U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Infrastructure Assistance Coordinating Council (IACC)

Ransomware Threats and Mitigations

Ian Moore, CISSP
Cybersecurity State Coordinator (CSC) for Washington State
Cybersecurity Advisor (CSA) Program
Cybersecurity and Infrastructure Security Agency

October 19th, 2021

CISA
CYBER+INFRASTRUCTURE

Contents

- Ransomware Defined
- Ransomware Demographics
- Who is Targeting You?
- Ransomware Threats in the Wild!
- Mitigations You Can Do Now!
- CISA Services
- PISCES & ISACs

Fear, Uncertainty, and Doubt

Awareness to make better decisions.

CISA
CYBER+INFRASTRUCTURE

Ransomware Defined

- Ransomware is malware that encrypts your data that the attacker can use for extortion or to demand a ransom.
- Phishing or drive-by hacked sites
- Get in by remote access
  - Unmonitored Internet access
- Claim to use “military-grade” encryption
- Control malware manually or remote control
- Attackers rely on no backup plans and no redundancy
- You can’t trust a hacker
  - They may never give you the decryption key
- Extortion
  1. Single - Encryption
  2. Double - Release financial data on the Dark Web
  3. Triple - Contacting your customers and extorting their data

CISA CYBER+INFRASTRUCTURE

Who is targeting you?

Ransomware Demographics

Affected Industry

- Automobile & Parts
- Banks
- Chemicals
- Construction & Materials
- Consumer Goods
- Financial Services
- Gas, Water & Multi-utilities
- General Industrials
- Health Care Equipment & Services
- Industrial Transportation
- Legal
- Oil Equipment Services & Distribution
- Retail
- Technology

Target Geography

- Canada
- Turkey
- India
- Indonesia
- Singapore
- Switzerland
- Greece
- Italy
- Thailand
- United Arab Emirates
- New Zealand
- Taiwan
- Bulgaria
- Ireland
- South Korea
- Angola
- United States
- Spain
- Sri Lanka
- Brazil
- Puerto Rico
- Poland

Targeted Information

- Corporate Employee Info
- Customer Data
- Financial Data
- Intellectual Property
- Government Information
- IT Information
- Legal Documents

Ransomware in the Wild! – Sample from the week prior to 17 August 2021

AVOSLOCKER
- Moorfields NHS UK & Dubai (AE) - moorfields[.]ae.

BLACKMATTER
- Pine Labs (IN)
- HHCP Architects (US) - hhcp[.]com.
- Solar Coca-Cola (BR) - solarbr[.]com[.]br.

CLOP
- Zucchetti Rubinetteria S.p.A. (IT) - zucchettikos[.]it.
- ABCO Automation (US) - goabco[.]com.
- Rocky Mountain Instrument Co. (US) - rmico[.]com.
- AMPM Billing (US) - ampmbilling[.]com.
- Pension Benefit Consultants, Inc. (US) - penbens[.]com.

CONTI
- WEI (US) - wei[.]com.
- Enns Brothers (CA) - ennsbrothers[.]com.
- Welliver (US) - buildwelliver[.]com.

CUBA
- Quercus (PL) - quercus[.]pl.

HIVE
- Osprey Video (US) - ospreyvideo[.]com.
- Brakke (NZ) - brakke[.]eu.

LOCKBIT
- Smith, Gambrell & Russell, LLP (US) - sgrlaw[.]com.
- ESR Motor Systems (US) - esrmotors[.]com.
- Megawatts Engineering Services Pte Ltd (SG) - megawatts[.]com[.]sg.
- Accenture (IE) - accenture[.]com.
- The National Wild Turkey Federation (US) - nwtf[.]org.
- JINYANG OILSEAL (KR) - jy-oilseal[.]com.
- Audit Treuhand AG (CH) - audit-treuhand[.]ch.
- Seliner (CH) - selinerag[.]ch.
- Pike County Sheriff's Office (US) - pikecountysheriffsoffice[.]com.

LORENZ
- Sebastian (US) - sebastiancorp[.]com.

RAGNAROK
- Hitit Gümrük Müşavirliği (TR) - hititgumruk[.]com.
- DAE MYUNG RAINWEAR LANKA LTD (LK).

Released their decryption key and closed shop.

RANSOMEXX
- GIGABYTE (TW) - gigabyte[.]com.

SUNCRYPT
- Cornerstone Automation Systems, LLC (US) - casiusa[.]com.

CISA CYBER+INFRASTRUCTURE

Mitigations You Can Do Now! (1 of 2)

- Network Segmentation
- Multi-factor authentication
- Strong spam filters to prevent phishing emails from reaching end users
- User training program
- Filter network traffic
- Update all software
- Limit access to resources over networks
  - Restrict RDP and block SMB
- Set antivirus/antimalware programs to conduct regular scans
- Risk-based and prioritized asset inventory
- Prevent unauthorized execution by:
  - Disabling macro scripts entering your org
  - Implementing application allow listing
  - Monitor and/or block inbound connections
  - Detect and/or block inbound connection from Cobalt Strike servers and other post exploitation tools
- Establish and test a robust backup program
  - Frequent backups (full and incremental)
  - 3-2-1 strategy – (3 copies, 2 different media onsite, and one copy offsite)
  - Test by recovering from backups on a set schedule

CISA
CYBER+INFRASTRUCTURE

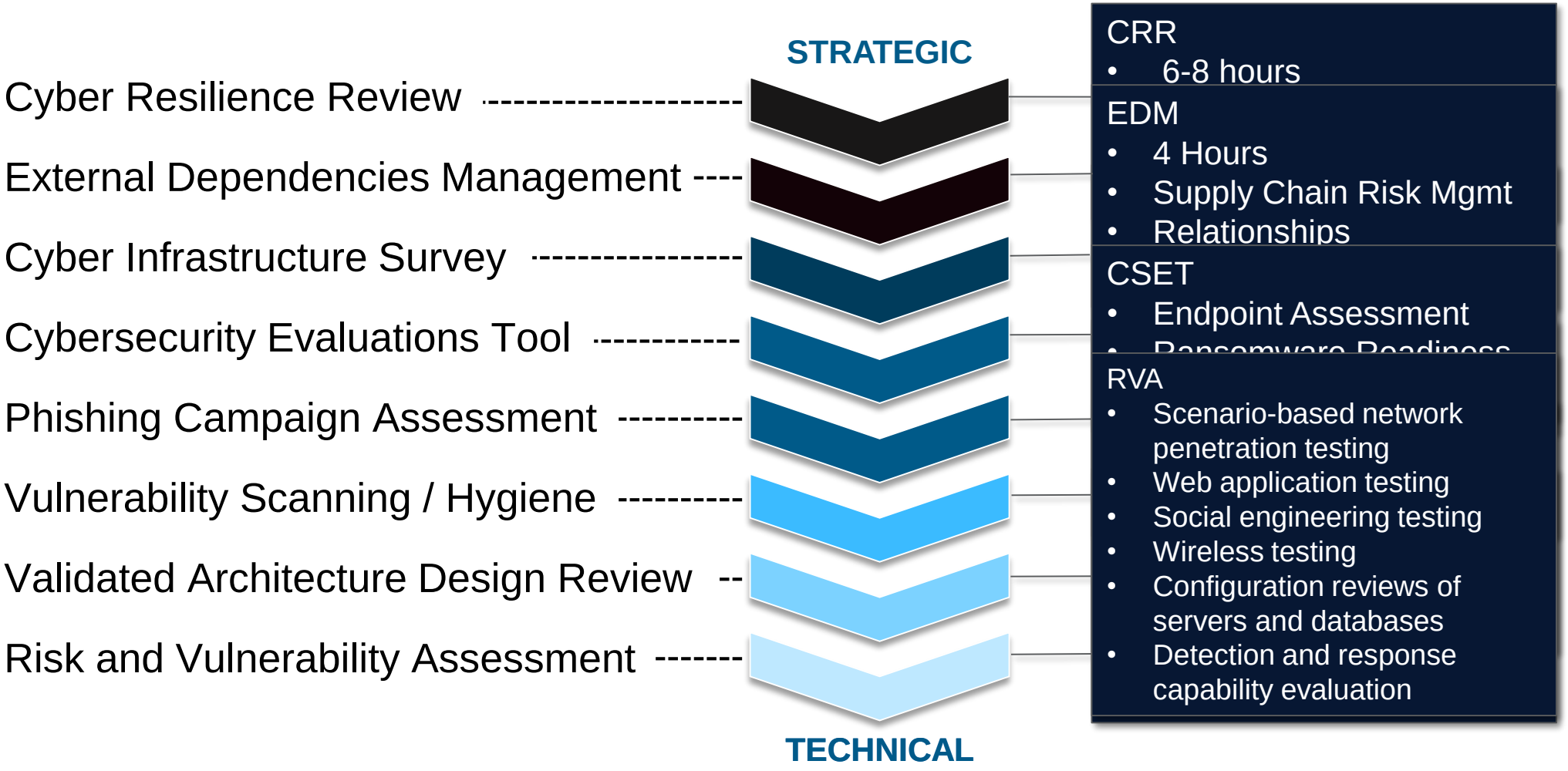
Mitigations You Can Do Now! (2 of 2)

- CISA and FBI urge Critical Infrastructure (CI) owners and operators to apply the following mitigations:
  - Implement network segmentation between IT and OT networks
  - Define a demilitarized zone
  - Logical zones for OT assets
  - Define acceptable communication conduits between the zones
  - Deploy security controls to filter network traffic and monitor communications between zones
  - Prohibit industrial control system (ICS) protocols from traversing the IT network

Operational Technology (OT) – The SCADA and ICS that manage and control the critical mission and infrastructure of the organization.

CISA
CYBER+INFRASTRUCTURE

Cybersecurity Assessments and Services



CISA
CYBER+INFRASTRUCTURE

PISCES and ISACs

- Public Infrastructure Security Cyber Education System (PISCES)
  - Provides a data-sharing network to small communities in need of critical cybersecurity analysis.
  - Students get hands-on experience
    - Security monitoring of real-time data on local government networks
    - Providing a crucial service for small cities and counties that might not otherwise be able to afford it
  - Academic Partners: Western Washington University, Spokane Falls CC, Central Washington University, Eastern Washington University, and Alabama A&M University
- Information Sharing and Analysis Centers (ISAC)
  - Through CISecurity.org
  - Information sharing
  - Many free services

CISA CYBER+INFRASTRUCTURE

https://pisces-intl.org/ / https://cisecurity.org

Conclusion

- Ransomware Defined
- Ransomware Demographics
- Who is Targeting You?
- Ransomware Threats in the Wild!
- Mitigations You Can Do Now!
- CISA Services
- PISCES & ISACs

Contacts and Questions?

Ian Moore
Region X
Cybersecurity State Coordinator for Washington State
(360) 594-1832
Ian.Moore@cisa.dhs.gov

Ron Watters
Region X (WA, OR, ID, AK)
Cybersecurity Advisor
(206) 348-4071
Ronald.Watters@cisa.dhs.gov

CISA
CYBER+INFRASTRUCTURE

For inquiries or further information,
contact cyberadvisor@cisa.dhs.gov