Conti Ransomware and the Health Sector

07/08/2021
Agenda

- Recent Ransomware Activity
- Overview of Conti Ransomware
- Conti vs. Healthcare
- FBI Alert on Conti
- Example of a Conti Infection
- Real-world Conti Attacks
- Conti Mapper to MITRE ATT&CK
- Conti Mitigation Practices
- References
- Questions

Slides Key:

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

**Technical**: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)
How has ransomware evolved over time?

- Standard attack: Deploy ransomware, demand ransom
- Managed Service Provider (MSP) compromise
- Big game hunting
- Double encryption
- Multi-stage attack (Emotet, Trickbot, etc…)
  - Sets up other effects
- Ransomware-as-a-service (RaaS)
  - Division of labor
  - Quiet since Colonial Pipeline attack
- Double extortion/Ransomware 2.0
  - Additional fee for not leaking data
  - Leak sites
- Triple extortion
  - Additional fee demanded of partners/customers
- “Quadruple monetization”
- Phone threats
- Executing payloads in virtual machines for obfuscation
- Ransomware groups funded by venture capital

Bottom line: Ransomware operators continue to improve their efficiency and effectiveness, in many cases mirroring the practices of legitimate businesses
• Recent high-profile ransomware attacks against critical infrastructure:
  o Energy
    ▪ Colonial Pipeline
  o Transportation
    ▪ NYC Subway system
  o Chemical
    ▪ Brenntag
  o Information Technology
    ▪ Acer
  o Food & Agriculture
    ▪ JBS
  o Healthcare and Public Health
    ▪ Health Service Executive
  o Emergency Services
    ▪ Washington DC Metropolitan Police Department
  o Financial Services
    ▪ Valley Bank
Recent Government Action on Ransomware

- Cl0p associates arrested
  - Money launderers and not technical operators
- Emotet takedown
  - US Cyber Command and Microsoft action (Fall 2020)
  - Arrest (January 2021)
- Department of Justice – Latvian TrickBot associate Alla Witte detained and indicted
- Biden named-and-shamed Darkside; met with Putin to discuss
- White House executive order
  - Mostly applies to federal government and federal government contractors
- FBI Ransomware task force established
  - Restoration of Colonial Pipeline money
- Seizure of APT29 domains (USAID phishing campaign)
- DHS/CISA Darkside Ransomware Guide
- The Department of Justice hired a liaison prosecutor to help hunt cybercriminals in Eastern Europe
Overview of Conti Ransomware

- First observed in December 2019; significant activity began in July 2020
- Leverages unique AES-256 encryption key per file, then encrypted with an RSA-4096 encryption key
- Often conducts double extortion (leak site launched September 2020)
- “Human-operated” as opposed to automatic
- Conti deletes Windows Volume Shadow Copies prior to encryption and disables 146 Windows services related to backup, security and database capabilities
- During encryption, Conti utilizes the Windows Restart Manager API to terminate Windows services that would otherwise keep a file open and unencryptable
• Connections to Ryuk:
  o Conti’s code appears to be closely based on the malware code from version 2 of Ryuk
  o Distribution: Similar to Ryuk, Conti is typically delivered via TrickBot
  o Ransom note: Conti utilizes the same ransom note template used in early Ryuk attacks
  o Incident rate: ID Ransomware showed Conti submissions increased as Ryuk submissions declined

• Ransom demands reported to be an average of ~$900K and at least as high as $25M (Source: Coveware)

• FBI Flash Alert: May 2021

• Common attack vectors: Phishing, RDP compromise

• Early stage: Malicious Word documents (PowerShell scripts, Cobalt Strike, Emotet, Trickbot and Mimikatz)

• Other TTPs: Living off the land (Sysinternals), poisoned DLLs, Anchor DNS (beaconing)

• Dwell time: One to three weeks

• Uses 32 threads to encrypt system – speed over stealth
Conti Ransom Note

• Four standard components:
  o Notification of attack
  o Futility of non-cooperation
  o Justification for trust
  o Instructions

```
All of your files are currently encrypted by CONTI strain.

As you know (if you don’t - just “google it”), all of the data that has been encrypted by our software cannot be recovered by any means without contacting our team directly. If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of charge.

You can contact our team directly for further instructions through our website:

TOR VERSION:
(you should download and install TOR browser first https://torproject.org)

http://conti[redacted].onion/

HTTPS VERSION:
https://conti[redacted]

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We’ve downloaded a pack of your internal data and are ready to publish it on our news website if you do not respond. So it will be better for both sides if you contact us as soon as possible.

---BEGIN ID---

---END ID---
```
Per Sophos, healthcare is high on Conti’s list of targets:

**Sector/industry represented by organizations with data published on "Conti News" site**

- Retail: 26
- Manufacturing: 25
- Construction: 20
- Public sector - Government: 14
- Public sector - Healthcare: 13
- Information Technology: 12
- Food: 11
- Logistics: 9
- Services: 8
- Legal: 6
- Non-profit: 6
- Real estate: 6
- Education: 4
- Financial: 3
- Pharmaceutical: 2
- Energy: 2
- News Media: 1
- Accounting: 1
- Communication: 1
- Entertainment: 1
- Hospitality: 1
- Mining: 1
- Utilities: 1

Source: "Conti News" site, data analyzed by Sophos, February 2021
HEALTHCARE VICTIMS BY RANSOMWARE FAMILY IN 2020

- Maze: 20
- Conti: 16
- Netwalker: 10
- Revil: 8
- Ryuk: 7
- DoppelPaymer: 6
- Egregor: 5
- Pyra: 4
- Delfy777: 3
- Clop: 2
- LockBit: 1
- MedusaLocker: 1
- Netty X: 1
- RagnaLocker: 1
- Avaddon: 1
- Ekans: 1
- MountLocker: 1
- SunCrypt: 1
If you are a client who declined the deal and did not find your data on cartel's website or did not find valuable files, this does not mean that we forgot about you, it only means that data was sold and only therefore it did not publish in free access!
Ransomware and Malware Relationships

CONTI

Exploit vulnerability or use stolen credentials on exposed infrastructure (VPN, RDP, web servers)

Malspam

Nefilim

Gootkit

Modern ransomware

Flyuk

Triokbot

Emotet

Malspam

Conti

Triokbot

BazarLoader

IcedID

BitPaymer

DoppelPaymer

Egregor

Maze

Emotet

Dridex

Emotet

Dridex

QakBot

QakBot

Malspam

Malspam

Malspam

Malspam

Malspam

Malspam

Malspam

Malspam

Malspam

Malspam
GBs of leaked data as of February to June, 2021:

- **Conti** - 207 GBs
- DoppelPaymer - 155 GBs
- Egregor - 151 GBs
- REvil - 139 GBs
- DarkSide - 38 GBs
- Avaddon - 34 GBs
- Nefilim - 29 GBs
- CI0p - 25 GBs
- Ragnar - 23 GBs
- SunCrypt - 18 GBs
- Ragnarok - 18 GBs
- Mount Locker - 12 GBs
- LockBit - 9 GBs
- Cuba - 8 GBs
- Babuk - 5 GBs
- Ranzy - 3 GBs
Conti – Frequency of Targeting

Per DarkTracer as of June 28, 2021:

Who is the King of Ransomware on the DarkWeb?
(number of affected organizations)
## Most Common Ransomware Variants in Q1 2021

<table>
<thead>
<tr>
<th>Rank</th>
<th>Ransomware Type</th>
<th>Market Share %</th>
<th>Change in Ranking from Q4 2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sodinokibi</td>
<td>14.2%</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>Conti V2</td>
<td>10.2%</td>
<td>+4</td>
</tr>
<tr>
<td>3</td>
<td>Lockbit</td>
<td>7.5%</td>
<td>+6</td>
</tr>
<tr>
<td>4</td>
<td>Clop</td>
<td>7.1%</td>
<td>New in Top Variants</td>
</tr>
<tr>
<td>5</td>
<td>Egregor</td>
<td>5.3%</td>
<td>-3</td>
</tr>
<tr>
<td>6</td>
<td>Avaddon</td>
<td>4.4%</td>
<td>+3</td>
</tr>
<tr>
<td>7</td>
<td>Ryuk</td>
<td>4.0%</td>
<td>-4</td>
</tr>
<tr>
<td>8</td>
<td>Darkside</td>
<td>3.5%</td>
<td>New in Top Variants</td>
</tr>
<tr>
<td>9</td>
<td>Suncrypt</td>
<td>3.1%</td>
<td>-1</td>
</tr>
<tr>
<td>9</td>
<td>Netwalker</td>
<td>3.1%</td>
<td>-5</td>
</tr>
<tr>
<td>10</td>
<td>Phobos</td>
<td>2.7%</td>
<td>-1</td>
</tr>
</tbody>
</table>

*Top 10: Market Share of the Ransomware attacks*
Conti is “a global threat affecting victims mainly in North America and Western Europe”. (Sophos)

What’s missing? Russia and CIS countries
• Released on May 20, 2021
• Title: Conti Ransomware Attacks Impact Healthcare and First Responder Networks
• Previous year’s targeting:
  ▪ 400 organizations worldwide
  ▪ 290 organizations in the U.S.
  ▪ 16 healthcare and first responder organizations in the U.S.
  
  o Ransom demands
  ▪ As high as $25M
  
  o Tactics, Techniques and Procedures:
  ▪ Phishing
    • Word document drops PowerShell script drops Cobalt Strike and Emotet, which drops Conti (via DLLs)
  ▪ Remote Desktop Protocol (credential theft)
  ▪ Living off the land
  ▪ Anchor DNS for beaconing
  ▪ Dwell Time: 4 days to 3 weeks

FBI Alert on Conti
Conti – Average Incident Length

AVERAGE LENGTH OF CONTI INCIDENT

Incident Length in Days

Conti

All Ransomware
Conti – Common Attack Vectors

Attack Vectors used by the Top Three Ransomware Variants

**Attack Vectors - Top 3 Ransomware Types**

- **Email Phishing**, **RDP Compromise**, **Software Vulnerability**, **Other**

**Sodinokibi**

- Email Phishing: 25%
- RDP Compromise: 25%
- Software Vulnerability: 50%
- Other: 0%

**Conti v2**

- Email Phishing: 50%
- RDP Compromise: 25%
- Software Vulnerability: 25%
- Other: 0%

**Lockbit**

- Email Phishing: 10%
- RDP Compromise: 30%
- Software Vulnerability: 60%
- Other: 0%

*Top 3 Ransomware Types: Sodinokibi, Conti v2, and Lockbit.*
Example of a Conti Infection

- Phishing e-mail with zipped attachment includes malicious JavaScript file, which downloads IcedID
- System information, including the computer name and Operating System, are exfiltrated through encoded cookie values
IcedID further reconnaissance efforts:

<table>
<thead>
<tr>
<th>Command Line</th>
<th>Parent Image Path</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cmd.exe /c chcp &amp;gt; &amp;lt;2</code></td>
<td><code>C:\Windows\System32\rundll32.exe</code></td>
</tr>
<tr>
<td><code>ipconfig /all</code></td>
<td><code>C:\Windows\System32\rundll32.exe</code></td>
</tr>
<tr>
<td><code>systeminfo</code></td>
<td><code>C:\Windows\System32\rundll32.exe</code></td>
</tr>
<tr>
<td><code>net config workstation</code></td>
<td><code>C:\Windows\System32\rundll32.exe</code></td>
</tr>
<tr>
<td><code>nlttest /domain_trusts</code></td>
<td><code>C:\Windows\System32\rundll32.exe</code></td>
</tr>
<tr>
<td><code>nlttest /domain_trusts /all_trusts</code></td>
<td><code>C:\Windows\System32\rundll32.exe</code></td>
</tr>
<tr>
<td><code>net view /all /domain</code></td>
<td><code>C:\Windows\System32\rundll32.exe</code></td>
</tr>
<tr>
<td><code>net view /all</code></td>
<td><code>C:\Windows\System32\rundll32.exe</code></td>
</tr>
<tr>
<td><code>net group \&quot;Domain Admins\&quot; /domain</code></td>
<td><code>C:\Windows\System32\rundll32.exe</code></td>
</tr>
</tbody>
</table>
Discovery:

- Additional discovery commands were executed by Cobalt Strike.

<table>
<thead>
<tr>
<th>Initiating Process File Name</th>
<th>Process Command Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>icju1.exe</td>
<td>cmd.exe /C whoami /groups</td>
</tr>
<tr>
<td>icju1.exe</td>
<td>cmd.exe /C query session</td>
</tr>
<tr>
<td>icju1.exe</td>
<td>cmd.exe /C dir %HOMEDRIVE%%HOMEPATH%</td>
</tr>
<tr>
<td>icju1.exe</td>
<td>cmd.exe /C nltest /domain_trusts</td>
</tr>
<tr>
<td>icju1.exe</td>
<td>cmd.exe /C nltest /dclist:</td>
</tr>
<tr>
<td>icju1.exe</td>
<td>cmd.exe /C net group &quot;Enterprise admins&quot; /domain</td>
</tr>
<tr>
<td>icju1.exe</td>
<td>cmd.exe /C net group &quot;Domain admins&quot; /domain</td>
</tr>
</tbody>
</table>
After moving laterally to a domain controller, the attackers use `Dsquery` to look for existing networks across the enterprise infrastructure.

- `cmd.exe /C dsquery subnet - limit 0`

The next step is often port scanning.

Below is port scanning as performed by Conti:
Cobalt Strike Beacon DLL dropped on ADMIN$ share and then distributed throughout environment using PsExec:

<table>
<thead>
<tr>
<th>Initiating Process</th>
<th>Parent File Name</th>
<th>Initiating Process File Name</th>
<th>Initiating Process Command Line</th>
<th>Process Command Line</th>
<th>Action Type</th>
<th>File Name</th>
<th>Library Load</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSEXESVC.exe</td>
<td>rund1132.exe</td>
<td>&quot;rundll32.exe&quot; c:\windows\192145.dll,StartW</td>
<td>cmd.exe /c echo NGAt0DGJpvJwPL6Pfdj&quot; C:\Windows\TEMP\DEM238D.exe &amp;exit</td>
<td>ProcessCreated</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSEXESVC.exe</td>
<td>rund1132.exe</td>
<td>&quot;rundll32.exe&quot; c:\windows\192145.dll,StartW</td>
<td>cmd.exe /c echo NGAt0DGJpvJwPL6Pfdj&quot; C:\Windows\TEMP\DEM238D.exe &amp;exit</td>
<td>ProcessCreated</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSEXESVC.exe</td>
<td>rund1132.exe</td>
<td>&quot;rundll32.exe&quot; c:\windows\192145.dll,StartW</td>
<td>cmd.exe /c echo NGAt0DGJpvJwPL6Pfdj&quot; C:\Windows\TEMP\DEM238D.exe &amp;exit</td>
<td>ProcessCreated</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSEXESVC.exe</td>
<td>rund1132.exe</td>
<td>&quot;rundll32.exe&quot; c:\windows\192145.dll,StartW</td>
<td>cmd.exe /c echo NGAt0DGJpvJwPL6Pfdj&quot; C:\Windows\TEMP\DEM238D.exe &amp;exit</td>
<td>ProcessCreated</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSEXESVC.exe</td>
<td>rund1132.exe</td>
<td>&quot;rundll32.exe&quot; c:\windows\192145.dll,StartW</td>
<td>cmd.exe /c echo NGAt0DGJpvJwPL6Pfdj&quot; C:\Windows\TEMP\DEM238D.exe &amp;exit</td>
<td>ProcessCreated</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSEXESVC.exe</td>
<td>rund1132.exe</td>
<td>&quot;rundll32.exe&quot; c:\windows\192145.dll,StartW</td>
<td>cmd.exe /c echo NGAt0DGJpvJwPL6Pfdj&quot; C:\Windows\TEMP\DEM238D.exe &amp;exit</td>
<td>ProcessCreated</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSEXESVC.exe</td>
<td>rund1132.exe</td>
<td>&quot;rundll32.exe&quot; c:\windows\192145.dll,StartW</td>
<td>cmd.exe /c echo NGAt0DGJpvJwPL6Pfdj&quot; C:\Windows\TEMP\DEM238D.exe &amp;exit</td>
<td>ProcessCreated</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSEXESVC.exe</td>
<td>rund1132.exe</td>
<td>&quot;rundll32.exe&quot; c:\windows\192145.dll,StartW</td>
<td>cmd.exe /c echo NGAt0DGJpvJwPL6Pfdj&quot; C:\Windows\TEMP\DEM238D.exe &amp;exit</td>
<td>ProcessCreated</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSEXESVC.exe</td>
<td>rund1132.exe</td>
<td>&quot;rundll32.exe&quot; c:\windows\192145.dll,StartW</td>
<td>cmd.exe /c echo NGAt0DGJpvJwPL6Pfdj&quot; C:\Windows\TEMP\DEM238D.exe &amp;exit</td>
<td>ProcessCreated</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSEXESVC.exe</td>
<td>rund1132.exe</td>
<td>&quot;rundll32.exe&quot; c:\windows\192145.dll,StartW</td>
<td>cmd.exe /c echo NGAt0DGJpvJwPL6Pfdj&quot; C:\Windows\TEMP\DEM238D.exe &amp;exit</td>
<td>ProcessCreated</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSEXESVC.exe</td>
<td>rund1132.exe</td>
<td>&quot;rundll32.exe&quot; c:\windows\192145.dll,StartW</td>
<td>cmd.exe /c echo NGAt0DGJpvJwPL6Pfdj&quot; C:\Windows\TEMP\DEM238D.exe &amp;exit</td>
<td>ProcessCreated</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSEXESVC.exe</td>
<td>rund1132.exe</td>
<td>&quot;rundll32.exe&quot; c:\windows\192145.dll,StartW</td>
<td>cmd.exe /c echo NGAt0DGJpvJwPL6Pfdj&quot; C:\Windows\TEMP\DEM238D.exe &amp;exit</td>
<td>ProcessCreated</td>
<td>-</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Privilege escalation

- They next obtain system level privileges
  - Cobalt Strike’s built-in named pipe impersonation (GetSystem) functionality.

Lateral movement

- Cobalt Strike Beacon service binaries

---

<table>
<thead>
<tr>
<th>data.win.system.channel</th>
<th>data.win.eventdata.serviceName</th>
<th>data.win.eventdata.imagePath</th>
<th>data.win.eventdata.accountName</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>7a277c9</td>
<td>\ADMIN$\7a277c9.exe</td>
<td>LocalSystem</td>
</tr>
<tr>
<td>System</td>
<td>c30dce8</td>
<td>\ADMIN$\c30dce8.exe</td>
<td>LocalSystem</td>
</tr>
<tr>
<td>System</td>
<td>a43f562</td>
<td>\ADMIN$\a43f562.exe</td>
<td>LocalSystem</td>
</tr>
<tr>
<td>System</td>
<td>d7f0cde</td>
<td>\ADMIN$\d7f0cde.exe</td>
<td>LocalSystem</td>
</tr>
<tr>
<td>System</td>
<td>d8d6deb</td>
<td>\ADMIN$\d8d6deb.exe</td>
<td>LocalSystem</td>
</tr>
<tr>
<td>System</td>
<td>a068564</td>
<td>\ADMIN$\a068564.exe</td>
<td>LocalSystem</td>
</tr>
</tbody>
</table>
Persistence

- Account “nuuser” created by beacon; Commands run on domain controller

```bash
net user /add /Y nuuser 7HeC00l3stP@ssw0rd
net localgroup administrators nuuser /add
```
• The operators use RDP to connect from the beachhead host to the domain controller and other systems throughout the enterprise.

• This RDP activity was being proxied through the IcedID process running on that host, to a remote proxy over port 8080.

The below traffic is the RDP session including the username (nuuser) in the cookie:

<table>
<thead>
<tr>
<th>No.</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>650</td>
<td>38.135.122.194</td>
<td>65164</td>
<td>38.135.122.194</td>
<td>8080</td>
<td>TCP</td>
<td>66</td>
<td>8080 → 65164 SYN Seq=0 Win=64240 Len=0 MSS=1460</td>
</tr>
<tr>
<td>651</td>
<td>38.135.122.194</td>
<td>65164</td>
<td>8080</td>
<td>65164</td>
<td>TCP</td>
<td>66</td>
<td>8080 → 65164 SYN, ACK Seq=0 Ack=1 Win=64240 Len=0</td>
</tr>
<tr>
<td>652</td>
<td>38.135.122.194</td>
<td>65164</td>
<td>38.135.122.194</td>
<td>8080</td>
<td>TCP</td>
<td>60</td>
<td>65164 → 8080 ACK Seq=1 Ack=1 Win=262656 Len=0</td>
</tr>
<tr>
<td>653</td>
<td>38.135.122.194</td>
<td>65164</td>
<td>8080</td>
<td>65164</td>
<td>TCP</td>
<td>67</td>
<td>8080 → 65164 Continuation</td>
</tr>
<tr>
<td>654</td>
<td>38.135.122.194</td>
<td>65164</td>
<td>38.135.122.194</td>
<td>8080</td>
<td>TPKT</td>
<td>60</td>
<td>8080 → 65164 [ACK] Seq=1 Ack=14 Win=64256 Len=0</td>
</tr>
<tr>
<td>655</td>
<td>38.135.122.194</td>
<td>65164</td>
<td>8080</td>
<td>65164</td>
<td>TPKT</td>
<td>60</td>
<td>Continuation</td>
</tr>
<tr>
<td>656</td>
<td>38.135.122.194</td>
<td>65164</td>
<td>38.135.122.194</td>
<td>8080</td>
<td>TPKT</td>
<td>60</td>
<td>Continuation</td>
</tr>
<tr>
<td>657</td>
<td>38.135.122.194</td>
<td>65164</td>
<td>8080</td>
<td>65164</td>
<td>TCP</td>
<td>60</td>
<td>65164 → 8080 ACK Seq=2 Ack=16 Win=64256 Len=0</td>
</tr>
<tr>
<td>658</td>
<td>38.135.122.194</td>
<td>65164</td>
<td>38.135.122.194</td>
<td>8080</td>
<td>TCP</td>
<td>66</td>
<td>Continuation</td>
</tr>
<tr>
<td>659</td>
<td>38.135.122.194</td>
<td>65164</td>
<td>8080</td>
<td>65164</td>
<td>TCP</td>
<td>66</td>
<td>Continuation</td>
</tr>
<tr>
<td>660</td>
<td>38.135.122.194</td>
<td>65164</td>
<td>38.135.122.194</td>
<td>8080</td>
<td>TPKT</td>
<td>66</td>
<td>Continuation</td>
</tr>
<tr>
<td>661</td>
<td>38.135.122.194</td>
<td>65164</td>
<td>8080</td>
<td>65164</td>
<td>TPKT</td>
<td>66</td>
<td>Continuation</td>
</tr>
<tr>
<td>662</td>
<td>38.135.122.194</td>
<td>65164</td>
<td>38.135.122.194</td>
<td>8080</td>
<td>RDP</td>
<td>98</td>
<td>Cookie: mstshash=nuuser, Negotiate Request</td>
</tr>
<tr>
<td>663</td>
<td>38.135.122.194</td>
<td>65164</td>
<td>8080</td>
<td>65164</td>
<td>RDP</td>
<td>73</td>
<td>Negotiate Response</td>
</tr>
</tbody>
</table>
Port scanning of the network, looking for port 445:

<table>
<thead>
<tr>
<th>Source</th>
<th>Source Port</th>
<th>Destination</th>
<th>Destination Port</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>50216</td>
<td>10</td>
<td>445</td>
<td>SMB2</td>
<td>210</td>
<td>Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \10\NC$</td>
</tr>
<tr>
<td>10</td>
<td>50216</td>
<td>10</td>
<td>445</td>
<td>SMB2</td>
<td>130</td>
<td>Ioctl Response, Error: STATUS_FS_DRIVER_REQUIRED</td>
</tr>
<tr>
<td>10</td>
<td>50216</td>
<td>10</td>
<td>445</td>
<td>SMB2</td>
<td>138</td>
<td>Tree Connect Request Tree: \10\NC$</td>
</tr>
<tr>
<td>10</td>
<td>50216</td>
<td>10</td>
<td>445</td>
<td>SMB2</td>
<td>382</td>
<td>Create Request File: readme.txt</td>
</tr>
<tr>
<td>10</td>
<td>50216</td>
<td>10</td>
<td>445</td>
<td>SMB2</td>
<td>410</td>
<td>Create Response File: readme.txt</td>
</tr>
<tr>
<td>10</td>
<td>50216</td>
<td>10</td>
<td>445</td>
<td>SMB2</td>
<td>1036</td>
<td>Write Request Len:866 Off:0 File: readme.txt</td>
</tr>
<tr>
<td>10</td>
<td>50216</td>
<td>10</td>
<td>445</td>
<td>SMB2</td>
<td>138</td>
<td>Write Response</td>
</tr>
<tr>
<td>10</td>
<td>50216</td>
<td>10</td>
<td>445</td>
<td>SMB2</td>
<td>162</td>
<td>GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: readme.txt</td>
</tr>
<tr>
<td>10</td>
<td>50216</td>
<td>10</td>
<td>445</td>
<td>SMB2</td>
<td>186</td>
<td>GetInfo Response</td>
</tr>
</tbody>
</table>

Ransomware deployed, ransom note dropped:

```
All of your files are currently encrypted by CONTI ransomware.
If you try to use any additional recovery software - the files might be damaged or lost.

To make sure that we REALLY CAN recover data - we offer you to decrypt samples.
You can contact us for further instructions through:

Our website
TOR VERSION:
(you should download and install TOR browser first https://torproject.org)
http://*
HTTPS VERSION:
https://*

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We’ve downloaded your data and are ready to publish it on our news website if you do not respond.

---BEGIN ID---

---END ID---
```
• February 2021: Not-for-profit hospital in New Mexico, was compromised by Conti.

• Impact:
  o Significant operational disruption; EHR downtime, staff resorted to pen and paper
  o Attackers first accessed systems on January 21
  o Attack continued until February 5
  o FBI investigating
  o Data exfiltrated: Sensitive patient information, including patient ID cards, passports and treatment information, as well as employee files like job applications and background check authorizations
  o Over 200,000 patients were notified that their data had been leaked

• Primary regional healthcare provider for the Navajo Nation
  o The population of 175,000 people suffered upwards of 29,000 recorded COVID cases and at least 1,184 COVID-related deaths
In mid-May, the Irish national healthcare system, Health Service Executive (HSE), was attacked with Conti. They immediately shut down all IT systems, though their national ambulance system continued operations and there were no interruptions to COVID-19 vaccine appointments.

Impacts:
- Some hospitals could not access electronic systems and records and had to rely on paper records
- Some hospitals cancelled routine treatments, including maternity checkups and scans
- Many out-patient appointments were also cancelled
- Some cancer and stroke services (radiology diagnostics) had been affected over the short term

The HSE has maintained that they have not paid the ransom.

Conti released a decryptor for free to Ireland’s health service. On June 23, it was confirmed that at least three quarters of the HSE’s IT servers had been decrypted and 70% of computer devices were back in use. Conti also attempted an attack against Ireland’s Department of Health, which apparently was not successful.

Conti threatened to leak stolen data unless HSE paid a ransom. On 28 May, the HSE confirmed that data relating to 520 patients, including sensitive information, was published online.
MITRE ATT&CK Tactics and Techniques

- Command and Scripting Interpreter – T1059
- External Proxy – T1090.002
- Remote Desktop Protocol – T1021.001
- OS Credential Dumping – T1003
- Pass the Hash – T1550.002
- Service Execution – T1569.002
- SMB/Windows Admin Shares – T1021.002
- Data Encrypted for Impact – T1486
- System Owner/User Discovery – T1033
- Permission Groups Discovery – T1069

- Application Layer Protocol – T1071
- Process Injection – T1055
- Group Policy Modification – T1484
- Access Token Manipulation – T1134
- Create Account – T1136
- Remote System Discovery – T1018
- Network Service Scanning – T1046
- Domain Account – T1087.002
- Impair Defenses – T1562
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 Conti.

<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>
</tbody>
</table>

Background information can be found here:  
Mitigation Practices: Conti, Part 2

Other mitigation information and actions:

- IOCs, Yara rule: [https://thedfirreport.com/2021/05/12/conti-ransomware/](https://thedfirreport.com/2021/05/12/conti-ransomware/)
  
  o Covers Darkside Ransomware by the mitigations and resources apply to many ransomware variants

<table>
<thead>
<tr>
<th>DEFENSE/MITIGATION/COUNTERMEASURE</th>
<th>405(d) HICP REFERENCE</th>
</tr>
</thead>
<tbody>
<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. Restricting/Minimizing/eliminating RDP usage.</td>
<td>[7.S.A], [7.M.D]</td>
</tr>
</tbody>
</table>
• 207K Rehoboth McKinley Patients Tied to Conti Ransomware, Data Leak

• FBI Flash: Conti Ransomware Attacks Impact Healthcare and First Responder Networks

• Conti Ransomware Gang: An Overview
https://unit42.paloaltonetworks.com/conti-ransomware-gang/

• Explainer: What is a ransomware attack and why has the HSE been targeted?
https://www.thejournal.ie/hse-it-system-ransomware-attack-explained-5437064-May2021/

• Ragnar Locker ransomware deploys virtual machine to dodge security

• FBI Flash: Conti Ransomware Attacks Impact Healthcare and First Responder Networks

• Ransomware: Growing Number of Attackers Using Virtual Machines

• The DFIR Report: Conti Ransomware
https://thedfirreport.com/2021/05/12/conti-ransomware/

• A Conti ransomware attack day-by-day
https://news.sophos.com/en-us/2021/02/16/conti-ransomware-attack-day-by-day/
Questions
Questions

Upcoming Briefs

• 7/22 – Qbot/QakBot

Requests for Information

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

Product Evaluations

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

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.
HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

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

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

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

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