|  |  |  |  |
| --- | --- | --- | --- |
| Incident Response –  Sample accident: Argous Co. | * Incidents can get complex very quickly * To illustrate this, we’ll look at a simple incident * Victim’s name is Argous (Fictitious for class purpose) * Threat actors are called Green Penguin * They are state-sponsored “Consultants” * Help avoid attribution to their sponsor. | 1 | 10 |
| Incident Response –  Webserver compromise | Related to the Argous incident. A Sys admin notified that some odd traffic on a CRM server. TCP port 4444 is listening and the process is called Office\_remoter.exe, and they also see a process called Office\_techneter.exe which makes periodic outbound connections to the Microsoft social.technet.microsoft.com server over TCP/443 port. Defender promptly kill these processes which is common thing to do. | 1 | 11 |
| CRM | Customer Relationship Management, web application that sales employees us both when on the road and while at the office. | 1 | 11 |
| Incident Response –  Reconnaissance:  Argous Example | Scanned the publicly accessible address space of Argous and discovered a firewall, the CRM web application, and the other servers on the internet-isolated network. In this instance the threat actors didn’t take many steps to ne stealthy, while they dis use a VPN to obscure their IPaddress, they scanning activity generated a handful of alerts n the firewall, the IP address of the VPN servers were known to be malicious. | 1 | 12 |
| Anonymity tools | Tools used to provide anonymity such hiding your IP address. | 1 | 12 |
| Threat intel information | Used to identify proxy servers that is used for malicious activity | 1 | 12 |
| Mistake #1 | Ignored firewalls alerts of pre-attack traffic | 1 | 12 |
| Mistake #2 | No threat intel about known malicious IP | 1 | 12 |
| Incident Response –  Scan and Exploit Web app | The SSRF vulnerability allowed threat actors to read the source code of the CRM application leading to the discovery of a command injection vulnerability. The command injection vulnerability gave the threat actors the ability to run arbitrary commands. Both vulnerabilities could be exploited without needed to log into the web application. | 1 | 13 |
| Mistake #3 | Failed to fix know server-side request Forgery (SSRF) and command injection vulnerabilities | 1 | 13 |
| SSRF – Server-side Request Forgery | Involves an attacker abusing server functionality to access or modify resources. | 1 | 13 |
| Incident Response –  Pivot and internal Scanning | The threat actors realized the CRM web app had both public and private facing IP address. This was done so both remote and local employees could access the CRM functionality. A proxy that listened on TCP port 4444 was downloaded and forwarded access to internal network allowing the threat actors to pivot and send tragic around the firewalls filtering mechanism. “ Office\_Remoter.exe. | 1 | 14 |
| Mistake #4 | Dual-home host allowed pivot around the firewall | 1 | 14 |
| Mistake #5 | No monitoring on the internal network | 1 | 14 |
| Incident Response – Lateral movement | The threat actors stared performing reconnaissance and scanning again from behind the firewall. After finding passwords were accessible, they were able to crack them and realized a database administrator who had local administration permissions reused his password, allowing the threat actors to pivot and gain control. |  |  |
| White papers |  | 1 | 15 |
| Mistake #6 | Easily cracked password | 1 | 15 |
| Mistake #7 | Password reuse from CRM to domain | 1 | 15 |
| Incident Response –  Domain password Access and Pivoting | Threat actors noticed there was a local account on each system with the same AssetMgtAcct. Focusing their attention this account, the used their local administrator privileges on the database server to extract the NT hashes from memory and cracked the password offline. | 1 | 16 |
| Mistake #8 | Asset mgt account had same password on all systems | 1 | 16 |
| Mistake #9 | No alerts for new software on critical systems | 1 | 16 |