Incident Response and Review Sprint

Tools Used:

- VirusTotal
- AbuseIPdb
- ChatGPT

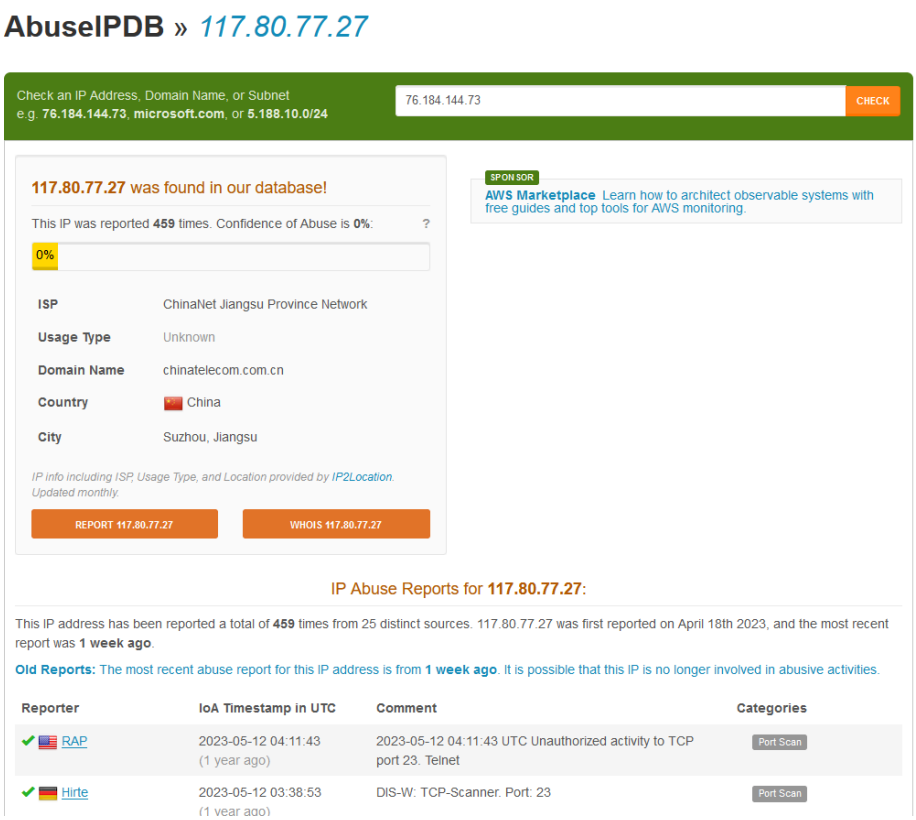
Incident Overview:

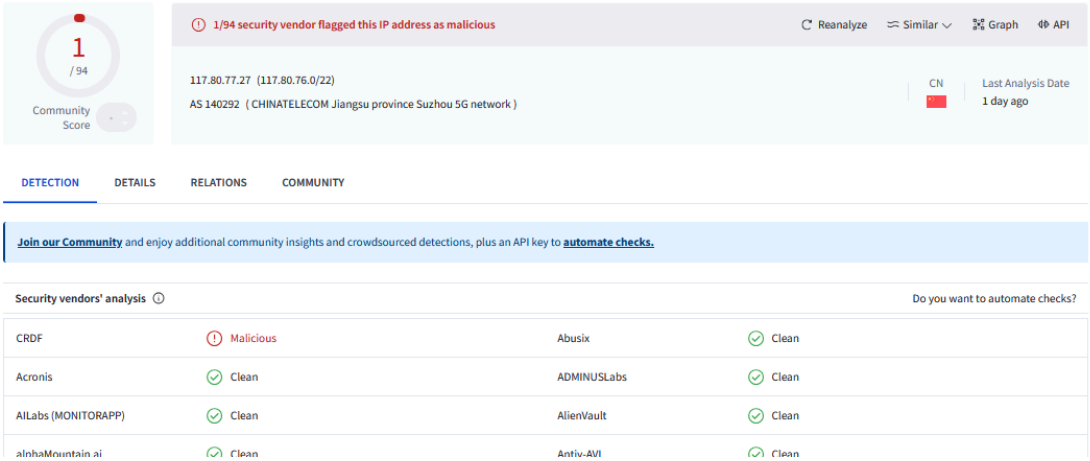
Date: September 20, 2023

Identification and Investigation Phase:

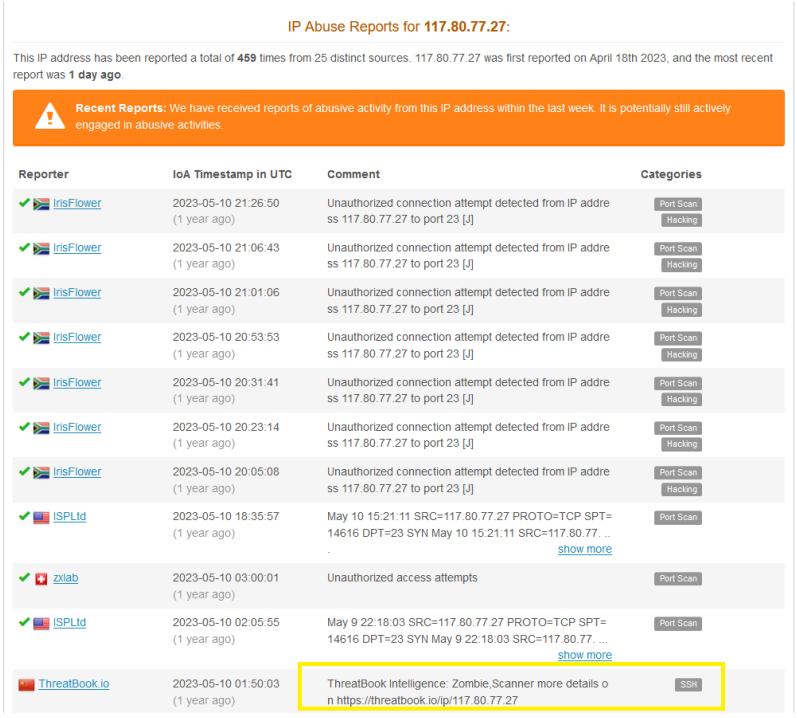
Scanning the suspicious IPs

- Among all the IPs, the IP address 117.80.77.27 has been identified as malicious by both VirusTotal and AbuseIPdb





- According to AbuseIPdb's Threatbook threat intel, this IP has been flagged as a zombie scanner, indicating that the system may be compromised and part of a botnet, scanning the network for open SSH ports



Windows Event Logs

Timeline and Analysis

1. **08:10:23:** Log 3 Analysis - User John Doe(IP-192.168.1.2) successfully logged (event ID 4624) into Desktop 1234567 via a remote session. The logon type is 10, indicating the use of Remote Desktop Protocol (RDP).
    a. Source NW address- John Doe - 192.168.1.2 - IP has been flagged for brute force

2. **09:45:32:** Log 5 Analysis - A policy (audit policy) was changed using an admin account on the computer DC-SERVER-01.Windows logs this event whenever there is an update to what kinds of actions are being monitored and recorded by the system's audit policies

3. **10:32:17, 10:32:19** - failed login attempts(Username - admin) to Desktop 1234567 from 192.168.1.100

4. **10:32:21:** Successfully login(Username - admin) to Desktop 1234567 from 192.168.1.100

5. **10:33:45** : Log 13 Analysis - After admin login , a firewall rule is modified successfully to allow traffic from 192.168.1.100 to 192.168.1.1 over port 445 - SMB, this protocol is used to share files on same network

6. **12:01:15:** Log 1 analysis - On the computer (Desktop 1234567), Windows Explorer (also known as File Explorer) has crashed, as indicated by Event ID 1000, which typically signals an application failure.

7. **13:23:15**: Log 6 Analysis - A firewall warning for the desktop -1234567 - detected traffic on TCP port 22 (SSH), originating from 192.168.1.25 and targeting 192.168.1.1 - the outbound rules triggered a firewall log

8. **14:10:12:** Log 7 Analysis - Desktop -1234567\JohnDoe tried to connect to SERVER-12345 over port 53(DNS Server)- But the connection was not allowed.

9. **15:23:52:** Log 2 Analysis - Event ID 823 is a critical warning in SQL Server indicating an I/O error and a bad page ID in the mydatabase.mdf file. This is a sign of potential corruption in the database, likely caused by disk issues or other hardware-related problems

10. **15:34:56**: log 8 Analysis - A failed login attempt(user name - admin) to Desktop 1234567 from 192.168.1.50

11. **16:45:32 :** Log 9 Analysis - an inbound HTTP connection from 10.0.0.2 to SERVER-12345(10.0.0.1) was allowed over port 80 by the Windows firewall. However, the process responsible for this connection, unknown.exe.

12. 1**7:34:56:** Log 4 Analysis - There was a failed local login attempt(Event ID 529) on the computer SERVER-12345 using the username Admin. The failure was due to an unknown username or incorrect password. This was an interactive logon attempt (Logon Type 2), which means someone tried to log in directly at the machine - Local logon failed

Analysis of the Potential Attack

- ➔ **Initial compromise** was done using John Doe's Account via RDP
- ➔ **Privilege Escalation,lateral movement and interception of traffic** - The attackers gained admin privileges on Desktop1234567, changed a firewall policy to access the 192.168.1.1 via port 445, likely a router. Indicating lateral movement (Intercepting the traffic)
- ➔ **Further Exploitation -** After gaining admin priviliges, The attacker tried to communicate with router via SSH Traffic from 192.168.1.25 and also there is a failed DNS connection from John doe to Server12345 suggests attempt to exfiltrate data or communicate with C2C Servers.
- ➔ **SQL Server Corruption -** An SQL Server I/O error could indicate tampering or DOS attacks on critical databases
- ➔ **Presence of malware -** An unknown file was found on server12345 which initiated an inbound connection from 10.0.0.1 - This implies presence of malware on the server
- ➔ Failed login attempts from 192.168.1.50 to the admin account implies that the attacker wants to control the network further
- ➔ A failed local login attempt on SERVER-12345 indicates an insider threat.

Potential compromised accounts or services

- ➔ **John Doe's Account** : Used to initiate RDP sessions.
- ➔ **Admin Account - Desktop 1234567** : Compromised from 192.168.1.100, with successful logins leading to firewall rule changes and lateral movement.
- ➔ **Desktop 1234567**: Involved in lateral movement, potentially controlled via RDP and used to tamper with firewall rules and initiate SSH connections.
- ➔ **SERVER-12345**: SQL database corruption and inbound HTTP traffic via unknown.exe suggest that SERVER-12345 was compromised with malware.
- ➔ **Firewall Rules** were Modified

Response Containment and eradication Phase

The short-term containment strategy aims to isolate affected systems, remove malware, and secure compromised accounts. The long-term strategy focuses on strengthening the network's overall security posture through 2FA, network segmentation, firewall audits, and user training.

Short term Containment plan

- ➔ **Reset** John doe's and admin account **credentials**
- ➔ **Disconnect compromised systems** from the network Desktop1234567, Server12345, and the Router (192.168.1.1). Ensure a data backup
- ➔ **Check the extent of corruption of mydatabase.mdf** in SQL Server and prepare for isolation
- ➔ **Analyze the malware (unknown.exe)** on the server
- ➔ **Block the IPs** which were used for the attack -192.168.1.100,192.168.1.50,192.168.1.25, 192.168.1.2.
- ➔ **Review and update the modified(SMB Traffic and DNS Traffic) firewall rules** to restrict unauthorized access

Long term Containment plan

- ➔ **Implement MFA** for all user accounts and espesially for the Privileged accounts like Administrator accounts
- ➔ **Implement strong Password policies** and also **account lockout policies** should be set to temporarily lock accounts after multiple failed login attempts, preventing sustained brute-force attacks
- ➔ **Remote Systems connection should be allowed only through a VPN connection** rather than exposing the RDP port directly to the internet. This ensures that only users who have successfully authenticated to the VPN can access remote services
- ➔ **Network Segmentation**, Critical systems like databases and file servers should be placed in separate network segments/VLANS with strict firewalls rules and Access control lists
- ➔ An **IDS/IPS** can monitor the network traffic for suspicious patterns (e.g., brute-force attempts, lateral movement, or unusual ports being used) and can alert administrators or automatically block such traffic
- ➔ Regular **firewall rule audits** ensuring that only necessary rules are in place and no unauthorized rules exist
- ➔ **Strict Access controls** and auditing those Access Control Lists
- ➔ **Restricting access to the server room** ensures that only authorized personnel can physically access critical system

Eradication Goals

EG_01 After,analyzing the malware(unknown.exe) on the server and identifying its origin, **remove the malware**
EG_02 Investigate whether this malware left any **backdoors** or additional malicious payloads on the system
EG_03 Identify and patch any vulnerabilities that the malware exploited to prevent re-infection. Ensure systems are up to date with **security patches**
EG_04 Reimage the compromised systems (Desktop1234567, Server12345) to a clean state
EG_05 For Router, perform **factory resetting** and **installing updated firmware** to remove any tampering
EG_06 After blocking the IPs conduct a **network-wide scan** to ensure that no communications are ongoing with these IPs

Business Impact Analysis

Goal	Timeline	Downtime	Financial Impact	Organizational Impact
EG_01	The process of removing the unknown.exe malware it typically takes **1 business day**	**Server12345** will need to be **isolated and taken offline** for malware analysis and removal. This could result in **2-6 hours** of downtime,	The organization may incur costs related to **forensic analysis** tools, Estimated financial impact: **$5,000 - $10,000**	Short-term **operational disruptions**, especially for systems reliant on **Server12345**
EG_02	Completing a thorough investigation and ensuring there are no residual backdoors may take **1-3 days**, as it requires both manual analysis and automated scans.	Systems must remain offline during the investigation for backdoors and additional malicious payloads. Downtime is expected to be 4-8 hours, with additional downtime if backdoors are discovered.	The cost includes the use of specialized security tools and extended staff hours for a deeper forensic investigation. Estimated costs could range from $8,000 - $10,000	There could be prolonged **disruptions in services**. **Customer-facing services** may experience reduced availability, Internally **critical operations** may be delayed.
EG_03	The process of identifying vulnerabilities, testing patches, and applying	Applying patches and updating systems requires **rebooting servers** and verifying	Costs related to **patch management**, **testing**, and	If vulnerabilities are not patched quickly, the business

	updates across all systems could take **1-2 business days**	that patches do not introduce new issues. Expected downtime: **2-4 hours** for each affected system.(This can be done during non office hours)	**post-implementation monitoring**. Estimated financial impact: **$3,000 - $10,000**	remains at risk of **re-infection** or new attacks.
EG_04	Reimaging both **Desktop1234567** and **Server12345** could take **1-2 business days**, considering the time for reinstallation, data restoration, and post-reimaging testing	**Reimaging** a system (including reinstalling the operating system, applications, and restoring data) generally causes **6-12 hours of downtime**	Financial costs include **labor**, potential overtime for IT staff, and lost productivity. Additionally, purchasing replacement software licenses or upgrading infrastructure may add costs. Estimated impact: **$7,000 - $25,000**	**System unavailability** during reimaging can disrupt key business processes. For instance, if **Server12345** supports customer-facing applications, this downtime could affect **customer experience**
EG_05	The reset, firmware installation, and configuration restoration process typically takes **2-4 hours**	Resetting the router and applying firmware updates will take the network device offline for **1-2 hours**	Costs are mainly **operational** in terms of labor to reset, reconfigure, and test the router, with minimal hardware or software expenses. Estimated financial impact: **$1,000 - $3,000**	The **network outage** may impact all systems relying on the router, particularly if it's responsible for routing network traffic across segments. The **entire office or segment** connected to that router could lose network connectivity, affecting productivity
EG_06	A **full network-wide scan** could take **4-8 hours**, depending on the size of the network and the number of IP	A network scan usually doesn’t require downtime, but if active threats are detected, systems	The cost of running network scans is relatively low, especially if	Minimal, as the scan itself doesn't disrupt operations. However, if

	addresses being scanned	may need to be **temporarily isolated**. No immediate downtime unless issues are found	automated tools are already in place. Estimated costs: **$500 - $2,000** (depending on the tools and scope of the scan).	malicious traffic is found, certain systems may need to be isolated for further investigation, which could briefly impact operations.

Post Incident review

1. Financial Impact

➔ **Direct Costs**: $30,000 - $50,000 for incident response, malware removal, and system restoration.
➔ **Indirect Costs**: $10,000 - $30,000 in lost productivity and potential business losses from downtime and reputational damage.
➔ **Total Estimated Impact**: $30,000 - $100,000.

2. How to Prevent Future Incidents

➔ Implement **MFA** for all accounts, especially privileged ones.
➔ Enforce **strong password policies** and **account lockouts**.
➔ Use **network segmentation** and **firewall rules** to isolate critical systems.
➔ Deploy **IDS/IPS** for monitoring and detecting abnormal traffic.
➔ Limit **remote access** via **VPN with MFA**.
➔ Conduct regular **phishing awareness training** and **firewall audits**.

3. What We Learned

➔ **Compromised credentials** pose major risks, highlighting the need for MFA.
➔ **Lateral movement** through SMB traffic requires better network monitoring.
➔ **SQL database corruption** underscores the importance of regular backups and integrity checks.
➔ Thorough **malware analysis** is essential to remove backdoors and vulnerabilities.

4. Security Posture: Now and Future

➔ **Current Posture**: Systems have been isolated, malware removed, and patches applied, but further improvements are needed.
➔ **Future Posture**: Strengthen with **24/7 monitoring**, **proactive threat hunting**, regular **audits**, **training programs**, and improved **incident response planning**. Security will be

embedded into company culture, with enhanced access controls and continuous monitoring to prevent future incidents.