**Hive Ransomware – More than a Ransomware**

Report by – Harsh Sharma

Before starting the report let us get started with some terminologies being used in the report.

1. Ransomware – A malicious software or service when injected to a device locks the system and encrypts the data using certain cryptography techniques. Hackers use these types of acts to breakdown the organizations economy and reputation.
2. Cryptography – Conversion of an information into some unreadable bytes using some cryptographic form like Sha256, Sha1 or MD5.
3. RaaS - RaaS (Ransomware-as-a-Service) is a business model whereby malware developers lease out ransomware and its control infrastructure to other cybercriminals. RaaS is a variation of the MaaS (Malware-as-a-Service) model, which in turn is a malicious variant of the SaaS (Software-as-a-Service) mode.
4. Double-Extortion – Exfiltration or making a copy of data in addition to encrypting it refers to Double-Extortion. This technique makes organization more feared to pay the ransom and loss/leak of data.
5. Restoration Period – It is the period which is given by the threat actors to the organization to respond to the demands of the hackers. So that the organization can get restored from the situation.

**Introduction to Hive Ransomware**

Hive ransomware was made by group of threat actors called “Hive” residing in Russia. it provides Ransomware-as-a-Service Hive and adopts a double-extortion model threatening to publish data stolen from the victims on their leak site (HiveLeaks). Hive Ransomware got popular in no time i.e., it has exploited over 355 companies in the tenure of just 6 months which makes it one of the most dangerous and fast-growing ransomware in the world of internet.

Hive was coming into light in June 2021, where it is only used in windows and later it was discovered in Linux and Mac Os.

Written in Go and use of rust in data encryption which makes encryption faster.

A real-time screenshot of Hive ransomware in wild is attached here:



**Working of Hive Ransomware (TTP’s)**

Step1: Proxy Shell and Web Shell

The threat actors exploited the vulnerabilities of Exchange Security known as Proxy Shell. Then the attacked placed a malicious backdoor referred to as web shell. These web scripts could then execute malicious Power Shell code over the compromised server with system privileges.

Step 2: Cobalt Strike

After the exploitation, Command and Control were made by Cobalt Strike Framework.

Step 3: Mimikatz and Pass-the-hash

It was used to gain privilege escalation; threat actors created a new system administrator account user and gets to credential dumping stage calling Mimikatz.

Step 4: Scanning for Sensitive Information

In this step threat actors look for more juicy data such as usernames with passwords, names with passwords, collection of ip address’s,

Step 5: Ransomware Deployment

A payload named as “windows.exe” was injected in the various devices making the data encrypted and denial of access within the organization.

**Mitre TTPS of the Hive Ransomware Attack**

1. Gaining Access

Exploit Public-Facing Application ([T1190](https://attack.mitre.org/techniques/T1190/))

[CVE-2021-34473](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34473)

[CVE-2021-34523](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34523)

[CVE-2021-31207](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31207)

1. Execution

User Execution ([T1204](https://attack.mitre.org/techniques/T1204/))

Malicious File ([T1204.002](https://attack.mitre.org/techniques/T1204/002/))

Command and Scripting Interpreter ([T1059](https://attack.mitre.org/techniques/T1059/))

PowerShell ([T1059.001](https://attack.mitre.org/techniques/T1059/001/))

1. Persistence

Create Account([T1136](https://attack.mitre.org/techniques/T1136/))

Domain Account([T1136.002](https://attack.mitre.org/techniques/T1136/002/))

Command and Scripting Interpreter([T1059](https://attack.mitre.org/techniques/T1059/))

PowerShell ([T1059.001](https://attack.mitre.org/techniques/T1059/001/))

1. Privilege Escalation

* Valid Accounts ([T1078](https://attack.mitre.org/techniques/T1078/002/))
* Domain Accounts ([T1078.002](https://attack.mitre.org/techniques/T1078/002/))

1. Defense Evasion

* Deobfuscate/Decode Files or Information ([T1140](https://attack.mitre.org/techniques/T1140/))
* Indicator Removal on Host ([T1070](https://attack.mitre.org/techniques/T1070/))
* Clear Windows Event Logs ([T1070.001](https://attack.mitre.org/techniques/T1070/001/))

1. Credential Access

* OS Credential Dumping ([T1003](https://attack.mitre.org/techniques/T1003/))
* Cached Domain Credentials ([T1003.005](https://attack.mitre.org/techniques/T1003/005/))

1. Discovery

* Remote System Discovery ([T1018](https://attack.mitre.org/techniques/T1018/))

1. Lateral Movement

* Remote Services ([T1021](https://attack.mitre.org/techniques/T1021/001/))
* Remote Desktop Protocol ([T1021.001](https://attack.mitre.org/techniques/T1021/001/))

1. Command and Control

Application Layer Protocol ([T1071](https://attack.mitre.org/techniques/T1071/))

Web Protocols ([T1071.001](https://attack.mitre.org/techniques/T1071/001/))

10. Impact

Data Encrypted for Impact ([T1486](https://attack.mitre.org/techniques/T1486/))