LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

PyXie Remote Access Trojan (RAT)

02/20/2020

Report #: 202002201000

Agenda

- Overview
- Functionality
- Infection Stages
- Commands
- Cobalt Strike
- Historic Activity
- Industry Best Defense and Mitigations
- Indicators of Compromise (IOCs)
- Yara rule
- References
- Questions

Image source: ThreatVector

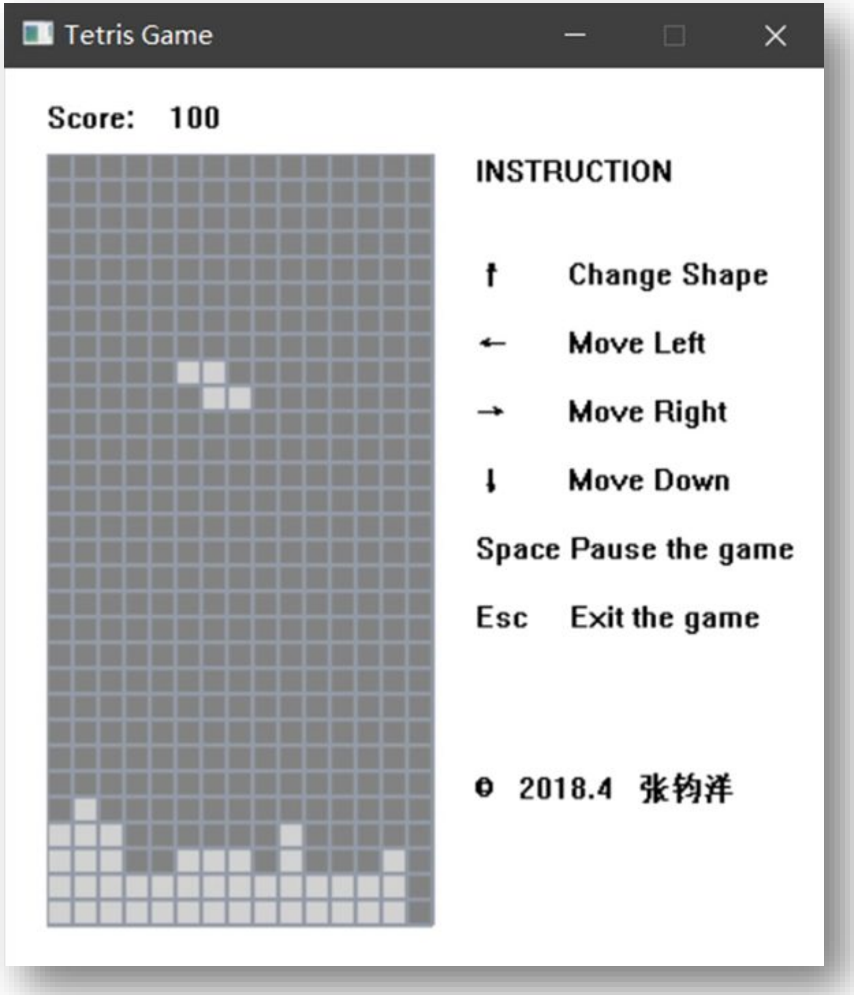
Slides Key:

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

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

Overview

- Remote Access Trojan (RAT) – often inserted into free software
  - Also capable of various forms of data collection and exfiltration, privilege escalation, code execution and leveraging/dropping additional malware
- PyXie has been described as, “highly customized, indicating that a lot of time and resources have gone into building it.”
- Infection vector: Sideloading: Injecting malicious code into legitimate software
- BlackBerry Cylance discovered it, named it PyXie and noted PyXie’s similarities to the banking trojan Shifu



Tetris Game

Score: 100

INSTRUCTION

↑ Change Shape

← Move Left

→ Move Right

↓ Move Down

Space Pause the game

Esc Exit the game

© 2018.4 张钧洋

Image source: ThreatVector

Overview (continued)

- Python-based malware
  - Utilizes .pyx file extension (instead of .py or .pyc)
- Active since 2018
  - Recent uptick in activity, targeting education and healthcare
- Actors are unknown, described as a “sophisticated cyber-criminal operation”; Possibly but not confirmed to be Shifu operators
- Targets many industry verticals, ultimately attempting to deliver ransomware – most recently education and healthcare

Functionality

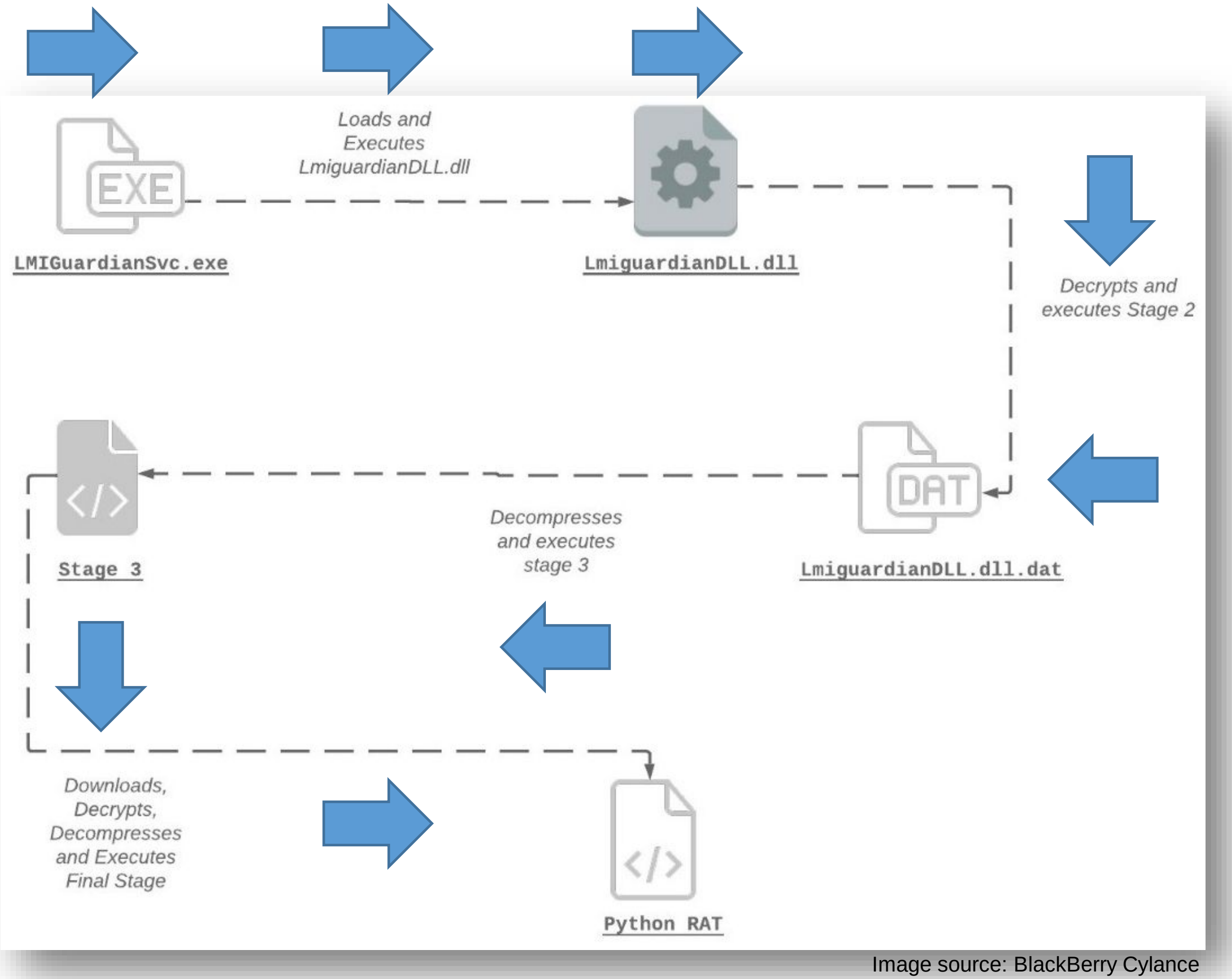
PyXie has the following capabilities:

- Remote Access Trojan (RAT) – Initial access
- Establishing command and control (C2 server)
  - Can alternatively receive commands via GitHub comments
- Privilege escalation (usually via PowerShell)
- Code execution
- Network scanning
- Keylogging
- Screen captures
- Recording videos
- Credential theft
- Cookie theft
- SOCK5 proxy (traffic masking/evasion of detection)
- Often utilized with Cobalt Strike
- Designed to be used with Mimikatz
- Has been observed delivering ransomware

Infection Stages

Loading stages:

- Binary drops .dll
- .dll drops encrypted payload
- Payload decrypted, second stage executed
- Attempt to escalate privileges if running as administrator
- Attempt to achieve persistence by editing the registry
- Third stage (Cobalt Mode) decompressed and executed
- Connects to C2 server, downloads encrypted payload and decrypts it
- Conduct environmental checks
- Injects PyXie RAT into a newly-spawned process
- PyXie RAT executes



EXE
LMIGuardianSvc.exe
Loads and Executes LmiguardianDLL.dll
LmiguardianDLL.dll
Decrypts and executes Stage 2
DAT
LmiguardianDLL.dll.dat
Decompresses and executes stage 3
Stage 3
Downloads, Decrypts, Decompresses and Executes Final Stage
Python RAT

Image source: BlackBerry Cylance

Commands

BlackBerry Cylance has enumerated the following functions:

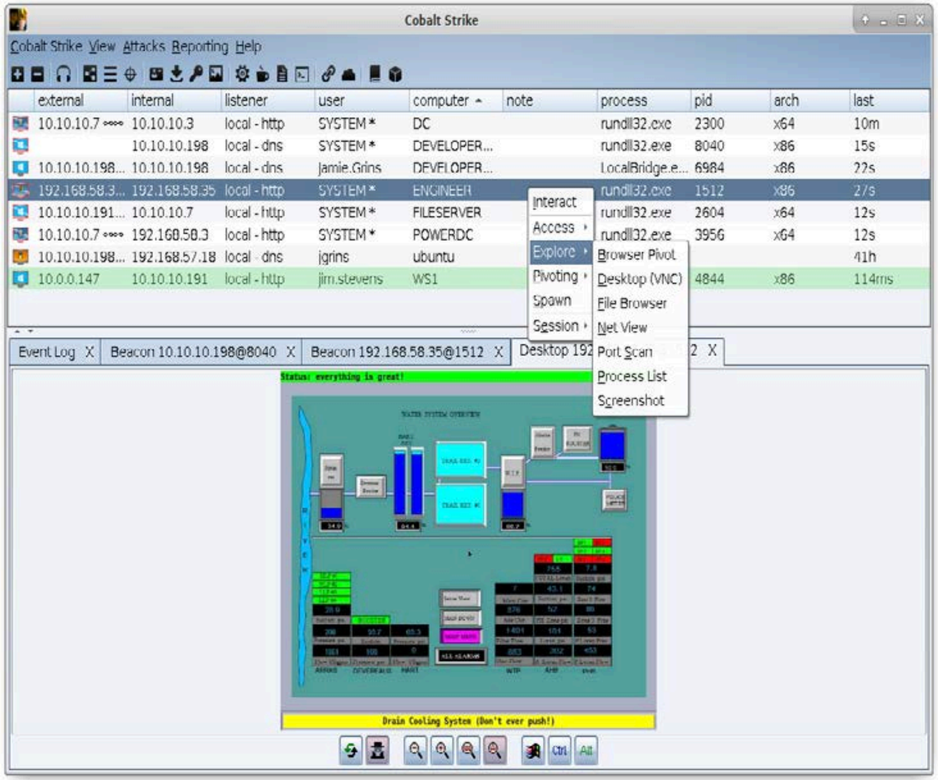
COMMAND	DESCRIPTION
!load	Download and run an executable
!get_config	Retrieve current config
!set_config	Set config
!update	Update
!update2	Update
!update3	Update
!get_keylog	Retrieve keylog
!get_cookies	Retrieve cookies
!get_sysinfo	Retrieve system info
!scan_lan	SMB scan local network
!scan_lan_ex	SMB scan specified IP ranges
!webdav	Start WebDAV server
!webdav_stop	Stop WebDAV server
!active_sk	Start SOCKS5 server
!deactive_sk	Stop SOCKS5 server
!active_bc	Start HVNC module
!deactive_bc	Stop HVNC module
!eval	Download and execute Python code
!self_destruct	Uninstall RAT
!get_screens	Retrieve Screenshots
!mem_load	Download and execute DLL in memory

Commands (Continued)

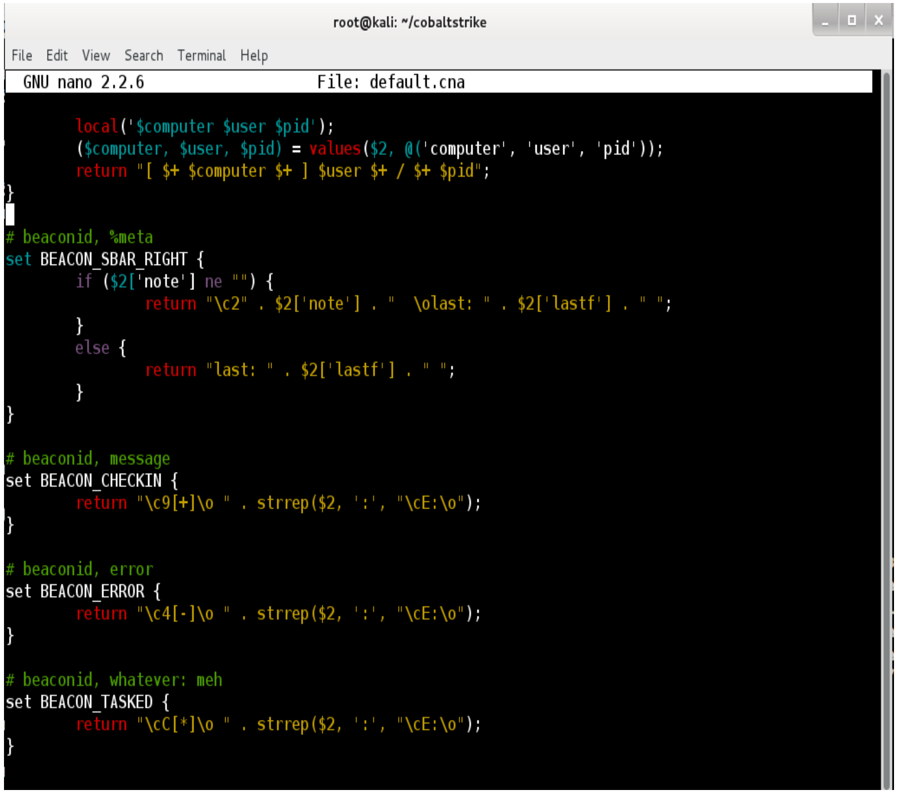
COMMAND	DESCRIPTION
!shellcode	Download and execute shellcode
!get_passwords	Dump passwords with LaZagne
!docfind	Retrieve file
!filefind	Find files matching certain criteria
!del_cookies	Clear cookies
!export_certs	Retrieve certificates from certificate store
!del_keylog	Clear keylog
!reboot	Reboot system
!check_soft	Check for installed software
!install_ffmpeg	Download ffmpeg binaries
!record_video	Record video with ffmpeg
!shell	Run command and capture output
!kill_lgmn_tokens	Retrieve LogMeIn credentials
!get_lgmn_tokens	Clear LogMeIn credentials
!sharphound	Enumerate domain with Sharphound
!bot_hashes	Retrieves hashes of loader and DLL
!mimi_32	Download Mimikatz
!mimi_64	Download Mimikatz
!mimi_grab	Execute Mimikatz
!get_kdbx	Retrieve keepass databases
!research_domain	SMB scan of computers identified by Sharphound
!research_full	SMB scan and port scan of computers identified by Sharphound
!wipe_rdp_creds	Clear RDP creds

Cobalt Strike

- Commercial penetration testing tool, described as “software for Adversary Simulations and Red Team Operations”
- Capable of reconnaissance, phishing, keystroke logging, screenshots, file exfiltration, covert communication, delivering additional payloads and reporting/logging



external	internal	listener	user	computer ▲	note	process	pid	arch	last
10.10.10.7 ∞∞	10.10.10.3	local - http	SYSTEM *	DC		rundll32.exe	2300	x64	10m
	10.10.10.198	local - dns	SYSTEM *	DEVELOPER...		rundll32.exe	8040	x86	15s
10.10.10.198...	10.10.10.198	local - dns	jamie.Grins	DEVELOPER...		LocalBridge.e...	6984	x86	22s
192.168.58.3...	192.168.58.35	local - http	SYSTEM *	ENGINEER		rundll32.exe	1512	x86	27s
10.10.10.191...	10.10.10.7	local - http	SYSTEM *	FILESERVER		rundll32.exe	2604	x64	12s
10.10.10.7 ∞∞	192.168.58.3	local - http	SYSTEM *	POWERDC		rundll32.exe	3956	x64	12s
10.10.10.198...	192.168.57.18	local - dns	jgrins	ubuntu					41h
10.0.0.147	10.10.10.191	local - http	jim.stevens	WS1			4844	x86	114ms


root@kali: ~/cobaltstrike
File Edit View Search Terminal Help

```
GNU nano 2.2.6                          File: default.cna

        local('$computer $user $pid');
        ($computer, $user, $pid) = values($2, @('computer', 'user', 'pid'));
        return "[ $+ $computer $+ ] $user $+ / $+ $pid";
}

# beaconid, %meta
set BEACON_SBAR_RIGHT {
        if ($2['note'] ne "") {
                return "\c2" . $2['note'] . "  \olast: " . $2['lastf'] . " ";
        }
        else {
                return "last: " . $2['lastf'] . " ";
        }
}

# beaconid, message
set BEACON_CHECKIN {
        return "\c9[+]\o " . strrep($2, ':', "\cE:\o");
}

# beaconid, error
set BEACON_ERROR {
        return "\c4[-]\o " . strrep($2, ':', "\cE:\o");
}

# beaconid, whatever: meh
set BEACON_TASKED {
        return "\cC[*]\o " . strrep($2, ':', "\cE:\o");
}
```

Images courtesy of Cobalt Strike

Historic Activity

- Unknown operators
- PyXie is known to have been active since 2018
- “Sophisticated Campaign“
  - Evasion techniques and operational tactics have made it challenging to detect
  - Complex in its engineered, fully-featured, utilizes PowerShell to escalate privileges and maintain persistence
- Similarities with Shifu,
  - Believed to be run by a cybercrime group located in Japan or the general East Asia region

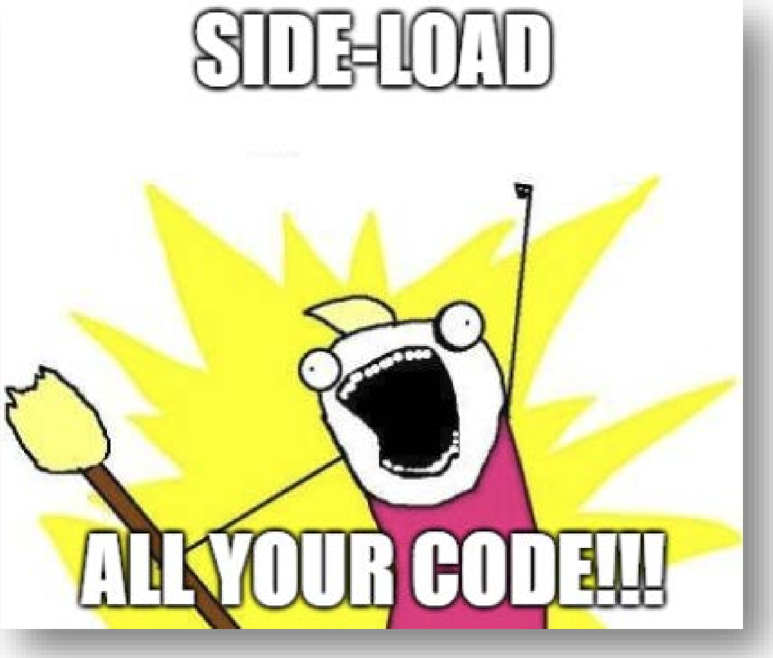


Image source: a12d404.net

Mitigation Practices: PyXie RAT

The HHS 405(d) Program published the Health Industry Cybersecurity Practices (HICP), which is a free resource that identifies the top five cyber threats and the ten best practices to mitigate them. Below are the practices from HICP that can be used to mitigate PyXie RAT.

DEFENSE/MITIGATION/COUNTERMEASURE	405(d) HICP REFERENCE
Provide social engineering and phishing training to employees.	[10.S.A], [1.M.D]
Develop and maintain policy on suspicious e-mails for end users; Ensure suspicious e-mails are reported.	[10.S.A], [10.M.A]
Ensure emails originating from outside the organization are automatically marked before received.	[1.S.A], [1.M.A]
Apply patches/updates immediately after release/testing; Develop/maintain patching program if necessary.	[7.S.A], [7.M.D]
Implement Intrusion Detection System (IDS).	[6.S.C], [6.M.C], [6.L.C]
Implement spam filters at the email gateways.	[1.S.A], [1.M.A]
Block suspicious IP addresses at the firewall.	[6.S.A], [6.M.A], [6.L.E]
Implement whitelisting technology to ensure that only authorized software is allowed to execute.	[2.S.A], [2.M.A], [2.L.E]
Implement access control based on the principal of least privilege.	[3.S.A], [3.M.A], [3.L.C]
Implement and maintain anti-malware solution.	[2.S.A], [2.M.A], [2.L.D]
Conduct system hardening to ensure proper configurations.	[7.S.A], [7.M.D]
Disable the use of SMBv1 (and all other vulnerable services and protocols) and require at least SMBv2.	[7.S.A], [7.M.D]

Background information can be found here:
https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

Indicators of Compromise

Please note several things about the indicators of compromise (IOCs) on the following slides:

- We have attempted to include a significant sample of indicators of compromise related to PyXie in this presentation. However, there may be some available to the public not included here. Furthermore, there are commercial cyber threat analysis companies that release IOCs, many are subscription-based, to their paying customers. We recommend healthcare organizations consider IOCs that are freely available as well as those with an associated cost.
- Upon being released to the public, IOCs may become "burned" which is to say that the attackers will adjust their tactics, techniques and procedures (TTPs), weapons and infrastructure so that the public IOCs are no longer used.

Indicators of Compromise

Indicators of Compromise Continued:

- There are instances of obsolete IOCs being reused, so any organization attempting to defend themselves should consider all possibilities.
- New IOCs are constantly being released, especially with a tool as prominent and frequently used as TrickBot. It is therefore incumbent upon any organization attempting to defend themselves to remain vigilant, maintain situational awareness and be ever on the lookout for new IOCs to operationalize in their cyber defense infrastructure.

Indicators of Compromise (continued)

INDICATOR	TYPE	DESCRIPTION
1d970f2e7af9962ae6786c35fcd6bc48bb860e2c8ca74d3b81899c0d3a978b2b	SHA256	Loader DLL
3a47e59c37dce42304b345a16ba6a3d78fc44b21c4d0e3a0332eee21f1d13845	SHA256	Loader DLL
3aa746bb94acee94c86a34cb0b355317de8404c91de3f00b40e8257b80c64741	SHA256	Loader DLL
56e96ce15ebd90c197a1638a91e8634dbc5b0b4d8ef28891dcf470ca28d08078	SHA256	Loader DLL
5937746fc1a511d9a8404294b0caa2aedae2f86b5b5be8159385b6c7a4d6fb40	SHA256	Loader DLL
7330fa1ca4e40cdfea9492134636ef06cd999efb71f510074d185840ac16675d	SHA256	Loader DLL
78471db16d7bd484932c8eb72f7001db510f4643b3449d71d637567911ca363b	SHA256	Loader DLL
814357417aa8a57e43d50cb3347c9d287b99955b0b8aee4e53e12b463f7441a0	SHA256	Loader DLL
92a8b74cafa5eda3851cc494f26db70e5ef0259bc7926133902013e5d73fd285	SHA256	Loader DLL
a765df03fffa343aa7a420a0a57d4b5c64366392ab6162c3561ff9f7b0ad5623	SHA256	Loader DLL
c3b3f46a5c850971e1269d09870db755391dcbe575dc7976f90ccb1f3812d5ea	SHA256	Loader DLL
c9400b2fff71c401fe752aba967fa8e7009b64114c9c431e9e91ac39e8f79497	SHA256	Loader DLL
d271569d5557087aecc340bb570179b73265b29bed2e774d9a2403546c7dd5ff	SHA256	Loader DLL
de44656b4a3dde6e0acdc6f59f73114ce6bb6342bec0dcd45da8676d78b0042e	SHA256	Loader DLL
e0f22863c84ee634b2650b322e6def6e5bb74460952f72556715272c6c18fe8e	SHA256	Loader DLL
ea27862bd01ee8882817067f19df1e61edca7364ce649ae4d09e1a1cae14f7cc	SHA256	Loader DLL
edd1480fe3d83dc4dc59992fc8436bc1f33bc065504dccf4b14670e9e2c57a89	SHA256	Loader DLL
f9290cd938d134a480b41d99ac2c5513a964de001602ed34c6383dfeb577b8f7	SHA256	Loader DLL
366d47b95e216863ee64e0024e2bbf0bf1b66420986fe0a5b3e805ce795dcf9f	SHA256	Encrypted Payload
d031081b8c211994b5406bf3f2544c0d6ebcbab384f23e393f084b49563e1d12	SHA256	Encrypted Payload
f466bc20544bf203155142cf14456e55b0e756aa93ecfb5edc74ba7ed60f9573	SHA256	Encrypted Payload
ca68f02bd01650383af68f0c129482faf283329dd1e6a18821ad26fc2c3d00b2	SHA256	Encrypted Payload
d776235e628422ada7f1e976a3cf771049286edf2219583028fbbd6229af72b9	SHA256	Encrypted Payload
50a4b19b38caea4eea042704314f5ae1acf2162c7353fb92bc896dcada14b86a	SHA256	Encrypted Payload
610c3536ceafc0e4ad0d60c683052ee7272e29049ceac909b1d1e55ac1206f49	SHA256	Encrypted Payload
7ee6235f0e653a36a818a12531657f6dac5f3fb41efa1e1c63f6761ba3faeb90	SHA256	Encrypted Payload
265e5e1389b3145bf2ac1a017b67a54d84bc361dc3795120656dcabc1212c34a	SHA256	Encrypted Payload
8d2b3b0cbb32618b86ec362acd142177f5890917ae384cb58bd64f61255e9c7f	SHA256	PyXie RAT interpreter
d1429f54baaad423a8596140a3f70f7d9f762373ad625bda730051929463847d	SHA256	PyXie RAT bytecode
ade8f07bf7918343bf307ec35837327efc7a85a0edac5ab5b2cd037134af8d57	SHA256	Cobalt Mode
fd93858f4e7356bebe30dd0dfe07367e3ddf6164bb78725e1c543b093558cf64	SHA256	Cobalt Strike Loader
a50b58e24eb261157c4f85d02412d80911abe8501b011493c7b393c1905fc234	SHA256	Cobalt Strike Loader
0d14a1b5574dc12f6286d37d0a624232fb63079416b98c2e1cb5c61f8c2b66ff	SHA256	Cobalt Strike Loader
625c22b21277c8a7e1b701da9c1c21b64bfa02baef5d7a530a38f6d70a7a16d0	SHA256	Cobalt Strike Loader
bd7da341a28a19618b53e649a27740dfeac13444ce0e0d505704b56335cc55bd	SHA256	Cobalt Strike Loader
d612144c1f6d4a063530ba5bfae7ef4e4ae134bc55dcf067439471934b841b00	SHA256	Cobalt Strike Loader
ce0936366976f07ea24e86733888e97e421393829ecfd0fde66bd943d4b992ab	SHA256	Cobalt Strike Loader
3259dd0efed1d28a149d4e8c4f980a19199d9bead951ee1231e3a26521185f2f	SHA256	Cobalt Strike Loader

Indicators of Compromise (continued)

INDICATOR	TYPE	DESCRIPTION
e5fede5eb43732c7f098acf7b68b1350c6524962215b476de571819b6e5a71fc	SHA256	Cobalt Strike Loader
f6ff873e1bd3d0e6b6182792aebd781f4f60be39d49085ba3d64658456260402	SHA256	Cobalt Strike Loader
608f34a79e5566593b284ef0d24f48ea89bc007e5654ae0969e6d9f92ec87d32	SHA256	Cobalt Strike Loader
b1f54b88c9b7680877981f6bebde6aea9effbc38a0a8b27a565fb35331094680	SHA256	Cobalt Strike Loader
d50f28cf5012e1ffde1cd28655e07519dadcf94218b15c701c526ab0f6acb915	SHA256	Cobalt Strike Loader
56934547dcf0d7ecf61868ae2f620f60e94c094dbd5c3b5aaf3d3a904d20a693	SHA256	Cobalt Strike Loader
73609f8ebd14c6970d9162ec8d7786f5264e910573dff73881f85b03163bd40e	SHA256	Cobalt Strike Loader
2ceb5de547ad250140c7eb3c3d73e4331c94cf5a472e2806f93bf0d9df09d886	SHA256	Cobalt Strike Loader
840985b782648d57de302936257ba3d537d21616cb81f9dce000eaf1f76a56c8	SHA256	Cobalt Strike Loader
e48e88542ec4cd6f1aa794abc846f336822b1104557c0dfe67cff63e5231c367	SHA256	Cobalt Strike Loader
cb2619b7aab52d612012386d88a0d983c270d9346169b75d2a55010564efc55c	SHA256	Cobalt Strike Loader
88565b4c707230eac34d4528205056264cd70d797b6b4eb7d891821b00187a69	SHA256	Cobalt Strike Loader
91c62841844bde653e0357193a881a42c0bc9fcc798a69f451511c6e4c46fd18	SHA256	Cobalt Strike Loader
ddf83c02effea8ae9ec2c833bf40187bed23ec33c6b828af49632ef98004ea82	SHA256	Cobalt Strike Loader
edecfdd2a26b4579ecacf453b9dff073233fb66d53c498632464bca8b3084dc5	SHA256	Cobalt Strike Loader
sarymar[.]com	Network	PyXie RAT C&C
benreat[.]com	Network	PyXie RAT C&C
planlamaison[.]com	Network	PyXie RAT C&C
teamchuan[.]com	Network	PyXie RAT C&C
tedxns[.]com	Network	PyXie RAT / Cobalt Mode C&C
athery[.]bit	Network	PyXie RAT C&C
babloom[.]bit	Network	PyXie RAT C&C
Floppys[.]bit	Network	PyXie RAT C&C
104[.]200[.]67[.]173	Network	PyXie RAT C&C
Hwartless[.]bit	Network	Cobalt Mode C&C
c1oudflare[.]com	Network	Cobalt Mode C&C
foods-pro[.]com	Network	Cobalt Strike C&C
dopearos[.]com	Network	Cobalt Strike C&C
fearlesslyhuman[.]org	Network	Cobalt Strike C&C
185[.]82[.]202[.]109	Network	Cobalt Strike C&C
192[.]52[.]167[.]241	Network	Seen hosting malicious Loader DLL
ololo[.]space	Network	Seen hosting malicious Loader DLL
%Appdata%\Wireshark\	File	Presence of Goopdate.dll or LmiGuardianDLL.dll in this directory
%Appdata%\WinRAR\	File	Presence of Goopdate.dll or LmiGuardianDLL.dll in this directory
%Appdata%\VisualAssist\	File	Presence of Goopdate.dll or LmiGuardianDLL.dll in this directory
%Appdata%\UltraVNC\	File	Presence of Goopdate.dll or LmiGuardianDLL.dll in this directory
%Appdata%\TortoiseSVN\	File	Presence of Goopdate.dll or LmiGuardianDLL.dll in this directory
%Appdata%\TeamViewer\	File	Presence of Goopdate.dll or LmiGuardianDLL.dll in this directory

Yara Rule

```
rule PyXie_RAT
{
    meta:
        description = "Detects PyXie RAT"

    strings:
        $mz = "MZ"
        $op = {C6 06 68 89 46 01 C7 46 05 9C 81 74 24 C6 46 09 04 89 4E 0A 66 C7 46 0E 9D C3}

    condition:
        ($mz at 0) and $op
}
```

Reference Materials

References

- New 'PyXie' RAT Used Against Multiple Industries
  - https://www.securityweek.com/new-pyxie-rat-used-against-multiple-industries
- Meet PyXie: A Nefarious New Python RAT
  - https://threatvector.cylance.com/en_us/home/meet-pyxie-a-nefarious-new-python-rat.html
- New Malware Campaign Uses Trojanized 'Tetris' Game: Report**
  - https://www.databreachtoday.com/new-malware-campaign-uses-trojanized-tetris-game-report-a-13465
- This trojan malware is being used to steal passwords and spread ransomware
  - https://www.zdnet.com/article/this-trojan-malware-is-being-used-to-steal-passwords-and-spread-ransomware/
- New Malware “PyXie” Uses Trojanized Tetris Game
  - https://www.cisomag.com/new-malware-pyxie-uses-trojanized-tetris-game/
- PyXie – A Python RAT Escalate The Windows Admin Privilege to Deliver Ransomware, MitM Attack, Keylogging & Steal Cookies
  - https://gbhackers.com/python-rat/
- Where Are They Today? Cybercrime Trojans That No One Misses: Shifu Malware
  - https://securityintelligence.com/where-are-they-today-cybercrime-trojans-that-no-one-misses-shifu-malware/
- GitHub: BloodHoundAD/SharpHound
  - https://github.com/BloodHoundAD/SharpHound

Questions

Questions

Upcoming Briefs

- NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management
- Wearable Device Security

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to HC3@HHS.GOV.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

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

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently 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 document and presentation that provides 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 call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV