THREAT BULLETINS

BlackMatter Ransomware Joint Cybersecurity Advisory

TLP:WHITE

Oct 19, 2021

On October 18, 2021, a joint advisory was distributed via the efforts of Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) to provide information on BlackMatter ransomware. The advisory provides details on cyber actor tactics, techniques, and procedures (TTPs) derived from a sample of BlackMatter ransomware analyzed in a sandbox environment and other vetted sources.

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.

First seen in July 2021, BlackMatter is Ransomware-as-a-Service (Raas) tool that allows the ransomware's developers to profit from cybercriminal affiliates, or 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 US-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 sample below of BlackMatter ransomware, which was analyzed in a sandbox environment, as well as from trusted third parties:

SHA-256: 706f3eec328e91ff7f66c8f0a2fb9b556325c153a329a2062dc85879c540839d

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.

Additional Details:
For additional information including detection signatures, mitigations, and tips on how to respond to ransomware attacks, please see the full report available here.

Reference(s)	cisa, Bleeping Computer, Threat Post
Report Source(s)	CISA, FBI, NSA

Sources
Joint Cyber Security Alert – AA21-291A

FBI, CISA, NSA Share Defense Tips for BlackMatter Ransomware Attacks

Threatpost: Feds Warn BlackMatter Ransomware Gang is Poised to Strike

Alert ID da61e028

View Alert

Tags BlackMatter Ransomware, NSA, CISA, FBI

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**