LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Hive Ransomware

10/21/2021

TLP: WHITE, ID# 202110211300

Agenda

- Hive Ransomware Overview
- Legitimate Applications and Closed Source Code
- Hive Ransomware Attacks
- Hive Ransomware Activity Targeting the U.S. HPH
- Hive Tactics, Techniques, and Procedures (TTPs)
- Mitigations

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Hive Ransomware Overview

- First observed in June 2021
- According to the Federal Bureau of Investigation (FBI), it “likely operates as an affiliate-based ransomware”
- Double extortion ransomware
- Human-operated attacks
- Uses legitimate commercial applications
- Utilizes their own closed-source ransomware (complied for both 32-bit and 64-bit machines)
- Possible Russian-speaking actors

Additional information can be found in the August 25, 2021 FBI report, *TLP: WHITE Flash Alert (MU-000150-MW) Indicators of Compromise Associated with Hive Ransomware*

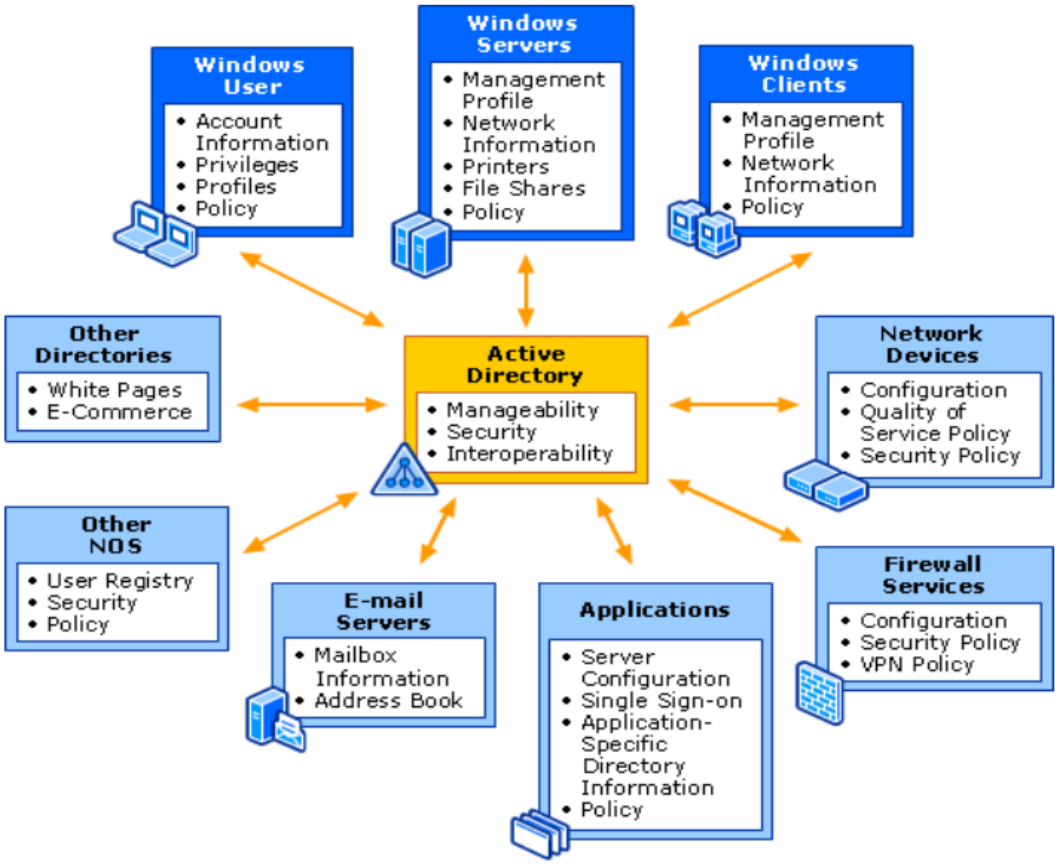
Legitimate Applications and Closed Source Code

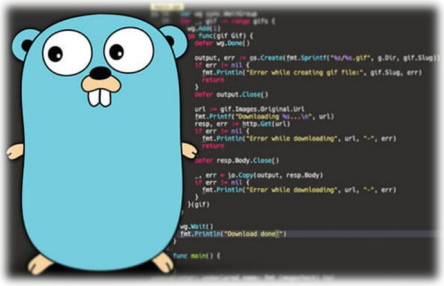
Legitimate Commercial Applications Used by Hive

- Cobalt Strike
- ConnectWise
- ADrecon

Closed Source Code Hive Ransomware

- Written in Go programming language
- Compiled in UPX
- Windows specific





ConnectWise®

Hive Ransomware Attacks

Initial Access

- Phishing Emails
- Remote Desktop Protocols

First Hive Actions

```
Windowssystem32cmd.exe /C rundll32.exe
WindowsSystem32comsvcs.dll MinDump 752 lsass.dmp full
```

- Attempts to dump credentials

- Cache cleartext credential data

- ADrecon (legitimate commercial software) used to “map, traverse, and enumerate” the Active Directory (AD) environment

```
Windowssystem32cmd.exe /C reg add
HKLMSYSTEMCurrentControlSetControlSecurityProvidersWDigest /v
UseLogonCredential /t REG_DWORD /d 1 && gpupdate /force
```

Hive Ransomware Attacks – 2

Hive Payload Executes

- Terminates:
  - Computer backup and restore
  - Antivirus and antispyware
  - File copying

```
"bmr|sql|oracle|postgres|redis|vss|backup|sstp"
```

- Identifies and stops the following services:
  - Database (sql, oracle, postgres, redis)
  - Backup (bmr, vss)
  - Protocol (sstp)

hive.bat

```
1  :Repeat
2  timeout 1 || sleep 1
3  del "C:\Users\Analyst\Desktop\hive\hive.exe"
4  if exist "C:\Users\Analyst\Desktop\hive\hive.exe" goto Repeat
5  del "hive.bat"
6
```

- Processes are terminated:
  - mspub and msdesktop

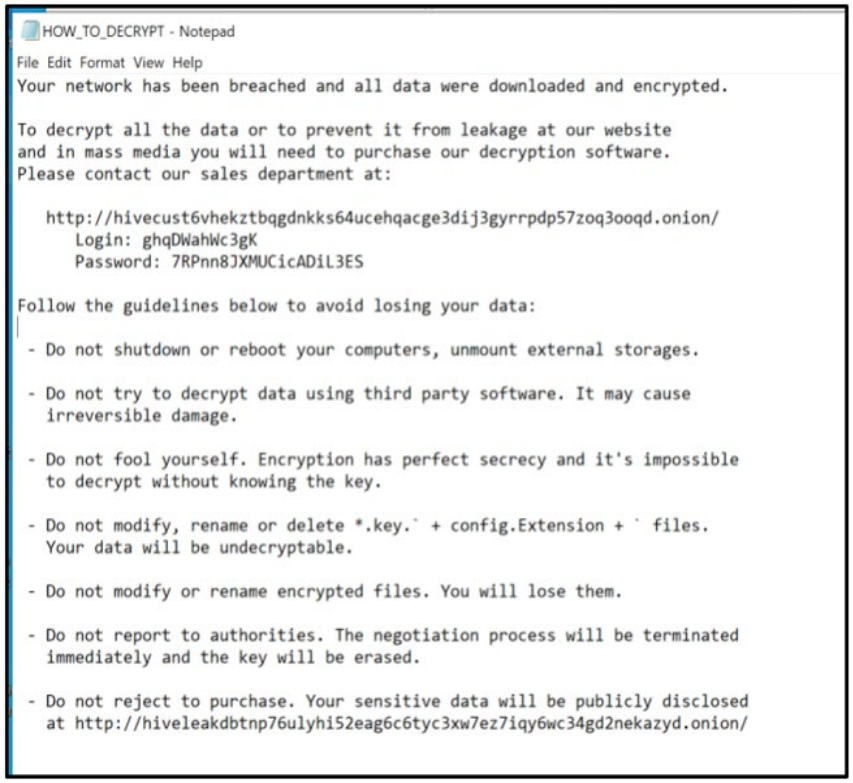
- "hive.bat" and "shadow.bat" → Encryption Process Begins
  - Excluding the C:\Windows" drive

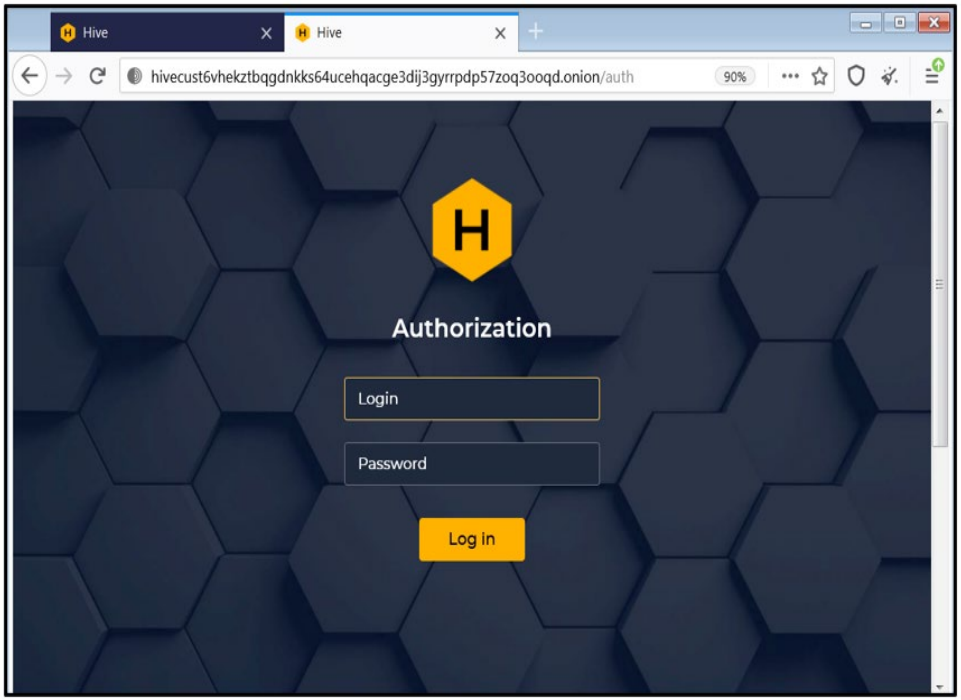
```
vssadmin.exe delete shadows /all /quiet

del shadow.bat
```

Hive Ransomware Attacks – 3

Hive Portal

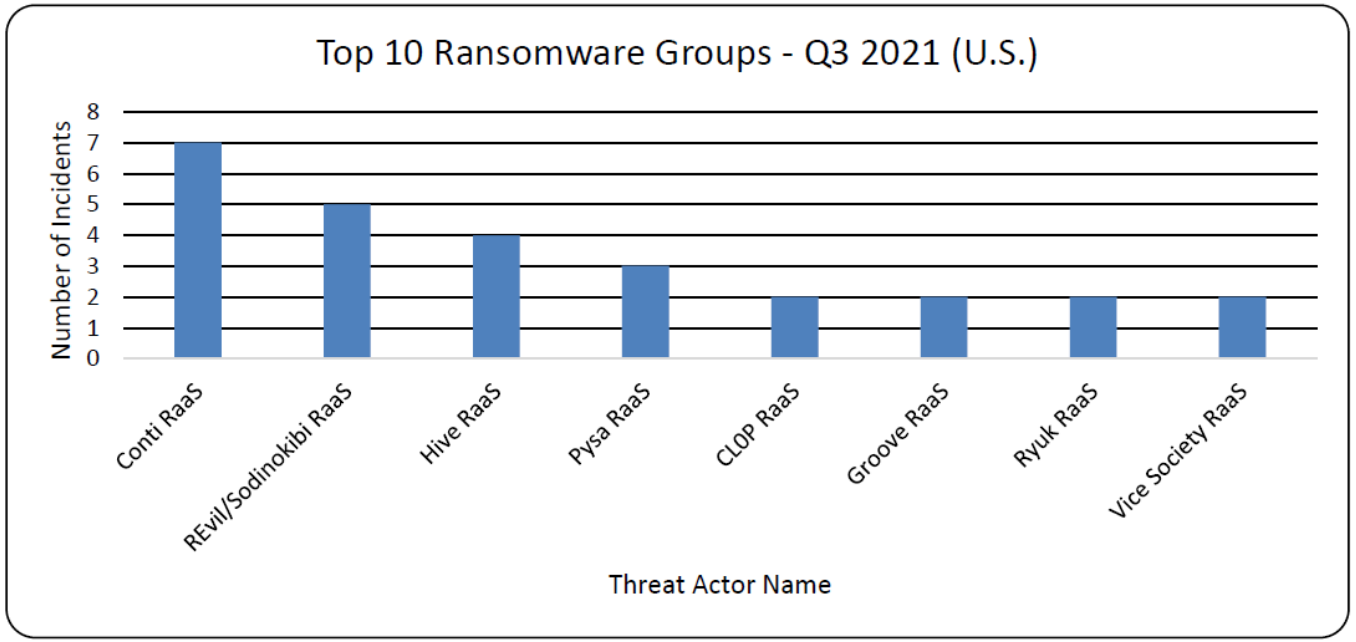
- Ransom note
- Unique credentials given to victim
- 2–6 days for payment; if not, data is leaked to HiveLeaks





Hive Ransomware Activity Targeting the U.S. HPH

HC3 Tracked Hive Ransomware Attacks on U.S. HPH Sector Since June 2021	
Approximate Date of Attack Identification	**Sub-Industry Targeted**
03AUG21	Healthcare Industry Services
15AUG21	Hospital
25AUG21	Healthcare Industry Services
29AUG21	Health or Medical Clinic
02OCT21	Hospital



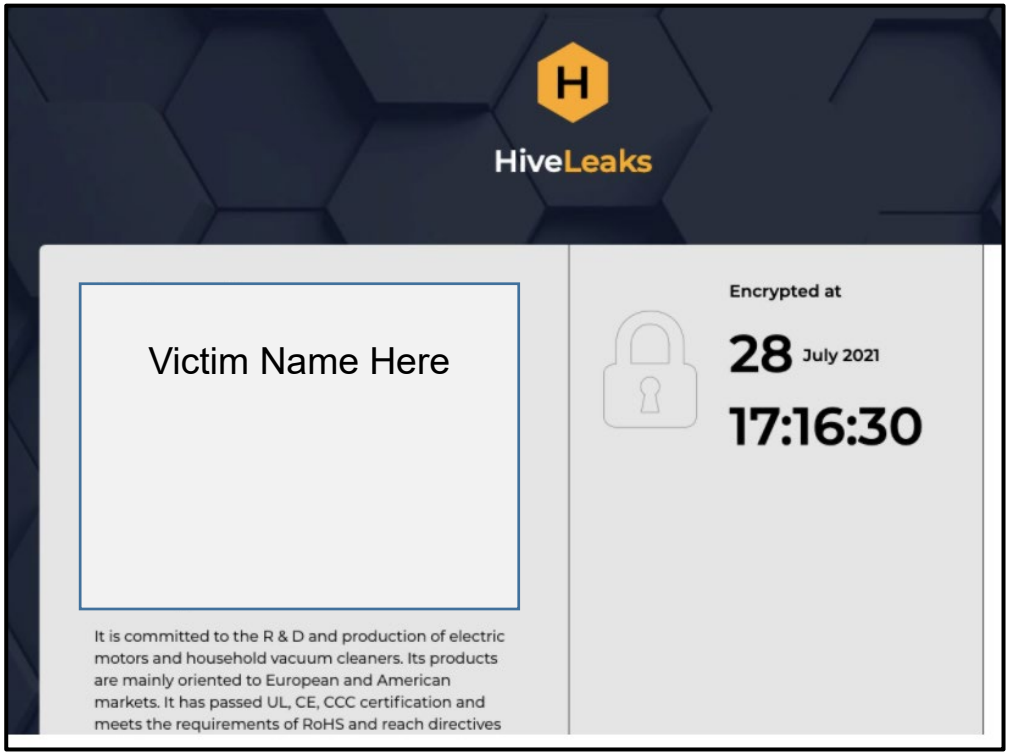
Hive Ransomware Activity Targeting the U.S. HPH (cont.)

Results of the attacks for patient services

- Canceled surgeries, diversion of ambulances, and closed urgent care units

Information Stolen

- 62–400 GB of information/data related to:
  - Medical records/care
  - Financial documents
  - Proprietary company work
  - Insurance forms, court documents
  - General work product, passwords
  - Employees' PII
  - Confidential clients' names



Hive Tactics, Techniques, and Procedures (TTPs)

Hive MITRE ATT&CK TTPs	
Technique ID	Technique
T1574.001	Hijack Execution Flow: DLL Search Order Hijacking
TA0005	Defense Evasion
TA0004	Privilege Escalation
T1486	Data Encrypted for Impact
T1027.002	Obfuscated Files or Information: Software Packing
T1003.001	OS Credential Dumping: LSASS Memory
T1007	System Service Discovery
T1059	Command and Scripting Interpreter
T1059.001	Command and Scripting Interpreter: PowerShell
T1059.003	Command and Scripting Interpreter: Windows Command Shell
T1490	Inhibit System Recovery

Mitigations/Detections

General efforts to help prevent ransomware attacks include:

- Maintain offline, encrypted backups of data and regularly test your backups.
- Create, maintain, and exercise a basic cyber incident response plan, resiliency plan, and associated communications plan.
- Mitigate internet-facing vulnerabilities and misconfigurations.
- Reduce the risk of phishing emails from reaching end users.
- Practice good cyber hygiene.

CISA ransomware tips:
https://www.cisa.gov/sites/default/files/publications/CISA_Fact_SheetProtecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf

Specific Mitigations/Detections for Hive Ransomware

- Remove applications not deemed necessary for day-to-day operations
- Abnormal termination of the bmr, sql, oracle, postgres, redis, vss, backup, and sst services
- Abnormal termination of the mspub and msdesktop processes
- Log monitoring

Reference Materials

References

Federal Bureau of Investigation. “Flash Alert (MU-000150-MW) Indicators of Compromise Associated with Hive Ransomware,” Internet Crime Complaint Center. 25 August 2021. https://www.ic3.gov/Media/News/2021/210825.pdf

Vaidya, Anuja. “Hive is a new & potentially devastating type of ransomware. Here’s what you need to know.,” MedCityNews. 16 September 2021. https://medcitynews.com/2021/09/hive-is-a-new-potentially-devastating-type-of-ransomware-heres-what-you-need-to-know/

Walter, Jim. “Hive Attacks | Analysis of the Human-Operated Ransomware Targeting Healthcare,” Sentinel Labs. 23 Augsust 2021. https://www.sentinelone.com/labs/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-healthcare/

The BlackBerry Research & Intelligence Team. “Threat Thursday: Bee-ware of Hive Ransomware,” BlackBerry. 22 July 2021. https://blogs.blackberry.com/en/2021/07/threat-thursday-hive-ransomware

Kim, Christopher. “Hive Ransomware,” InfoBlox. 30 August 2021. https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/hive-ransomware/

Health Sector Cybersecurity Coordination Center. “Health Sector Ransomware Trends for Third Quarter 2021,” HealthCare Intelligence. 13 October 2021. https://www.intelligence.healthcare/index.php?option=com_phocadownload&view=category&download=282:hc3-analyst-note-health-sector-ransomware-trends-for-2021-q3&id=8:hccic-e-briefs&Itemid=1220&start=220

McKeon, Jill. "Hive Ransomware Continues to Attack Healthcare Providers," Health Security. 23 September 2021. https://healthitsecurity.com/news/hive-ransomware-continues-to-attack-healthcare-providers

Vaas, Lisa. "Cobalt Strike Usage Explodes Among Cybercrooks," ThreatPost. 29 June 2021. https://threatpost.com/cobalt-strike-cybercrooks/167368/

Questions

Upcoming Briefs

- 11/4 – Cobalt Strike vs the Health Sector

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV**.

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback, please complete the HC3 Customer Feedback Survey.

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or visit us at www.HHS.Gov/HC3.

Contact

www.HHS.GOV/HC3

HC3@HHS.GOV