

Identification and Investigation

Timeline Overview

Date: 2023-09-20

Timezone: EDT/EST

1. 08:10:23
 - a. **Log 3** -> New Login for JohnDoe on DESKTOP-1234567
2. 09:45:32
 - a. **Log 5** -> Policy Change Success
3. 10:32:17 - 10:33:45 (00:01: 28 timeframe)
 - a. **Log 10** -> Failed Logon for admin
 - b. **Log 11** -> Failed Logon for admin
 - c. **Log 12** -> Successful Logon for admin
 - d. **Log 13** -> Windows Firewall Warning for Protocol TCP
4. 12:01:15
 - a. **Log 1** -> Application Error for Application Path 'C:\Windows\explorer.exe'
5. 13:23:15
 - a. **Log 6** -> Windows Firewall Warning for Protocol TCP
6. 14:10:12
 - a. **Log 7** -> Security-Auditing Error on unknown application for Protocol UDP by JohnDoe, was not allowed
7. 15:23:52
 - a. **Log 2** -> MSSQLSERVER Warning for I/O error on a database file
8. 15:34:56
 - a. **Log 8** -> Failed Logon for admin
9. 16:45:32
 - a. **Log 9** -> Warning for Application of an unknown executable file for inbound direction
10. 17:34:56

- a. **Log 4** -> Failed Logon for Admin

IP Addresses

From Data Set 1

- 192.168.1.2 -> **Log 3** as Source Network Address for New Logon
- 192.168.1.100 -> **Log 10/11/12** as Source Network Address for Logons
 - > **Log 13** as Source IP for TCP
 - From VirusTotal: **CRDF was flagged as 'Malicious'**
- 192.168.1.1 -> **Log 13/6** as Destination IP for TCP
 - From VirusTotal:
 - 0/94 flagged for Security Vendor Analysis
 - **Tagged with 'suspicious-udp'**
- 192.168.1.25 -> **Log 6** as Source IP for TCP
- 192.168.1.50 -> **Log 8** as Source Network Address for Logon
- 10.0.0.2 -> **Log 9** as Source Address
- 10.0.0.1 -> **Log 9** as Destination Address

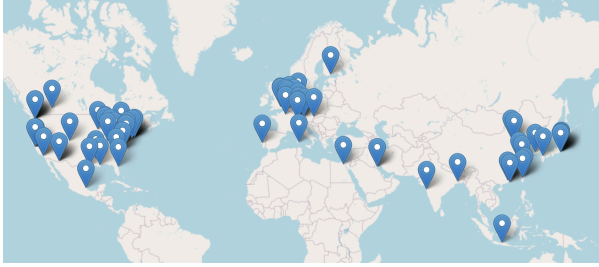

From Bulk IP Lookup:

#	IP	Country	City	Region	ISP	Org	Latitude	Longitude
1	192.168.1.2	private range						
2	192.168.1.100	private range						
3	192.168.1.1	private range						
4	192.168.1.25	private range						
5	192.168.1.50	private range						
6	10.0.0.2	private range						
7	10.0.0.1	private range						

From Excel IPs

Noted as making a connection on or around the time of the unusual activity

From Bulk IP LookUp: [Excel sheet](#) and map view below

Column A	Column B
	

- Outliers from clusters (**7 total**)
 - 36.80.174.222 (Semarang, Central Java, Indonesia)
 - 110.153.152.100 (Xingfulu, Xinjiang, China)
 - 95.190.155.120 (Drachenino, Kemerovo Oblast, Russia)
 - 177.51.226.32 (Santos, São Paulo, Brazil)
 - 186.211.64.122 (Goiânia, Goiás, Brazil)
 - 191.105.100.77 (Bogotá, Bogota D.C., Colombia)
 - 158.222.55.116 (Anchorage, Alaska, United States)

Suspicious Activities

Potential Brute Force Attack

10:32:17 EDT - 10:32:21 EDT (4 seconds)

- 3 logins were shown on **Log 10/11/12** in a 4-second timeframe
- This happened on Workstation Name **DESKTOP-1234567** for Account Name **admin** on Source Network Address **192.168.1.100**, which was flagged as malicious

Suspicious Network Traffic

10:33:45 EDT, 13:23:15 EDT, 14:10:12 EDT

- **Log 13** occurred at **10:33:45 EDT**, which is **1 minutes 24 seconds** after the Potential Brute Force Attack
- **Log 6/13** received a **Windows Firewall Warning** for Protocol **TCP** with the same Destination IP address **192.168.1.1**
- **Log 7** received an **Security-Auditing Error** on an unknown application for Protocol **UDP** from User **DESKTOP-1234567\JohnDoe** on Computer **SERVER-12345** at **14:10:12 EDT**,
 - Note: **JohnDoe** had a new login at **08:10:23** on **Log 3** on **DESKTOP-1234567**

Potential SQL Database Compromise

15:23:52 EDT

- **Log 2** received a **MSSQLSERVER Warning** for on Computer **SERVER-12345** in file **C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\DATA\mydatabase.mdf**

Running Unknown Executable

16:45:32 EDT

- **Log 9** received a **Windows Security Auditing Warning** for Application **C:\Program Files (x86)\UnknownApp\unknown.exe** with **inbound** network traffic
 - Note: Occurred on Computer **SERVER-12345**

Tools Used

- VirusTotal - Check for flagged security vendors for IPs in Data Set 1
- Bulk IP LookUP - To geolocate multiple IP addresses
- Google Gemeni - To search for resources