David Scott - Google Cybersecurity Course - Incident Handler’s Journal Portfolio Piece

Incident handler's journal

Scenario 1

A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job.

Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key.

The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded.

Once the attackers gained access, they deployed their ransomware, which encrypted critical files. The company was unable to access critical patient data, causing major disruptions in their business operations. The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance.

Date: December 5, 2023	**Entry:** 0001
Description	Medical facility suffering a ransomware attack.
Tool(s) used	None
	At 9:00 AM, employees discovered they were unable to access business files including customer information. The files were found to be encrypted along with a ransomware message from known threat actor Crystal Tornado (Microsoft designation), seeking a sum of money.

	The preceding day an employee had received a phishing email containing a malicious link. Clicking on the link allowed Crystal Tornado access to the systems and to install the encryption malware.
Additional notes	● Does the facility have pertinent back-ups which can be used to restore the systems? ● Does the facility use proper authorization techniques? ● Has the staff had cybersecurity training courses?

Scenario 2

You are a level one security operations center (SOC) analyst at a financial services company. You receive an alert about a suspicious file being downloaded on an employee's computer.

You investigate and discover the employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was executed on their computer.

Date: December 7, 2023	**Entry:** 002
Description	Probably malicious email attachment
Tool(s) used	SHA256 hash, Virus Total
The 5 W's	– 1:11 p.m.: An employee received an email containing a spreadsheet attachment along with a password. – 1:13 p.m.: The employee successfully downloads and opens the file. – 1:15 p.m.: Multiple unauthorized executable files are created on the employee's computer. – 1:20 p.m.: An IDS detects the executable files and sends an alert to the SOC.

	I retrieved the file and created a SHA256 hash (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b). Virus Total investigation reveals the file to a backdoor trojan called Flagpro used by the threat actor BlackTech with a high confidence rate.
Additional notes	Block org.misecure.com and IP address 207.148.109.242