DSCI
THREAT INTELLIGENCE
AND RESEARCH INITIATIVE
THREAT ADVISORY

Special Advisory
New Malware & Variants continue to hit Businesses: **Snake Malware**

**Threat Identification – DTINRS001**

**Synopsis**

The operators of the Snake Ransomware have launched a worldwide cyberattack campaign infecting numerous businesses like Honda, Enel group.

**Infection and Propagation Vector**

The malware is written in ‘Go’ programming language and developed in a complicated way, targeting an organization’s entire corporate network. The malware is spread via email attachment Malicious ads, downloading from non-auth sources. But in the updated version, it wouldn’t encrypt files unless a DNS query to an internal domain belonging to the organization would respond, and if a user gets compromised, the files are encrypted and stored on all computers within a network using the AES-256 and RSA-2048 cryptographic algorithm.

After the process is done, a text file is left over the desktop named Fix-Your-Files.txt (Fig 1).

---

**Fig.1.** [https://www.pcrisk.com/removal-guides/16723-snake-ransomware](https://www.pcrisk.com/removal-guides/16723-snake-ransomware)
Characteristics and Symptoms:

This ransomware is capable of locking down industrial control systems and machinery in factories. It initially targets a system and then removes Shadow Volume Copies, then kills all processes related to SCADA Systems, Virtual Machines, Industrial Control Systems, Remote Management Tools, Network Management Software, and more. Then encrypting of files is done in order to get ransom in exchange for unlocking the data (Fig.2).

![Fig.2: Encryption of files](image)

Signature/ IoCs

- e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60
- 3d1cc4ef33bad0e39c757fce317ef82a

Recommendation

- Do not open suspicious and irrelevant emails, especially those received from unknown/suspect senders
- Block the installation of programs from unknown sources
- Download from relevant and trusted sources
- Do a regular backup of your data
- Use trusted scanner to detect the malware
Threat Identification – DTINRS002

Synopsis:
ElvisPresley Ransomware is a malicious program, part of the Jigsaw ransomware family. It encrypts the data of infected systems and was first discovered in June 2020.

Infection and Propagation:
This ransomware usually fools users via suspicious and irrelevant spam emails that come with attachments or links present in them. When users click on those links/files, they get infected. After the user gets infected, encryption of data takes place in order to demand payment for the decryption. Affected files are then appended with the "ElvisPresley" extension. Once the whole process is done, a ransom note is displayed (Fig.3).

If the user is unable to pay within a given time, the hacker starts deleting the files and the ransom amount gets double.

Characteristics and Symptoms
In recent updates of this ransomware, it has been observed that while targeting windows-based systems, users’ additional password-stealing Trojans and malware infections can be...
installed together with this ransomware infection. Ransomware is a malicious software designed to encrypt data and demand ransoms for the decryption tools/software. There are two significant differences between ElvisPresley ransomware and other ransomware, is of the cryptographic algorithms they use (symmetric or asymmetric) and size of the demanded sum (Fig.4).

![File Explorer](https://www.pcrisk.com/removal-guides/17986-elvispresley-ransomware)

**Signature/ IoCs**

**Cyber Criminal Crypto wallet Address**
1C1pAkwpvuxr4ZxzqHSeTLpFGQMDMJKS3U

**Cyber Criminal Contact**
zemblax@protonmail.com

**MD5**
99a11be362937bf460bbcd89a5697637

**SHA1**
32c3c0ce3f34fe195af72768b96f7585cd26ad65

**SHA256**
SSDEEP
768:aeZpcCFormLTGwoblYki8vYydqm1rphL+UpRx6KSSsH3aLfnGeznZPgtijs1rpBAiMSex

Recommendation
- Don’t download attachments or click on links received from unwanted/untrusted sources
- Keep your antivirus updated and ensure you are using the latest version
- Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity
- Do a regular backup of the data

Threat Identification – DTINRS003

Synopsis:
MAZE Ransomware is active since, at least, May 2019. The ransomware was initially distributed via spam emails and exploit kits before shifting to being deployed post-compromise. Recently, it has hit large industry player.

Infection and Propagation:
MAZE ransomware was initially distributed directly via exploit kits and spam campaigns through late 2019 in a wide range of industries where healthcare and manufacturing sectors were compromised frequently, and the user receives an email from a registrant address gladkoff1991@yandex.ru.

In the next version of the attack, attackers were sending emails using the subjects “Missed package delivery” and “Your AT&T wireless bill is ready to view” with the registrant address abusereceive@hitler.rocks.

Later, attackers made a shift in their attack vector.

1. Deploying the ransomware Post-Compromise- With this method, more hosts are infected within a victim’s environment and exfiltrate data, putting a pressure over organizations to pay the ransom.

2. Initial Compromise- With few clear patterns, this was consistent where they use MAZE soliciting partners with network access.
   - A user downloads a malicious document that contained macros which launched an IcedID payload, to execute an instance of BEACON.
   - Other users logged into an internet-facing system via RDP.
- Exploited a misconfiguration on an Internet-facing system. Enabling to deploy tools into the internal network.
- When users log in a web portal account with a weak password. This authenticated access enabled the actor to launch a Meterpreter payload on an internal system.

3. Establish Foothold & Maintain Presence- Then With the use of legitimate credentials, it helps in the establishment of a foothold, meeting the goal of deploying MAZE ransomware.
- Web shells were deployed to an internet-facing system. To grant system-level access and enable initial privilege escalation and the execution of a backdoor
- New domain account is created and added to the domain administrators group.

4. Escalate Privileges- In this, MAZE operators employ Mimikatz to collect credentials to enable privilege escalation.
- After initial access, mimi.zip malware is downloaded, having credential harvesting tool Mimikatz.
- Looks for the word “password” within the environment.
- Malware initially used ProcDump and Mimikatz to collect credentials which are used in the intrusion. Notably, both Bloodhound and PingCastle were also used to understand the organization’s Active Directory configuration. It also helps to exfiltrate collected credentials to multiple different cloud file storage services.

5. Reconnaissance- With this, the best responsible actors of the malware deal with the victim’s network.
- Execution of reconnaissance scripts via Cobalt Strike to collect network, host, filesystem, and domain-related information.
- With multiple built-in Windows commands and Advanced IP Scanner, Adfind was used to reconnaissance of the impacted environment.
- A batch script named '2.bat' is used to reconnaissance network and output is stored into a file named '2.txt'.
- Data and documents are pushed to attacker-controlled FTP server via an encoded PowerShell script.
- Over a period, Bloodhound, PowerSploit/PowerView (Invoke-ShareFinder) is used for reconnaissance.
- smbtools.exe is executed to check whether accounts can be login into systems across the environment or not.
- Finally providing the actors with data they may have used to identify sensitive data for future exfiltration

6. Lateral Movement- lateral movement was achieved via Cobalt Strike BEACON and using previously harvested credentials.
- Cobalt Strike BEACON was a key source to move across the impacted environment, though through RDP with ngrok utility, and employed tscon to hijack legitimate rdp sessions to enable both lateral movement and privilege escalation.
- With crawling in networks compromised user accounts were obtained on which they gained their initial foothold which helps them to obtain immediate access to additional systems.
- Stolen credentials helped in rendering the network via RDP and to install BEACON payloads providing the actors with access to nearly one hundred hosts.
- Using Metasploit and local administrator account, Cobalt Strike payload was deployed to the systems
- Used EternalBlue in early and late 2019, but they were not successful.

7. Final stage - A threat actor has been observed exfiltrating data to FTP servers using a base64-encoded PowerShell script designed to upload any files with .7z file extensions to a predefined FTP server using a hard-coded username and password, also used the utility WinSCP to exfiltrate data to an attacker-controlled FTP server. It has even employed a file replication utility and copying the stolen data to a cloud file hosting/sharing service. In addition to data theft, actors also deploy MAZE ransomware to encrypt files identified on the victim network.

Characteristics and Symptoms
Maze ransomware utilizes RSA and ChaCha20 encryption and appends different extensions to the files.

Actors will release victim data if a ransom is not paid.

Signature/ IOCs

064058cf092063a5b69ed8fd2a1a04fe
0f841c6332c89ea7cac14c9d5b1d35b
108a298b4ed5b4e77541061f32e55751
11308e450b1f17954f531122a56fae3b
15d7dd126391b0e7963c562a6cf3992c
21a563f958b73d453ad91e251b11855c
27c5ecbb94b84c315d56673a851b6cf9
2f78ff32cbb3c478865a88276248d419
335aba8d135cc2e66549080ec9e8c8b7
3bfca2dd05e1c75f86c008f4d245f62
Check-in IP's 91.218.114.11

91.218.114.11
91.218.114.25
91.218.114.26
91.218.114.31
91.218.114.32
91.218.114.37
91.218.114.38
91.218.114.4
91.218.114.77
91.218.114.79
92.63.11.151
92.63.15.6
92.63.15.8
92.63.17.245
92.63.194.20
92.63.194.3
92.63.29.137
92.63.32.2  
92.63.32.52  
92.63.32.55  
92.63.32.57  
92.63.37.100  

**Recommendation:**

- Back up your most important files on a regular basis  
- Personalize your anti-spam settings  
- Patch, keep your software and system up-to-date  
- Always keep the Windows Firewall turned on and properly configured  
- Disable Windows Script Host  
- Disable Windows PowerShell, which is a task automation framework  
- Disable macros and ActiveX  
- Use strong passwords that cannot be brute forced  
- Block known-malicious IP addresses  
- Use proper antivirus so that the unwanted execution doesn’t take place  
- Do not click on suspicious links  
- Provide awareness about these kinds of threats to the user  

**Threat Identification – DTINRS004**

**Synopsis:**

**DemonWare Ransomware:** The motive of this ransomware is to encrypt the user data and ask for the ransom in exchange for the data. This is widely spread via malicious attachments, emails, unauthorized downloads, cracked software, etc.

**Infection and Propagation:**  
During the encryption process, DemonWare appends all of the affected files with the ".DEMON" extension. For example, it modifies "one.jpg" to "one.jpg.DEMON." It shows a ransom note in a pop-up window and creates another one in a text file README.txt (Fig.5).
Characteristics and Symptoms
If you cannot access files stored on the computer, an extension of the files is changed, and ransom demand message is displayed on your desktop. Cyber criminals demand payment of a ransom (usually in bitcoins) to unlock your files. (Fig.6).

Signature/ IOCs

MD5
2f8eee0d39dc0be5c5cd970e0fa33f52

SHA1
e8a9cf2dae297aa9014f9f3708621f93aed62f11

SHA256
809f8e79150028559f6ac924a27581a07ec6348a3913370442c29be2af634411

SSDEEP
196608: mwqYgMicrGyDLlXzhneX38DXDQ9/tbYPvbJQlHz2rBO2SvJy8CQQ+xzzRSQy:L qY5icrGyAlh0MDTQ9/kJQIC95kI

Recommendation

● Do not open suspicious emails
● Use spam filters and an antivirus program to detect and filter malicious emails
● Enable an endpoint security product or endpoint protection suite
● Keep your software up-to-date
● Back up data on a regular basis and keep archived copies offsite