

Incident Report: Maven Clinic Network Intrusion

Executive Summary:

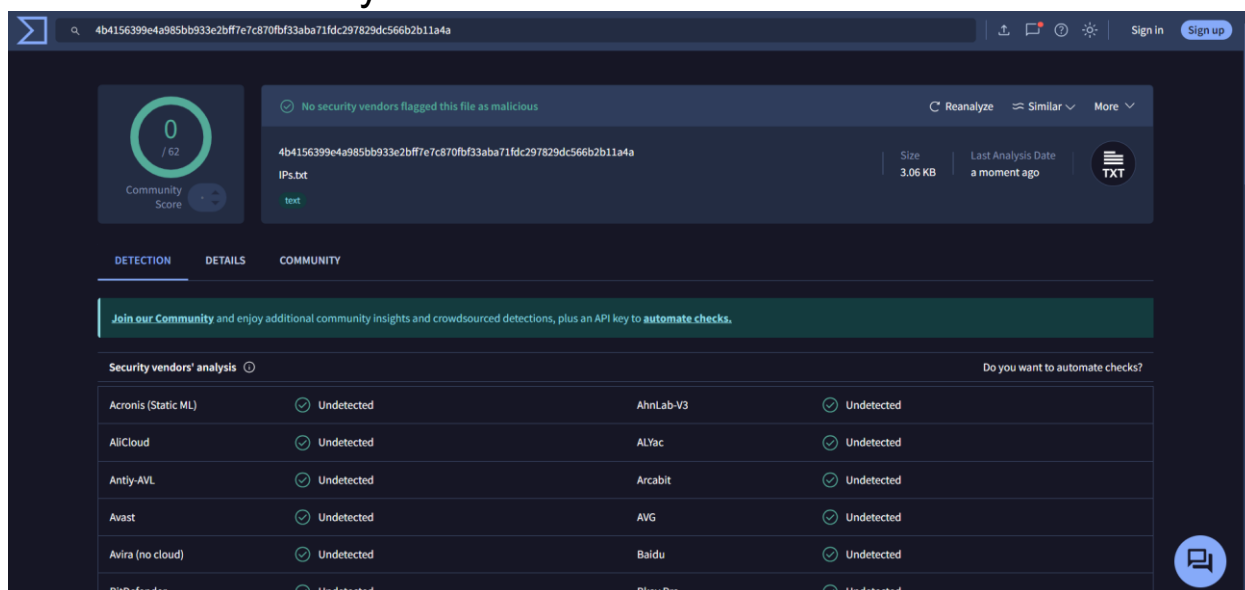
On September 20, 2023, Maven Clinic experienced a cybersecurity incident involving multiple systems within our network. The incident involved unauthorized access attempts, successful intrusion, and potential data compromise. This report details our findings, response actions, and recommendations for future prevention.

Identification and Investigation:

Checking the Ip's :

As part of the team's ongoing investigation into the recent network activity, all identified IP addresses were analyzed using both **VirusTotal** and **Angry IP Scanner**.

The result of VirusTotal showed no suspicious or malicious activity associated with any of the IPs.



The screenshot shows the VirusTotal interface for a file named 'IPs.txt' with SHA256 hash 4b4156399e4a985bb933e2bfff7e7c870bf33aba71fdc297829dc566b2b11a4a. The file is 3.06 KB and was analyzed 'a moment ago'. The community score is 0/62. A message states 'No security vendors flagged this file as malicious'. Below, a table lists 10 security vendors, all of which reported the file as 'Undetected'.

Security vendors' analysis		Do you want to automate checks?	
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AllCloud	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	Bkav Pro	Undetected

IP	Ping	Hostname	Ports [6+]
🟢 34.43.135.24	46 ms	24.135.43.34.bc.googleusercontent.com	21,22,80,443,3389,8080
🟢 50.250.108.52	109 ms	[n/a]	21
🟢 4.14.112.222	116 ms	PATTERSON-U.ear2.Denver1.Level3.net	[n/a]
🟢 189.233.48.137	151 ms	[n/a]	[n/a]
🟢 47.33.188.38	147 ms	syn-047-033-188-038.res.spectrum.com	[n/a]
🟢 113.61.139.65	259 ms	113-61-139-65.veetime.com	8080
🟢 82.84.224.29	143 ms	[n/a]	[n/a]
🟢 127.244.61.142	0 ms	[n/a]	[n/a]
🟢 21.63.239.104	112 ms	[n/a]	[n/a]
🟢 85.1.146.186	184 ms	186.146.1.85.dynamic.cust.swisscom.net	[n/a]
🟢 104.168.160.196	122 ms	[n/a]	21,80,443
🟢 178.116.144.99	141 ms	178-116-144-99.access.telenet.be	[n/a]
🟢 93.176.22.237	149 ms	[n/a]	[n/a]
🟢 43.137.126.176	301 ms	[n/a]	[n/a]
🟢 123.135.15.161	330 ms	[n/a]	[n/a]
🟢 60.127.252.1	263 ms	softbank060127252001.bbtec.net	[n/a]
🟢 95.190.155.120	217 ms	[n/a]	[n/a]
🟢 118.33.172.166	307 ms	[n/a]	[n/a]

Open Ports: The presence of open sensitive ports, such as **Port 21 (FTP)**, **Port 22 (SSH)**, or **Port 3389 (RDP)**, could indicate exposure of critical services to the public internet. If these services are not properly secured, they may pose significant vulnerabilities. During the analysis, IP addresses highlighted in **green** were flagged as potentially suspicious due to their access to these open ports.

Hostnames: Recognizable hostnames, such as those associated with trusted domains like **"googleusercontent.com" (Google)**, are generally considered low risk. However, IP addresses without recognizable hostnames or with unknown origins warrant further scrutiny.

Unknown IPs: IPs that do not resolve to a hostname, showing as [n/a], may indicate that the IP is not properly mapped to a domain. This can often be an indicator of less reliable or potentially malicious hosts and should be treated as more suspicious.

Based on the results of Ip I have used Ip Blacklist checker and I found the following result:

Blacklist Check Results for 34.43.135.3

DNSBL	Status	Description
zen.spamhaus.org	Listed	Spamhaus SBL, XBL and PBL
bl.spamcop.net	Not Listed	SpamCop Blocking List
cbl.abuseat.org	Not Listed	Composite Blocking List
dnsbl.sorbs.net	Not Listed	SORBS Domain Name System Blackhole List
b.barracudacentral.org	Not Listed	Barracuda Reputation Block List
bl.emailbasura.org	Listed	EmailBasura
blacklist.woody.ch	Not Listed	Woody's SMTP Blacklist
bogons.cymru.com	Not Listed	Team Cymru Bogon List
combined.abuse.ch	Not Listed	abuse.ch Combined List
db.wpbl.info	Not Listed	Weighted Private Block List

Blacklist Check Results for 50.250.108.52

DNSBL	Status	Description
zen.spamhaus.org	Not Listed	Spamhaus SBL, XBL and PBL
bl.spamcop.net	Not Listed	SpamCop Blocking List
cbl.abuseat.org	Not Listed	Composite Blocking List
dnsbl.sorbs.net	Not Listed	SORBS Domain Name System Blackhole List
b.barracudacentral.org	Not Listed	Barracuda Reputation Block List
bl.emailbasura.org	Listed	EmailBasura
blacklist.woody.ch	Not Listed	Woody's SMTP Blacklist
bogons.cymru.com	Not Listed	Team Cymru Bogon List
combined.abuse.ch	Not Listed	abuse.ch Combined List
db.wpbl.info	Not Listed	Weighted Private Block List

Blacklist Check Results for 113.61.139.65

DNSBL	Status	Description
zen.spamhaus.org	Not Listed	Spamhaus SBL, XBL and PBL
bl.spamcop.net	Not Listed	SpamCop Blocking List
cbl.abuseat.org	Not Listed	Composite Blocking List
dnsbl.sorbs.net	Not Listed	SORBS Domain Name System Blackhole List
b.barracudacentral.org	Not Listed	Barracuda Reputation Block List
bl.emailbasura.org	Listed	EmailBasura
blacklist.woody.ch	Not Listed	Woody's SMTP Blacklist
bogons.cymru.com	Not Listed	Team Cymru Bogon List
combined.abuse.ch	Not Listed	abuse.ch Combined List
db.wpbl.info	Not Listed	Weighted Private Block List

Blacklist Check Results for 104.168.160.96

DNSBL	Status	Description
zen.spamhaus.org	Not Listed	Spamhaus SBL, XBL and PBL
bl.spamcop.net	Not Listed	SpamCop Blocking List
cbl.abuseat.org	Not Listed	Composite Blocking List
dnsbl.sorbs.net	Not Listed	SORBS Domain Name System Blackhole List
b.barracudacentral.org	Not Listed	Barracuda Reputation Block List
bl.emailbasura.org	Listed	EmailBasura
blacklist.woody.ch	Not Listed	Woody's SMTP Blacklist
bogons.cymru.com	Not Listed	Team Cymru Bogon List
combined.abuse.ch	Not Listed	abuse.ch Combined List
db.wpbl.info	Not Listed	Weighted Private Block List

DNS Blacklists (DNSBL): If an IP address is listed on any DNS Blacklist (DNSBL) services, it may suggest that the IP has been associated with **spam or malicious activity**. IPs appearing on such lists may face restrictions, including having their emails blocked or marked as spam by various email providers. This is a potential indicator of compromised or misused systems, warranting further investigation and remediation.

Windows Event Logs:

Log #	Date	Time (ET)	Event Type	Event Source	Event ID
1	2023-09-20	12:01:15	Error	Application Error	1000
2	2023-09-20	15:23:52	Warning	MSSQLSERVER	823
3	2023-09-20	08:10:23	Information	Security-Auditing	4624
4	2023-09-20	17:34:56	Failure Audit	Security	529
5	2023-09-20	09:45:32	Success Audit	Security	4719
6	2023-09-20	13:23:15	Warning	Windows Firewall	2004
7	2023-09-20	14:10:12	Error	Security-Auditing	861
8	2023-09-20	15:34:56	Failure Audit	Security	4625
9	2023-09-20	16:45:32	Warning	Microsoft-Windows-Security-Auditing	5156
10	2023-09-20	10:32:17	Failure Audit	Security	4625
11	2023-09-20	10:32:19	Failure Audit	Security	4625
12	2023-09-20	10:32:21	Success Audit	Security	4624
13	2023-09-20	10:33:45	Warning	Windows Firewall	2004

Log Overview and Key Findings

1. **Date of Events:** All logs are from **2023-09-20**, occurring within a 24-hour period.
2. **Event Types:** Logs cover **errors, warnings, information, and failure/success audits**.
3. **Critical Security Events:**
 - **Failed login attempts** followed by a **successful login** from the same IP address (logs 10, 11, 12).
 - **Firewall warnings** indicating potential unauthorized connection attempts (logs 6, 13).
4. **Affected Systems and Services:** Includes **SQL Server, Windows Security, and Firewall** logs.

Suspicious IPs

Internal IP Addresses Involved in Suspicious Activity:

1. **192.168.1.50:** One failed login attempt (log 8).
2. **192.168.1.100:** Multiple failed login attempts followed by a successful login (logs 10, 11, 12).
3. **10.0.0.2:** Inbound connection attempt to an unknown application (log 9).

These internal IP addresses do not appear in the provided external IP list. Their involvement suggests possible insider threats or compromised internal systems.

Windows Event Logs Analysis

Failed Login Attempts:

- **Logs 10, 11:** Multiple failed login attempts for user "**admin**" from **192.168.1.100**, suggesting a brute-force attempt.
- **Log 4, Log 8:** Failed logins for user "**Admin**" from **192.168.1.50** and **SERVER-12345**.

Successful Login:

- **Log 12:** Successful login for user "**admin**" from **192.168.1.100** after multiple failed attempts, indicating potential credential compromise.

Firewall Warnings:

- **Log 6:** Attempted connection to **Port 22 (SSH)** from **192.168.1.25**.
- **Log 13:** Attempted connection to **Port 445 (SMB)** from **192.168.1.100**.

Other Suspicious Events:

- **Log 2: SQL Server I/O error** could indicate database tampering.
- **Log 5: Policy change** under "Object Access" on **DC-SERVER-01**, requiring verification.
- **Log 7:** Blocked **UDP connection to Port 53 (DNS)**, suggesting unauthorized DNS activity.
- **Log 9: Unknown inbound connection** from **10.0.0.2** to an unknown application.

Category	Finding	Severity	Evidence
Authentication	Multiple failed login attempts for "admin" account	High	Logs 8, 10, 11
Authentication	Successful login after failed attempts	High	Log 12
Network	Firewall warnings for SSH and SMB connections	Medium	Logs 6, 13
System	Explorer.exe application error	Low	Log 1
Database	SQL Server I/O error	Medium	Log 2
Policy	Security policy change by Administrator	Medium	Log 5
Network	Unknown application attempting inbound communication	Medium	Log 9

Systems & Services Impact

Affected Systems:

DESKTOP-1234567: The primary target for login attempts and associated firewall warnings.

SERVER-12345: Experienced a blocked UDP connection attempt and inbound communication from an unknown application.

SQLSERVER-12345: Detected an I/O error, indicating potential issues with data integrity.

DC-SERVER-01: Recorded a policy change that requires verification.

Potentially Affected Services:

Microsoft SQL Server: The I/O error on **SQLSERVER-12345** could affect database operations and integrity.

Windows Firewall: Logged multiple warnings on **DESKTOP-1234567**, suggesting potential unauthorized access attempts.

Active Directory: Changes made on **DC-SERVER-01** could impact user access and permissions.

Potential Compromises

Admin Account Compromise: The "admin" account may be compromised, as indicated by a successful login following multiple failed attempts from **192.168.1.100**.

Targeted System: **DESKTOP-1234567** exhibits signs of being a primary target, warranting further investigation for potential compromise.

SQL Server Integrity Risk: The I/O error on **SQLSERVER-12345** raises concerns about possible data integrity issues or unauthorized modifications.

Unknown Application Threat: The inbound connection from an unknown application on **SERVER-12345** could signify malware or unauthorized software, necessitating a thorough investigation.

Questions for Stakeholders

1. Is the successful "admin" login expected behavior after the failed attempts from the same IP address (192.168.1.100)?
2. Was the security policy change on DC-SERVER-01 authorized and what specific changes were made?
3. Are the firewall warnings for SSH (port 22) and SMB (port 445) connections expected for normal operations?
4. What is the nature of the unknown application attempting inbound communication on SERVER-12345?
5. Has there been any recent maintenance or changes to the SQL Server on SQLSERVER-12345 that could explain the I/O error?

RESPONSE CONTAINMENT & ERADICATION:

Based on the identified unusual network activity at Maven Clinic, the following short-term and long-term containment plans are outlined to prevent further damage and eliminate the threat. These plans focus on isolating affected systems, implementing necessary security measures, and strengthening overall system protection.

Short-Term Containment Plan

1. Isolate Affected Systems

DESKTOP-1234567 will be immediately disconnected from the network, as it is identified as the primary target of suspicious activities.

Network access for **SERVER-12345** and **SQLSERVER-12345** will be temporarily disabled to prevent the potential spread of malicious activity.

2. Block Suspicious IP Addresses

Firewalls will be configured to block incoming connections from **192.168.1.100**, which was involved in multiple failed login attempts followed by a successful admin login.

Connections from **192.168.1.25** (attempted SSH connection) and **192.168.1.50** (failed login attempt) will also be temporarily blocked.

3. Disable Compromised Accounts

The "admin" account, which was successfully accessed after multiple failed login attempts, will be immediately disabled.

Other accounts showing suspicious activity will be reviewed and temporarily disabled as necessary.

4. Preserve Evidence

Forensic images of the affected systems (DESKTOP-1234567, SERVER-12345, SQLSERVER-12345) will be created for later analysis.

All relevant logs will be securely backed up and preserved to ensure they remain intact for investigation.

5. Monitor Network Traffic

Enhanced logging and monitoring will be implemented across all systems, with a focus on outbound connections to detect potential data exfiltration attempts.

Long-Term Containment Plan

1. System Patching and Updates

A comprehensive patching plan will be developed, prioritizing critical security updates across all systems.

Regular patch management cycles will be scheduled to ensure ongoing system security and reduce vulnerabilities.

2. Firewall Rule Enhancement

Firewall rules will be reviewed and updated to restrict unnecessary inbound and outbound traffic.

Application-level firewalls will be implemented for critical services, especially for the SQL Server on **SQLSERVER-12345**.

3. Intrusion Detection/Prevention System (IDS/IPS) Implementation

Network-based IDS/IPS will be deployed to monitor and block suspicious activities in real time.

Host-based IDS will be implemented on critical systems such as DESKTOP-1234567 and SERVER-12345 to detect potential threats.

4. Network Segmentation

The network architecture will be redesigned to isolate critical systems, limiting lateral movement in case of a breach.

VLANs will be implemented to segment different types of systems and data for added protection.

5. Access Control Enhancement

The principle of least privilege will be enforced across all systems and applications to reduce access risks.

Strong password policies will be implemented, and password managers will be considered for better security management.

Multi-factor authentication (MFA) will be deployed for all user accounts, with priority given to administrative and privileged accounts.

6. Regular Security Audits and Vulnerability Assessments

Periodic security audits and penetration testing will be scheduled to identify and mitigate vulnerabilities.

Continuous vulnerability scanning will be conducted for early detection of weaknesses and risks.

By following these short-term and long-term containment plans, **Maven Clinic** will effectively respond to the current incident and significantly enhance its overall security posture. Regular reviews and updates to these plans will ensure ongoing protection against evolving threats and future incidents.

Maven Clinic Cybersecurity Incident Review

Confidential Internal Document

1. Executive Summary

On September 20, 2023, Maven Clinic experienced a significant cybersecurity incident involving unauthorized access attempts, successful intrusion, and potential data compromise across multiple systems. This report details our findings, response actions, and recommendations for future prevention.

2. Incident Timeline

All times in this report are in Eastern Time (ET)

Detection Phase: September 20, 2023

08:10:23: Normal user login (JohnDoe) on DESKTOP-1234567

09:45:32: Security policy change on DC-SERVER-01

10:32:17 - 10:32:21: Multiple failed login attempts for "admin" account, followed by successful login on DESKTOP-1234567

10:33:45: Firewall warning for SMB connection from suspicious IP (192.168.1.100)

12:01:15: Application error in explorer.exe on DESKTOP-1234567

13:23:15: Firewall warning for SSH connection attempt from 192.168.1.25

15:23:52: SQL Server I/O error on SQLSERVER-12345

16:45:32: Unknown application attempting inbound communication on SERVER-12345

Response Phase: September 20-21, 2023

Isolation of affected systems (DESKTOP-1234567, SERVER-12345, SQLSERVER-12345)

Blocking of suspicious IP addresses (192.168.1.100, 192.168.1.25)

Disabling of compromised "admin" account

Resolution Phase: September 22-24, 2023

System patching and updates

Implementation of enhanced firewall rules

Access control enhancements

3. Security Review

What Went Well

Quick detection of unusual login patterns

Prompt isolation of affected systems

Successful containment of potential spread

Areas for Improvement

Delay in detecting initial security policy change

Lack of immediate alerting for multiple failed login attempts

Insufficient network segmentation allowed potential lateral movement

Weak access controls enabled successful brute-force attack

4. Impact Assessment

Affected Systems

DESKTOP-1234567: Primary target of login attempts, application error

SERVER-12345: Unknown application activity, blocked UDP connection

SQLSERVER-12345: Database I/O error

DC-SERVER-01: Unauthorized security policy change

Potential Business Impact

Temporary disruption of services during containment and recovery

Possible data integrity issues on SQLSERVER-12345

Risk of data exfiltration or unauthorized access to sensitive information

Potential reputational damage if customer data was compromised

Legal Implications

Possible breach notification requirements depending on data accessed

Regulatory compliance concerns (e.g., HIPAA for healthcare data)

Potential liability if customer data was exposed

5. Stakeholder Considerations

Relevant Department Heads

- IT Department
- Legal Counsel
- Public Relations
- Human Resources
- Finance Department

Communication Effectiveness

Evaluate timeliness and clarity of internal communications during the incident

Assess effectiveness of external communication strategies, if applicable

6. Recommendations

Short-term Actions

1. Implement multi-factor authentication across all systems
2. Enhance log monitoring and alerting capabilities
3. Conduct immediate security awareness training for all employees

Long-term Strategies

1. Develop a robust network segmentation plan
2. Implement a Privileged Access Management (PAM) solution
3. Establish a continuous security improvement program
4. Regular penetration testing and vulnerability assessments

7. Future Preventive Measures and Estimated Costs

Short-term Actions

1. Implement multi-factor authentication across all systems

Estimated Cost: \$15,000 - \$25,000

Includes licensing for MFA solution and initial setup

2. Enhance log monitoring and alerting capabilities

Estimated Cost: \$30,000 - \$50,000

Includes SIEM tool implementation or upgrade and initial configuration

3. Conduct immediate security awareness training for all employees

Estimated Cost: \$10,000 - \$15,000

Includes development of training materials and delivery platform

Long-term Strategies

1. Develop a robust network segmentation plan

Estimated Cost: \$50,000 - \$100,000

Includes network analysis, design, and implementation of new network architecture

2. Implement a Privileged Access Management (PAM) solution

Estimated Cost: \$75,000 - \$150,000

Includes software licensing, implementation, and integration with existing systems

3. Establish a continuous security improvement program

Estimated Cost: \$100,000 - \$200,000 annually

Includes ongoing training, regular security assessments, and dedicated security personnel

Note: The costs provided are approximate and may vary depending on factors such as vendor selection, the clinic's existing infrastructure, and the complexities involved in implementation. It is recommended that a more detailed cost analysis be conducted for each initiative to obtain accurate estimates tailored to Maven Clinic's specific needs.

7. Next Steps

1. Schedule an all-hands meeting to brief the entire organization on the incident

2. Conduct department-specific sessions to address unique concerns and responsibilities

3. Implement short-term security enhancements immediately

4. Develop a detailed roadmap for long-term security improvements

8. Conclusion

This incident has highlighted critical vulnerabilities in our cybersecurity posture. By implementing the recommended measures and fostering a culture of security awareness, we can significantly reduce the risk of future incidents and better protect our systems and data.

This document provides a comprehensive review of the incident, addressing the key points requested. It's structured to be suitable for a company-wide communication, with enough detail for technical teams while remaining accessible to non-technical stakeholders.