**ACME Data Breach After-Action Report**

**September 13th 2021**

**Marvin the Martian SOC**

**Icon

Description automatically generated**

**Incident Overview**

**Incident Name:** ACME Data Breach

**Incident Dates:** On or about 17th of December 20xx

**Situation:** Three weeks ago, a data breach was found by ACME’s SOC, outsource to Cybersecurity Stooges. Threat actor was able to infiltrate system and obtain Intellectual Property and exfiltrate said property from the system. Marvin the Martian SOC group was brought in for analysis and recommendations of ACME Security system, as well as diagnosis of the event and timeline of actions.

**Mission Area(s):** Risk Assessment, Response

**Threat or Hazard:** Remote Access Trojan and Exfiltration

**Participating Orgs:** ACME Company

Road Runner Consulting Group

Marvin the Martian SOC

**Point of Contact:** Wiley E Coyote

**INITIAL INCIDENT SUMMARY:**

On or about the 17th of December, a threat actor gained access to the ACME industries network and installed jSpy.jar spyware – a Remote Access Trojan that allows the remote computer to take control of a real physical target device as if they have physical access to that system with the following capabilities:

* Able to run files.
* Execute commands.
* Remote keylogger.
* Remote cam.
* Remote desktop.
* File manager and many other features.

During the course of the infiltration, Intellectual Property was taken from the file management server and removed from the system.

The attack was discovered a few days later by ACME’s SOC, an organization outsourced to a company known as Cybersecurity Stooges. Soon after the attack was discovered the former CISO of ACME, Fudd, announced his resignation.

Soon after a new CISO was hired, Wiley E Coyote, and the Marvin the Martian SOC was formed to investigate the incident.

**ROOT CAUSE:**

On or about the 17th of December, multiple events were flagged by company firewall as two machines were targeted by various attacks. Between December 13 to 17, there were multiple DNS requests and attacks on the 14.01 and the 16.04 Ubuntu machines. During this time, the 16.04 (classified as Machine 2) workstation user “triddle” is believed to have downloaded (either purposefully or through negligence) the Remote Access Trojan jSpy.jar into their home directory in a file titled “DoomWhoPullsTheStrings”. On Machine 2 the threat actor was able to escalate privileges through the SMB system and obtain administrator privileges.

The threat actor then used these threat privileges to traverse to other systems via the Samba share architecture, which had not been secured against traversal and was still using SMB1 protocol in some cases, allowing the malware to spread to both Windows workstations as well as the Linux 14 machine, which was operating at the organizations file directory system. Because the NETBIOS/SMB share password is default, null, or missing and has inappropriate access control, these were specifically allowing for DoomWhoPullsTheStrings to be shared using a NULL session on port 445, host being 192.168.0.2 (the 16.04 Machine 2). Logs show that the threat actor also attempted to share files containing usernames and passwords for other users in an attempt to gain access to other parts of the organizations system. Where the file was removed to is unknown at this time, and there has been no attempted contact regarding a ransomware request or further breaches.

The attacker(s) were unaware of which machine was holding the intellectual property but did target two machines in particular with attempts to breach. Their behavior indicated that they wished to infect all machines on the network with the Remote Access Trojan and were only able to do so on the four machines listed because of their open and unprotected ports (see following diagrams)

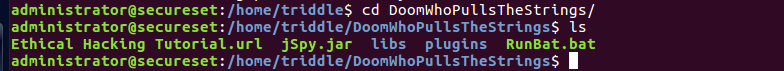


Diagram 1: Inside of directory ‘DoomWhoPullsTheStrings’

Open ports found with Nessus vulnerability Scanning tool


Diagram 2: Machine IP’s with their open ports (Nessus)

Microsoft SMB Share showing access hosted by "Doom" directory


Diagram 3: “Doom” Directory shown with SMB shares vulnerability (Nessus)

**ACME Vulnerability Report**

**Overview of Systems Vulnerability**

After conducting a risk analysis on the network, assets and systems, ACME Corporation is considered at very high risk. The network had many unsafe ports open, the vulnerability scanners and anti-malware software were outdated or unused, there was very little evidence of data backup and the file sharing system being used, Samba, is highly considered to be unsafe. The computers and systems on the network also contributed to the high-risk level. There was a high confidentiality risk, with many inactive users, users with elevated privileges, and many accounts with passwords that do not expire. The integrity risk was also deemed high. There were many computers with almost no files encoded or hashed and the entire system uses SHA-512 hash, a hash no longer considered secure. There was further evidence of high risk in the availability of the files. Many systems cannot pull the proper file, systems cannot perform regular updates without error notifications and many of the computers could not perform tasks without crashing.

**Network**

When inspecting the network, the first course of action was to check the ports open and the devices on the network. The most concerning port open was from the DV Linux machine, port 3306. This is most commonly used in SQL injection and attacks and was closed immediately. The Spiceworks and LDAP machine both had port 22 open, most commonly used to SSH into another system and can be used to overtake a network. Ports 137, 138, 139 and 445 are open and used in the file sharing system Samba. It is recommended to switch from using Samba and close these ports as they can easily be used by threat actors to share files. Port 445 being left open was used in the infamous 2017 WannaCry attack. Lastly, the avahi-daemon,  media servers most commonly used with Apple streaming, is running on ports 5353, 42465 and 53732.  It is recommended all of these ports are closed when not being used.

When conducting a scan to see the IP addresses connected on the network all devices were accounted for, indicating low risk. However, when mapping the IP addresses of the systems there was evidence of the IP addresses skipping numbers. This is not uncommon when devices are commonly switching networks, however this is a closed environment, and the finding was documented.

**Assets**

There are fourteen assets on this network: the router, network switch, Vulnerability scanner, LDAP server, Spiceworks Server, five Ubuntu machines, DV Linux, and two windows machines.

The Network infrastructure Devices, the router, switch and firewalls, is deemed moderately high risk. The router is not password secured. This is a major security flaw. Even though it is protected by firmware that encrypts the data and the built-in firewalls are enabled, a malicious actor could easily gain access to the network and take control. We recommend requiring a password and upgrading the Wi-Fi-security to WPA2.

The servers are also deemed moderate to high, depending on the actual server. The most pressing and common issues found with the servers was the out-of-date software. Ubuntu machines were running version 14.04, 16.04 and 18.04. Many security bugs in 14.04 and 16.04 may compromise the entire system. We recommend all these machines are upgraded to 20.04 and the DV Linux be removed immediately.

Server risks are often defined in three categories: Confidentiality, Integrity, and availability. Confidentiality Risk refers to the number of users on a network and the number of elevated privileges associated with non administrative accounts.

With the exception of one Ubuntu 16.04 machine and the Spiceworks Server there are many inactive accounts that could be removed. We recommend removing these immediately. It is also recommended to set passwords to expire after a set time. The Windows machines followed this guideline, yet every other machine had no such protocol. Because of these reasons, the confidentiality risk was deemed high.

Integrity risk is based on the number of files that are encoded or hashed. Although most servers did have confidential information hashed, the hash used is SHA-512. This hashing system is no longer considered secure. SHA-512 does not use a salt, meaning the data is hashed in the same code every time. For example, if my password is ‘password’ it will read the same hash on each computer. This makes every system with this password compromised. It is recommended to upgrade this hash to BCRYPT, SCRYPT or Argon2. The integrity risk was also heightened with the use of Samba file sharing system. This system does not encrypt data before it is shared, and it is recommended administrators disable this entirely. Microsoft Sharepoint, Git or SmarTransfer are all recommended in its place (see recommendations later I document). For these reasons, the integrity risk is deemed high.

Availability risk is the risk that performance and availability of the systems and data are compromised. This can include not being able to reach files in a timely manner, being unable to perform simple updates and the availability of data bak-ups. Because so many of these systems are out of date, simple backups and system upgrades became impossible. These computers provide a very high-risk environment for the network. For example, running ClamAV, an antivirus engine, was impossible on three quarters of the network. Many of these computers crash if running an update. This leaves a large hole for threat actors to insert malicious content. These reasons make the availability risk very high.

**Scan Results**

After completing a Nessus Host Discovery Scan and a Basic Network Scan it was clear there has never been a working vulnerability scan on this network. With over forty vulnerabilities only the highest risk vulnerabilities are being documented here. Using Tenable’s patented Vulnerability Priority Rating system, VPR, the highest threat came from the Vulnerability Scanner on the network. At the highest priority the scan showed this Vulnerability Scanner had escalated privileges, giving admin access over the entire network It was with this authority the threat actor disabled the strict flags in the machine. Strict flags enable additional security checks of the certificate present in a certificate chain. Without these enabled, it is easier for malicious code to be inserted in data without the system flagging the change. It is highly recommended to disable any privilege access, change passwords, include two-factor authentication, upgrading to OpenSSL 3.0 and resetting all flags to enabled.

Another high-risk event was from the Ubuntu 16.04 Machine 1(192.168.0.2). Microsoft Windows SMB shares unprivileged access. In other words, the user from this computer had escalated privileges, and used these to read, write and share SMB files to the Windows machines.

The final high risk noted by the Nessus Scan was IP forwarding enabled on the router. This was done by the escalated privilege user to route packets through the host and potentially bypass any firewalls, routers, or NAC filtering

**Vulnerability Conclusion**

Using the scanner one can assume the user from192.168.0.2 escalated his privileges, used these to disable flags on the vulnerability scanner, to change Samba files into malicious code, and to send this data out to the network. After scanning 192.168.0.2 computer and the windows machine we can see user Tom Riddle sent DoomWhoPullsTheStrings.exe with jSpy.jar file containing malicious content through the Samba File system. We recommend disabling user triddle, returning Vulnerability Scanner to all flags enabled, upgrading to OpenSSL 3.0, adding a password to the router, upgrading Wi-Fi security to WPA2, closing open ports, switching from Samba to a safer file sharing system, updating the software to be on the most recent version, install an anti-malware system on all systems, using a safer hash system, removing the unused accounts, reset passwords on all admin accounts, include multi-factor authentication, install a reminder to change passwords regularly and creating safer back-ups for the system immediately.

**Vulnerability and Incident Response Findings:**

Detailed findings can be found in the attached **Risk Assessment Report** and **Incident Response Plan**.

Each machine was found to have vulnerabilities that were a risk to the ACME Corporation. Starting with the multiple Ubuntu machines, they were not updated to the current OS. The Linux machine had many open ports and was not securely configured. The LDAP machine was not securely configured for use. The Spiceworks machine was not being used. On top of all of that, the system's firewall configuration was unknown. There were no password management protocols present. There were access control management protocols in place that were not necessary.

Doing a network scan, analysts were able to determine that the assessed threat level is very high. Using Tenable Nessus, a vulnerability scanner, it was determined the remote host is affected by multiple vulnerabilities. We can determine that the age of vulnerability is between 60-180 days. The CVSv3 Impact Score is 5.2. The exploit code maturity is unproven. The product coverage is very high. The threat intensity is very low. The threat recency is 120 to 365 days. We can determine that the affected host IP is 192.168.0.8. But this was not the only one, there are multiple open ports on different IPs.

Upon taking inventory and assessing of hardware and software applications on the ACME system and running vulnerability scans on the network, the following is the deduction of the assessment with recommendations/opportunities in accordance with NIST 800-53 and CIS Controls.

* Some machine hardware residing on the network that are non-essential and pose vulnerabilities.
* Linux machine (open ports, not securely configured, should at minimum be segmented off from the network)
* Spiceworks machine but application not in use or utilized.
* LDAP machine not securely configured for use.
* Multiple Ubuntu machines not updated to current OS.
* Firewall configuration and integrity unknown.
* Password management protocols are absent.
* Account Management & Access Control Management are not implemented (users with administrative privileges that are not required).
* File sharing application (Samba) not recommended for enterprise deployment.

In the time range approximately December 13-17th there were multiple DNS requests logged and attacks on two of the legacy Ubuntu machines (14 & 16-1) and traverse directories, compromise those directories and gain access to sensitive data with administrator access through Samba (TRiddle account). The Samba file sharing system was sharing access with the LDAP server as well as shared Samba ports with the Ubuntu 14 machine which is setup as a server with access to multiple machines on the network. This allowed for remote access and infiltration through SMB protocols and eventually exfiltration of data.

Recommendations

Recommended **Moving Forwards Timeline** for Implementation of suggested changes attached to this document for further details

1. **Close ports:** It was also discovered that port 139 (open) which is utilized by NetBIOS Session Service provides access to shared resources to anyone on the internet. Port 445 which was also discovered open, is used by Microsoft Directory Services for Active Directory and SMB protocol over TCP/IP. Port 8834, Nessus Web. Port 631, Internet Printing Protocol of UDP and port 3306 for MySQL. SSH ports were also open on both Spiceworks Server and LDAP machines.
2. **VPN**: VPNs bolster your device's security and control. A VPN will ensure your data is kept secure, information is remotely accessible, personal data remains anonymous and that you have access to file sharing between groups.
3. **Proxy Server**: You can configure your proxy server to encrypt your web requests to keep prying eyes from reading your transactions. You can also prevent known malware sites from any access through the proxy server.
4. **Hardware:** As previously stated, segment or decommission hardware not applicable, relevant or in use for business objectives.
5. **Event Monitoring**: Procurement and deployment of SIEM monitoring capabilities to flag and alert of abnormal events from baselines.
6. **CIS Controls:** Employ & deploy the top five CIS Controls over the next 12 months:
7. Inventory and Control of Enterprise Assets
8. Inventory and Control of Software Assets
9. Data Protection
10. Secure Configuration of Enterprise Assets
11. Account/Access Control Management

Cyberthreats are constantly emerging and evolving. As a result, we needed a comprehensive approach to protect against today's advanced threats. As employers at ACME share information publicly that can be potentially harmful to the company, we created a plan to reduce findings by implementing the OSINT framework which includes collecting information from public sources, analyzing it, and using it for intelligence purposes.

ACME has a digital footprint as do all Organizations, and their staff. These footprints can contain a wealth of sensitive or weaponizable information. Implementing the OSINT framework lets you see what the hackers can see. At ACME there were several findings that we deemed vulnerable starting with SAMBA which is a network file sharing protocol that allows users or applications to request files and services over the network, samba is riddled with security concerns. There are alternatives such as Microsoft SharePoint, Git, or even a Linux network file share are all better options in comparison.

The best option presented would be the Microsoft SharePoint it has a plethora of features such as access to sensitive documentation which can be controlled at folder level. This means it can be limited to certain employees. It also adds extra detail to the access of the documents, letting you keep a trail of who accessed it, who changed it and when it was viewed. It is also a safer alternative as hazards that can affect paper are no longer applicable. You can back up your documents to cloud storage. If the files are lost at any point, the backup can easily restore your work. This could save ACME lots of money if they needed to recreate them. On top of all that, ACME can even recover older versions of documents in case they regret any of the more recent changes to it. With guaranteed safety controlled at every level and a proven durability, digital documentation managed by a dedicated system is the best option for important documents, especially in large businesses.