JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA21-291A

October 18, 2021

BlackMatter Ransomware

SUMMARY

This joint Cybersecurity Advisory was developed by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) to provide information on BlackMatter ransomware. Since July 2021, BlackMatter ransomware has targeted multiple U.S. critical infrastructure entities, including two U.S. Food and Agriculture Sector organizations.

This advisory provides information on cyber actor tactics, techniques, and procedures (TTPs) obtained from a sample of BlackMatter ransomware analyzed in a sandbox environment as well from trusted third-party reporting. Using embedded, previously compromised credentials, BlackMatter leverages the Lightweight Directory Access Protocol (LDAP) and Server Message Block (SMB) protocol to access the Active Directory (AD) to discover all hosts on the network. BlackMatter then remotely encrypts the hosts and shared drives as they are found.

Ransomware attacks against critical infrastructure entities could directly affect consumer access to critical infrastructure services; therefore, CISA, the FBI, and NSA urge all organizations, including critical infrastructure organizations, to implement the recommendations listed in the Mitigations section of this joint advisory. These mitigations will help organizations reduce the risk of compromise from BlackMatter ransomware attacks.

Actions you Can Take Now to Protect Against BlackMatter Ransomware:

- Implement and enforce backup and restoration policies and procedures.
- Use strong, unique passwords.
- Use multi-factor authentication.
- Implement network segmentation and traversal monitoring.

Victims of ransomware should report it immediately to CISA at us-cert.cisa.gov/report, a local FBI Field Office, or U.S. Secret Service Field Office. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. For NSA client requirements or general cybersecurity inquiries, contact the NSA Cybersecurity Requirements Center at 410-854-4200 or Cybersecurity_Requests@nsa.gov.

This document was developed by CISA, the FBI, and NSA in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp/.

TECHNICAL DETAILS

Overview

First seen in July 2021, BlackMatter is ransomware-as-a-service (Raas) tool that allows the ransomware's developers to profit from cybercriminal affiliates (i.e., BlackMatter actors) who deploy it against victims. BlackMatter is a possible rebrand of DarkSide, a RaaS which was active from September 2020 through May 2021. BlackMatter actors have attacked numerous U.S.-based organizations and have demanded ransom payments ranging from $80,000 to $15,000,000 in Bitcoin and Monero.

Tactics, Techniques, and Procedures

This advisory provides information on cyber actor TTPs obtained from the following sample of BlackMatter ransomware, which was analyzed in a sandbox environment, as well as from trusted third parties: SHA-256: `706f3eec328e91ff7f66c8f0a2fb9b556325c153a329a2062dc85879c540839d`. (**Note**: click here to see the sample's page on VirusTotal.)

> This advisory uses the MITRE ATT&CK® framework, version 9. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques.

The BlackMatter variant uses embedded admin or user credentials that were previously compromised and `NtQuerySystemInformation` and `EnumServicesStatusExW` to enumerate running processes and services, respectively. BlackMatter then uses the embedded credentials in the LDAP and SMB protocol to discover all hosts in the AD and the `srvsvc.NetShareEnumAll` Microsoft Remote Procedure Call (MSRPC) function to enumerate each host for accessible shares. Notably, this variant of BlackMatter leverages the embedded credentials and SMB protocol to remotely encrypt, from the original compromised host, all discovered shares' contents, including `ADMIN$`, `C$`, `SYSVOL`, and `NETLOGON`.

BlackMatter actors use a separate encryption binary for Linux-based machines and routinely encrypt ESXI virtual machines. Rather than encrypting backup systems, BlackMatter actors wipe or reformat backup data stores and appliances.

Table 1 maps BlackMatter's capabilities to the MITRE ATT&CK for Enterprise framework, based on the analyzed variant and trusted third-party reporting.

Table 1: BlackMatter Actors and Ransomware TTPs

Tactic	Technique	Procedure
Persistence [TA0003]	External Remote Services [T1133]	BlackMatter leverages legitimate remote monitoring and management software and remote desktop software, often by setting up trial accounts, to maintain persistence on victim networks.

Tactic	Technique	Procedure
Credential Access [TA0006]	OS Credential Dumping: LSASS Memory [T1003.001]	BlackMatter harvests credentials from Local Security Authority Subsystem Service (LSASS) memory using `procmon`.
Discovery [TA0007]	Remote System Discovery [T1018]	BlackMatter leverages LDAP and SMB protocol to discover all hosts in the AD.
	Process Discovery [T1057]	BlackMatter uses `NtQuerySystemInformation` to enumerate running processes.
	System Service Discovery [T1007]	BlackMatter uses `EnumServicesStatusExW` to enumerate running services on the network.
Lateral Movement [TA0008]	Remote Services: SMB/Windows Admin Shares [T1021.002]	BlackMatter uses `srvsvc.NetShareEnumAll` MSRPC function to enumerate and SMB to connect to all discovered shares, including `ADMIN$`, `C$`, `SYSVOL`, and `NETLOGON`.
Exfiltration [TA0010]	Exfiltration Over Web Service [T1567]	BlackMatter attempts to exfiltrate data for extortion.
Impact [TA0040]	Data Encrypted for Impact [T1486]	BlackMatter remotely encrypts shares via SMB protocol and drops a ransomware note in each directory.
	Disk Wipe [T1561]	BlackMatter may wipe backup systems.

DETECTION SIGNATURES

The following Snort signatures may be used for detecting network activity associated with BlackMatter activity.

Intrusion Detection System Rule:

```
alert tcp any any -> any 445 ( msg:"BlackMatter remote encryption attempt";
content:"|01 00 00 00 00 00 05 00 01 00|";  content:"|2e 00 52 00 45 00 41 00 44
00 4d 00 45 00 2e 00 74 00|"; distance:100; detection_filter: track by_src, count
4, seconds 1; priority:1; sid:11111111111; )
```

Inline Intrusion Prevention System Rule:

```
alert tcp any any -> any 445 ( msg:"BlackMatter remote encryption attempt";
content:"|01 00 00 00 00 00 05 00 01 00|";  content:"|2e 00 52 00 45 00 41 00 44
00 4d 00 45 00 2e 00 74 00|"; distance:100; priority:1; sid:10000001; )

rate_filter gen_id 1, sig_id 10000001, track by_src, count 4, seconds 1,
new_action reject, timeout 86400
```

MITIGATIONS

CISA, the FBI, and NSA urge network defenders, especially for critical infrastructure organizations, to apply the following mitigations to reduce the risk of compromise by BlackMatter ransomware:

Implement Detection Signatures

- **Implement the detection signatures identified above**. These signatures will identify and block placement of the ransom note on the first share that is encrypted, subsequently blocking additional SMB traffic from the encryptor system for 24 hours.

Use Strong Passwords

- **Require all accounts with password logins (e.g., service account, admin accounts, and domain admin accounts) to have strong, unique passwords**. Passwords should not be reused across multiple accounts or stored on the system where an adversary may have access. **Note**: devices with local administrative accounts should implement a password policy that requires strong, unique passwords for each individual administrative account.

Implement Multi-Factor Authentication

- Require multi-factor authentication for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.

Patch and Update Systems

- **Keep all operating systems and software up to date**. Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats.

Limit Access to Resources over the Network

- **Remove unnecessary access to administrative shares**, especially `ADMIN$` and `C$`. If `ADMIN$` and `C$` are deemed operationally necessary, restrict privileges to only the necessary service or user accounts and perform continuous monitoring for anomalous activity.
- **Use a host-based firewall** to only allow connections to administrative shares via SMB from a limited set of administrator machines.

Implement Network Segmentation and Traversal Monitoring

Adversaries use system and network discovery techniques for network and system visibility and mapping. To limit an adversary from learning the organization's enterprise environment, limit common system and network discovery techniques by taking the following actions.

- **Segment networks** to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement.

- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.** To aid in detecting the ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.

Use Admin Disabling Tools to Support Identity and Privileged Access Management

If BlackMatter uses compromised credentials during non-business hours, the compromise may not be detected. Given that there has been an observed increase in ransomware attacks during non-business hours, especially holidays and weekends, CISA, the FBI, and NSA recommend organizations:

- **Implement time-based access for accounts set at the admin level and higher**. For example, the Just-in-Time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model). This is a process where a network-wide policy is set in place to automatically disable admin accounts at the AD level when the account is not in direct need. When the account is needed, individual users submit their requests through an automated process that enables access to a system, but only for a set timeframe to support task completion.
- **Disable command-line and scripting activities and permissions**. Privilege escalation and lateral movement often depend on software utilities that run from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally.

Implement and Enforce Backup and Restoration Policies and Procedures

- **Maintain offline backups of data**, and regularly maintain backup and restoration. This practice will ensure the organization will not be severely interrupted, have irretrievable data, or be held up by a ransom demand.
- **Ensure all backup data is encrypted, immutable** (i.e., cannot be altered or deleted) and covers the entire organization's data infrastructure.

CISA, the FBI, and NSA urge critical infrastructure organizations to apply the following additional mitigations to reduce the risk of credential compromise.

- **Disable the storage of clear text passwords in LSASS memory**.
- **Consider disabling or limiting New Technology Local Area Network Manager (NTLM)** and WDigest Authentication.
- **Implement Credential Guard** for Windows 10 and Server 2016 (Refer to Microsoft: Manage Windows Defender Credential Guard for more information). For Windows Server 2012R2, enable Protected Process Light for Local Security Authority (LSA).
- **Minimize the AD attack surface** to reduce malicious ticket-granting activity. Malicious activity such as "Kerberoasting" takes advantage of Kerberos' Ticket Granting service and can be used to obtain hashed credentials that attackers attempt to crack.

- Set a strong password policy for service accounts.
- Audit Domain Controllers to log successful Kerberos Ticket-Granting Service requests and ensure the events are monitored for anomalous activity.

Refer to the CISA-Multi-State information and Sharing Center (MS-ISAC) Joint Ransomware Guide for general mitigations to prepare for and reduce the risk of compromise by ransomware attacks.

Note: critical infrastructure organizations with industrial control systems/operational technology networks should review joint CISA-FBI Cybersecurity Advisory AA21-131A: DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks for more mitigations, including mitigations to reduce the risk of severe business or functional degradation should their entity fall victim to a ransomware attack.

RESPONDING TO RANSOMWARE ATTACKS

If a ransomware incident occurs at your organization, CISA, the FBI, and NSA recommend:

- **Following the Ransomware Response Checklist** on p. 11 of the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.
- **Scanning backups.** If possible, scan backup data with an antivirus program to check that it is free of malware.
- **Reporting incidents immediately** to the FBI at a local FBI Field Office, CISA at us-cert.cisa.gov/report, or the U.S. Secret Service at a U.S. Secret Service Field Office.
- **Applying incident response best practices** found in the joint Advisory, Technical Approaches to Uncovering and Remediating Malicious Activity, developed by CISA and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom.

Note: CISA, the FBI, and NSA strongly discourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or may fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered.

RESOURCES

- For more information and resources on protecting against and responding to ransomware, refer to StopRansomware.gov, a centralized, whole-of-government webpage providing ransomware resources and alerts.
- CISA's Ransomware Readiness Assessment (RRA) is a no-cost self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.
- CISA offers a range of no-cost cyber hygiene services to help critical infrastructure organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.

Note: the information you have accessed or received is being provided “as is” for informational purposes only. CISA, the FBI, and NSA do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA, the FBI, or NSA.