HRSD

Cleaning wastewater every day for a better Bay.

Round Table Discussion:
Cyber Incidents and the Public Sector
(HRSD Ransomware Incident)

VA AWWA/VWEA ITC Meeting
05/20/2021

80 years of sustainability

HRSD

Agenda

- Little about me
- What is RYUK?
- Anatomy of the incident
- What could have been and what was
- Threats and trends
- What we must do

About Me…

Roger Caslow

Chief Information Security Officer

Contact Information:

rcaslow@hrsd.com

Experience

- ✓ 30 years security experience
  - ✓ Physical Security/Force Protection
  - ✓ Insider Threat/Counterintelligence
  - ✓ Cybersecurity
- ✓ 20 years as a cybersecurity professional
- ✓ 7 years working with securing operational technology
  - ✓ Automotive – Dana
  - ✓ Power & Water - GE
  - ✓ Water & Wastewater – Suez WTS
- ✓ 13 years National Security experience (DIA, CIA, DoD)
- ✓ Cross business vertical experience

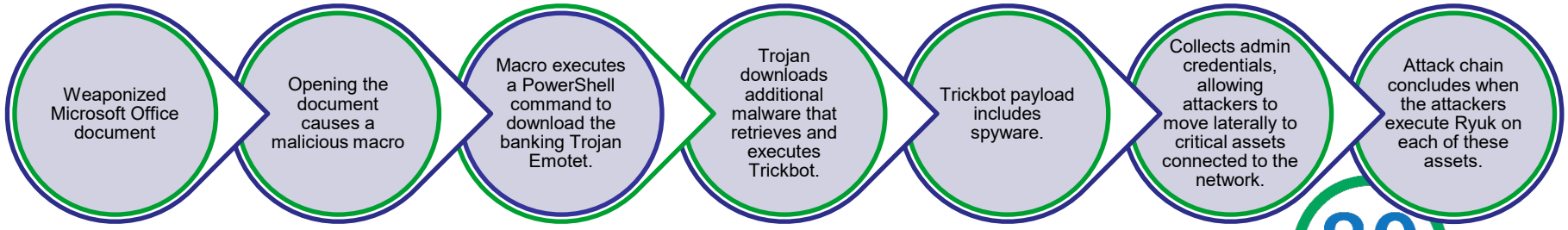
Education and Certifications

- National Intelligence University - Post Graduate Intelligence Program, Information Operations
- University of Central Florida – Master of Arts, Applied Economics (MAAE)
- Certified Information Systems Security Professional (CISSP)

80 years of sustainability HRSD

HRSD Ransomware Attack - What is RYUK?

- Ryuk is the name of the ransomware family that we dealt with
  - First discovered in the wild in August 2018.
  - It is one of the nastiest ransomware families to ever plague systems worldwide.
- What is Ryuk ransomware?
  - Ransomware is a category of malware that locks your files or systems and holds them hostage for ransom.
  - Ryuk is a type of ransomware used in targeted attacks, where the threat actors make sure that essential files are encrypted so they can ask for large ransom amounts.
- How does Ryuk work?
  - Ryuk is one of the first ransomware families to include the ability to identify and encrypt network drives and resources.
  - Attackers can then disable Windows System Restore for users, making it impossible to recover from an attack without external backups or rollback technology.
- Who are Ryuk's targets?
  - Ryuk's targets tend to be high-profile organizations where the attackers know they are likely to get paid their steep ransom demands. Victims include cities, EMCOR, UHS hospitals, and several newspapers.
  - In targeting these organizations, Ryuk was estimated to have generated a revenue of $61 million for its operators between February 2018 and October 2019 and rising.
- How is Ryuk delivered?



80 years of sustainability
HRSD

Anatomy of the HRSD Incident

1) Earliest evidence of Threat Actor activity in the HRSD environment occurred on October 23, 2020, at 11:27 EST
   - First file, BaEeqfgJ.dat, of 13 randomly named folders and 12 randomly named files in paths C:\Users\Public and C:\Users\XXXX was created on XXXXXXXX.
   - A file created in the same folder, upot.dll, subsequently created at 11:30 EST on the same day attributed via hash to ZLoader malware. (Financial services credential harvester and malware delivery platform)
   - Highly likely all file and folders created within the timeframe of October 23, 2020, at 11:27 to 11:31 EST were related to the ZLoader malware.
2) Initial entry point of the ZLoader malware identified to a specific end user.
   - Shortly before the first ZLoader file was created on October 23, 2020, on system XXXXXX, there was the creation of a LNK file (linker file) for an Excel spreadsheet, rec9628.xls on October 23, 2020, at 11:27 EST created in path C:\Users\XXXXXX\AppData\Roaming\Microsoft\Windows\Recent\.
   - Presence of the LNK file indicated that the user opened the spreadsheet shortly before the ZLoader malware creation occurred on the system.
   - Activity is consistent with the opening of a potentially malicious spreadsheet designed to infect the system via embedded malicious code in the spreadsheet that executes on opening.
3) Threat Actor used the system SSADS3 extensively for their malicious activities.
   - Indicators of compromise ("IOCs") on system SSADS3, indicating the Threat Actor used this system as a main location of malicious activity.
   - This included creation of a service related to a Cobalt Strike (Commercial Red Team Software) beacon for command and control on November 17, 2020, at 15:03 EST, and the first noted creation of the Ryuk binaries, v2.exe and v2c.exe, on the HRSD network on November 18, 2020.

Anatomy of the HRSD Incident Cont.

4) Ryuk ransomware related files found on 45 unique systems in the HRSD network.
   - Evidence showed 45 unique systems with Ryuk ransomware related IOCs including ransomware binaries, GPO deployment policies, or encrypted files with .ryk extensions.

5) Most recent evidence of Threat Actor activity in the HRSD environment occurred on December 3, 2020, at 05:35 EST.
   - Observed the creation of a ZLoader file rapi.exe in path C:\Users\XXXXXX\AppData\Local\Temp\ on system XXXXXX.
   - New endpoint sensors installed on this system on December 3, 2020, at 09:16 EST and subsequently three detections for process hollowing (method of executing arbitrary code in the address space of a separate live process to evade anti-malware) were made on:
     - December 3, 2020, at 11:13 EST,
     - December 4, 2020, at 07:23 EST,
     - December 4, 2020, at 12:26 EST.
   - Forensics reported the system to HRSD as compromised on December 7, 2020, - removed from the network.
6) No forensic evidence of data staging/exfiltration identified in the HRSD environment…

Impact – What Was and What Could Have Been…

What DID Happen:

- Windows Business Systems Down For Three Weeks
  - PCs
  - Connected Services
- All Internet Connections Physically Disconnected
- Accounting and Billing Ceased Operations
- Linux Based Systems Disconnected

What Did NOT Happen:

- Length of Time to Recover
- Corrupted Back-Ups
- Spread Through Partner Connections
- Data Loss/Breach
- Linux Systems Compromised
- ICS – DCS – SCADA Systems Loss/Compromise

Threats Keep Growing …

General

Shamoon - spreads across network, compiles file locations, upload's locations o the attacker, and erases them.

Wiper - a class of malware whose intention is to wipe the hard drive of the computer it infects.

Flame - most complex malware ever found. Spreads over local network (LAN). It can record audio, screenshots, keyboard activity and network traffic. The program also records Skype conversations and can turn infected computers into Bluetooth beacons which attempt to download contact information from nearby Bluetooth-enabled devices.

Gauss (Flame platform) - nation state sponsored banking Trojan which carries a warhead of unknown designation.

Night Dragon - (Compiled attack) Compromises public-facing web servers via SQL injection; install malware and RATs.

Target Attack - initial penetration point of the attackers was through stolen HVAC vendor's credentials, attackers used the vendor's stolen credentials to gain access to a Target hosted web services for vendors, deployed malware on many Target's POS machines which was used to steal credit card information.

Not Petya - malware harvests passwords - claims to be ransomware, like Petya, the encryption routine is modified, and the malware cannot technically revert changes

WannCry - ransomware cryptoworm targeting Windows

ICS Specific

Stuxnet targeted SCADA systems, specifically PLCs

Duqu (Stuxnet platform) looks for information that could be useful in attacking industrial control systems.

Havex - two primary components: A RAT and a C&C server written in PHP. Havex also includes a scanning module used to search for industrial devices on a network. The scanning module was designed to scan ports of known ICS/SCADA solutions.

Crash Override – Uses an open backdoor to control all other components of the malware, connected to a remote C&C server to receive commands from the attackers. Components target open-source industrial communication protocols.

Triton - disables safety instrumented systems, which can then contribute to a plant disaster. It has been called "the world's most murderous malware."

Sam Sam – ransomware group, exploiting ICS

Cybersecurity Trends – Last 30 Days

Vulnerabilities

- CVE-2021-31166 | CVE-2021-26311 | CVE-2021-1477 | CVE-2021-21224 | CVE-2021-27342

Malware

- Lizar | TeaBot | Avaddon Ransomware | DarkSide Ransomware | Bizarro

Attackers

- Magecart | Conti Gang | APT36 | Anonymous Mexico | AnonGh0st

Targets

- Liferay Portal | Health Service Executive | Toshiba | AXA S.A. | Apple AirTag

Operations

- OpIsrael | OpCloudHopper | Operation INFEKTION | OpPLATO | Operation Arid Viper

Use Some Best Practices for Normal Hygiene

- Follow a framework – PICK ONE and execute on it! (CIS, CSF, ISO, etc)
- Asset Management - Know your assets
- Patch Management – Maintain a vulnerability-based program
- Change Management – Plan, execute, and verify configuration changes
- Configuration Management - Consistency and standardization
- Have a risk register – maintain it
- Know your requirements – don't follow shiny objects
- Have an IR Plan
  - OT-specific IR plans and procedures are necessary to help organize and guide IT, InfoSec, and OT teams to success in RW events
  - Use relevant IOCs with your tabletops and gamification
- Maintain a disaster recovery plan
  - Backup plan and follow-through
  - Backup regimen to follow your industry best practices and then add one layer UP
  - Test, test, test, and TEST
- Enforce MFA
- RDP is a fact of life in many industries… make it SECURE
- Patch your employees – ALL of your employees

10

Final Take Away

Only THREE routes known for ransomware to hit your environment:

- Email Phishing
- Default/Shared Password Use
- Unsecured Remote Desktop Access

Not “If” But When

“Luck is what happens when preparation meets opportunity” …Seneca