Mphasis
The Next Applied

BlackCat/ALPHV Ransomware Advisory

Severity: High

Date: 17th April 2023

Description

The ALPHV ransomware group (AKA BlackCat) was first observed by cybersecurity researchers in November 2021. The group targets victims from various countries, such as the United States, Australia, and India, the ransomware operators are Russian speakers. In February 2022, one of the group members confirmed that ALPHV consists of former members of the BlackMatter ransomware group (formerly DarkSide). This gang is also named as AlphaVM, AphaV, BlackCat, BlackCat Hand, Noberus.

How it works

The ransomware, written in Rust, is distributed in a ransomware-as-a-service (RaaS) model, in which affiliates who operate it earn 80-90% of the ransom fee. It is command-line driven, highly configurable, and has various unique capabilities, such as using different encryption methods, terminating virtual machines and ESXi VMs, and deleting ESXi snapshots to prevent recovery. In addition, the malware can delete Volume Shadow Copies and scan for other network devices. The ransomware executable includes a JSON configuration that enables the customization of extensions, ransom notes, encryption methods, excluded file and folder extensions, and more.

ALPHV's encryption process follows the normal routine of appending a new, random extension to the encrypted files and dropping a ransom note in the format of "RECOVER-[extension]-FILES.txt." The file extension can also be configured with the domain credentials. The ransom notes are changed by the operating affiliate and are different for each victim. Some of the notes include links to Tor leak sites which can also be unique per victim. The ransom demand usually ranges between 400,000 and 3,000,000 dollars, in Bitcoin or Monero. However, ALPHV's affiliates were observed to ask for ransom amounts of up to 14 million dollars.

The group uses the double-extortion method of stealing the data before the encryption and threatening to publish it in case the ransom is not paid. The extortion method can also be tripled when the threat actors threaten to perform DDoS attacks until the ransom is paid. To avoid third-party analysis, the negotiation chats can only be accessed by those holding an access token key or ransom note.

ALPHV is a highly sophisticated ransomware group that was created to fill the void left by the BlackMatter and REvil groups that halted their operations due to law enforcement activities.

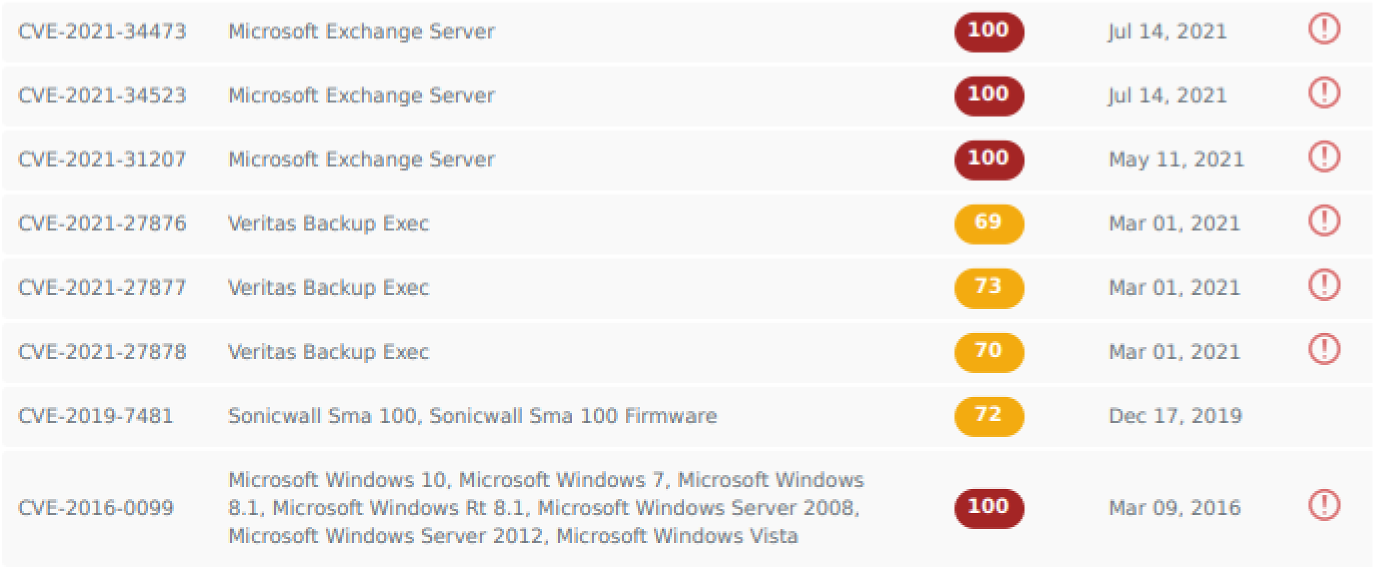
Commonly used tools: PsExec, CobaltStrike, Mimikatz, WebBrowserPassView, Koadic, Empire, LaZagne

There are many organizations which are affected because of this ransomware gang one of them is a US-based software and technology consulting company, NCR, disclosed an outage on its Aloha point of sale (POS) platform following a ransomware attack, later claimed by ALPHV. The outage caused significant disruptions to Aloha POS hospitality customers, with some being forced to move to manual work. ALPHV claimed to steal credentials of NCR's customers and threatened to leak them if the ransom is not paid.

Targeted Industries

Education, Energy, Food & Beverage, Government, Insurance, Materials & Construction, Metals & Mining, Pharmaceuticals, Retail, Telecommunications, Transportation, Automotive, Healthcare, Manufacturing.

Related CVEs:



CVE-2021-34473	Microsoft Exchange Server	100	Jul 14, 2021	❗
CVE-2021-34523	Microsoft Exchange Server	100	Jul 14, 2021	❗
CVE-2021-31207	Microsoft Exchange Server	100	May 11, 2021	❗
CVE-2021-27876	Veritas Backup Exec	69	Mar 01, 2021	❗
CVE-2021-27877	Veritas Backup Exec	73	Mar 01, 2021	❗
CVE-2021-27878	Veritas Backup Exec	70	Mar 01, 2021	❗
CVE-2019-7481	Sonicwall Sma 100, Sonicwall Sma 100 Firmware	72	Dec 17, 2019	
CVE-2016-0099	Microsoft Windows 10, Microsoft Windows 7, Microsoft Windows 8.1, Microsoft Windows Rt 8.1, Microsoft Windows Server 2008, Microsoft Windows Server 2012, Microsoft Windows Vista	100	Mar 09, 2016	❗

Mitigation

- Back-up critical data.
- Secure back-ups and ensure data are not accessible for modification or deletion from the system where the data resides.
- Use multi-factor authentication with strong passwords, including for remote access services.
- Keep computers, devices, and applications patched and up to date.

Indicators of compromise

ALPHV_Blackcat IOCs.xlsx

Please block the IOCs at respective controls.

- Hash values at Endpoint security,
- IP addresses at firewalls for both inbound and outbound communication
- Domains and URLs at proxy level.

Reference Links

https://www.bleepingcomputer.com/news/security/ncr-suffers-aloha-pos-outage-after-blackcat-ransomware-attack/amp/

https://www.varonis.com/blog/blackcat-ransomware

https://www.securityweek.com/payments-giant-ncr-hit-by-ransomware/

https://siliconangle.com/2023/04/17/ransomware-attack-causes-outages-payments-giant-ncr/