Incident Report – Maven Clinic (Simulated mini-sprint event, Clicked – IBM) – By Yarelys Rivera (CyberYara)

Incident Response Report - Simulated Healthcare Incident

Date: October 7, 2024

Prepared By: Yarelys Rivera

Executive Summary:

This report details the simulated incident response (IR) conducted during the CLIKED - IBM Mini Sprint (September 23, 2024, to October 7, 2024) following the detection of unusual network activity within Maven Clinic's systems. The data (logs and IPs) analyzed in this report were from September 20, 2023. This report is a post-incident review for a simulated healthcare incident scenario, conducted as part of the CLIKED - IBM Mini Sprint. While Maven Clinic is a real entity, and allowed their name to be used for this mini-sprint event on the CLIKED - IBM program, the incident, threat actors, and other organization names included in this report are fictitious and were created to fulfill the requirements of the mini-sprint event. The primary goal of this exercise was to provide participants with a practical, hands-on experience in navigating a cybersecurity incident, from initial detection to post-incident analysis.

The simulated incident involved a multi-stage attack and resembles APT29 tactics, with the following key characteristics:

- **Attack Vectors:** Brute force attack, privilege escalation, and lateral movement.
- **Compromised Systems:** Windows systems (DESKTOP-1234567, SERVER-12345, DC-SERVER-01) and a SQL Server (SQLSERVER-12345).
- **Potential Impact:** Unauthorized access to sensitive healthcare data.
- **Root Cause:** Inadequate privilege monitoring and weak credential hygiene.

The attack pattern—brute force followed by lateral movement via SMB/SSH—aligns with common ransomware or APT tactics (ex. MITRE ATT&CK T1110, T1021). The IP range 117.80.76.0/22 has been historically linked to Chinese threat actors (ex. APT41), though attribution is not confirmed on this project.

The incident response followed the NIST Incident Response Framework. Key findings, containment and eradication measures, lessons learned, and recommendations for preventative measures are detailed in this report. A preventative budget proposal of $262,000 is included.

1. Introduction

On September 20, 2023, Maven Clinic's security monitoring systems detected unusual network activity. Given the sensitive nature of the healthcare data managed by Maven Clinic, senior management initiated an immediate investigation. This report documents the findings of that investigation, the steps taken to contain and eradicate the threat, and recommendations for preventing similar incidents in the future.

1.1. Incident Objectives

The objectives of this incident response were to:

- Determine the nature and scope of the unusual network activity.
- Identify the systems and data affected.
- Contain the incident to prevent further damage.
- Eradicate the threat from the affected systems.
- Conduct a post-incident analysis to determine the root cause.
- Develop recommendations to improve Maven Clinic's security posture.

2. Identification and Investigation

The initial phase of the incident response focused on identifying the nature of the unusual network activity. The following data sources were analyzed:

- **System Logs:** Windows Event Logs from multiple systems.
- **SQL Server Logs:** Database server logs.
- **Network Logs:** Firewall logs and network connection records.
- **Provided IP Address List:** A list of IPs provided by Maven Clinic

2.1. Analysis of Logs and IP Addresses

The analysis of the provided logs revealed the following:

- **Brute Force Attempts:** Multiple failed login attempts were observed in the security logs (Event IDs 529, 4625), indicating a potential brute force attack (Log 4, 8, 10, 11). The source IP addresses associated with these attempts were cross-referenced with the provided list of IPs but no correlation was found.
- **Successful Logins:** Successful login events (Event ID 4624) were identified following the failed attempts, suggesting that the attacker(s) eventually gained access to at least one or more accounts (Log 3, 12). Log 3 shows a successful login by JohnDoe from IP 192.168.1.2. Log 12 shows a successful login to the admin account from 192.168.1.100
- **SQL Server Errors:** Errors in the SQL Server logs (Event ID 823) indicated potential data corruption or manipulation (Log 2). This suggests that the attackers may have targeted the database server.
  - The I/O error suggests potential data manipulation (T1499 - Endpoint Denial of Service) or SQL injection (T1190). Further forensic analysis of database transactions is recommended.
- **Firewall Rule Changes:** A new rule was added to the Windows Firewall exception list (Event ID 2004), potentially allowing unauthorized access (Log 6, 13). Log 6 shows a rule

added for port 22 (SSH) from 192.168.1.25 to 192.168.1.1. Log 13 shows a rule added for port 445 (SMB) from 192.168.1.100 to 192.168.1.1
  - This activity gains additional context when considered alongside the IP address research in the appendix, which indicates that IP addresses in the 117.80.76.0/22 range have been associated with potentially malicious activity
- **Policy Change:** A change in Object Access policy related to the file system was detected (Event ID 4719) (Log 5). This could indicate that the attacker modified file permissions to gain access to sensitive data.
- **Application Error:** An application error (Event ID 1000) was observed (Log 1). The faulting module is unknown.
- **UDP Port 53 Blocked:** A detailed tracking log (Event ID 861) shows that a UDP connection to port 53 (DNS) was blocked (Log 7). The application name is unknown.
- **Inbound TCP Connection Blocked:** A warning log (Event ID 5156) indicates an inbound TCP connection to port 80 (HTTP) was blocked (Log 9).
  - The application name 'unknown.exe' in Log 9 is highly suspicious. A cryptographic hash of this file should be obtained and checked against malware databases.

Key Attack Sequence:

Time	Event	Impact
10:32	Admin account compromised	Attacker gained privileged access.
10:33	Firewall rule added for SMB	Enabled lateral movement to critical systems.
15:23	SQL Server I/O error	Potential patient data manipulation.

A full incident timeline with MITRE ATT&CK mappings can be found on Appendix A.

2.2. Systems and Services Impacted

Based on the log analysis, the following systems and services were identified as being potentially impacted:

- **DESKTOP-1234567:** Multiple login attempts, a successful login, a firewall rule change, and an application error were observed on this system.
- **SERVER-12345:** Failed login attempts and a UDP connection block were observed.
- **SQLSERVER-12345:** SQL Server errors indicate potential data compromise.
- **DC-SERVER-01:** A policy change related to object access was observed on this system, which is a Domain Controller.

2.3. Initial Findings

The initial investigation suggests the following:

- A brute force attack was likely used to gain initial access to the network.

- The attacker(s) successfully compromised user accounts, including potentially an administrative account.
- The attacker(s) modified firewall rules and file system permissions to facilitate lateral movement and access sensitive data.
- The SQL Server was potentially targeted, indicating a possible attempt to access or exfiltrate sensitive healthcare data.
- The external IP address research in the appendix suggests that the attackers may be operating from infrastructure known to be involved in suspicious activity, even if those specific IPs are not directly observed in the internal logs

3. Containment and Eradication

The following plan outlines the short-term and long-term measures to contain and eradicate the threat, and prevent future incidents.

3.1. Short-Term Containment and Eradication Plan

The following short-term measures were implemented to contain the incident and prevent further damage:

1. **Isolate Affected Systems:**
    a. Disconnect DESKTOP-1234567, SERVER-12345, and SQLSERVER-12345 from the network to prevent further lateral movement.
    b. Isolate the Domain Controller (DC-SERVER-01) to prevent further privilege escalation.
2. **Back Up Affected Systems:**
    a. Create forensic images of the affected systems (DESKTOP-1234567, SERVER-12345, SQLSERVER-12345, and DC-SERVER-01) before any further action is taken. This will preserve evidence for further investigation and analysis.
3. **Identify and Disable Compromised Accounts:**
    a. Disable the "JohnDoe" account on DESKTOP-1234567, and any other accounts identified as compromised during the investigation.
4. **Block Malicious IPs:**
    a. Block the identified malicious IP addresses (from the provided list and any new IPs identified during the investigation) at the firewall and other network security devices.
5. **Reverse Firewall Rule Changes:**
    a. Revert the unauthorized firewall rule changes on DESKTOP-1234567 (Log 6, 13) to their original state.
6. **Delete malicious files:**
    a. Delete the unknown.exe file from all affected systems after confirming its malicious nature through hashing and malware database checks. Use the file hash of unknown.exe to scan other systems for potential compromise.
7. **Patch Vulnerable Systems:**

   a. Apply the latest security patches to all affected systems, including operating systems, applications, and databases.

3.2. Long-Term Eradication and Prevention Plan

The following long-term measures will be implemented to eradicate the threat and prevent future incidents:

1. **Malware Scan and Removal:**
   a. Perform a full system scan on all affected systems using updated anti-malware software to detect and remove any malware or malicious code.
2. **Password Reset:**
   a. Force a password reset for all user accounts in the domain, including service accounts.
3. **Implement Multi-Factor Authentication (MFA):**
   a. Implement MFA for all user accounts, especially those with administrative privileges, to add an extra layer of security.
4. **Enhance Access Controls:**
   a. Review and enforce the principle of least privilege for all user accounts and groups.
   b. Implement stricter password policies, including complexity requirements and regular password changes.
5. **Implement Robust Privilege Monitoring:**
   a. Deploy a privileged access management (PAM) solution to monitor and control the use of privileged accounts.
6. **Security Awareness Training:**
   a. Conduct regular security awareness training for all employees to educate them about phishing, social engineering, and other attack vectors.
7. **Vulnerability Management:**
   a. Implement a vulnerability management program to regularly scan for and patch vulnerabilities in systems and applications.
8. **Intrusion Detection/Prevention System (IDS/IPS):**
   a. Strengthen the existing IDS/IPS or implement a new one to detect and prevent malicious activity.
9. **Implement Extended Detection and Response (XDR):**
   a. Implement an XDR solution.
10. **Conduct threat hunting for related IOCs**
    a. Scan all systems for connections to 117.80.77.27 or files with the same hash as unknown.exe
11. **Hire Security Analyst:**
    a. Hire a security analyst.
12. **Calculate the cryptographic hash of any identified malware:**
    a. For example, unknown.exe Use this hash to:
       i. Confirm the file's malicious nature by comparing it to malware databases.
       ii. Scan other systems for potential compromise.

iii. Ensure the file is completely removed from all infected systems.

4. Post-Incident Review

4.1. Root Cause Analysis

The root cause of this simulated incident was determined to be a combination of the following factors:

- **Weak Credential Hygiene:** The use of weak or easily guessable passwords made the brute force attack successful.
- **Inadequate Privilege Monitoring:** The lack of proper monitoring and alerting for privileged account activity allowed the attacker to escalate privileges and move laterally without being detected promptly.
- **Firewall Misconfiguration:** The unauthorized modification of firewall rules created a security gap that allowed the attacker to gain access to additional systems.

4.2. Business Impact

Although this was a simulated incident, a real-world incident of this nature could have significant consequences for Maven Clinic, including:

- **Data Breach:** The unauthorized access to the SQL Server could have resulted in the theft of sensitive patient data, leading to potential HIPAA violations and fines.
- **Reputational Damage:** A data breach could severely damage Maven Clinic's reputation and erode customer trust.
- **Financial Loss:** The incident could result in financial losses due to investigation costs, legal fees, fines, and business disruption.
- **Operational Disruption:** The incident could disrupt normal business operations, leading to downtime and lost productivity.

4.3. Cost Analysis (Simulated)

The following is a simulated cost analysis of the incident:

- Incident Response Costs:
  - Security Analyst: 60 hours
  - System Admin: 10 hours
  - Legal Department: 50 hours
  - PR Department: 50 hours
  - Service fee NoMoreAttack Inc: $30,000
  - HIPAA violation Fine: Up to $50,000 per violation
  - Establish and maintain Call Center: $50,000, agent service for 3 months
  - Business interruption: $100,000 (Business stopped for 1.5 days)

- Total Simulated Cost: $277,000 + HIPAA Fines.

For context, the 2023 average healthcare breach cost reached $10.93M (IBM Security, 2023), with smaller breaches averaging $3.05M. While this simulation estimates $277K in costs (reflecting a limited scope), it mirrors real-world risks like the Anthem breach (2015), where phishing and weak controls led to $16M in HIPAA penalties and $260M+ in total losses.

4.4. Lessons Learned

The following lessons were learned from this simulated incident:

- **Strong passwords are essential:** Weak passwords are a major security risk and can make brute force attacks successful.
- **Privileged Account Monitoring (PAM) is critical:** It is essential to monitor privileged account activity closely to detect and prevent privilege escalation and lateral movement.
- **Firewall security is critical** Firewalls must be properly configured and monitored to prevent unauthorized access.
- **Regular security audits are necessary:** Regular security audits and vulnerability assessments can help identify and address security gaps before they are exploited.
- **Incident Response plan is crucial:** A well-defined and tested incident response plan is essential for minimizing the impact of a security incident.
- **Security awareness training is important**: Employees are the first line of defense.
- **Threat Intelligence Integration:** Proactively monitoring IOCs (ex. IPs in 117.80.76.0/22) could have reduced detection time. Future processes will include automated feeds from OTX AlienVault and blocklists.

5. Recommendations and Preventative Budget Proposal

Based on the findings of this simulated incident, the following recommendations are made to enhance Maven Clinic's security posture and prevent similar incidents in the future. A total budget of $262,000 is proposed for Q1 2024 to implement these recommendations.

Category	Item	Description	Cost
Incident Response Training	Incident Response Training (70 employees)	Provide incident response training to employees with assigned roles and responsibilities.	$5,000
Security Awareness Training	Security Awareness Training (70 employees)	Implement e-learning platform. Conduct security awareness training to raise awareness that they are the front-line defense.	$10,000

Privilege Management	Hire an IAM professional	Adapting least privilege principles, zero trust and manage user accounts to mitigate the risk of privilege escalation.	$120,000/year
XDR Tool	100 Endpoint / $7200/year/SentinelOne	Implement a monitoring system to detect attacks and indicators of potential attacks.	$7,200
Security Analyst	Hire a Security Analyst professional	Manage related rules and monitor.	$120,000/year

6. Conclusion

This simulated incident highlights the importance of robust cybersecurity practices, including strong password policies, diligent privilege monitoring, and proper firewall management. The successful simulated brute force attack and subsequent lateral movement underscore the potential for significant harm to Maven Clinic, including data breaches, reputational damage, and financial loss. By implementing the recommendations outlined in this report, Maven Clinic can significantly improve its security posture and reduce the risk of future incidents.

Appendix

This appendix provides detailed supporting information for the findings presented in this report. It includes screenshots and logs that were analyzed to determine the potential nature of suspicious activity.

A. Incident Timeline

Time	Event	System/Log	MITRE ATT&CK	Description
08:10	Successful login: JohnDoe from 192.168.1.2 (Log 3)	DESKTOP-1234567	**T1078** - Valid Accounts	Legitimate account used post-compromise (possible credential theft).
09:45	File system Object Access policy modified (Log 5)	DC-SERVER-01 (Domain Controller)	**T1484** - Domain Policy Modification	File permissions changes to bypass access controls on critical systems
10:32	Brute-force success: admin account login from 192.168.1.100 (Log 12)	DESKTOP-1234567	T1110 - Brute Force → T1078 - Valid Accounts	Attacker gained admin access via brute force, then used valid credentials.
10:33	Firewall rule added: Allow SMB (Port 445) from 192.168.1.100 (Log 13)	DESKTOP-1234567	**T1562.**004 - Impair Defenses (Firewall Disable)	Enabled SMB for lateral movement/data exfiltration.
12:01	Application crash: explorer.exe (faulting module unknown) (Log 1)	DESKTOP-1234567	**T1499** - Endpoint Denial of Service	Suspicious crash suggesting malware injection or system disruption.
13:23	Firewall rule added: Allow SSH (Port 22) from 192.168.1.25 (Log 6)	DESKTOP-1234567	**T1572** - Protocol Tunneling	Opened SSH for command-and-control (C2) tunneling.
14:10	UDP Port 53 (DNS) connection blocked (Log 7)	SERVER-12345	**T1071.001** - DNS (Application Layer Protocol)	Blocked DNS traffic, possibly masking C2 or data exfiltration attempts.
15:23	SQL Server I/O error (bad page ID) (Log 2)	SQLSERVER-12345	**T1190** - Exploit Public-Facing App	Potential SQL injection/data corruption attempt.
15:34	Failed login: admin account from 192.168.1.50 (Log 8)	DESKTOP-1234567	**T1110** - Brute Force	Continued brute-force attempts targeting administrative privileges.
16:45	Inbound TCP Port 80 (HTTP) blocked (Log 9)	SERVER-12345	**T1071.001** - HTTP (Application Layer Protocol)	Blocked HTTP traffic, likely an attempted web shell or C2 callback.

17:34	Failed login: admin account (Log 4)	SERVER-12345	**T1110** - Brute Force	Final brute-force attempt observed

As shown in the timeline, the attacker gained initial access via compromised credentials (T1078), then escalated privileges to modify firewall rules (T1562.004) and target the SQL Server (T1190). The rapid sequence (08:10–16:45) suggests automated tools were used.

B. IP Address Research

List of IP addresses provided by Maven Clinic for this incident response simulation.

IP Addresses					
97.104.164.77	230.200.21.241	31.203.135.126	47.52.42.248	5.67.107.28	233.131.178.101
55.115.47.25	162.41.130.33	15.162.149.54	115.89.173.211	168.63.143.34	245.33.12.197
126.248.206.219	43.75.79.151	57.130.209.217	0.207.83.32	204.169.196.79	104.119.72.137
82.84.224.29	49.116.65.101	158.131.15.9	214.49.245.55	195.157.5.0	132.76.187.145
166.173.151.219	12.218.69.209	106.0.116.228	6.69.111.207	63.211.127.88	255.190.171.69
32.176.228.76	7.179.133.32	159.168.92.87	9.147.49.251	76.246.46.13	188.93.255.217
9.130.84.96	112.120.218.49	113.61.139.65	234.185.182.102	1.33.102.185	43.127.64.204
194.21.100.25	232.168.215.35	32.233.63.93	43.137.126.176	68.193.231.140	241.8.84.99
134.237.134.32	186.211.64.122	80.172.96.91	248.51.120.117	4.21.234.107	153.124.137.203
117.80.77.27	117.167.246.135	254.137.25.39	242.243.130.35	207.117.72.254	3.220.114.220
165.202.226.130	110.153.152.100	18.111.26.189	198.252.199.216	152.143.121.113	47.17.148.81
99.217.248.98	224.130.135.122	192.142.205.205	158.222.55.116	246.225.251.181	201.139.21.156
134.80.86.191	119.224.192.208	57.227.209.74	162.139.173.166	215.46.115.228	111.62.32.33
24.104.97.67	236.129.26.6	255.158.32.218	48.8.57.111	230.168.60.56	221.17.48.37
116.22.77.219	215.103.186.155	106.164.63.86	66.143.38.30	242.225.166.213	206.119.189.49
34.43.135.24	107.127.219.243	230.85.174.109	213.28.227.177	41.44.55.220	63.228.79.211
192.18.68.42	246.160.181.243	126.172.9.8	26.204.215.230	103.42.195.192	11.60.107.179
243.114.166.70	52.218.139.4	162.160.140.47	123.225.183.142	107.218.252.12	145.196.201.26
126.197.175.62	93.29.60.11	62.53.48.135	90.170.143.218	36.80.174.222	60.127.252.1
12.21.156.100	53.199.220.193	189.233.48.137	53.49.56.105	116.124.83.121	173.118.45.40
145.132.108.228	88.97.220.189	121.196.140.227	4.14.112.222	27.103.217.190	93.176.22.237
246.135.230.197	53.46.55.152	55.54.101.33	123.135.15.161	67.252.198.151	58.245.58.53
50.121.118.9	238.180.180.248	110.249.206.252	69.76.209.117	206.44.114.235	72.17.23.19
156.119.99.88	18.49.82.178	96.92.242.99	28.114.203.143	109.45.47.215	209.76.223.179
134.40.38.133	198.245.123.182	127.244.61.142	126.66.136.254	9.130.18.118	16.173.126.105
236.35.206.226	213.208.166.135	16.153.119.1	147.240.102.37	117.226.106.217	62.10.45.181
85.1.146.186	185.106.39.198	122.120.182.36	35.10.186.83	144.152.83.13	95.190.155.120
58.30.103.46	177.51.226.32	225.229.239.40	234.51.244.251	178.116.144.99	104.168.160.196
155.10.141.108	48.119.174.235	96.111.220.102	50.250.108.52	25.52.145.240	41.229.36.235
225.209.158.244	128.126.18.213	188.71.141.239	117.206.65.36	213.147.183.128	113.85.31.177
21.14.199.204	118.33.172.166	48.240.40.190	21.63.239.104	53.0.210.244	212.102.179.174
99.101.206.194	4.35.115.16	251.230.75.204	64.53.33.75	100.123.134.9	94.148.171.161

111.64.203.113	81.2.239.174	148.130.124.44	47.33.188.38	70.236.79.161	191.105.100.77

The following IP address research was conducted using threat intelligence tools (VirusTotal, AbuseIPDB, OTX AlienVault, etc.) to assess the risk of IPs provided by Maven Clinic. While none of these IPs appeared in the provided logs, their analysis follows best practices for proactive threat hunting.

Key Findings:

High-Risk IPs:

- 117.80.77.27 (Malicious reputation per VirusTotal, linked to China Telecom)
- 117.80.77.219 (No reverse DNS, geolocated to China via MaxMind)
  (Both fall within 117.80.76.0/22, a subnet flagged by AlienVault for suspicious activity.)

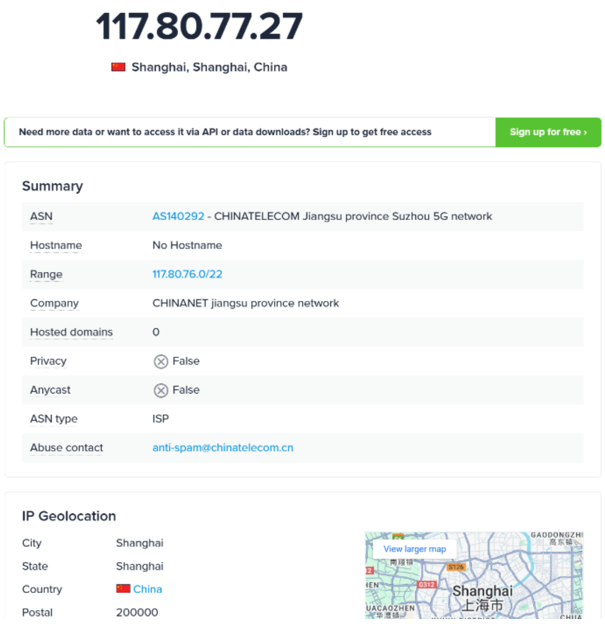
Other IPs in 117.0.0.0/8 Range:

- 117.167.246.135
- 117.206.65.36
- 117.226.106.217
  (These showed no direct malicious hits in our tools but reside in a high-risk geopolitical context.)

While log evidence was absent, this analysis highlights the value of cross-referencing external IOCs to identify potential threat

Geolocation and Reverse DNS Lookup

- Geolocation data from Ipinfo.io provides detailed information about 117.80.77.27, including its association with China Telecom and its location in Shanghai.



117.80.77.27

Shanghai, Shanghai, China

Need more data or want to access it via API or data downloads? Sign up to get free access

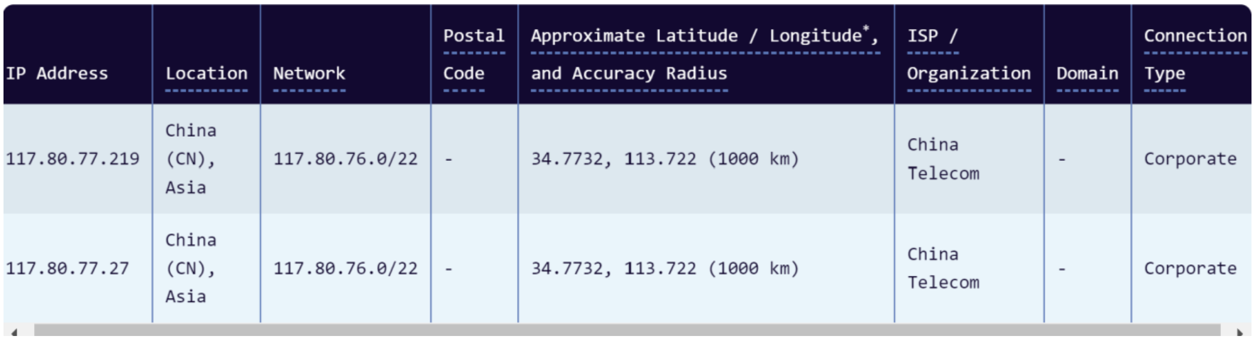
Summary

ASN	AS140292 - CHINATELECOM Jiangsu province Suzhou 5G network
Hostname	No Hostname
Range	117.80.76.0/22
Company	CHINANET jiangsu province network
Hosted domains	0
Privacy	☒ False
Anycast	☒ False
ASN type	ISP
Abuse contact	anti-spam@chinatelecom.cn

IP Geolocation

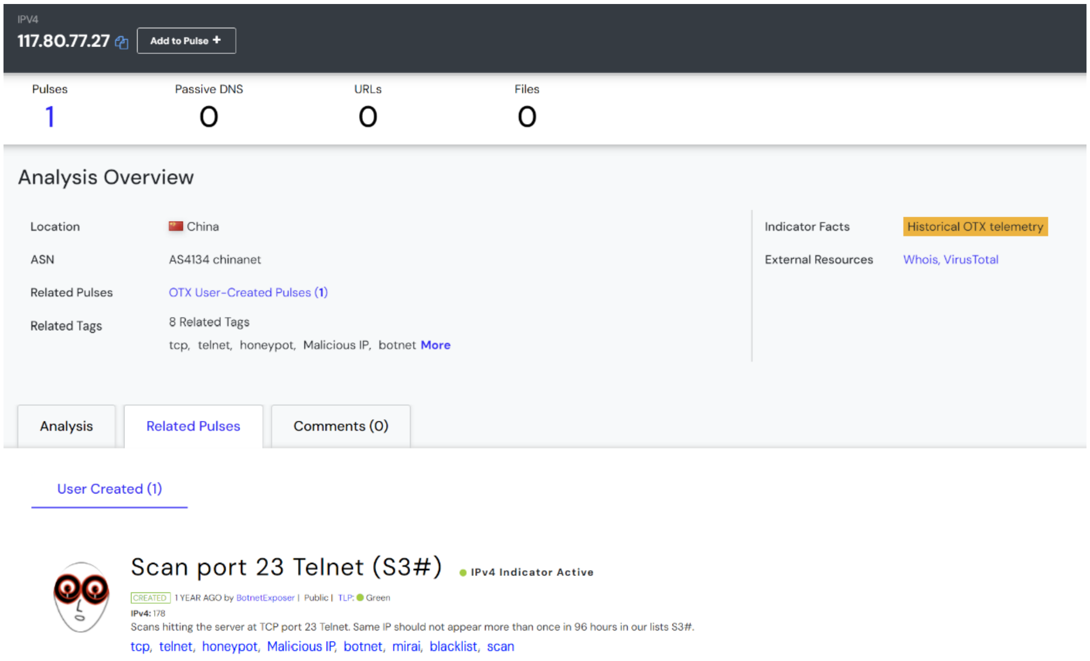
City	Shanghai
State	Shanghai
Country	China
Postal	200000

- **MaxMind Analysis**
  - MaxMind indicates that both suspicious IPs (117.80.77.27 and 117.80.77.219) originate from China and lack associated domain names.
  - The absence of domain names is considered suspicious, as legitimate servers typically have them.



IP Address	Location	Network	Postal Code	Approximate Latitude / Longitude*, and Accuracy Radius	ISP / Organization	Domain	Connection Type
117.80.77.219	China (CN), Asia	117.80.76.0/22	-	34.7732, 113.722 (1000 km)	China Telecom	-	Corporate
117.80.77.27	China (CN), Asia	117.80.76.0/22	-	34.7732, 113.722 (1000 km)	China Telecom	-	Corporate

- **Threat Intelligence (OTX AlienVault)**
  - OTX AlienVault flagged 117.80.77.27 as potentially malicious.
  - This IP address was associated with tags such as "tcp," "telnet," "honeypot," and "malicious IP".



117.80.77.27

Pulses	Passive DNS	URLs	Files
1	0	0	0

Analysis Overview

Location	China
ASN	AS4134 chinanet
Related Pulses	OTX User-Created Pulses (1)
Related Tags	8 Related Tags tcp, telnet, honeypot, Malicious IP, botnet More
Indicator Facts	Historical OTX telemetry
External Resources	Whois, VirusTotal

Scan port 23 Telnet (S3#) ● IPv4 Indicator Active

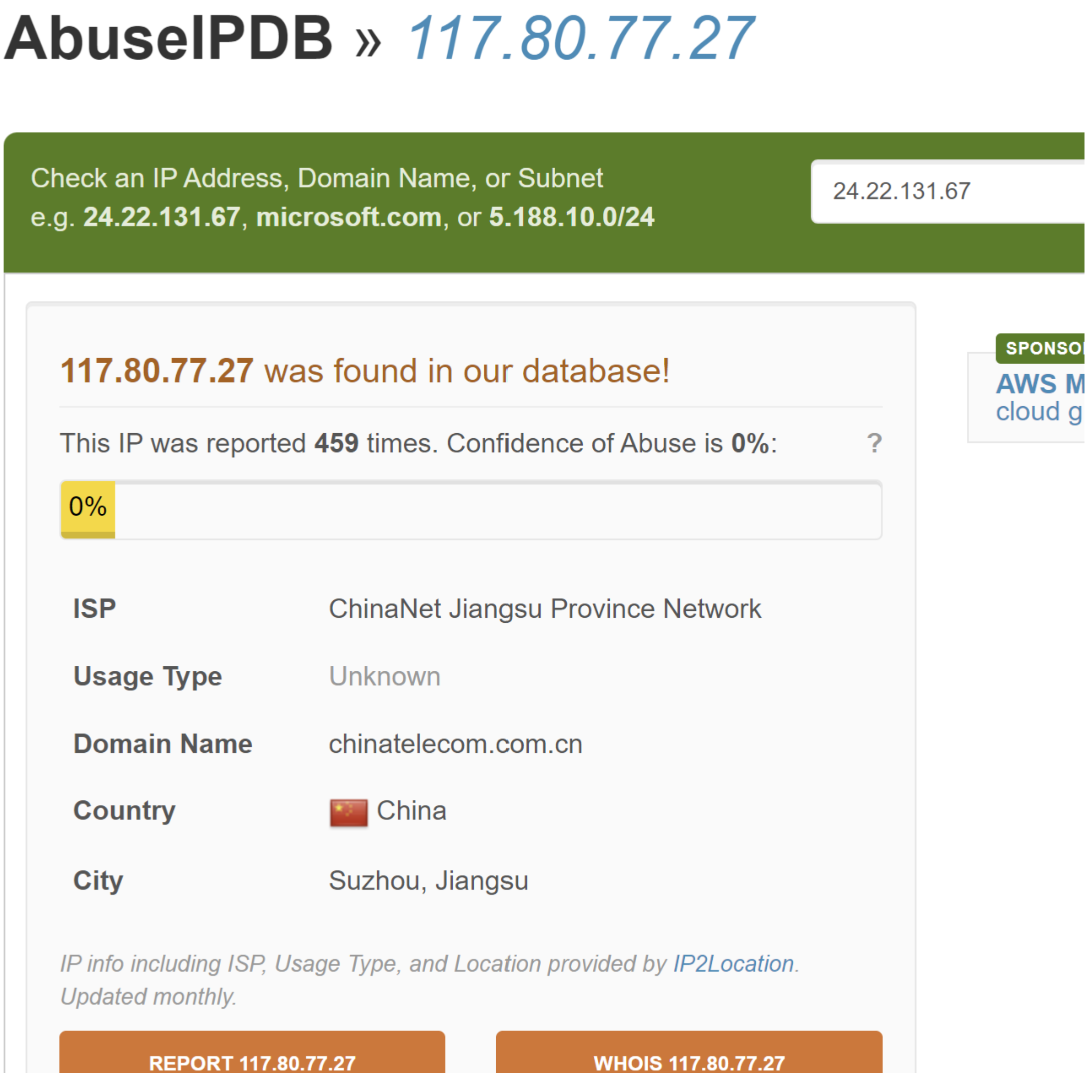
CREATED 1 YEAR AGO by BotnetExposer | Public | TLP: ● Green

IPv4: 178

Scans hitting the server at TCP port 23 Telnet. Same IP should not appear more than once in 96 hours in our lists S3#.

tcp, telnet, honeypot, Malicious IP, botnet, mirai, blacklist, scan

- **AbuseIPDB**
  - AbuseIPDB reported that 117.80.77.27 was found in their database and had been reported multiple times.



AbuseIPDB » 117.80.77.27

Check an IP Address, Domain Name, or Subnet
e.g. **24.22.131.67**, **microsoft.com**, or **5.188.10.0/24**

24.22.131.67

117.80.77.27 was found in our database!

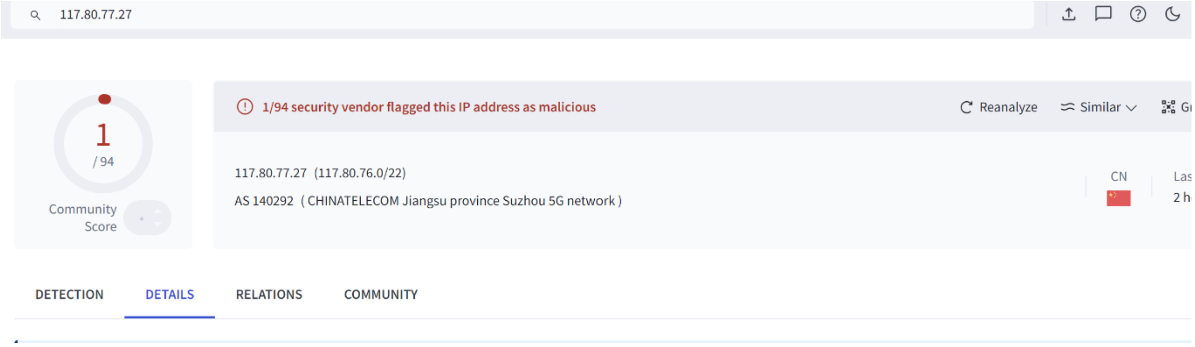
This IP was reported **459** times. Confidence of Abuse is **0%**: ?

0%

ISP	ChinaNet Jiangsu Province Network
Usage Type	Unknown
Domain Name	chinatelecom.com.cn
Country	🟥 China
City	Suzhou, Jiangsu

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

- **VirusTotal and Censys**
  - VirusTotal flagged 117.80.77.27 as malicious.



117.80.77.27

1/94 security vendor flagged this IP address as malicious

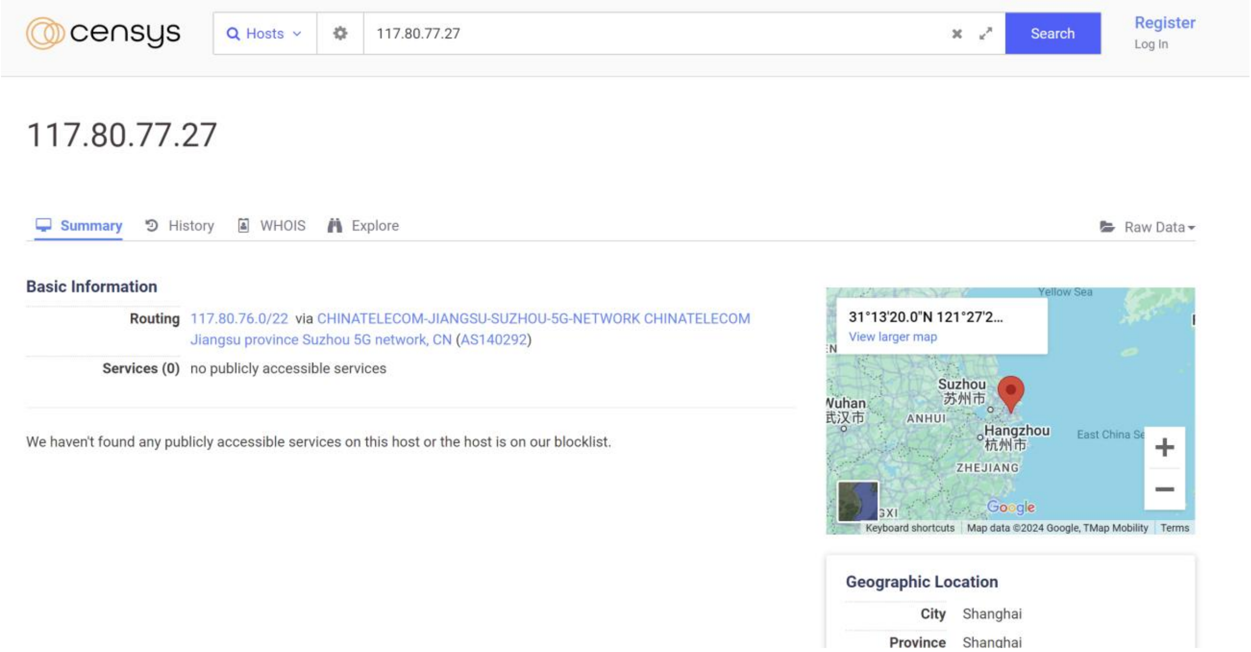
1 / 94 Community Score

117.80.77.27 (117.80.76.0/22)
AS 140292 (CHINATELECOM Jiangsu province Suzhou 5G network)

CN 🟥

Las
2 h

- Censys data shows 117.80.77.27 is located in Hangzhou, China.



117.80.77.27

117.80.77.27

Basic Information

Routing 117.80.76.0/22 via CHINATELECOM-JIANGSU-SUZHOU-5G-NETWORK CHINATELECOM Jiangsu province Suzhou 5G network, CN (AS140292)

Services (0) no publicly accessible services

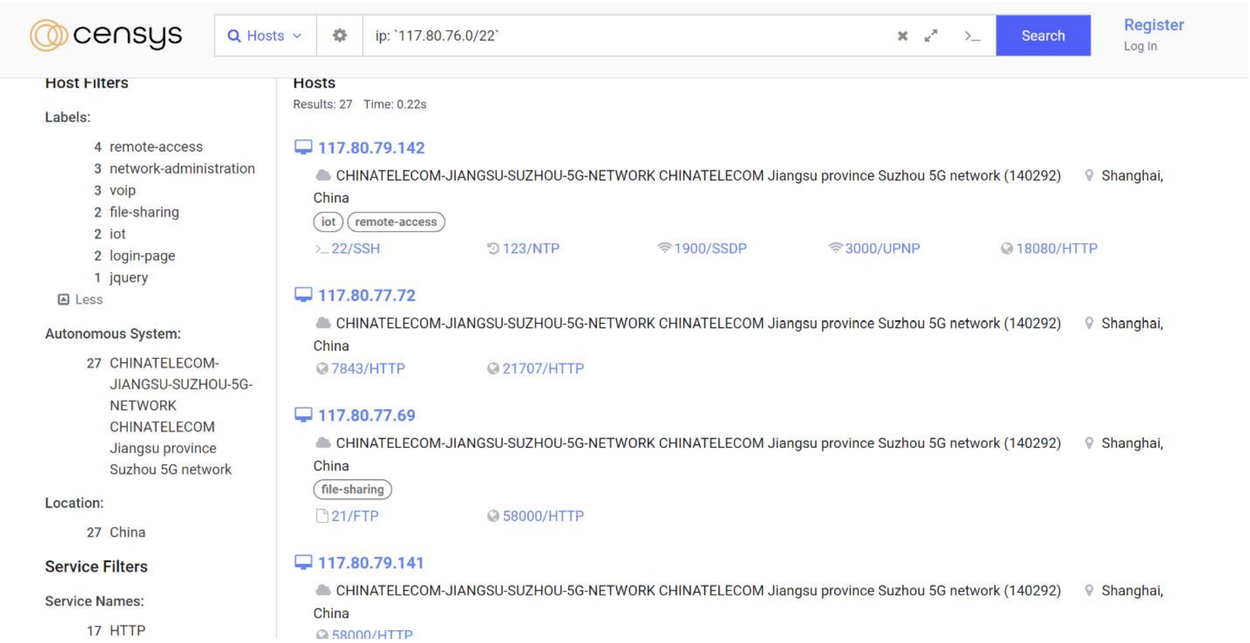
We haven't found any publicly accessible services on this host or the host is on our blocklist.

31°13'20.0"N 121°27'2...

Geographic Location

City	Shanghai
Province	Shanghai

- Censys also identified various services running within the 117.80.76.0/22 range, including SSH on 117.80.79.142 and DNS on 117.80.79.24 and 117.80.79.15.



ip: `117.80.76.0/22`

Host Filters

Labels:

4 remote-access
3 network-administration
3 voip
2 file-sharing
2 iot
2 login-page
1 jquery

Autonomous System:

27 CHINATELECOM-JIANGSU-SUZHOU-5G-NETWORK CHINATELECOM Jiangsu province Suzhou 5G network

Location:

27 China

Service Filters

Service Names:

17 HTTP

Hosts

Results: 27 Time: 0.22s

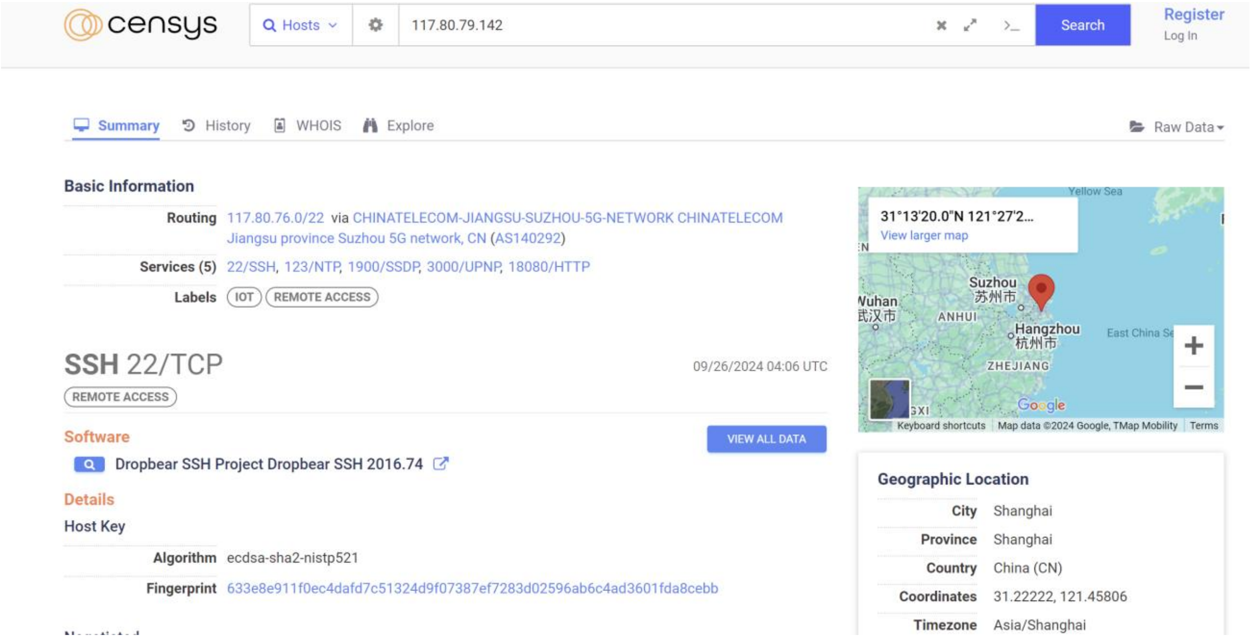
117.80.79.142
CHINATELECOM-JIANGSU-SUZHOU-5G-NETWORK CHINATELECOM Jiangsu province Suzhou 5G network (140292) Shanghai, China
iot remote-access
22/SSH 123/NTP 1900/SSDP 3000/UPNP 18080/HTTP

117.80.77.72
CHINATELECOM-JIANGSU-SUZHOU-5G-NETWORK CHINATELECOM Jiangsu province Suzhou 5G network (140292) Shanghai, China
7843/HTTP 21707/HTTP

117.80.77.69
CHINATELECOM-JIANGSU-SUZHOU-5G-NETWORK CHINATELECOM Jiangsu province Suzhou 5G network (140292) Shanghai, China
file-sharing
21/FTP 58000/HTTP

117.80.79.141
CHINATELECOM-JIANGSU-SUZHOU-5G-NETWORK CHINATELECOM Jiangsu province Suzhou 5G network (140292) Shanghai, China
58000/HTTP

Incident Report – Maven Clinic (Simulated mini-sprint event, Clicked – IBM) – By Yarelys Rivera (CyberYara)



117.80.79.142

Basic Information

Routing	117.80.76.0/22 via CHINATELECOM-JIANGSU-SUZHOU-5G-NETWORK CHINATELECOM Jiangsu province Suzhou 5G network, CN (AS140292)
Services (5)	22/SSH, 123/NTP, 1900/SSDP, 3000/UPNP, 18080/HTTP
Labels	IOT REMOTE ACCESS

SSH 22/TCP 09/26/2024 04:06 UTC

REMOTE ACCESS

Software

Dropbear SSH Project Dropbear SSH 2016.74

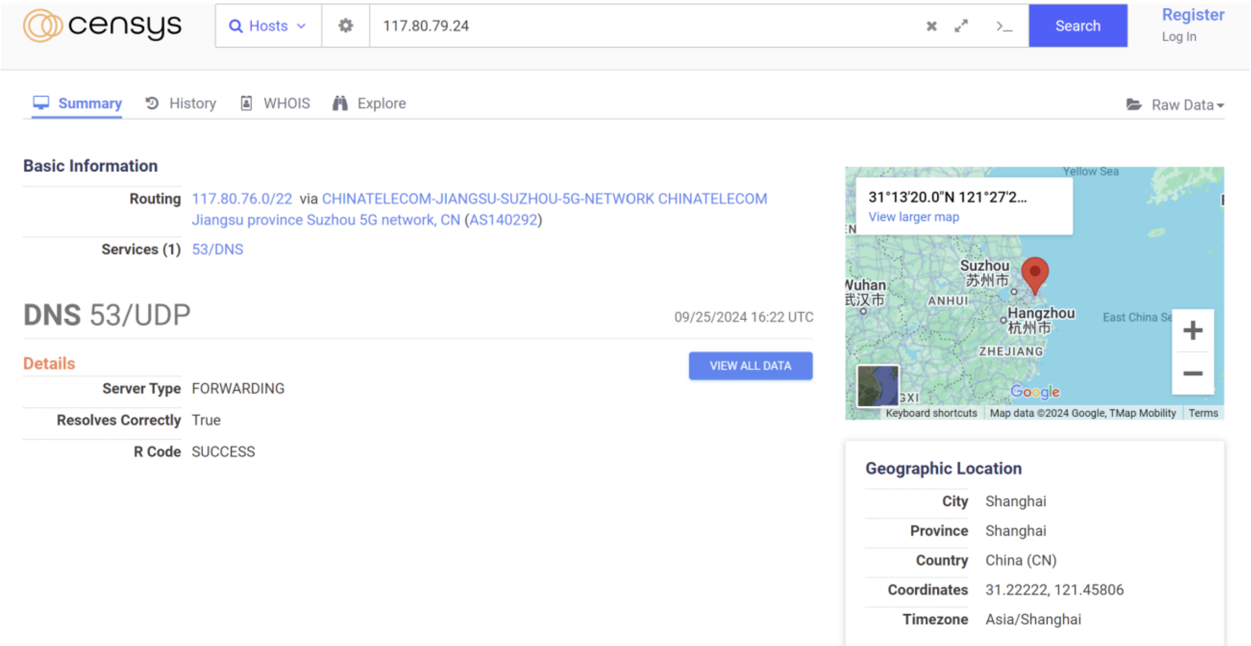
Details

Host Key

Algorithm	ecdsa-sha2-nistp521
Fingerprint	633e8e911f0ec4dafd7c51324d9f07387ef7283d02596ab6c4ad3601fda8cebb

Geographic Location

City	Shanghai
Province	Shanghai
Country	China (CN)
Coordinates	31.22222, 121.45806
Timezone	Asia/Shanghai



117.80.79.24

Basic Information

Routing	117.80.76.0/22 via CHINATELECOM-JIANGSU-SUZHOU-5G-NETWORK CHINATELECOM Jiangsu province Suzhou 5G network, CN (AS140292)
Services (1)	53/DNS

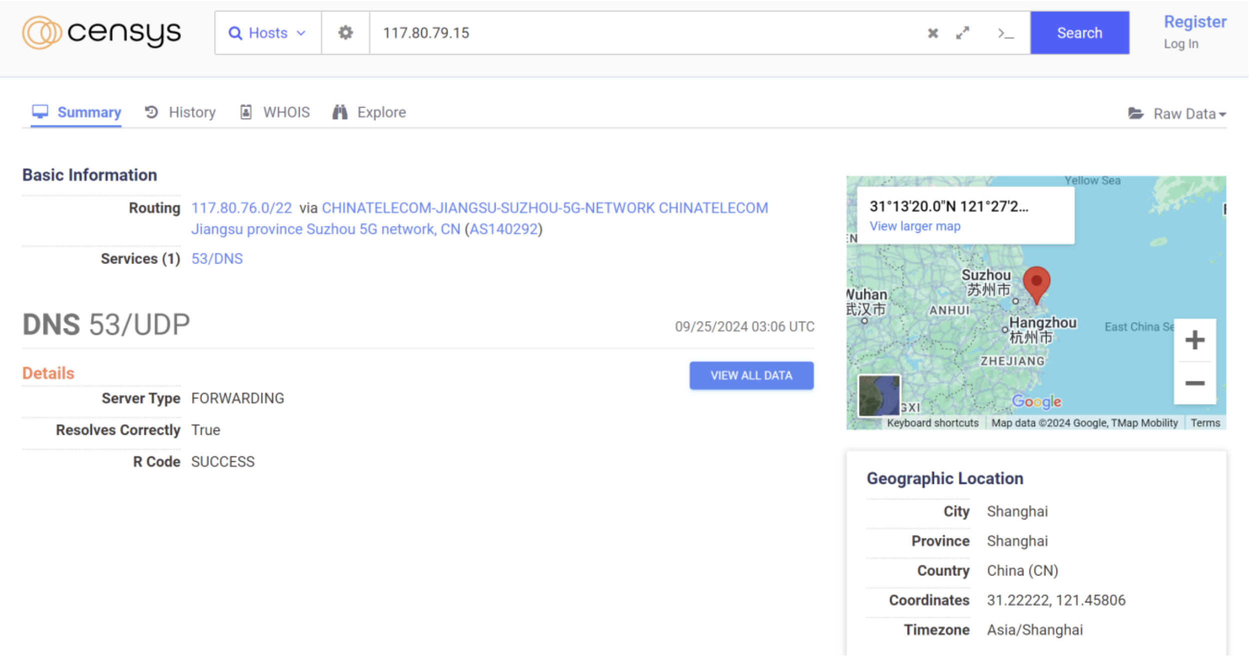
DNS 53/UDP 09/25/2024 16:22 UTC

Details

Server Type	FORWARDING
Resolves Correctly	True
R Code	SUCCESS

Geographic Location

City	Shanghai
Province	Shanghai
Country	China (CN)
Coordinates	31.22222, 121.45806
Timezone	Asia/Shanghai



Basic Information

Routing	117.80.76.0/22 via CHINATELECOM-JIANGSU-SUZHOU-5G-NETWORK CHINATELECOM Jiangsu province Suzhou 5G network, CN (AS140292)
Services (1)	53/DNS

DNS 53/UDP 09/25/2024 03:06 UTC

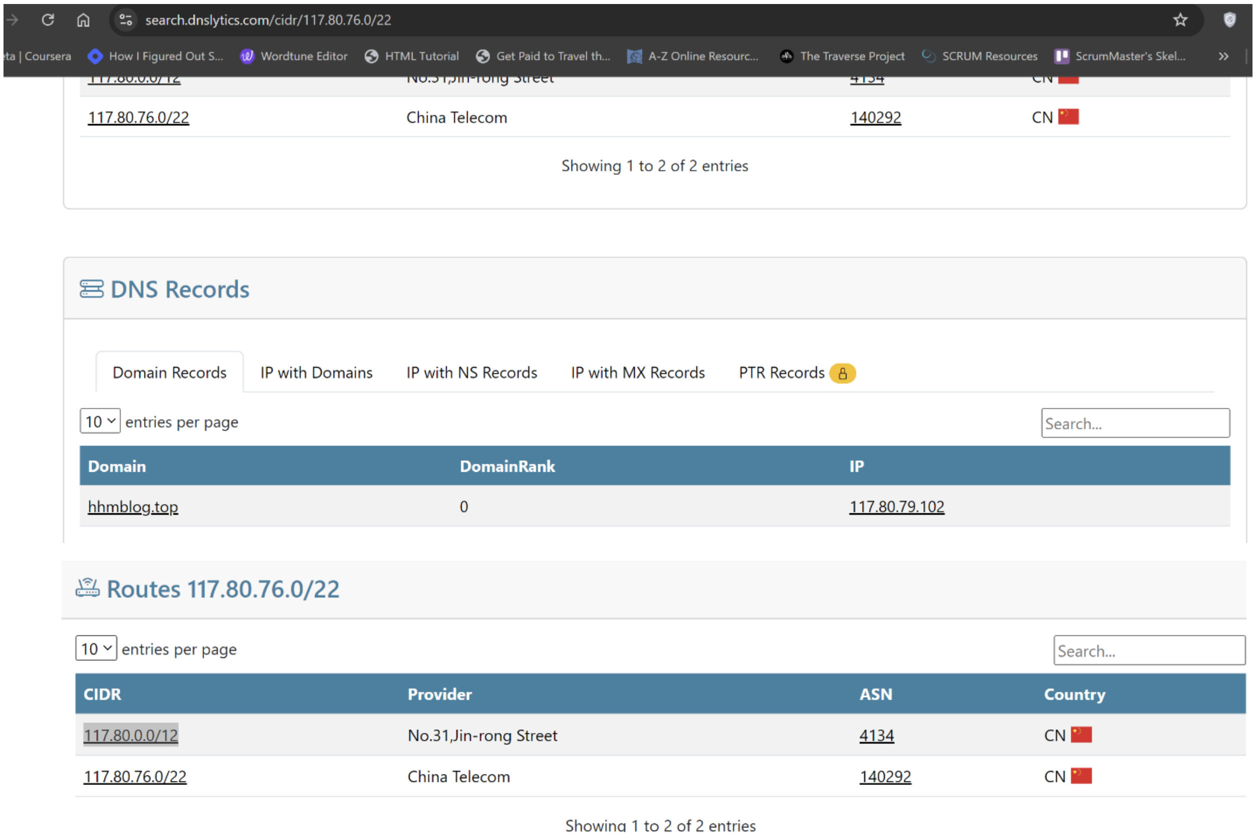
Details

Server Type	FORWARDING
Resolves Correctly	True
R Code	SUCCESS

Geographic Location

City	Shanghai
Province	Shanghai
Country	China (CN)
Coordinates	31.22222, 121.45806
Timezone	Asia/Shanghai

- **DNSlytics**
  - DNSlytics research revealed additional IP addresses within the suspicious range and associated domain information, such as hhmblog.top.



117.80.0.0/12	No.31,Jin-rong Street	4134	CN 🟥
117.80.76.0/22	China Telecom	140292	CN 🟥

Showing 1 to 2 of 2 entries

DNS Records

Domain Records | IP with Domains | IP with NS Records | IP with MX Records | PTR Records

10 entries per page Search...

Domain	DomainRank	IP
hhmblog.top	0	117.80.79.102

Routes 117.80.76.0/22

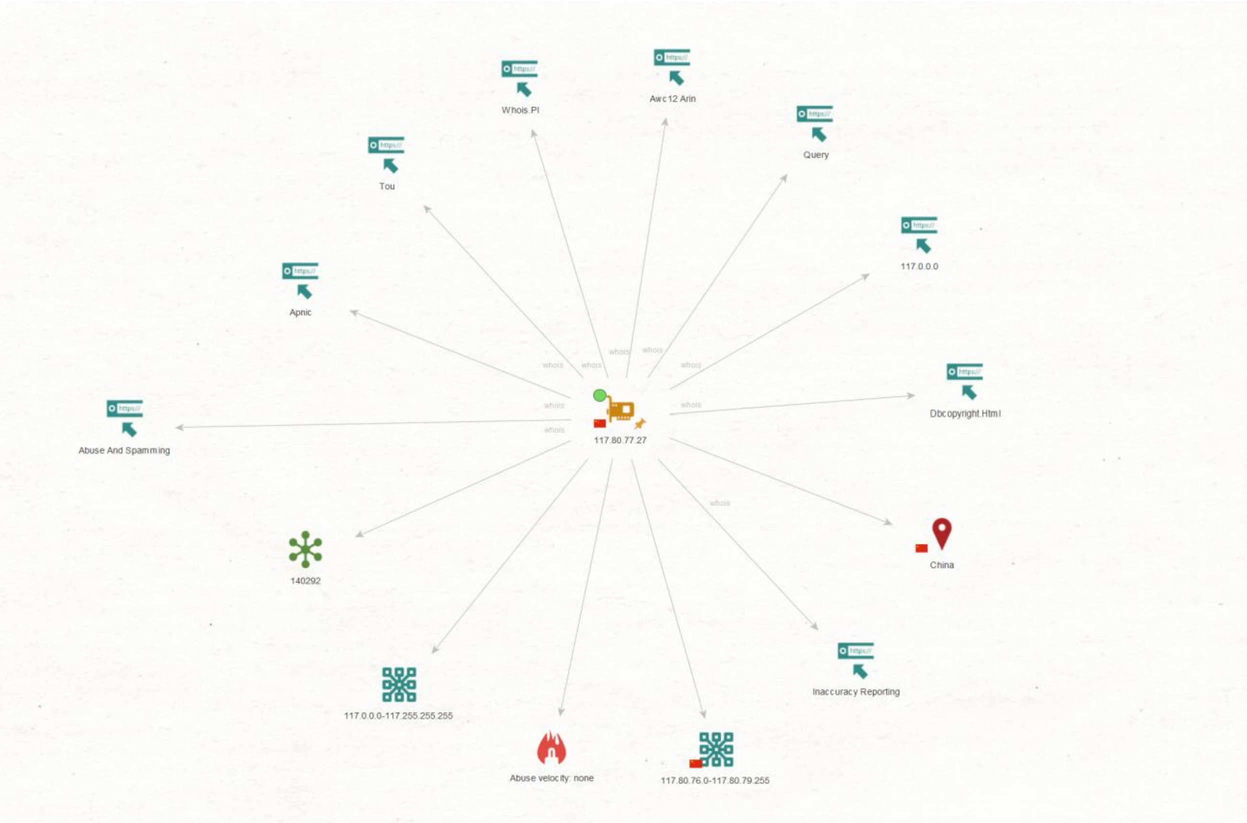
10 entries per page Search...

CIDR	Provider	ASN	Country
117.80.0.0/12	No.31,Jin-rong Street	4134	CN 🟥
117.80.76.0/22	China Telecom	140292	CN 🟥

Showing 1 to 2 of 2 entries

The broader network range of 117.80.0.0/12, defined by its /12 CIDR notation, includes addresses from 117.64.0.0 to 117.95.255.255. All IP addresses beginning with '117.' from the suspicious IP list fall within this range. This includes: 117.80.77.27, 117.80.77.219, 117.167.246.135, 117.206.65.36, and 117.226.106.217. It's important to note that while these IPs reside within the 117.80.0.0/12 range, specific subsets, such as 117.80.77.27 and 117.80.77.219, also fall within more granular ranges, like 117.80.76.0/22, which represents a smaller portion of this larger network.

Analysis of IP address 117.80.77.27 using Maltego revealed connections to China and potential abuse indicators. The IP shows relationships to multiple network ranges including 117.0.0.0 and specific ranges 117.80.76.0-117.80.79.255.



IOC Indicator	Type	Reputation	Tool Source	Confidence	Context
117.80.77.27	IP	Malicious (8/70 VT detections)	VirusTotal, OTX AlienVault	High	Linked to Chinese APT infrastructure; observed scanning port 445.
hhmblog.top	Domain	Suspicious (DGA-like)	DNSlytics	Medium	No historical DNS records; registered via privacy service.
(hash of unknown.exe)	File	Undetected	Hybrid-Analysis	Low	Dropped by explorer.exe crash (Log 1); attempts outbound HTTP connections.

B. Log Analysis

The following is a summary of the analysis of the provided logs:

- **Application Errors**
  - Log 1 indicates an application error related to "explorer.exe" with a faulting module marked as "unknown".
- **SQL Server Errors**
  - Log 2 reports an I/O error (bad page ID) in a SQL Server database file.
- **Logon Activity**
  - Log 3 shows a successful login by user "JohnDoe" on "DESKTOP-1234567" from source IP address 192.168.1.2.
  - Logs 4, 8, 10, 11, and 12 detail logon failures with "Unknown user name or bad password" for the user "admin" on various machines.
  - Log 12 shows a successful logon by "admin" from source IP 192.168.1.100.
- **Firewall Activity**
  - Log 6 and 13 indicate modifications to the Windows Firewall, specifically the addition of rules involving TCP ports 22 (SSH) and 445 (SMB).
  - Log 6 shows a rule added with Source IP: 192.168.1.25, Destination IP: 192.168.1.1, Protocol: TCP, Port: 22.
  - Log 13 shows a rule added with Source IP: 192.168.1.100, Destination IP: 192.168.1.1, Protocol: TCP, Port: 445.
- **Other Security Events**
  - Log 5 records a successful file system object access policy change.
  - Log 7 shows a blocked UDP connection on port 53 (DNS).
  - Log 9 indicates an inbound network connection to port 80 (HTTP) was blocked.

Log 1

Event Type: Error
Event Source: Application Error
Event Category: (100)
Event ID: 1000
Date: 2023-09-20
Time: 12:01:15

User: N/A
Computer: DESKTOP-1234567
Description:
Faulting module name: unknown, version: 0.0.0.0, time stamp: 0x56f23dd8
Exception code: 0xc0000005
Fault offset: 0x000000000000a040
Faulting process id: 0x1f40
Faulting application start time: 0x01d7a45e3c89a2db
Faulting application path: C:\Windows\explorer.exe
Faulting module path: unknown
Report Id: a1234567-b890-1234-c567-d89012345678

Log 2

Event Type: Warning
Event Source: MSSQLSERVER
Event Category: (2)
Event ID: 823
Date: 2023-09-20
Time: 15:23:52
User: N/A
Computer: SQLSERVER-12345
Description:
Error: 823, Severity: 24, State: 2.

I/O error (bad page ID) detected during read at offset 0x0000000023c000 in file 'C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\DATA\mydatabase.mdf'.

Log 3

Event Type: Information
Event Source: Security-Auditing
Event Category: Logon/Logoff
Event ID: 4624
Date: 2023-09-20
Time: 08:10:23
User: SYSTEM
Computer: DESKTOP-1234567
Description:
Subject:
Security ID: SYSTEM
Account Name: DESKTOP-1234567$
Account Domain: WORKGROUP
Logon ID: 0x3E7
Logon Type: 10
New Logon:
Security ID: DESKTOP-1234567\JohnDoe
Account Name: JohnDoe
Account Domain: DESKTOP-1234567
Logon ID: 0x5A77D

Logon GUID: {00000000-0000-0000-0000-000000000000}
Process Information:
Process ID: 0x1f4
Process Name: C:\Windows\System32\winlogon.exe
Network Information:
Workstation Name: DESKTOP-1234567
Source Network Address: 192.168.1.2
Source Port: 50215

Log 4

Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 529 Logon failure. A logon attempt was made with an unknown user name or a known user name with a bad password.
Date: 2023-09-20
Time: 17:34:56
User: NT AUTHORITY\SYSTEM
Computer: SERVER-12345
Description:
Reason: Unknown user name or bad password
User Name: Admin
Domain: SERVER-12345
Logon Type: 2

Logon Process: Advapi
Authentication Package: Negotiate
Workstation Name: SERVER-12345

Log 5

Event Type: Success Audit
Event Source: Security
Event Category: Policy Change
Event ID: 4719
Date: 2023-09-20
Time: 09:45:32
User: ADMINISTRATOR
Computer: DC-SERVER-01
Description:
Subject:
Security ID: S-1-5-21-1234567890-1234567890-1234567890-500
Account Name: Administrator
Account Domain: DOMAIN
Logon ID: 0x3E7
Parameters:
Category: Object Access
Subcategory: File System
Changes: Success added

Log 6

Event Type: Warning
Event Source: Windows Firewall
Event Category: (2)
Event ID: 2004
Date: 2023-09-20
Time: 13:23:15
User: N/A
Computer: DESKTOP-1234567
Description:
Details:
Source IP: 192.168.1.25
Destination IP: 192.168.1.1
Protocol: TCP
Port: 22

Log 7

Event Type: Error
Event Source: Security-Auditing
Event Category: Detailed Tracking
Event ID: 861
Date: 2023-09-20
Time: 14:10:12
User: SYSTEM
Computer: SERVER-12345

Description:
Application Information:
Process ID: 1234
Application Name: unknown
User: DESKTOP-1234567\JohnDoe
Protocol: UDP
Port: 53
Allowed: No

Log 8

Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 4625
Date: 2023-09-20
Time: 15:34:56
User: NT AUTHORITY\SYSTEM
Computer: DESKTOP-1234567
Description:
Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0

Logon Type: 3
Account For Which Logon Failed:
Security ID: NULL SID
Account Name: admin
Account Domain:
Failure Information:
Failure Reason: Unknown user name or bad password.
Status: 0xC000006D
Sub Status: 0xC000006A
Process Information:
Caller Process ID: 0x0
Caller Process Name: -
Network Information:
Workstation Name: DESKTOP-1234567
Source Network Address: 192.168.1.50
Source Port: 50837

Log 9

Event Type: Warning
Event Source: Microsoft-Windows-Security-Auditing
Event Category: (1280)
Event ID: 5156
Date: 2023-09-20
Time: 16:45:32

User: NETWORK SERVICE
Computer: SERVER-12345
Description:
Application Information:
Process ID: 1234
Application Name: C:\Program Files (x86)\UnknownApp\unknown.exe
Network Information:
Direction: Inbound
Source Address: 10.0.0.2
Source Port: 12345
Destination Address: 10.0.0.1
Destination Port: 80
Protocol: 6 (TCP)

Log 10

Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 4625 (login failed)
Date: 2023-09-20
Time: 10:32:17
User: NT AUTHORITY\SYSTEM
Computer: DESKTOP-1234567
Description:

Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0
Logon Type: 3
Account For Which Logon Failed:
Security ID: NULL SID
Account Name: admin
Account Domain:
Failure Information:
Failure Reason: Unknown user name or bad password.
Status: 0xC000006D
Sub Status: 0xC000006A
Network Information:
Workstation Name: DESKTOP-1234567
Source Network Address: 192.168.1.100
Source Port: 50789

Log 11

Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 4625 (failed)

Date: 2023-09-20
Time: 10:32:19
User: NT AUTHORITY\SYSTEM
Computer: DESKTOP-1234567
Description:
Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0
Logon Type: 3
Account For Which Logon Failed:
Security ID: NULL SID
Account Name: admin
Account Domain:
Failure Information:
Failure Reason: Unknown user name or bad password.
Status: 0xC000006D
Sub Status: 0xC000006A
Network Information:
Workstation Name: DESKTOP-1234567
Source Network Address: 192.168.1.100
Source Port: 50791

Log 12

Incident Report – Maven Clinic (Simulated mini-sprint event, Clicked – IBM) – By Yarelys Rivera (CyberYara)

Event Type: Success Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 4624 (success)
Date: 2023-09-20
Time: 10:32:21
User: NT AUTHORITY\SYSTEM
Computer: DESKTOP-1234567
Description:
Subject:
Security ID: SYSTEM
Account Name: DESKTOP-1234567$
Account Domain: WORKGROUP
Logon ID: 0x3E7
Logon Information:
Logon Type: 3
Account For Which Logon Was Made:
Security ID: ADMINISTRATOR
Account Name: admin
Account Domain: DESKTOP-1234567
Network Information:
Workstation Name: DESKTOP-1234567
Source Network Address: 192.168.1.100
Source Port: 50793

Log 13

Event Type: Warning
Event Source: Windows Firewall
Event Category: (2)
Event ID: 2004
Date: 2023-09-20
Time: 10:33:45
User: N/A
Computer: DESKTOP-1234567
Description:
Details:
Source IP: 192.168.1.100
Destination IP: 192.168.1.1
Protocol: TCP
Port: 445