



REN-ISAC

Ransomware: Threats & Mitigations

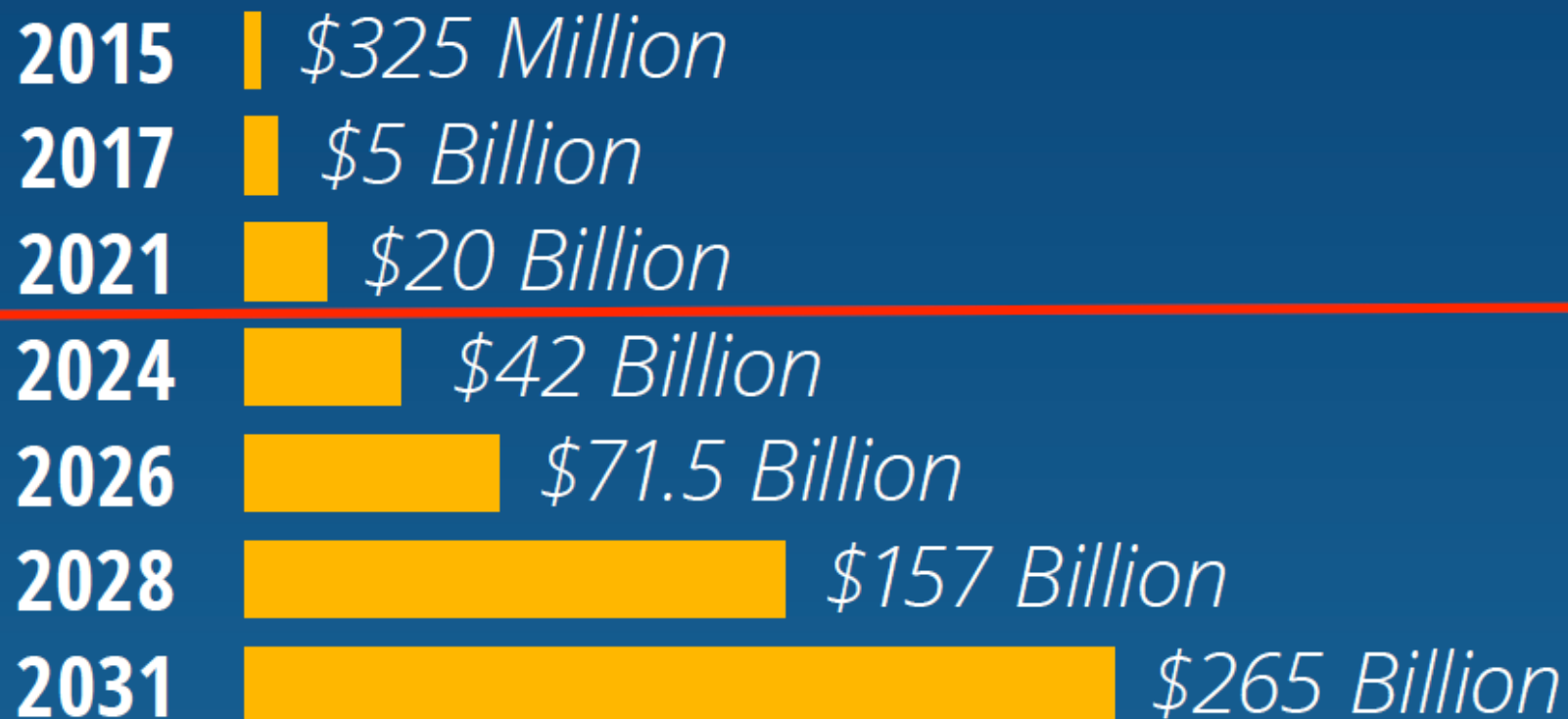
Sarah Bigham

Lead Security Analyst, REN-ISAC

Agenda

- The Numbers
- Ransomware Evolution
- Adversary Trends
- Heavy Hitters in Higher Ed
- Payments
- Best Practices
- Guidance

Global Cost of Ransomware



Source: <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/>



As a result...

- Security Awareness Training market expected to surge to \$10 billion within 5 years
- Premiums for cyber insurance policies went up by 92% in 2021

Source: <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/>

RANSOMWARE EVOLUTION TIMELINE

1989

First known ransomware attack

Traditional ransomware attack: encrypt data → extort for money → decryption key provided if ransom paid

WannaCry and Not-Petya caused global security crisis

- WannaCry attack included 150 countries⁶
- NotPetya caused about \$10 billion in damages worldwide⁷

2017

2019

First known double-extortion attack

935% increase in the number of companies that have had their data exposed on a data leak site during the study period⁸

First known triple-extortion attack

Ransomware's 93% surge was mainly fueled by triple extortion⁹

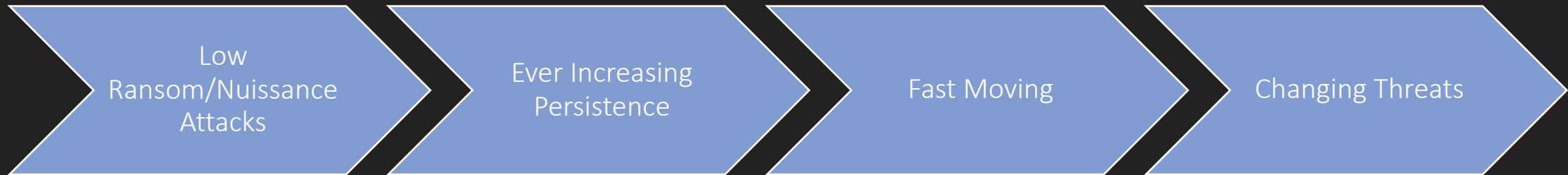
2020

2021

First known quadruple-extortion attack

- These types of attacks are not as frequent
- The average payment surged 171%, to more than \$312K¹⁰

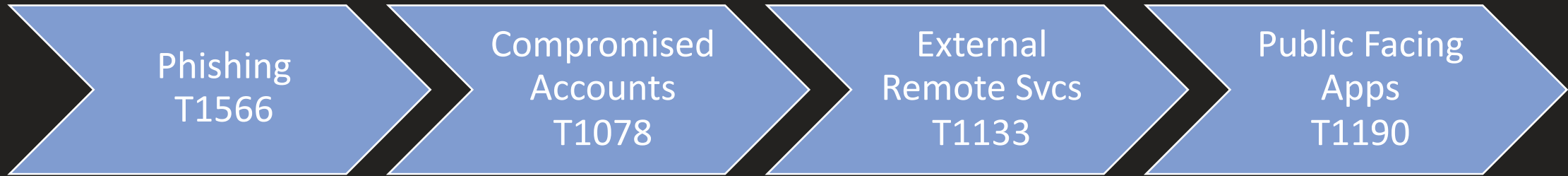
Ransomware Era



Adversary Trends

- Rapid Weaponization
- Knowledge of Victims
- Fileless Malware
- Increased Automation

Top 4 Initial Access Methods



Higher Education Heavy Hitters

AvosLocker

The Basics

- First appeared in 2021
- RaaS model
- Double extortion
- Phone calls and DDoS attacks
- Monero payments preferred
 - 10-25% premium for Bitcoin
- Performs reconnaissance

The Basics (Cont.)

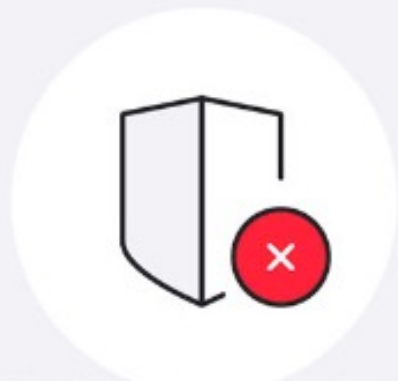
- Exploits internet-facing apps with compromised creds for initial access
 - Depends on skillset of the actor
- Infects Windows and Linux
- Optional command line arguments to enable/disable features

While not as prominent or active as LockBit or Conti, AvosLocker's clever use of familiar tactics makes it a ransomware variant worth monitoring today.



Lateral movement

Uses Paint Data Query (PDQ) Deploy for lateral movement



Defense evasion

Runs on safe mode to avoid certain security measures



Credential access

Uses Mimikatz and XenArmor Password Recovery Pro tool to get credentials



Command and control

Installs AnyDesk, a remote management tool to gain control of targeted systems

© TrendMicro, 2022

Other Malware, Tools, and Exploits

AvosLocker uses a variety of tools and exploits in its campaigns. Some of these are:

Tools



NetScan



AnyDesk



PDQ Deploy



Mimikatz

Exploits



CVE-2021-31207
CVE-2021-34523
CVE-2021-34473
CVE-2021-26855
CVE-2021-40539

© TrendMicro, 2022

The Basics (Cont.)

- Creates a mutex object to avoid re-infection
- Maps accessible drives and enumerated files in directories
- Encrypts files while creating a ransom note in every directory
- Observed cases use the following file extensions:
 - .avos
 - .avos2
 - AvosLinux

Ransom Note

AvosLocker

Attention!

Your systems have been encrypted, and your confidential documents were downloaded.

In order to restore your data, you must pay for the decryption key & application.

You may do so by visiting us at

<http://avosjon4pfh3y7ew3jdwz6ofw7lljcxlbk7hcxxmnlh5kvf2akcqjad.onion>.

This is an onion address that you may access using Tor Browser which you may download at <https://www.torproject.org/download/>

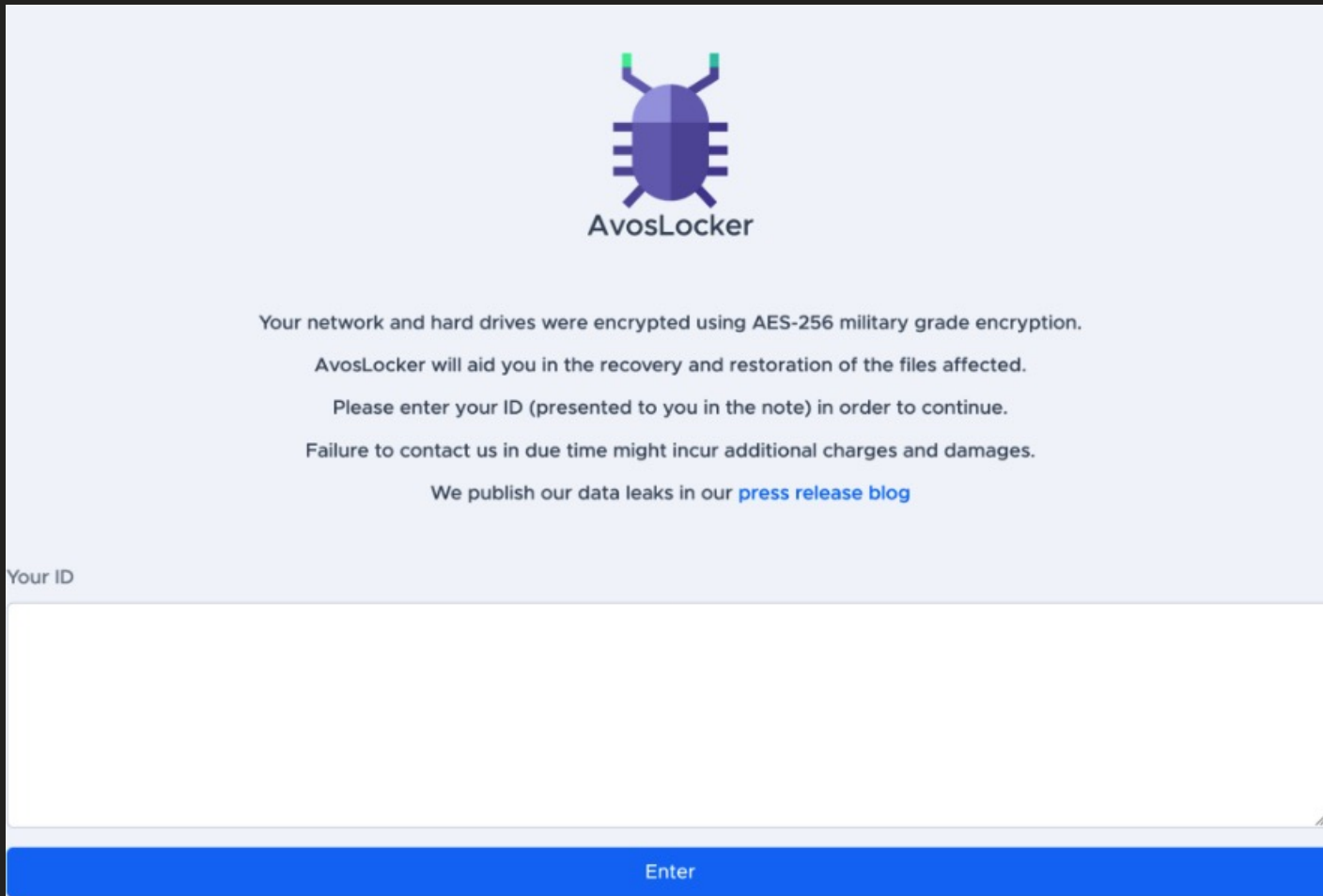
Details such as pricing, how long before the price increases and such will be available to you once you enter your ID presented to you below in this note in our website.


Contact us soon, because those who don't have their data leaked in our press release blog and the price they'll have to pay will go up significantly.

The corporations whom don't pay or fail to respond in a swift manner have their data leaked in our blog, accessible at <http://avosqxh72b5ia23dl5fgwcpndkctuzqvh2iefk5imp3pi5gfhel5klad.onion>

© CISA, 2022

Initial Site to Contact Threat Actor(s)




AvosLocker

Your network and hard drives were encrypted using AES-256 military grade encryption.
AvosLocker will aid you in the recovery and restoration of the files affected.
Please enter your ID (presented to you in the note) in order to continue.
Failure to contact us in due time might incur additional charges and damages.
We publish our data leaks in our [press release blog](#)

Your ID

Enter

- Ransom note link directs users to this Onion website
- Victims prompted to enter unique ID

© Unit 42, 2021

Your network and hard drives were encrypted using AES-256 military grade encryption.
The only method of restoration for your files is using our decryptor. You may buy it for the quoted price below.
You are an enterprise client of ours, thus we will be providing you live-chat support throughout the process.

AvosLocker is not involved in any attacks itself and it acts merely as an arbitrator. It's in our interest that both parties are satisfied with our service.

Countdown

The price will increase to **\$150,000.00 USD** in
0 days 1 hours 41 minutes

Test decryption

You may test our decryption process by uploading a single encrypted image file (.PNG, .JPG, .JPEG) less than 1 MB in size.


No file selected.

Support

Staff Sun, 18 Jul 2021 14:55:24 GMT
Hey, I see that you've visited our payment page. You can text us using this chat.

Staff
As you are an enterprise client of ours, we will provide you with customer support throughout the process. You may use this chat to get in contact with us.

Payment information



Status: Pay 398.94~ XMR (\$75,000.00 USD) to
44VPPFyr1W52iCnv1LJ593jkkZGMbNFPYKV6beMVipx2gTaZeahLKc4ZAj4RrgQSFEBHj4VoJu583aYqJ6KxdRxM1G1Zupg with the payment id:0382b150cb33bfe971f73617885245b35ea0c7973a3c7bee27bdb894138de4a

1. Buy Monero. We have prepared a list of reputable exchanges & retailers for you at the bottom of this page.
2. Send 398.94 XMR to
44VPPFyr1W52iCnv1LJ593jkkZGMbNFPYKV6beMVipx2gTaZeahLKc4ZAj4RrgQSFEBHj4VoJu583aYqJ6KxdRxM1G1Zupg with the payment id 0382b150cb33bfe971f73617885245b35ea0c7973a3c7bee27bdb894138de4a.
3. Wait as we approve your payment.
4. After we approve your transaction our decryptor application will be available for you to download. You will still be able to contact us for assistance through-out the decryption process.

Warning: Ensure that you are paying to the address given to you above and with the correct payment ID unless you are instructed by our staff to do otherwise. If your computer's infected with other malware, they may change your clipboard contents to another Monero address, causing you to lose your funds.

How to buy Monero?

You may buy Monero (XMR) from OTC brokers or exchanges such as Binance.com, Kraken.com. We recommend OTC brokers.

- Upon ID submission, victims are redirected to this payment site.
- Countdown
- Test decryption
- Payment Information
- Support

Vice Society

The Basics

- First observed in 2021
- Double extortion
- No unique ransomware variant
 - Latest payload is a Zeppelin variant
- Exploits internet-facing apps with compromised creds for initial access
- Perform reconnaissance
- TTPs difficult to quantify

The Basics (Cont.)

- Exploiting PrintNightmare
- Variety of tools to move laterally
- "Living off of the Land" Techniques
- Maintain persistence by:
 - Leveraging scheduled tasks
 - Creating undocumented autostart Registry keys
 - DLL side-loading

Ransom Note

ALL YOUR FILES HAVE BEEN ENCRYPTED BY "VICE SOCIETY"
All your important documents, photos, databases were stolen and encrypted.

If you don't contact us in 7 days we will upload your files to darknet.

The only method of recovering files is to purchase an unique private key.
We are the only who can give you tool to recover your files.

To prove that we have the key and it works you can send us 2 files and we decrypt it for free (not more than 2 MB each).

This file should be not valuable!

Write to email: [REDACTED]@onionmail.org
Alternative email: [REDACTED]@onionmail.org

Public email: [REDACTED]@onionmail.org

Our tor website: [REDACTED].onion

Attention!

- * Do not rename encrypted files.
- * Do not try to decrypt your data using third party software, it may cause permanent data loss.
- * Decryption of your files with the help of third parties may cause increased price (they add their fee to ours) or you can become a victim of a scam.

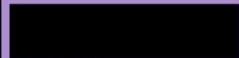


FOR JOURNALISTS **FOR VICTIMS** **OUR BLOG**

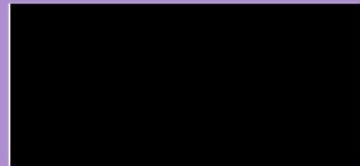
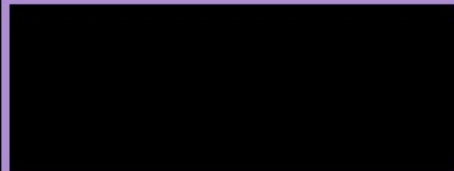
We are also here:

m: [redacted]id.onion
v: [redacted]id.onion
ss: [redacted]id.onion

OUR PARTNERS



Local State



[View documents >>](#)

Example of Vice Society's Data Leak Site

- Victims referred to as "Our Partners"
- Areas blacked out are victim info
 - Company Name
 - Logo
 - Website
 - Mission Statement

IOCs

Email Addresses	
v-society.official@onionmail[.]org	
ViceSociety@onionmail[.]org	
OnionMail email accounts in the format of [First Name][Last Name]@onionmail[.]org	
IP Addresses for C2	Confidence Level
5.255.99[.]59	High Confidence
5.161.136[.]176	Medium Confidence
198.252.98[.]184	Medium Confidence
194.34.246[.]90	Low Confidence

IOCs (Cont.)

TOR Address	
http://vsociethok6sbprvevl4dlwbqrzyhxcxaqpvcqt5belwvsuxaxsutyaad[.]onion	
MD5	SHA1
fb91e471cfa246beb9618e1689f1ae1d	a0ee0761602470e24bcea5f403e8d1e8bfa29832
	3122ea585623531df2e860e7d0df0f25cce39b21
	41dc0ba220f30c70aea019de214eccd650bc6f37
	c9c2b6a5b930392b98f132f5395d54947391cb79

© CISA, 2022

AlphaV/BlackCat

The Basics

- First observed in 2021
- Compromised creds for initial access though not exclusively
- Each build is victim-specific
 - Unique info hard-coded into the binary at compile time
- Difficult to share samples due to the uniqueness
- Uses Windows Task Scheduler
- PowerShell scripts/Cobalt Strike for initial deployment
- Steals any data stored on the cloud

The Basics (Cont.)

- Rust programming language
- Targets and encrypts Windows and Linux devices and VMWare instances
- Self-propagation
- Can bypass UAC

Ransom Note

>> What happened?

Important files on your network was ENCRYPTED and now they have "iz5zhcr" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your network was DOWNLOADED.
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:

- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Private financial information including: clients data, bills, budgets, annual reports, bank statements.
- Manufacturing documents including: datagrams, schemas, drawings in solidworks format
- And more...

>> CAUTION

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

>> What should I do next?

- 1) Download and install Tor Browser from: <https://torproject.org/>
- 2) Navigate to:



Source: HSDI

To Pay or Not to Pay.....

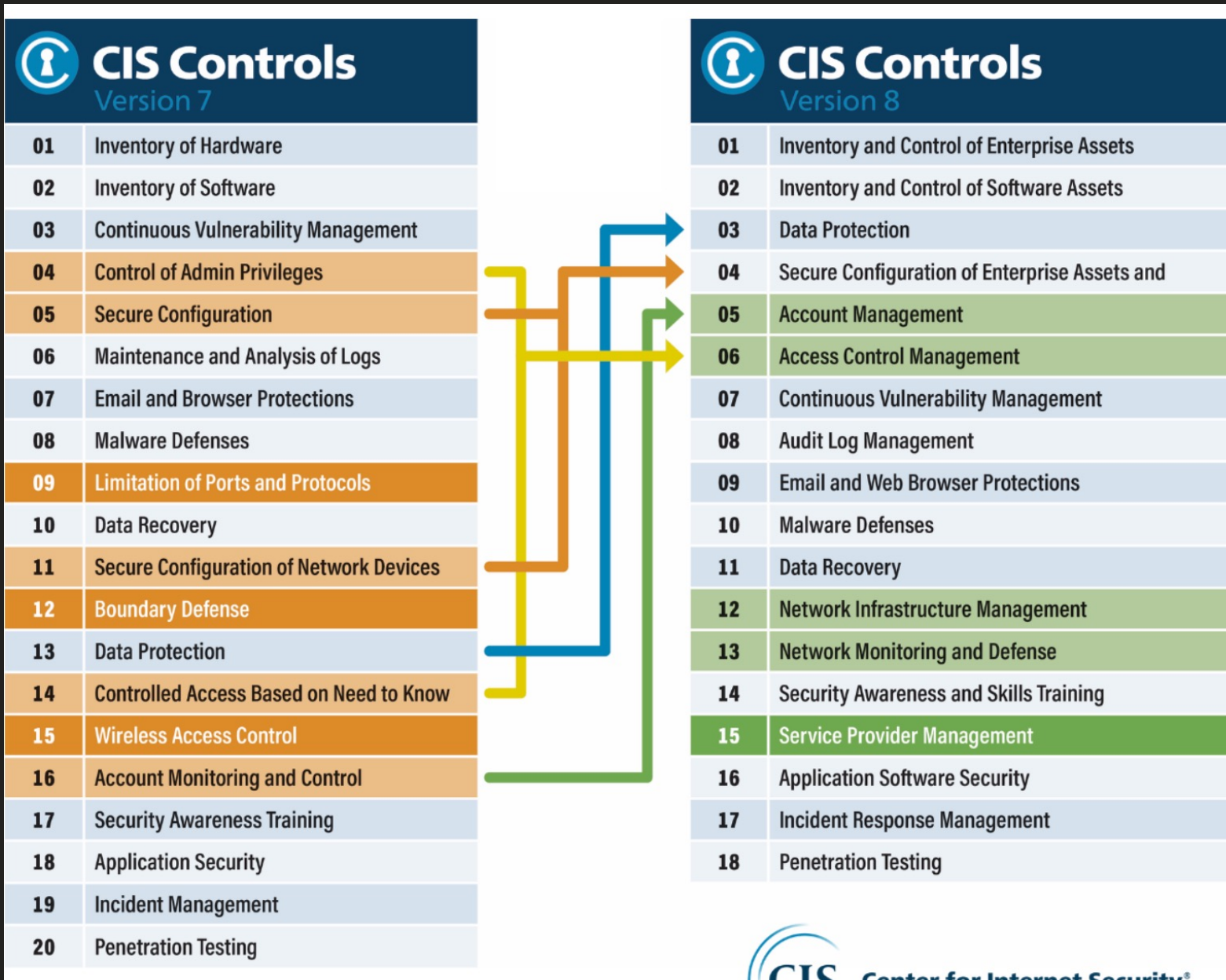
- Repeat Attacks
- Double, Triple, & Quadruple Extortion
- Reputation of the Ransomware Author
 - Likelihood of getting the decryption key (WannaCry)
 - Does the decryption key work? (NotPetya)
- Insurance considerations

Best Practices

- Mitre ATT&CK Framework
- CIS Control Framework
- Incident Response
 - Policy
 - Plan
 - Playbooks
- Principal of Least Privilege
- Asset Management
- Baseline network behavior
- Workshops/Tabletops
- Threat/Intel/Best Practices Sharing
- Network Segmentation
- Backups -
 - Air Gap & TEST!!!
- Multiple copies of critical data and servers in different physical locations
- Vulnerability Management
- MFA

Guidance

- REN-ISAC Peer Assessment
- CISA Ransomware Readiness Assessment
- CISA Cyber Hygiene Services
- Alert & Advisories with IOCs



CIS Control Framework

- Where To Start?
 - • Focus on the basics! Start with IG1
 - • Know your asset inventory (CIS Control 1 & 2)
 - • Protect your data (CIS Control 13 & 14)
 - • Securely configure your assets (CIS Control 5)
 - • Patch and update (CIS Control 3)
 - • Scan for vulnerabilities (CIS Control 3)
 - • Have backups - protect and test them (CISControl 10)
 - • Train your workforce (CIS Control 17)
 - • If all else fails...have a plan! (CIS Control 19)

Sources

Brumaghin, Edmund, et al. “Vice Society Leverages PrintNightmare in Ransomware Attacks.” *Cisco Talos Blog*, 19 Sept. 2022, blog.talosintelligence.com/vice-society-ransomware-printnightmare.

Cimpanu, Catalin. “ALPHV (BlackCat) Is the First Professional Ransomware Gang to Use Rust.” *The Record by Recorded Future*, 9 Dec. 2021, therecord.media/alphv-blackcat-is-the-first-professional-ransomware-gang-to-use-rust.

FBI. *CU-000167-MW: BlackCat/ALPHV Ransomware Indicators of Compromise*. 19 Apr. 2022, www.ic3.gov/Media/News/2022/220420.pdf.

---. *#StopRansomware: Vice Society | CISA*. 8 Sept. 2022, www.cisa.gov/uscert/ncas/alerts/aa22-249a.

FinCERT and FBI. *CU-000164-MW: IOCs Associated With AvosLocker Ransomware*. 17 Mar. 2022, www.ic3.gov/Media/News/2022/220318.pdf.

Fooks, Natasha. “AvosLocker – the Rising Star of Ransomware.” *Cyberint*, 17 Feb. 2022, cyberint.com/blog/research/avoslocker-the-rising-star-of-ransomware.

An In-Depth Look at AvosLocker Ransomware. www.avertium.com/resources/threat-reports/in-depth-look-at-avoslocker-ransomware.

Malwarebytes Threat Intelligence Team. *AvosLocker Enters the Ransomware Scene, Asks for Partners*. 23 July 2021, www.malwarebytes.com/blog/threat-intelligence/2021/07/avoslocker-enters-the-ransomware-scene-asks-for-partners.

Sources (Cont.)

McCafferty, Katie. “DEV-0832 (Vice Society) Opportunistic Ransomware Campaigns Impacting US Education Sector.” *Microsoft Security Blog*, 25 Oct. 2022, www.microsoft.com/en-us/security/blog/2022/10/25/dev-0832-vice-society-opportunistic-ransomware-campaigns-impacting-us-education-sector.

Meskauskas, Tomas. “VICE SOCIETY Ransomware.” *Decryption, Removal, and Lost Files Recovery (Updated)*, 21 July 2022, www.pcrisk.com/removal-guides/21962-vice-society-ransomware.

Oliveria, Paul. “The Many Lives of BlackCat Ransomware.” *Microsoft Security Blog*, 18 Aug. 2022, www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware.

Team, The BlackBerry Research Intelligence. *Threat Thursday: AvosLocker Prompts Advisory From FBI and FinCEN*. 7 Apr. 2022, blogs.blackberry.com/en/2022/04/threat-thursday-avoslocker-prompts-advisory-from-fbi-and-fincen.

Trend Micro Research. *Ransomware Spotlight: AvosLocker*. 22 Apr. 2022, www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-avoslocker.