detection Stealth Examples

Signatures / Checksums


iTerm2 Shell Edit View Session Scripts Profiles Toolbelt Window Help
99%
Wed Oct 31 10:18:13 PM
Aadhithya Kannan
MIT Admissions - SlideRoom
VirusTotal
https://www.virustotal.com/#/home/upload
New
Apps
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
Sign in
Choose file
VirusTotal
Contact Us
How It Works
Community
Join Community
Vote and Comment
Tools
API Scripts
YARA
Documentation
Get Started
Searching

Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community.

4. nc -l 1337 (nc)

```
aadhi0319@Macbook-Pro ~$ nc -l 1337
bash: no job control in this shell
bash-3.2$ ls
Audio
Network
cli.js
gps
imagesnap
kolasi
root.bin
snapshot.jpg
bash-3.2$ ./imagesnap -w 1
Capturing image from device "FaceTime HD Camera (Built-in)"...snapshot.jpg
bash-3.2$ open snapshot.jpg
bash-3.2$ whereami -f human
Austin, Texas, United States
bash-3.2$ whereami -f json

_
```

3. ./kolasi (sox)

./kolasi (sox) ⌘1 | ..ibrary/Kolasi (zsh) ⌘2

```
Password:Sorry, try again.
Password:
sudo: 1 incorrect password attempt
Password:Sorry, try again.
Password:
sudo: 1 incorrect password attempt
Password:Sorry, try again.
Password:Sorry, try again.
Password:sudo: 3 incorrect password attempts
Password:Sorry, try again.
Password:Sorry, try again.
Password:sudo: 3 incorrect password attempts
Password:
Input File     : 'default' (coreaudio)
Channels       : 2
Sample Rate    : 44100
Precision      : 32-bit
Sample Encoding: 32-bit Signed Integer PCM

In:0.00% 00:00:33.67 [00:00:00.00] Out:1.48M [  ====|====  ]        Clip:0    /u
sr/local/Cellar/sox/14.4.2/bin/sox WARN coreaudio: coreaudio: unhandled buffer o
verrun.  Data discarded.
/usr/local/Cellar/sox/14.4.2/bin/sox WARN coreaudio: coreaudio: unhandled buffer
 overrun.  Data discarded.
In:0.00% 00:00:40.24 [00:00:00.00] Out:1.77M [      |      ]        Clip:0    _
```

Machine Learning

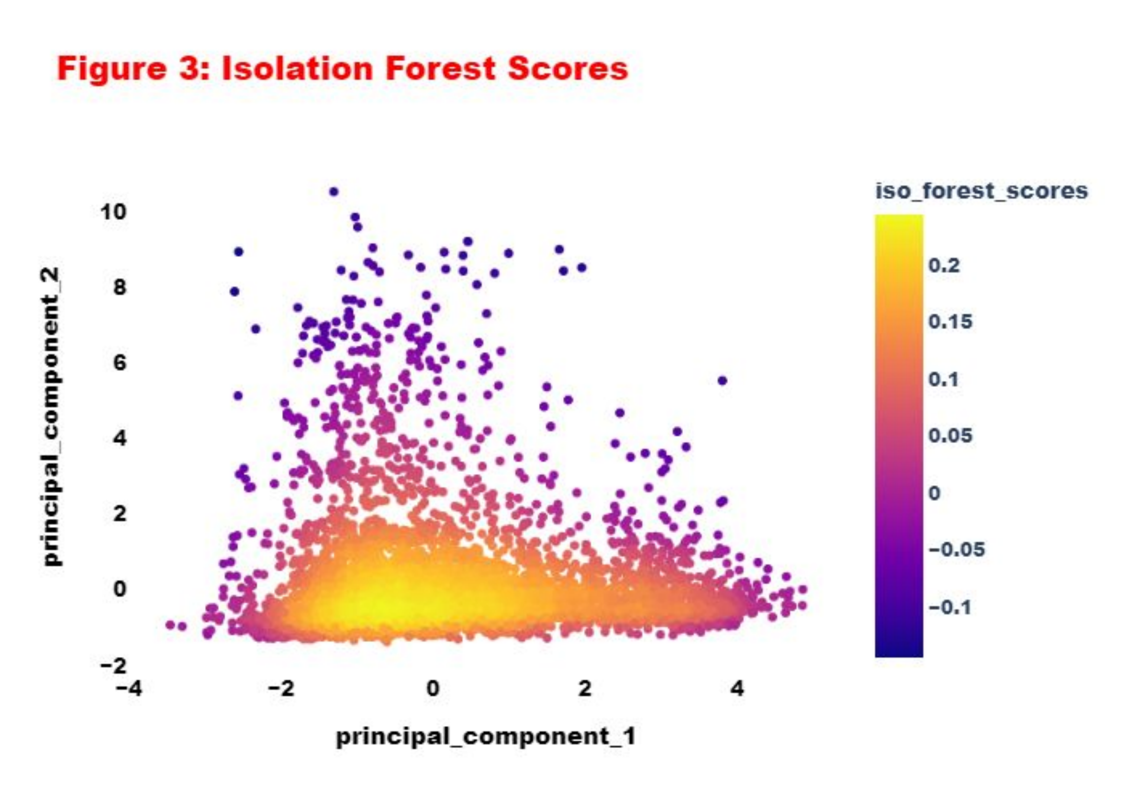
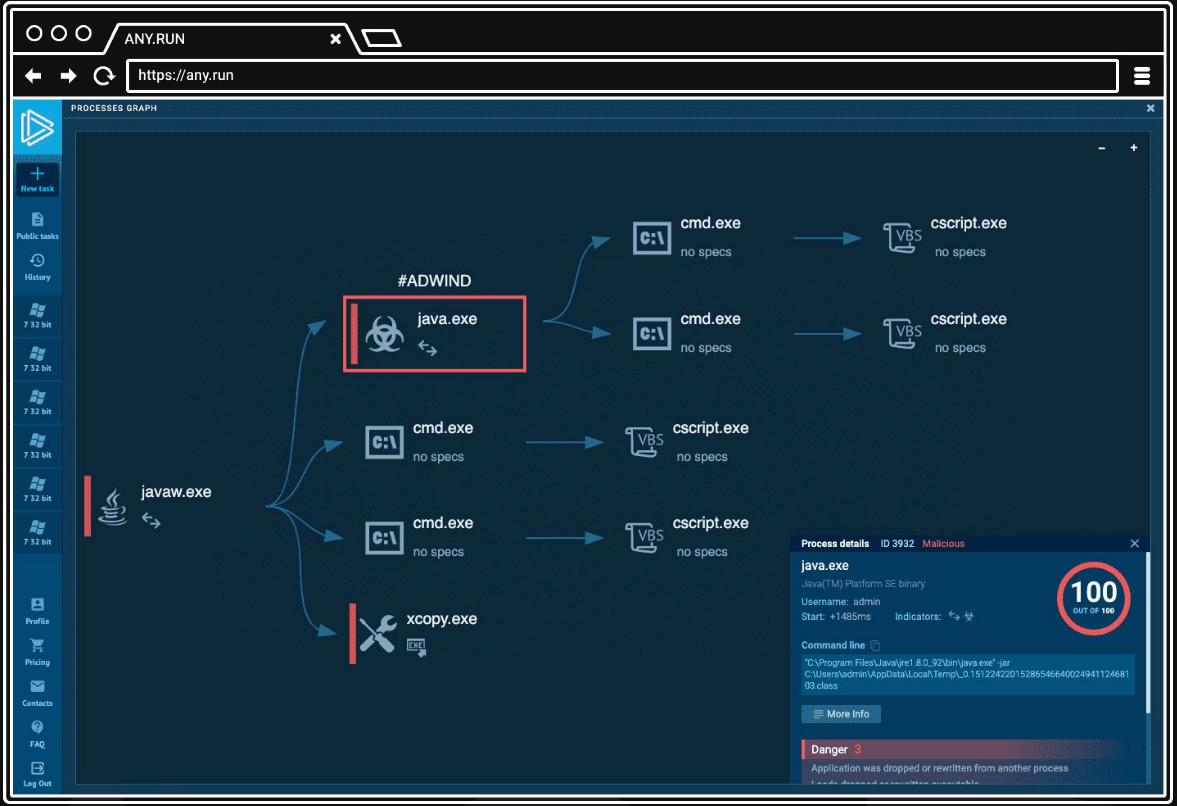


Figure 3: Isolation Forest Scores

Dynamic Analysis



Process details ID 3932 Malicious

java.exe

Java(TM) Platform SE binary

Username: admin

Start: +1485ms Indicators:

100 OUT OF 100

Command line

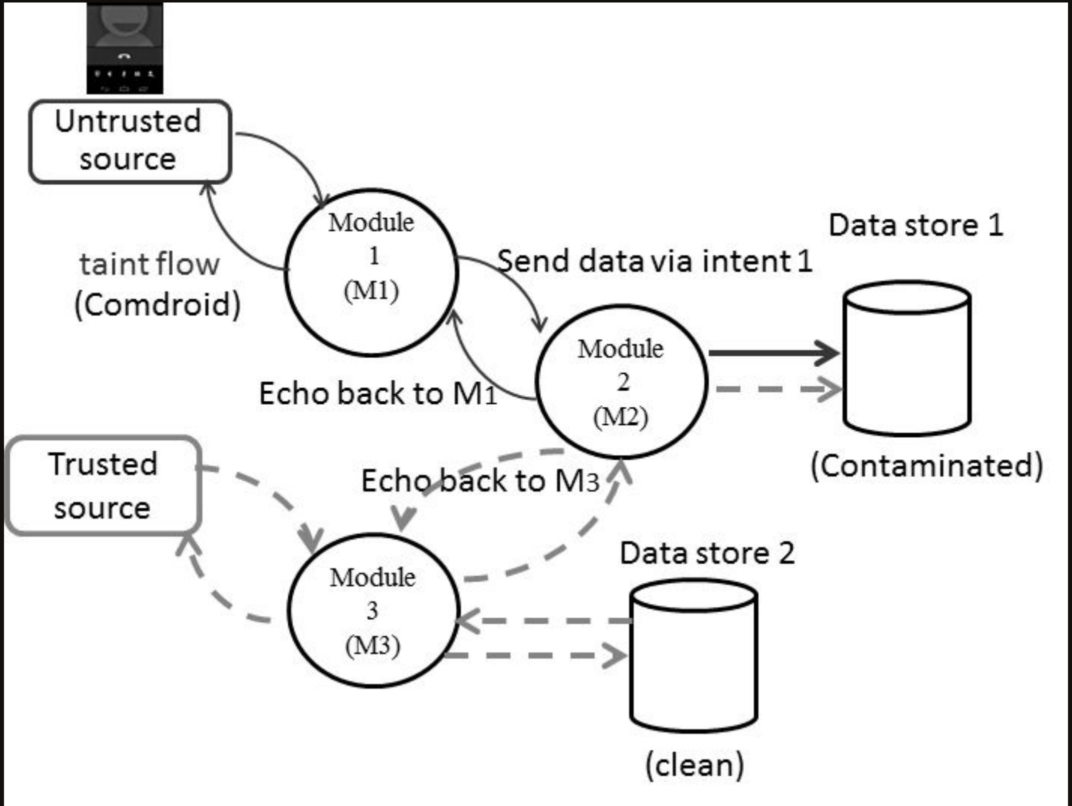
```
"C:\Program Files\Java\jre1.8.0_92\bin\java.exe" -jar
C:\Users\admin\AppData\Local\Temp\_0.151224220152865466400249411246810
3.class
```

Danger 3

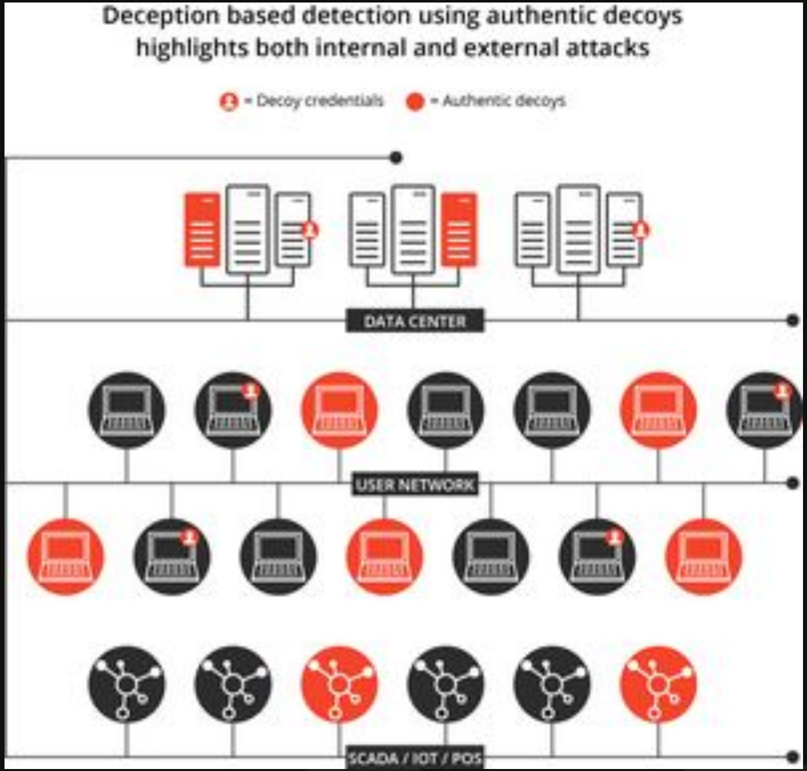
Application was dropped or rewritten from another process

Loads dropped or rewritten executable

Taint Tracking / MAC



Deception Technology

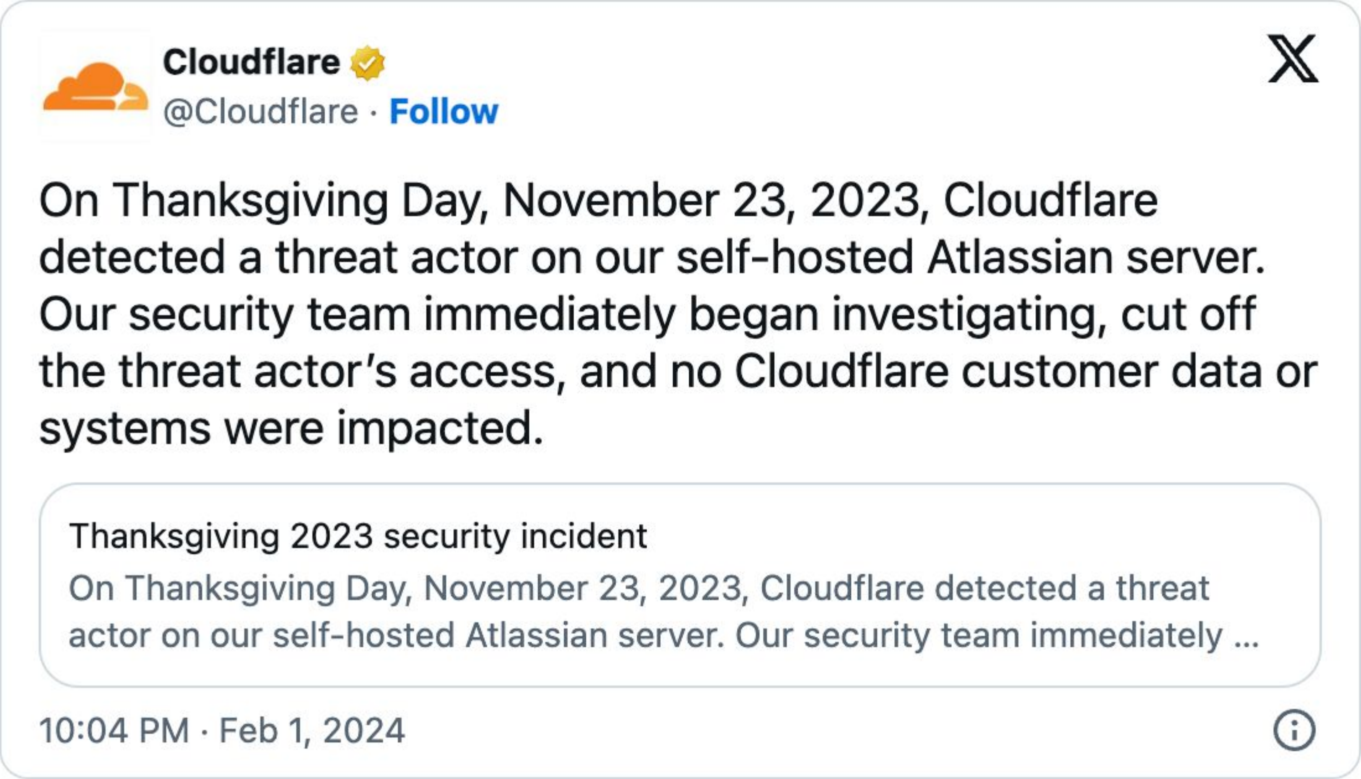


Deception based detection using authentic decoys highlights both internal and external attacks

Security Operations Center

Impact

Impact



Cloudflare

@Cloudflare · Follow

On Thanksgiving Day, November 23, 2023, Cloudflare detected a threat actor on our self-hosted Atlassian server. Our security team immediately began investigating, cut off the threat actor's access, and no Cloudflare customer data or systems were impacted.

Thanksgiving 2023 security incident

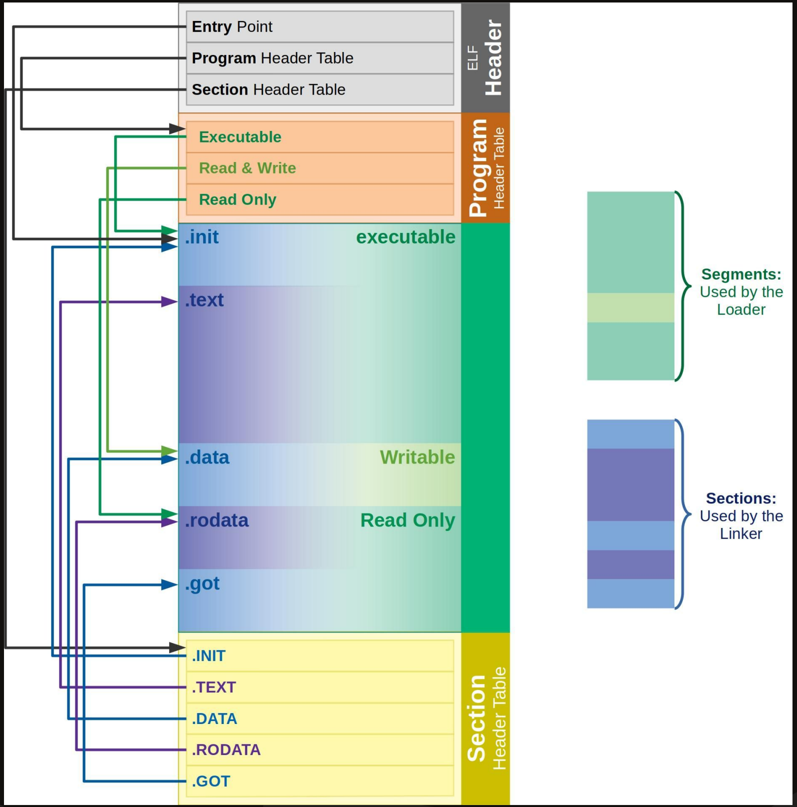
On Thanksgiving Day, November 23, 2023, Cloudflare detected a threat actor on our self-hosted Atlassian server. Our security team immediately ...

10:04 PM · Feb 1, 2024

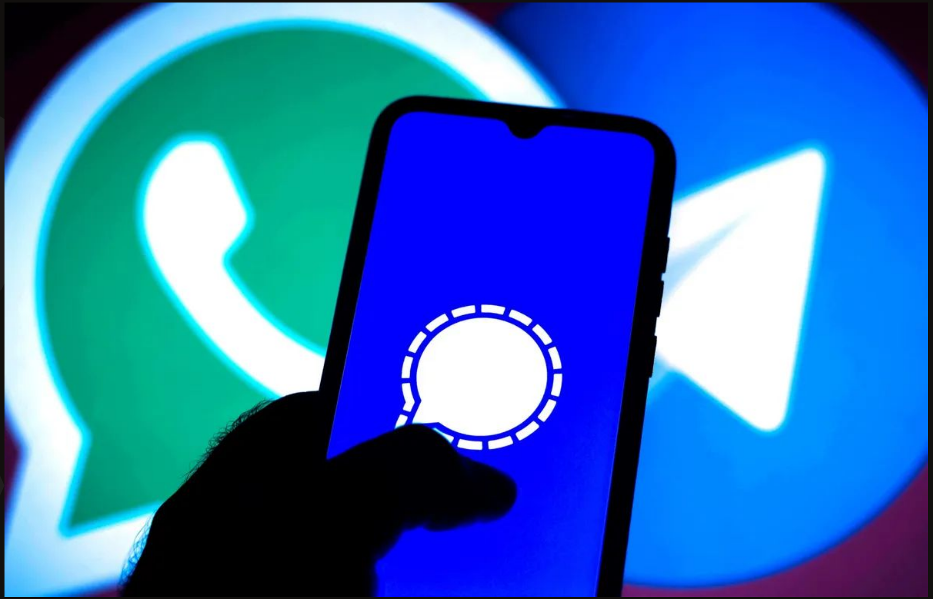
So What Can We Do?

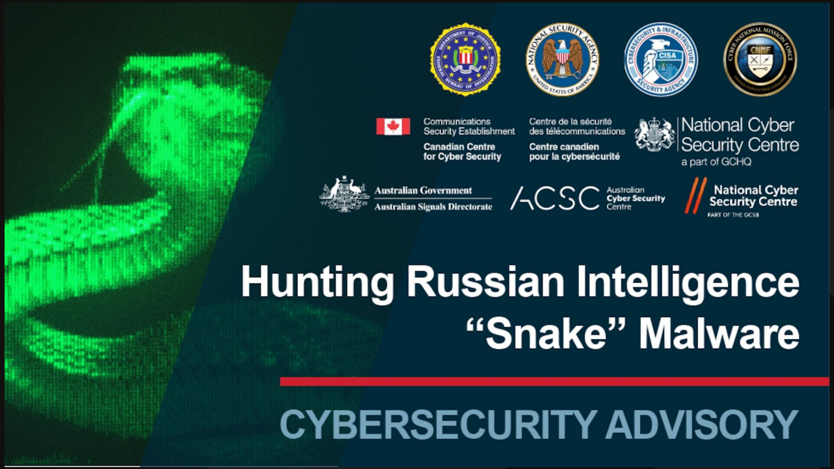
Staying In Memory

- Separate stager and malware
  - Cross compile malware
  - Easily use third party libraries
  - Can easily integrate packer
- Use stager to load and execute memory



Sophisticated Exfiltration





Communications
Security Establishment
Canadian Centre
for Cyber Security

Centre de la sécurité
des télécommunications
Centre canadien
pour la cybersécurité

National Cyber
Security Centre
a part of GCHQ

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

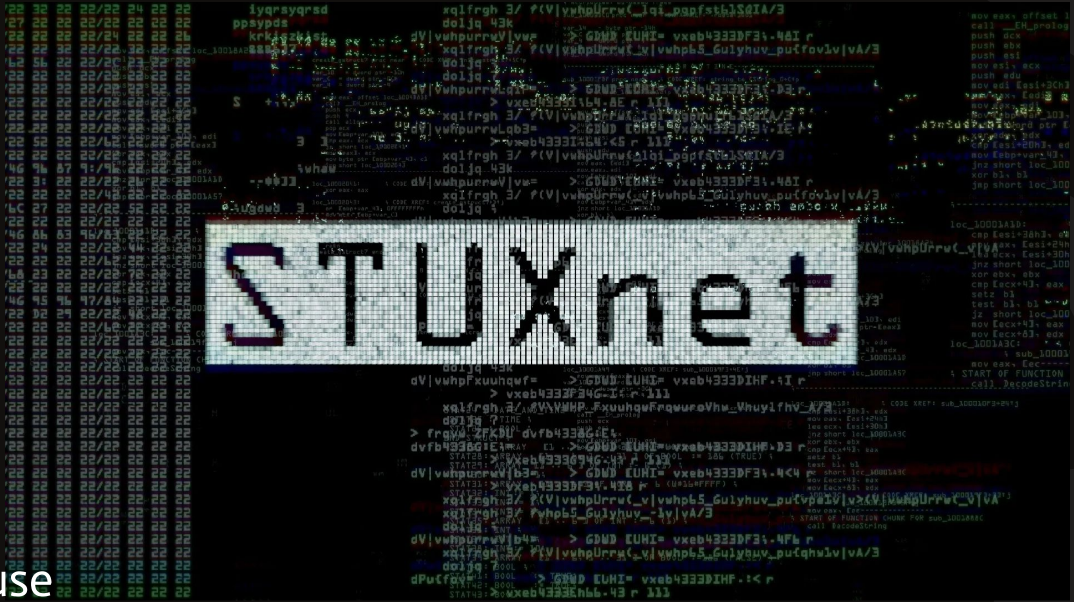
National Cyber
Security Centre
PART OF THE GCSB

Hunting Russian Intelligence “Snake” Malware

CYBERSECURITY ADVISORY

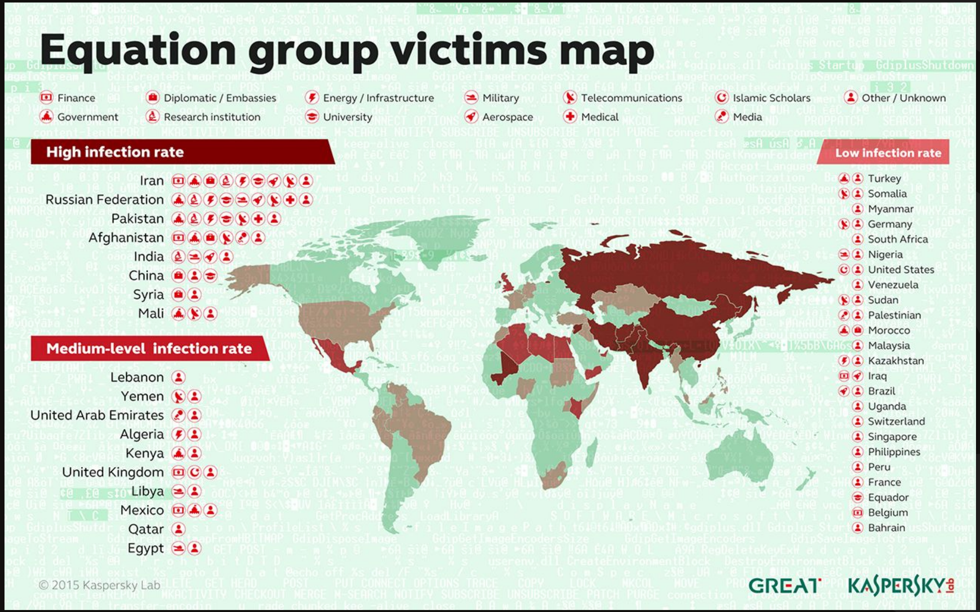
Sandbox / VM / Debugger Detection

- Process arguments
- CPU type
- External devices
- Browser Profiles
- Scan memory for int3
- Registry key checks
- Running processes
- Open network connections
- Environment variables
- Use of keyboard and/or mouse
- Measure uptime
- Delay execution
- Validate targets



Use Crypto

- Encrypt / obfuscate strings
- Encrypt comms
- Don't roll your own crypto – unless you're Equation Group
- Validate C2 using signatures
- Make use of chains of trust
- Garbled Circuits
- Make sure you wipe any keys from memory after use
- Code encryption / obfuscation

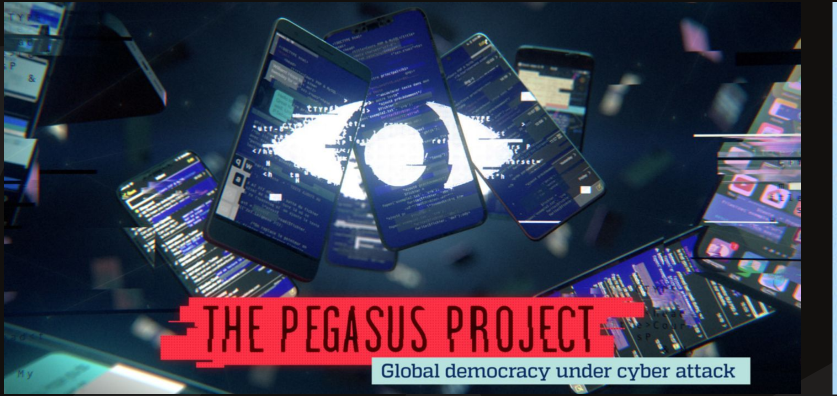


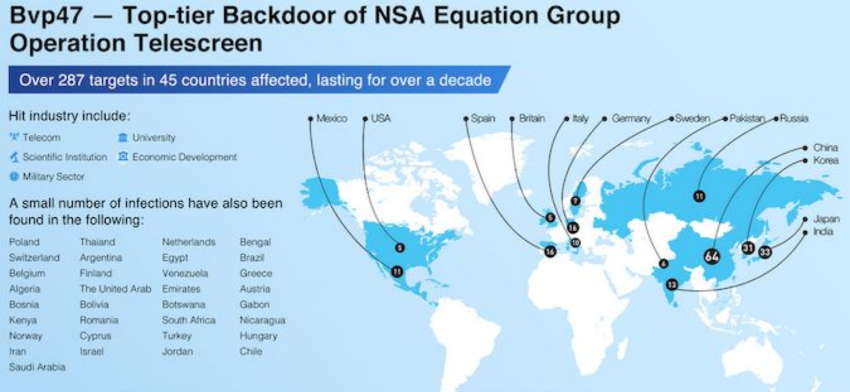
Networking

- TOR
- VPN
- UDP Hole Punching (ZeroTier)
- Reverse TCP
- Include a failsafe bind and a burnoff date

Notable Mentions

SOC PRIME
BPFDOOR MALWARE
Red Menshen APT Leverages Highly-Evasive Backdoor to Spy on Linux Devices





Bvp47 — Top-tier Backdoor of NSA Equation Group
Operation Telescreen

Over 287 targets in 45 countries affected, lasting for over a decade

Hit industry include:

- Telecom
- University
- Scientific Institution
- Economic Development
- Military Sector

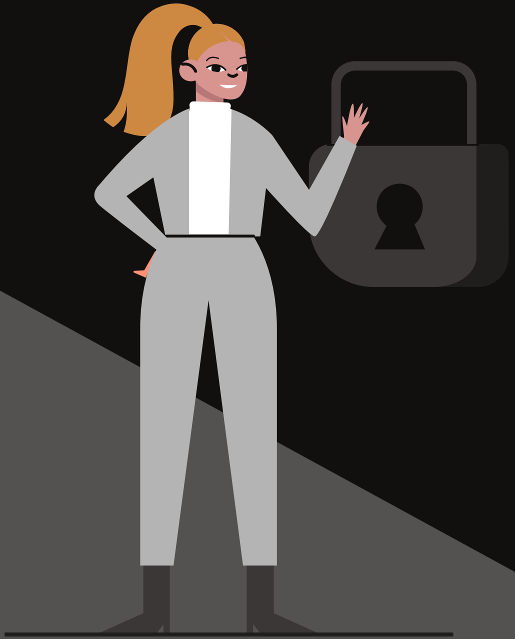
A small number of infections have also been found in the following:

Poland
Switzerland
Belgium
Algeria
Bosnia
Kenya
Norway
Iran
Saudi Arabia

Thaiand
Argentina
Finland
The United Arab
Bolivia
Romania
Cyprus
Israel

Netherlands
Egypt
Venezuela
Emirates
Botswana
South Africa
Turkey
Jordan

Bengal
Brazil
Greece
Austria
Gabon
Nicaragua
Hungary
Chile



04.

Conclusion

Malware is cool. Don't be unethical.
Be creative.

QUESTIONS?