NetWalker Ransomware

09/24/2020
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

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
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
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
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:

Image source: McAfee
Timeline of Major Activity

• August / September 2019: Began operations
• March 2020: Significant changes to operations
  o Shift to network intrusion-focused Ransomware-as-a-Service (RaaS) model
• May 2020: Continuing to change and evolve tactics and operations
  o Observed using reflective dynamic-link library (DLL) injection to infect victims
  o Actively recruiting partners for RaaS operations; specific set of criteria
  o 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
  o 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
  o NetWalker is attacking healthcare organizations during the pandemic
• September 2020:
  o Compromise of K-Electric
  o Compromise of American data center
Affiliates

• To be an affiliate:
  o Preconditions and screening
  o 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
  o “Quality, not quantity”
  o What targets is a potential affiliate interested in?
  o What experience do they have? How can they prove it?
  o Proof of persistent access to valuable targets and intentions

Image source: Sentinel Labs
Affiliates (continued)

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

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.
• Features of their software:
  o Fully automated TOR-based chat panel
  o Support for Windows 2000 and above
  o Full visibility into potential target environments
  o Fast and multi-threaded locker
  o Highly flexible configuration options
  o Encrypts adjacent network volumes
  o Unique build and obfuscation process
  o Automated blog for victim data posting
Netwalker threat actor toolset on the ATT&CK matrix

**Initial access**
- Exploit Tomcat
- Exploit Weblogic
- Phishing email

**Execution**
- PowerShell scripts
  - psexec

**Privilege escalation**
- CVE-2020-0796
- CVE-2019-1458
- CVE-2017-0213
- CVE-2015-1701

**Defense evasion**
- Fileless loading
  - Eset AV remover
  - Gordon’s Eset password recovery
  - Trend Micro’s Security Agent Uninstall Tool
  - Microsoft Security Client uninstall

**Credential access**
- Mimikatz
- Mimidogz
- Mimirkttonz
- Windows Credentials Editor
  - pwdump
  - NLBrute
  - LaZagne
  - WinPwn

**Discovery**
- SoftPerfect Network Scanner
- NLBrute

**Lateral movement**
- psexec
- Teamviewer
- Anydesk

**Impact**
- Netwalker ransomware
- Zeppelin ransomware
- Data exfiltration
Attack Process

- Standard attack:

### MITRE Tactic | MITRE Techniques
---|---
Initial Access | Exploit Public Facing Application (T1103)
Initial Access | Spear Phishing Attachment (T1566.001) Email
Initial Access | Valid Accounts (T1078) RDP Compromised

### MITRE Tactic | MITRE Techniques
---|---
Execution | PowerShell Script (T1050.001), Service Execution (T1568.002), Command and Scripting Interpreter (T1059.003), Native API (T1100), WMI (T1047)
Persistence | Registry Key - Place Value on Run Once Key (T1060), Modify Registry key – Create own key (T1112)
Privilege Escalation | Exploitation for Privilege Escalation (T1068), Process Injection (T1055.001)
Defensive Evasion | Disabling Security Tools (T1180), Process Injection (T1055), Deobfuscate/Decode Files or Information (T1404), Obfuscated Files or Information (T1027)
Credential Access | Credential Dumping (T1043), Brute Force (T1110)

### MITRE Tactic | MITRE Techniques
---|---
Discovery | Network Service Scanning (T1046), Security Software Discovery (T1538.001), 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 (T1003), Data from network shared drive (T1059)
Command and Control | Ingress Tool Transfer (T1105)
Impact | Data Encrypted (T1486), Network Ransomware, Inhibit System Recovery (T1400), Service Stop (T1489)

Image source: McAfee
Communications between victim and NetWalker

Ransom portal login

For enter, please use user code or user key

User key: 

User code: 

Captcha code:

Submit ▶

Source of image: McAfee
Communications between victim and NetWalker

Portal to upload files to test decryption

For test we can upload and decrypt 3 images or document files free
File must be less than 3 megabyte.
Allow formats: .jpg, jpeg, .png, .bmp, .doc, .docx

Choose a file or drag it here

Upload and decrypt file free

Source of images: McAfee
Communications between victim and NetWalker

Ransom portal landing page

Source of image: McAfee
Communications between victim and NetWalker

**Negotiation**

- **Operator**: I can see from log you decrypted 2 files, the text will be decrypted too.
  - **You**: I don't know. $54,500 is really our limit. It's probably a little more than what the rebuilding costs are but I think decryption will be faster. We're open to going with either option, but if you can accept $14,500 then we have a deal.
  - **Operator**: ok. 14,500
- **Operator**: we can make you a 10% discount if you pay in 5 days time
  - **You**: 07.30.19 (11:00)

**Payment and invoice**

- Source of images: McAfee

**Delivery of decryptor**

- decrypt.exe
- decrypter.zip
- info.txt

This decrypt file for ALL NETWORK / ALL COMPUTERS / ALL FILES

Run decrypt.exe on PC which you want decrypt. Click "Auto decrypt" -> click "Delete decrypter mode file" -> click "Decrypt".

The program will automatically decrypt all files on an encrypted PC. The decryption program will fit all encrypted PCs.

After running the decryption in automatic or manual mode, the program can be closed only when the close button becomes active. Never kill the process, if you kill the process your files will be damaged and they will not be able to recover.

If you want to decrypt the entire network at once, use the following command:

```
addc.exe parameters = "decrypt.exe" /S /D
```

/s - silent mode.
/d - delete lending (optional, not work without /s).

The program exit code will indicate the number of decrypted files.
Communications between victim and NetWalker

Frequently Asked Questions (FAQ)

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.coindeX.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 decrypter program, you get technical support.

Source of image: McAfee
### Critical security controls likely to be effective against initial infection and exploitation techniques:

<table>
<thead>
<tr>
<th>MITRE Tactic</th>
<th>MITRE Technique</th>
<th>CIS Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Access</td>
<td>Exploit Public-Facing Applications (T1190) Tomcat, Web Logic</td>
<td>CSC 2 – Inventory of Software Assets&lt;br&gt;CSC 3 – Continuous Vulnerability Assessment&lt;br&gt;CSC 5 – Secure Configuration&lt;br&gt;CSC 9 – Limitation of Network Ports and Protocols&lt;br&gt;CSC 12 – Boundary Defense&lt;br&gt;CSC 18 – Application Software Security</td>
</tr>
<tr>
<td>Initial Access</td>
<td>Spear Phishing Attachments (T1566.001)</td>
<td>CSC 7 – Email and Web Browser Protection&lt;br&gt;CSC 8 – Malware Defenses &lt;br&gt;CSC 5 – Secure Configuration of hardware and software&lt;br&gt;CSC 9 – Limitation of Network Ports and Protocols&lt;br&gt;CSC 12 – Boundary Defense</td>
</tr>
<tr>
<td>Initial Access</td>
<td>Valid Accounts (T1078) RDP Compromised</td>
<td>CSC 5 – Secure Configuration&lt;br&gt;CSC 8 Malware Defenses &lt;br&gt;CSC 9 – Limitation of Network Ports and Protocols&lt;br&gt;CSC 12 – Boundary Defense</td>
</tr>
<tr>
<td>Execution</td>
<td>PowerShell (T1059.001) PowerShell Script</td>
<td>CSC 5 Secure Configuration&lt;br&gt;CSC 8 Malware Defenses</td>
</tr>
<tr>
<td>Execution</td>
<td>Service Execution (T1569.002) PS Exec</td>
<td>CSC 5 Secure Configuration&lt;br&gt;CSC 8 Malware Defenses</td>
</tr>
<tr>
<td>Execution</td>
<td>Command and Scripting Interpreter (T1059.003) Windows Command Shell</td>
<td>CSC 5 Secure Configuration&lt;br&gt;CSC 8 Malware Defenses</td>
</tr>
<tr>
<td>Execution</td>
<td>Native API (T1106) Use Windows API functions to inject DLL</td>
<td>CSC 5 Secure Configuration&lt;br&gt;CSC 8 Malware Defenses</td>
</tr>
<tr>
<td>Execution</td>
<td>Windows Management Instrumentation (T1047)</td>
<td>CSC 4 Controlled Use of Admin Privileges&lt;br&gt;CSC 5 Secure Configuration&lt;br&gt;CSC 9 Limitation of Network Ports and Protocols&lt;br&gt;CSC 8 Malware Defenses</td>
</tr>
</tbody>
</table>

Data source: McAfee
Technical Operations

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

<table>
<thead>
<tr>
<th>MITRE Tactic</th>
<th>MITRE Technique</th>
<th>CIS Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persistence</td>
<td>Registry Key – Place Value on Run Once Key (T1060)</td>
<td>CSC 5 Secure Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CSC 8 Malware Defenses</td>
</tr>
<tr>
<td>Persistence</td>
<td>Modify Registry key – Create own key (T1112)</td>
<td>CSC 5 Secure Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CSC 8 Malware Defenses</td>
</tr>
</tbody>
</table>

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

Data source: McAfee
• Critical security controls likely to be effective against defensive evasion, credential access and discovery techniques:

<table>
<thead>
<tr>
<th>MITRE Tactic</th>
<th>MITRE Technique</th>
<th>CIS Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defensive Evasion</td>
<td>Disabling Security Tools (T1562.001) ESET, Trend Micro, MS</td>
<td>CSC 5 Secure Configuration</td>
</tr>
<tr>
<td>Defensive Evasion</td>
<td>Process Injection: Reflective DLL (T1055)</td>
<td>CSC 8 Malware Defenses</td>
</tr>
<tr>
<td>Defensive Evasion</td>
<td>Deobfuscate / Decode Files or Information (T1140)</td>
<td>CSC 5 Secure Configuration</td>
</tr>
<tr>
<td>Defensive Evasion</td>
<td>Obfuscated Files or Information (T1027): PowerShell Script uses Base64 and hexadecimal encoding and XOR-encryption</td>
<td>CSC 8 Malware Defenses</td>
</tr>
<tr>
<td>Credential Access</td>
<td>Credential Dumping (T1003) Mimikatz, Mimidogz, Mimikittenz, Pwdump, LaZagne, Windows Credentials</td>
<td>CSC 4 Controlled Use of Admin Privileges</td>
</tr>
<tr>
<td>Credential Access</td>
<td>Brute Force (T1110) NL Brute</td>
<td>CSC 5 Secure Configuration</td>
</tr>
<tr>
<td>Discovery</td>
<td>Network Service Scanning (T1046) Network Scanner</td>
<td>CSC 8 Malware Defenses</td>
</tr>
</tbody>
</table>

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

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

Data source: McAfee
Mitigation Practices: CIS Security Controls

- Mapping NetWalker capabilities against CIS Controls:
Mitigation Practices: YARA Rule

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 89 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
        $ = "fille" fullword
        $ = "mpk" fullword
        $ = "namesz" fullword
        $ = "pspath" fullword
        $ = "rwsz" fullword
        $ = "spsz" fullword
        $ = "svcwait" fullword
        $ = "unlocker" fullword
        $ = "onion1" fullword
    condition:
        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

Mitigation Practices: NetWalker

- 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.

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

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

The DFIR Report: NetWalker Ransomware in 1 Hour
https://thedefirreport.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

Netwalker ransomware tools give insight into threat actor

Reflective Loading Runs Netwalker Fileless Ransomware

NetWalker Ransomware Group Enters Advanced Targeting “Game”
https://www.advanced-intel.com/post/netwalker-ransomware-group-enters-advanced-targeting-game
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

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

Amid coronavirus scare, ransomware targets public health agency in 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

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

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

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

University After University, NetWalker Operators on a Ransomware Attack Spree

Netwalker ransomware continues assault on US colleges, hits UCSF

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

UCSF Pays $1.14M to NetWalker Hackers After Ransomware Attack

Netwalker ransomware hits Pakistan's largest private power utility

Australian firm Tandem Corp hit by Windows NetWalker ransomware

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

Equinix Breach: 7 Things To Know About Netwalker Ransomware Attacks

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

FBI Alerts to Rise in Targeted Netwalker Ransomware Attacks

New Ransomware Strain Halts Toll Group Deliveries
MISCELLANEOUS

NetWalker Ransomware – What You Need to Know

How the Nasty Netwalker Behaved in Past Few Months

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

Threat intelligence and the importance of knowing your ‘attackers’

Hackers are still running coronavirus-related campaigns, CrowdStrike warns

NetWalker Ransomware Tools Reveal Attacker Tactics and Techniques

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

FBI: COVID-19-Themed Phishing Spreads Netwalker Ransomware
References

Netwalker Yara Rule

Netwalker Ransomware Infecting Users via Coronavirus Phishing

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

NetWalker adjusts ransomware operation to only target enterprise

Netwalker ransomware actors go fileless to make attacks untraceable

This is Netwalker, the ransomware that has hospitals in its sights
https://webeenow.com/this-is-netwalker-the-ransomware-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

NetWalker RaaS Makes $25m in Five Months

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

Upcoming Briefs
• Zero Trust in Healthcare
• TrueFighter and RDP Access

Interested in learning more about CIS controls?

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](mailto: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