

BazarLoader Adds Compromised Installers, ISO to Arrival and Delivery Vectors

By Ian Kenefick Nov 23, 2021 Read time: 4 min (1078 words)

Published: 2021-11-23 · Archived: 2026-04-05 14:33:17 UTC

We continue monitoring the campaigns using information stealer [BazarLoadernews- cybercrime-and-digital-threats](#) (detected by Trend Micro as TrojanSpy.Win64.BAZARLOADER, TrojanSpy.Win64.BAZARLOADER, and Backdoor.Win64.BAZARLOADER). While InfoSec forums have [noted](#) the spike in detections during the third quarter, we noticed two new arrival mechanisms included in the existing roster of delivery techniques that malicious actors abused for data theft and ransomware.

One of the methods involves the use of compromised software installers as malicious actors bundle BazarLoader with legitimate programs. The second method involves the use of an ISO file with a Windows link (LNK) and dynamic link library (DLL) payload. We observed the Americas as the region with the highest counts of BazarLoader. For more technical analysis and insights into BazarLoader’s infection chains and campaigns, read our technical brief [hereopen on a new tab](#).

Arrival via compromised installers

During one of our monitoring routines, we found compromised versions of VLC and TeamViewer packages bundled with BazarLoader. While the initial delivery mechanism has yet to be identified, it’s possible that the use of these packages are part of a wider social engineering technique to deceive users into downloading and implementing the compromised installers.

	Detections	Size	First seen	Last seen	Submitters
<input type="checkbox"/> vlc-3.0.16-win32.exe overlay direct-cpu-clock-access checks-user-input runtime-modules	2 / 63	41.44 MB	2021-10-08 20:38:52	2021-10-08 20:38:52	1
<input type="checkbox"/> C:\Users\...\ overlay runtime-modules detect-debug-environment long-sleeps direct-cpu-clock-access checks-user-input ...	18 / 67	35.09 MB	2021-10-08 15:19:50	2021-10-08 15:19:50	1

Figure 1. Compromised installers bundled with BazarLoader

As the installers load, it drops and executes a BazarLoader executable. This is also one of the notable differences from recent BazarLoader arrival mechanisms wherein the malicious actors appeared to favor dynamic link libraries (DLL).

15:02:34.0024568	vlc.exe	1352	5056	WriteFile	C:\Users\...AppData\Local\Temp\vnz6E2A.tmp
15:02:34.0029298	vlc.exe	1352	5056	WriteFile	C:\Users\...AppData\Local\Temp\vnz6E2A.tmp
15:02:34.0031993	ste.exe	3004	5056	CreateFile	C:\NepJmQUMYQhei\epJmQUMYQhei\ste.exe
15:02:34.0032309	ste.exe	3004	5056	QueryNetwork...	C:\NepJmQUMYQhei\epJmQUMYQhei\ste.exe
15:02:34.0032565	ste.exe	3004	5056	CloseFile	C:\NepJmQUMYQhei\epJmQUMYQhei\ste.exe
15:02:34.0040539	ste.exe	3004	5056	Process Create	C:\NepJmQUMYQhei\epJmQUMYQhei\ste.exe

Figure 2. As the VLC installer executes, the bundle drops and executes ste.exe, a BazarLoader executable

Using Trend Micro Vision One, we tracked the installer creating a process, “vlc-3.0.16-win3..2.tmp,” after executing ste.exe, which copies the latter executable to the disk and executes it. It then connects with the command and control (C&C) server and injects a copy of itself into a new suspended MS Edge process.

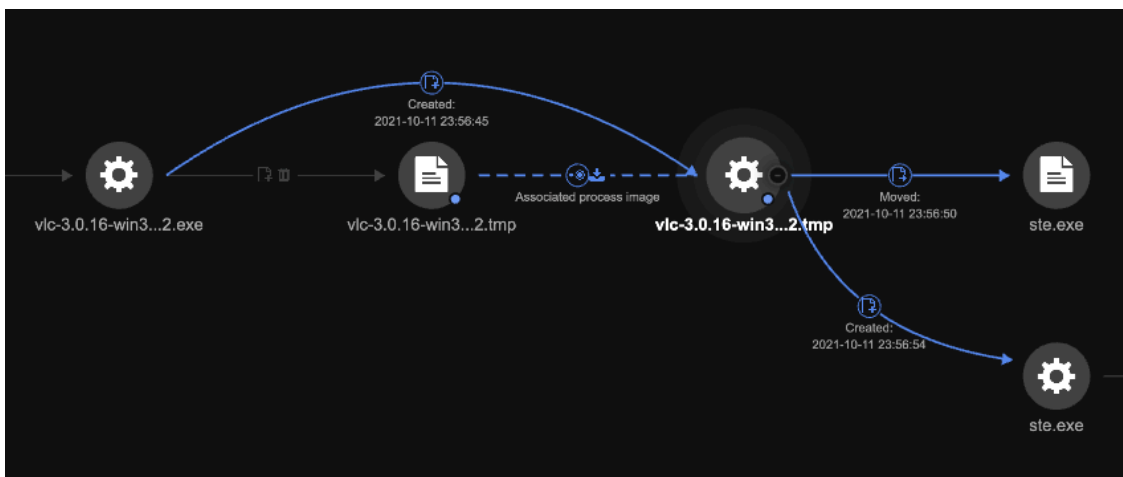


Figure 3. Tracking the BazarLoader executable’s process

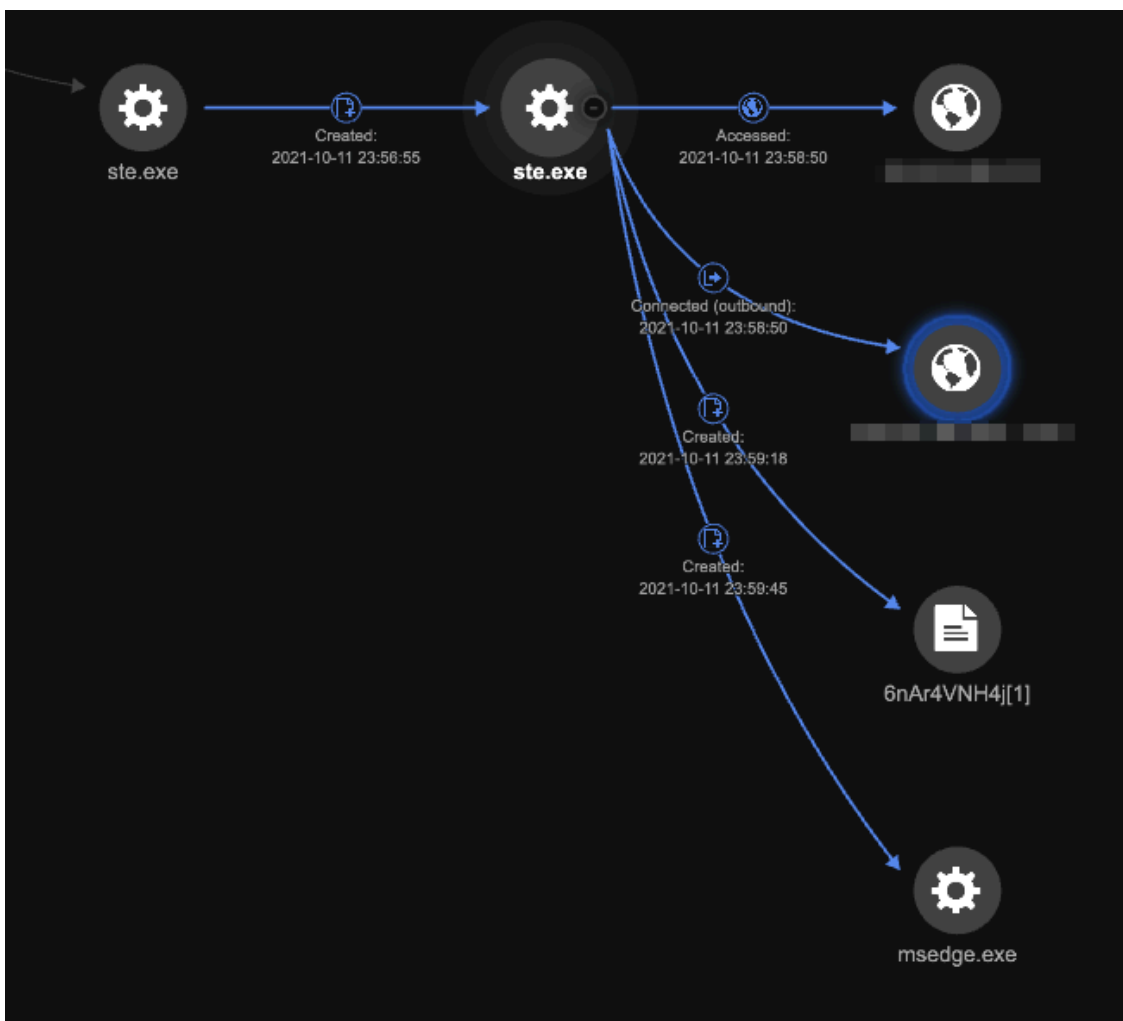


Figure 4. The ste.exe executable connects to the C&C server via MS Edge

Arrival via ISO file

Meanwhile, we also found a delivery mechanism abusing ISO files, wherein DLL and LNK files contained inside execute the BazarLoader DLL in it. The LNK file uses a folder icon to deceive the user into double clicking the icon, enabling the file to run the enclosed BazarLoader DLL file.

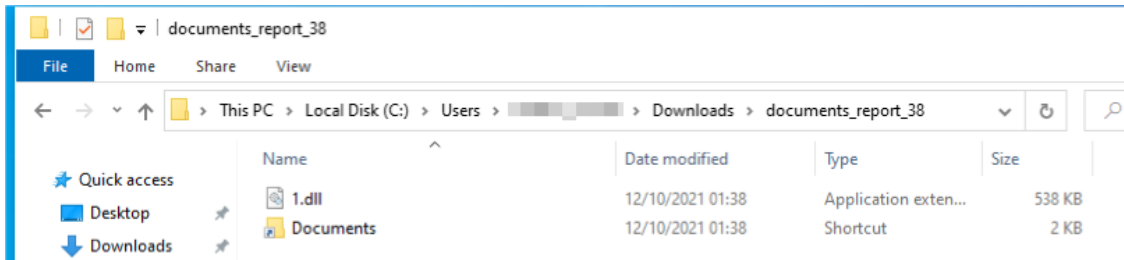


Figure 5. LNK using a folder icon to trick users into double-clicking the BazarLoader DLL

It then calls the export function “EnterDLL,” a function that BazarLoader has used recently. Rundll32.exe loads the malicious DLL and communicates with the C&C server, then proceeds to spawn a suspended MS Edge process to inject itself into it.

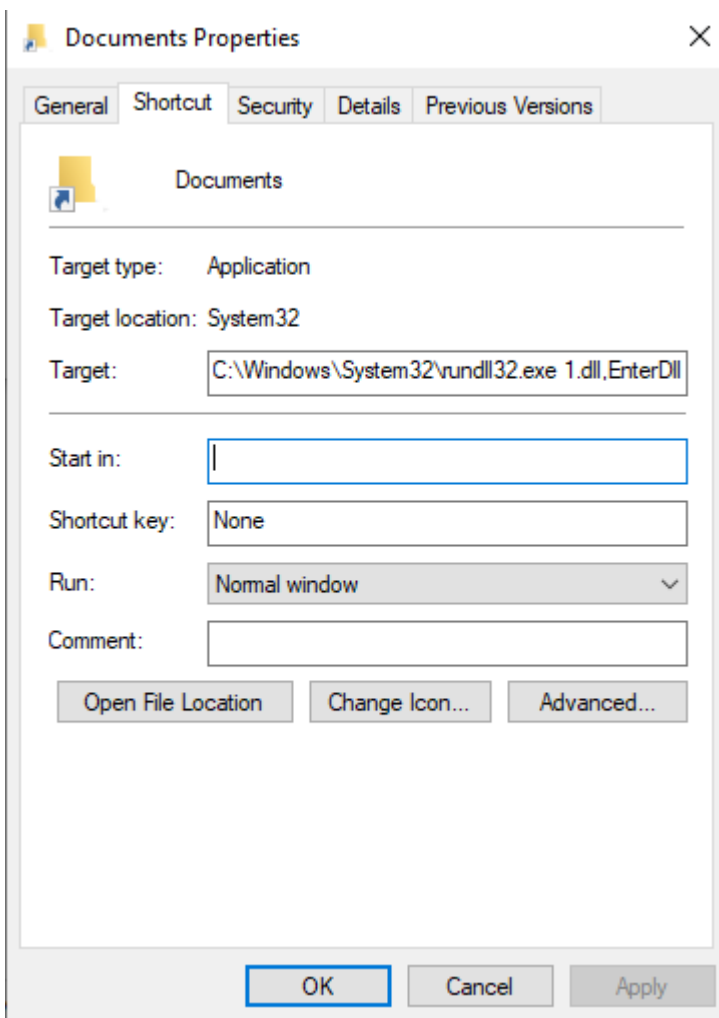


Figure 6. Observing EnterDll, an export function previously used by BazarLoader actors



Figure 7. Tracking BazarLoader opening MS Edge and injecting itself to it

Conclusion

The number of arrival mechanism variations used in BazarLoader campaigns continue to increase as threat actors diversify their attack patterns to evade detection. However, both techniques are noteworthy and still work despite their lack of novelty due to singular detection technologies' limitations. For instance, while the use of compromised installers has been observed with other malware, the large file size can still challenge detection solutions — such as sandboxes — which may implement file size limits. On the other hand, LNK files serving as shortcuts will also likely be obfuscated for the additional layers created between the shortcut and the malicious files itself.

In addition, the deployment of BazarLoader malware for initial access is a known technique for modern ransomware such as Conti and Ryuk as service affiliates. Aside from these known ransomware families including more tools for entry into their arsenal, other malware groups and ransomware operators may pick up on the additional means, if they have not already done so.

Best practices

BazarLoader is an example of a versatile malware delivery mechanism that will likely find more ways to adapt to deceive more users. For details on all the other measures that BazarLoader uses to get into systems, read our technical brief [hereopen on a new tab](#).

Here are some best practices to defend against this threat:

- Enable security solutions that allow for visibility in tracking processes of files, allowing security teams to detect malicious outgoing and incoming network communication and traffic.
- Download installers and updates only from their respective official websites and platforms.

Trend Micro solutions

BazarLoader will continue to evolve as an information stealer malware on its own, an initial access malware-as-a-service (MaaS) for other malware operators, and as an enabler for secondary payload delivery for even more disruptive attacks like modern ransomware. Security teams must make monitoring and tracking for known threats more visible based on known data and use multilayered solutions capable of pattern recognition and behavior monitoring for unknown threats.

[Trend Micro Vision One™ products](#) helps detect and block suspicious activity, even those that might seem insignificant when monitored from only a single layer, through multilayered protection and behavior detection. It helps spot and block BazarLoader and its other components wherever it might be on the system. [Trend Micro Apex One™ products](#) employs behavior analysis to protect systems against malicious scripts, injection, ransomware, and memory and browser attacks related to fileless threats from initial access, execution, and C&C communication. [Trend Micro Worry-Free™ Business Security](#) can protect users and businesses from BazarLoader by detecting malicious files and spammed messages, JavaScript droppers, and DLL loaders, as well as URLs associated with the threat.

[Trend Micro Email Security products](#) delivers continuously updated protection to stop spam, malware, spear phishing, ransomware, and advanced targeted attacks before they reach the network. It protects Microsoft Exchange, [Microsoft Office 365 products](#), Google Apps, and other hosted and on-premises email solutions. [Trend Micro™ Deep Discovery™](#) provides detection, in-depth analysis, and proactive response to ransomware attacks through specialized engines, custom sandboxing, and seamless correlation across the entire attack life cycle such as tool ingress, exploits, C&C activities, and lateral movements. [Trend Micro™ Deep Discovery™ Email Inspector products](#) and [InterScan™ Web Security products](#) perform custom sandboxing and advanced analysis techniques to prevent malware from ever reaching end users, especially potentially vulnerable users working remotely. These effectively deter potential ransomware attacks that are delivered through malicious emails.

Cloud-specific security solutions such as [Trend Micro™ Hybrid Cloud Security products](#) can help protect cloud-native systems and their various layers. [Trend Micro Cloud One™ products](#) protects cloud-native systems by securing continuous-integration and continuous-delivery (CI/CD) pipelines and applications. It also helps identify and resolve security issues sooner and improves delivery time for DevOps teams.

Indicators of Compromise (IOCs)

Visit [this page open on a new tab](#) to view the full list of IOCs.

Tags

Source: https://www.trendmicro.com/en_us/research/21/k/bazarloader-adds-compromised-installers-iso-to-arrival-delivery-vectors.html