LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Conti Ransomware and the Health Sector

07/08/2021

TLP: WHITE, ID# ***202107081300***

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

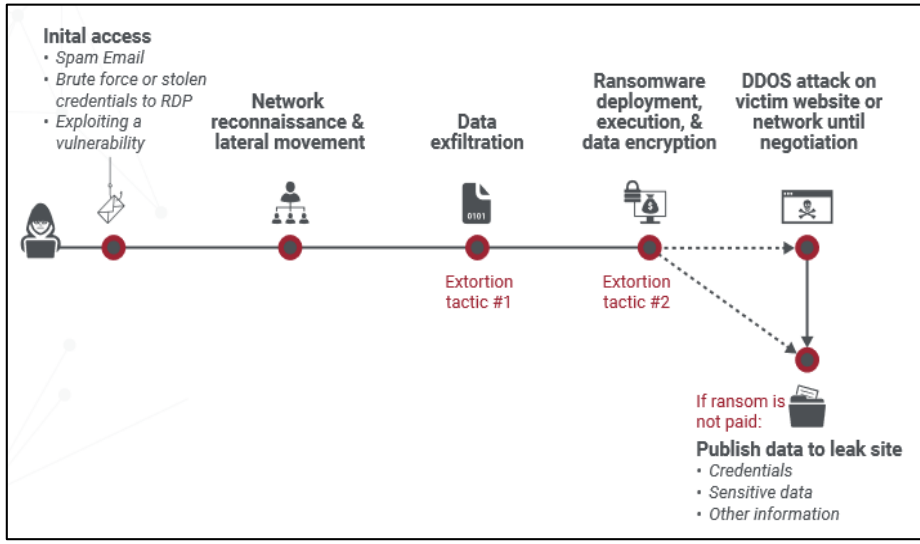
Slides Key:

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

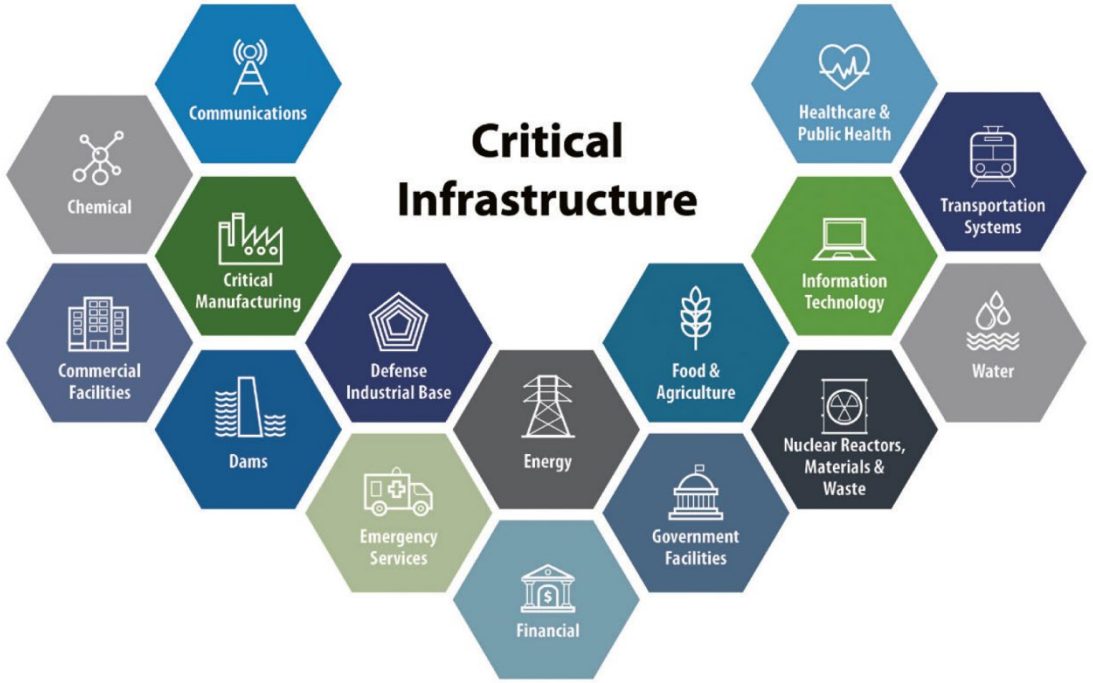
Double Extortion process flow:



- Bottom line: Ransomware operators continue to improve their efficiency and effectiveness, in many cases mirroring the practices of legitimate businesses

Ransomware Heavily Targeting Critical Infrastructure

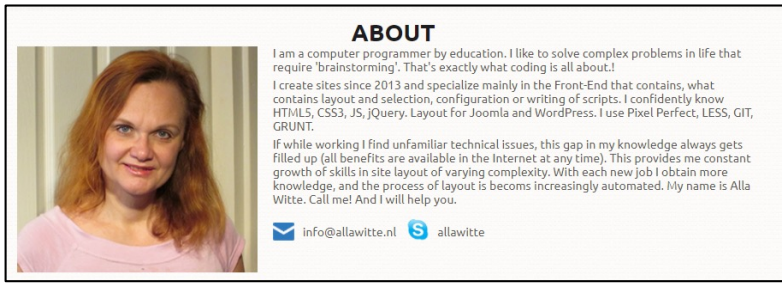
- Recent high-profile ransomware attacks against critical infrastructure:
  - Energy
    - Colonial Pipeline
  - Transportation
    - NYC Subway system
  - Chemical
    - Brenntag
  - Information Technology
    - Acer
  - Food & Agriculture
    - JBS
  - Healthcare and Public Health
    - Health Service Executive
  - Emergency Services
    - Washington DC Metropolitan Police Department
  - Financial Services
    - Valley Bank



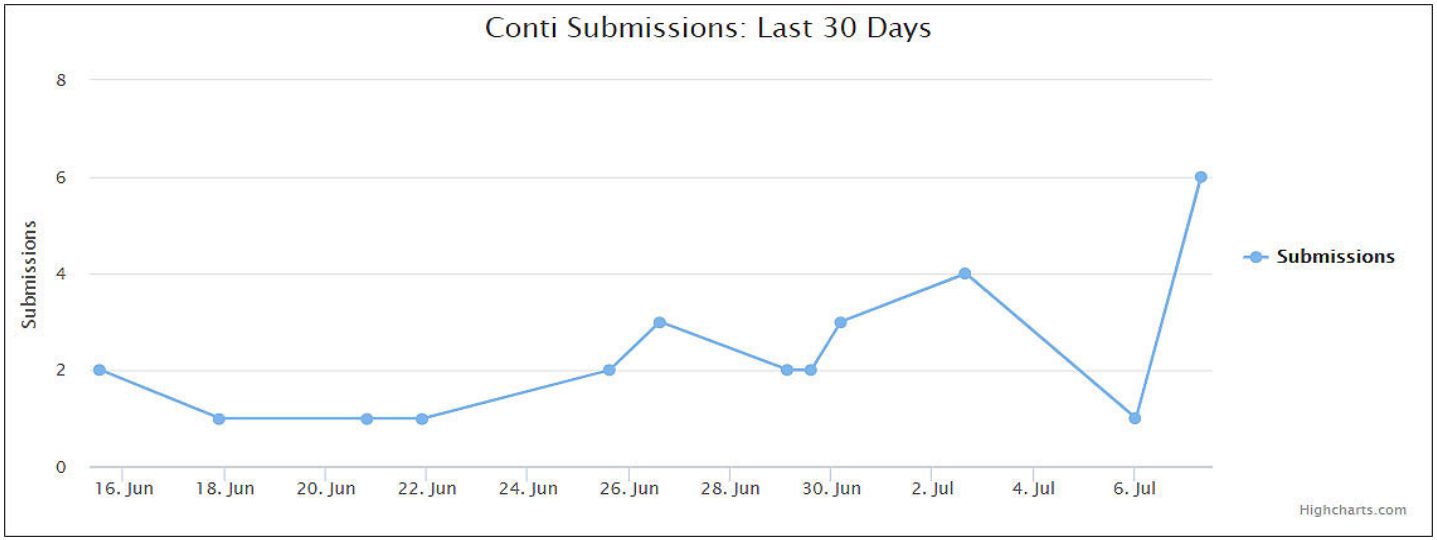
© US Cybersecurity & Infrastructure Security Agency (CISA)

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



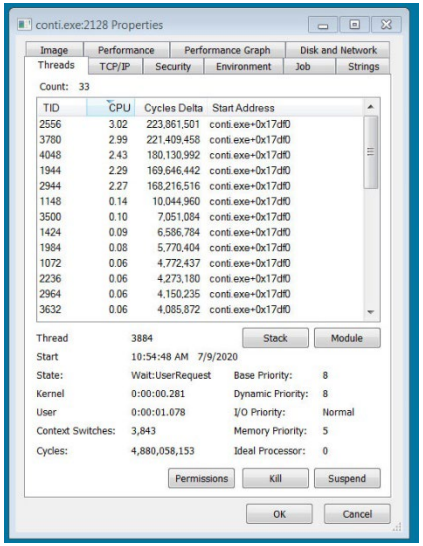
- First observed in December 2019; significant activity began in July 2020
- Leverages unique AES-256 encryption key per file, then encrypted with an RSA-4096 encryption key
- Often conducts double extortion (leak site launched September 2020)
- “Human-operated” as opposed to automatic
- Conti deletes 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

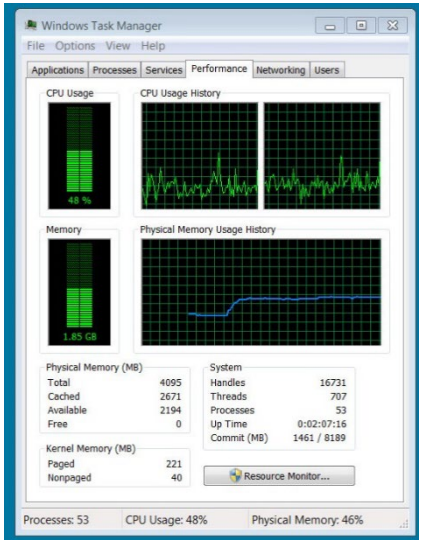


Conti Submissions to ID Ransomware in June/July 2020

Overview of Conti Ransomware, Part 2

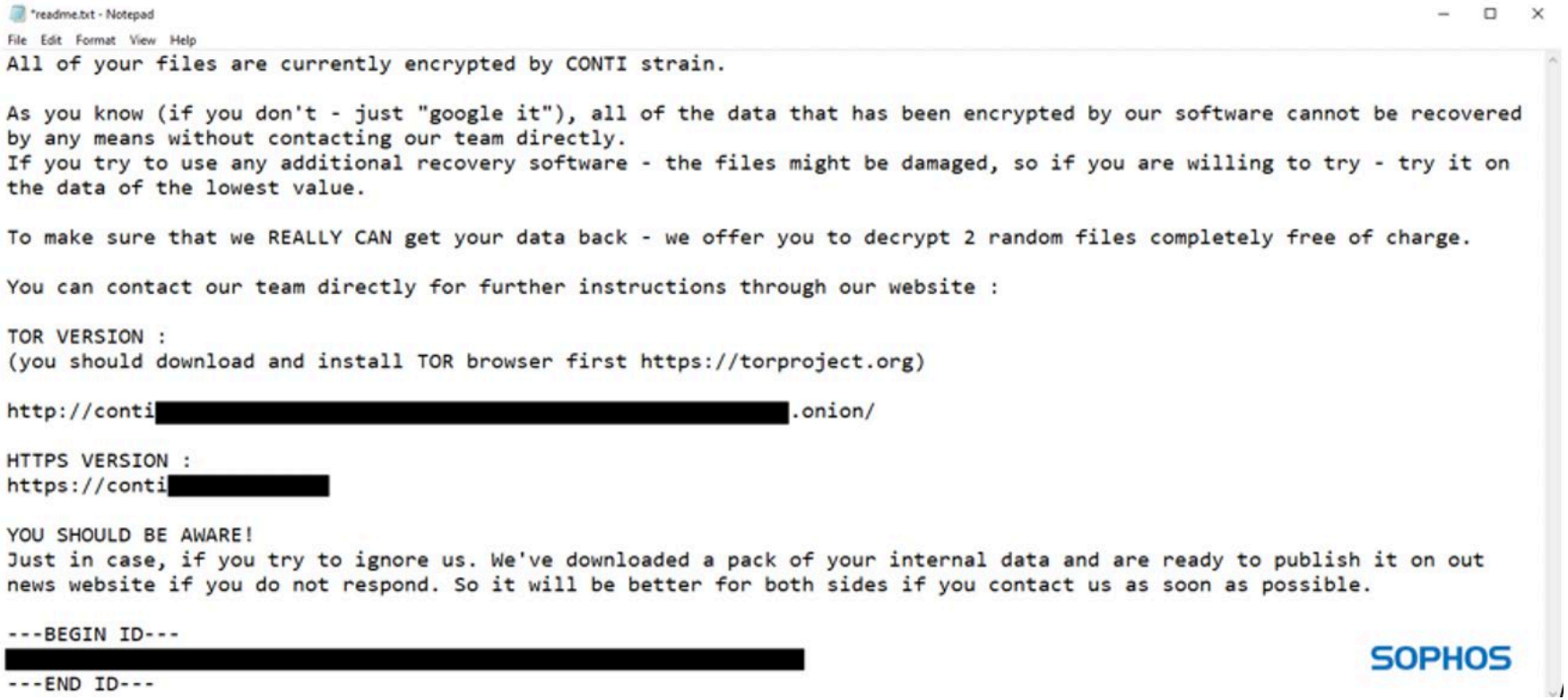
- Connections to Ryuk:
  - Conti's code appears to be closely based on the malware code from version 2 of Ryuk
  - Distribution: Similar to Ryuk, Conti is typically delivered via TrickBot
  - Ransom note: Conti utilizes the same ransom note template used in early Ryuk attacks
  - Incident rate: ID Ransomware 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:
  - Notification of attack
  - Futility of non-cooperation
  - Justification for trust
  - Instructions



*readme.txt - Notepad

File Edit Format View Help

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/

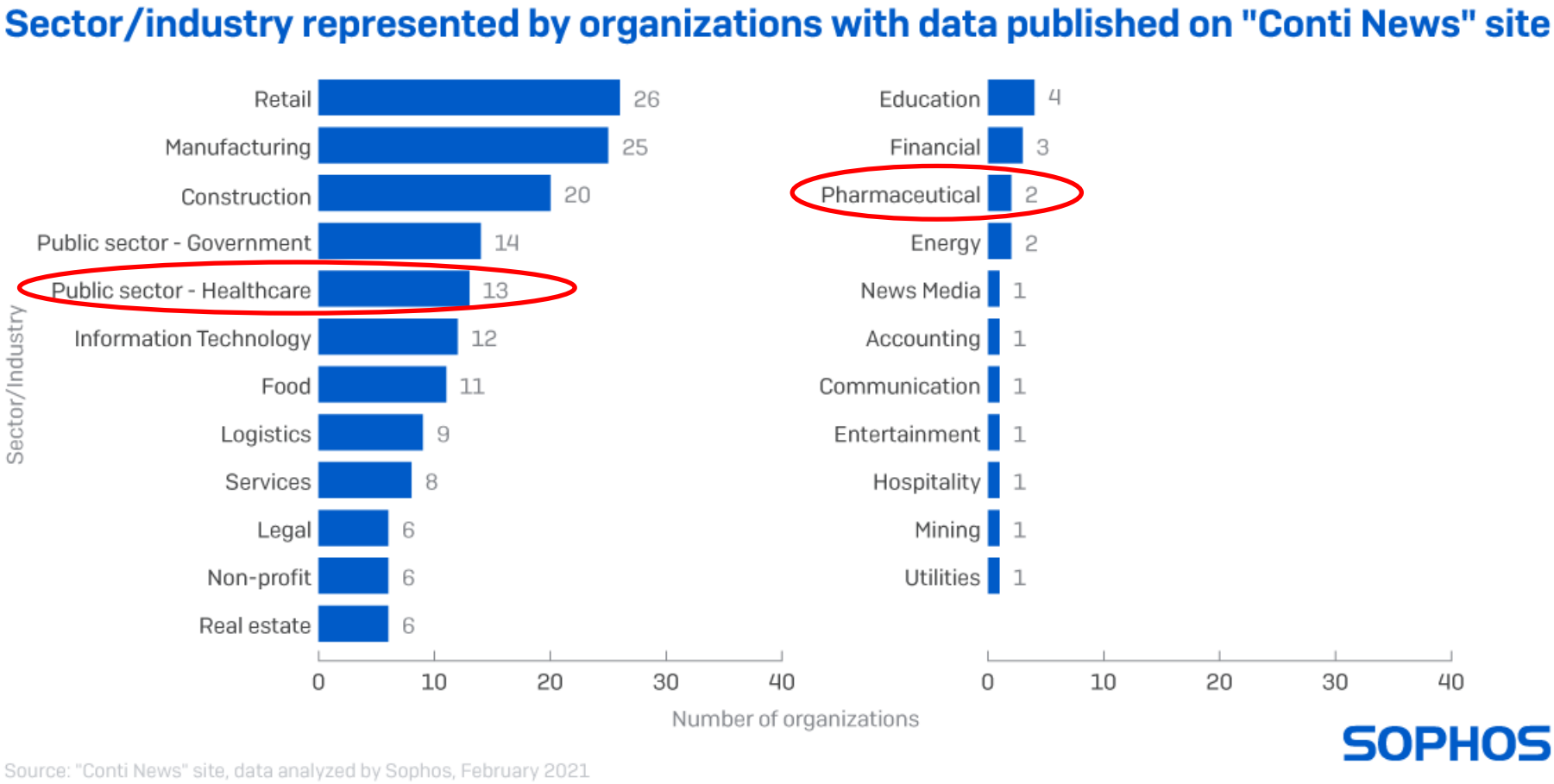
HTTPS VERSION :
https://conti[redacted]

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 out news website if you do not respond. So it will be better for both sides if you contact us as soon as possible.

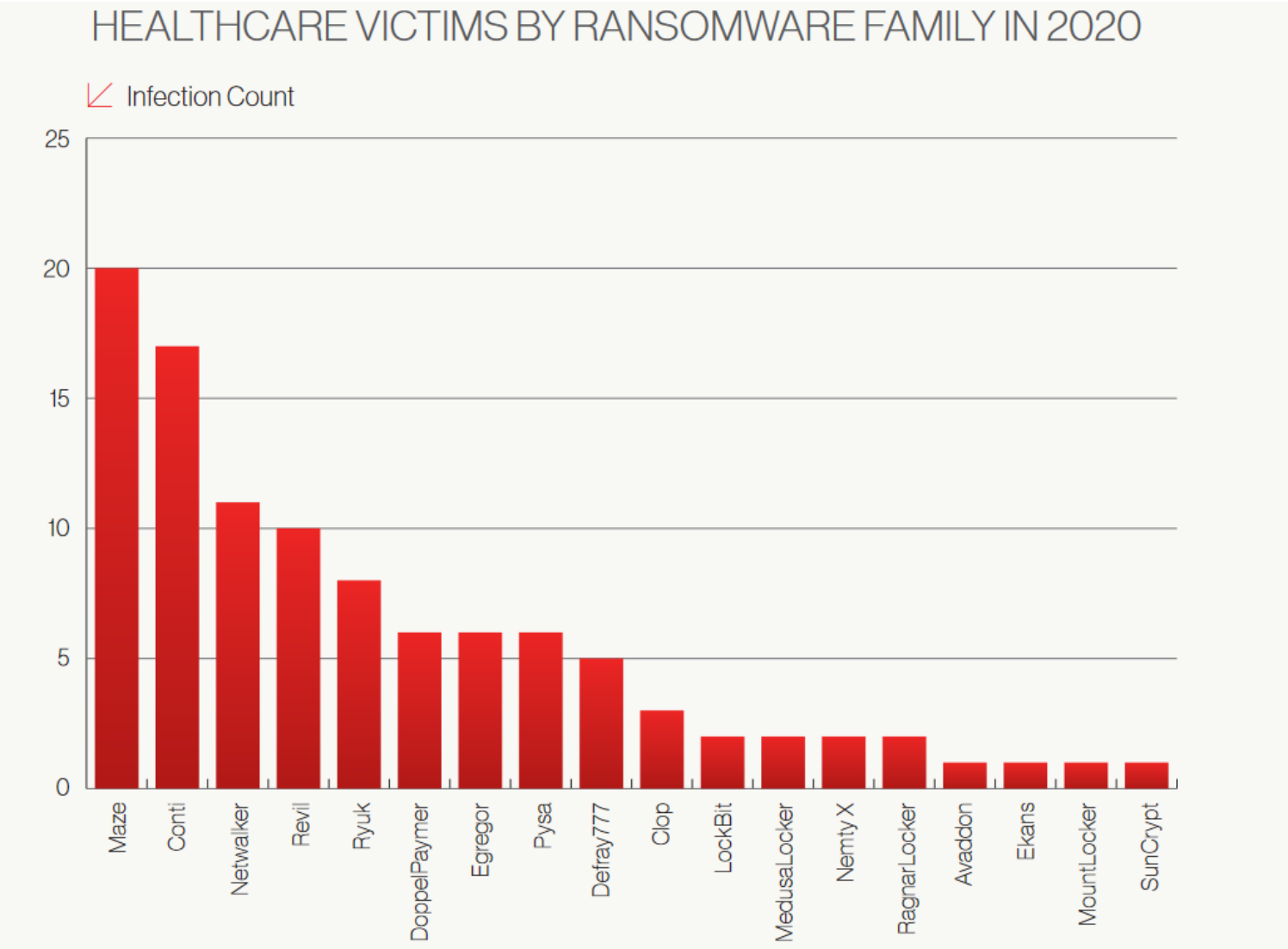
---BEGIN ID---
[redacted]
---END ID---

SOPHOS

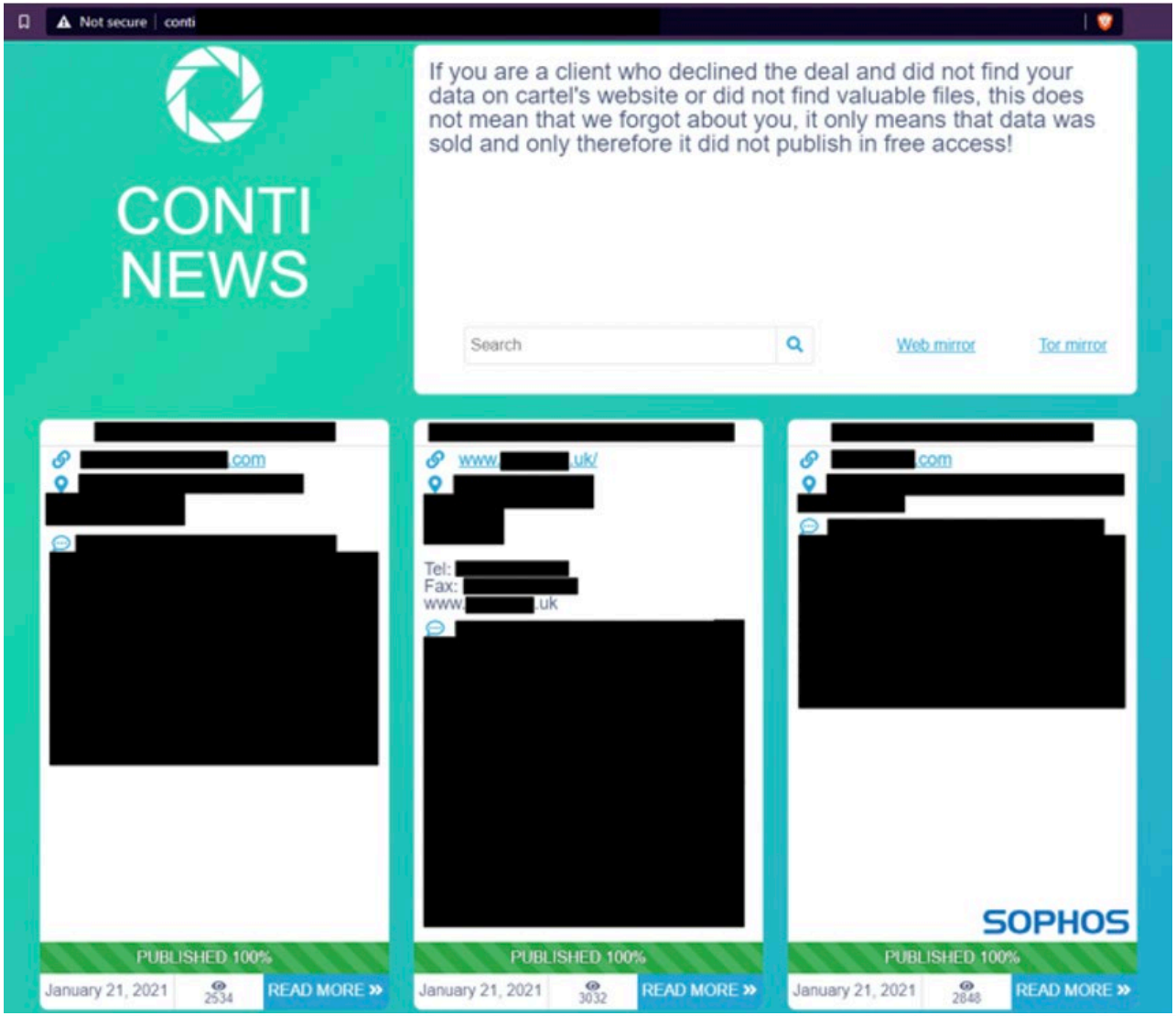
Per Sophos, healthcare is high on Conti's list of targets:

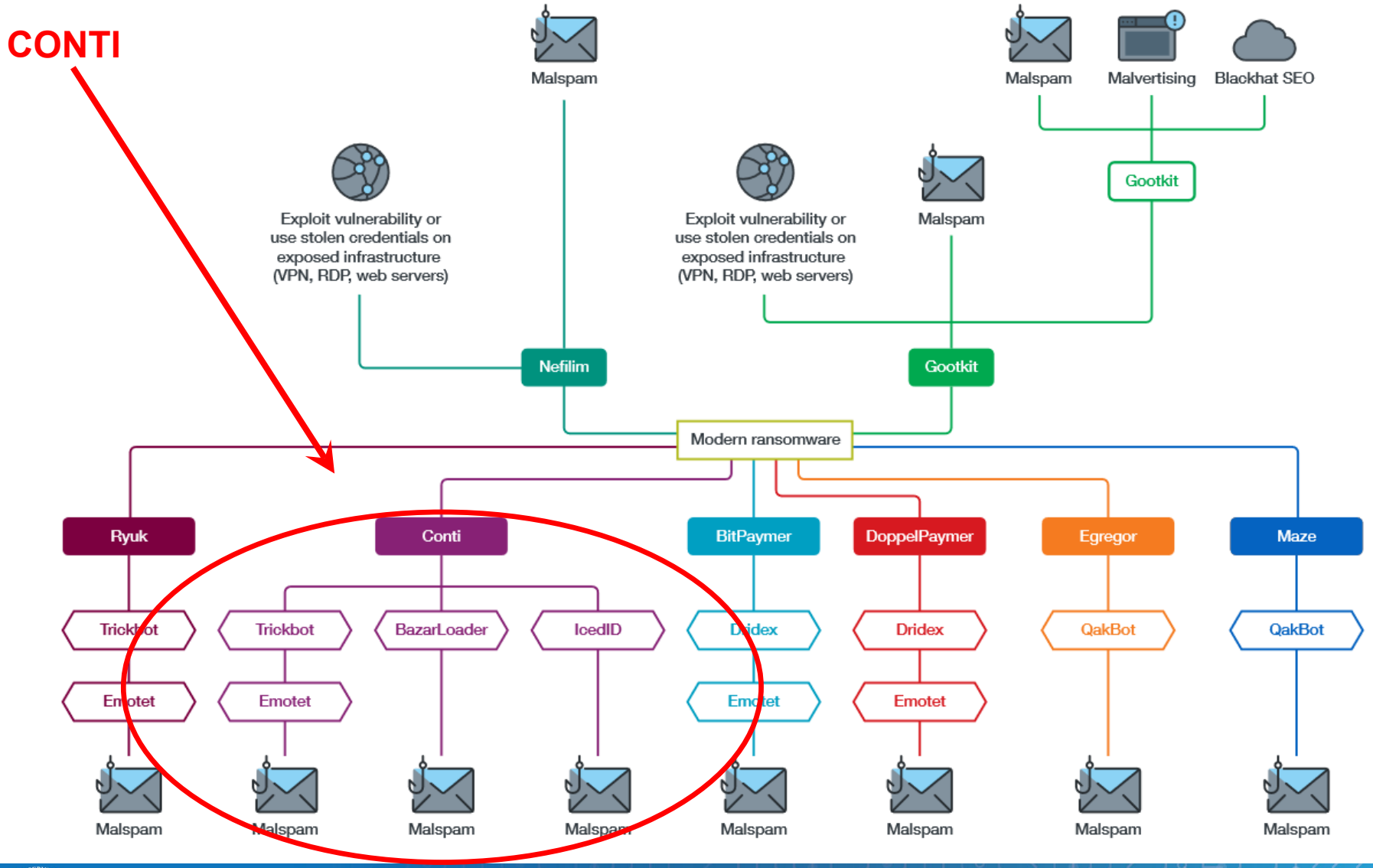


Conti vs. Healthcare, Part 2



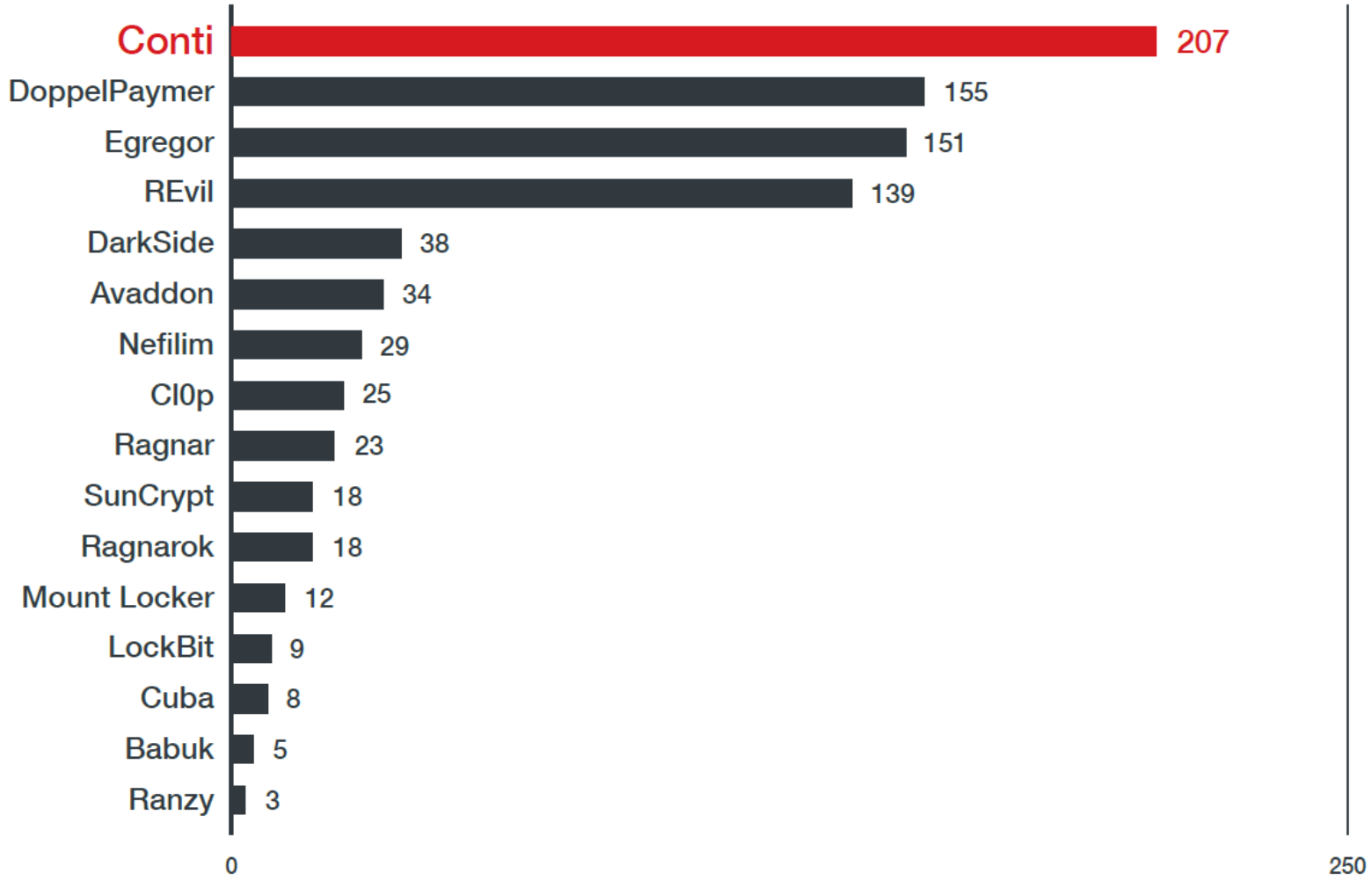
Conti Leak Site




CONTI
Malspam
Malspam
Malvertising
Blackhat SEO
Gootkit
Exploit vulnerability or use stolen credentials on exposed infrastructure (VPN, RDP, web servers)
Exploit vulnerability or use stolen credentials on exposed infrastructure (VPN, RDP, web servers)
Malspam
Nefilim
Gootkit
Modern ransomware
Ryuk
Conti
BitPaymer
DoppelPaymer
Egregor
Maze
Trickbot
Trickbot
BazarLoader
IcedID
Dridex
Dridex
QakBot
QakBot
Emotet
Emotet
Emotet
Emotet
Malspam
Malspam
Malspam
Malspam
Malspam
Malspam
Malspam
Malspam

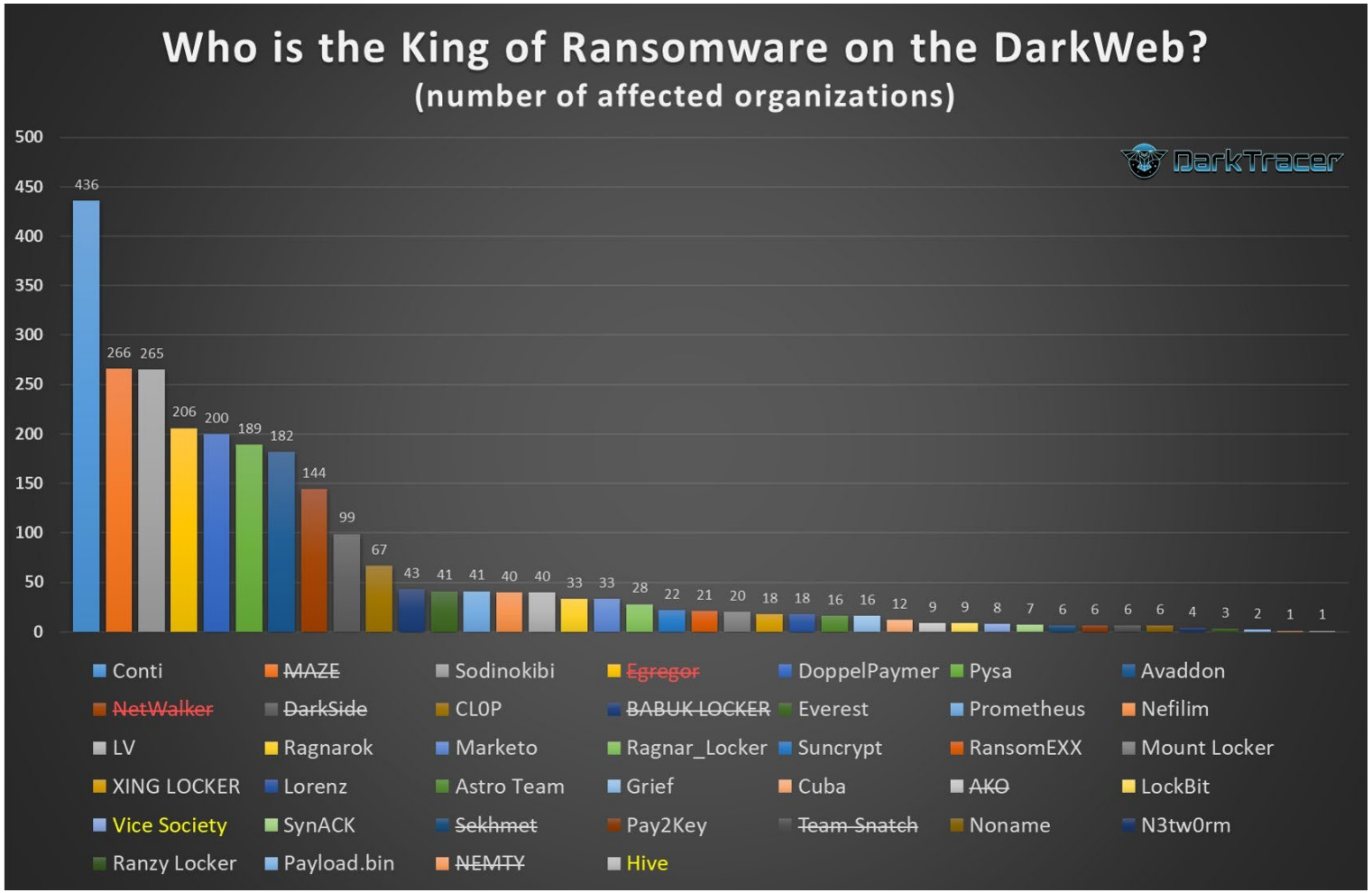
Conti – Leaked Data

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



Conti – Frequency of Targeting

Per DarkTracer as of June 28, 2021:



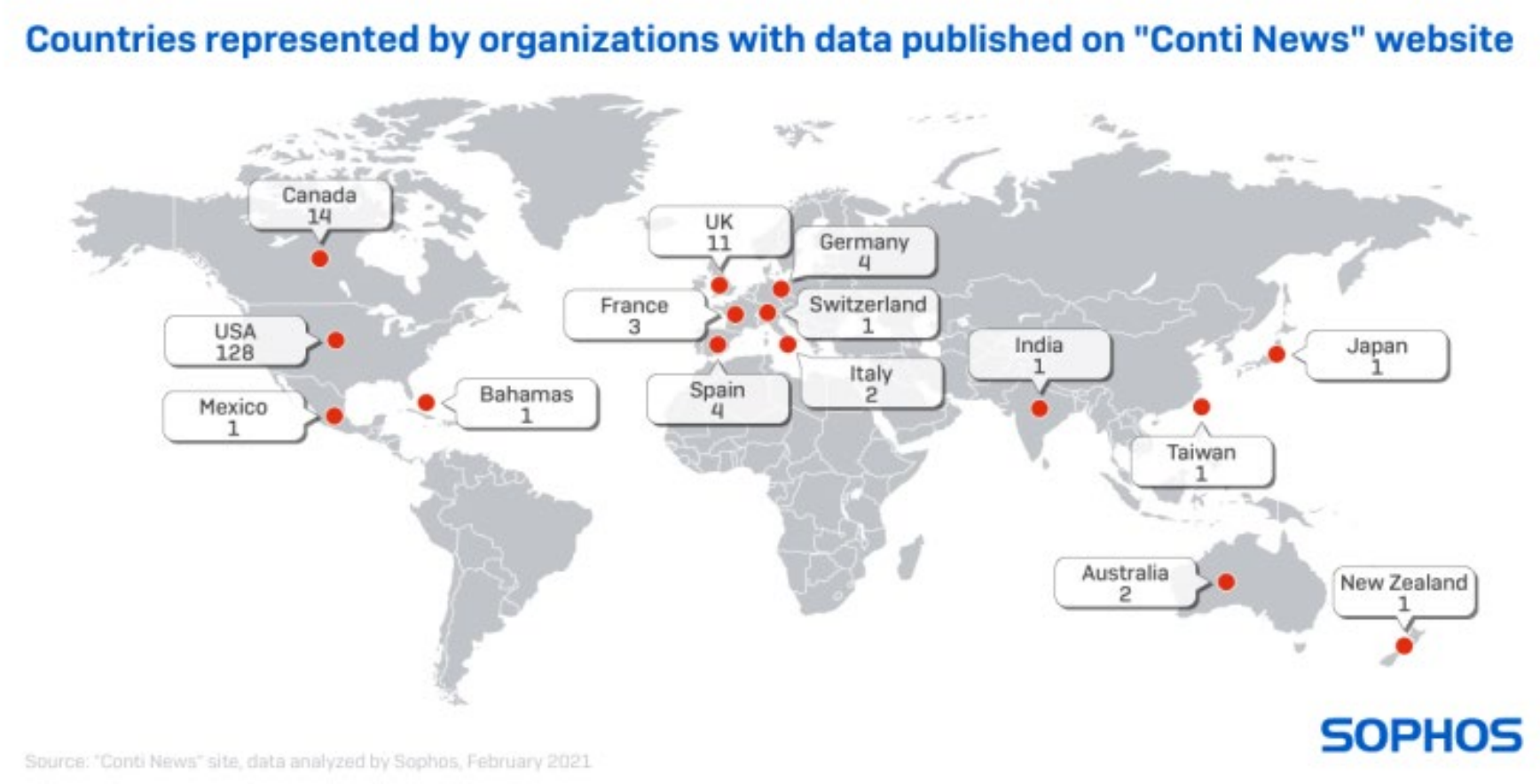
Most Common Ransomware Variants in Q1 2021

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

Top 10: Market Share of the Ransomware attacks

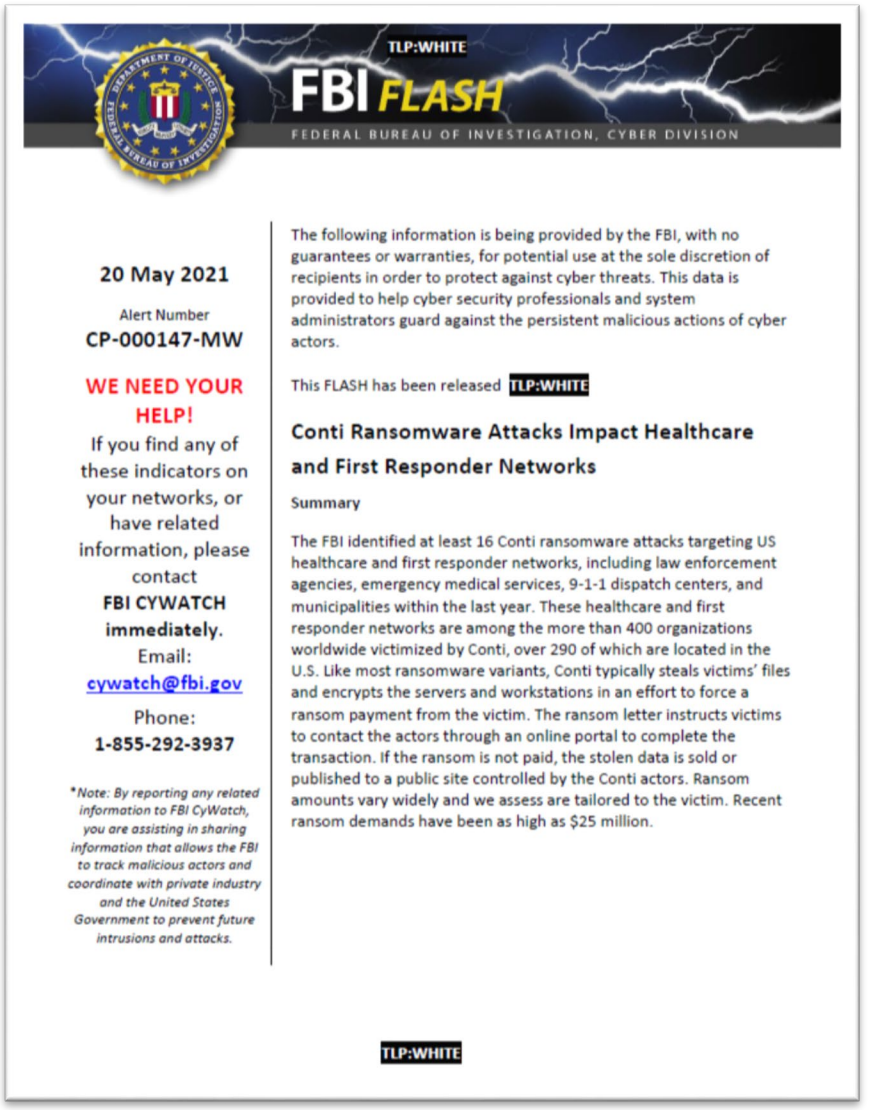
Conti – Targeting by Geography

- Conti is “a global threat affecting victims mainly in North America and Western Europe”. (Sophos)
- What’s missing? Russia and CIS countries



FBI Alert on Conti

- 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.
  - Ransom demands
    - As high as $25M
  - 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



TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

20 May 2021

Alert Number
CP-000147-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately.**
Email:
cywatch@fbi.gov
Phone:
1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.

This FLASH has been released TLP:WHITE

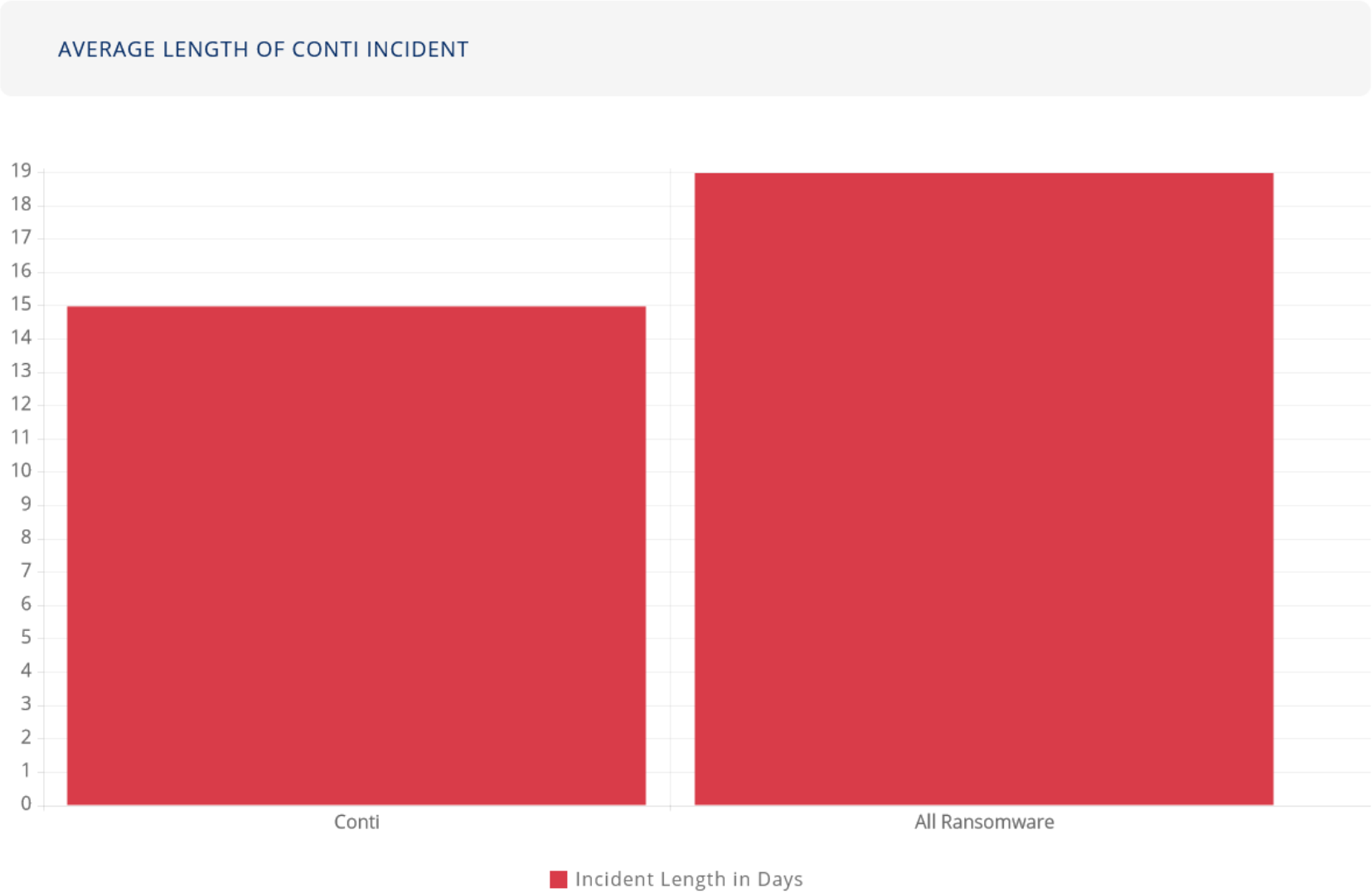
Conti Ransomware Attacks Impact Healthcare and First Responder Networks

Summary

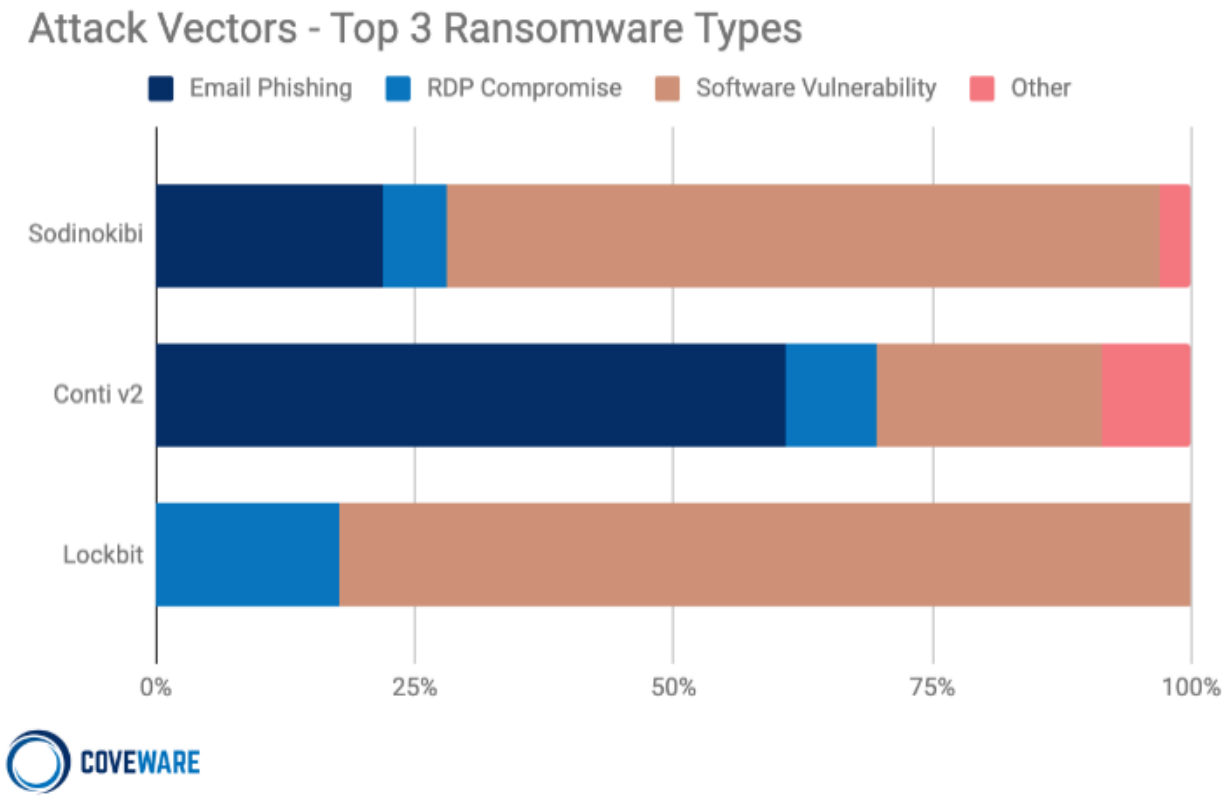
The FBI identified at least 16 Conti ransomware attacks targeting US healthcare and first responder networks, including law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, and municipalities within the last year. These healthcare and first responder networks are among the more than 400 organizations worldwide victimized by Conti, over 290 of which are located in the U.S. Like most ransomware variants, Conti typically steals victims' files and encrypts the servers and workstations in an effort to force a ransom payment from the victim. The ransom letter instructs victims to contact the actors through an online portal to complete the transaction. If the ransom is not paid, the stolen data is sold or published to a public site controlled by the Conti actors. Ransom amounts vary widely and we assess are tailored to the victim. Recent ransom demands have been as high as $25 million.

TLP:WHITE

Conti – Average Incident Length



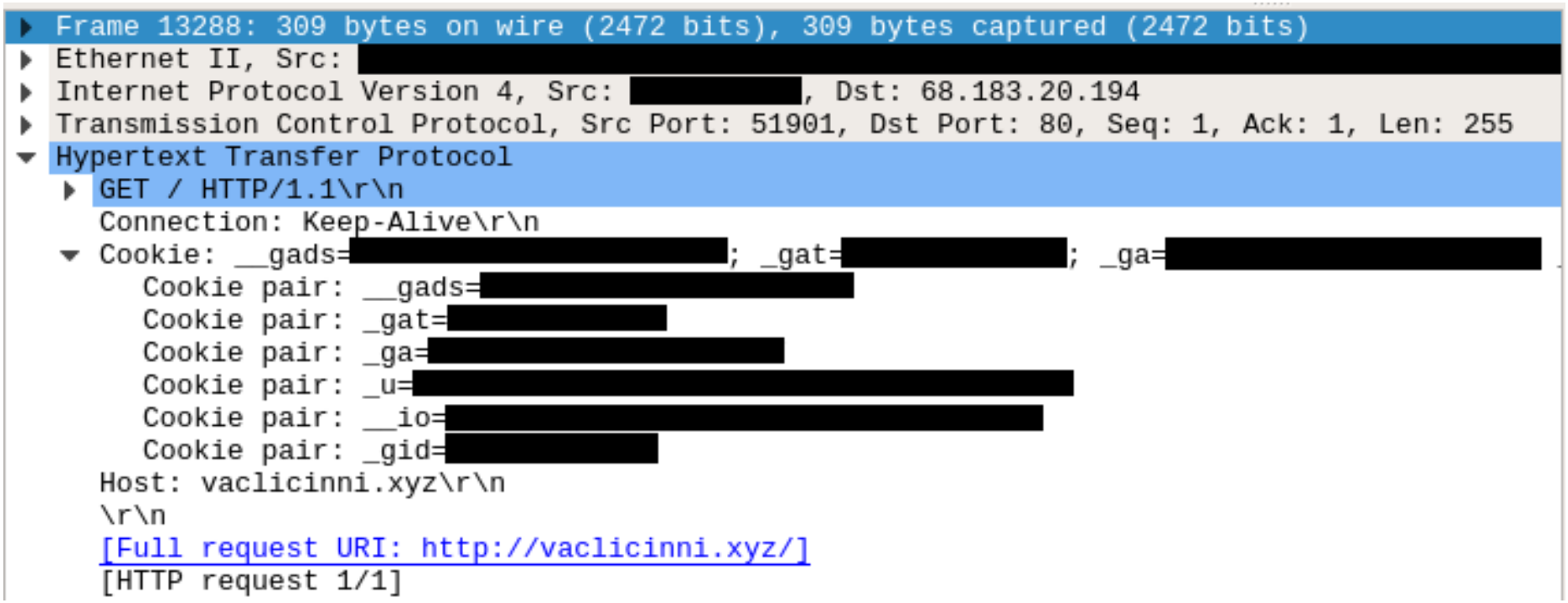
Attack Vectors used by the Top Three Ransomware Variants



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



Example of a Conti Infection, Part 2

IcedID further reconnaissance efforts:

data.win.eventdata.commandLine	data.win.eventdata.parentImage
cmd.exe /c chcp >&2	C:\\Windows\\System32\\rundll32.exe
ipconfig /all	C:\\Windows\\System32\\rundll32.exe
systeminfo	C:\\Windows\\System32\\rundll32.exe
net config workstation	C:\\Windows\\System32\\rundll32.exe
nltest /domain_trusts	C:\\Windows\\System32\\rundll32.exe
nltest /domain_trusts /all_trusts	C:\\Windows\\System32\\rundll32.exe
net view /all /domain	C:\\Windows\\System32\\rundll32.exe
net view /all	C:\\Windows\\System32\\rundll32.exe
net group \"Domain Admins\" /domain	C:\\Windows\\System32\\rundll32.exe

Discovery:

- Additional discovery commands were executed by Cobalt Strike.

Initiating Process File Name	Process Command Line
icju1.exe	cmd.exe /C whoami /groups
icju1.exe	cmd.exe /C query session
icju1.exe	cmd.exe /C dir %HOMEDRIVE%%HOMEPATH%
icju1.exe	cmd.exe /C nltest /domain_trusts
icju1.exe	cmd.exe /C nltest /dclist:
icju1.exe	cmd.exe /C net group "Enterprise admins" /domain
icju1.exe	cmd.exe /C net group "Domain admins" /domain

Example of a Conti Infection, Part 4

- 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:

Initiating Pro…	Initiating Process Folder Path	Local IP	Local Port	Remote IP	Remote Port
runonce.exe	c:\windows\system32\runonce.exe	10.	64077	10.	22
runonce.exe	c:\windows\system32\runonce.exe	10.	64076	10.	135
runonce.exe	c:\windows\system32\runonce.exe	10.	64075	10.	445
runonce.exe	c:\windows\system32\runonce.exe	10.	64074	10.	1433
runonce.exe	c:\windows\system32\runonce.exe	10.	64073	10.	1434
runonce.exe	c:\windows\system32\runonce.exe	10.	64072	10.	3389
runonce.exe	c:\windows\system32\runonce.exe	10.	64071	10.	4343
runonce.exe	c:\windows\system32\runonce.exe	10.	64070	10.	5000
runonce.exe	c:\windows\system32\runonce.exe	10.	64069	10.	5985

Example of a Conti Infection, Part 5

- Cobalt Strike Beacon DLL dropped on ADMIN$ share and then distributed throughout environment using PsExec:

Initiating Process Parent File Name	Initiating Process File Name	Initiating Process Command Line	Process Command Line	Action Type	File Name
PSEXESVC.exe	rundll32.exe	"rundll32.exe" c:\windows\192145.dll,StartW	cmd.exe /c echo NGAtoDgLpvgJwPLEPFdj>"C:\Windows\TEMP\DEM238D.tmp"&exit	ProcessCreated	-
PSEXESVC.exe	rundll32.exe	"rundll32.exe" c:\windows\192145.dll,StartW	cmd.exe /c echo NGAtoDgLpvgJwPLEPFdj>"C:\Windows\TEMP\DEM238D.tmp"&exit	ProcessCreated	-
PSEXESVC.exe	rundll32.exe	"rundll32.exe" c:\windows\192145.dll,StartW	-	AbnormalDynamicLinkLibraryLoad	192145.dll
PSEXESVC.exe	rundll32.exe	"rundll32.exe" c:\windows\192145.dll,StartW	-	AbnormalDynamicLinkLibraryLoad	192145.dll
PSEXESVC.exe	rundll32.exe	"rundll32.exe" c:\windows\192145.dll,StartW	-	AbnormalDynamicLinkLibraryLoad	192145.dll
PSEXESVC.exe	rundll32.exe	"rundll32.exe" c:\windows\192145.dll,StartW	-	ImageLoaded	192145.dll
PSEXESVC.exe	rundll32.exe	"rundll32.exe" c:\windows\192145.dll,StartW	-	ConnectionSuccess	-
PSEXESVC.exe	rundll32.exe	"rundll32.exe" c:\windows\192145.dll,StartW	runonce.exe	CreateRemoteThreadApiCall	-
PSEXESVC.exe	rundll32.exe	"rundll32.exe" c:\windows\192145.dll,StartW	runonce.exe	ProcessCreated	-

Example of a Conti Infection, Part 6

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

eventdata.accountName	LocalSystem
eventdata.imagePath	\\\\ [redacted] \\ADMIN$\\a43f562.exe
eventdata.serviceName	a43f562
eventdata.serviceType	user mode service
eventdata.startType	demand start
system.channel	System
system.computer	[redacted]
system.eventID	7045
system.eventRecordID	5145
system.eventSourceName	Service Control Manager

data.win.system.channel	data.win.eventdata.serviceName	data.win.eventdata.imagePath	data.win.eventdata.accountName
System	7a277c9	\\\\ \\ADMIN$\\7a277c9.exe	LocalSystem
System	c30dce8	\\\\ \\ADMIN$\\c30dce8.exe	LocalSystem
System	a43f562	\\\\ \\ADMIN$\\a43f562.exe	LocalSystem
System	d7f0cde	\\\ \ADMIN$\\d7f0cde.exe	LocalSystem
System	d8d6deb	\\\ \\ADMIN$\\d8d6deb.exe	LocalSystem
System	a068564	\\\ \\ADMIN$\\a068564.exe	LocalSystem

Example of a Conti Infection, Part 7

Persistence

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

```
net user /add /Y nuuser 7HeC00l3stP@ssw0rd
net localgroup administrators nuuser /add
```

commandLine	C:\\Windows\\system32\\cmd.exe /C net localgroup administrators nuuser /add
company	Microsoft Corporation
currentDirectory	c:\\programdata\\
description	Windows Command Processor
fileVersion	[redacted]
hashes	SHA1=8C5437CD76A89EC983E3B364E219944DA3DAB464,MD5=975B45B669930B0CC773EAF2B4
image	C:\\Windows\\System32\\cmd.exe
integrityLevel	System
logonGuid	{46d5468e-3c49-607f-e703-000000000000}
logonId	0x3e7
originalFileName	Cmd.Exe
parentCommandLine	\"rundll32.exe\" c:\\windows\\192145.dll,StartW
parentImage	C:\\Windows\\System32\\rundll32.exe

Example of a Conti Infection, Part 8

- 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.

Initiating Process Command Line	Local IP	Local Port	Remote Port	Remote IP
rundll32.exe "C:\Users\[redacted]\AppData\Local\Temp\rate_x32.dat",update /i:"LaborBetray\license.dat"	10.[redacted]	65148	3389	10.[redacted]
rundll32.exe "C:\Users\[redacted]\AppData\Local\Temp\rate_x32.dat",update /i:"LaborBetray\license.dat"	10.[redacted]	65161	3389	10.[redacted]
rundll32.exe "C:\Users\[redacted]\AppData\Local\Temp\rate_x32.dat",update /i:"LaborBetray\license.dat"	10.[redacted]	65216	3389	10.[redacted]
rundll32.exe "C:\Users\[redacted]\AppData\Local\Temp\rate_x32.dat",update /i:"LaborBetray\license.dat"	10.[redacted]	65264	3389	10.[redacted]
rundll32.exe "C:\Users\[redacted]\AppData\Local\Temp\rate_x32.dat",update /i:"LaborBetray\license.dat"	10.[redacted]	65375	3389	10.[redacted]
rundll32.exe "C:\Users\[redacted]\AppData\Local\Temp\rate_x32.dat",update /i:"LaborBetray\license.dat"	10.[redacted]	65393	3389	10.[redacted]
rundll32.exe "C:\Users\[redacted]\AppData\Local\Temp\rate_x32.dat",update /i:"LaborBetray\license.dat"	10.[redacted]	49278	3389	10.[redacted]
rundll32.exe "C:\Users\[redacted]\AppData\Local\Temp\rate_x32.dat",update /i:"LaborBetray\license.dat"	10.[redacted]	49318	3389	10.[redacted]

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

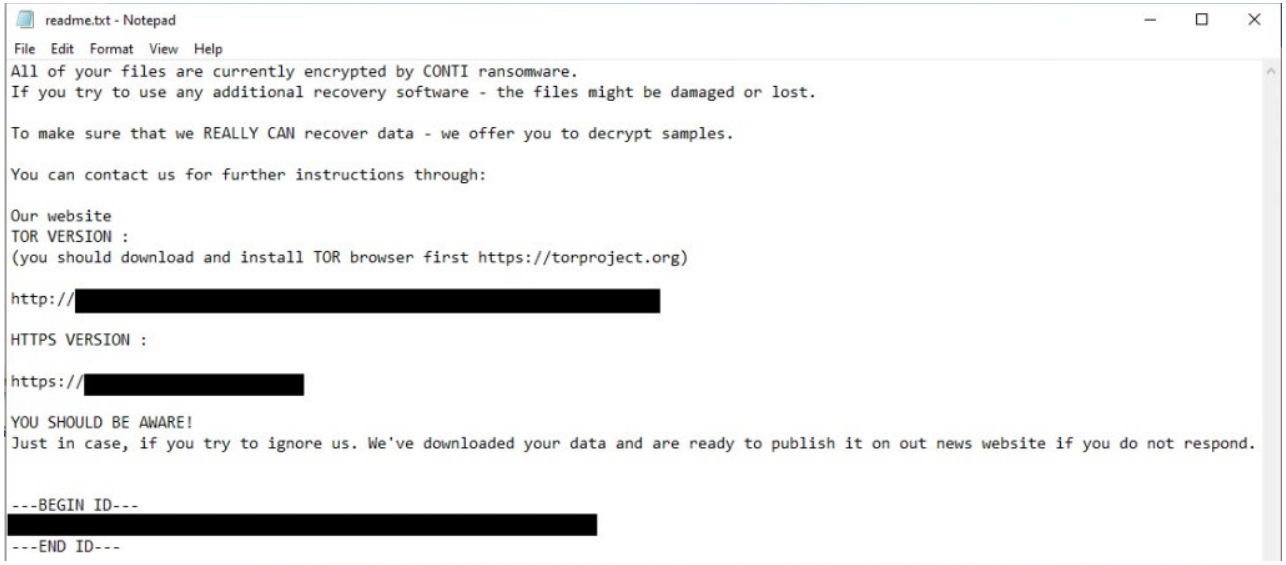
No.	Source	Source Port	Destination	Destination F	Protocol	Length	Info
650	[redacted]	65164	38.135.122.194	8080	TCP	66	65164 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
651	38.135.122.194	8080	[redacted]	65164	TCP	66	8080 → 65164 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
652	[redacted]	65164	38.135.122.194	8080	TCP	60	65164 → 8080 [ACK] Seq=1 Ack=1 Win=262656 Len=0
653	[redacted]	65164	38.135.122.194	8080	TPKT	67	Continuation
654	38.135.122.194	8080	[redacted]	65164	TCP	60	8080 → 65164 [ACK] Seq=1 Ack=14 Win=64256 Len=0
655	[redacted]	65164	38.135.122.194	8080	TPKT	60	Continuation
656	38.135.122.194	8080	[redacted]	65164	TPKT	60	Continuation
657	[redacted]	65164	38.135.122.194	8080	TCP	60	65164 → 8080 [ACK] Seq=16 Ack=2 Win=262656 Len=0
658	38.135.122.194	8080	[redacted]	65164	TCP	60	8080 → 65164 [ACK] Seq=2 Ack=16 Win=64256 Len=0
659	38.135.122.194	8080	[redacted]	65164	TPKT	66	Continuation
660	[redacted]	65164	38.135.122.194	8080	TPKT	66	Continuation
661	38.135.122.194	8080	[redacted]	65164	TCP	60	8080 → 65164 [ACK] Seq=14 Ack=28 Win=64256 Len=0
662	38.135.122.194	8080	[redacted]	65164	RDP	98	Cookie: mstshash=nuuser, Negotiate Request
663	[redacted]	65164	38.135.122.194	8080	RDP	73	Negotiate Response

Example of a Conti Infection, Part 9

Port scanning of the network, looking for port 445:

Source	Source Port	Destination	Destination Port	Protocol	Length	Info
10[redacted]	50216	10[redacted]	445	SMB2	210	Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \10[redacted]\C$
10[redacted]	445	10[redacted]	50216	SMB2	130	Ioctl Response, Error: STATUS_FS_DRIVER_REQUIRED
10[redacted]	50216	10[redacted]	445	SMB2	160	Tree Connect Request Tree: \\10[redacted]\C$
10[redacted]	445	10[redacted]	50216	SMB2	138	Tree Connect Response
10[redacted]	50216	10[redacted]	445	SMB2	382	Create Request File: readme.txt
10[redacted]	445	10[redacted]	50216	SMB2	410	Create Response File: readme.txt
10[redacted]	50216	10[redacted]	445	SMB2	1036	Write Request Len:866 Off:0 File: readme.txt
10[redacted]	445	10[redacted]	50216	SMB2	138	Write Response
10[redacted]	50216	10[redacted]	445	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: readme.txt
10[redacted]	445	10[redacted]	50216	SMB2	186	GetInfo Response
10[redacted]	50216	10[redacted]	445	SMB2	146	Close Request File: readme.txt

Ransomware deployed, ransom note dropped:


readme.txt - Notepad

File Edit Format View Help

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://[redacted]

HTTPS VERSION :

https://[redacted]

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 out news website if you do not respond.

---BEGIN ID---
[redacted]
---END ID---

Attack on New Mexico Hospital

- February 2021: Not-for-profit hospital in New Mexico, was compromised by Conti.
- Impact:
  - Significant operational disruption; EHR downtime, staff resorted to pen and paper
  - Attackers first accessed systems on January 21
  - Attack continued until February 5
  - FBI investigating
  - 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
  - Over 200,000 patients were notified that their data had been leaked
- Primary regional healthcare provider for the Navajo Nation
  - The population of 175,000 people suffered upwards of 29,000 recorded COVID cases and at least 1,184 COVID-related deaths

Attack on Irish Health System

- 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

MITRE ATT&CK™

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.

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]**

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

DEFENSE/MITIGATION/COUNTERMEASURE	405(d) HICP REFERENCE
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. Restricting/Minimizing/eliminating RDP usage.	**[7.S.A], [7.M.D]**

Other mitigation information and actions:

- IOCs, Yara rule: https://thedfirreport.com/2021/05/12/conti-ransomware/
- Virtual Machine IOCs: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-virtual-machines
- CISA Alert (AA21-131A): https://us-cert.cisa.gov/ncas/alerts/aa21-131a
  - Covers Darkside Ransomware by the mitigations and resources apply to many ransomware variants

Reference Materials

References

- 207K Rehoboth McKinley Patients Tied to Conti Ransomware, Data Leak
  https://healthitsecurity.com/news/207k-rehoboth-mckinley-patients-tied-to-conti-ransomware-data-leak
- FBI Flash: Conti Ransomware Attacks Impact Healthcare and First Responder Networks
  https://www.aha.org/system/files/media/file/2021/05/fbi-tlp-white-report-conti-ransomware-attacks-impact-healthcare-and-first-responder-networks-5-20-21.pdf
- 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
  https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/
- FBI Flash: Conti Ransomware Attacks Impact Healthcare and First Responder Networks
  https://www.aha.org/system/files/media/file/2021/05/fbi-tlp-white-report-conti-ransomware-attacks-impact-healthcare-and-first-responder-networks-5-20-21.pdf
- Ransomware: Growing Number of Attackers Using Virtual Machines
  https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-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

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.

Contact

www.HHS.GOV/HC3

HC3@HHS.GOV