“NEW EPSILON RED RANSOMWARE TARGETING UNPATCHED MICROSOFT EXCHANGE SERVERS”

By
Aastha Sahni

SPEAKER INTRODUCTION

- **Lead CyberSecurity Instructor- Flatiron School**
- **OWASP WIA Committee Member**
- **Founder - CyberPreserve (CyberSecurity Mentoring Initiative ,YouTube channel)**
- **Founder & Lead – Lean In: Breaking Barriers (Women in CyberSecurity)**

AGENDA

What is Ransomware?

Epsilon Red – Background

Microsoft Zero Day Vulnerabilities

Victim – Epsilon Red

Attack Details

Barebones Ransomware

Ransomware as a Service - RAAS

Remediation

Paying for a Ransomware

Prevention – Epsilon Red

Prevention - Ransomware

So, what is a Ransomware?

- Ransomware is a form of malware where cybercriminals attack your system with malicious code. Their intent is to lock you out of your system and encrypt your important and sensitive data. Further, they demand ransom from you before they provide a decryption key for your locked system and encrypted data.

EPSILON RED - BACKGROUND

It appears that an enterprise Microsoft Exchange server was the initial point of entry by the attackers into the enterprise network.

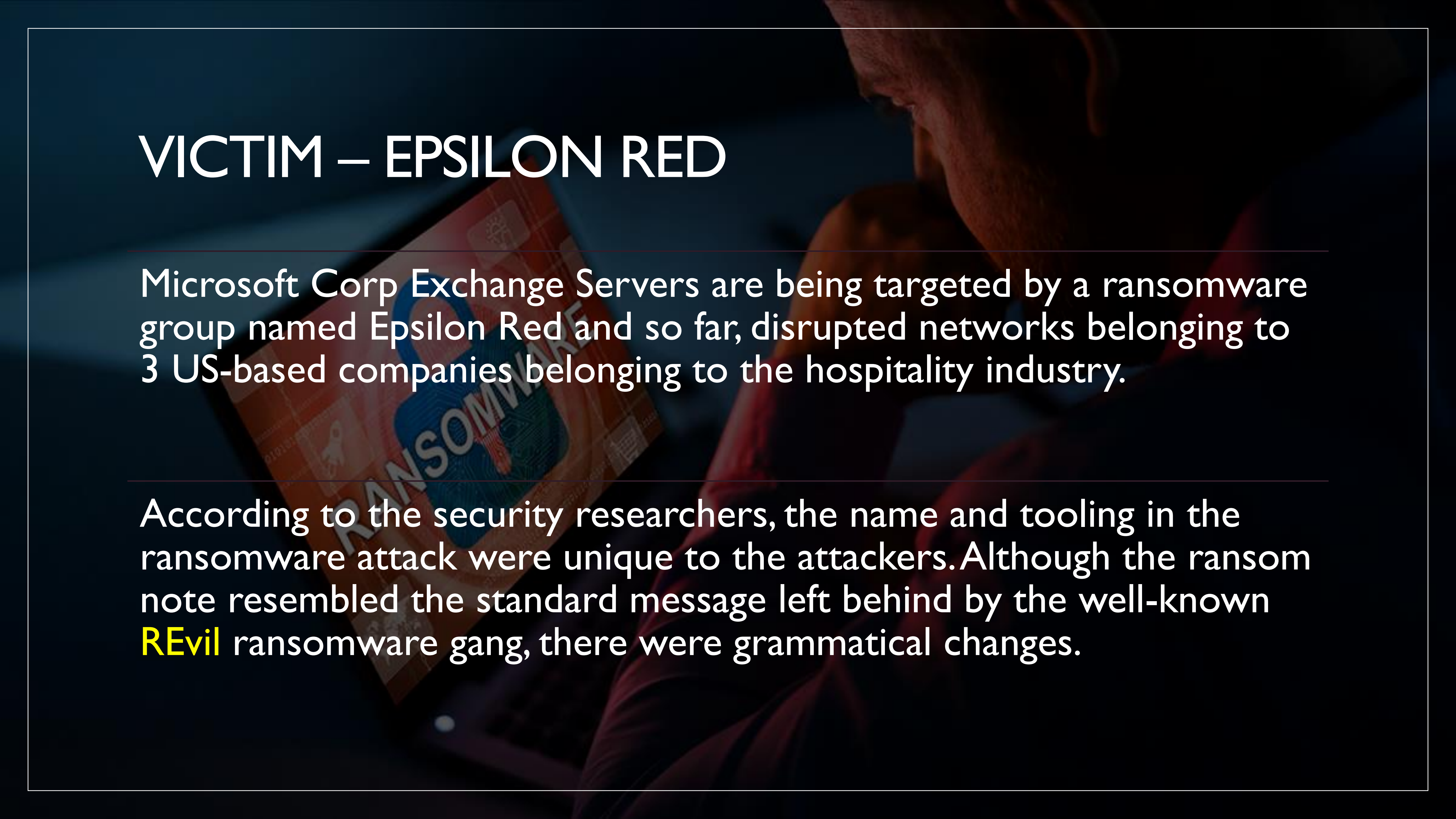
It isn't clear whether this was enabled by the ProxyLogon exploit or another vulnerability, but it seems likely that the root cause was an unpatched server.

From that machine, the attackers used WMI to install other software onto machines inside the network that they could reach from the Exchange server.

MICROSOFT ZERO DAY VULNERABILITIES

Microsoft Exchange Server 2013, 2016, or 2019 - March 2021:

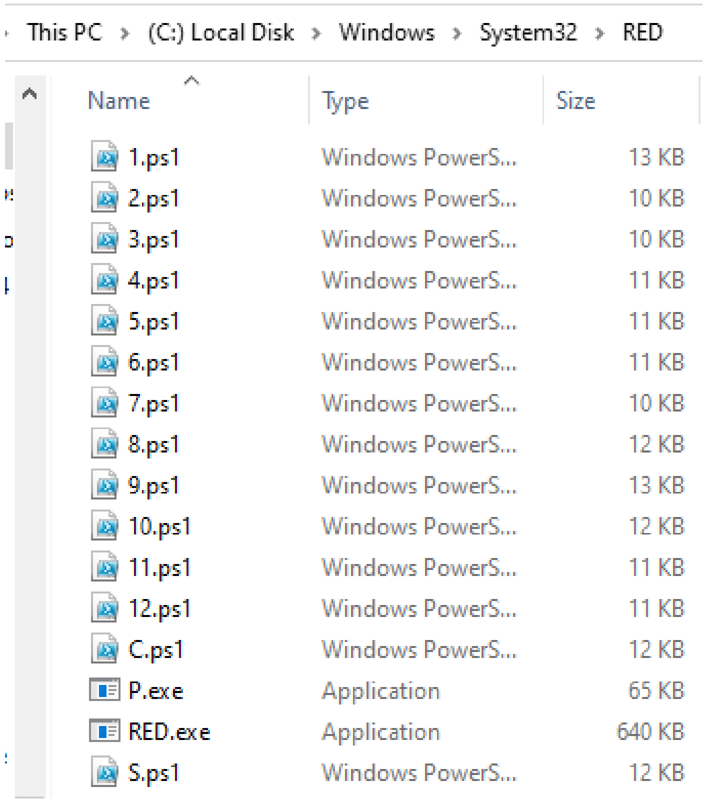
- CVE-2021-26855 is a server-side request forgery (SSRF) vulnerability in Exchange Server.
- CVE-2021-26857 is an insecure deserialization vulnerability in the Unified Messaging service.
- CVE-2021-26858 & CVE-2021-27065 - a post-authentication arbitrary file write vulnerability in Exchange.



VICTIM – EPSILON RED

Microsoft Corp Exchange Servers are being targeted by a ransomware group named Epsilon Red and so far, disrupted networks belonging to 3 US-based companies belonging to the hospitality industry.

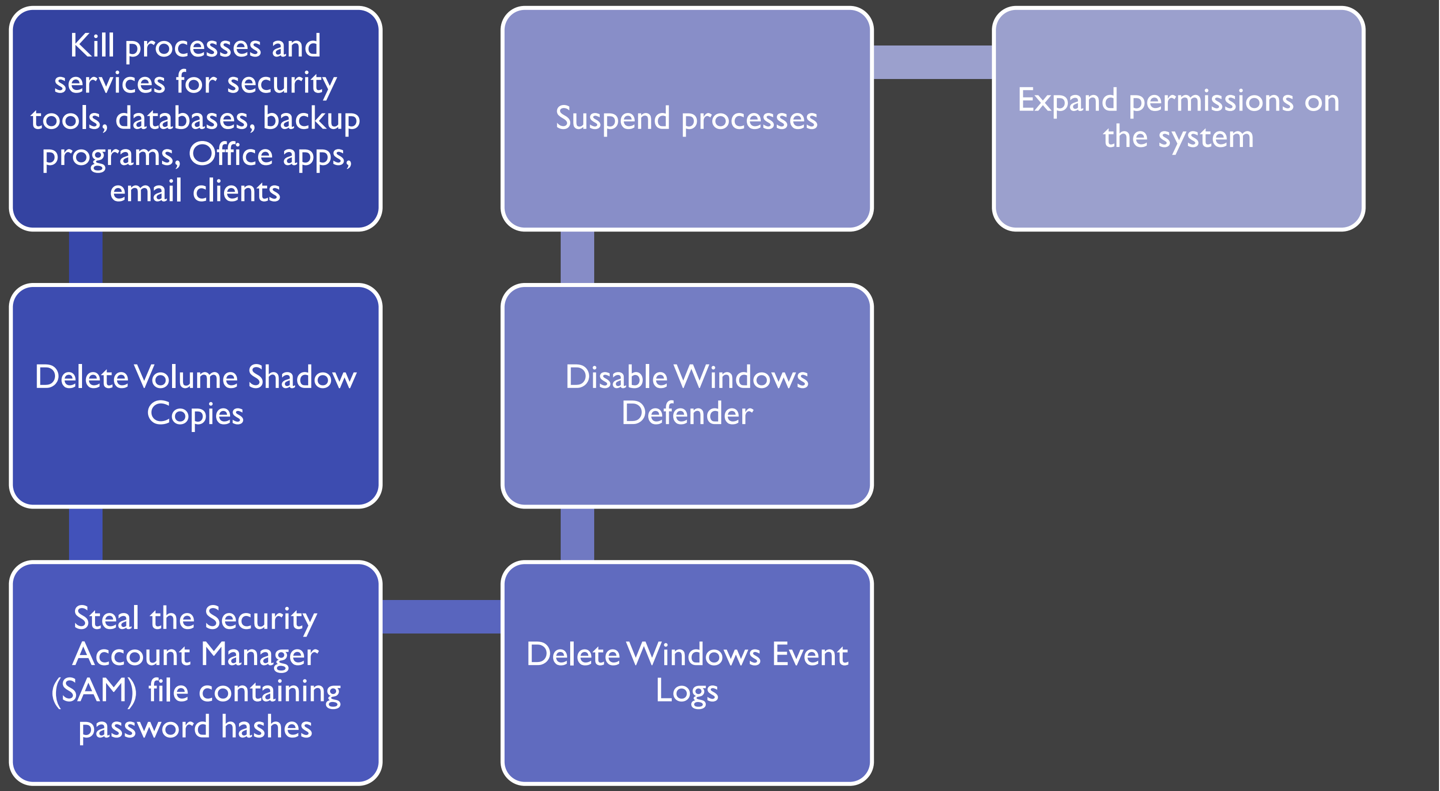
According to the security researchers, the name and tooling in the ransomware attack were unique to the attackers. Although the ransom note resembled the standard message left behind by the well-known REvil ransomware gang, there were grammatical changes.



This PC › (C:) Local Disk › Windows › System32 › RED

Name	Type	Size
1.ps1	Windows PowerS...	13 KB
2.ps1	Windows PowerS...	10 KB
3.ps1	Windows PowerS...	10 KB
4.ps1	Windows PowerS...	11 KB
5.ps1	Windows PowerS...	11 KB
6.ps1	Windows PowerS...	11 KB
7.ps1	Windows PowerS...	10 KB
8.ps1	Windows PowerS...	12 KB
9.ps1	Windows PowerS...	13 KB
10.ps1	Windows PowerS...	12 KB
11.ps1	Windows PowerS...	11 KB
12.ps1	Windows PowerS...	11 KB
C.ps1	Windows PowerS...	12 KB
P.exe	Application	65 KB
RED.exe	Application	640 KB
S.ps1	Windows PowerS...	12 KB

ATTACK DETAILS



Kill processes and services for security tools, databases, backup programs, Office apps, email clients

Delete Volume Shadow Copies

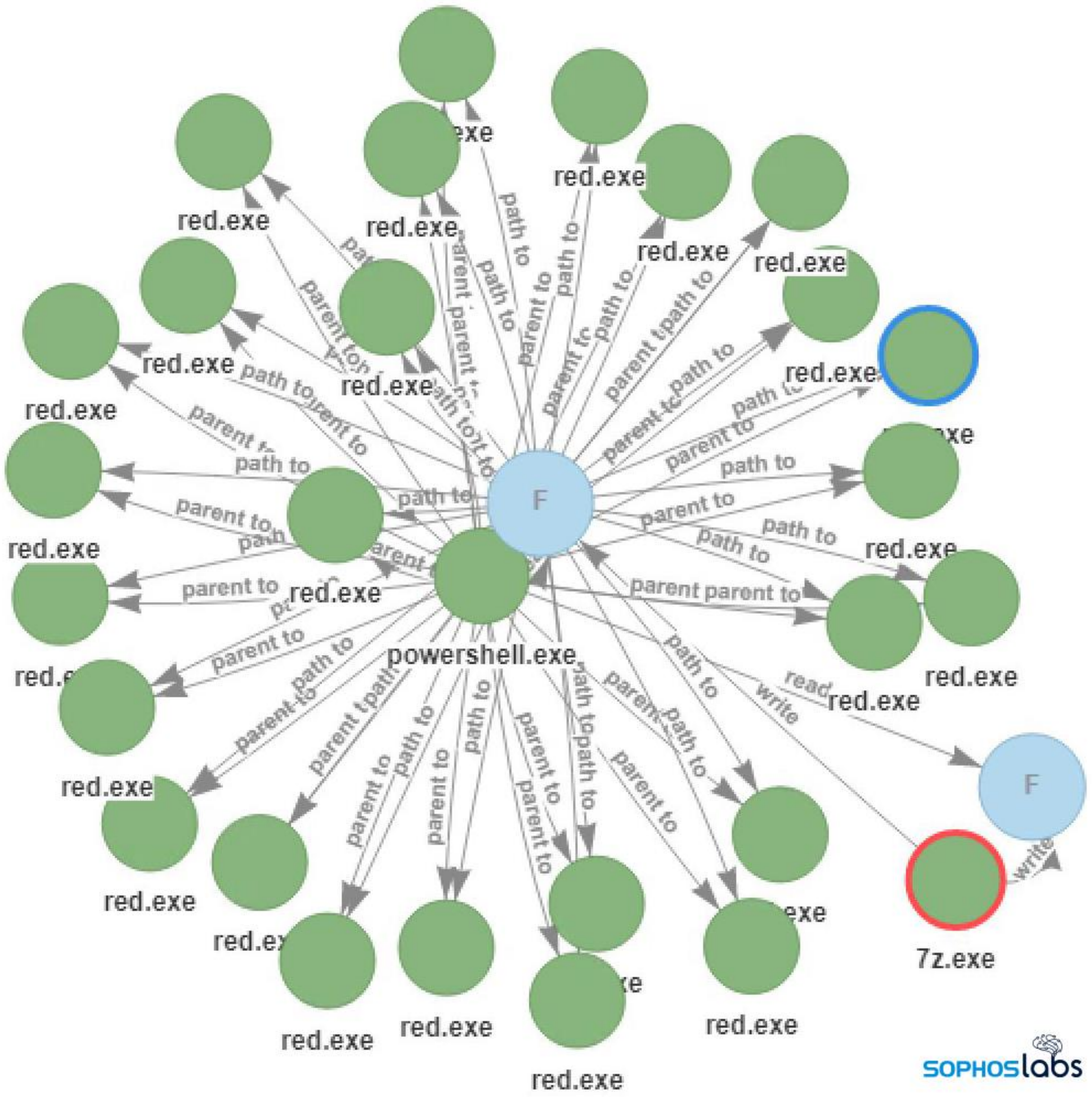
Steal the Security Account Manager (SAM) file containing password hashes

Delete Windows Event Logs

Disable Windows Defender

Suspend processes

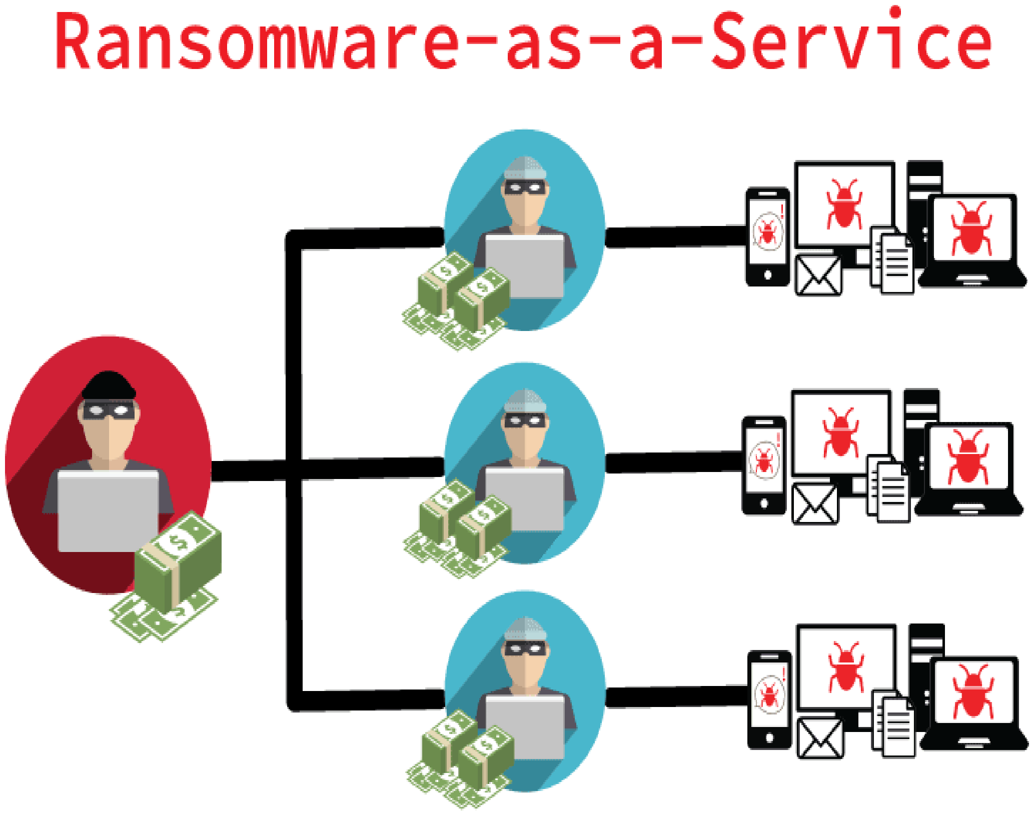
Expand permissions on the system



BAREBONES RANSOMWARE

According to Sophos, Epsilon Red is notable for the fact that most of its early-stage components are PowerShell scripts.

The ransomware component itself is a bare-bones 64-bit executable written in the Go programming language. Its only function is to encrypt files on the target system.



Ransomware as a service - RAAS

- Ransomware-as-a-Service (RaaS) borrows from the Software-as-a-Service (SaaS) model. This subscription-based malicious model enables even the novice cybercriminal to launch ransomware attacks without much difficulty.
- Example - REvil, also known as Sodinokibi, was identified as the ransomware behind one of the largest ransom demands on record: $10 million. It is sold by criminal group PINCHY SPIDER, which sells RaaS under the affiliate model and typically takes 40% of the profits.

REMEDIATION

- Restore systems or servers from backups
- Break the encryption
- Pay the Ransom?

THE DEPARTMENT OF THE TREASURY
1789

OFAC

PAYING FOR RANSOMWARE

Do you think paying for ransomware is the solution?

"Available data suggests that at least one Epsilon Red victim paid a ransom of around $210,000 in Bitcoin in mid-May."

PREVENTION – EPSILON RED

RECOMMENDED SOLUTION

- ***Install the security patch***
- Details - The following has details on how to install the security update: Patch

INTERIM MITIGATIONS

- Implement an IIS Re-Write Rule to filter malicious https requests
- Disable Unified Messaging (UM), Exchange Control Panel (ECP) Vdir and Offline Address Book (OAB) Vdir.

Ransomware Prevention

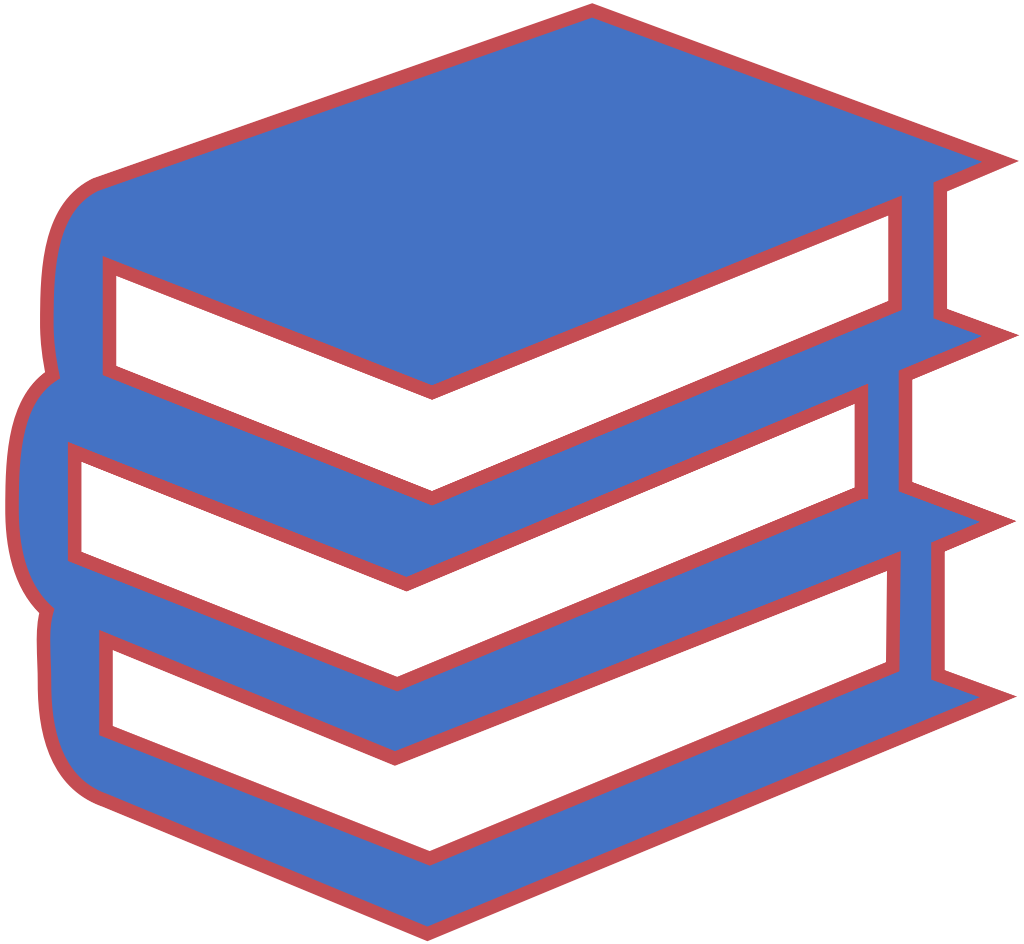
Keep your security tools up to date.

Perform regular and frequent backups. Make multiple backups and store them on separate devices in different locations.

Maintain a rigorous patch program to protect from known and unknown vulnerabilities.

Security Awareness & Skill Training

THANK YOU ANY QUESTIONS?



References

- https://cyber.gc.ca/en/alerts/active-exploitation-microsoft-exchange-vulnerabilities
- https://news.sophos.com/en-us/2021/05/28/epsilonred/
- https://logrhythm.com/blog/guide-to-detecting-microsoft-exchange-zero-day-exploits/
- https://www.marsh.com/sg/insights/risk-in-context/40-million-ransom-do-you-pay.html
- https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware
- https://news.sophos.com/en-us/2021/06/08/six-in-the-wild-exploits-patched-in-microsofts-june-security-fix-release/
- https://www.tripwire.com/state-of-security/security-data-protection/ransomware-service-raas-works/
- https://beta.darkreading.com/vulnerabilities-threats/new-barebones-ransomware-strain-surfaces