THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Hive

Threat Actor Criminal

CATEGORY

Criminal

SEVERITY

High

Platforms

Windows

IMPACT

- Unauthorized Access to Information
- Extraction of Confidential Data
- Disclosure of Critical Details

Description

HIVE

Hive is a ransomware group actively targeting critical sectors such as healthcare and financial institutions, with operations currently observed in Pakistan. The group uses a Ransomware-as-a-Service (RaaS) model, enabling affiliates to deploy ransomware in exchange for profit shares. Hive employs a double extortion strategy, encrypting data and threatening to leak stolen information if the ransom is not paid. It has also been exploiting multiple vulnerabilities, including **CVE-2020-12812**, **CVE-2022-3236**, **CVE-2020-1472**, **CVE-2023-3519**, **CVE-2018-0798**, **CVE-2018-13379**, **CVE-2022-26134**, **CVE-2022-41040**, **CVE-2022-30190**, **CVE-2023-40044**, **CVE-2022-41080**, and **CVE-2022-41082**, to gain initial access to victim networks. Indicators of Hive's attacks include unusual network activity, unauthorized file encryption, and data exfiltration, making it a significant threat to organizations with inadequate security measures.

In recent campaigns, Hive has focused on exploiting zero-day vulnerabilities and targeting supply chains to maximize disruption. Notable incidents include attacks leveraging these CVEs in healthcare and financial sectors, leading to substantial ransom demands. Drawing comparisons to groups like Conti and REvil, Hive continues to evolve its tactics, emphasizing the urgent need for robust cybersecurity defenses, timely patch management, and proactive monitoring to prevent potential breaches.

Kill Chain

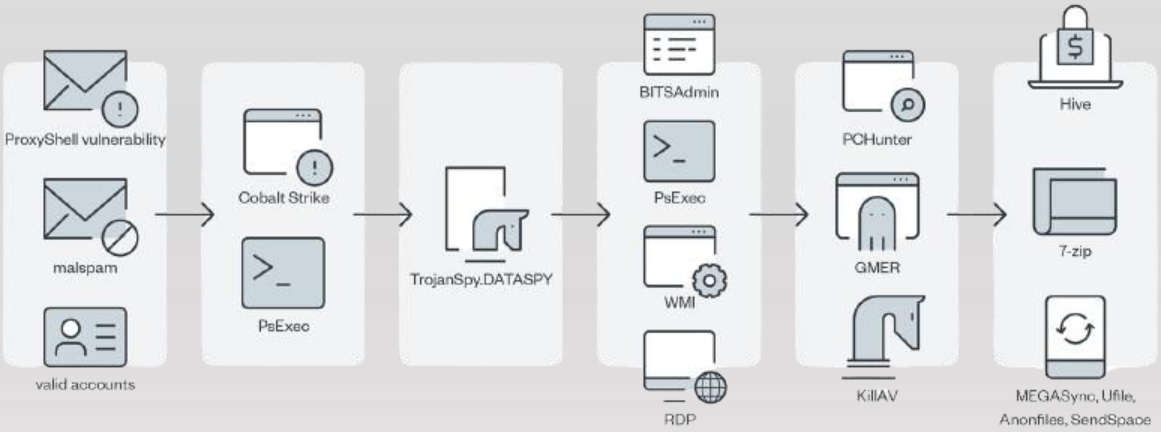

Figure 1 Kill Chain

Indicator of Compromise

SHA256

1dab85cf02cf61de30fcda209c8daf15651d649f32996fb9293b71d2f9db46e1
97c9caaaf7d3861e30d9ff647e952e880b670c5c3dca4537c515b38438ee18ee
18a72a5f52e9da32098cb60b38a3b07e311428bb379f1f6d438031337f855d95
b25b87cfcedc69e27570afa1f4b1ca85aab07fd416c5d0228f1fe32886e0a9a6
c4d39db132b92514085fe269db90511484b7abe4620286f6b0a30aa475f64c3e
94b6cf6c30f525614672a94b8b9788b46cbe061f89ccbb994507406404e027af

Indicator of Compromise

MD5

```
5795b4bc71f6bb9d40f5250443086e5d
29040db8da4799d5ce8e539be9d26ef0
7b33a1c3deb68cfc25352c8a115dc36d
181aa5e09dbfc1c202a0732a0acbf077
46fc4776db5e40ee5e0341746ddd3443
53a91e0aa7be826797fe4f3095198fd4
```

Remediation

- Establish an effective patch management system to quickly address and resolve identified vulnerabilities.
- Strengthen network defenses by configuring robust firewall rules and deploying intrusion detection systems to identify and prevent unauthorized activities.
- Frequently back up essential data, storing backups securely offline or in a protected cloud environment.
- Provide ongoing security awareness training for staff to keep them informed about emerging threats and strategies to safeguard sensitive data.

ThreatCure

Cyber Threat Advisory

Secure your byte world

HIVE

Threat Actor Criminal

Get Started Today

For more information about the ThreatCure ShieldOps Platform or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net