Design by Paradigm | Incident Reporting Template

By Jordan Biggs

SECTION A: INCIDENT DETAILS	
Incident number(s):	HDE-1001,HDE-1050,HDE-1072
Incident date(s):	13 Dec 10:00 am, 13 Dec 3:14 pm, 13 Dec 3:20 pm
Report author:	WGU student ID: 012678994
Report date:	December 1st
Summary of incident:	The engineering application server has had unusually high GPU & CPU usage. The affected users have not been able to update models using the CAD Application (Pro-Engineer)
Impacted system(s):	WIN-6JNN6RLT6IL
Primary function of the impacted system(s):	Update models
Impacted user(s):	Maya Patel, Diego Martin, Alex Lee
Incident timeline:	13 Dec 10:00 am, 13 Dec 3:14 pm, 13 Dec 3:20 pm
Functional impact: (*See section: Glossary*)	☒HIGH ☐MEDIUM ☐LOW ☐NONE
Incident priority:	☒HIGH ☐MEDIUM ☐LOW
Additional notes:	An affected user stated that, application will run slowly & time out. Another affected user stated that the issue isn't machine or file-specific.

Incident type: (*check all that apply*)

☒Compromised system	☐Lost equipment/theft
☐Compromised user credentials *(e.g., lost password)*	☐Physical break-in
	☐Social engineering *(e.g., phishing)*
☐Network attack *(e.g., DoS)*	☐Law enforcement request
☐Malware *(e.g., virus, worm, Trojan)*	☐Policy violation *(e.g., acceptable use)*
☐Reconnaissance *(e.g., scanning, sniffing)*	☐Other: Click or tap here to enter text.

SECTION B: DETECT	
Hostname of the impacted system(s):	WIN-6JNN6RLT6IL
IP address of the impacted system(s):	10.10.20.10
Operating system of the impacted system(s):	Windows Server 2019

SECTION C: INVESTIGATE	
Destination port of malicious traffic:	3333
Additional notes & observations:	Attacks happened on Nov 28 17:35:33, Nov 28 17:35:30, Feb 8 10:17:03 The application that uses the most CPU is XMRig Miner. Which is a crypto miner application

SECTION D: REMEDIATE	
Summary of actions taken to restore functionality of impacted system(s):	Turned Windows defender back on
Summary of actions taken to restore network security:	After finding the miner using Quick scan, I selected the remove action to rid the compromised device of the crypto miner.
Additional notes & observations:	A new firewall rule was added to the DMZ, which blocked the traffic coming and going to port 3333

SECTION E: LESSONS LEARNED

Recommendation for preventative actions:	**ACTION**	**NEGATIVE IMPACT ADDRESSED**	**PREVENTION METHOD**
	1. Turn on Windows Defender antivirus	Allowed the removal of malicious software	Check to ensure that Windows Defender antivirus isn't turned on
	2. Configure DMZ firewall rules	Blocked malicious traffic	Ensure that only necessary ports are open
	3.		
	4.		

PART G: Sources

Background Information.pdf

Glossary

Functional Impact

Functional impact categories to prioritize resources in incident response:

CATEGORY	DEFINITION
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide critical service to a subset of system
High	Organization is no longer able to provide some critical services to any users