LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

# Ransomware Trends in the HPH Sector (Q1 2022)

**05/05/2022**

TLP: WHITE, ID# ***202205051300***

# Agenda

- Initial Access Broker Trends in the HPH Sector
- Ransomware Trends in the HPH Sector
- Notable Ransomware Techniques Observed
- Detections for Notable Techniques Observed with Mitre ATT&CK Framework
- Mitigations and Takeaways

**Slides Key:**

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

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

# Initial Access Broker (IAB) Trends

- IABs are known to sell network access to ransomware groups and affiliates
- HC3 has observed that threat actors selling network access to HPH entities worldwide on various cybercriminal forums during Q1 2022 compared to all of 2021 remains somewhat consistent
- More than half of forum advertisements were for general VPN/RDP access to HPH entities
- About ¼ of threat activity involved selling alleged access to compromised Citrix VPN appliances
- The COVID-19 pandemic drove organizations to accelerate adoption of remote access and cloud applications, often without implementing basic security features
- IABs enable RaaS groups to focus time and energy on developing payloads and coordinating operations with affiliates

**Access to Remote Access Products Allegedly Belonging to HPH Entities Advertised on Cybercriminal Forums - Breakdown by Product Type (Source: HC3)**

| Remote Access Product | 2021 | 2022 Q1 |
|---|---|---|
| VPN/RDP | 56% | 54% |
| Citrix | 25% | 23% |
| Fortinet | 0% | 0.07% |
| RDWeb | 0.06% | 0.07% |
| PulseSecure | 0.04% | 0.07% |
| GlobalProtect | 0.04% | 0% |
| TIBCO EBX MDM | 0.02% | 0% |
| WebVPN | 0.02% | 0% |
| Palo Alto | 0.02% | 0% |

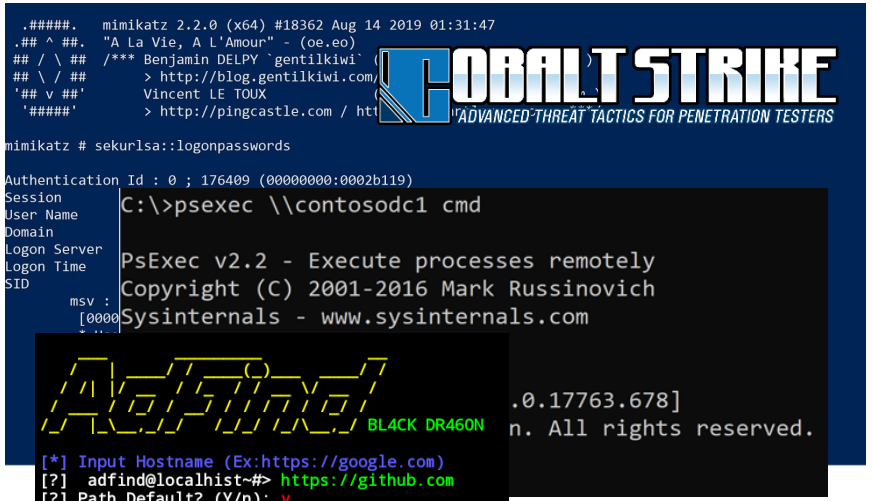
1. **LockBit, Conti, SunCrypt, ALPHV/BlackCat, and Hive were the Top 5 RaaS groups impacting the HPH sector in Q1 2022**
    1. LockBit releases a statement that they will not take a side in Russia's invasion of Ukraine; just business
    2. Conti states that they will side with Russia amidst invasion of Ukraine; Karakurt identified as the data extortion arm of Conti
    3. SunCrypt gains new capabilities in 2022, although it seems like the ransomware is still under development
    4. ALPHV/BlackCat/Noberus ransomware linked to BlackMatter, DarkSide; BlackCat speeds up encryption process
    5. Nokoyawa ransomware possibly related to Hive, Karma/Nemty
2. **Financially-motivated groups shifting to ransomware operations**
    - FIN7: Shift beginning at the end of 2021 and into 2022; ransomware variants used in connection with the group's operations include Maze, Ryuk and ALPHV/BlackCat.
    - FIN12: In April 2022, ransomware attacks conducted by FIN12 could reportedly be achieved in less than two days, compared to the previous timeframe of five days when the group was first identified; FIN12 has specifically targeted the healthcare industry; FIN12 leveraged Ryuk, Beacon, SystemBC, and Metasploit to carry out some of the most prolific intrusions seen throughout 2021.

| Top RaaS Groups Impacting HPH Sector Worldwide in Q1 2022 (Source: HC3) | | |
|---|---|---|
| **Place** | **RaaS Name** | **Percentage** |
| **1** | LockBit 2.0 | 31% |
| **2** | Conti | 31% |
| **3** | SunCrypt | 16% |
| **4** | ALPHV | 11% |
| **5** | Hive | 11% |

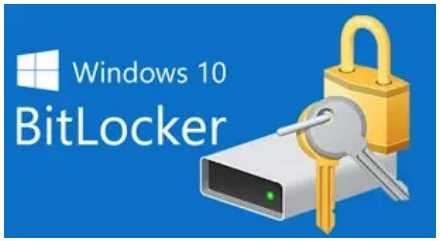
3. **Ransomware groups increasingly leverage legitimate tools during ransomware intrusions**
   - Remote access tools: AnyDesk, Windows Safe Mode, Atera, ScreenConnect, ManageEngine
   - Encryption tools: Microsoft's BitLocker, Jetico's BestCrypt, DiskCryptor
   - File transfer tools: FileZilla FTP
   - Microsoft Sysinternals Utilities: PsExec, Procdump, Dumpert
   - Open-source tools: Cobalt Strike, Mimikatz, AdFind, Process Hacker, and MegaSync.

*Key Resource*:

CyberArk, Living Off the Land Ransomware Attacks: A Step-By-Step Plan for Playing Defense https://www.cyberark.com/resources/blog/living-off-the-land-ransomware-attacks-a-step-by-step-plan-for-playing-defense





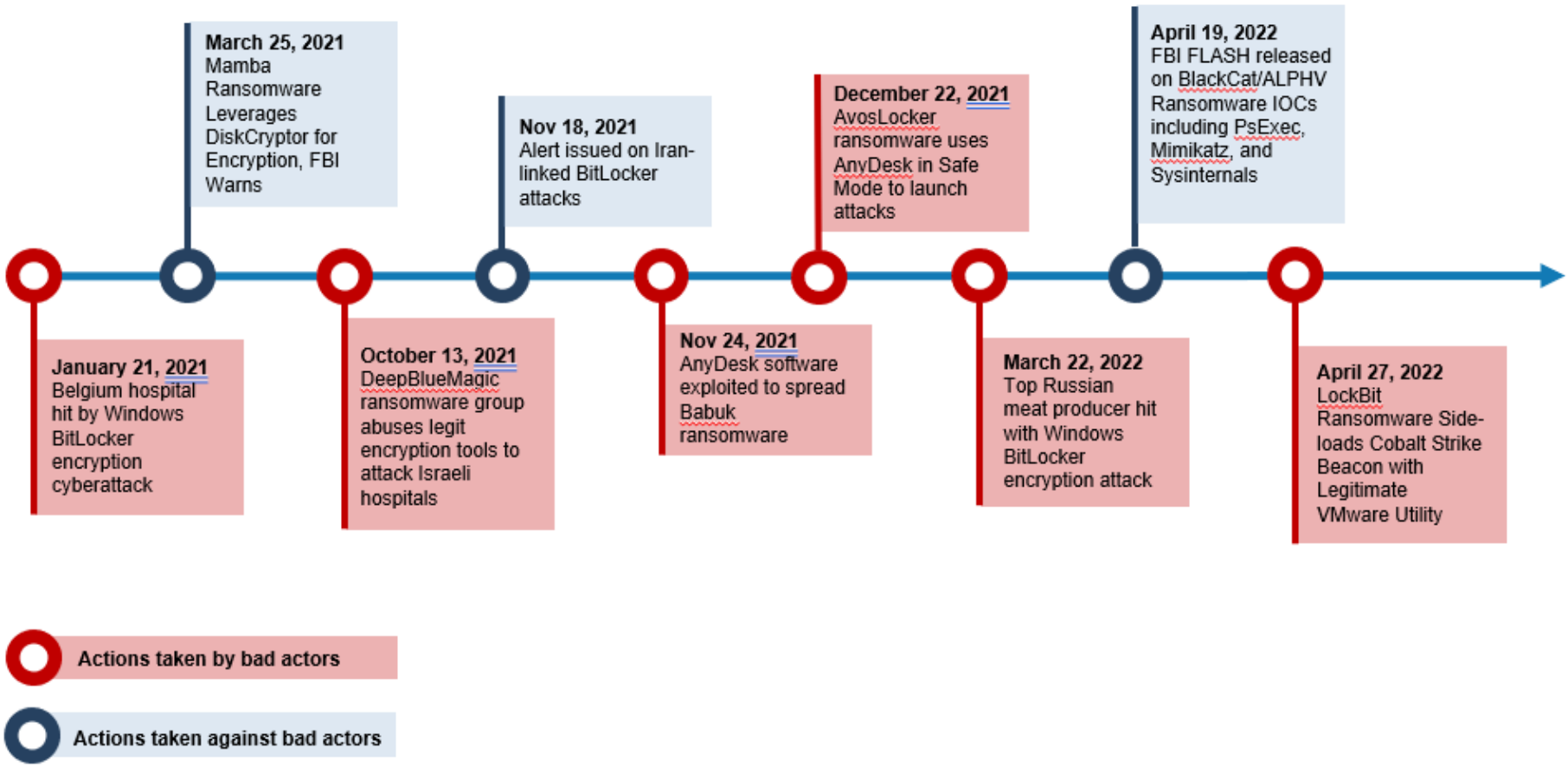



# Living Off the Land (LOTL) Attacks

- **What is LOTL?** Threat actors leverage what is already available in the target environment instead of deploying custom tools and malware.
- **What are the benefits to the attacker?**
  - Malicious actions are less likely to flag antivirus or alert endpoint detection tools
  - Malicious actions are more likely to blend in with normal administrative tasks
- **How do attackers "Live off the Land"?**
  - Leverage native Windows tools such as CMD.exe, PowerShell, Task Scheduler, MSHTA, and Sysinternals
  - Leverage common remote management tools such as TeamViewer, Kaseya, LogMeIn, etc.

Windows Sysinternals

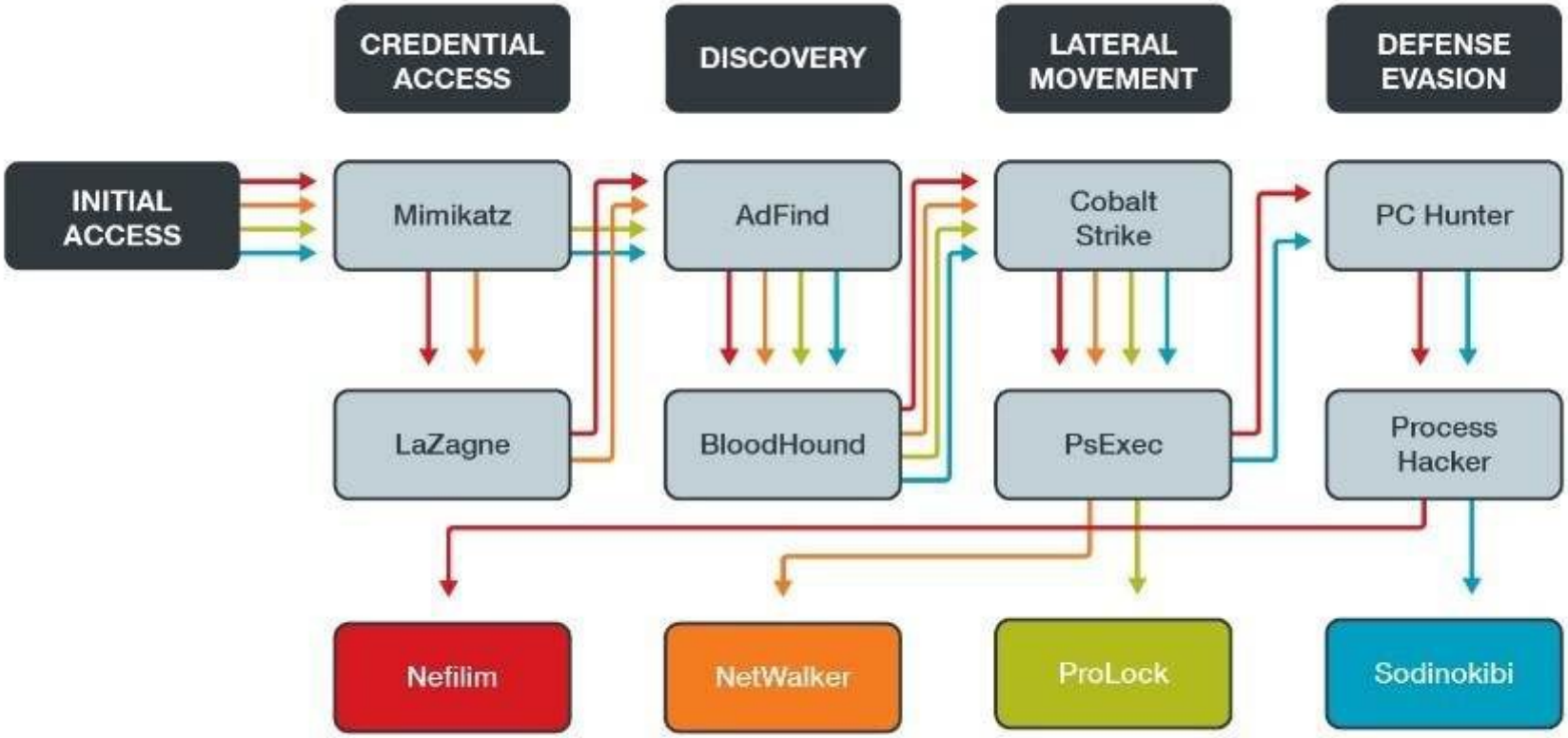
# Historical Ransomware Activity Leveraging Legitimate Tools



# Commonly Abused Legitimate Tools for Ransomware Campaigns

| Tool | Intended Use | How It Is Used for Ransomware Campaigns | Ransomware Campaigns That Used This Tool |
|---|---|---|---|
| Cobalt Strike (S0154) | Threat emulation | Lateral movement, backdoor<br><br>Has many other capabilities as a remote access trojan (RAT) | Clop, Conti, DoppelPaymer, Egregor, Hello (WickrMe), Nefilim, NetWalker, ProLock, RansomExx, Ryuk, Conti, BlackCat/ALPHV, Hive, SunCrypt, Karakurt, Quantum |
| PsExec (S0029) | Executing processes on other systems | Arbitrary command shell execution, lateral movement | DoppelPaymer, Nefilim, NetWalker, Maze, Petya, ProLock, Ryuk, Sodinokibi, Wizard Spider, LockBit 2.0, Conti, SunCrypt, LockBit, Hive, Quantum, BlackCat/ALPHV |
| Mimikatz (S0002) | Proof-of-concept for demonstrating vulnerabilities | Credential dumping and credential access for privilege escalation | DoppelPaymer, Nefilim, NetWalker, Maze, ProLock, RansomExx, Sodinokibi, SunCrypt, LockBit, Hive, Conti, BlackCat/ALPHV, Karakurt |
| Process Hacker | Monitoring system resources, debug software, and detect malware | Process/service discovery and termination (including antimalware and endpoint security solutions) | Crysis, Nefilim, Sodinokibi, Conti, LockBit, DoppelPaymer |
| AdFind (S0552) | Active Directory (AD) search utility | AD discovery (can be a prerequisite for lateral movement), privilege escalation | Nefilim, NetWalker, ProLock, Egregor, Sodinokibi, Conti, Hive, Quantum |
| MegaSync | Cloud-based synchronization | Data exfiltration | Pysa, Hades, LockBit, Nefilim, Conti, BlackCat/ALPHV |

# Commonly Abused Legitimate Tools for Ransomware Campaigns (cont.)



# Detection Opportunities for Commonly Abused Legitimate Tools

| Tool | Relevant ATT&CK Techniques | Detection Opportunities |
|---|---|---|
| Cobalt Strike (S0154) | Lateral Tool Transfer (T1570) | Command Execution (DS0017); File Creation and File Metadata (DS0022); Named Pipe Metadata (DS0023); Network Share Access (DS0033); Network Traffic Content and Flow (DS0029); Process Creation (DS0009) |
| PsExec (S0029) | Create Account: Domain Account (T1136.002); Create or Modify System Process: Windows Service (T1543.003); Lateral Tool Transfer (T1570); Remote Services: SMB/Windows Admin Shares (T1021.002); System Services: Service Execution (T1569.002) | Command Execution (DS0017); Process Creation (DS0009); User Account Creation (DS0002); Driver Load (DS0027); OS API Execution and Process Creation (DS0009); Service Creation and Modification (DS0019); Windows Registry Key Creation and Modification (DS0024); Named Pipe Metadata (DS0023); Network Share Access (DS0033); Network Traffic Content/Flow and Network Connection Creation (DS0029); Logon Session Creation (DS0028) |
| Mimikatz (S0002) | Credentials from Password Stores (T1555) | Command Execution (DS0017); File Access (DS0022); OS API Execution and Process Access and Creation (DS0009) |

**Mitre ATT&CK website**: https://attack.mitre.org/

# Detection Opportunities for Commonly Abused Legitimate Tools (cont.)

| Tool | Relevant ATT&CK Techniques | Detection Opportunities |
|---|---|---|
| Process Hacker | Process Discovery (T1057)<br>Service Stop (T1489) | Command Execution (DS0017); OS API Execution, Process Creation and Process Termination (DS0009); Service Creation and Service Metadata (DS0019); File Modification (DS0022); Windows Registry Key Modification (DS0024) |
| AdFind (S0552) | Account Discovery: Domain Account (T1087.002); Domain Trust Discovery (T1482); Permission Groups Discovery: Domain Groups (T1069.002); Remote System Discovery (T1018); System Network Configuration Discovery (T1016) | Command Execution (DS0017); OS API Execution and Process Creation (DS0009); Script Execution (DS0012); File Access (DS0022); Network Connection Creation (DS0029) |
| MegaSync | Exfiltration to Cloud Storage (T1567.002) | Command Execution (DS0017); File Access (DS0022); Network Traffic Content and Network Traffic Flow (DS0029) |

**Mitre ATT&CK website**: https://attack.mitre.org/

- Consider using the host firewall to restrict file sharing communications, such as SMB (M1037)
- Network intrusion detection and prevention systems that use network signatures (M1031)
- Use multi-factor authentication for user and privileged accounts (M1032)
- Configure access controls and firewalls to limit access to domain controllers and systems used to create and manage accounts (M1030)
- Operate intrusion detection, analysis, and response systems on a separate network from the production environment to lessen the chances that an adversary can see and interfere with critical response functions (M1030)
- Employ network segmentation for sensitive domains (M1030)
- Protect domain controllers by ensuring proper security configuration for critical servers (M1028)
- Do not allow domain administrator accounts to be used for day-to-day operations that may expose them to potential adversaries on unprivileged systems (M1026)
- Deny remote use of local admin credentials to log into systems. Do not allow domain user accounts to be in the local Administrators group multiple systems (M1026)

- On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent an application from writing a signed vulnerable driver to the system. On Windows 10 and 11, enable Microsoft Vulnerable Driver Blocklist to assist in hardening against third party-developed service drivers. (M1040)
- On Windows 10, enable Attack Surface Reduction (ASR) rules to block processes created by PsExec from running. (M1040)
- Enforce registration and execution of only legitimately signed service drivers where possible (M1045)
- Ensure that Driver Signature Enforcement is enabled to restrict unsigned drivers from being installed (M1028)
- Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service configurations (M1018)
- Consider disabling Windows administrative shares (M1035)
- Do not reuse local administrator account passwords across systems. Ensure password complexity and uniqueness such that the passwords cannot be cracked or guessed (M1027)

- The password for the user's login keychain can be changed from the user's login password. This increases the complexity for an adversary because they need to know an additional password. Organizations may consider weighing the risk of storing credentials in password stores and web browsers. If system, software, or web browser credential disclosure is a significant concern, technical controls, policy, and user training may be used to prevent storage of credentials in improper locations (M1027)
- Use auditing tools capable of detecting privilege and service abuse opportunities on systems within an enterprise, and correct them (M1047)
- Map the trusts within existing domains/forests and keep trust relationships to a minimum (M1047)
- Ensure that high permission level service binaries cannot be replaced or modified by users with a lower permission level (M1022)
- Ensure proper process and file permissions are in place to inhibit adversaries from disabling or interfering with critical services (M1022)
- Ensure that permissions disallow services that run at a higher permissions level from being created or interacted with by a user with a lower permission level (M1026)

- Ensure proper registry permissions are in place to inhibit adversaries from disabling or interfering with critical services (M1024)
- Prevent administrator accounts from being enumerated when an application is elevating through UAC, since it can lead to the disclosure of account names (M1028)
- Web proxies can be used to enforce an external network communication policy that prevents use of unauthorized external services (M1021)

# Takeaways

- Financially-motivated and state-sponsored threat actors are highly likely to continue to evolve their Tactics, Techniques, and Procedures (TTPs) for successful attacks
- Legitimate tools are likely to continue to be abused/weaponized in ransomware campaigns in an attempt by threat actors to avoid detection
- Living off the Land (LotL) techniques leveraging legitimate tools are difficult but possible to detect
- The behavior-based approach that a modern security information and event management (SIEM) tool provides will be able to detect living-off-the-land techniques that signature-based detection cannot
- Some types of attack techniques cannot be easily mitigated with preventive controls since it is based on the abuse of system features; fortunately, there are detection opportunities for these techniques

# Reference Materials

# References


- Bryce Abdo, Zander Work, Iona Teaca, Brendan McKeague. 2022. FIN7 Power Hour: Adversary Archaeology and the Evolution of FIN7. April 2. Accessed April 20, 2022. https://www.mandiant.com/resources/evolution-of-fin7.
- Buber, Zohar. 2020. *How to Identify Cobalt Strike on Your Network.* November 18. Accessed 19 2022, April. https://www.darkreading.com/threat-intelligence/how-to-identify-cobalt-strike-on-your-network.
- Davis, Griffin. 2022. *New FIN12 Ransomware Group Faster and More Dangerous Among Other Hacking Groups.* April 20. Accessed April 21, 2022. https://www.techtimes.com/articles/274519/20220420/new-fin12-ransomware-group-faster-more-dangerous-hacking-groups.htm.
- Don Ovid Ladores, Ian Kenefick, Earle Maui Earnshaw. 2022. *New Nokoyawa Ransomware Possibly Related to Hive.* March 9. Accessed April 20, 2022. https://www.trendmicro.com/en_us/research/22/c/nokoyawa-ransomware-possibly-related-to-hive-.html.
- FBI Cyber Division. 2022. BlackCat/ALPHV Ransomware Indicators of Compromise. April 19. Accessed April 21, 2022. https://www.ic3.gov/Media/News/2022/220420.pdf.
- FRSECURE. 2021. *Living Off The Land Attacks: Tools, Tactics, and Prevention.* August 2. Accessed April 20, 2022. https://frsecure.com/blog/living-off-the-land-attacks/.
- Haughom, James. 2022. LockBit Ransomware Side-loads Cobalt Strike Beacon with Legitimate VMware Utility. April 27. Accessed April 2022, 27. https://www.sentinelone.com/labs/lockbit-ransomware-side-loads-cobalt-strike-beacon-with-legitimate-vmware-utility/.

- Hill, Jason. 2021. *Good for Evil: DeepBlueMagic Ransomware Group Abuses Legit Encryption Tools.* October 19. Accessed April 12, 2022. https://www.varonis.com/blog/deepbluemagic-ransomware.
- Murphy, Bryan. 2021. Living Off the Land Ransomware Attacks: A Step-By-Step Plan for Playing Defense. August 10. Accessed April 22, 2022. https://www.cyberark.com/resources/blog/living-off-the-land-ransomware-attacks-a-step-by-step-plan-for-playing-defense.
- Red Canary. 2022. 2022 Threat Detection Report. March 22. Accessed April 21, 2022. https://redcanary.com/threat-detection-report/threats/.
- Riley, Tonya. 2022. *Notorious hacking group FIN7 adds ransomware to its repertoire.* April 4. Accessed April 20, 2022. https://www.cyberscoop.com/fin7-ransomware-mandiant/.
- Scroxton, Alex. 2021. *Alert over spate of Iran-linked BitLocker attacks.* November 18. Accessed April 11, 2022. https://www.computerweekly.com/news/252509689/Alert-over-spate-of-Iran-linked-BitLocker-attacks.
- Sophos. 2021. *AvosLocker Ransomware Uses Remote Desktop Software in Safe Mode to Launch Attacks, Sophos Reports.* December 22. Accessed April 11, 2022. https://www.sophos.com/en-us/press-office/press-releases/2021/12/avoslocker-ransomware-uses-anydesk-in-safe-mode-to-launch-attacks.
- The Stack. 2021. *BitLocker used to attack servers in "intrusion with almost no malware".* November 15. Accessed April 20, 2022. https://thestack.technology/ransomware-attack-bitlocker/.

- Trend Micro. 2021. *Locked, Loaded, and in the Wrong Hands: Legitimate Tools Weaponized for Ransomware in 2021.* April 29. Accessed April 15, 2022. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/locked-loaded-and-in-the-wrong-hands-legitimate-tools-weaponized-for-ransomware-in-2021.
- U.S. Department of Health and Human Services, Health Sector Cybersecurity Coordination Center (HC3). 2021. *Cobalt Strike as a Threat to Healthcare.* November 4. Accessed April 20, 2022. https://www.hhs.gov/sites/default/files/cobalt-strike-tlpwhite.pdf.
- Unit 42. 2022. *2022 Unit 42 Ransomware Threat Report Highlights: Ransomware Remains a Headliner.* March 24. Accessed April 20, 2022. https://unit42.paloaltonetworks.com/2022-ransomware-threat-report-highlights/.

# Questions

**Upcoming Briefs**

- Russian Cyber Intel Services (5/19)
- The Return of Emotet (6/2)

***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