Notes

- CIO Company Address
- Introduction to Advanced Persistent Threats
- Equipment
- Interviews

CIO Company Address

CIO Update

Network Issues

```
- Slowdowns
- Webpages taking forever to load
- Difficulty accessing services or complete downtime
- servers randomly crashing & rebooting without any clear Explanation
- Spike in network traffic & bandwitdth
- Infastructure strain
- Revenue loss
- Potential client distrust & client loss
```

Notes

```
- Possible Denial of Service Attack
    - Competitor to steal business?
    - Nation State Actor?
        - Clients are private sector, government, and infastructure, trasnportation, and
energy.
        - Possibly they want to disrupt critical services and criple economy.
```

Introduction to Advanced Persistent Threats

Email from John Carter to Fellow IT Team

Potential Cyber Threat Actors responsible for the attack impacting Nexora Dynamics

APT - Sophisticated Cyebr Attackers that operate golablly each with their own targets tools and motivations

Four Groups: APT 33 - Elfin Originating from Iran Focuses on Sectors like Energy, aerospace, petrochemcials, and manufacturing Main motivation is Espionage and disruption of critical infastructure, particular interest in middle east and the western world Attack Vectors: Spear Phishing (Highly Targeted Emails that exploit vulnerabiliteis in attachements or links putting malware directly on the victims systems.) Powershell based malware to enable persistent backdoors into victims systems. Credential Harvesting and Lateral Movement Once inside use tools to steal credentials and move laterally. Known to deploy destructive wiper malware APT 28 - Fancy Bear Russia Based Group Targeting government entities, political organizations, media outlets, and defense contractors Attack Vectors: Spear Phishing Credential Theft Use social engineering to steal credentials to high profile accounts Toolkit of sophisticated malware Espionage, Remote Access, C2 Infastructure Politically Motivated
APT 34 - OilRig Iran Linked group Targets financial Sector, telecommunications, government agencies, and energy firms Emphasis on middle eastern companies, and their allies. Attack Vectors: Phishing Use social engineering tactics to compromise networks Credential Harvesting Gather user credentails WEb based Exploits and VPN attacks Exploit vulnerabilites in web applications and vpns to gain access to internal systems. Allows them to remain hidden while they gather intelligence Custom Backdoors and Scanning Tools Used to maintain access Also known for their lateral movement capabilities Find high value targets Espionage, Survillence, long term footholds in network APT 29 - Cozy Bear Russian Linked Group Known for is stealthy focus on government agencies, dimplocatic institutions, and think tanks High rofile espionage campaigns aimed at gathering intelligence from werstern targets Attack Vecotrs: Sohpicsticated Speat Phishing Deploy Advanced Malware, through attachments or cloud services, Supply Chain Attacks

Infiltrate Third party vendors to reach tehir targets Custom malware and advanced persistence Invade detection and maintain longterm access Living Off the Land Techniques CLoud servies and legitimate software to blend in with network traffic Difficult to detect thier activiteis

Equipment

Key Infastructure Imacated, Integral to both inertnal operationbs and external system delivery

Web Server puiblic facing application Substancial delays in response times and service availablitlity to to abnormla traffic volumes Increase page load times and intermittented unavailabliltiy Database Server | proccessing and storing critical business data Resource exhaustion CPU and Memory usuage spiked significantly during the period of disruption leading to crashes and data restrieval issues Load Balancer unable to handle the suddent increase in incoming requests system strugled to maintain an even distribution causing some servers to become overwhelmeed while other remained under utalized Firewall Has been under heacvy strain due to to the high volume of incoming connection attempts Many were flagged as suspicious proccesing and inspection processes caused bottlenecks further contributing to system slowdowns Router handling a significant amount of unexpected traffic resulted in packet loss and increased latency distrupted data flow and contributed to network instability switch experienced congestion due to excessive traffic between devices Delays in internal communications and degraded performance or critical internal applications Contend Delivery Network (CDN) Responsible for distributing content to users has experienced significant delays in delivering services to clients Unuasally high traffic volumes have overburdened the CDNs capactity causing delys and occasianl time outs in content delivery DNS Server Heaveliy targeted leading to disruptions in resolving domain names to ip addresses Caused widespread connectivity issues in both internal and extneral users Email Server Significant backlog of emails and delays in delivery due to netwokr congestions impacted internal communication and delayed responses to external queryies VPN Gateway Responsible for managing secure remote connections has been intermittenlty inaccessible Influx of connection attempts overloaded the gateway affecting access for employees and partners

Interviews

Sarah

About

- Employee
- Describes challanges she has recently faces with Nexora network and web server.

Notes

- Network Slow
- Affects productivity
- Tasks such as sending and email or accessing files take longer than they should
- Webserver was working one day and then stopped the next
    - No one could access it
- Lots of disruption
- Access to workday & benefits are inconsistent and sometimes does not load

John Carter

About

- Employee | Junior Network Engineer
- Update on his oversvations regarding the network issues
- Started 1 Week ago

Notes

- Noticable slowdown on network
- webpages taking much longer to load than usual
- Users reported difficulty accessing services
    - Few cases sevice unavailable errors
- Sudden spike of traffic from a range of IP Addresses that do not typically interact with the

```
network
- Bandwidth usage unusally high
    - No increase in legitimate user activity
-Possiblity of more down time & performace issues
```

Oberservations

```
- Increase Network Traffic
- Slow and unresponsive web traffic and devices
- Productivity lowered
    - Denial of service by increasing network traffic to a point of inusability
```