Incident Response and Review – Maven Clinic

Identification and Investigation

Timeline based on Windows Event Logs:

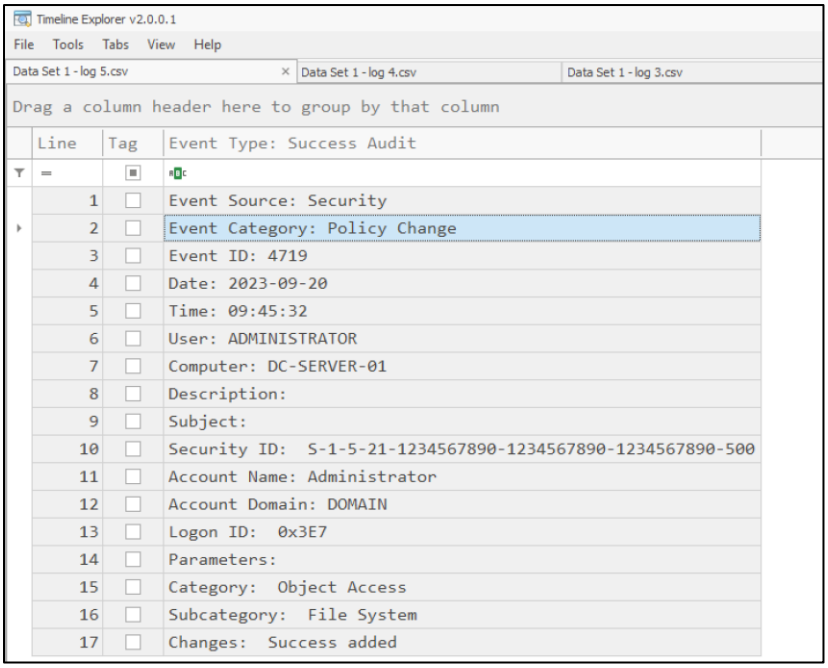
Log	Time (EDT)	Event ID	Attack	Notes
3	08:10:23	4624	Successful logon	By JohnDoe into DESKTOP-1234567 from 192.168.1.2:50215, logon type 10 (RDP)
5	09:45:32	4719	Policy changed	On Domain Controller with Account Name: Administrator
10	10:32:17	4625	Failed logon	From 192.168.1.100:50789, logon type 3 (Network logon) on DESKTOP-1234567
11	10:32:19	4625	Failed logon	From 192.168.1.100:50791, logon type 3 (Network logon) on DESKTOP-1234567
12	10:32:21	4624	Successful logon	From 192.168.1.100:50793, on DESKTOP-1234567, using admin, logon type 3 (Network logon)
13	10:33:45	2004	Firewall rule change	Allow traffic using TCP on port 445 (SMB), from 192.168.1.100 to 192.168.1.1
1	12:01:15	1000	Application error	explorer.exe program crashed
6	13:23:15	2004	Firewall rule change	Allow traffic using TCP on port 22 (SSH) from 192.168.1.25 to 192.168.1.1
7	14:10:12	861	Some application is tracking activity (eavesdropping)	By user JohnDoe on SERVER-12345 using UDP on port 53 (DNS)

2	15:23:52	823	MSSQLSERVER	Failed read/write into database
8	15:34:56	4625	Failed logon	On DESKTOP-1234567 from source IP, 192.168.1.50, logon type 3 (Network logon)
9	16:45:32	5156	WFP permit connection	Unknown application, inbound traffic from 10.0.0.2:12345 to 10.0.0.1:80
4	17:34:56	529	Failed logon	With username, Admin on SERVER-12345, logon type 2 (interactive logon)

Date: 2023-09-20

Timezone: New York, EDT (GMT-4), based on Maven clinic HQ location

Tools like Timeline Explorer helped clear the fog from the data set to make better deductions of what took place during the attack:

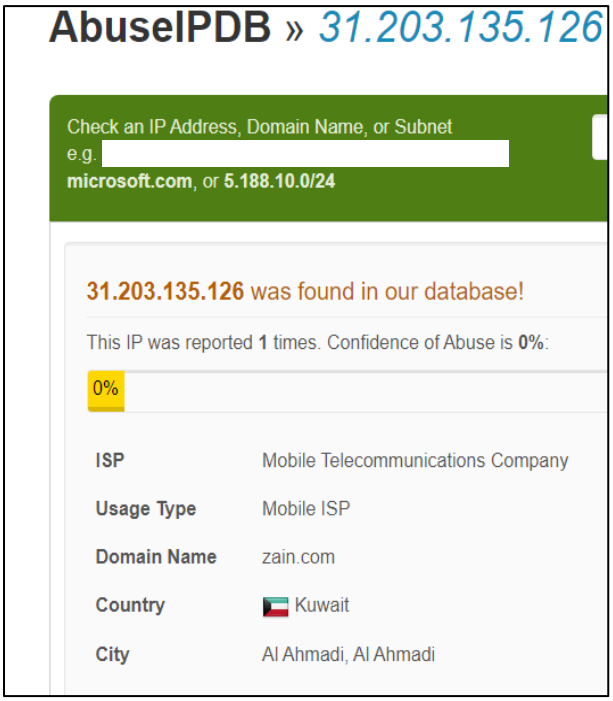


<u>Log Analysis:</u>

- Upon using the showmyip bulk IP lookup tool, the IPs geolocations are visualized on the world map to see where the requests are from:

#	IP	Country	City	Region	ISP	Org	Latitude	Longitude
1	31.203.135.126	Kuwait	Kuwait City	Al Asimah	Mobile Telecommunications Company	MTC GPRS AS Number	29.3645	47.9889
2	15.162.149.54	United States	Seattle	Washington	Amazon Technologies Inc.	DXC US Latin America Corporation	47.6224	-122.337
3	57.130.209.217	France	Roubaix	Hauts-de-France	OVH SAS	OVH	50.6924	3.20113
4	158.131.15.9	Finland	Helsinki	Uusimaa	OUTONET	Outokumpu Oyj	60.1699	24.9384
5	106.0.116.228	China	Guangzhou	Guangdong	CHINANET-GD	Chinanet GD	23.1317	113.266
6	159.168.92.87	Switzerland	Ehrendingen	Aargau	Aveniq Avectris AG	Avectris AG	47.5105	8.3489
7	113.61.139.65	Taiwan	Taichung	Taichung City	EMAX	e-MAX NETWORK CORP.	24.144	120.6844

- Using these locations, we can determine whether it is legitimate network requests or not
- Tool like Abuseipdb showed specific IPs which may have been used in prior attacks:



Affected systems, services:

- DESKTOP-1234567
- MSSQLSERVER database file, “mydatabase.mdf”
- Policy changed on DC-SERVER-01
- DNS tracking on SERVER-12345

Patterns/Anomalies:

- Lateral movement from using logon type: 3 (failed and successful attempts)
- Brute force attacks from logs 10, 11, 12
- Unauthorized access into DESKTOP-1234567 using RDP and log 12
- Privilege escalation

Questions for stakeholders:

- Is there a list of assets (inventory) that can be accessed to understand potential impact of system? I.e, where can lateral movement take the attacker.

//next page

Response Containment and Eradication

Short-term plan: (Snapshot, Isolate comprised systems, uninstall malware, revert changes, traffic analysis)

Actions	**Steps to take**
Snapshot	Take snapshot of current system to take closer look at changes and unauthorized access, modifications etc.
Isolate systems	Isolate data and systems like DESKTOP-1234567, SERVER-12345, DC-SERVER-01, SQLSERVER-12345
	Isolate the SQL database and use backup until resolved
Uninstall/remove unwanted software	Uninstall software unknown.exe and all data related to it
	Remove tracking application on SERVER-12345
Make changes	Revert changed policy on Domain controller
	Change JohnDoe account password and access
	Mandatory password reset on all accounts
Traffic analysis	Block/filter traffic from identified malicious IP addresses involved in the attack

Long-term plan: (Further investigation, monitoring, improved access controls, user education)

Actions	**Steps to take**
Further investigation	Identify how credentials were acquired by JohnDoe (data leak?)
	Identify how to prevent privilege escalation to Admin account via User and Groups
	Plan how to prevent lateral movement of attackers once access is gained to network
Monitoring	Continue monitoring network for malicious activity
Improved access controls	Firewall rules changed need to be reverted
	Implement stringent intrusion detection systems
	Enable MFA for database access
	Update all software on SERVERS and apply necessary patches
Education	User education and training to prevent credential leak

Overview:

- Inform authorities and patients on such a security gap
- Unauthorized access of network can mean PII data of patients has been compromised
- Ensure compliance with HIPAA, PCI DSS, GDPR (legal team)
- Prevent any more downtime of servers or database (which has patient records)
- Consider company branding and image (PR)

Cost-analysis:

- Tools
    - IDS/IPS - $10,000 to $50,000
- User education & training - $30 to $100 per employee annually
- Business disruptions/downtime (SQL database, patient details) - $300,000+
- Penalties involved with compliance violations
- Cybersecurity insurance

Presentation to CTO:

Affected systems have been isolated to prevent spread of attack
Eradicated malware and resolved vulnerabilities
Policy changes are required
Continue to monitor for further network security events
Provide user education and training on security incidents
Implement improved access controls
Perform further investigation
Get legal team involved for compliance and regulations (HIPAA, PII)
Consider potential company branding as a result of security incident
Decide on financial impact and decisions to be made

Post Incident Review

Target audience:

- Upper management interested in financial impacts and business objectives
- Affected business units interested in how to prevent such security incidents
- Considering that the security gap caused violations of HIPAA and GDPR, legal team and PR will have to be involved in this meeting.

Timeline:

- Security incident occurred on 2023-09-20 from 8am to 6pm.
- Attacker gained access to network and activities were logged by security controls in place, including potential data exfiltration.
- Once alarms were raised from this security incident, the security team conducted initial investigations and containment of the attack on 2023-09-21.
- Affected systems and services (including patient records) were restored on 2023-09-22, and necessary access control measures deployed.

Impact to business:

- Loss of trust in customers (patients)
- Compliance violations and fees involved with that
- Downtime of affected systems and business lost as a result of that

Security Review:

What went right:

- Immediate detection and response to security incident
- Proper protocols and policies followed to respond and contain the attack and consequences

What could be better:

- More hands-on deck to respond to such incidents
- Implementation of SOAR and SIEM tools to detect and respond faster
- To prevent such re-occurrences improve overall security posture by reducing attack vectors and surfaces for potential vulnerabilities
- Move forward with more user training, employ concepts of defense-in-depth and least privilege.

Lessons learned:

- Security incidents can occur even when mitigative strategies and access management tools are in place, ie, ensure cyber hygiene at all times (do not let guard down)
- Incidents such as these can have impacts not just on affected systems but also the end user (patients and compliance)

The future:

- Hire external security consultation company to recommend potential security measures
- Consider cybersecurity insurance plan in place for security incidents
- In the event of security events to have business continuity and risk management plans