Post-Incident Report

Prepared By: Aishwarya Shankar (Lead Security Analyst)

Executive Summary

Incident ID: INC2023-0920-023
Incident Severity: High
Incident Status: Resolved

Incident Overview and Key Findings: Beginning on the morning of September 20, 2023, suspicious network activity was detected on th**e com**pany's corporate network. The security team responding to the incident determined that unauthorized system access, potential data exposure, port scanning, privilege escalation, database corruption, and malware infection have occurred.

Technical Timeline

- **Incident Timeline**

1. There was a successful login as user "JohnDoe" on DESKTOP-1234567 on 09/20/2023 at 8:10:23 AM EST initiated from IP address 192.168.1.2 port 50215 using RDP.
2. There was a successful policy change by user ADMINISTRATOR on machine DC-SERVER-01 on 09/20/2023 at 9:45:32 AM EST. They created a new file or folder on the system.
3. There was a failed login as user "admin" on DESKTOP-1234567 on 09/20/2023 at 10:32:17 AM EST initiated from IP address 192.168.1.100 port 50789. The login failed due to bad username or password. This is the first attempt at port scanning detected in the Windows Event logs from 09/20/2023. [4] and [5] listed below show this as multiple ports are being probed in quick succession.
4. There was a failed login as user "admin" on DESKTOP-1234567 on 09/2020/2023 at 10:32:19 initiated from IP address 192.168.1.100 port 50791. The login failed due to a bad username or password.
5. There was a successful login as user "admin" on DESKTOP-1234567 on 09/20/2023 at 10:32:21 AM EST initiated from 192.168.1.100 port 50793. This indicates privilege escalation and compromise of admin credentials.
6. There was a firewall warning on DESKTOP-1234567 on 09/20/2023 at 10:33:45 AM EST due to a successful login attempt initiated from IP address 192.168.1.100 to IP address 192.168.1.1 using TCP protocol at port 445.
7. There was an application error on DESKTOP-1234567 on 09/20/2023 at 12:01:15 PM EST due to an access violation in an attempt to access Windows Explorer.
8. There was a firewall warning on DESKTOP-1234567 on 09/20/2023 at 1:23:15 PM EST due to a successful SSH login from IP address 192.168.1.125 to IP address 192.168.1.1.

9. There was an error on SERVER-12345 on 09/20/2023 at 2:10:12 PM EST as user DESKTOP-1234567/JohnDoe attempted to use UDP at port 53 (not allowed).
10. There was an MS SQL SERVER warning on SQLSERVER-12345 on 09/20/2023 at 3:23:52 PM EST. Error: 823, Severity: 24, State: 2 indicates that MS SQL SERVER was having trouble reading data from disk (I/O error) when it was trying to read from mydatabase.mdf (this is the primary database file which contains schema and data). This indicates database corruption.
11. There was a failed login as user "admin" on DESKTOP-1234567 on 09/20/2023 at 3:34:56 PM EST initiated from IP address 192.168.1.50 port 50837. The login failed due to a bad username or password.
12. There was a Microsoft Windows Security warning on SERVER-12345 on 09/20/2023 at 4:45:32 PM EST due to an allowed network connection from IP address 10.0.0.2 port 12345 to IP address 10.0.0.1 port 80 (a suspicious application "unknown.exe" is running here). This is an unsecure connection established between the two IP addresses.
13. There was a failed login as user "Admin" on SERVER-12345 on 09/20/2023 at 5:34:56 PM on SERVER-12345. Logon type 2 indicates an interactive login (user was physically at the system). The login failed due to a bad username or password.

- **Response, Containment, and Eradication Timeline**

1. On 09/20/2023 at 4:00 PM EST, the security team was engaged and began the incident investigation and analysis process.
2. On 09/20/2023 at 7:00 PM EST, the security team completed forensic investigation and commenced response, containment, and eradication.
3. On 09/21/2023 at 11 AM EST, the incident was officially resolved and all affected systems were restored to normal operations. Long-term measures started to be implemented.
4. On 09/21/2023 at 2 PM EST, communication was sent out to relevant stakeholders.

Affected Systems

- DESKTOP-1234567 - user JohnDoe was compromised, admin credentials were compromised and privilege escalation occurred, port scanning was observed, and system contains PHI and other PII which were potentially exposed
- SQLSERVER-12345 - database corruption was observed
- SERVER-12345 - contains malicious application "unknown.exe"

Indicators of Compromise (IoCs)

- Unusual network traffic - port scanning on DESKTOP-1234567
- Several incorrect login attempts in quick succession on DESKTOP-1234567
- Privilege escalation - admin credentials compromised on DESKTOP-1234567
- Database corruption on SQLSERVER-12345

- Malware - unknown.exe seen on SERVER-12345 is malware

Response and Recovery

To respond to the incident and prevent further damage and spread of the malicious activity, the security team performed the following actions:

1. Isolated the suspected affected systems DESKTOP-1234567, SERVER-12345, and SQLSERVER-12345 from the company network. Backed up the systems to retain a snapshot of the environments.
2. Locked out user JohnDoe on DESKTOP-1234567.
3. Changed admin credentials on DESKTOP-1234567.
4. Performed malware analysis on the suspicious program, unknown.exe, running on SERVER-12345. Used malware removal tool to remove the malicious file.
5. Analyzed the corrupted SQL database on SQLSERVER-12345 and returned it to operational state.
6. Examined systems to determine the extent of the potential data exposure and what data (particularly PHI and other PII) had been exposed on DESKTOP-1234567, SERVER-12345, and SQLSERVER-12345.
7. Restored the affected systems using backups.

Business Impact

The incident resulted in the temporary loss of access to critical servers and databases and caused an outage of approximately 19 hours. The downtime caused delays in fulfilling client contracts, potentially impacting customer trust and satisfaction.

Operationally, productivity was reduced during the outage as employees were unable to access internal systems like DESKTOP-1234567, SERVER-12345, and SQLSERVER-12345.

PHI and other PII were potentially exposed, and the company followed the HIPAA Breach Notification Rule to notify likely affected individuals, the Department of Health and Human Services, and the media. The company is likely to incur fines due to the potential exposure of sensitive customer information and may experience long-term damage to customer trust.

Post-Incident Reflection

- **What went well**
    1. Security team responded to the incident in a prompt manner.
    2. Affected systems were isolated quickly to prevent further damage.
    3. Stakeholders (legal counsel, IT & Operations team, PR team, senior IT and security management, CEO, CFO, CIO, CISO, COO, clients, customers, and HHS) were informed of impacts promptly.

- **Areas for improvement**
    1. Approval for remediation actions from management was delayed, resulting in slower-than-expected response time.

Recommendations for Enhanced Security Posture

To improve **the compan**y’**s** security posture in the long-term, the security team proposes the following actions:

1. Implement a strong password policy and MFA on company systems.
2. Update antivirus software on systems.
3. Close unused ports in order to minimize the organization’s attack surface.
4. Enhance security monitoring. Implement an NIDS solution to enable continuous monitoring of network traffic, in addition to the existing host-based monitoring and logging.
5. Implement DLP software to prevent data exfiltration from the company network.
6. Ensure that systems are regularly backed up.
7. Invest in comprehensive, thorough security awareness training for employees.