Hermes Ransomware Cyber Report

Overview

Hermes is a ransomware family that was first detected in February 2017. While the initial version of Hermes was quickly reverse engineered, subsequent versions, including the latest (version 2.1) from February 2018, are still being observed in the wild and continue to pose a threat. In the week of 23-27 July, Infoblox observed an influx of spam emails delivering malicious Microsoft Word documents that downloaded Hermes 2.1 via the AZORult trojan.

Customer Impact

As with other variants of ransomware, Hermes encrypts a user's files so that they cannot be recovered without contacting the attacker for a decryption key. The ransom note that we reviewed did not request a specific payment amount; however, other reports on Hermes claim a typical ransom is between $500 and $1500.[1] Whereas earlier Hermes encryption was relatively easy to decrypt, files encrypted by version 2.1 cannot be decrypted with third-party tools.

According to a report from Cybersecurity Ventures, the total costs to business from ransomware exceeded $5 billion in 2017.[2] The impacts range from direct losses to workday disruptions and damage to reputations. A breach of the Taiwanese Far Eastern International Bank last year included Hermes as a tool to destroy evidence following earlier data theft and fraudulent transfers.[3]

Campaign Analysis

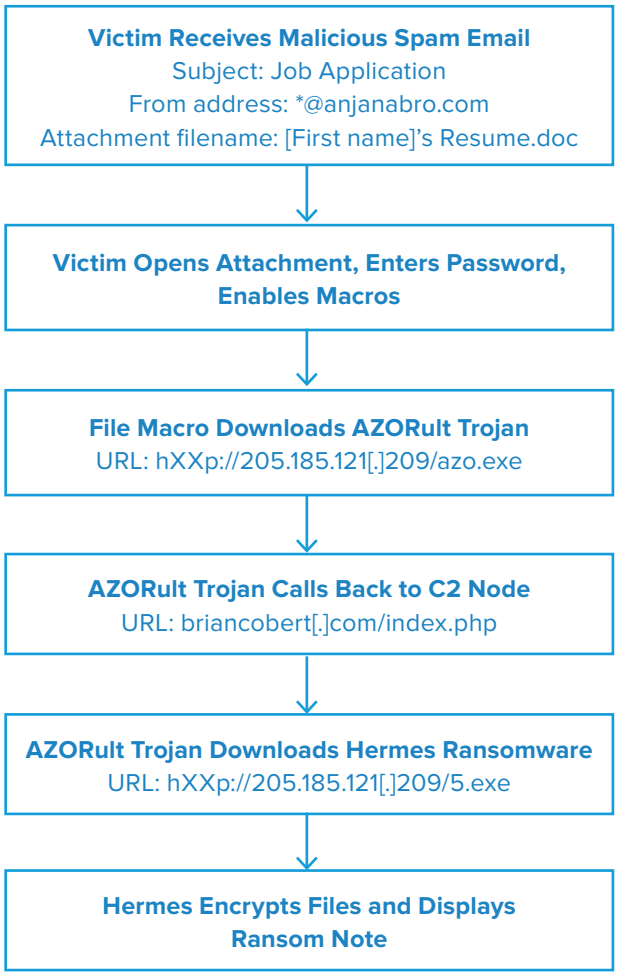
In this campaign, email messages claim to come from job applicants searching for employment. Each message contains the subject "Job Application" and is sent from an email address on the domain anjanabro[.]com. The email contains instructions for the recipient to open the attached file (purportedly a resume), and enter the password included in the body of the message.

Once the user opens the malicious file, it displays a warning that its content cannot be viewed until the recipient enables macros for the document. After macros are enabled, the document downloads additional files that will infect the recipient's device.

The initial payload that we observed in this campaign is the AZORult trojan. Once it has been dropped, the infected machine reaches out to a command and control (C2) server and downloads Hermes, the secondary payload.

Hermes begins surreptitiously encrypting all the files on the machine. Upon completion, it displays a ransom note with instructions to contact the attacker and pay them a ransom in Bitcoin to recover the files.

Attack Chain



Vulnerabilities & Mitigation

Hermes employs social engineering to spread malspam related to fake job applications. Educating users on the dangers posed by malspam and ransomware is crucial to limiting its success and impact. Also, regularly backing up data and systems will minimize the potential impact of ransomware in general. To avoid these infections, users should:

- Always be suspicious of unexpected emails and unknown senders.
- Always be suspicious of vague emails, especially when there is a prompt to open an attachment.
- Do not open unexpected attached files and do not enable macros, particularly those in Microsoft Office products. Macros are a very common infection vector used by many families of malware.
- Always stay up-to-date with the latest security patches.

Appendix

Representative Indicators of Compromise	Description
Subject: Job Application From address: *@anjanabro.com Attachment filename: [First name]'s Resume.doc (password protected)	Email characteristics
hXXp://205.185.121[.]209/azo.exe	AZORult trojan download URL
briancobert[.]com/index.php	AZORult C2 server
hXXp://205.185.121[.]209/5.exe	Hermes ransomware download URL
decryptsupport@protonmail.com decryptsupport1@cock.li	Ransom contact information

Endnotes

1. https://www.pcrisk.com/removal-guides/13175-hermes-21-ransomware
2. https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/
3. ttps://www.bleepingcomputer.com/news/security/north-korean-hackers-used-hermes-ransomware-to- hide-recent-bank-heist/

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com