Abuse of Legitimate Security Tools and Health Sector Cybersecurity

October 6, 2022

TLP: WHITE, ID# *202210061300*

Agenda

The same tools used to operate, maintain and secure healthcare systems and networks can also be turned against their own infrastructure.

- Cobalt Strike
- PowerShell
- Mimikatz
- Sysinternals
- Anydesk
- Brute Ratel
- References

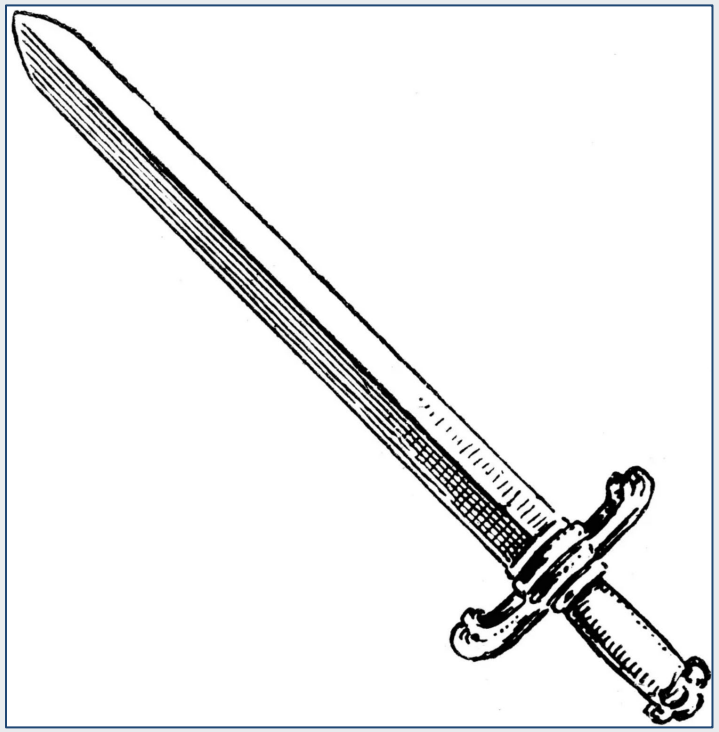
Slides Key:

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

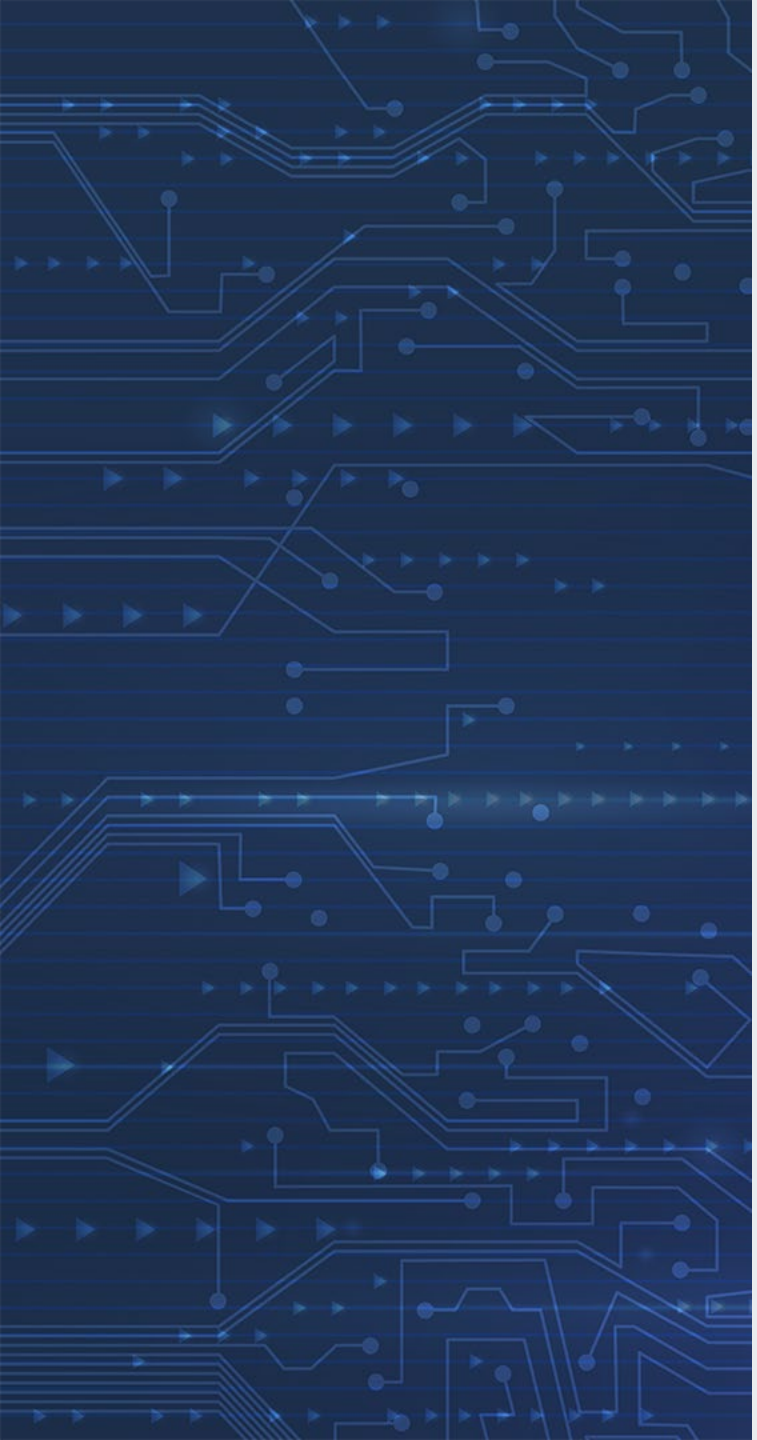
Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

A Few Caveats…

- This presentation is neither an endorsement nor a criticism of the tools that are described.
  - The HHS has no position on the legitimate use of these or any other open source or vendor tools/capabilities. Each should be evaluated based on its own merits and drawbacks.
  - This is also not a condemnation of these tools nor is it a call for healthcare organizations to avoid them. They have value, as evidenced by their popularity.
- Ultimately, healthcare organizations should weigh the risks and rewards of each of these tools and be aware of both the value and risk they bring with them.



The proverbial double-edged sword cuts both ways.
(image source: US adult literacy)



Cobalt Strike

Red-team framework for adversary simulation

Cobalt Strike Background

"Since its introduction, Cobalt Strike has become one of the most prevalent threat emulation software packages used by infosec red teams." – Dark Reading

- Created in 2012 by Raphael Mudge; one of the first widely-available red team frameworks
- Offered as a penetration testing/red team tool to simulate an attack
  - Used for risk/vulnerability assessments
- Abused with increasing frequency against many industries, including the Healthcare and Public Health (HPH) sector
  - Used by many threat actors who target the HPH sector specifically
    - Ransomware operators and Advanced Persistent Threats (APTs)
- Cobalt Strike has many functions – we will only cover a few in this presentation
  - For full coverage, please see our Cobalt Strike presentation: https://www.hhs.gov/sites/default/files/cobalt-strike-tlpwhite.pdf

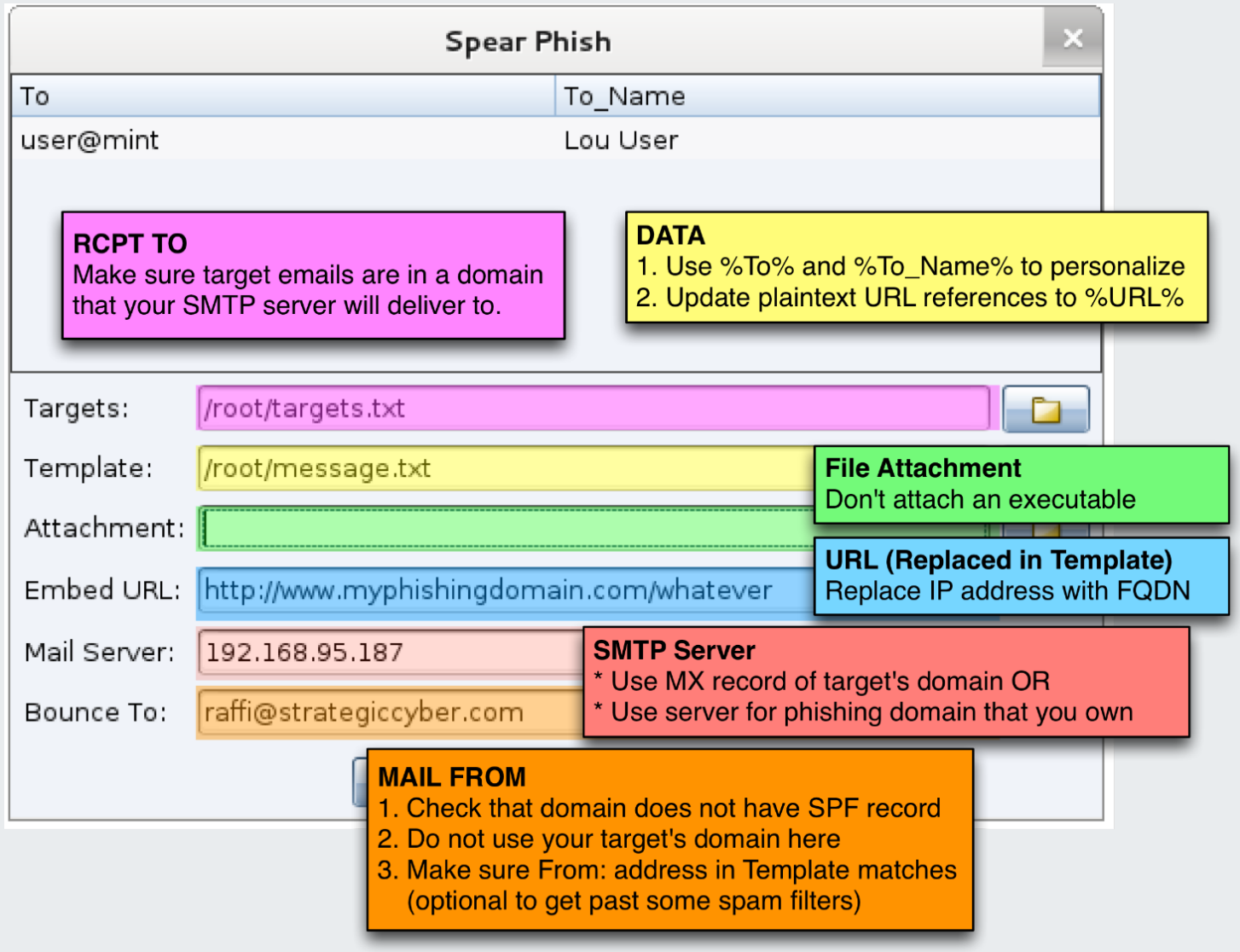
Cobalt Strike as a Spear Phishing Tool

Cobalt Strike is capable of emulating one of the most prolific infection vectors – phishing.

This capability is highly customizable and can therefore simulate many environments.

More information can be found here:

https://hstechdocs.helpsystems.com/manuals/cobaltstrike/current/userguide/content/topics/init-access_spear-phishing.htm



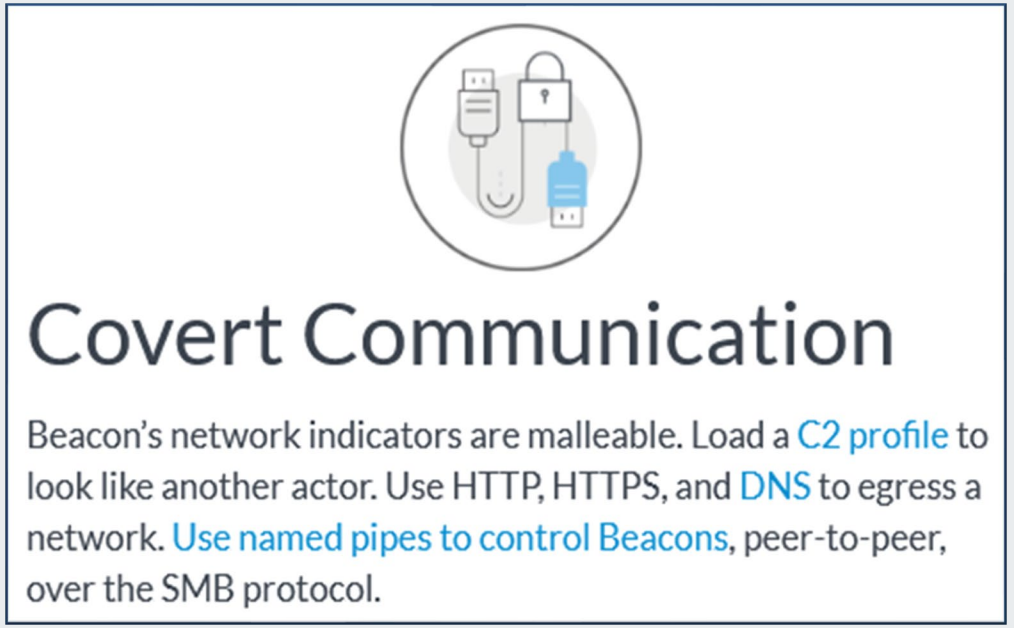
Cobalt Strike: Beacon

Cobalt Strike's beacon, a malleable command-and-control server, is the primary tool used for adversary emulation, allowing for several exploitation and post-exploitation capabilities.

Beacon can discover client-side applications and conduct exploitation/post-exploitation activities.

Beacon can:

- Load a malleable command and control profile
- Uses HTTP/HTTPS/DNS to egress a network
- Use named pipes to control Beacons, peer-to-peer, over server message block (SMB)
- More information: https://www.cobaltstrike.com/blog/beacon-an-operators-guide/



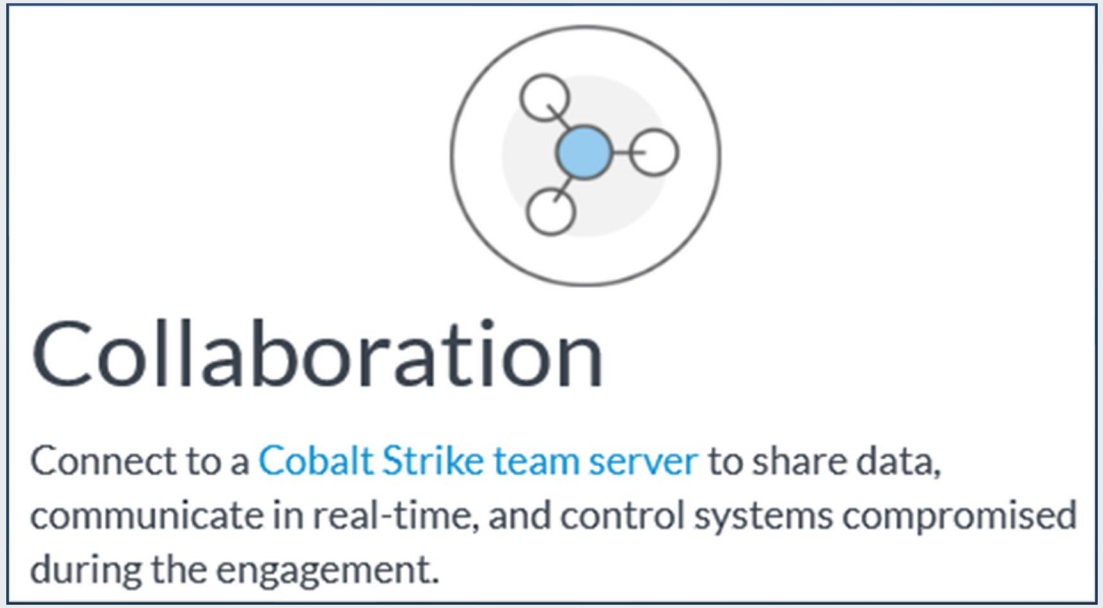
Cobalt Strike: Team Server

What is collaboration with regards to Cobalt Strike? For Cobalt Strike, collaboration is the ability of the two components of the tool (client and server) to communicate and work with each other.

Cobalt Strike Team Server controls the Beacon and the host for its social engineering capabilities.

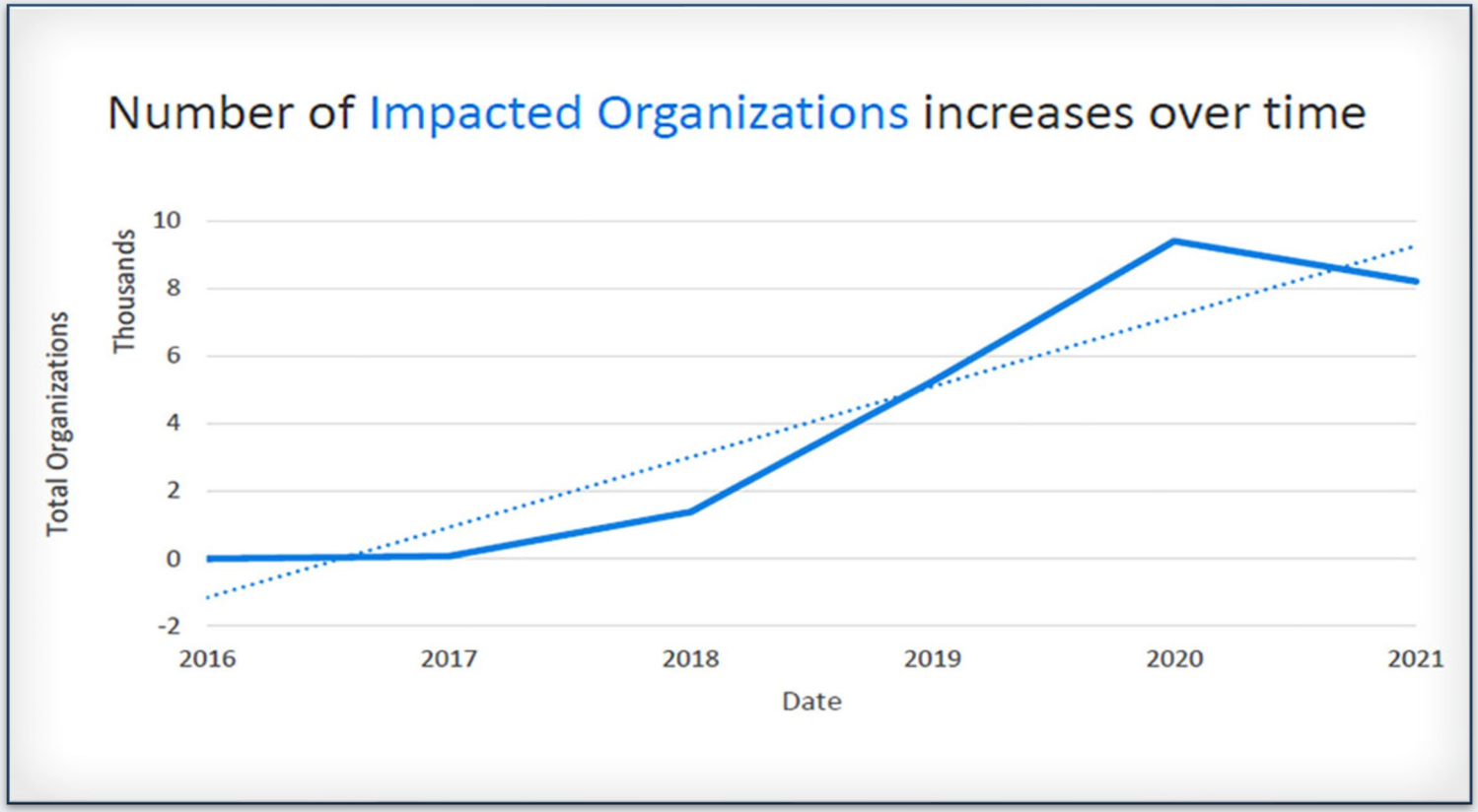
The Cobalt Strike Team Server allows for:

- Data transfers
- Real-time communications
- Command/control of compromised systems
- More information: https://hstechdocs.helpsystems.com/manuals/cobaltstrike/current/userguide/content/topics/welcome_starting-cs-team-server.htm



Cobalt Strike Malicious Usage: 2017 – 2021

Cobalt Strike has been increasingly used for malicious purposes over the last five years.



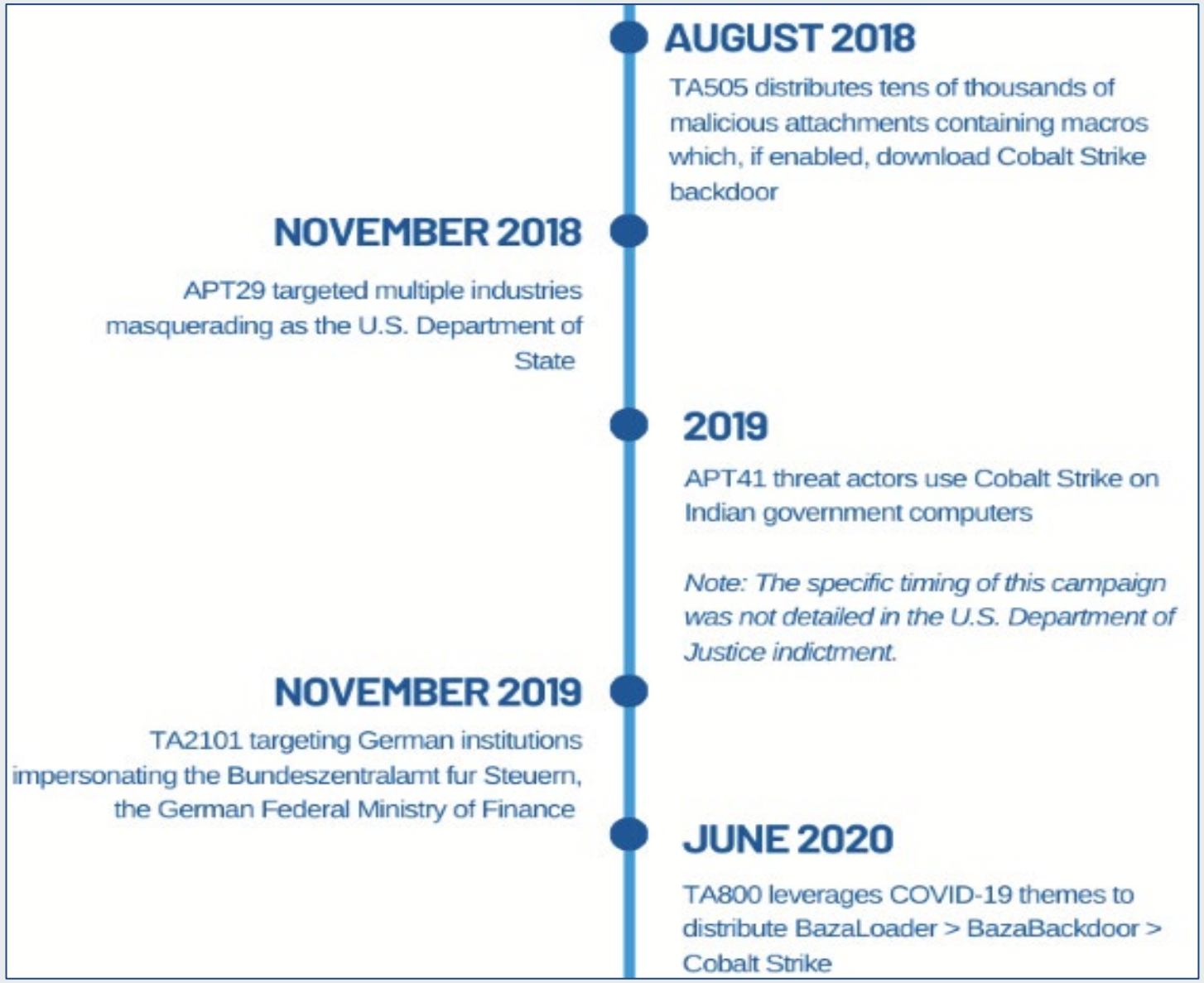
Data courtesy of Proofpoint

Noteworthy Cobalt Strike Attacks: 2016 – 2018

Cobalt Strike has been increasingly used for malicious purposes over the last five years.

Noteworthy Cobalt Strike Attacks: 2018 – 2020

Cobalt Strike has been increasingly used for malicious purposes over the last five years.



Noteworthy Cobalt Strike Attacks: 2020 – 2021

Cobalt Strike has been increasingly used for malicious purposes over the last five years.

Cobalt Strike: Threat Actors

Cobalt Strike is used maliciously by several state-sponsored actors and cybercriminal groups, many of whom pose a significant threat to the health sector.

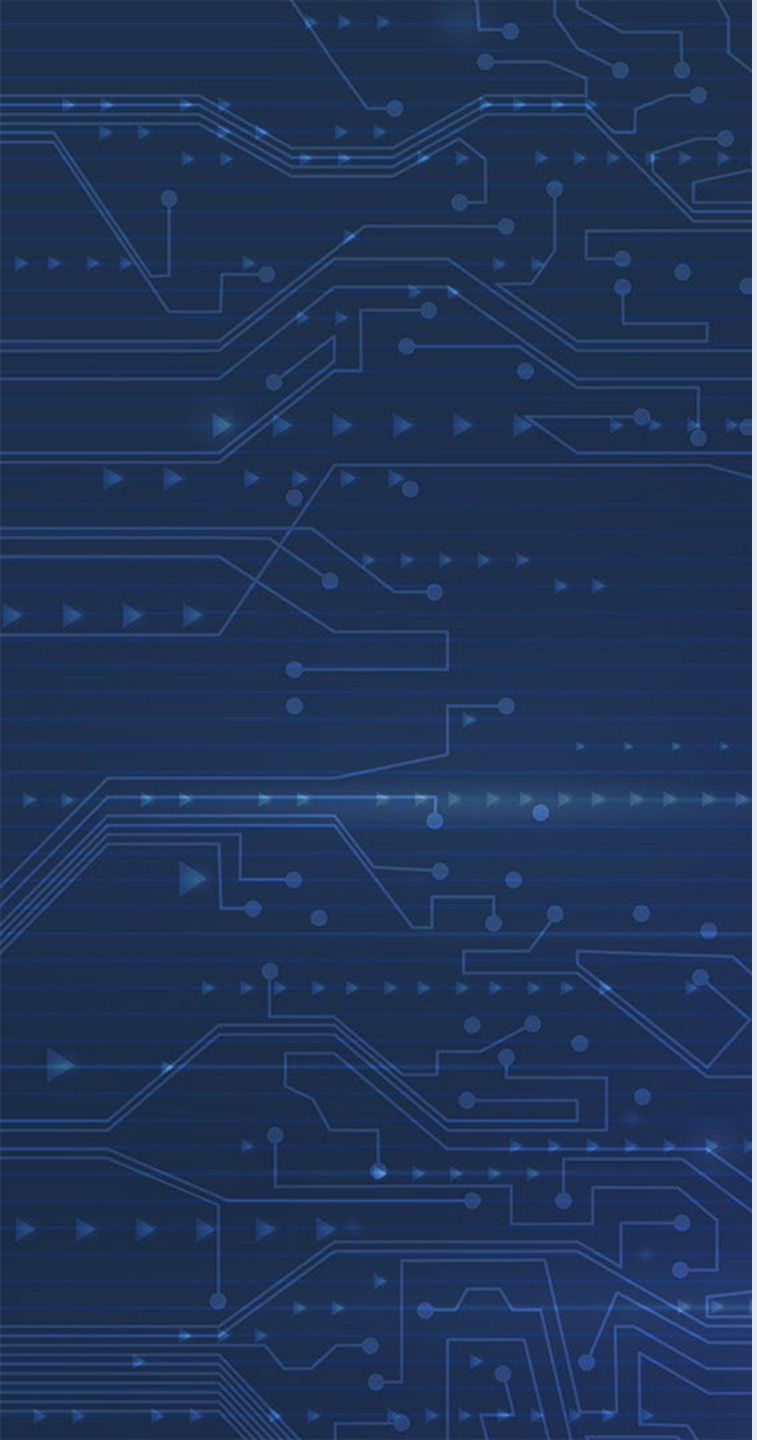
THREAT ACTOR (associations are not 100% confidence)	APPROXIMATE ATTRIBUTION
APT29, Dukes, Group 100, Cozy Duke, EuroAPT, CozyCar, Cozer, Office Monkeys, OfficeMonkeys, Cozy Bear, The Dukes, Minidionis, SeaDuke, Hammer Toss, YTTRIUM, Iron Hemlock, Grizzly Steppe	Russian Intelligence Agency (Possibly Federal Security Service [FSB] or their Foreign Intelligence Service [SVR])
APT32, OceanLotus Group, Ocean Lotus, OceanLotus, Cobalt Kitty, APT-C-00, SeaLotus, Sea Lotus, APT-32, Ocean Buffalo, POND LOACH, TIN WOODLAWN, BISMUTH	Vietnamese government
FIN7, Carbanak, Anunak, Carbon Spider, Gold Waterfall	Cybercriminal group (Ukraine-based)
Cobalt Group, Cobalt Gang, GOLD KINGSWOOD, COBALT SPIDER	Cybercriminal group (Unknown location but possibly Russia/CIS)
UNC1878, RYUK, FIN12	Cybercriminal group (Likely located in Russia/CIS)
FIN6, SKELETON SPIDER, ITG08, MageCart Group 6, White Giant, GOLD FRANKLIN	Cybercriminal group (Unknown location)

Cobalt Strike: Threat Actors

THREAT ACTOR (associations are not 100% confidence)	APPROXIMATE ATTRIBUTION
Leviathan, TEMP.Periscope, TEMP.Jumper, APT40, BRONZE MOHAWK, GADOLINIUM, Kryptonite Panda	Chinese Ministry of State Security's (MSS) Hainan State Security Department
BRONZE PRESIDENT, HoneyMyte, Red Lich, Mustang Panda	Chinese government
APT 19, KungFu Kittens, Black Vine, Group 13, PinkPanther, Sh3llCr3w, BRONZE FIRESTONE, Shell Crew, Deep Panda	Chinese government
APT10, MenuPass, Menupass Team, menuPass, menuPass Team, happyyongzi, POTASSIUM, DustStorm, Red Apollo, CVNX, HOGFISH, Cloud Hopper, BRONZE RIVERSIDE, Stone Panda	Chinese government
Winnti, Axiom, APT17, and Ke3chang	Chinese government
APT41 (possibly BARIUM and Winnti Group)	Chinese government
DarkHydrus, LazyMeerkat, ATK77 (APT 19, Deep Panda, C0d0so0 and Turbine Panda, APT 26, Shell Crew, WebMasters, KungFu Kittens)	Iranian government
CopyKittens, Slayer Kitten	Iranian government

Cobalt Strike: Protection/Detection

- Cobalt Strike's versatility makes defense a headache
  - How do you contain so many capabilities at once?
    - Apply resources knowing that containment is not nearly sufficient
    - The MITRE D3FEND framework can be helpful for general guidance: https://d3fend.mitre.org/
  - Prevention, detection and containment are paramount
- How do you prevent Cobalt Strike from being used maliciously on your infrastructure?
  - Reduce attack surface against common infection vectors such as phishing, known vulnerabilities, and remote access capabilities
- How do you detect Cobalt Strike?
  - Signatures for intrusion detection and endpoint security systems
  - YARA Rules:
    - Intel471: Cobalt Strike - A Toolkit for Pentesters Whitepaper: https://intel471.com/resources/whitepapers/cobalt-strike-a-toolkit-for-pentesters
    - Technical Analysis of Operation Diànxùn: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-dianxun.pdf

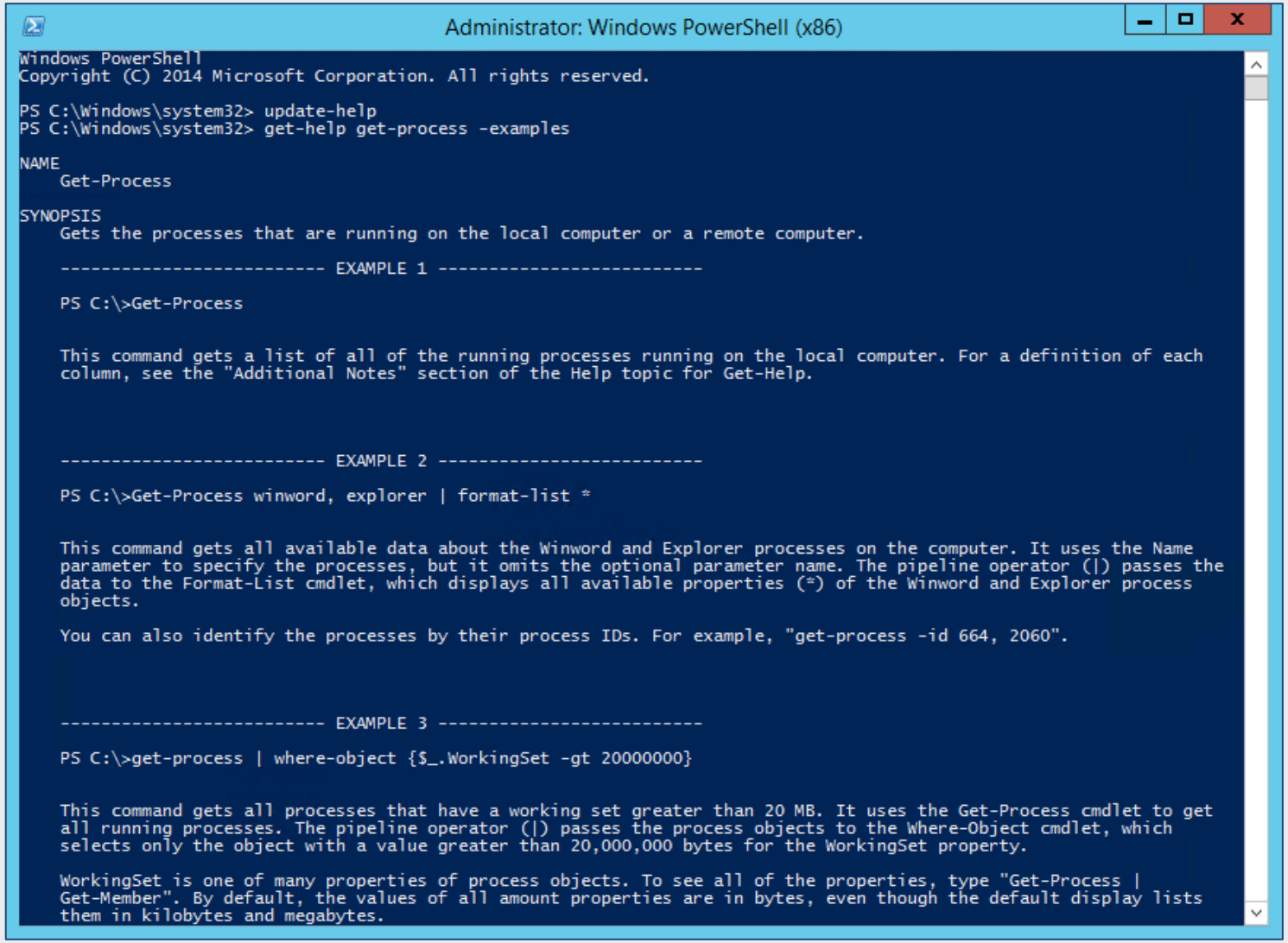


PowerShell

A Microsoft scripting language and command-line tool for configuration management and task automation

PowerShell Basics

- Command shell and scripting language
- Automation and configuration management
- Microsoft developed a command line interface in 2002 called Monad
- Monad renamed PowerShell in 2006
- Made open-source and cross-platform in 2016
- Includes extensive help (similar to manpages)



PowerShell Cmdlets

These cmdlets give administrators the ability to manage their networks, but also allow for opportunities for attackers to compromise resources.

More information on cmdlets can be found here:

https://learn.microsoft.com/en-us/powershell/scripting/developer/cmdlet/cmdlet-overview?view=powershell-7.2

- **Active Directory (module):** This module is used by PowerShell to extend management capabilities to Active Directory objects, including computers, users, and groups and attributes stored within accounts.
- **Exchange Server (module):** This module is used by PowerShell to enable full administration of Exchange Servers. Included within the module are additional cmdlets that fully support all aspects of your Exchange email server.
- **Get-Help (cmdlet):** This built-in cmdlet within PowerShell core provides helpful information, including syntax use and examples of commands and what they accomplish.
- **Get-Command (cmdlet):** When executed, this built-in cmdlet within PowerShell core provides a list of commands that are available. It's useful in identifying which commands are available for each module.
- **Set-Variable (cmdlet):** This built-in cmdlet within PowerShell allows the user to create variables used to store data, such as file paths, multiple objects, or snippets of code you wish to reuse.
- **Invoke-Command (cmdlet):** This built-in cmdlet within PowerShell calls upon another cmdlet, usually run from a local computer, to execute the invoked command on remote computers.
- **Pipeline (|):** One of the features of PowerShell is the ability to chain commands together by means of the pipe character. Piping commands causes PowerShell to run the first part of the command and then output the results for use by the second command and so on until the entire sequence is run. It is useful when performing a multiple-step task, such as creating a username, adding the username to a security group, and resetting the default password.
- **Function ({ }):** Similar to the pipeline feature in that cmdlets may be linked together, functions allow for greater control over the scripting process. By wrapping cmdlets in braces, a function is created that serves to run the sequence one or more times.
- **Out-File (cmdlet):** This built-in cmdlet within PowerShell allows a command's output to be exported to a file. Typically used with the pipe feature, a user can get a list of user accounts that are disabled in Active Directory, for example, and export that list to a text file for future use.
- **Import-Module (cmdlet):** This built-in cmdlet within PowerShell imports one or more modules into PowerShell to further its feature set, cmdlets, and functionality.
- **Third-party Modules:** Software developers can program code to group multiple cmdlets together as Third-party modules that are imported into PowerShell to extend functionality and support for specific applications. Notable third-party modules exist from VMware (virtualization), Dell (PowerEdge servers), and PowerSploit (Security/Pentesting).

Threat Actors Using PowerShell

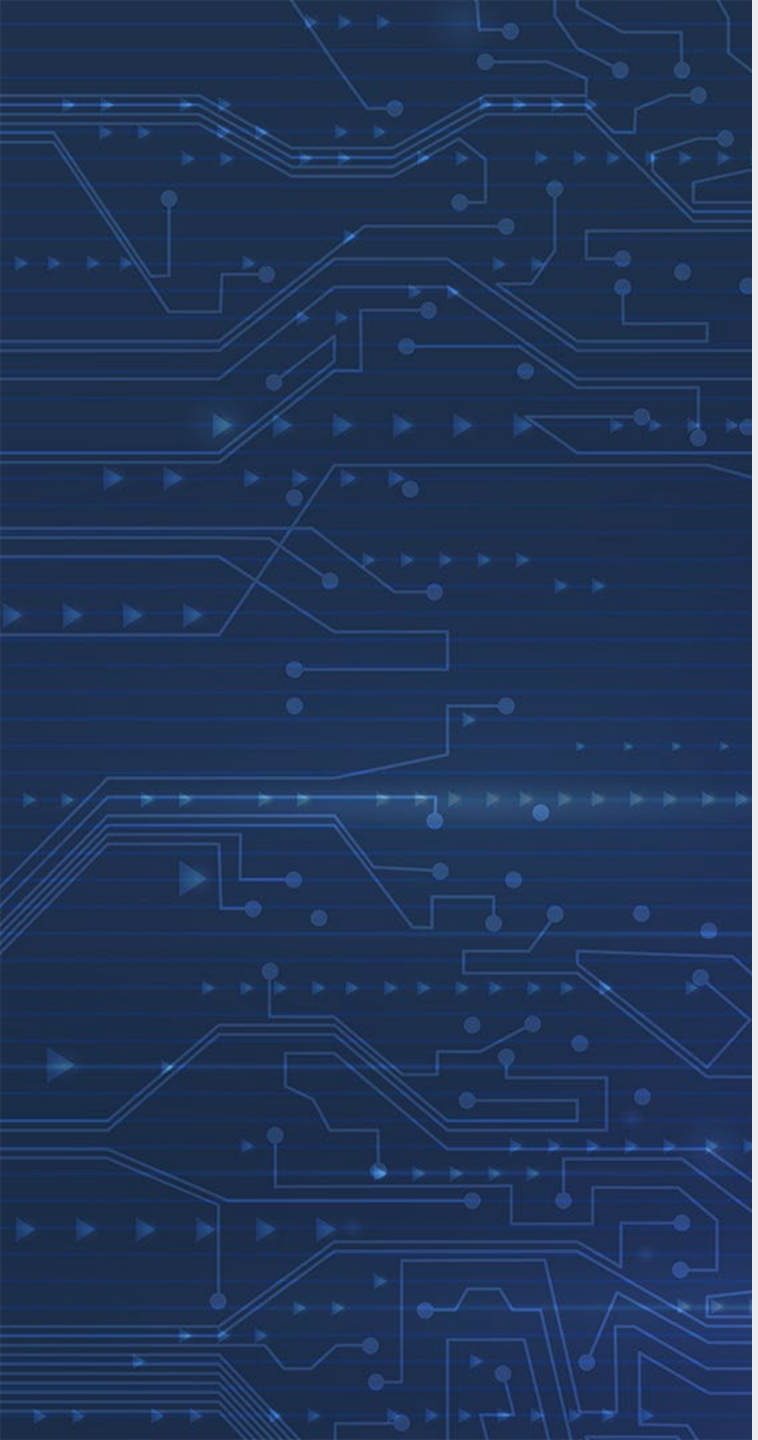
- APT19
- APT28
- APT29
- APT3
- APT32
- APT33
- APT38
- APT39
- APT41
- Aquatic Panda
- Blue Mockingbird
- BRONZE BUTLER
- Chimera
- Cobalt Group
- Confucius
- CopyKittens
- DarkHydrus
- DarkVishnya
- Deep Panda
- Dragonfly
- FIN10
- FIN6
- FIN7
- FIN8
- Fox Kitten
- Frankenstein
- GALLIUM
- GalImaker
- Gamaredon Group
- GOLD SOUTHFIELD
- Gorgon Group
- HAFNIUM
- Inception
- Indrik Spider
- Kimsuky
- Lazarus Group
- LazyScripter
- Leviathan
- Magic Hound
- menuPass

Threat Actors Using PowerShell, part 2

- Molerats
- MuddyWater
- Mustang Panda
- Nomadic Octopus
- OilRig
- Operation Wocao
- Patchwork
- Poseidon Group
- Sandworm Team
- Sidewinder
- Silence
- Stealth Falcon
- TA459
- TA505
- TeamTNT
- TEMP.Veles
- Threat Group-3390
- Thrip
- Tonto Team
- Turla
- WIRTE
- Wizard Spider

Protection/Defense Against PowerShell

- Options for defending against PowerShell:
  - Disable it if you don't need it
    - Block using Group Policy
    - Block using Security Policy
    - Disable access to PowerShell ISE
- The U.S. federal government recommends NOT disabling it due to its functionality
  - NSA/CISA/NSCS/NCSC-UK have provided guidance: https://media.defense.gov/2022/Jun/22/2003021689/-1/-1/1/CSI_KEEPING_POWERSHELL_SECURITY_MEASURES_TO_USE_AND_EMBRACE_20220622.PDF



Mimikatz

Post-exploitation credential theft tool

Mimikatz: Overview

"One of the world's most powerful password stealers" – Wired Magazine

- Released by Benjamin Delpy in 2011 (closed source)
  - Microsoft initially declined to fix the flaw it exploited (WDigest), noting that it requires access first
  - Mimikatz exploitation capabilities expanded beyond exploitation of WDigest in 2013
- Moscow, 2012
  - Hotel room incident: Russian attempt to acquire the code from his laptop
  - Conference incident: Russian demand that he provide code and presentation slides
  - Release of source code
- Repurposed for NotPetya
- Repurposed for BadRabbit

Image of Mimikatz prompt after initial startup.
Image source: Mimikatz GitHub page

Features of Mimikatz

Mimikatz began as a credential theft tool but has since been expanded with other capabilities.

What can Mimikatz do?

Pass-the-hash: Attackers use Mimikatz to pass an exact hash string to log in to the target computer.

Pass-the-ticket: Mimikatz provides functionality for a user to pass a Kerberos ticket to another computer and log in with that user's ticket.

Overpass-the-hash: This technique passes a unique key obtained from a domain controller to impersonate a user.

Kerberoast golden tickets: A golden ticket gives you non-expiring domain admin credentials to any computer on the network.

Kerberoast silver tickets: Kerberos grants a user a TGS ticket that's used to log into any services on the network.

Pass-the-cache: Generally the same as a pass-the-ticket, but uses the saved and encrypted login data on a Mac/UNIX/Linux system.

Image source: Varonis

Mimikatz – Capabilities Mapped to MITRE ATT&CK

ATT&CK ID	Name
T1134	Access Token Manipulation: SID-History Injection
T1098	Account Manipulation
T1547	Boot or Logon Autostart Execution: Security Support Provider
T1555	Credentials from Password Stores
T1555	Credentials from Web Browsers
T1555	Windows Credential Manager
T1003	OS Credential Dumping: LSASS Memory
T1003	OS Credential Dumping: Security Account Manager
T1003	OS Credential Dumping: LSA Secrets
T1003	OS Credential Dumping: DCSync

ATT&CK ID	Name
T1207	Rogue Domain Controller
T1558	Steal or Forge Kerberos Tickets: Golden Ticket
T1558	Steal or Forge Kerberos Tickets: Silver Ticket
T1552	Unsecured Credentials: Private Keys
T1550	Use Alternate Authentication Material: Pass the Hash
T1550	Use Alternate Authentication Material: Pass the Ticket

How Popular is Mimikatz?

Mimikatz is referenced in the second season of the USA Network television show *Mr. Robot*, when one of the characters used it to compromise password credentials.

Season 2, episode 9 of the show Mr. Robot.
Image source: Eventsentry

Threat Actors Using Mimikatz

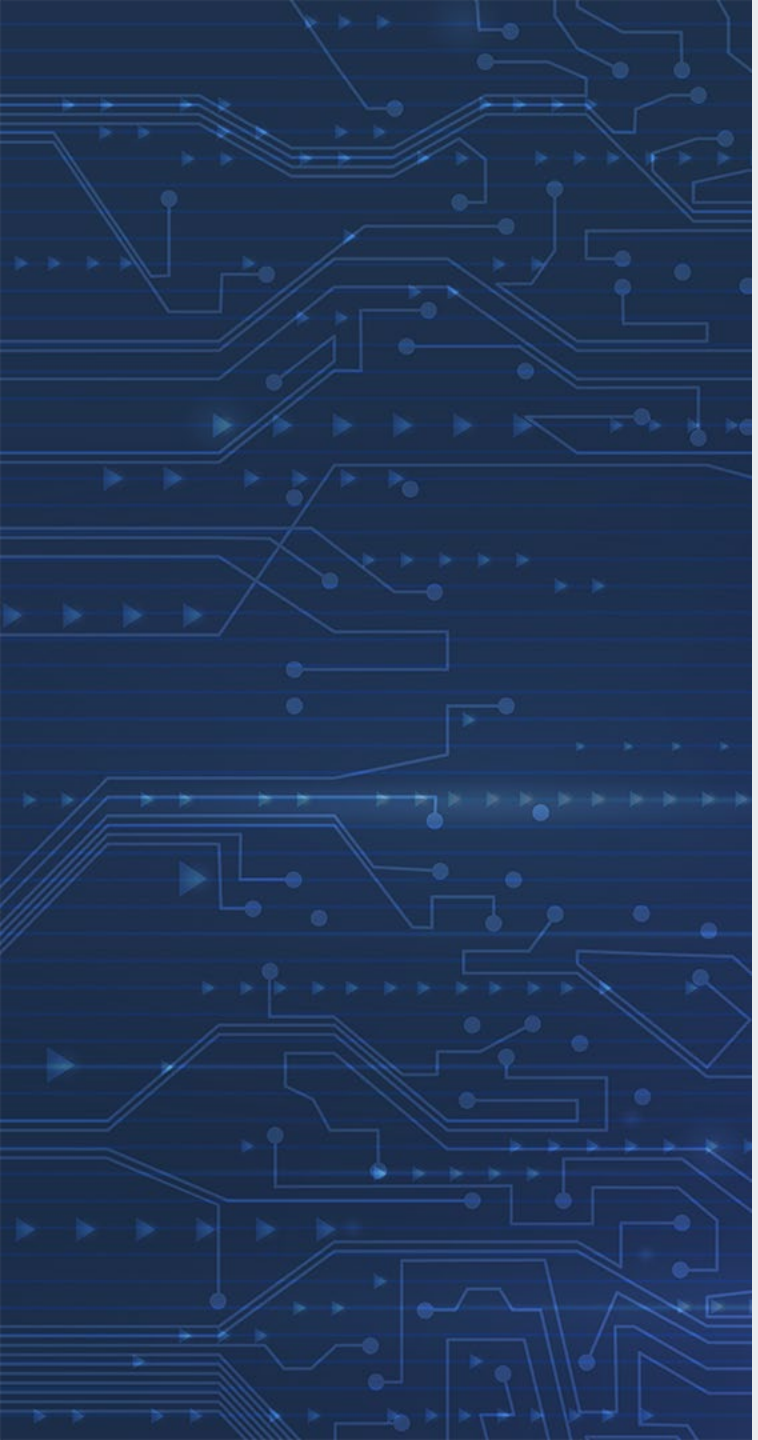
- APT1
- APT28
- APT29
- APT32
- APT33
- APT38
- APT39
- APT41
- FIN6
- FIN7
- Wizard Spider
- Kimsuky
- Threat Group-3390
- Cobalt Group
- menuPass
- Dragonfly
- Whitefly
- Tonto Team
- Chimera
- TEMP.Veles
- Magic Hound
- GALLIUM
- Thrip
- Blue Mockingbird
- BackdoorDiplomacy
- Operation Wocao
- Ke3chang
- MuddyWater
- Indrik Spider
- Turla
- Carbanak
- DarkHydrus
- OilRig
- Sandworm Team
- BRONZE BUTLER
- PittyTiger
- Cleaver
- Leafminer

Mimikatz: Defense

Mimikatz requires administrative access, and so if a threat actor is using it, the bigger problem would be that access.

Developing, implementing and enforcing basic administrative policies can help protect an enterprise network.

Image source: Varonis



Sysinternals

Windows system utilities that can be used for nefarious purposes

Sysinternals: Overview

- Advanced system utilities and resources, first developed in 1996 and acquired by Microsoft in 2006
- Dozens of tools, including:
  - File and Disk Utilities
  - Networking Utilities
  - Process Utilities
  - Security Utilities
  - System Information
  - Miscellaneous
- Some of the more noteworthy:
  - PSExec
  - ProcDump
  - PSList

Sysinternals Tools: File and Disk Utilities

AccessEnum
This simple yet powerful security tool shows you who has what access to directories, files and Registry keys on your systems. Use it to find holes in your permissions.

DiskExt
Display volume disk-mappings.

DiskMon
This utility captures all hard disk activity or acts like a software disk activity light in your system tray.

DiskView
Graphical disk sector utility.

Disk Usage (DU)
View disk usage by directory.

EFSDump
View information for encrypted files.

MoveFile
Schedule file rename and delete commands for the next reboot. This can be useful for cleaning stubborn or in-use malware files.

PendMoves
See what files are scheduled for deletion or rename the next time the system boots.

Process Monitor
Monitor file system, Registry, process, thread and DLL activity in real-time.

PsFile
See what files are opened remotely.

PsTools
The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

Sdelete
Securely overwrite your sensitive files and cleanse your free space of previously deleted files using this DoD-compliant secure delete program.

ShareEnum
Scan file shares on your network and view their security settings to close security holes.

Sysinternals Tools: Networking Utilities

AD Explorer
Active Directory Explorer is an advanced Active Directory (AD) viewer and editor.

AD Insight
AD Insight is an LDAP (Light-weight Directory Access Protocol) real-time monitoring tool aimed at troubleshooting Active Directory client applications.

AdRestore
Undelete Server 2003 Active Directory objects.

PipeList
Displays the named pipes on your system, including the number of maximum instances and active instances for each pipe.

PsFile
See what files are opened remotely.

PsPing
Measures network performance.

PsTools
The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

ShareEnum
Scan file shares on your network and view their security settings to close security holes.

TCPView
Active socket command-line viewer.

Whois
See who owns an Internet address.

Sysinternals Tools: Process Utilities

Autoruns
See what programs are configured to startup during system boot. Displays list of Registry and file locations that contain auto-start settings.

Handle
This handy command-line utility will show you what files are open by which processes, and much more.

ListDLLs
List all the DLLs that are currently loaded, including where they are loaded and their version numbers. Version 2.0 prints the full path names of loaded modules.

PortMon
Monitor serial and parallel port activity with this advanced monitoring tool. Version 3.x has powerful new UI enhancements and advanced filtering capabilities.

ProcDump
This command-line utility is aimed at capturing process dumps of otherwise difficult to isolate and reproduce CPU spikes.

Process Explorer
Identify files, registry keys and other objects processes have open, and which DLLs they have loaded, and the process owner.

Process Monitor
Monitor file system, Registry, process, thread and DLL activity.

PsExec
Execute processes remotely.

PsKill
Terminate local or remote processes.

PsList
Show information about processes and threads.

PsService
View and control services.

PsTools
List processes running on local or remote computers, run processes remotely, reboot systems, dump event logs, and more.

Sysinternals Tools: System Information

AccessChk
This tool shows you the accesses the user or group you specify has to files, Registry keys or Windows services.

AccessEnum
This simple yet powerful security tool shows you who has what access to directories, files and Registry keys on your systems. Use it to find holes in your permissions.

Autologon
Bypass password screen during logon.

Autoruns
See what programs configured to startup during system boot. Displays list of Registry and file locations containing auto-start settings.

LogonSessions
List active logon sessions

Process Explorer
Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

PsLoggedOn
Show users logged on to a system.

PsLogList
Dump event log records.

Rootkit Revealer
RootkitRevealer is an advanced rootkit detection utility.

Sdelete
Securely overwrite your sensitive files and cleanse your free space of previously deleted files using this DoD-compliant secure delete program.

ShellRunas
Launch programs as a different user via a convenient shell context-menu entry.

Sigcheck
Dump file version information and verify that images on your system are digitally signed.

Sysmon
Monitors and reports key system activity via the Windows event log.

Sysinternals Tools Used by Malicious Actors

- ProcDump
  - APT1
  - APT28
  - KE3chang
  - Lazarus Group
  - TG-3390
- PsList
  - KE3chang
  - Black Energy
  - APT33
  - APT34
  - APT35
- PsExec
  - Cleaver
  - Cobalt Group
  - Turla
  - Kimsuky
  - KE3chang
  - Indrik Spider
  - DarkVishnya
  - CostaRicto
  - menuPass
  - OilRig
  - Threat Group-1314
  - Night Dragon
  - GALLIUM
  - BlackTech
  - Magic Hound
  - Leafminer
  - Chimera
  - Dragonfly
  - TEMP.Veles
  - HAFNIUM
  - Sandworm Team
  - Carbanak
  - Wizard Spider
  - Naikon
  - Fox Kitten
  - Thrip
  - Black Energy
  - APT1
  - APT29
  - APT33
  - APT34
  - APT35
  - APT39
  - FIN5
  - FIN6

AnyDesk

Remote Desktop Software used for good and evil

AnyDesk: Overview

- Yet another way attackers will compromise remote desktop technologies
- Facilitates legitimate uses:
  - Remote access to several operating systems (Windows, macOS, Linux, as well as mobile platforms)
  - File transfers
  - Virtual private network services
  - Auto-discovery
  - Session protocol
- Leverages TLS 1.2 and AES-256
- Utilized by ransomware operators

Elicit Usage of AnyDesk

AnyDesk has garnered attention for its abuse in recent months, utilized especially to deliver ransomware to targets.

- Per Sophos (December 2021), the AvosLocker Ransomware gang is using AnyDesk to deploy ransomware.
- Per FBI (March 2022), AvosLocker continues to leverage AnyDesk for ransomware.
- Per Broadcom (December 2021), Babuk ransomware leverages fake AnyDesk sites to deploy ransomware.
- Per Asec (July 2022), AnyDesk is being used in cyberattacks.
- Per the DFIR Report (December 2021), Bazarloader uses AnyDesk to deploy ransomware.
- Solution: Secure use of remote tools in your organization.
  - Limit people, times and port access as much as possible.

> "...even if the ransomware fails to run, until every trace of the attackers' AnyDesk deployment is gone from every impacted machine, the targets will remain vulnerable to repeated attempts..."
> — Sophos

Brute Ratel

“Customized command and control center for red team and adversary simulation”

Brute Ratel: Overview

Provides adversary emulation, attack timelines and graphs, as well as OpSec features.

- Features:
  - SMB and TCP payloads for functionality to write custom external C2 channels over legitimate sites such as Slack, Discord, MS Teams
  - Built-in debugger to detect EDR userland hooks
  - Hide memory artifacts
  - Direct Windows SYS calls
  - Egress over HTTP, HTTPS, DNS Over HTTPS, SMB, TCP
  - GUI interface to analyze
  - LDAP queries to domain/ forest.
  - Multiple C2 channels, pivot options such as SMB, TCP, WMI, WinRM and managing remote services over RPC
  - Screenshots.
  - x64 shellcode loader
  - Reflective & object file loader
  - Decoding KRB5 ticket and converting it to hashcat
  - Patching Event Tracing for Windows (ETW) and Anti Malware Scan Interface (AMSI).
  - Create Windows system services.
  - Upload and download files.
  - Create files via CreateFileTransacted.
  - Port scans

Brute Ratel: Elicit Use and Defense

- Unit42: "While this capability has managed to stay out of the spotlight and remains less commonly known than its Cobalt Strike brethren, it is no less sophisticated"
- Per AdvIntel CEO Vitali Kremez, "ex-Conti ransomware members have also started to acquire licenses by creating fake US companies to pass the licensing verification system."
- Sophos (July 14): BlackCat ransomware operators leveraging Brute Ratel
- Most importantly, Brute Ratel was cracked, and the source code was leaked for anyone to leverage. It is now being leveraged by a group that has attacked healthcare.
- Mitigation actions are similar to Cobalt Strike – challenging to mitigate against a versatile tool.
- Part of building a defense against Brute Ratel will be maintaining situational awareness of both its developing capabilities and its increasing use.
- Monitor both open source and proprietary threat feeds for possible indicators of compromise.

Conclusions

- The tools in this presentation represent especially challenging security issues.
  - Mitigating the risk associated with them is not as simple as deploying a patch or reconfiguring an application.
  - Several of them are resident on common systems, making them even more challenging to detect when used maliciously.
- This list is not comprehensive, but simply highlights some of the more common and powerful tools that have a legitimate and valuable purpose but are also abused.
- This presentation is neither an endorsement nor a condemnation of these tools – each healthcare organization should evaluate these tools against their own risk posture and make decisions to employ them accordingly.

Reference Materials

References

Cobalt Strike

Defining Cobalt Strike Components So You Can BEA-CONfident in Your Analysis
https://www.mandiant.com/resources/defining-cobalt-strike-components

How to Detect Cobalt Strike: An Inside Look at the Popular Commercial Post-Exploitation Tool
https://www.recordedfuture.com/detect-cobalt-strike-inside-look/

Vermilion Strike: Linux and Windows Re-implementation of Cobalt Strike
https://www.intezer.com/blog/malware-analysis/vermilionstrike-reimplementation-cobaltstrike/

Hacker-made Linux Cobalt Strike beacon used in ongoing attacks
https://www.bleepingcomputer.com/news/security/hacker-made-linux-cobalt-strike-beacon-used-in-ongoing-attacks/

Cobalt Strike PowerShell Payload Analysis
https://michaelkoczwara.medium.com/cobalt-strike-powershell-payload-analysis-eecf74b3c2f7

References

Cobalt Strike

Cobalt Strike, a Defender's Guide
https://thedfirreport.com/2021/08/29/cobalt-strike-a-defenders-guide/

When Dridex and Cobalt Strike give you Grief
https://redcanary.com/blog/grief-ransomware/

TA551 (Shathak) continues pushing BazarLoader, infections lead to Cobalt Strike
https://isc.sans.edu/forums/diary/TA551+Shathak+continues+pushing+BazarLoader+infections+lead+to+Cobalt+Strike/27738/

Critical Cobalt Strike bug leaves botnet servers vulnerable to takedown
https://arstechnica.com/gadgets/2021/08/critical-cobalt-strike-bug-leaves-botnet-servers-vulnerable-to-takedown/

BazarCall to Conti Ransomware via Trickbot and Cobalt Strike
https://thedfirreport.com/2021/08/01/bazarcall-to-conti-ransomware-via-trickbot-and-cobalt-strike/

References

Cobalt Strike

IcedID and Cobalt Strike vs Antivirus
https://thedfirreport.com/2021/07/19/icedid-and-cobalt-strike-vs-antivirus/

Fake Kaseya VSA security update backdoors networks with Cobalt Strike
https://www.bleepingcomputer.com/news/security/fake-kaseya-vsa-security-update-backdoors-networks-with-cobalt-strike/

Attackers Increasingly Using Cobalt Strike
https://www.databreachtoday.com/attackers-increasingly-using-cobalt-strike-a-16959

Hancitor Continues to Push Cobalt Strike
https://thedfirreport.com/2021/06/28/hancitor-continues-to-push-cobalt-strike/

How legitimate security tool Cobalt Strike is being used in cyberattacks
https://www.techrepublic.com/article/how-legitimate-security-tool-cobalt-strike-is-being-used-in-cyberattacks/

References

Cobalt Strike

Cobalt Strike: Favorite Tool from APT to Crimeware
https://www.proofpoint.com/us/blog/threat-insight/cobalt-strike-favorite-tool-apt-crimeware

Cobalt Strike 2021 – Analysis of Malicious PowerShell Attack Framework
https://blogs.quickheal.com/cobalt-strike-2021-analysis-of-malicious-powershell-attack-framework/

Smoking Out a DARKSIDE Affiliate's Supply Chain Software Compromise
https://www.mandiant.com/resources/darkside-affiliate-supply-chain-software-compromise

Malware Analysis Report (AR21-148A) MAR 10339794-1.v1 – Cobalt Strike Beacon
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-148a

Cybercriminals are deploying legit security tools far more than before, researchers conclude
https://www.cyberscoop.com/cybercriminals-cobalt-strike-proofpoint/

References

Cobalt Strike

Look how many cybercriminals love Cobalt Strike
https://intel471.com/blog/cobalt-strike-cybercriminals-trickbot-qbot-hancitor

Conti Ransomware
https://thedfirreport.com/2021/05/12/conti-ransomware/

Detecting Exposed Cobalt Strike DNS Redirectors
https://labs.f-secure.com/blog/detecting-exposed-cobalt-strike-dns-redirectors

Sophos MTR in Real Time: What is Astro Locker Team?
https://news.sophos.com/en-us/2021/03/31/sophos-mtr-in-real-time-what-is-astro-locker-team/

COVID-19 Phishing With a Side of Cobalt Strike
https://www.domaintools.com/resources/blog/covid-19-phishing-with-a-side-of-cobalt-strike

References

Cobalt Strike

BazarCall Method: Call Centers Help Spread BazarLoader Malware
https://unit42.paloaltonetworks.com/bazarloader-malware/

Hancitor's Use of Cobalt Strike and a Noisy Network Ping Tool
https://unit42.paloaltonetworks.com/hancitor-infections-cobalt-strike/

Technical Analysis of Operation Diànxùn
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-dianxun.pdf

Cobalt Strikes Again, Spam Runs Target Russian Banks
https://www.trendmicro.com/en_us/research/17/k/cobalt-spam-runs-use-macros-cve-2017-8759-exploit.html

Loncom packer: from backdoors to Cobalt Strike
https://securelist.com/loncom-packer-from-backdoors-to-cobalt-strike/96465/

References

Cobalt Strike

New Snort, ClamAV coverage strikes back against Cobalt Strike
https://blog.talosintelligence.com/2020/09/coverage-strikes-back-cobalt-strike-paper.html

Evilnum hackers use the same malware supplier as FIN6, Cobalt
https://www.bleepingcomputer.com/news/security/evilnum-hackers-use-the-same-malware-supplier-as-fin6-cobalt/

Ryuk's Return
https://thedfirreport.com/2020/10/08/ryuks-return/

Ryuk in 5 Hours
https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/

Bazar, No Ryuk?
https://thedfirreport.com/2021/01/31/bazar-no-ryuk/

References

Cobalt Strike

Microsoft Defender ATP scars admins with false Cobalt Strike alerts
https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-atp-scars-admins-with-false-cobalt-strike-alerts/

Alleged source code of Cobalt Strike toolkit shared online
https://www.bleepingcomputer.com/news/security/alleged-source-code-of-cobalt-strike-toolkit-shared-online/

GitHub-hosted malware calculates Cobalt Strike payload from Imgur pic
https://www.bleepingcomputer.com/news/security/github-hosted-malware-calculates-cobalt-strike-payload-from-imgur-pic/

Raindrop: New Malware Discovered in SolarWinds Investigation
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware

References

Cobalt Strike

Povlsomware Ransomware Features Cobalt Strike Compatibility
https://www.trendmicro.com/en_us/research/21/c/povlsomware-ransomware-features-cobalt-strike-compatibility.html

Cobalt Strike, a penetration testing tool abused by criminals
https://blog.malwarebytes.com/researchers-corner/2021/06/cobalt-strike-a-penetration-testing-tool-popular-among-criminals/

Department of Justice Office of Public Affairs: Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research
https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion

Quick Tip: Cobalt Strike Beacon Analysis
https://isc.sans.edu/forums/diary/Quick+Tip+Cobalt+Strike+Beacon+Analysis/26818/

References

Mimikatz

The Untold Story of NotPetya, the Most Devastating Cyberattack in History
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Bad Rabbit: The Full Research Investigation
https://research.checkpoint.com/2017/bad-rabbit-full-research-investigation/

Trickbot Update: Brief Analysis ofa Recent Trickbot Payload
https://www.sentinelone.com/labs/trickbot-update-brief-analysis-of-a-recent-trickbot-payload/

Dumping User Passwords from Windows Memory with Mimikatz
http://woshub.com/how-to-get-plain-text-passwords-of-windows-users/

Manipulating User Passwords Without Mimikatz
https://www.trustedsec.com/blog/manipulating-user-passwords-without-mimikatz/

References

Mimikatz

Security 101: The Rise of Fileless Threats that Abuse PowerShell
https://www.trendmicro.com/vinfo/mx/security/news/security-technology/security-101-the-rise-of-fileless-threats-that-abuse-powershell

PowerShell Abuse: Good Tool Gone Bad
https://redcanary.com/resources/webinars/powershell-abuse/

How Hackers Use PowerShell And How To Take Action
https://www.forbes.com/sites/forbestechcouncil/2021/09/10/how-hackers-use-powershell-and-how-to-take-action/?sh=33f6a53b5cea

Tracking, Detecting, and Thwarting PowerShell-based Malware and Attacks
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/tracking-detecting-and-thwarting-powershell-based-malware-and-attacks

References

Anydesk

Diavol Ransomware
https://thedfirreport.com/2021/12/13/diavol-ransomware/

Case of Attack Exploiting AnyDesk Remote Tool (Cobalt Strike and Meterpreter)
https://asec.ahnlab.com/en/36159/

Babuk ransomware spread via fake Anydesk software websites
https://www.broadcom.com/support/security-center/protection-bulletin#bltfade3ddec4215697_en-us

Indicators of Compromise Associated with AvosLocker Ransomware
https://www.ic3.gov/Media/News/2022/220318.pdf

Avos Locker remotely accesses boxes, even running in Safe Mode
https://news.sophos.com/en-us/2021/12/22/avos-locker-remotely-accesses-boxes-even-running-in-safe-mode/

References

Brute Ratel

Hackers now sharing cracked Brute Ratel post-exploitation kit online
https://www.bleepingcomputer.com/news/security/hackers-now-sharing-cracked-brute-ratel-post-exploitation-kit-online/

Brute Ratel cracked and shared across the Cybercriminal Underground
https://blog.bushidotoken.net/2022/09/brute-ratel-cracked-and-shared-across.html

Ransomware, hacking groups move from Cobalt Strike to Brute Ratel
https://www.bleepingcomputer.com/news/security/ransomware-hacking-groups-move-from-cobalt-strike-to-brute-ratel/

BlackCat Ransomware Group Deploys Brute Ratel Pen Testing Kit
https://www.infosecurity-magazine.com/news/blackcat-ransomware-group-pen-test/

When Pentest Tools Go Brutal: Red-Teaming Tool Being Abused by Malicious Actors
https://unit42.paloaltonetworks.com/brute-ratel-c4-tool/

Questions

FAQs

Upcoming Briefing

- 11/3 – Iranian Threat Actors

Product Evaluations

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

Requests for Information

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

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. The HHS does not endorse any specific person, entity, product, service, or enterprise.

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

Sector and 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.

Alerts and Analyst Notes

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

Threat Briefings

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.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Contacts

HHS.GOV/HC3

HC3@HHS.GOV