LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

NetWalker Ransomware

09/24/2020

Report #: 202009241030

Agenda

- Why does this matter?
- Introduction to Netwalker
- Attack / Execution overview
- Ransom note example
- Targeting
- Telemetry
- Timeline of major activity
- Affiliates
- NetWalker and MITRE ATT&CK
- Attack process
- Technical Operations
- CIS Security Controls
- Yara rules
- Indicators of Compromise
- Mitigation steps
- References

Image source: Heimdal Security

Slides Key:

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

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

A reminder of why this matters

- Ransomware has always been a plague to the healthcare community
  - Combined with data breaches, these make up a predominance of cyber threats to healthcare
- Ransomware is a disruptive attack that can jeopardize health and potentially lives of healthcare patients
- As of last week, the loss of life is no longer potentially possible, but an actuality
- Technical details are still limited but we do know:
  - A ransomware attack on the Düsseldorf University Clinic occurred on September 10 which disabled 30 servers, impacting operations
  - A critically ill patient was relocated to another hospital in Wuppertal (roughly 45 minutes away) and the delay in treatment caused her death
  - It's believed exploited an arbitrary code execution vulnerability in a Citrix device (CVE-2019-19781)
    - Was initially made public in December 2019 and a patch released in January 2020, nine months prior to the attack
  - The attackers also reportedly had access for months prior
  - German authorities have traced the attacks to Russia (not necessarily government-sanctioned) and are pressing negligent homicide charges
  - There has been speculation but no proof as to who the attackers are, likely a cybercrime group

A patient has died after ransomware hackers hit a German hospital

This is the first ever case of a fatality being linked to a cyberattack.

by **Patrick Howell O'Neill**

September 18, 2020

MIT Technology Review

Introduction to NetWalker Ransomware

- Initially discovered in September 2019 with a compilation timestamp dating back to August 28, 2019
- Also known as: Malito, Koko, KazKavKovKiz
- Operated as Ransomware-as-a-Service (RaaS) by a cybercrime group known as CIRCUS SPIDER
  - Advertised as a closed-affiliate program, and verifies applicants before they are being accepted as an affiliate
- Significant targeting in the Asia Pacific (APAC) region, but can reach globally
  - Often target hospitals in the US and Spain
  - Big game hunters
- Ransom demands from $1K USD to $3M USD; use “double extortion”; over $25 million since March
- Leveraging coronavirus and exploiting healthcare organizations during pandemic
- Coded in C++, PowerShell
- Use common tools, post-exploit toolkits and Living-off-the-Land (LOTL) tactics
  - Mimikatz, various PSTools, AnyDesk, TeamViewer, NLBrute and more
- Russian-speaking; prohibits infection of Russian and the Commonwealth of Independent States systems
- Uses a combination of ChaCha and Elliptic Curve Cryptography (ECC)
- Ransomware attacks on healthcare can:
  - Steal and leak sensitive data, including patient information
  - Disrupt operations

Attack/Execution Overview

- The Spider threat actors
  - Circus Spider is not represented in this diagram as they are not as prominent as some of the other groups, but they are all part of the same larger network of cybercriminal groups

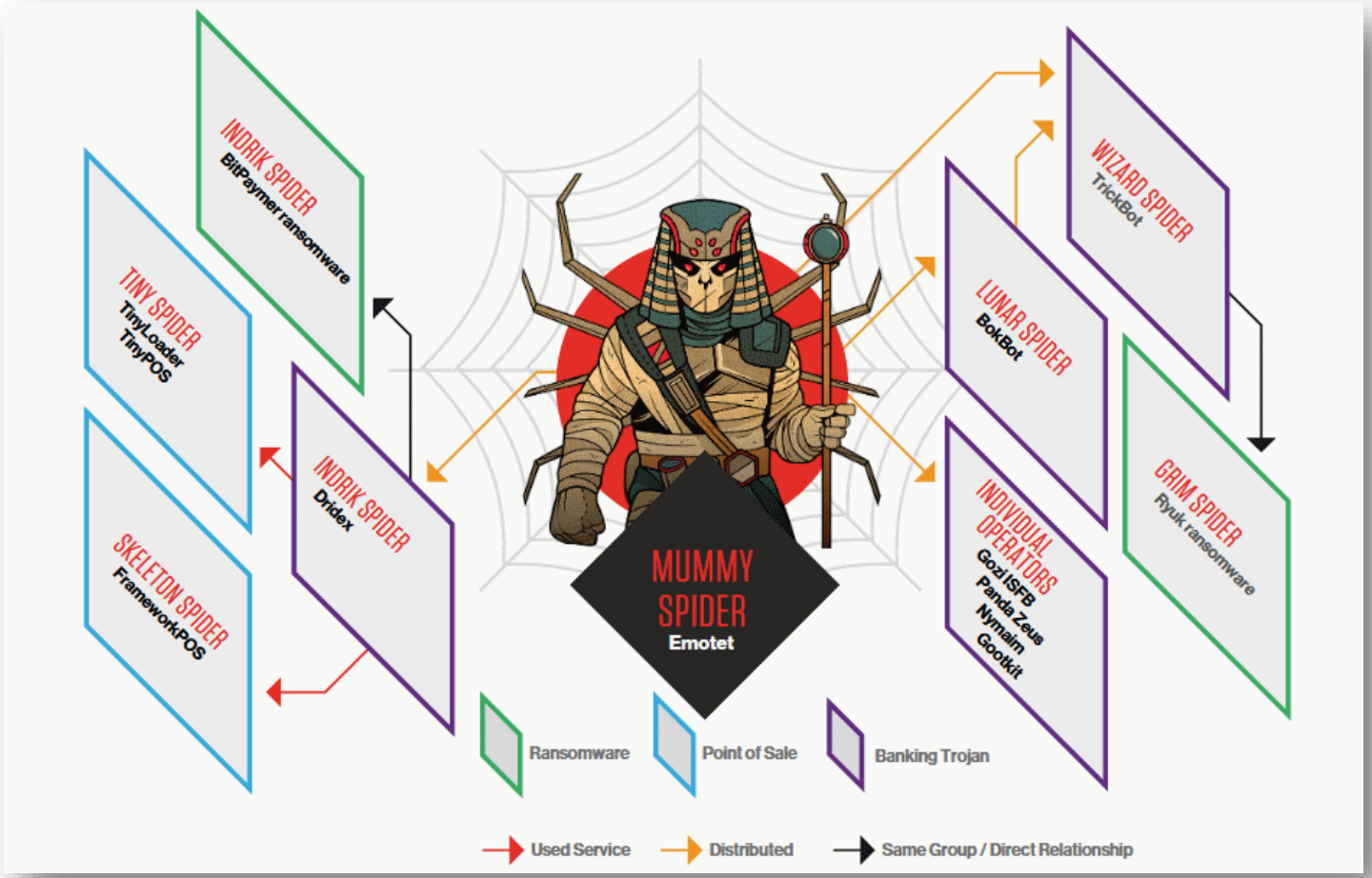


Image source: CrowdStrike

Attack/Execution Overview

- Initial infection is performed through either:
  - Vulnerability exploitation, or
  - Spear phishing
- Double extortion
  - Trend began with Maze operators in November of 2019; other ransomware operators followed suit, including CIRCUS SPIDER
  - Exfiltrate data prior to encryption
  - Forbes describes this as the five “uneasy Es”:
    - **Exfiltrate**: Capture and send data to a remote attacker server for later leverage
    - **Eliminate**: Identify and delete enterprise backups to improve odds of payment
    - **Encrypt**: Use leading encryption protocols to fully encrypt data
    - **Expose**: Provide proof of data and threaten public exposure and a data auction if payment is not made
    - **Extort**: Demand an exorbitant payment paid via cryptocurrency
- Highly active during pandemic, especially against healthcare organization
  - One phishing campaign is using an attachment named "CORONAVIRUS_COVID-19.vbs" (contains NetWalker)
  - After script is executed, executable saved to *%Temp%\qeSw.exe* and launched

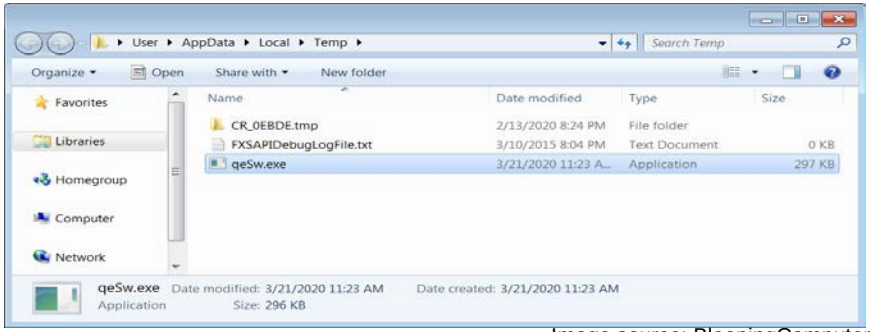
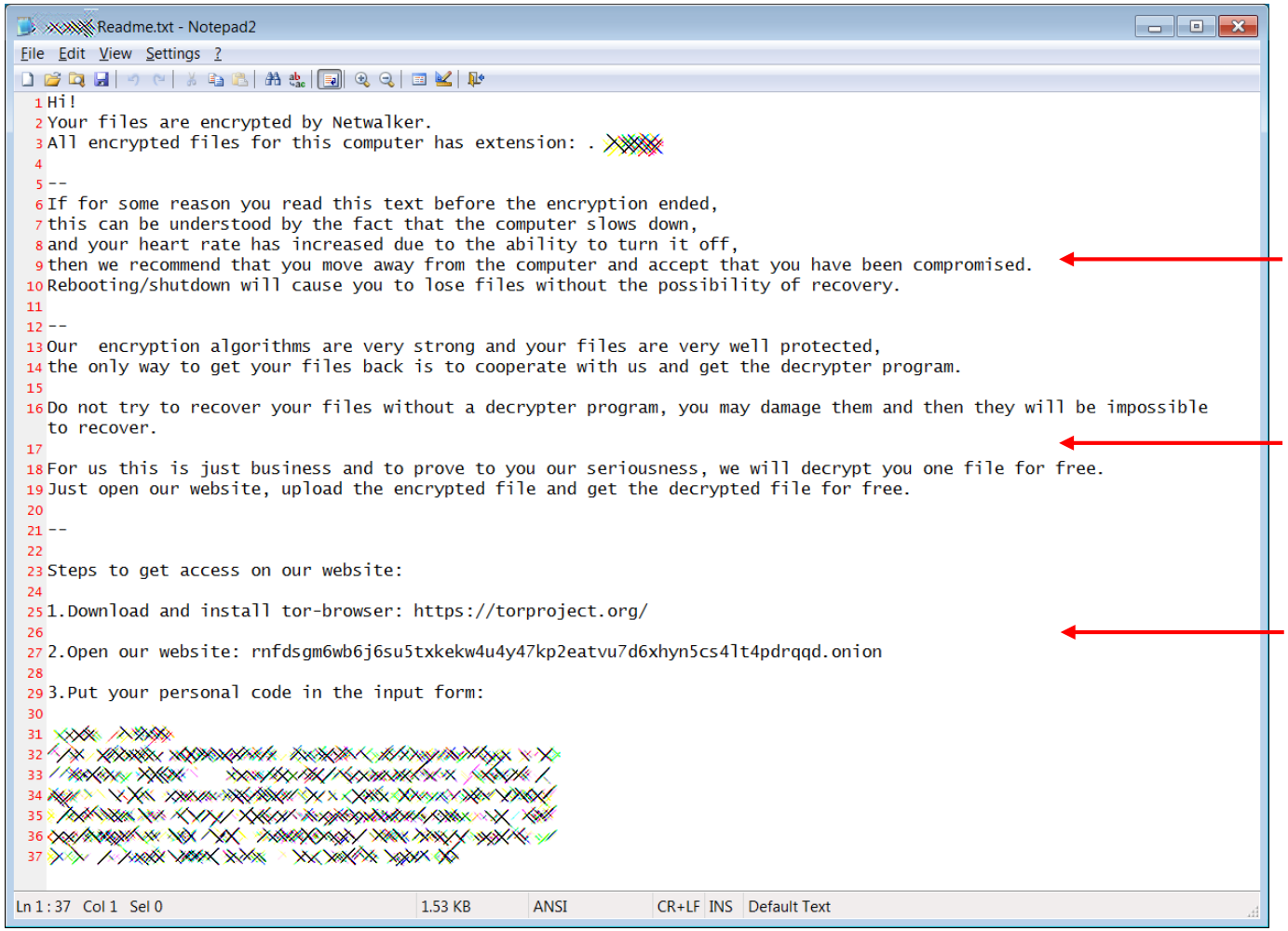


Image source: BleepingComputer

Ransom Note

- NetWalker ransom notes have the standard elements found in most ransomware notes:



Futility of non-cooperation

Justification for trust

Instructions

Image source: BleepingComputer

Targeting

- Activity increased during the coronavirus pandemic, directed at the healthcare sector
  - Notable victims:
    - Health service provider in Maryland
    - Public health agency in Illinois
    - Medical facility in Pennsylvania
    - Health system in Pennsylvania
    - University school of medicine in California
- Besides healthcare, the ransomware has been used to target various other industry verticals:
  - Manufacturing
  - Business management solutions
  - Customer experience management
  - Electromobility and battery solutions
  - Education
  - And many more:
- Most recently, attacks in September 2020:
  - Targeted K-Electric, Pakistan's largest private power utility company
    - Demanded $3.85M initially, $7.7M after a week
  - American, a data center service provider, attacked with NetWalker
    - Demanded $4.5M in ransom

Image source: Tripwire

Telemetry

Telemetry:

Image source: McAfee

Timeline of Major Activity

- August / September 2019: Began operations
- March 2020: Significant changes to operations
  - Shift to network intrusion-focused Ransomware-as-a-Service (RaaS) model
- May 2020: Continuing to change and evolve tactics and operations
  - Observed using reflective dynamic-link library (DLL) injection to infect victims
  - Actively recruiting partners for RaaS operations; specific set of criteria
  - Compromised the Austrian city of Weiz using coronavirus-themed phishing
- July 2020: Repeatedly exploited CVE-2019-11510 and CVE-2019-18935
- March to July 2020: Strong revenue
  - NetWalker collected around 2,795 Bitcoin (roughly $30M as of mid-September 2020 Bitcoin value), purportedly making it one of the most profitable active variants of ransomware
- July 2020: FBI released a flash alert
  - NetWalker is attacking healthcare organizations during the pandemic
- September 2020:
  - Compromise of K-Electric
  - Compromise of American data center

Affiliates

- To be an affiliate:
  - Preconditions and screening
  - Requirements range from providing proof of previous revenue in similar affiliates programs, to experience in the field, and what type of industry the applicant is targeting
  - “Quality, not quantity”
  - What targets is a potential affiliate interested in?
  - What experience do they have? How can they prove it?
  - Proof of persistent access to valuable targets and intentions

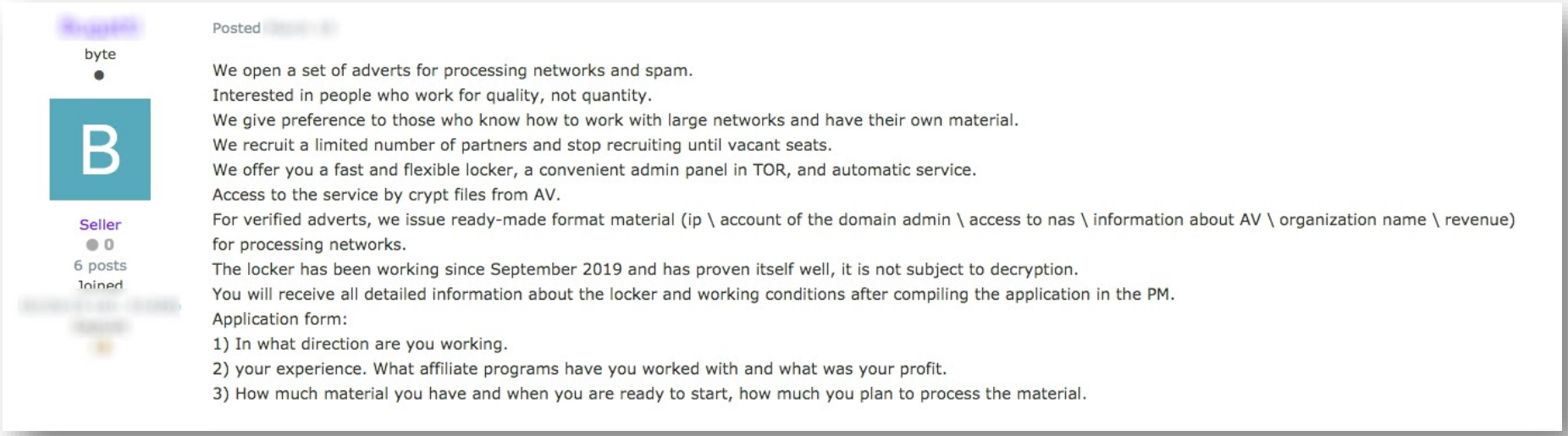
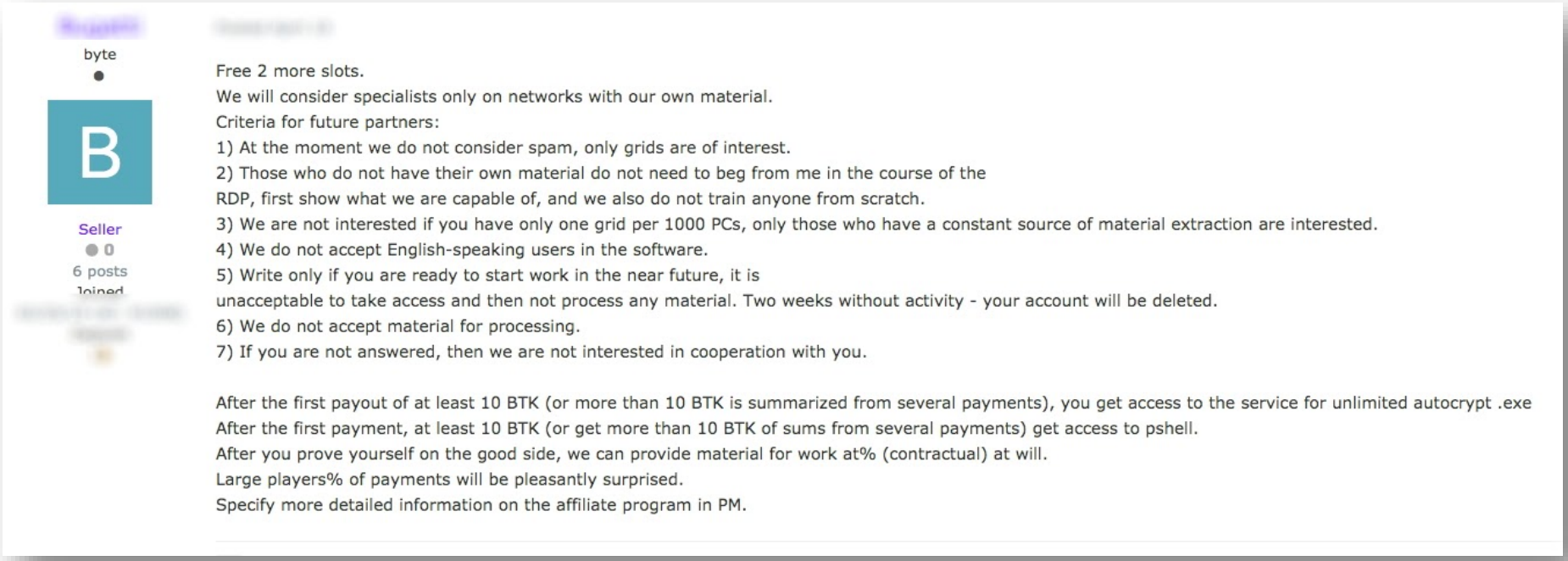


Image source: Sentinel Labs

- Further preconditions:
  - Cannot be an English speaker
  - Do not train anyone from scratch
  - Be ready to take action and be decisive



byte

B

Seller
0
6 posts
Joined

Free 2 more slots.
We will consider specialists only on networks with our own material.
Criteria for future partners:
1) At the moment we do not consider spam, only grids are of interest.
2) Those who do not have their own material do not need to beg from me in the course of the
RDP, first show what we are capable of, and we also do not train anyone from scratch.
3) We are not interested if you have only one grid per 1000 PCs, only those who have a constant source of material extraction are interested.
4) We do not accept English-speaking users in the software.
5) Write only if you are ready to start work in the near future, it is
unacceptable to take access and then not process any material. Two weeks without activity - your account will be deleted.
6) We do not accept material for processing.
7) If you are not answered, then we are not interested in cooperation with you.

After the first payout of at least 10 BTK (or more than 10 BTK is summarized from several payments), you get access to the service for unlimited autocrypt .exe
After the first payment, at least 10 BTK (or get more than 10 BTK of sums from several payments) get access to pshell.
After you prove yourself on the good side, we can provide material for work at% (contractual) at will.
Large players% of payments will be pleasantly surprised.
Specify more detailed information on the affiliate program in PM.

Image source: Sentinel Labs

Affiliates (continued)

- Features of their software:
  - Fully automated TOR-based chat panel
  - Support for Windows 2000 and above
  - Full visibility into potential target environments
  - Fast and multi-threaded locker
  - Highly flexible configuration options
  - Encrypts adjacent network volumes
  - Unique build and obfuscation process
  - Automated blog for victim data posting

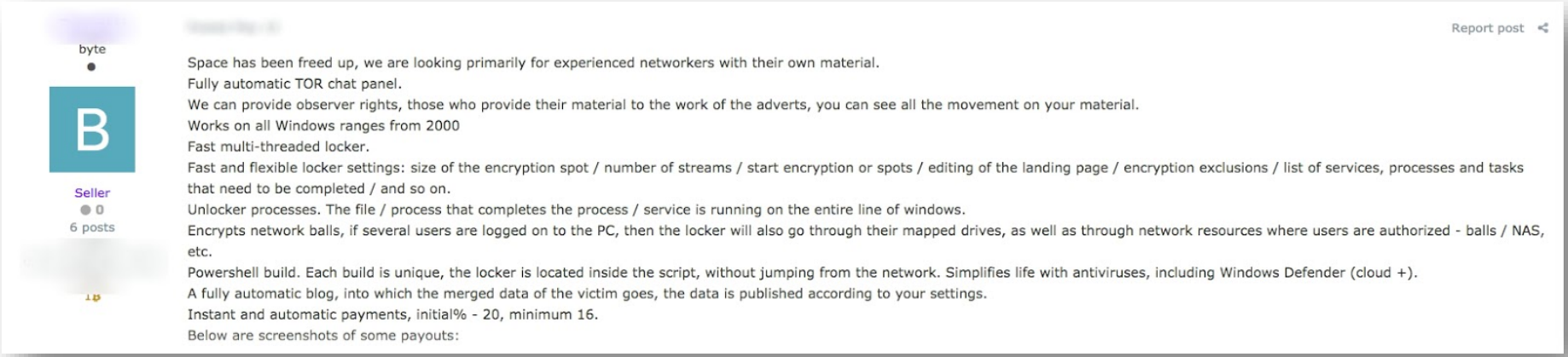
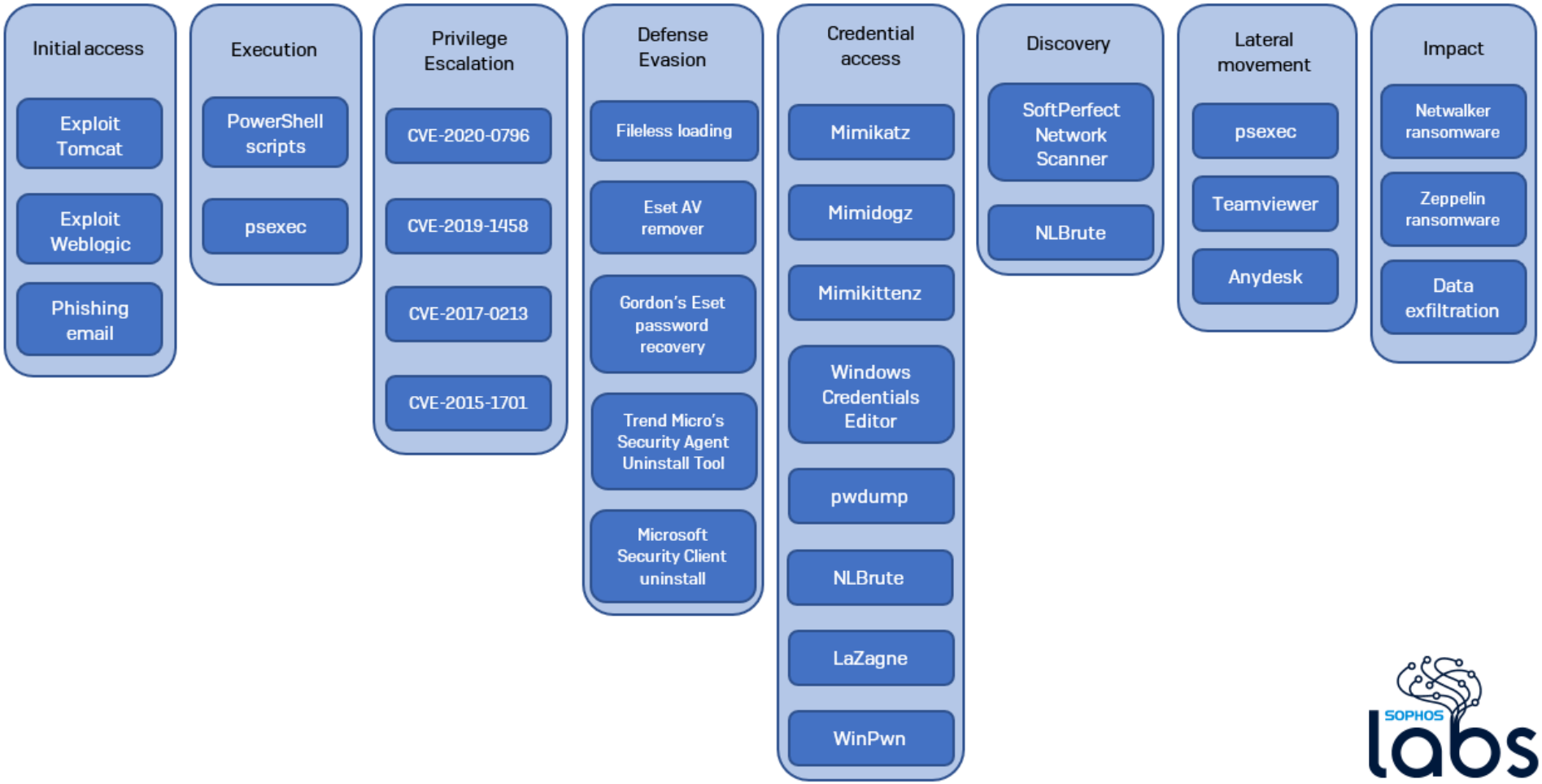


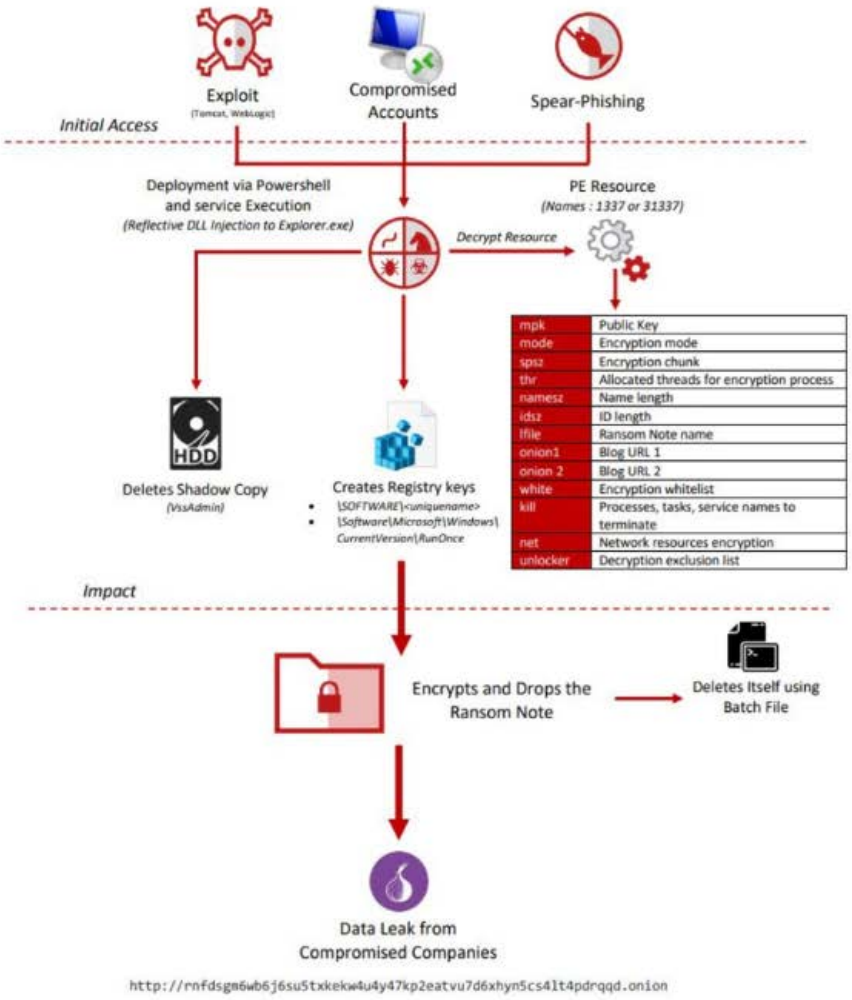
Image source: Sentinel Labs

Netwalker threat actor toolset on the ATT&CK matrix



Attack Process

- Standard attack:



MITRE Tactic	MITRE Techniques
Initial Access	Exploit Public Facing Application (T1190)
Initial Access	Spear Phishing Attachment (T1566.001) Email
Initial Access	Valid Accounts (T1078) RDP Compromised

MITRE Tactic	MITRE Techniques
Execution	Powershell Script(T1059.001), Service Execution (T1569.002, Command and Scripting Interpreter (T1059.003), Native API (T1106), WMI (T1047)
Persistence	Registry Key - Place Value on Run Once Key (T1060), Modify Registry key – Create own key (T1112)
Privilege Escalation	Exploitation for Privilege Exploitation ((T1068), Process Injection (T1055.001)
Defensive Evasion	Disabling Security Tools (T1089), Process Injection (T1055), Deobfuscate/Decode Files or Information (T1140), Obfuscated Files or Information (T1027)
Credential Access	Credential Dumping (T1003), Brute Force (T1110)

MITRE Tactic	MITRE Techniques
Discovery	Network Service Scanning (T1046); Security Software Discovery (T1518.001), System Information Discovery (T1082)
Lateral Movement	Third Party Software (T1072), Service Execution (T1569.002), Lateral Tool Transfer (T1570)
Collection	Data from Information Repositories (T1213), Data from local system (T1005), Data from network shared drive (T1039)
Command and Control	Ingress Tool Transfer (T1105)
Impact	Data Encrypted (T1486) Netwalker Ransomeware, Inhibit System Recovery (T1490), Service Stop (T1489)

Image source: McAfee

Communications between victim and NetWalker

Ransom portal login

Source of image: McAfee

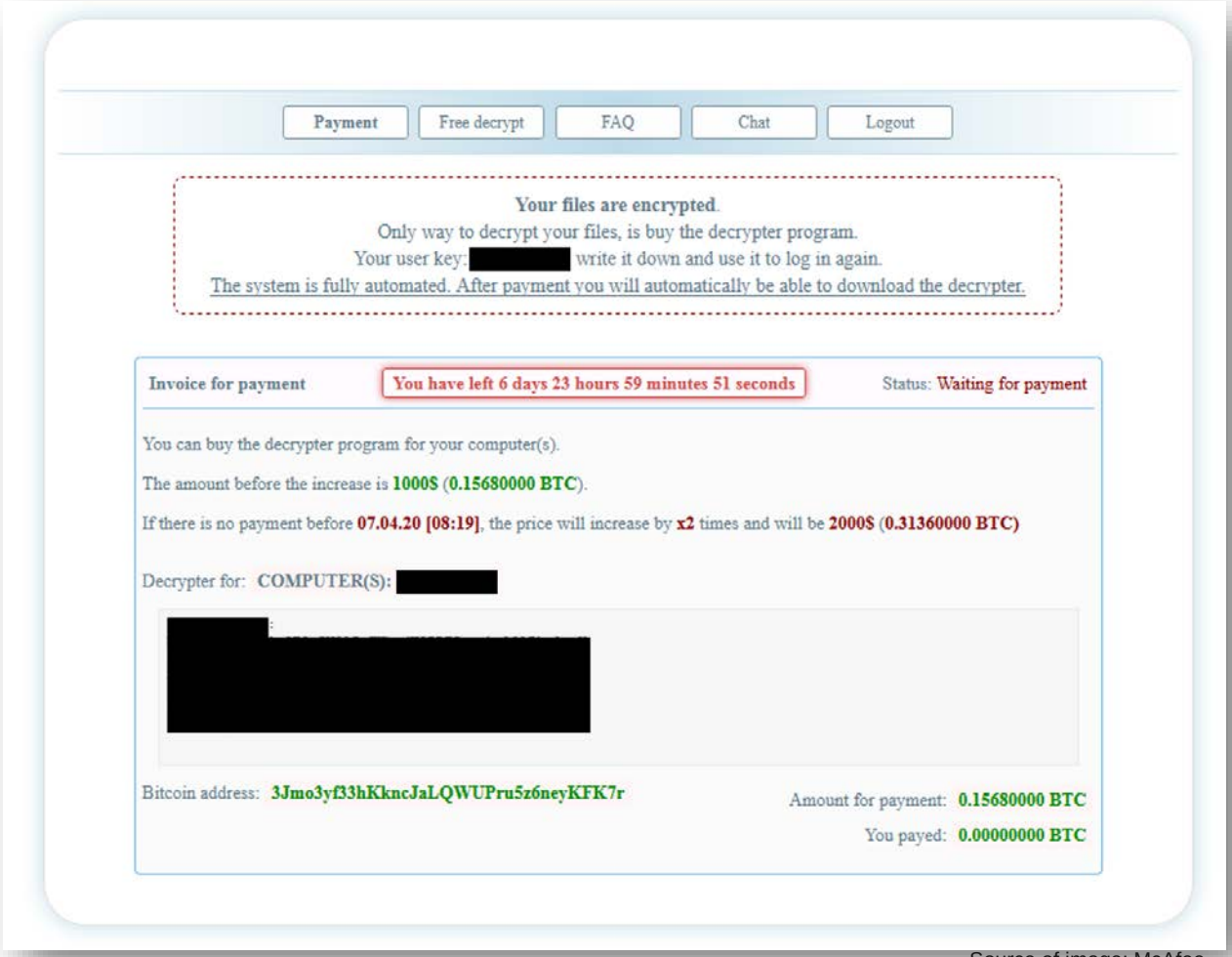
Communications between victim and NetWalker

Portal to upload files to test decryption

Source of images: McAfee

Communications between victim and NetWalker

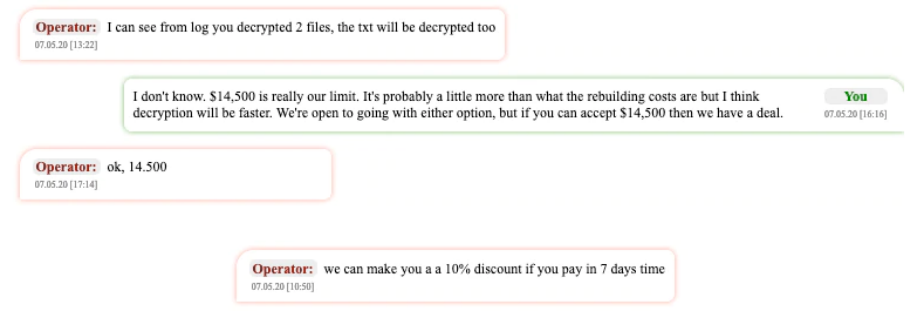
Ransom portal landing page



Source of image: McAfee

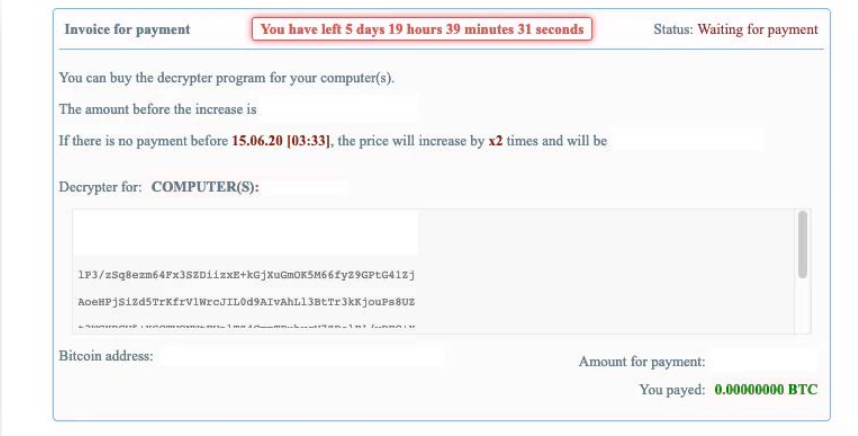
Communications between victim and NetWalker

Negotiation



Delivery of decryptor

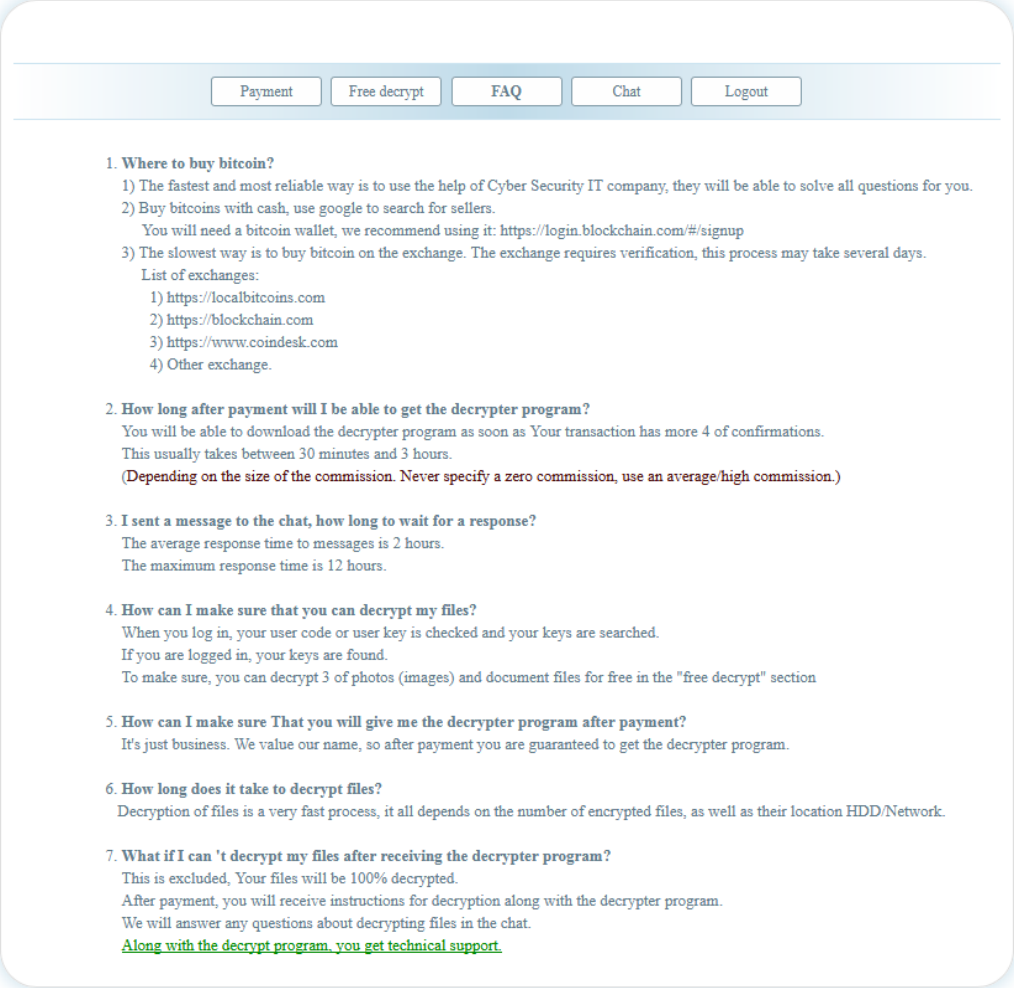
Payment and invoice



Source of images: McAfee

Communications between victim and NetWalker

Frequently Asked Questions (FAQ)



Payment | Free decrypt | FAQ | Chat | Logout

1. **Where to buy bitcoin?**
   1) The fastest and most reliable way is to use the help of Cyber Security IT company, they will be able to solve all questions for you.
   2) Buy bitcoins with cash, use google to search for sellers.
      You will need a bitcoin wallet, we recommend using it: https://login.blockchain.com/#/signup
   3) The slowest way is to buy bitcoin on the exchange. The exchange requires verification, this process may take several days.
      List of exchanges:
      1) https://localbitcoins.com
      2) https://blockchain.com
      3) https://www.coindesk.com
      4) Other exchange.

2. **How long after payment will I be able to get the decrypter program?**
   You will be able to download the decrypter program as soon as Your transaction has more 4 of confirmations.
   This usually takes between 30 minutes and 3 hours.
   (Depending on the size of the commission. Never specify a zero commission, use an average/high commission.)

3. **I sent a message to the chat, how long to wait for a response?**
   The average response time to messages is 2 hours.
   The maximum response time is 12 hours.

4. **How can I make sure that you can decrypt my files?**
   When you log in, your user code or user key is checked and your keys are searched.
   If you are logged in, your keys are found.
   To make sure, you can decrypt 3 of photos (images) and document files for free in the "free decrypt" section

5. **How can I make sure That you will give me the decrypter program after payment?**
   It's just business. We value our name, so after payment you are guaranteed to get the decrypter program.

6. **How long does it take to decrypt files?**
   Decryption of files is a very fast process, it all depends on the number of encrypted files, as well as their location HDD/Network.

7. **What if I can 't decrypt my files after receiving the decrypter program?**
   This is excluded, Your files will be 100% decrypted.
   After payment, you will receive instructions for decryption along with the decrypter program.
   We will answer any questions about decrypting files in the chat.
   Along with the decrypt program, you get technical support.

Source of image: McAfee

- Critical security controls likely to be effective against initial infection and exploitation techniques:

MITRE Tactic	MITRE Technique	CIS Control
Initial Access	Exploit Public-Facing Applications (T1190) Tomcat, Web Logic	CSC 2 – Inventory of Software Assets CSC 3 – Continuous Vulnerability Assessment CSC 5 – Secure Configuration CSC 9 – Limitation of Network Ports and Protocols CSC 12 – Boundary Defense CSC 18 – Application Software Security
Initial Access	Spear Phishing Attachments (T1566.001)	CSC 7 – Email and Web Browser Protection CSC 8 – Malware Defenses
Initial Access	Valid Accounts (T1078) RDP Compromised	CSC 5 – Secure Configuration of hardware and software CSC 9 – Limitation of Network Ports and Protocols CSC 12 – Boundary Defense

MITRE Tactic	MITRE Technique	CIS Control
Execution	PowerShell (T1059.001) PowerShell Script	CSC 5 Secure Configuration CSC 8 Malware Defenses
Execution	Service Execution (T1569.002) PS Exec	CSC 5 Secure Configuration CSC 8 Malware Defenses
Execution	Command and Scripting Interpreter (T1059.003) Windows Command Shell	CSC 5 Secure Configuration CSC 8 Malware Defenses
Execution	Native API (T1106) Use Windows API functions to inject DLL	CSC 5 Secure Configuration CSC 8 Malware Defenses
Execution	Windows Management Instrumentation (T1047)	CSC 4 Controlled Use of Admin Privileges CSC 5 Secure Configuration CSC 9 Limitation of Network Ports and Protocols CSC 8 Malware Defenses

Data source: McAfee

- Critical security controls likely to be effective against persistence and privilege escalation techniques:

MITRE Tactic	MITRE Technique	CIS Control
Persistence	Registry Key – Place Value on Run Once Key (T1060)	CSC 5 Secure Configuration CSC 8 Malware Defenses
Persistence	Modify Registry key – Create own key (T1112)	CSC 5 Secure Configuration CSC 8 Malware Defenses

MITRE Tactic	MITRE Technique	CIS Control
Privilege Escalation	Exploitation for Privilege Exploitation (T1068) CVE-2020-0796	CSC 3 Vulnerability Management CSC 5 Secure Configuration CSC 8 Malware Defenses CSC 12 Boundary Defenses
Privilege Escalation	Exploitation for Privilege Exploitation (T1068) CVE-2019-1458	CSC 3 Vulnerability Management CSC 5 Secure Configuration CSC 8 Malware Defenses CSC 12 Boundary Defenses
Privilege Escalation	Exploitation for Privilege Exploitation (T1068) CVE-2017-0213	CSC 3 Vulnerability Management CSC 5 Secure Configuration CSC 8 Malware Defenses CSC 12 Boundary Defenses
Privilege Escalation	Exploitation for Privilege Exploitation (T1068) CVE-2015-1701	CSC 3 Vulnerability Management CSC 5 Secure Configuration CSC 8 Malware Defenses CSC 12 Boundary Defenses
Privilege Escalation	Process Injection: Reflective DLL (T1055)	CSC 5 Secure Configuration CSC 8 Malware Defenses

Data source: McAfee

- Critical security controls likely to be effective against defensive evasion, credential access and discovery techniques:

MITRE Tactic	MITRE Technique	CIS Control
Defensive Evasion	Disabling Security Tools (T1562.001) ESET, Trend Micro, MS	CSC 5 Secure Configuration CSC 8 Malware Defenses
Defensive Evasion	Process Injection: Reflective DLL (T1055)	CSC 5 Secure Configuration CSC 8 Malware Defenses
Defensive Evasion	Deobfuscate / Decode Files or Information (T1140)	CSC 5 Secure Configuration CSC 8 Malware Defenses
Defensive Evasion	Obfuscated Files or Information (T1027): PowerShell Script uses Base64 and hexadecimal encoding and XOR-encryption	CSC 5 Secure Configuration CSC 8 Malware Defenses CSC 12 Boundary Defenses

MITRE Tactic	MITRE Technique	CIS Control
Credential Access	Credential Dumping (T1003) Mimikatz, Mimidogz, Mimikittenz, Pwdump, LaZagne, Windows Credentials	CSC 4 Controlled Use of Admin Privileges CSC 5 Secure Configuration CSC 8 Malware Defenses
Credential Access	Brute Force (T1110) NL Brute	CSC 4 Controlled use of admin privileges CSC 16 Account Monitoring

MITRE Tactic	MITRE Technique	CIS Control
Discovery	Network Service Scanning (T1046) Network Scanner	CSC 5 Secure Configuration CSC 8 Malware Defenses CSC 12 Boundary Defenses

Data source: McAfee

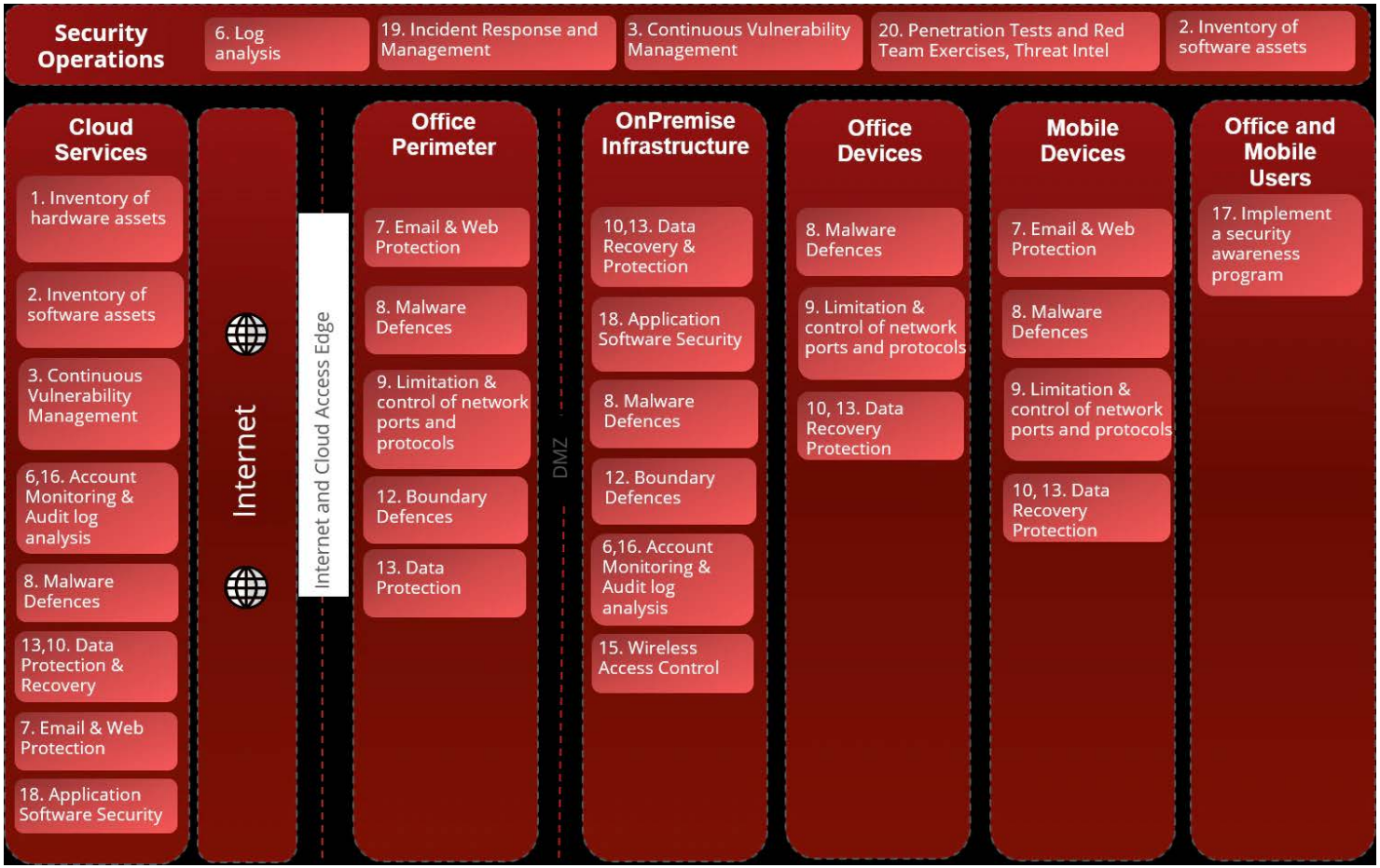
- Critical security controls likely to be effective against defensive evasion and credential access techniques:

MITRE Tactic	MITRE Technique	CSC Control
Lateral Movement	Third Party Software (T1072) TeamViewer, Anydesk	CSC 5 Secure Configuration CSC 8 Malware Defenses CSC 12 Boundary Defenses
Lateral Movement	Service Execution (T1035) PS Exec	CSC 5 Secure Configuration CSC 8 Malware Defenses CSC 12 Boundary Defenses
MITRE Tactic	**MITRE Technique**	**CSC Control**
Collection	Data from Information Repositories (T1213)	CSC 4 Control Admin Privileges CSC 5 Secure Configuration CSC 6 Log Analysis
Collection	Data from local system (T1005)	CSC 4 Control Admin Privileges CSC 5 Secure Configuration CSC 6 Log Analysis
Collection	Data from network shared drive (T1039)	CSC 4 Control Admin Privileges CSC 5 Secure Configuration CSC 6 Log Analysis
MITRE Tactic	**MITRE Technique**	**CSC Control**
Command and Control	Ingress Tool Transfer (T1105)	CSC 8 Malware Defenses CSC 12 Boundary Defenses
MITRE Tactic	**MITRE Technique**	**CSC Control**
Impact	Data Encrypted (T1486) NetWalker Ransomeware	CSC 5 Secure Configuration CSC 8 Malware Defenses
Impact	Inhibit System Recovery (T1490) Shadow	CSC 5 Secure Configuration CSC 8 Malware Defenses

Data source: McAfee

Mitigation Practices: CIS Security Controls

- Mapping NetWalker capabilities against CIS Controls:



yara

https://raw.githubusercontent.com/k-vitali/Malware-Misc-RE/master/2020-03-19-netwalker-yara-config-yar-vk.yar

```
///////////////////////////////////////////////////////////////////////////////////////
///////////////////////////////////////////////////////////////////////////////////////
/////////////////////////////// NETWALKER YARA ////////////////////////////////////////
///////////////////////////////////////////////////////////////////////////////////////

rule crime_win32_netwalker_1 {
meta:
        description = "Detects Netwalker Ransomware Variant"
        author = "@VK_Intel"
        reference = "twitter"
        date = "2020-03-19"

strings:
        $str1 = "unlock"
        $str2 = "spsz"
        $str3 = "onion"


$start_code = {e8 ?? ?? ?? ?? 85 c0 74 ?? e8 ?? ?? ?? ?? 85 c0 74 ?? e8 ?? ?? ?? ?? 85 c0 74 ?? e8 ?? ?? ?? ?? e8 ?? ?? ?? ?? 6a 01 8b ?? ?? ?? ?? ?? ff d0 6a 01 ff ?? ?? ?? ?? ?? 33 c0 c2 10 00}


condition:
( uint16(0) == 0x5a4d and
( 3 of them )
) or ( all of them )
}

///////////////////////////////////////////////////////////////////////////////////////
///////////////////////////////////////////////////////////////////////////////////////
/////////////////////////////// NETWALKER CONFIG //////////////////////////////////////
///////////////////////////////////////////////////////////////////////////////////////
```


```
{"mpk :"/fqCb2TTvBeb3VoL4lXa1fgDDn+sEO4+mBhIj9vrLEk= ","mode :0,"spsz :15360,"thr :1000,"namesz :8,"idsz :6,"lfile :"{id}-Readme.txt ,"onion :"rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion
,"lend
:"SGkhDQpZb3VyIGZpbGVzIGFyZSBlbmNyeXB0ZWQgYnkgTmV0d2Fsa2VyLg0KQWxsIGVuY3J5cHRlZCBmaWxlcyBmb3IgdGhpcyBjb21wdXRlciBoYXMgZXh0ZW5zaW9uOiAue2lkfQ0KDQotLQ0KSWYgZm9yIHNvbWUgcmVhc29uIHlvdSByZWFkIHRoaXMgdGV4dCBiZWZvcm
UgdGhlIGVuY3J5cHRpb24gZW5kZWQsDQp0aGlzIGNhbiBiZSBlbmRlcnN0b29kIGJ5IHRoZSBmYWN0IHRoYXQgdGhlIGNvbXB1dGVyIHNsb3dzIGRvd24sIA0KYW5kIHlvdXIgaGVhcnQgcmF0ZSBoYXMgaW5jcmVhc2VkIGR1ZSB0byB0aGUgYWJpbGl0eSB0byB0dXJuIG10IG
9mZiwNCnRoZW4gd2UgcmVjb21tZW5kIHRoYXQgeW91IG1vdmUgYXdheSBmcm9tIHRoZSBjb21wdXRlciBhbmQgYWNjZXB0IHRoYXQgeW91IGhhdmUgYmVlbiBjb21wcm9taXNlZC4NClJlYm9vdGluZy9zaHV0ZG93biB3aWxsIGNhdXNlIHlvdSB0byBsb3NlIGZpbGVzIHdpdG
hvdXQgdGhlIHBvc3NpYmlsaXR5IG9mIHJlY292ZXJ5Lg0KDQotLQ0KT3VyICBlbmNyeXB0aW9uIGFsZ29yaXRobXMgYXJlIHZlcnkgc3Ryb25nIGFuZCB5b3VyIGZpbGVzIGFyZSB2ZXJ5IHdlbGwgcHJvdGVjdGVkLCANCnRoZSBvbmx5IHdheSB0byBnZXQgeW91ciBmaWxlcy
BiYWNrIGlzIHRvIGNvb3BlcmF0ZSB3aXRoIHVzIGFuZCBnZXQgdGhlIGRlY3J5cHRlciBwcm9ncmFtLg0KDQpEbyBub3QgdHJ5IHRvIHJlY292ZXIgeW91ciBmaWxlcyB3aXRob3V0IGEgZGVjcnlwdGVyIHByb2dyYW0sIHlvdSBtYXkgZGFtYWdlIHRoZW0gYW5kIHRoZW4gdG
hleSB3aWxsIGJlIGltcG9zc2libGUgdG8gcmVjb3Zlci4NCg0KRm9yIHVzIHRoaXMgaXMganVzdCBidXNpbmVzcyBhbmQgdG8gcHJvdmUgdG8geW91IG91ciBzZXJpb3VzbmVzcywgd2Ugd2lsbCBkZWNyeXB0IHlvdSBvbmUgZmlsZSBmb3IgZnJlZS4NCkp1c3Qgb3BlbiBvdX
Igd2Vic2l0ZSwgdXBsb2FkIHRoZSBlbmNyeXB0ZWQgZmlsZSBhbmQgZ2V0IHRoZSBkZWNyeXB0ZWQgZmlsZSBmb3IgZnJlZS4NCg0KLS0NCg0KU3RlcHMgdG8gZ2V0IGFjY2VzcyBvbiBvdXIgd2Vic2l0ZToNCg0KMS5Eb3dubG9hZCBhbmQgaW5zdGFsbCB0b3ItYnJvd3Nlcj
ogaHR0cHM6Ly90b3Jwcm9qZWN0Lm9yZy8NCg0KMi5PcGVuIG91ciB3ZWJzaXRlOiB7b25pb259DQoNCjMuUHV0IHlvdXIgcGVyc29uYWwgY29kZSBpbiB0aGUgaW5wdXQgZm9ybToNCg0Ke2NvZGV9 ,"white :{"path :["*system volume information
,"*windows.old ,"*:\users\*\*temp mp","*msocache ,"*:\winnt ","*$windows.~ws ,"*perflogs ,"*boot ,"*:\windows ","*:\program file*\vmware e","\\*\users\*\*temp temp","\\*\winnt nt","\\*\windows ws","*\program
file*\vmware e","*appdata*microsoft ,"*appdata*packages ,"*microsoft\provisioning ","*dvd maker ,"*Internet Explorer ,"*Mozilla ,"*Mozilla* ,"*Old Firefox data ,"*\program file*\windows media* *","*\program
file*\windows portable* *","*windows defender ,"*\program file*\windows nt t","*\program file*\windows photo* *","*\program file*\windows side* *","*\program file*\windowspowershell l","*\program file*\cuass*
*","*\program file*\microsoft games s","*\program file*\common files\system em","*\program file*\common files\*shared ed","*\program file*\common files\reference ass* s*","*\windows\cache* *","*temporary
internet* ,"*media player ,"*:\users\*\appdata\*\microsoft soft","\\*\users\*\appdata\*\microsoft rosoft"],"file :["ntuser.dat* ,"iconcache.db ,"gdipfont*.dat ,"ntuser.ini ,"usrclass.dat ,"usrclass.dat*
,"boot.ini ,"bootmgr ,"bootnxt ,"desktop.ini ,"ntuser.dat ,"autorun.inf ,"ntldr ,"thumbs.db ,"bootsect.bak ,"bootfont.bin ],"ext :["msp ,"exe ,"sys ,"msc ,"mod ,"clb ,"mui ,"regtrans-ms ,"theme ,"hta ,"shs
,"nomedia ,"diagpkg ,"cab ,"ics ,"msstyles ,"cur ,"drv ,"icns ,"diagcfg ,"dll ,"ocx ,"lnk ,"ico ,"idx ,"ps1 ,"mpa ,"cpl ,"icl ,"msu ,"msi ,"nls ,"scr ,"adv ,"386 ,"com ,"hlp ,"rom ,"lock ,"386 ,"wpx ,"ani
,"prf ,"rtp ,"ldf ,"key ,"diagcab ,"cmd ,"spl ,"deskthemepack ,"bat ,"themepack ]},"kill :{"use :true,"prc :["nslsvice.exe ,"pg* ,"nservice.exe ,"cbvscserv* ,"ntrtscan.exe ,"cbservi* ,"hMailServer* ,"IBM*
,"bes10* ,"black* ,"apach* ,"bd2* ,"db* ,"ba* ,"be* ,"QB* ,"oracle* ,"wbengine* ,"vee* ,"postg* ,"sage* ,"sap* ,"bl* ,"fdlaunch* ,"msmdsrv* ,"report* ,"msdtssr* ,"coldfus* ,"cfdot* ,"swag* ,"swstrtr*
,"jetty.exe ,"wrsa.exe ,"team* ,"agent* ,"store.exe ,"sql* ,"sqbcoreservice.exe ,"thunderbird.exe ,"ocssd.exe ,"encsvc.exe ,"excel.exe ,"synctime.exe ,"mspub.exe ,"ocautoupds.exe ,"thebat.exe ,"dbeng50.exe
,"*sql* ,"mydesktopservice.exe ,"onenote.exe ,"outlook.exe ,"powerpnt.exe ,"msaccess.exe ,"tbirdconfig.exe ,"wordpad.exe ,"ocomm.exe ,"dbsnmp.exe ,"thebat64.exe ,"winword.exe ,"oracle.exe ,"xfssvccon.exe
,"firefoxconfig.exe ,"visio.exe ,"mydesktopqos.exe ,"infopath.exe ,"agntsvc.exe ],"svc :["Lotus* ,"veeam* ,"cbvscserv* ,"hMailServer ,"backup* ,"*backup* ,"apach* ,"firebird* ,"ibmiasrw ,"IBM Domino* ,"Simply
Accounting Database Connection Manager ,"IASJet ,"QB* ,"*sql* ,"sql* ,"QuickBooksDB* ,"IISADMIN ,"omsad ,"dc*32 ,"server Administrator ,"wbengine ,"mr2kserv ,"MSExchange* ,"ShadowProtectSvc ,"SP*4
,"teamviewer ,"MMS ,"AcronisAgent ,"ARSM ,"AcrSch2Svc ,"vsnapvss ,"SPXService ,"StorageCraft ImageManager ,"wrsvc ,"stc_endpt_svc ,"acrsch2svc* ],"svcwait :0,"task :["reboot ,"restart ,"shutdown ,"logoff
,"back ]},"net :{"use :true,"ignore :{"use :true,"disk :true,"share :["ipc$ ,"admin$ ]}},"unlocker :{"use :true,"ignore :{"use :true,"pspath :["*:\windows* ","*:\winnt* ","*:\program file*\vmwar*
*","*\Program File*\Fortinet t"],"prc :["psexec.exe ,"system ,"forti*.exe ,"fmon.exe ,"fcaptmon.exe ,"FCHelper64.exe ]}}}
```

Mitigation Practices: YARA Rule


```
rule CrowdStrike_CSIT_20081_01 : circus_spider netwalker ransomware
{
    meta:
        copyright = "(c) 2020 CrowdStrike Inc."
        description = "Detects the NetWalker ransomware"
        reports = "CSIT-20081"
        version = "202004281747"
        last_modified = "2020-04-28"
        malware_family = "NetWalker"
    strings:
        $salsaconst = "expand 32-byte kexpand 16-byte k"
        $ins_getapi = { 55 8B EC A1 ?? ?? ?? ?? 5D C3 }
        $ins_crc32 = { 25 20 83 B8 ED 33 D0 }
        $ins_push1337 = { 68 39 05 00 00 68 69 7A 00 00 }
        $ins_rc4 = { 8B 45 ( E? |F? ) 83 C0 01 33 D2 B9 00 01 00 00 F7 F1 89 55 }
        $ins_c25519 = { 6A 00 68 41 DB 01 00 }
    condition:
        3 of them
}
rule CrowdStrike_CSIT_20081_02 : circus_spider netwalker ransomware

{
    meta:
        copyright = "(c) 2020 CrowdStrike Inc."
        description = "Detects the NetWalker ransomware"
        reports = "CSIT-20081"
        version = "202004281748"
        last_modified = "2020-04-28"
        malware_family = "NetWalker"
    strings:
        $ = "namesz" fullword
        $ = "crmask" fullword
        $ = "idsz" fullword
        $ = "lend" fullword
        $ = "lfile" fullword
        $ = "mpk" fullword
        $ = "namesz" fullword
        $ = "pspath" fullword
        $ = "rwsz" fullword
        $ = "spsz" fullword
        $ = "svcwait" fullword
        $ = "unlocker" fullword
        $ = "onion1" fullwordcondition:10 of them
}
```

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

- There is a significant quantity of indicators of compromise related to NetWalker available on the Internet. Only a very small sample of them are included below.
- Upon being released to the public, IOCs may become “burned” - the attackers will adjust their TTPs, weapon and infrastructure so that the public IOCs are no longer used.
- 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 cyberdefense infrastructure.

https://github.com/advanced-threat-research/IOCs/blob/master/2020/2020-08-03-Take-a-NetWalk-on-the-wild-side/2020-08-03-Take-a-NetWalk-on-the-wild-side.csv

https://labs.sentinelone.com/netwalker-ransomware-no-respite-no-english-required/

- 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 Maze.

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); Keep signatures and rules updated.	[6.S.C], [6.M.C], [6.L.C]
Implement spam filters at the email gateways; Keep signatures and rules updated.	[1.S.A], [1.M.A]
Block suspicious IP addresses at the firewall; Keep firewall rules are updated.	[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

Reference Materials

References

TECHNICAL REPORTS

Take a “NetWalk” on the Wild Side

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/take-a-netwalk-on-the-wild-side

CrowdStrike Intelligence Report: A Technical Analysis of the NetWalker Ransomware

https://www.crowdstrike.com/resources/reports/netwalker-ransomware-technical-analysis/

NetWalker Ransomware: No Respite, No English Required

https://labs.sentinelone.com/netwalker-ransomware-no-respite-no-english-required/

The DFIR Report: NetWalker Ransomware in 1 Hour

https://thedfirreport.com/2020/08/31/netwalker-ransomware-in-1-hour/

FBI Flash: MI-000-130-MW (TLP: WHITE)

https://www.documentcloud.org/documents/7009488-FBI-FLASH-7-28-2020-BC.html

McAfee Defender’s Blog: NetWalker

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-defenders-blog-netwalker/

Netwalker ransomware tools give insight into threat actor

https://news.sophos.com/en-us/2020/05/27/netwalker-ransomware-tools-give-insight-into-threat-actor/

Reflective Loading Runs Netwalker Fileless Ransomware

https://www.trendmicro.com/en_us/research/20/e/netwalker-fileless-ransomware-injected-via-reflective-loading.html

NetWalker Ransomware Group Enters Advanced Targeting “Game”

https://www.advanced-intel.com/post/netwalker-ransomware-group-enters-advanced-targeting-game

References

PUBLIC ATTACKS

Ransomware Attack Hinders Toll Group Operations
https://threatpost.com/ransomware-attack-hinders-toll-group-operations/152552/

Fresh virus misery for Illinois: Public health agency taken down by... web ransomware. Great timing, scumbags
https://www.theregister.com/2020/03/12/ransomware_illinois_health/

Michigan State University hit by ransomware gang
https://www.zdnet.com/article/michigan-state-university-hit-by-ransomware-gang/

City of Weiz (Austria): Computers infected with ransomware?
https://borncity.com/win/2020/05/22/sterreich-it-der-stadt-weiz-mit-ransomware-infiziert/

Lorien Health Services discloses ransomware attack affecting nearly 50,000
https://www.bleepingcomputer.com/news/security/lorien-health-services-discloses-ransomware-attack-affecting-nearly-50-000/

Amid coronavirus scare, ransomware targets public health agency in Illinois
https://statescoop.com/amid-coronavirus-scare-ransomware-targets-public-health-agency-illinois/

Netwalker allegedly breached The Center for Fertility and Gynecology
https://cybleinc.com/2020/08/06/netwalker-claims-to-have-breached-the-center-for-fertility-and-gynecology/

Ransomware Strikes Third US College in a Week
https://www.infosecurity-magazine.com/news/ransomware-strikes-third-us/

Philadelphia-area health system says it 'isolated' a malware attack
https://www.cyberscoop.com/crozer-keystone-cyber-attack-netwalker-ransomware/

References

PUBLIC ATTACKS

The University Of California Pays $1 Million Ransom Following Cyber Attack

https://www.forbes.com/sites/daveywinder/2020/06/29/the-university-of-california-pays-1-million-ransom-following-cyber-attack/#48986c1918a8

Philadelphia-area health system says it 'isolated' a malware attack

https://www.cyberscoop.com/crozer-keystone-cyber-attack-netwalker-ransomware/

University After University, NetWalker Operators on a Ransomware Attack Spree

https://cyware.com/news/university-after-university-netwalker-operators-on-a-ransomware-attack-spree-be715f25

Netwalker ransomware continues assault on US colleges, hits UCSF

https://www.bleepingcomputer.com/news/security/netwalker-ransomware-continues-assault-on-us-colleges-hits-ucsf/

US uni admits paying US$1.14m ransom to gang using NetWalker

https://www.itwire.com/security/us-uni-admits-paying-us$1-14m-ransom-to-gang-using-netwalker.html

UCSF Pays $1.14M to NetWalker Hackers After Ransomware Attack

https://healthitsecurity.com/news/ucsf-pays-1.14m-to-netwalker-hackers-after-ransomware-attack

Netwalker ransomware hits Pakistan's largest private power utility

https://www.bleepingcomputer.com/news/security/netwalker-ransomware-hits-pakistans-largest-private-power-utility/

Australian firm Tandem Corp hit by Windows NetWalker ransomware

https://www.crn.com/slide-shows/security/equinix-breach-7-things-to-know-about-netwalker-ransomware-attacks

NetWalker Ransomware Operators Targets Stellar Corporation, Leading Customer Experience Management Organisation

https://cybleinc.com/2020/05/26/netwalker-ransomware-operators-targets-stellar-corporation-leading-customer-experience-management-organisation/

References

PUBLIC ATTACKS

Ransomware Hacking Groups Post Data from 5 Healthcare Entities

https://healthitsecurity.com/news/ransomware-hacking-groups-post-data-from-5-healthcare-entities

Equinix Breach: 7 Things To Know About Netwalker Ransomware Attacks

https://www.crn.com/slide-shows/security/equinix-breach-7-things-to-know-about-netwalker-ransomware-attacks

FBI warns of Netwalker ransomware targeting US government and orgs

https://www.bleepingcomputer.com/news/security/fbi-warns-of-netwalker-ransomware-targeting-us-government-and-orgs/

NetWalker ransomware group claims attack on Fort Worth transportation agency

https://www.scmagazine.com/home/security-news/ransomware/netwalker-ransomware-group-claims-attack-on-fort-worth-transportation-agency/

NetWalker Ransomware Expands Operations, Targeting Healthcare

https://healthitsecurity.com/news/netwalker-ransomware-expands-operations-targeting-healthcare

FBI Alerts to Rise in Targeted Netwalker Ransomware Attacks

https://healthitsecurity.com/news/fbi-alerts-to-rise-in-targeted-netwalker-ransomware-attacks

New Ransomware Strain Halts Toll Group Deliveries

https://www.bleepingcomputer.com/news/security/new-ransomware-strain-halts-toll-group-deliveries/

References

MISCELANEOUS

NetWalker Ransomware – What You Need to Know

https://www.tripwire.com/state-of-security/featured/netwalker-ransomware-what-need-know/

How the Nasty Netwalker Behaved in Past Few Months

https://cyware.com/news/how-the-nasty-netwalker-behaved-in-past-few-months-257c8217

Beware Of This New Windows 10 Ransomware Threat Hiding In Plain Sight

https://www.forbes.com/sites/daveywinder/2020/03/05/beware-of-this-new-windows-10-ransomware-threat-hiding-in-plain-sight/#1e76bb652958

Mailto Ransomware under the skin of explorer.exe

https://blogs.quickheal.com/mailto-ransomware-hiding-under-explorer-exe/

Threat intelligence and the importance of knowing your 'attackers'

https://www.computerfutures.com/en-jp/blog/2020/06/threat-intelligence-and-the-importance-of-knowing-your-attackers/

Hackers are still running coronavirus-related campaigns, CrowdStrike warns

https://www.cyberscoop.com/coronavirus-hacking-disinformation-ransomware-spearphishing/

NetWalker Ransomware Tools Reveal Attacker Tactics and Techniques

https://www.darkreading.com/attacks-breaches/netwalker-ransomware-tools-reveal-attacker-tactics-and-techniques/d/d-id/1337929

Situational Awareness: Cyber Threats Heightened by COVID-19 and How to Protect Against Them

https://www.crowdstrike.com/blog/covid-19-cyber-threats/

FBI: COVID-19-Themed Phishing Spreads Netwalker Ransomware

https://www.bankinfosecurity.com/fbi-covid-19-themed-phishing-spreads-netwalker-ransomware-a-14744

References

Netwalker Yara Rule

https://raw.githubusercontent.com/k-vitali/Malware-Misc-RE/master/2020-03-19-netwalker-yara-config-yar-vk.yar

Netwalker Ransomware Infecting Users via Coronavirus Phishing

https://www.bleepingcomputer.com/news/security/netwalker-ransomware-infecting-users-via-coronavirus-phishing/

Situational Awareness: Cyber Threats Heightened by COVID-19 and How to Protect Against Them

https://www.crowdstrike.com/blog/covid-19-cyber-threats/

NetWalker adjusts ransomware operation to only target enterprise

https://www.bleepingcomputer.com/news/security/netwalker-adjusts-ransomware-operation-to-only-target-enterprise/

Netwalker ransomware actors go fileless to make attacks untraceable

https://www.scmagazine.com/home/security-news/ransomware/netwalker-ransomware-actors-go-fileless-to-make-attacks-untraceable/

This is Netwalker, the ramsonware that has hospitals in its sights

https://webeenow.com/this-is-netwalker-the-ramsonware-that-has-hospitals-in-its-sights/

McAfee Says NetWalker Ransomware Generated $25M Over 4 Months

https://cointelegraph.com/news/mcafee-says-netwalker-ransomware-generated-25m-over-4-months

Netwalker ransomware earned $25 million in just five months

https://www.bleepingcomputer.com/news/security/netwalker-ransomware-earned-25-million-in-just-five-months/

NetWalker RaaS Makes $25m in Five Months

https://www.infosecurity-magazine.com/news/netwalker-raas-makes-25-million-in/

IoCs/Ransomware-Netwalker

https://github.com/sophoslabs/IoCs/blob/master/Ransomware-Netwalker

Upcoming Briefs

- Zero Trust in Healthcare
- TrueFighter and RDP Access

Interested in learning more about CIS controls?

See our presentation here: https://www.hhs.gov/sites/default/files/cis-controls-and-the-hph.pdf

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.**

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

Products

Sector & Victim Notifications

Directs 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.

Questions

Contact

Health Sector Cybersecurity Coordination Center (HC3)

202-691-2110

HC3@HHS.GOV