HC3: Analyst Note

April 18, 2022 TLP: White Report: 202204181300

Hive Ransomware

Executive Summary

Hive is an exceptionally aggressive, financially-motivated ransomware group known to maintain sophisticated capabilities who have historically targeted healthcare organizations frequently. HC3 recommends the Healthcare and Public Health (HPH) Sector be aware of their operations and apply appropriate cybersecurity principles and practices found in this document in defending their infrastructure and data against compromise.

Report

The Hive ransomware group has been known to be operational since June of 2021 but in that time has been very aggressive in targeting the US health sector. One report covering the third quarter of 2021 – just months after they began operating – ranks them as the fourth most active ransomware operators in the cybercriminal ecosystem (see figure 1). Another report noted the observation of 355 companies in Hive's first 100 days of operation.

Their operations include the following features:

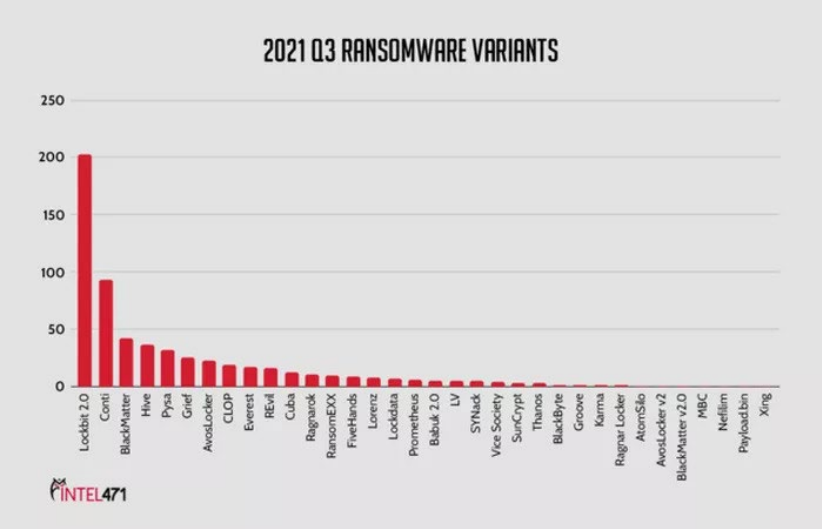

Figure 1: Hive Ransomware activity from Q3 of 2021 (source: Intel471)

- They conduct double extortion (data theft prior to encryption) and support this with their data leak site which is accessible on the dark web
- They operate via the ransomware as a service (RaaS) model, which involves them focusing on development and operations of the ransomware and other partners/affiliates to obtain initial access to the victim infrastructure and
- They leverage Golang, a language used by many cybercriminals to design their malware. They also ported their Linux VMware ESXi encryptor to Rust, making it more challenging for security researchers to analyze their operations.
- They leverage common (but effective) infection vectors such as RDP and VPN compromise as well as phishing
- Their encrypted files end with a .hive, .key.hive or .key extension
- Some victims have received phone calls from Hive to pressure them to pay and conduct negotiations
- Like some other ransomware variants, Hive searches victim systems for applications and processes which backup data and terminates or disrupts them. This includes deleting shadow copies, backup files, and system snapshots.

- Hive has replicated a number of features and practices of the Black Cat operators such as:
  - Hive removed Tor negotiation URLs from their encryptor to prevent security researchers from extracting the ransom note and listening in on negotiations, something which is known to have happened to other ransomware operators in the past.
- Hive extended their possible targets to Linux and FreeBSD systems by further developing their encryption algorithms
- They developed a new IPv4 obfuscation technique, called IPfuscation, which makes them more stealthy

Analyst Comment

Much of Hive's operations are standard practice amongst ransomware operators. They follow many of the typical practices including infection vectors, ransom note (see figure 2 for a sample), data exfiltration and double extortion and maintaining a name-and-shame dark web site. However, they also have a set of unique capabilities which make them especially noteworthy. As the FBI has noted, the Hive group, "employs a wide variety of tactics, techniques, and procedures (TTPs), creating significant challenges for defense and mitigation."

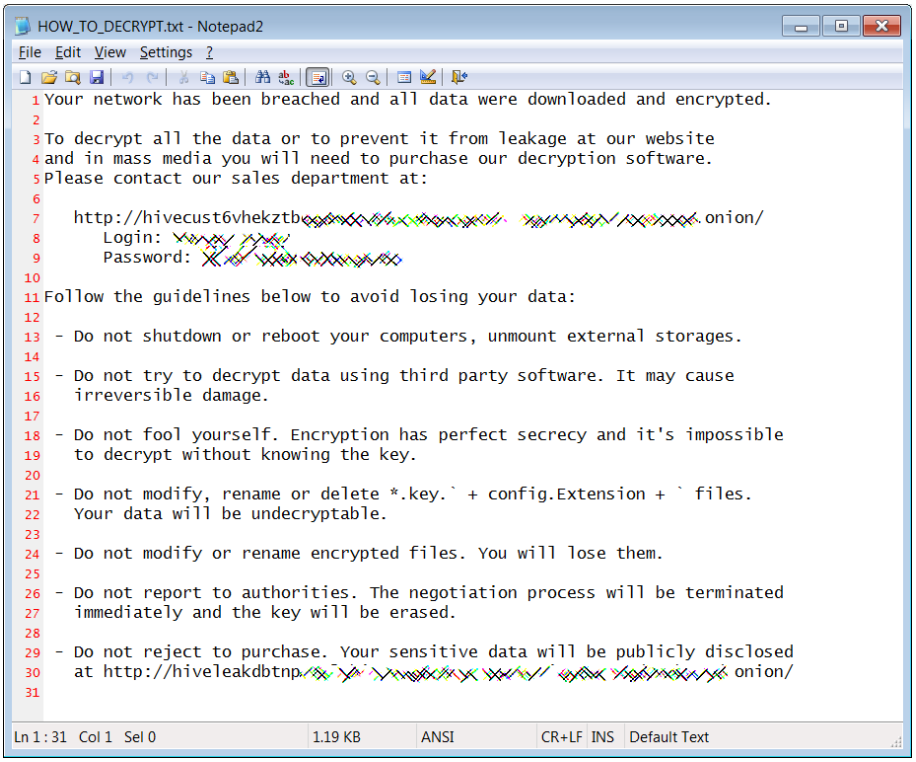

Figure 2: Hive ransom note (source: Bleeping Computer)

When defending against Hive or any other ransomware variant, there are standard practices that should be followed. Prevention is always the optimal approach. This includes but is not limited to the following:

- Use two-factor authentication with strong passwords – this is especially applicable for remote access services such as RDP and VPNs.
- Sufficiently backing up data, especially the most critical, sensitive and operationally necessary data is very important. We recommend the 3-2-1 Rule for the most important data: Back this data up in three different locations, on at least two different forms of media, with one of them stored offline.
- Continuous monitoring is critical, and should be supported by a constant input of threat data (open source and possibly proprietary as well)

- An active vulnerability management program must be comprehensive in scope and timely in implementation of the latest software updates. It should apply to traditional information technology infrastructure as well as any medical devices or equipment that is network-connected.
- Endpoint security should be comprehensive in scope and updated with the latest signatures/updates aggressively.

Detection during an attack can help contain/minimize its impact. Yara rules exist here and below in Appendix A. Indicators of Compromise exist in the FBI Flash Alert on Hive. Furthermore, researchers have identified a method for recovering the private key for decryption in order to avoid paying the ransom. It's worth noting, however, that Hive likely made adjustments as they continue to aggressively attack and continue to be one of the most active ransomware groups in the cybercriminal ecosystem.

We also recommend healthcare organizations thoroughly review the following resources:
DHS/CISA Stop Ransomware: https://www.cisa.gov/stopransomware
FBI Cybercrime: https://www.fbi.gov/investigate/cyber
FBI Ransomware: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware
FBI Internet Crime Complaint Center (IC3): https://www.ic3.gov/Home/ComplaintChoice/default.aspx/
HC3 Products: https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html

References

Hive ransomware enters big league with hundreds breached in four months
https://www.bleepingcomputer.com/news/security/hive-ransomware-enters-big-league-with-hundreds-breached-in-four-months/

A reset on ransomware: Dominant variants differ from prior years
https://intel471.com/blog/ransomware-attacks-2021-lockbit-hive-conti-clop-revil-blackmatter

Why Hive Attacks Are the Latest Menace to Healthcare Sector
https://www.govinfosecurity.com/interviews/hive-attacks-are-latest-menace-to-healthcare-sector-i-4977

Hive Attacks | Analysis of the Human-Operated Ransomware Targeting Healthcare

"THEY [HIVE] WILL RELEASE THAT SENSITIVE INFORMATION - PATIENT RECORDS, HIPAA DATA - PUBLICLY IN ORDER TO MAKE IT VERY PAINFUL FOR THE VICTIM."
Adam Meyers, Vice President of Intelligence, CrowdStrike

https://www.sentinelone.com/labs/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-

healthcare/

Infoblox Cyber Threat Advisory: Hive Ransomware
https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/hive-ransomware/

FBI Flash: Alert Number MC-000150-MW - Indicators of Compromise Associated with Hive Ransomware
https://www.ic3.gov/Media/News/2021/210825.pdf

Inside the Hive
https://blog.group-ib.com/hive

ESET Research (Twitter): #ESETresearch has identified Linux and FreeBSD variants of the #Hive #Ransomware. Just like the Windows version, these variants are written in #Golang, but the strings, package names and function names have been obfuscated, likely with gobfuscate.
https://twitter.com/ESETresearch/status/1454100591261667329

APPENDIX A: Yara Rules

The below two rules will help detect Hive variants (source: Malpedia)

---

win_hive_auto (20220411 | Detects win.hive.)

```
rule win_hive_auto {

   meta:
      author = "Felix Bilstein - yara-signator at cocacoding dot com"
      date = "2022-04-08"
      version = "1"
      description = "Detects win.hive."
      info = "autogenerated rule brought to you by yara-signator"
      tool = "yara-signator v0.6.0"
      signator_config = "callsandjumps;datarefs;binvalue"
      malpedia_reference = "https://malpedia.caad.fkie.fraunhofer.de/details/win.hive"
      malpedia_rule_date = "20220405"
      malpedia_hash = "ecd38294bd47d5589be5cd5490dc8bb4804afc2a"
      malpedia_version = "20220411"
      malpedia_license = "CC BY-SA 4.0"
      malpedia_sharing = "TLP:WHITE"

   /* DISCLAIMER
    * The strings used in this rule have been automatically selected from the
    * disassembly of memory dumps and unpacked files, using YARA-Signator.
    * The code and documentation is published here:
```

```
 * https://github.com/fxb-cocacoding/yara-signator
 * As Malpedia is used as data source, please note that for a given
 * number of families, only single samples are documented.
 * This likely impacts the degree of generalization these rules will offer.
 * Take the described generation method also into consideration when you
 * apply the rules in your use cases and assign them confidence levels.
 */


strings:
   $sequence_0 = { 31c0 31c9 31d2 bb06000000 }
      // n = 4, score = 300
      //   31c0               | xor             eax, eax
      //   31c9               | xor             ecx, ecx
      //   31d2               | xor             edx, edx
      //   bb06000000         | mov             ebx, 6

   $sequence_1 = { 31c0 b9e4000000 31d2 31db }
      // n = 4, score = 300
      //   31c0               | xor             eax, eax
      //   b9e4000000         | mov             ecx, 0xe4
      //   31d2               | xor             edx, edx
      //   31db               | xor             ebx, ebx

   $sequence_2 = { b807000000 b9d4000000 31d2 31db }
      // n = 4, score = 300
      //   b807000000         | mov             eax, 7
      //   b9d4000000         | mov             ecx, 0xd4
      //   31d2               | xor             edx, edx
      //   31db               | xor             ebx, ebx

   $sequence_3 = { b804000000 b9df000000 31d2 31db }
      // n = 4, score = 300
      //   b804000000         | mov             eax, 4
      //   b9df000000         | mov             ecx, 0xdf
      //   31d2               | xor             edx, edx
      //   31db               | xor             ebx, ebx

   $sequence_4 = { 83c440 c3 e8???????? 90 }
      // n = 4, score = 200
      //   83c440             | add             esp, 0x40
      //   c3                 | ret
      //   e8????????         |
      //   90                 | nop
```

```
$sequence_5 = { b803000000 b9b6000000 31d2 31db }
   // n = 4, score = 200
   //   b803000000         | mov             eax, 3
   //   b9b6000000         | mov             ecx, 0xb6
   //   31d2               | xor             edx, edx
   //   31db               | xor             ebx, ebx

$sequence_6 = { 83c420 c3 b905000000 e8???????? }
   // n = 4, score = 200
   //   83c420             | add             esp, 0x20
   //   c3                 | ret
   //   b905000000         | mov             ecx, 5
   //   e8????????         |

$sequence_7 = { b809000000 b90b000000 31d2 31db }
   // n = 4, score = 200
   //   b809000000         | mov             eax, 9
   //   b90b000000         | mov             ecx, 0xb
   //   31d2               | xor             edx, edx
   //   31db               | xor             ebx, ebx

$sequence_8 = { b805000000 b924000000 31d2 31db }
   // n = 4, score = 200
   //   b805000000         | mov             eax, 5
   //   b924000000         | mov             ecx, 0x24
   //   31d2               | xor             edx, edx
   //   31db               | xor             ebx, ebx

$sequence_9 = { 39b100000000 750a e8???????? e8???????? }
   // n = 4, score = 200
   //   39b100000000       | cmp             dword ptr [ecx], esi
   //   750a               | jne             0xc
   //   e8????????         |
   //   e8????????         |

$sequence_10 = { b801000000 b9ca000000 31d2 31db }
   // n = 4, score = 200
   //   b801000000         | mov             eax, 1
   //   b9ca000000         | mov             ecx, 0xca
   //   31d2               | xor             edx, edx
   //   31db               | xor             ebx, ebx

$sequence_11 = { 89c2 e8???????? b801000000 e8???????? }
   // n = 4, score = 200
   //   89c2               | mov             edx, eax
```

```
        //  e8????????          |
        //  b801000000          | mov             eax, 1
        //  e8????????          |

    condition:
        7 of them and filesize < 7946240
}

----------------------------------------------------------------

win_hive_w0   (20211222 | Hive v3 ransomware Windows/Linux/FreeBSD payload)

rule win_hive_w0 {
    meta:
        author = "rivitna"
        family = "ransomware.hive"
        description = "Hive v3 ransomware Windows/Linux/FreeBSD payload"
        source = "https://github.com/rivitna/Malware/blob/main/Hive/Hive.yar"
        severity = 10
        score = 100
        malpedia_reference = "https://malpedia.caad.fkie.fraunhofer.de/details/win.hive"
        malpedia_rule_date = "20211222"
        malpedia_hash = ""
        malpedia_version = "20211222"
        malpedia_sharing = "TLP:WHITE"

    strings:
        $h0 = { B? 03 52 DA 8D [6-12] 69 ?? 00 70 0E 00 [14-20]
                8D ?? 00 90 01 00 }
        $h1 = { B? 37 48 60 80 [4-12] 69 ?? 00 F4 0F 00 [2-10]
                8D ?? 00 0C 00 00 }
        $h2 = { B? 3E 0A D7 A3 [2-6] C1 E? ( 0F | 2F 4?)
                69 ?? 00 90 01 00 }

        $x0 = { C6 84 24 ?? 00 00 00 FF [0-14] 89 ?? 24 ?? 00 00 00 [0-6]
                89 ?? 24 ?? 0? 00 00 [0-20] C6 84 24 ?? 0? 00 00 34 }
        $x1 = { C6 44 24 ?? FF [0-14] 89 ?? 24 ?? [0-6] 89 ?? 24 ?? [0-12]
                C6 84 24 ?? 00 00 00 34 }

    condition:
        (((uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550)) or
         (uint32(0) == 0x464C457F)) and
        (
            (2 of ($h*)) or (1 of ($x*))
        )
```

}

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback