Design by Paradigm | Incident Reporting

By: Jordan Biggs

SECTION A: INCIDENT DETAILS	
Incident number(s):	HDE-1001,HDE-1050,HDE-1072
Incident date(s):	13 DEC 10:00 a.m.,13 DEC 3:14 p.m.,13 DEC 3:20 p.m.
Report author:	012678994
Report date:	October 18th
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
Incident priority:	HIGH
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	

SECTION B: DETECT	
Hostname of the impacted system(s):	002

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 using the most CPU usage is XMRig Miner. Which is a crypto miner application

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

SECTION E: LESSONS LEARNED

Recommendation for preventative actions:	**ACTION**	**NEGATIVE IMPACT ADDRESSED**	**PREVENTION METHOD**
	1. Turn on Windows Defender antivirus	Allowed the removal of Mailoucs 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.		