Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

HavanaCrypt ransomware spreads through fake google updates

Date of Publication	Last Updated	TA Number
July 13, 2022	A1	TA2022144

Summary

HavanaCrypt is a new ransomware that distinguishes itself as a Google software update. It evades detection using a Microsoft web hosting service IP address as the command-and-control (C&C) server.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	**T1027** Obfuscated Files or Information	**T1497** Virtualization/Sandbox Evasion	**TA0010** Exfiltration
T1041 Exfiltration Over C2 Channel			

Technical Details

#1 HavanaCrypt Ransomware is a .Net malware, which distinguishes itself as a google software update application. This malware uses Microsoft web hosting service IP address as the command-and-control (C&C) server to evade detection. It has anti virtualization techniques to hide from dynamic analysis as well as using an open-source tool 'obfuscar' to obfuscate the code.

#2 The malware uses four steps to check whether the machine is a virtual machine or not. If it's not a virtual machine, it downloads a text file from C2 server and saves it as a batch file. The batch file contains commands for configuring windows defender and allow detected threats.

#3 The malware can terminate processes that include database related applications. Additionally, it collects machine information and sends it to the C2 server. Lastly, it encrypts files and adds extension as ".Havana".

Indicator of Compromise (IOC)

TYPE	VALUE
SHA-256	B37761715d5a2405a3fa75abccaf6bb15b7298673aaad91a158725be3c518a87 Bf58fe4f2c96061b8b01e0f077e0e891871ff22cf2bc4972adfa51b098abb8e0 aa75211344aa7f86d7d0fad87868e36b33db1c46958b5aa8f26abefbad30ba17
URL	http://20[.]227[.]128[.]33/2.txt http://20[.]227[.]128[.]33/index.php http://20[.]227[.]128[.]33/ham.php

References

https://www.trendmicro.com/en_us/research/22/g/brand-new-havanacrypt-ransomware-poses-as-google-software-update.html

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

July 13, 2022 • 1:10 AM

More at www.hivepro.com