BlackMatter, LockBit, and THOR

umbrella.cisco.com/blog/cybersecurity-threat-spotlight-blackmatter-lockbit-thor

November 18, 2021

Cisco Umbrella
Cybersecurity Threat Spotlight:
BlackMatter, LockBit, and THOR
Read the Article

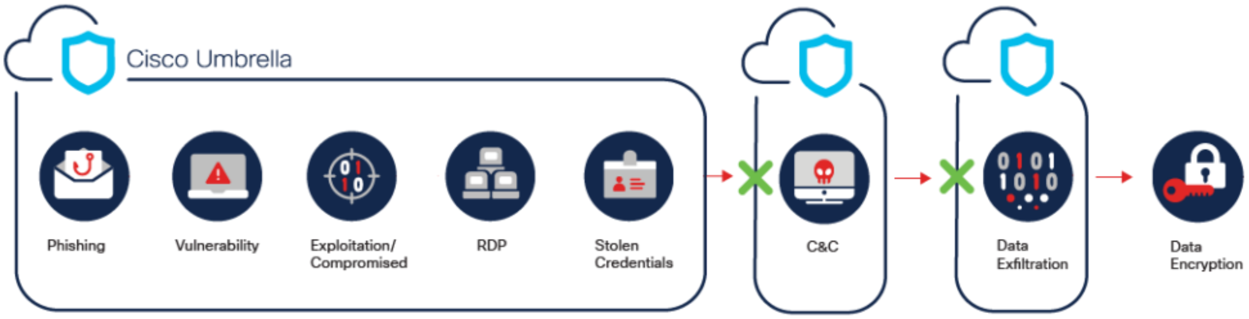
Ever wonder what happens when some of yesterday's most crippling ransomware or RAT attacks evolve? That's what we unpack in this month's Cybersecurity Threat Spotlight. Our three cyberattacks wreak havoc by borrowing some of the most effective techniques and tools formerly used by DarkSide, REvil, LockBit, and the PlugX RAT.

We break down this evolution in today's blog, and discuss the ways in which you can protect your network in an on-demand webinar.

Threat Name: BlackMatter

Threat Type: Ransomware

Attack Chain:



Description: BlackMatter ransomware is both a ransomware variant and a ransomware-as-a-service, borrowing techniques and tools from DarkSide and REvil RaaS platforms and from LockBit 2.0 ransomware. One interesting change in BlackMatter from similar variants is that it will encrypt Russian systems.

First appearing in July, 2021, BlackMatter appears to be the next generation of DarkSide, REvil, and LockBit 2.0, using the best techniques from each to be more effective at achieving its goals. The name BlackMatter applies to its operators, its use as a Ransomware-as-a-Service (RaaS), and the artifacts used in infections.

The operators have a presence on TOR, where they claim transparency with victims, recovery companies, and journalists while providing a list of verticals they do not target.

Many similarities between BlackMatter, DarkSide, REvil, and LockBit 2.0 exist. These include being provided as RaaS, multi-threading, in-place file encryption, and similar ransom desktop wallpaper on victim machines. Some of the notable differences with BlackMatter include a larger encryption size of 1,024 KB and the fact that it will encrypt Russian-language systems.

The ransom notes are similar to what has been observed in DarkSide infections in regard to file size, image format, and appearance. BlackMatter uses Initial Access Brokers, individuals or groups who are willing to sell access to compromised networks while also recruiting affiliates to deliver ransomware for a portion of the ransom payments. Variants exist for Windows and Linux, affecting Windows Server 2003 and later and Windows 7 and later on x86 and x64 architectures. Affected Linux versions include VMWare ESXI, Ubuntu, Debian, and CentOS.

Initial access is via compromised remote desktop, phishing, the use of stolen credentials, or exploitation of vulnerabilities in web browsers or operating systems. When a system is infected with BlackMatter, the privilege of the current user is verified and an attempt to escalate occurs. Processes are terminated to close any running programs that might prevent encryption of files, shadow volume copies are deleted, data is exfiltrated, and the files on the system are encrypted. During encryption, files are opened, checked to determine if they were already encrypted, renamed with a new extension, and partially encrypted. Then, data to indicate the file was encrypted is added and the file is closed. Access permissions for encrypted files are changed to ‘All’. Victims who choose to pay the ransom to recover files are unable to restore the original access permissions. If unable to run due to endpoint protection, BlackMatter will reboot a Windows system in safe mode. To inhibit analysis, string information in malware artifacts are encrypted and only decrypted while running in memory.

Target Geolocations: Any
Target Data: Any
Target Businesses: Financial, Legal, Manufacturing, Professional Services, Retail, Technology[1]
Exploits: Web Browser or OS Vulnerabilities

MITRE ATT&CK for BlackMatter
Initial Access: Phishing, External Remote Services
Persistence: Scheduled Task/Job
Evasion: Deobfuscate/Decode Files or Information, Obfuscated Files or Information, Process Injection: Dynamic-Link Library Injection
Collection: N/A
Exfiltration: Exfiltration Over Web Service, Transfer Data to Cloud Account, Exfiltration Over C2 Channel

IOCs

Domains:
kucukisletmeler[.]com
lentingbouw[.]nl
fluentzip[.]org
nowautomation[.]com
mojobiden[.]com
Paymenthacks[.]com

Additional Information:
BlackMatter ransomware emerges from the shadow of DarkSide
BlackMatter Ransomware Portal Tweet

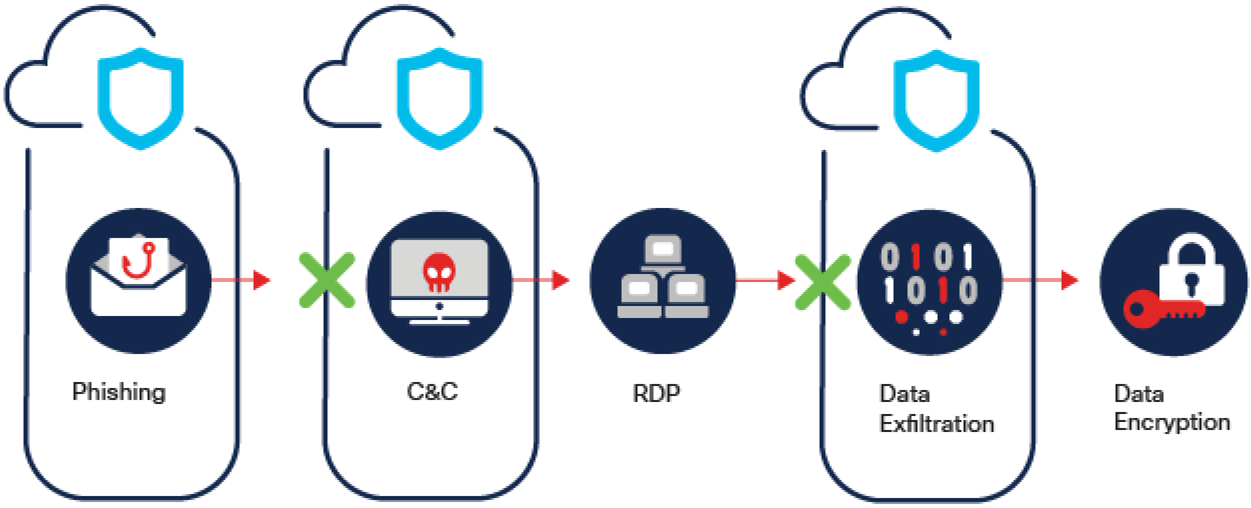
Which Cisco Products Can Block:
Cisco Secure Endpoint
Cisco Cloud Web Security
Cisco Network Security
Cisco Secure Network Analytics
Cisco Secure Cloud Analytics
Cisco Secure Malware Analytics
Cisco Umbrella
Cisco Secure Web Appliance

[1] These target businesses were identified by BlackMatter operators, but this attack may target other businesses

Threat Name: LockBit

Threat Type: Ransomware

Attack Chain:



Description: LockBit ransomware was first seen in 2019. A second version, called LockBit 2.0, appeared in July, 2021 and operates as ransomware-as-a-service (RaaS). It shares features with Ryuk and Egregor ransomware families, such as Wake-on-LAN and Print Bombing (sending the ransom note to connected printers). LockBit operators use double-extortion methods and attempt to recruit affiliates from within the targeted organizations. Automatic encryption on victim systems occurs across Windows domains by abusing Active Directory policies. LockBit uses multithreading for encryption and only partially encrypts files to increase speed.

Originally known as the .abcd virus, the first version of LockBit was able to self-replicate, performed host discovery using ARP tables, and would move laterally by exploiting SMB on Windows systems. It would spread via PowerShell and avoided encrypting Russian-language systems.

A new version of LockBit, called LockBit 2.0, began appearing in late 2019. The wallpaper that was set on victim systems would attempt to recruit internal affiliates or members of the victim organization to help further the infection and provide additional data for exfiltration in exchange for payment. LockBit 2.0 also attempted to recruit outside affiliates by advertising faster encryption speed than the first version of LockBit as well as other Ransomware variants. Delivery is typically via phishing, where a dropper is installed. C2 communication begins shortly after and additional tools are downloaded. Data exfiltration then occurs, followed by data encryption.

Once LockBit is installed on a system, Cobalt Strike and remote access tools are also installed. Some of these tools are legitimate, which helps to avoid detection. Data is then exfiltrated for additional ransom if payment is not made. LockBit 2.0 samples employ anti-analysis techniques similar to BlackMatter, where strings are encrypted until runtime. Shadow volume copies are deleted on victim systems prior to encryption. When encrypting files, the extension is changed to .lockbit and a custom icon is set to display for that file type. It then looks for connected drives and network volumes, creates a ransom note in all directories, encrypts the files, and changes the desktop background to a ransom message. One of the final steps is to print the ransom note to any connected printers.

Target Geolocations: Asia, North America, South America, Europe
Target Data: Any
Target Businesses: Any
Exploits: N/A

MITRE ATT&CK for LockBit
Initial Access: Unconfirmed
Persistence: Registry Run Keys / Startup Folder
Evasion: Virtualization/Sandbox Evasion
Collection: Data From Local System
Exfiltration: Exfiltration Over Command and Control Channel

IOCs

Domains:
None

IPs:
139.60.160[.]200
168.100.11[.]72
174.138.62[.]35
185.215.113[.]39
193.162.143[.]218
193.38.235[.]234
45.227.255[.]190
88.80.147[.]102
93.190.143[.]101

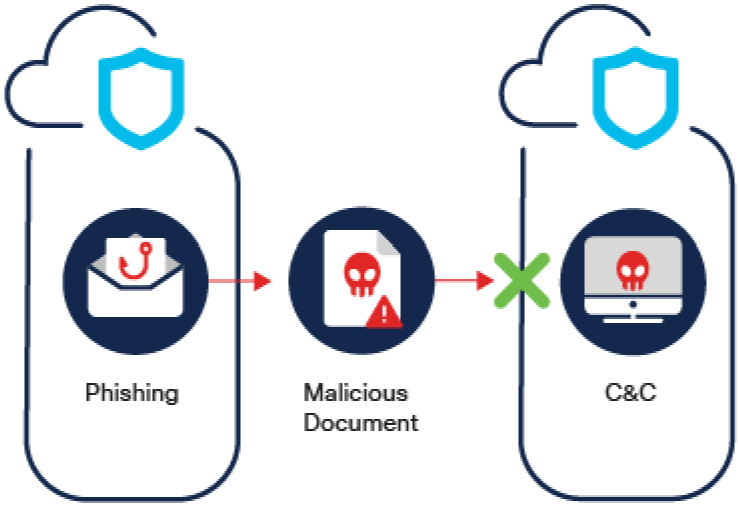
Additional Information:
[LockBit ransomware now infects Windows domains using group policies]
[LockBit Resurfaces With version 2.0 Ransomware Detections in Chile, Italy, Taiwan, UK]

Which Cisco Products Can Block:
Cisco Secure Endpoint
Cisco Cloud Web Security
Cisco Network Security
Cisco Secure Network Analytics
Cisco Secure Cloud Analytics
Cisco Secure Malware Analytics
Cisco Umbrella
Cisco Secure Web Appliance

Threat Name: THOR

Threat Type: RAT

Attack Chain:



Description: THOR is a variant of the PlugX Remote Access Tool (RAT). PlugX RATs have been in use since 2008 and have the ability to upload, download, and modify files, perform keystroke logging, webcam control, and provide access to a remote shell. THOR is unique from previous PlugX variants in that it changed the word ‘PLUG’ to ‘THOR’ in its source code. It is further differentiated from past PlugX RATs by its use of modified payload delivery mechanisms and the use of trusted binaries on a victim system to accomplish its goals. It first appeared in March, 2021 as part of an attack on Exchange Servers via CVE-2021-26855 and CVE-2021-27065.

THOR Spotlight: THOR is a new variant of the PlugX malware, which has been involved in targeted attacks and intrusions since 2008. PlugX is often installed as a second-stage implant following the initial infection. It’s built for modular use, allowing the use of plug-ins to achieve specific objectives. Delivery is via malicious documents in phishing emails and C2 communication occurs after infection. Additional components may be downloaded after communication begins.

In March of 2019, two zero-day exploits (CVE-2021-26855 and CVE-2021-27065) were discovered affecting Microsoft Exchange Servers. These exploits were used to upload a webshell to a publicly accessible web directory, allowing code execution, the ability to write malicious files to any path, run commands, escalate privilege, and allow remote access. In the attacks, a variant of PlugX was being used to install a remote access tool. This variant had a modification in its source code, changing a well-known variable name from PLUG to THOR.

When run, a legitimate Windows binary is used to download a dropper, which is designed to remain undetected and can only be run with a specific loader. All variants of PlugX require the use of DLL side-loading to run. The downloaded dropper has its first 1000 bytes filled with random padding until it has a NULL byte, signaling the beginning of the file. When loaded into memory, the code unpacks and communication with a command and control (C2) server begins.

When running, THOR behaves the same as previous PlugX variants, decrypting hard-coded and embedded configuration settings. Communication with the C2 server is over ports 80, 443, 53, and 8000 using UDP and TCP. While the first handshake with the C2 looks like HTTP data, it is made of random bytes with variable lengths. If the return value from the C2 is the correct length, actual HTTP communication between the victim and C2 starts. Various values in the C2 traffic are hard-coded, such as the user-agent and a known PlugX constant. When installation is complete, a Windows system service named HP Digital Image is created and system events are logged to a hidden file labeled NTUSER.dat. The MZ and PE headers of the running module are removed and replaced with ROHT, which is THOR written backwards.

The primary goals of THOR and other PlugX variants are to monitor, make changes, and interact with the system, as well as to install additional malware.

Target Geolocations: Myanmar, Taiwan, Vietnam, Indonesia, Mongolia, Tibet, Xinjiang
Target Data: Any
Target Businesses: Any
Exploits: CVE-2021-26855, CVE-2021-27065

MITRE ATT&CK for THOR
Initial Access: Spearphishing Attachments, Malspam
Persistence: Server Software Component

Evasion: Deobfuscate/Decode Files or Information, Hide Artifacts
Collection: Audio Capture, Clipboard Data, Input Capture, Screen Capture, Video Capture
Exfiltration: Exfiltration Over Command and Control Channel

IOCs

Domains:
apple-net[.]com
destroy2013[.]com
emicrosoftinterview[.]com
fitehook[.]com
flashplayerup[.]com
indonesiaport[.]info
manager2013[.]com
rainydaysweb[.]com
upload.ukbbcnews[.]com

IPs:
185.239.226[.]65
45.251.240[.]55
58.158.177[.]102

Additional Information
THOR: Previously Unseen PlugX Variant Deployed During Microsoft Exchange Server Attacks by PKPLUG Group
PKPLUG: Chinese Cyber Espionage Group Attacking Southeast Asia
Take a Deep Dive into PlugX Malware

Which Cisco Products Can Block:
Cisco Secure Endpoint
Cisco Cloud Web Security
Cisco Network Security
Cisco Secure Network Analytics
Cisco Secure Cloud Analytics
Cisco Secure Malware Analytics
Cisco Umbrella
Cisco Secure Web Appliance