# **Design by Paradigm |** Incident Report

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SECTION A: Incident Details | | | | | |
| Incident number(s): | HDE-1001 | | | | |
| Incident date(s): | 13 DEC 10:00 a.m. | | | | |
| Report author: | 011492128 | | | | |
| Report date: | 13 DEC | | | | |
| Summary of incident: | The operations team reported that the server storing th engineering files has been experiencing high utilization. The admin who installs vendor updates admitted that they have not been verifying the sender via email before downloading updates. Log analysis confirms high GPU & CPU usage on the engineering application server. | | | | |
| Impacted system(s): | WIN-6JNN6RLT6IL | | | | |
| Primary function of the impacted system(s): | CAD Application – Engineering Application – Stores engineering files | | | | |
| Impacted user(s): | Engineering team – referenced tickets: Maya Patel, Diego Martin, Alex Lee | | | | |
| Incident timeline: | 13 DEC. Service Interruption – ongoing | | | | |
| Functional impact:  (*See section: Glossary*) | HIGH | MEDIUM | | LOW | NONE |
| Incident priority: | HIGH | MEDIUM | | LOW |  |
| Additional notes: | This is of very high concern as a critical asset has been compromised. It appears that a malicious actor was able to impersonate a vendor and again access to an administrative account via spear phishing. The actor has also established a connection with an unknown IP address. | | | | |
| Incident type: (*check all that apply*) | | | | | |
| Compromised system  Compromised user credentials *(e.g., lost password)*  Network attack *(e.g., DoS)*  Malware *(e.g., virus, worm, Trojan)*  Reconnaissance *(e.g., scanning, sniffing)* | | | Lost equipment/theft  Physical break-in  Social engineering *(e.g., phishing)*  Law enforcement request  Policy violation *(e.g., acceptable use)*  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): | Microsoft Windows Server 2019 Standard |

|  |  |
| --- | --- |
| SECTION C: INVESTIGATE | |
| Destination port of malicious traffic: | 3333 |
| Additional notes & observations: | There were two source ports: 55974 & 15265. The Data Destination Ip was 159.203.162.18. I was able to identify two instances from my malicious traffic search. |

|  |  |
| --- | --- |
| SECTION D: REMEDIATE | |
| Summary of actions taken to restore functionality of impacted system(s): | Since the issue was in regard to CPU utilization within a server using Windows OS, I navigated to the task manager to identity the tasks with the highest utilization. I was able to identify a Cryptominer running. I located the file source and did further research into removal. I immediately ended the tasks removed the file and updated Windows Defender. |
| Summary of actions taken to restore network security: | In order to restore security I restored Windows Defender and ran a scan to ensure there were no malicious files running. I then set up a rule to block traffic in regard to Destination Port 3333. |
| Additional notes & observations: | The actions taken have restored functionality, removed malicious malware, and blocked malicious traffic. Since an administrative account was compromised I would recommend a more thorough analysis to see if the actor installed additional files in an attempt to achieve persistence. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SECTION E: LESSONS LEARNED | | | | |
| Recommendation for preventative actions: |  | **ACTION** | **NEGATIVE IMPACT ADDRESSED** | **PREVENTION METHOD** |
| 1. | Security Awareness Training | Employees clicking malicious links in emails. | Organization will ensure that employees complete educational training on phishing. In addition the organization will periodically send out simulated phishing emails to test employees. This will minimize the chances of employees clicking malicious links in the future without verififying the sender. |
| 2. | DMARC | Phishing Emails | The organization will use SPF and DKIM to verify authenticity of emails. By using the reject policy within DMARC the organization will be able to filter out more of the malicious emails from impersonators. |
| 3. | MFA | Account Credential Compromise | The admin was using very simple login credentials. By increasing password complexity and requiring multiple factors to login, it will make it more difficult for a malicious actor to gain access, even if they guess or bruteforce the password. |
| 4. | Redundancy | Server Availability | Depending upon the companies budget they may want to have a backup server. It seems that they currently have a single point of failure. By creating a backup they would have an alternative to prevent business operations from being interrupted should the main source go down for any reason. |

# 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 |