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)
Executive Summary – BlackMatter Ransomware

Malware

- **First Suraced:** 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

May 6, 2021
Colonial Pipeline ransomware attack (DarkSide)

May 13, 2021
XSS forum bans DarkSide and other ransomware collectives

June 7, 2021
Department of Justice seizes $2.3 Million in Cryptocurrency

July 2, 2021
Kaseya VSA ransomware attack (REvil/Sodinokibi)

July 12, 2021
REvil/Sodinokibi infrastructure and websites disappear

July 19, 2021
User account with alias ‘BlackMatter’ registered on forum

July 21, 2021
BlackMatter spokesperson announces new ransomware on high-tier hacking forums

August 4, 2021
Researchers identify Linux version of BlackMatter ransomware

August 11, 2021
(ongoing)
BlackMatter begins announcing first victims on the group’s data leak and extortion blog

August 13, 2021
BlackMatter spokesperson on Exploit follows up on thread soliciting network accesses for ransomware stating the need is still relevant with emphasis on working at a percentage
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.
BlackMatter

We are looking for corporate networks of the following countries:

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

All areas except:

- Medicine.
- State institutions.

Requirements:

- Zoom Revenue or 100k+.  
- 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 employees 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.
• 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:

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>REvil</th>
<th>Lockbit 2.0</th>
<th>DarkSide</th>
<th>BlackMatter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>RaaS</td>
<td>RaaS</td>
<td>RaaS</td>
<td>RaaS</td>
</tr>
<tr>
<td><strong>Network first</strong></td>
<td>-</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Multi-threaded</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>File encryption</strong></td>
<td>In-place</td>
<td>In-place</td>
<td>In-place</td>
<td>In-place</td>
</tr>
<tr>
<td><strong>Encrypt size</strong></td>
<td>Full</td>
<td>Partial, 4 KB</td>
<td>Partial, 512 KB</td>
<td>Partial, 1024 KB</td>
</tr>
<tr>
<td><strong>Rename</strong></td>
<td>After</td>
<td>After</td>
<td>Before</td>
<td>Before</td>
</tr>
<tr>
<td><strong>Decryption Blob</strong></td>
<td>End of File</td>
<td>End of File</td>
<td>End of File</td>
<td>End of File</td>
</tr>
<tr>
<td><strong>Wallpaper</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Encrypts Russian systems</strong></td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
BlackMatter Victim Geography, Industry, and Revenue Analysis

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.
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
Mitigations for BlackMatter Ransomware

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:

<table>
<thead>
<tr>
<th>DEFENSE / MITIGATION / COUNTERMEASURE</th>
<th>405(d) HICP REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide social engineering and phishing training to employees.</td>
<td>[10.S.A], [1.M.D]</td>
</tr>
<tr>
<td>Develop and maintain policy on suspicious e-mails for end users, and ensure suspicious e-mails are reported.</td>
<td>[10.S.A], [10.M.A]</td>
</tr>
<tr>
<td>Ensure emails originating from outside the organizations are automatically marked before being received.</td>
<td>[1.S.A], [1.M.A]</td>
</tr>
<tr>
<td>Apply patches/updates immediately after release/testing, develop/maintain the patching program if necessary.</td>
<td>[7.S.A], [7.M.D]</td>
</tr>
<tr>
<td>Implement spam filters at the email gateways, and keep signatures and rules updated.</td>
<td>[1.S.A], [1.M.A]</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>DEFENSE / MITIGATION / COUNTERMEASURE</th>
<th>405(d) HICP REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement whitelisting technology to ensure that only authorized software is allowed to execute.</td>
<td>[2.S.A], [2.M.A], [2.L.E]</td>
</tr>
<tr>
<td>Conduct system hardening to ensure proper configurations.</td>
<td>[7.S.A], [7.M.D]</td>
</tr>
<tr>
<td>Disable the use of SMBv1 (and all other vulnerable services and protocols) and require at least SMBv2. Restricting/Minimizing/eliminating RDP usage.</td>
<td>[7.S.A], [7.M.D]</td>
</tr>
</tbody>
</table>

Background information can be found here: [https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf](https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf)
Below are a sample of indicators of compromise (IOCs) from recent BlackMatter attacks:

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>598c53bfef81e489375f09792e487f1a</td>
<td>BlackMatter ransomware</td>
</tr>
<tr>
<td>a55bc3368a10ca5a92c1c9ecae97ced9</td>
<td>BlackMatter ransomware</td>
</tr>
<tr>
<td>ba375d0625001102fc1f2ccb6f582d91</td>
<td>BlackMatter ransomware</td>
</tr>
<tr>
<td>b06e2455a9c7c9485b85e9bdceeb8078</td>
<td>BlackMatter ransomware</td>
</tr>
<tr>
<td>605d939941c5df2df5dbfb8ad84cfed4</td>
<td>BlackMatter ransomware</td>
</tr>
<tr>
<td>3f9a28e8c057e7ea7ccf15a4db81f362</td>
<td>BlackMatter ransomware (Linux Variant)</td>
</tr>
<tr>
<td>paymenthacks[.]com</td>
<td>Command and Control (C2)</td>
</tr>
<tr>
<td>mojobiden[.]com</td>
<td>Command and Control (C2)</td>
</tr>
<tr>
<td>131.107.255[.]255</td>
<td>Command and Control (C2)</td>
</tr>
<tr>
<td>206.188.197[.]206</td>
<td>Command and Control (C2)</td>
</tr>
<tr>
<td>51.79.243[.]236</td>
<td>Command and Control (C2)</td>
</tr>
<tr>
<td>Bc1qlv2qdmlyuw62zw8qcd4n3uh84cy2edckv3ds7</td>
<td>Attacker Bitcoin address</td>
</tr>
</tbody>
</table>
Below are some basic MITRE ATT&CK® Techniques for BlackMatter Ransomware:

<table>
<thead>
<tr>
<th>Tactic</th>
<th>Technique ID</th>
<th>Technique Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Access</td>
<td>T1566</td>
<td>Phishing</td>
</tr>
<tr>
<td>Execution</td>
<td>T1204</td>
<td>User Execution</td>
</tr>
<tr>
<td>Discovery</td>
<td>T1082</td>
<td>System Information Discovery</td>
</tr>
<tr>
<td>Defense Evasion</td>
<td>T1497.003</td>
<td>Time-Based Evasion</td>
</tr>
<tr>
<td>Impact</td>
<td>T1490</td>
<td>Inhibit System Recovery</td>
</tr>
<tr>
<td></td>
<td>T1489</td>
<td>Service Stop</td>
</tr>
<tr>
<td></td>
<td>T1486</td>
<td>Data Encrypted for Impact</td>
</tr>
</tbody>
</table>

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](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:
  o IABs have been driven underground by law enforcement action.
  o Affiliates are leveraging multiple ransomware families to achieve goals.
  o Ransomware developers are rebranding to avoid law enforcement action.

• Threat to the HPH:
  o While there have not been any public healthcare victims yet, BlackMatter’s suspected predecessors targeted the healthcare sector.
  o HPH organizations should remain on alert despite the group’s claims to not target healthcare.
Reference Materials
References


References

References


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