LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Demystifying BlackMatter

09/02/2021

TLP: WHITE, ID# ***202109021300***

Agenda

- Executive Summary
- What the Group Claims To Be
- What We Know About the Group
- Technical Details
- Mitigations
- Outlook

Slides Key:

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

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

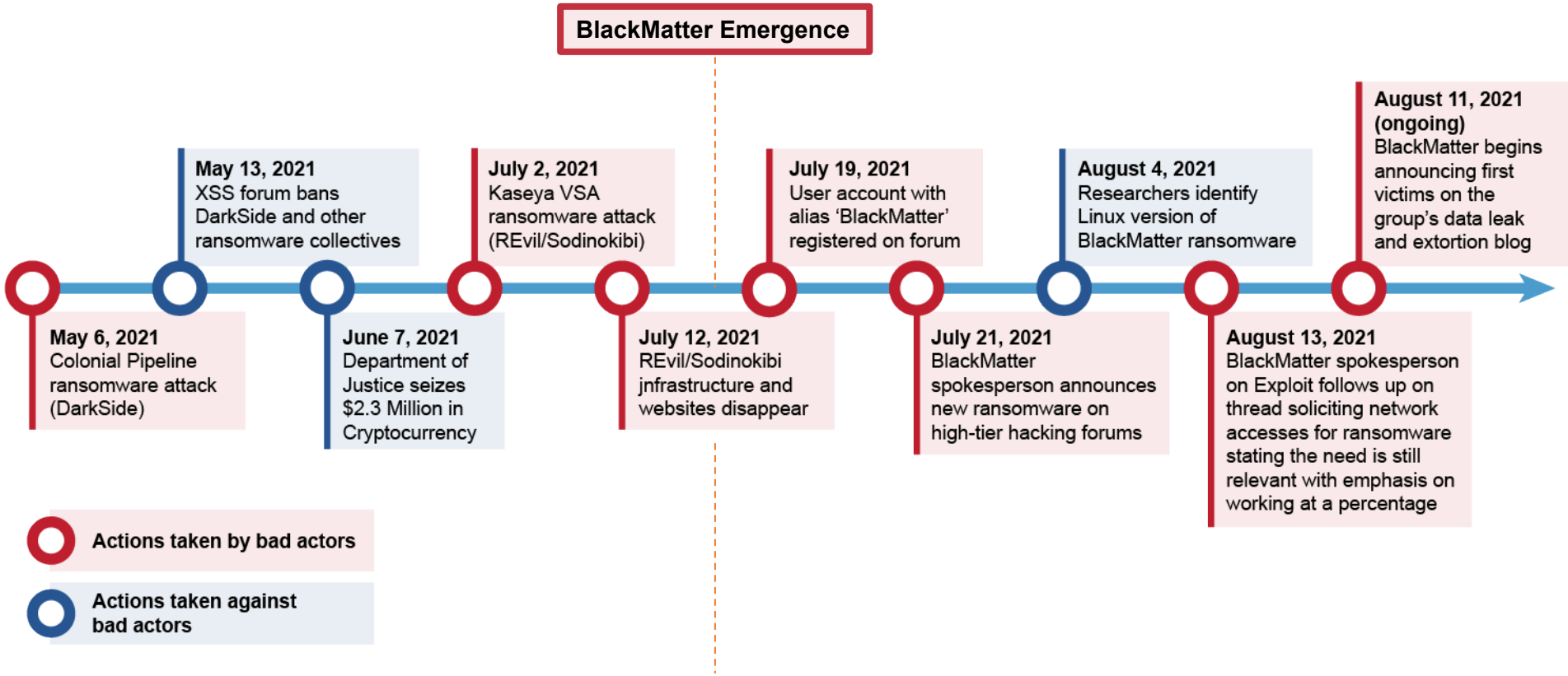
Malware

- **First Surfaced**: July 2021
- **Suspected Predecessor(s)**: DarkSide, REvil RaaS
- **Malware Capabilities**: Ransomware written in C that encrypts files using a combination of Salsa20 and 1024-bit RSA
- **Targeted Systems**: Windows and Linux servers

Group

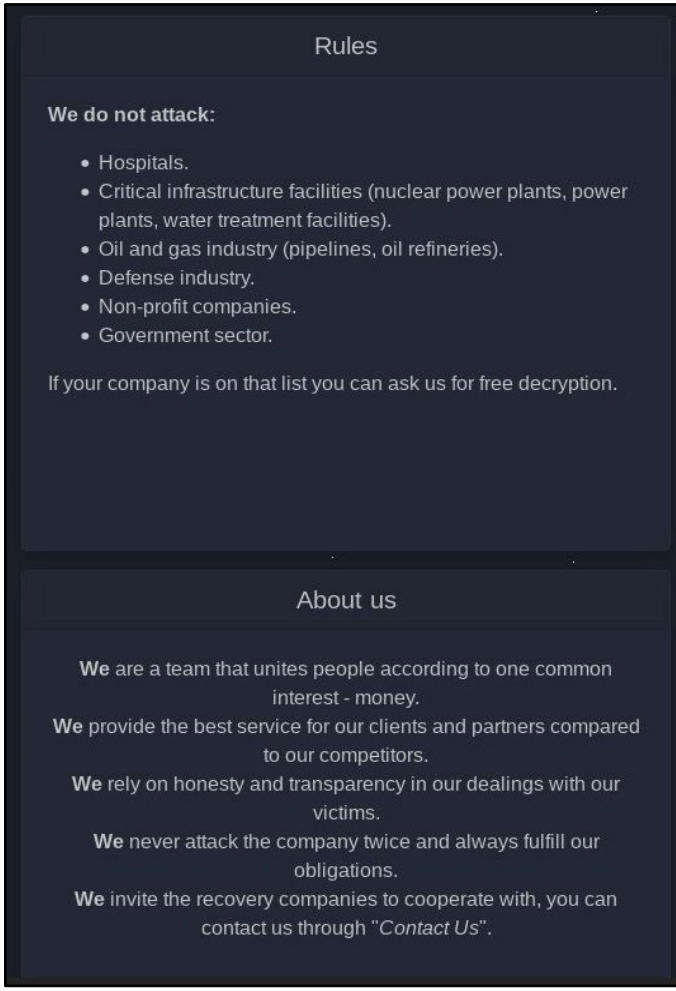
- **Origin**: Likely Eastern Europe, Russian-speaking
- **Forum Presence**: Exploit and XSS, BlackMatter blog
- **Targeted Countries**: United States, India, Brazil, Chile, Thailand, and growing
- **Targeted Industries**: Legal, Real Estate, IT Services, Food & Beverage, Architecture, Education, Finance
- **Status**: Actively seeking Initial Access Brokers (IABs) and affiliates for ransomware deployment
- **Classification**: Highly-sophisticated, financially-motivated cybercriminal operation
- **Threat to HPH Sector**: Elevated Risk

Timeline of Relevant Threat Activity



What the Group Claims to Be

- Sources include an interview with a BlackMatter representative, the BlackMatter Ransomware public extortion blog, hacking forum advertisements, affiliate panel information, and ransom notes.
- The BlackMatter representative claims they do not to attack a variety of industries, including hospitals, and if these entities are attacked, then the company can ask for free decryption.
- “We will not allow our project to be used to encrypt critical infrastructure that will attract unwanted attention to us.”
- Claims the ransomware development took six months and includes best features of LockBit, REvil, and Darkside.
- The security system is thoroughly developed, and the project uses a decentralized structure protected from various vulnerabilities.
- New stable Windows and Linux ransomware tested in various environments, including Windows Server 2021, Windows 11, ESXI 7.0, Ubuntu 18, Debian 10, CentOS 8.
- Note: These details are what BlackMatter claims to be, and may not be accurate.



What the Group Claims to Be, Part 2

BlackMatter
byte

B

Seller
0
1 post
Joined
07/19/21 (ID: 118280)
Activity
другое / other
Deposit
4.000000 ฿

Posted July 21

We are looking for corporate networks of the following countries:

- USA.
- THAT.
- TO.
- GB.

All areas except:

- Medicine.
- State institutions.

Requirements:

- Zoom Revenue от 100kk+.
- 500 - 15,000 hosts.
- We do not take networks with which someone has already tried to work.

2 options for work:

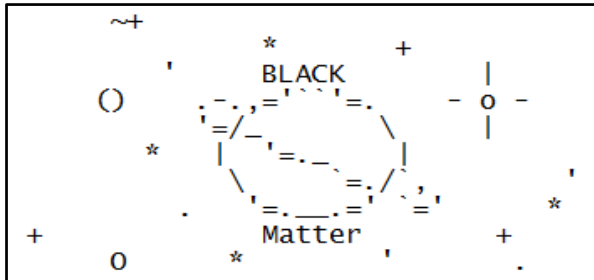
- We buy: From 3 to 100k.
- We take it to work (discussed individually).

Scheme of work:
Selecting a work option -> Access transfer -> Checking -> We take it or not (in case of discrepancy).

Deposit: 120k.

First contact of the PM. We are looking first of all for stable and adequate suppliers.

What the Group Claims to Be, Part 3




```
>>> What happens?
   Your network is encrypted, and currently not operational. We have downloaded 1TB from your
fileserver.
   We need only money, after payment we will give you a decryptor for the entire network and
you will restore all the data.

>>> What guarantees?
   We are not a politically motivated group and we do not need anything other than your money.
   If you pay, we will provide you the programs for decryption and we will delete your data.
   If we do not give you decrypters or we do not delete your data, no one will pay us in the
future, this does not comply with our goals.
   We always keep our promises.

>> Data leak includes
1. Full emloyeers personal data
2. Network information
3. Schemes of buildings, active project information, architect details and contracts,
4. Finance info


>>> How to contact with us?
   1. Download and install TOR Browser (https://www.torproject.org/).
   2. Open
http://supp24                                                    .onion/7NT6LXKC1XQHW5039BLOV.

>>> Warning! Recovery recommendations.
   We strongly recommend you to do not MODIFY or REPAIR your files, that will damage them.
```

Role of Initial Access Brokers (IABs)

- Initial Access Brokers (IABs) are individuals who sell access to compromised networks for further exploitation by ransomware operators.
- In general, Initial Access Brokers (IABs) play a major role in ransomware operations.
- Most commonly, hackers sell RDP credentials, VPN login details, and web shells.
- These details often include the victim's name, type of access, level, location, or industry. In some cases, the sellers detail the type and number of machines found on the compromised network, as well as the types of data that could be found there.
- HC3 has observed at least 65 instances of threat actors selling network access to healthcare entities on hacking forums in the past year.
- Ke-La analyzed 1,000 forum posts selling network access over the past year (since August), and found that the top affected country was the United States, with 4% in the healthcare industry.
- May serve as early warning to a more impactful ransomware incident, but is still an indicator of possible network compromise.

What We Know About BlackMatter Ransomware

- Written in C that encrypts files using a combination of Salsa20 and 1024-bit RSA
- Targets Windows and Linux systems
- Attempts to mount and encrypt unmounted partitions
- Targets files stored locally and on network shares, as well as removable media
- Can terminate processes prior to encryption
- Deletes volume shadow copies and ignores specific directories, files, or file extensions during encryption
- Can be configured to upload system information to a remote server via HTTP or HTTPS
- Collected system information may include system name, username, domain, language information, and list of enumerated drives

BlackMatter Leak Site URL: blackmax7su6mbwtcyo3xwtpfxpm356jjqrs34y4crcytpw7mifuedyd[.]onion/

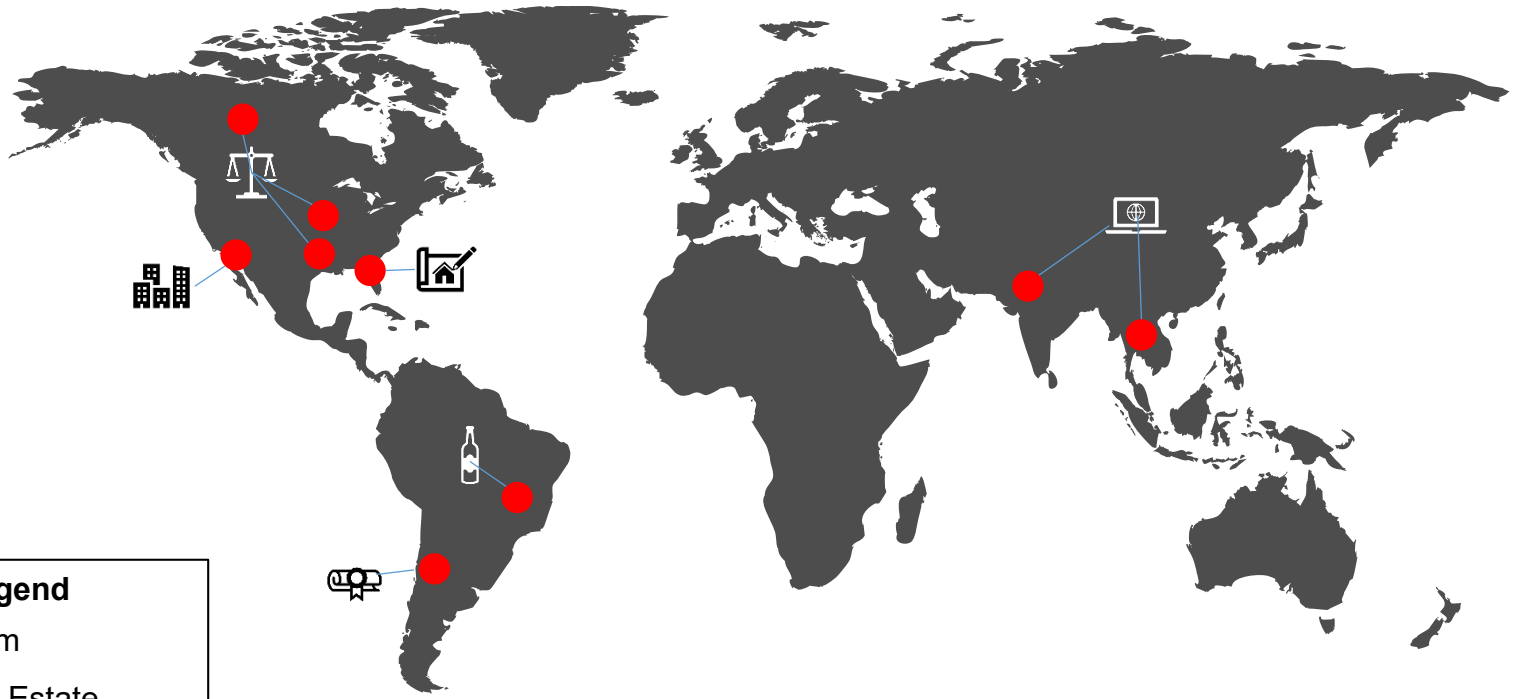
- Group-IB analysis revealed an obvious connection between BlackMatter and DarkSide and REvil samples, especially DarkSide, as shown in the simplified table below:

	DarkSide	REvil	BlackMatter
File Encryption	Salsa20 custom matrix; RSA-1024	Salsa20; Curve25519	Salsa20 custom matrix; RSA-1024
Obfuscation	Same	Same	Same
Privilege Escalation	UAC bypass optional with ICMLuaUtlil	UAC bypass optional with CVE-2018-8453	UAC bypass with ICMLuaUtil if necessary
Defense Evasion	Binary config data with custom encoding	JSON config data with RC4 encoding	Binary config data with custom encoding
Language Check	Optional (configuration)	Optional (configuration)	No
Mutex name	Optional (configuration)	Hardcoded	Optional (configuration)
Victim ID / Ransom Extension	Created based on MachineGuid	Random	Created based on MachineGuid
Linux Version	Yes	Yes	Yes

- To better understand the potential relationships between the ransomware groups, Sophos has analyzed a BlackMatter ransomware sample and uncovered a number of technical similarities with DarkSide and the other ransomware families that are worth noting:

Feature	REvil	Lockbit 2.0	DarkSide	BlackMatter
Type	RaaS	RaaS	RaaS	RaaS
Network first	-	Yes	No	No
Multi-threaded	Yes	Yes	Yes	Yes
File encryption	In-place	In-place	In-place	In-place
Encrypt size	Full	Partial, 4 KB	Partial, 512 KB	Partial, 1024 KB
Rename	After	After	Before	Before
Decryption Blob	End of File	End of File	End of File	End of File
Wallpaper	Yes	Yes	Yes	Yes
Encrypts Russian systems	No	Yes	No	Yes

BlackMatter Victims



Legend

- Victim
- Real Estate
- Legal
- Food & Beverage
- IT Services
- Education
- Architecture

Takeaways

- Some victims are outside initial target geography
- Most victims have far lower revenue than target of $100M
- No healthcare or public health sector victims observed

General efforts to help prevent ransomware attacks include:

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

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

The HHS 405(d) Program published the Health Industry Cybersecurity Practices (HICP), which is a free resource that identifies the top five cyber threats, and the ten best practices to mitigate them. Below are the practices from HICP that can be used to mitigate BlackMatter:

DEFENSE / MITIGATION / COUNTERMEASURE	405(d) HICP REFERENCE
Provide social engineering and phishing training to employees.	**[10.S.A], [1.M.D]**
Develop and maintain policy on suspicious e-mails for end users, and ensure suspicious e-mails are reported.	**[10.S.A], [10.M.A]**
Ensure emails originating from outside the organizations are automatically marked before being received.	**[1.S.A], [1.M.A]**
Apply patches/updates immediately after release/testing, develop/maintain the patching program if necessary.	**[7.S.A], [7.M.D]**
Implement Intrusion Detection Systems (IDS), and keep signatures and rules updated.	**[6.S.C], [6.M.C], [6.L.C]**
Implement spam filters at the email gateways, and keep signatures and rules updated.	**[1.S.A], [1.M.A]**
Block suspicious IP addresses at the firewall, and keep firewall rules updated.	**[6.S.A], [6.M.A], [6.L.E]**

Background information can be found here:
https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

The HHS 405(d) Program published the Health Industry Cybersecurity Practices (HICP), which is a free resource that identifies the top five cyber threats, and the ten best practices to mitigate them. Below are the practices from HICP that can be used to mitigate BlackMatter:

DEFENSE / MITIGATION / COUNTERMEASURE	405(d) HICP REFERENCE
Implement whitelisting technology to ensure that only authorized software is allowed to execute.	**[2.S.A], [2.M.A], [2.L.E]**
Implement access control based on the principal of least privilege.	**[3.S.A], [3.M.A], [3.L.C]**
Implement and maintain anti-malware solution.	**[2.S.A], [2.M.A], [2.L.D]**
Conduct system hardening to ensure proper configurations.	**[7.S.A], [7.M.D]**
Disable the use of SMBv1 (and all other vulnerable services and protocols) and require at least SMBv2. Restricting/Minimizing/eliminating RDP usage.	**[7.S.A], [7.M.D]**

Background information can be found here:
https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

Indicators of Compromise for BlackMatter Ransomware

- Below are a sample of indicators of compromise (IOCs) from recent BlackMatter attacks:

Indicator	Description
598c53bfef81e489375f09792e487f1a	BlackMatter ransomware
a55bc3368a10ca5a92c1c9ecae97ced9	BlackMatter ransomware
ba375d0625001102fc1f2ccb6f582d91	BlackMatter ransomware
b06e2455a9c7c9485b85e9bdcceb8078	BlackMatter ransomware
605d939941c5df2df5dbfb8ad84cfed4	BlackMatter ransomware
3f9a28e8c057e7ea7ccf15a4db81f362	BlackMatter ransomware (Linux Variant)
paymenthacks[.]com	Command and Control (C2)
mojobiden[.]com	Command and Control (C2)
131.107.255[.]255	Command and Control (C2)
206.188.197[.]206	Command and Control (C2)
51.79.243[.]236	Command and Control (C2)
Bc1qlv2qdmylyuw62zw8qcd4n3uh84cy2edckv3ds7	Attacker Bitcoin address

MITRE ATT&CK® Techniques for BlackMatter Ransomware

- Below are some basic MITRE ATT&CK® Techniques for BlackMatter Ransomware:

Tactic	Technique ID	Technique Name
Initial Access	T1566	Phishing
Execution	T1204	User Execution
Discovery	T1082	System Information Discovery
Defense Evasion	T1497.003	Time-Based Evasion
Impact	T1490 T1489 T1486	Inhibit System Recovery Service Stop Data Encrypted for Impact

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

- Ransomware trends:
  - IABs have been driven underground by law enforcement action.
  - Affiliates are leveraging multiple ransomware families to achieve goals.
  - Ransomware developers are rebranding to avoid law enforcement action.
- Threat to the HPH:
  - While there have not been any public healthcare victims yet, BlackMatter's suspected predecessors targeted the healthcare sector.
  - HPH organizations should remain on alert despite the group's claims to not target healthcare.

Reference Materials

References

- Abrams, Lawrence. “BlackMatter ransomware gang rises from the ashes of DarkSide, Revil,” BleepingComputer. 31 July 2021. https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-gang-rises-from-the-ashes-of-darkside-revil/
- Abrams, Lawrence. "Linux version of BlackMatter ransomware targets VMware ESXi servers," 5 August 2021. https://www.bleepingcomputer.com/news/security/linux-version-of-blackmatter-ransomware-targets-vmware-esxi-servers/
- Analyst1. "Absolute Ransom: Nation-State Ransomware," 11 August 2021. https://analyst1.com/whitepaper/nation-state-and-ransomware
- Beek, Christiaan. "DarkSide & BlackMatter Config Extractor by ValthekOn & S2 (@sisoma2)," 13 August 2021. https://github.com/advanced-threat-research/DarkSide-Config-Extract
- CISA, "Alert (AA21-131A) DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks," 8 July 2021. https://us-cert.cisa.gov/ncas/alerts/aa21-131a
- Cohen, Z. and Marquardt, A. "White House cyber official says 'commitment' by ransomware gang suggests Biden's warnings are being heard," 4 August 2021. https://www.cnn.com/2021/08/04/politics/neuberger-ransomware-blackmatter/index.html
- FireEye, "Shining a Light on DARKSIDE Ransomware Operations," 14 May 2021. https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html
- Flashpoint, "Chatter Indicates BlackMatter as REvil Successor," 27 July 2021. https://www.flashpoint-intel.com/blog/chatter-indicates-blackmatter-as-revil-successor/

References

- Krebs, Brian. “Ransomware Gangs and the Name Game Distraction,” 5 August 2021. https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
- Loman, Mark. "BlackMatter ransomware emerges from the shadow of DarkSide," Sophos. 9 August 2021. https://news.sophos.com/en-us/2021/08/09/blackmatter-ransomware-emerges-from-the-shadow-of-darkside/
- Naraine, Ryan. "DarkSide Ransomware Shutdown: An Exit Scam or Running for Hills?," 14 May 2021. https://www.securityweek.com/darkside-ransomware-shutdown-exit-scam-or-running-hills
- Recorded Future, “Protect Against BlackMatter Ransomware Before It’s Offered,” 4 August 2021. https://www.recordedfuture.com/blackmatter-ransomware-protection/
- Rijnders, Gijs. "Analysis of the BlackMatter ransomware," Tesorion. 5 August 2021. https://www.tesorion.nl/en/posts/analysis-of-the-blackmatter-ransomware/
- Riley, Duncan. “Initial Access Brokers lead ransomware efforts by selling access to compromised networks,” 2 August 2021. https://siliconangle.com/2021/08/02/initial-access-brokers-lead-ransomware-efforts-selling-access-compromised-networks/
- Schwartz, Mathew. "Secrets and Lies: The Games Ransomware Attackers Play," 5 August 2021. https://www.bankinfosecurity.com/blogs/secrets-lies-games-ransomware-attackers-play-p-3076
- Schwartz, Matthew. “BlackMatter Ransomware Claims to Be Best of REvil, DarkSide,” 28 July 2021. https://www.bankinfosecurity.com/revil-ransomware-operation-returning-as-blackmatter-a-17160
- Schwartz, Matthew. "BlackMatter Ransomware Appears to Be Spawn of DarkSide," 2 August 2021. https://www.bankinfosecurity.com/blogs/blackmatter-ransomware-appears-to-be-spawn-darkside-p-3075

References

- Sjouwerman, Stu. "DarkSide Ransomware Returns as BlackMatter After Sudden Shutdown of Operations," 11 August 2021. https://blog.knowbe4.com/darkside-ransomware-returns-as-blackmatter-after-sudden-shutdown-of-operations
- Smilyanets, Dimitry. “An interview with BlackMatter: A new ransomware group that’s learning from the mistakes of DarkSide and Revil,” 2 August 2021. https://therecord.media/an-interview-with-blackmatter-a-new-ransomware-group-thats-learning-from-the-mistakes-of-darkside-and-revil/
- Starks, Tim. “Threat intel firms suggest ransomware gang 'BlackMatter' has ties to DarkSide, REvil hackers,” 28 July 2021. https://www.cyberscoop.com/blackmatter-darkside-revil-ransomware-successor/
- Symantec, "Affiliates Unlocked: Gangs Switch Between Different Ransomware Families," 12 August 2021. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-trends-lockbit-sodinokibi
- Zhdanov, Andrey. "It's alive! The story behind the BlackMatter ransomware strain," 6 August 2021. https://blog.group-ib.com/blackmatter

Questions

Upcoming Briefs

- 9/23 – LockBit Ransomware

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