Quorum
Cyber

Threat Intelligence
ALPHV
Ransomware

TLP Status: CLEAR

☎ +44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Table of Contents

Document Control

Revision History

Version	Date	Summary of Changes
0.1	19/06/2023	Initial Report Drafted.
1.1	04/08/2023	PDF Formatting

Related Documents

The following documents are either referenced within, or are related to, the content of this document:

Document Name	Date	Version
	dd/mm/yyyy	

ALPHV Ransomware

Overview

The ALPHV ransomware (also known as BlackCat) operator is a financially motivated threat actor group that has been active since at least 2016. The group employs the double-extortion technique, threatening to leak stolen data to persuade victims to pay the ransom and has targeted various industry sectors, including manufacturing, finance, healthcare, law, and media. The group has been successful in extorting large ransom payments, with a reported average payment of US$1.7 million. As such, the ALPHV ransomware group is currently one of the leading ransomware actors, and it is highly likely that their operations will continue.

The group has been observed using different versions of the Sardonic backdoor to deploy the ALPHV ransomware. The Sardonic backdoor is a powerful malware that can exfiltrate system data, execute commands, and load and execute additional malware payloads. The group has also been associated with other ransomware variants such as Ragnar Locker and White Rabbit. The malware is typically distributed through malvertising campaigns, using tricks to distribute rogue installers of legitimate applications, such as WinSCP[1].

It was detected in July 2023 that the threat actor, tracked as FIN8, was involved in an attack campaign that involved the deployment of ALPHV ransomware via an enhanced rendition of the Sardonic backdoor[2].

Impact

Successful exploitation by ALPHV ransomware will almost certainly result in the encryption and exfiltration of significant quantities of data held on the compromised system, prior to a ransom of a predetermined value being issued. The ransom amount demanded will almost certainly depend on the estimated value of the compromised organisation. Furthermore, such a compromise of data will also result in the organisation incurring a negative reputational impact. Encrypted data may include private customer data, corporate finance data and system credentials that if released can assist threat actors with future attacks.

Incident Detection

A comprehensive endpoint detection and response (EDR) solution, such as Microsoft Defender, can provide additional protection against ransomware threats like that implemented by ALPHV ransomware. EDR solutions can alert system users of potential breaches and stop further progress before the malware can do significant damage.

Targeted Products

- Windows OS

[1] Malvertising Used as Entry Vector for BlackCat Actors Also Leverage SpyBoy Terminator (trendmicro.com)

[2] FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware | Symantec Enterprise Blogs (security.com)

Containment, Mitigations & Remediations

As mentioned previously, a primary method of reducing the threat of ALPHV ransomware is to detect it in the early stages through the use of an effective and monitored EDR solution. An effective EDR tool such as the Microsoft Defender suite will block ransomware attempts once detected.

Organisations can also perform routine back-ups of sensitive data that is required for business operations and to keep a copy offline in case back-ups are impacted by the attack. Therefore, if a breach occurs and the business can no longer function, a back-up is ready to use, and the business can continue to operate with minimal disruption.

Indicators of Compromise

ALPHV Associated File Hashes (SHA-256):

- 0c6f444c6940a3688ffc6f8b9d5774c032e3551ebbccb64e4280ae7fc1fac479
- 15b57c1b68cd6ce3c161042e0f3be9f32d78151fe95461eedc59a79fc222c7ed
- 1af1ca666e48afc933e2eda0ae1d6e88ebd23d27c54fd1d882161fd8c70b678e
- 28d7e6fe31dc00f82cb032ba29aad6429837ba5efb83c2ce4d31d565896e1169
- 2cf54942e8cf0ef6296deaa7975618dadff0c32535295d3f0d5f577552229ffc
- 3d7cf20ca6476e14e0a026f9bdd8ff1f26995cdc5854c3adb41a6135ef11ba83
- 4e18f9293a6a72d5d42dad179b532407f45663098f959ea552ae43dbb9725cbf
- 5121f08cf8614a65d7a86c2f462c0694c132e2877a7f54ab7fcefd7ee5235a42
- bd337d4e83ab1c2cacb43e4569f977d188f1bb7c7a077026304bf186d49d4117
- c3e5d4e62ae4eca2bfca22f8f3c8cbec12757f78107e91e85404611548e06e40
- f837f1cd60e9941aa60f7be50a8f2aaaac380f560db8ee001408f35c1b7a97cb
- 1e226d4f14a0a8718df742a8abae6d1527717ff9ef065b5be878cf8bd20d5899
- 32304c278117353bd112132323055e113b62182d1efcc83abec1e736cf8da9e1
- 99c71640bc985654db23b81ecb00e4d0cc160a25e1c58b6a90e379a559ea3440
- e55cc3426298f9f848849304d10b9222925eb19caebaebaa44dfb85ad2346062
- 1fd42d07b4be99e0e503c0ed5af2274312be1b03e01b54a6d89c0eef04257d6e
- 4fea41b61b2bd700fc6613c18c05aeb4df37bcbe777868081b0ed1076ee7aacb
- 87b02f674aa5b0c2b0e7f639b9c2e29446d0f90e9da082c2b219f42eeaed6736
- 8a22a91c931ac80ca91cf91fef678c4bee00e3eb5ad24f209bc8595e012ba5b0
- 94e56379b7a31b01cf826076a74fc4ddb7f86f7991a6f58300f28712d484aa33

ALPHV Associated IP Addresses:

- 185[.]220[.]102[.]253
- 146[.]0[.]77[.]15
- 45[.]153[.]160[.]140
- 142[.]234[.]157[.]246
- 152[.]89[.]247[.]207
- 198[.]144[.]121[.]93
- 23[.]106[.]223[.]97
- 45[.]134[.]20[.]66
- 89[.]163[.]252[.]230
- 89[.]44[.]9[.]243
- 94[.]232[.]41[.]155

ALPHV Associated URLs:

- hxxp[://]185[.]220[.]102[.]253/
- hxxp[://]142[.]234[.]157[.]246/
- hxxp[://]146[.]0[.]77[.]15/
- hxxp[://]152[.]89[.]247[.]207/
- hxxp[://]198[.]144[.]121[.]93/
- hxxp[://]23[.]106[.]223[.]97/
- hxxp[://]45[.]134[.]20[.]66/
- hxxp[://]45[.]153[.]160[.]140/
- hxxp[://]89[.]163[.]252[.]230/
- hxxp[://]89[.]44[.]9[.]243/
- hxxp[://]94[.]232[.]41[.]155/

Threat Group

The ALPHV ransomware group has been active since at least 2016 and is financially motivated. The group has been observed using additional ransomware variants, including Ragnar Locker and White Rabbit. The group targets a wide range of sectors, including manufacturing, healthcare, finance, law, and hospitality. It employs tactics such as malvertising campaigns, phishing, and exploiting vulnerabilities in software applications to gain initial access. They also utilise the double-extortion technique of threatening to leak stolen data to persuade organisations to pay the ransom. Recent events include attacks on various organisations, such as Beverly Hills Plastic Surgery, Eisai and Estee Lauder, resulting in data theft and disruption to business operations. The group has been listed as a prominent recipient of high-range ransom payments, with an average payment size of US$1.7 million.

It was detected in July 2023 that the threat actor, tracked as FIN8, was involved in an attack campaign that involved the deployment of ALPHV ransomware via an enhanced rendition of the Sardonic backdoor. This new version of Sardonic has altered features to avoid detection. FIN8 is a threat actor group that is primarily financially motivated and has recently pivoted to ransomware as a main payload variant. Due to the success of the recent campaign, it is likely that FIN8 will continue to deploy ALPHV ransomware within their attack chain.

Threat Landscape

Ransomware continues to be one of the prominent threats facing the private sector. Recent attacks and the developing nature of the ransomware threat landscape suggests that the threat is growing as criminal groups are becoming more comfortable demanding ever-increasing ransom fees.

Due to the significant number of targets within the first two months of its existence, it is likely that ALPHV ransomware will continue to exploit victims at a high frequency and as such will emerge into an increasingly notorious ransomware strain.

Mitre Methodologies

Execution

T1106 - Native API[3]

Command and Control

T1071.001 - Application Layer Protocol: Web Protocols[4]

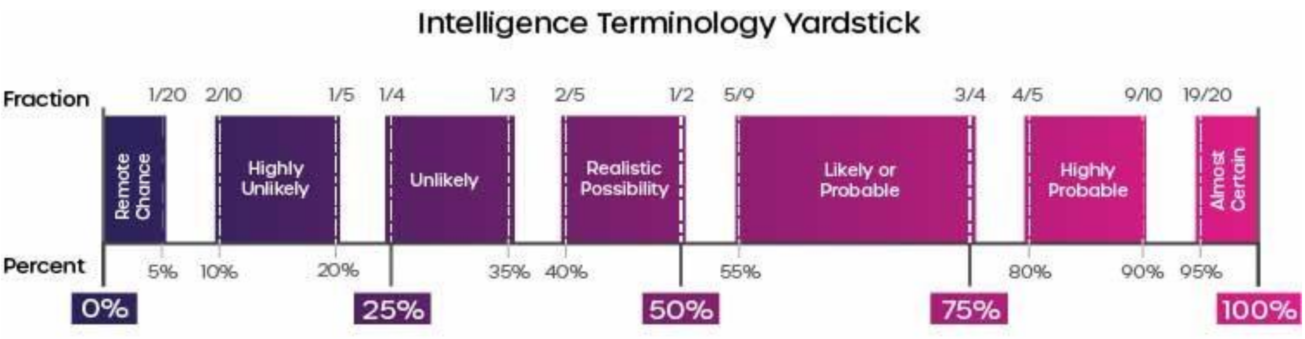
Further Information

- Trend Micro ALPHV Ransomware Analysis

[3] Native API, Technique T1106 - Enterprise | MITRE ATT&CK®

[4] Application Layer Protocol: Web Protocols, Sub-technique T1071.001 - Enterprise | MITRE ATT&CK®

Intelligence Cut-off Date (ICoD): 04/08/2023 10:00 UTC



Intelligence Terminology Yardstick

This threat report uses pre-defined language found within the Intelligence Terminology Yardstick to express the likelihood of events