Title: Log Analysis

Group/Name: Aimé Fraser

Indicators and Technical Details

Datetime	Identifier (IP, Domain, URL, Hostname)	MITRE Technique ID	Analyst Comment
Jan 11, 2021 @ 01:42:11.659	Jporter logs on		Logs on from DESKTOP-3A293CQ, 10.10.147.50 into his work machine 172.16.2.8
Jan 11, 2021 @ 01:42:14.253	rdpclip.exe	T0886 Remote services	Remote desktop clipboard
Jan 11, 2021 @ 01:42:16.028	atbroker.exe	T0886 Remote services	Manages remote desktop services.
Jan 11, 2021 @ 01:43:25.130	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	T1059.001 PowerShell	Starts PowerShell
Jan 11, 2021 @ 01:43:58.041	Whoami.exe/user, then Whoami.exe/groups, then Whoami.exe/priv	T1033 Discovery	Enumerate privileges
Jan 11, 2021 @ 01:46:07.503	"C:\Windows\system32\net.exe" user jporter /DOMAIN	T1087.002 Account Discovery: Domain	Discover domain accounts
Jan 11, 2021 @ 01:48:32.210	"C:\Windows\system32\ipconfig.exe" /all	T101E6 System Network Configuration Discovery	Enumerate network configuration.
Jan 11, 2021 @ 01:49:19.634	"C:\Windows\system32\netsh.exe" advfirewall firewall	T1562.004 Disable or Modify System Firewall	Alter firewall settings.
Jan 11, 2021 @ 01:52:05.794	"C:\Program Files\internet explorer\iexplore.exe" Then "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:9344 CREDAT:75020 /prefetch:2		Launch Internet Explorer

Jan 11, 2021 @ 01:55:31.076	C:\Windows\system32\rundll32.exe C:\Windows\system32\inetcpl.cpl,ClearMyTracksByProcess Flags:8388616 WinX:0 WinY:0 IEFrame:0000000000000000	T1070.003 Clear Command History	Clear IE history.
Jan 11, 2021 @ 01:55:52.873	C:\Windows\system32\ServerManager.exe		Launch Server manager to perform a wide range of tasks, such as adding or removing roles and features, configuring server settings, and monitoring server performance.
Jan 11, 2021 @ 01:56:01.038	Configure-SMRemoting.exe" -GET	T0888 Remote System Information Discovery	Displays the current Remoting settings, such as the status of the feature (enabled or disabled), the authentication level, and the encryption level.
Jan 11, 2021 @ 01:56:12.214	"C:\Windows\system32\rundll32.exe" C:\Windows\system32\iesetup.dll,IEShowHardeningDialog and "C:\Windows\SysWOW64\rundll32.exe" iesetup.dll,IEHardenMachineNow u		Allows administrators to configure various security settings for the browser, such as disabling unnecessary features, disabling add-ons, and setting the security zone level.
Jan 11, 2021 @ 01:57:40.868	C:\Windows\System32\rundll32.exe C:\Windows\System32\shell32.dll,SHCreateLocalServerRunDll {9aa46009-3ce0-458a-a354-715610a075e6} -Embedding		Create local server
Jan 11, 2021 @ 01:58:04.787	"C:\Users\jporter\Downloads\TeamViewer_Setup.exe"		Install Team Viewer
Jan 11, 2021 @ 01:58:18.387	C:\Windows\system32\schtasks /Create /TN TVInstallRestore /TR "C:\Users\jporter\AppData\Local\Temp\4\TeamViewer\TeamViewer_.exe /RESTORE" /RU SYSTEM /SC ONLOGON /F	T1053.005 Scheduled task	Creates Scheduled Task to run Team Viewer at startup.
Jan 11, 2021 @ 01:58:23.281	C:\Windows\system32\schtasks /Delete /TN TVInstallRestore /F		Deletes the scheduled task

Executive Summary

Jim Porter, a system administrator at GoodCorp with privileged network access, was laid off before the end of his shift on January 10, 2021, at 2400 UTC. Based on statements made by Mr. Porter, there were concerns that he may retaliate against the company.

The Security Operations Team analyzed his network traffic for the weeks before and after this event. From this, it was determined that in the hours immediately after being laid off, Mr. Porter logged into his workstation remotely. He altered security controls that allowed him to download, install, and configure tools for full access to the system. Despite this, he did not log on. His workstation continued to be up and running scheduled tasks (including those that assured his access) until 2400 January 20, but he did not log in.

To prevent similar events in the future, immediately revoke all privileges when employment ends so former employees have no access.

Technical Summary

Porter's shift ended at 11:59 on January 10. He did not log out when he left. On Jan 11, 2021, at 01:42 he logged into his work machine (172.16.2.8) from 10.10.

147.50 using Remote Desktop. He then started up PowerShell and enumerated privileges with whoami. Using net.exe, he then enumerated domain accounts, and then the network configuration with ipconfig /all.

He altered the firewall setting, changed the security policy settings on Internet Explorer, and then deleted the browser history to cover his tracks. Next, he downloaded Team Viewer and created a scheduled task to run it at startup.

There were five other events around 0204 that day, all logins. No other events occurred.

Porter's work machine continued to run. Although he had established remote access to the GoodCorp system, there is no sign he used it once it was set up. No remote activity occurs after that time. His desktop machine continued to run the same legitimate tasks in the weeks before these events. This activity ceased on January 20 at 2400.

Findings and Analysis

In the two hours immediately after his employment ended, Mr. Porter used his administrator privileges to access the network and create the environment for him to access the network remotely. He altered settings and configurations to give himself the highest privileges and had the capability to do extensive damage to the network, the business, and GoodCorp's reputation. Despite his ability to do harm, he did not log in. However, his workstation continued to operate for ten days, completing the scheduled tasks it had been doing for months. Including those that kept his access open.

This should not have been possible. His access should have been blocked immediately upon his being laid off.

Remediation and Recommendations

Create procedures for account deactivation soon after an employee leaves the company.

DS0017 Command Execution
Monitor executed commands and arguments to services specifically designed to accept remote connections, such as RDP, Telnet, SSH, and VNC. The adversary may then perform these actions using Valid Accounts.

Monitor for the execution of commands and arguments associated with enumeration or information gathering of domain accounts and groups, such as “net user /domain” and “net group /domain. “

System and network discovery techniques normally occur throughout an operation as an adversary learns the environment, and to an extent in normal network operations. Therefore, discovery data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Monitor executed commands and arguments for actions that could be taken to gather tasks may also be created through Windows system management tools such as Windows Management Instrumentation and PowerShell, so additional logging may need to be configured to gather the appropriate data.

M0801 Access Management
Access Management technologies can help enforce authentication on critical remote services. Examples include, but are not limited to, device management services (e.g., telnet, SSH), data access servers (e.g., HTTP, Historians), and HMI sessions (e.g., RDP, VNC).

M0937 Filter Network Traffic
Filter application-layer protocol messages for remote services to block any unauthorized activity.

M0804 Human User Authentication
All remote services should require strong authentication before providing user access.

M0918 User Account Management
Limit the accounts that may use remote services. Limit the permissions for accounts at higher risk of compromise; for example, configure SSH so users can only run specific programs.

M0814 Static Network Configuration
ICS environments typically have more statically defined devices, therefore, minimize the use of IT discovery protocols (e.g., DHCP, LLDP) and discovery functions in automation protocols.

DS0022 File Access
Monitor for files (such as /etc/hosts) being accessed that may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system.

DS0009 Process Creation
Monitor for newly executed processes that can be used to discover remote systems, such as ping.exe and tracert.exe, especially when executed in quick succession. Consider monitoring for new processes engaging in scanning activity or connecting to multiple systems by correlating process creation network data.

M1028 Operating System Configuration
Prevent administrator accounts from being enumerated when an application is elevating through UAC since it can lead to the disclosure of account names. The Registry key is located at HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators. It can be disabled through GPO: Computer Configuration > Policies > Administrative Templates > Windows Components > Credential User Interface: Enumerate administrator accounts on elevation.

DS0012 Script Execution
Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible, to determine their actions and intent.

M1022 Disable File and Directory Permissions
Ensure proper process and file permissions are in place to prevent adversaries from disabling or modifying firewall settings.

M1018 User Account Management
Ensure proper user permissions are in place to prevent adversaries from disabling or modifying firewall settings.
Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create scheduled tasks on remote systems.

DS0018 Firewall
Monitor for changes made to firewall rules that might allow remote communication over protocols such as SMD and RDP. Modifying firewall rules might also consider opening local ports and services for network profiles such as public and domain.

M1039 Environment Variable Permissions
Making the environment variables associated with command history read-only may ensure that the history is preserved.

DS0002 User Account
Monitor for attempts by a user to gain access to a network or computing resource, often by providing credentials via remote terminal services, that do not have a corresponding entry in a command history file.

--End--