Case Study: From BazarLoader to Network Reconnaissance

unit42.paloaltonetworks.com/bazarloader-network-reconnaissance/

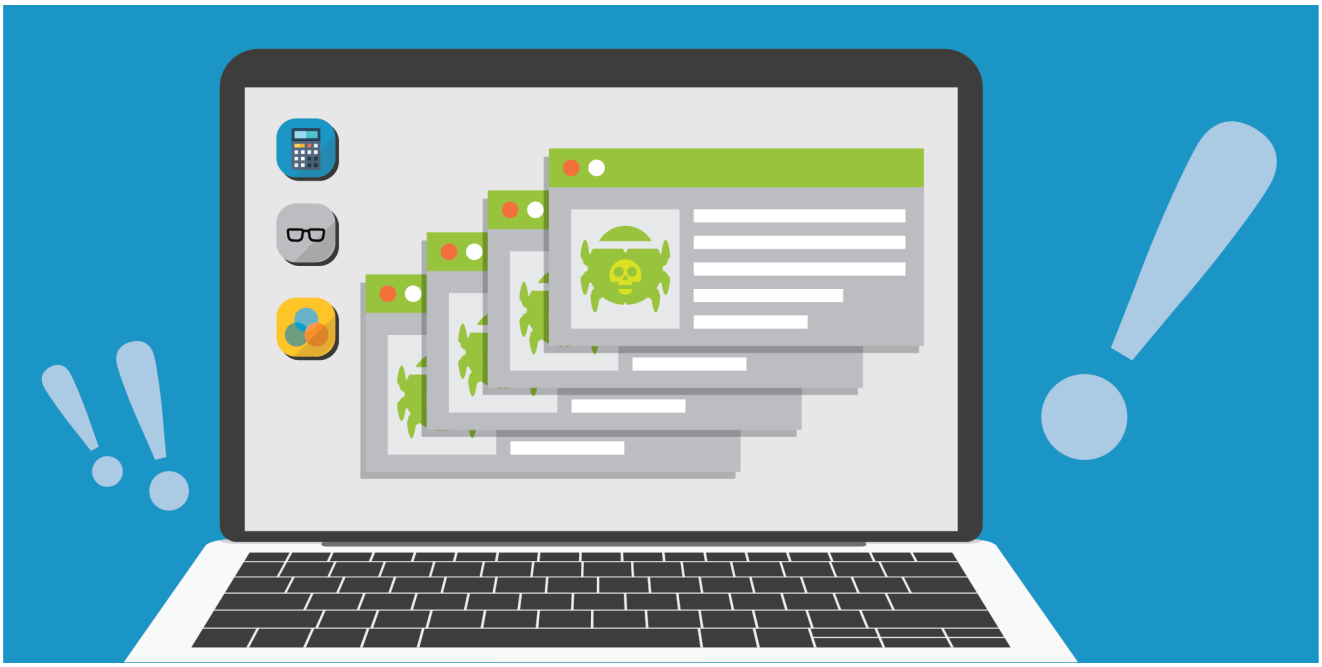
Brad Duncan October 18, 2021

By Brad Duncan

October 18, 2021 at 6:00 AM

Category: Unit 42

Tags: BazaLoader, BazarLoader, Cobalt Strike, CobaltStrike macros



This post is also available in: 日本語 (Japanese)

Executive Summary

BazarLoader is Windows-based malware spread through various methods involving email. These infections provide backdoor access that criminals use to determine whether the host is part of an Active Directory (AD) environment. If so, criminals deploy Cobalt Strike and perform reconnaissance to map the network. If the results indicate a high-value target, criminals attempt lateral movement and will often deploy ransomware like Conti or Ryuk.

This blog reviews a recent BazarLoader infection, how it led to Cobalt Strike, and how Cobalt Strike led to network reconnaissance. If you discover similar activity within your network, you could be a target for ransomware.

Organizations with decent spam filtering, proper system administration and up-to-date Windows hosts have a much lower risk of infection. Palo Alto Networks customers are further protected from this threat. Our Threat Prevention security subscription for the Next-Generation Firewall detects the BazarLoader sample from this infection and similar samples. Endpoint detection like Cortex XDR can prevent Cobalt Strike activity and criminal access to your network.

Distribution Methods for BazarLoader

During summer 2021, different campaigns distributed BazarLoader malware using emails. From late July through mid-August 2021, the majority of BazarLoader samples were spread through three campaigns.

The BazarCall campaign pushed BazarLoader using emails for initial contact and call centers to guide potential victims to infect their computers. By early July, a copyright violation-themed campaign using ZIP archives named Stolen Images Evidence.zip also began pushing BazarLoader. By late July, a long-running campaign known as TA551 (Shathak) started pushing BazarLoader through English-language emails.

In addition to those three major campaigns, we discovered at least one example of BazarLoader distributed through an Excel spreadsheet of undetermined origin. Our case study reviews an infection generated using this example on Aug. 19, 2021.

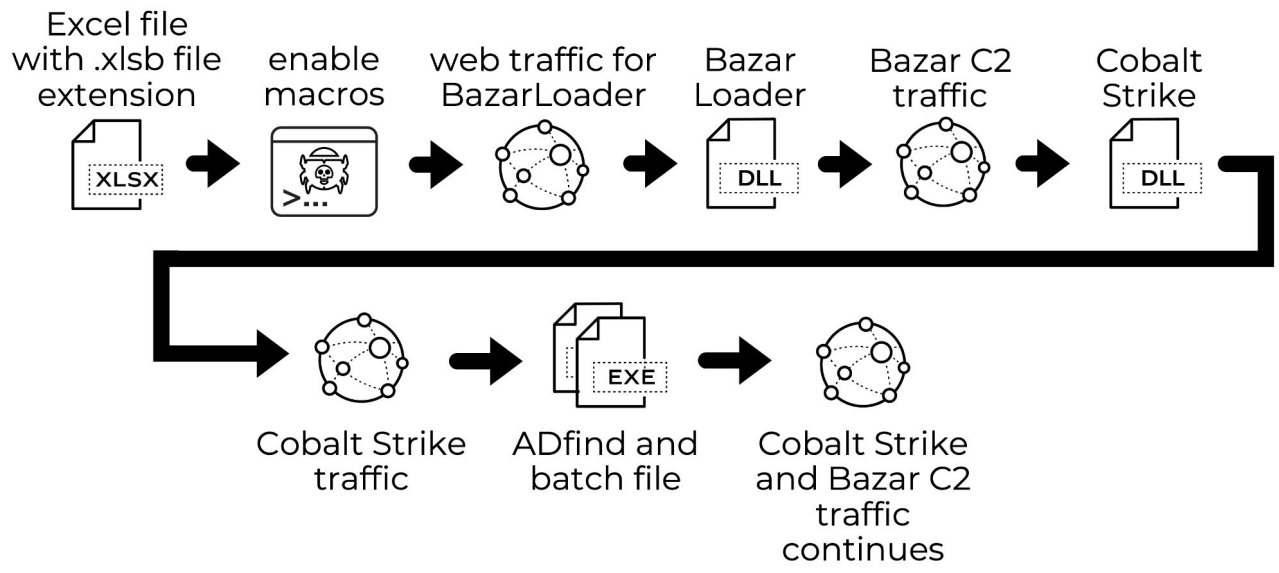


Figure 1. Chain of events from BazarLoader infection on Aug. 19, 2021.

Malicious Excel Spreadsheet

The malicious Excel spreadsheet was discovered on Wednesday, Aug. 18, 2021, and it has a last modified date of Tuesday, Aug. 17. The filename had an .xlsb file extension. This file has macros designed to infect a vulnerable Windows host with BazarLoader. Figure 2 shows a screenshot of the Excel file.

Though the DocuSign logo appears in Figure 2, this Excel template was created by a threat actor trying to instill confidence by taking advantage of the DocuSign brand name and image. Various threat actors use this and other DocuSign-themed images on a near-daily basis. DocuSign is aware of this ongoing threat and provides guidelines on how to handle these types of malicious files.

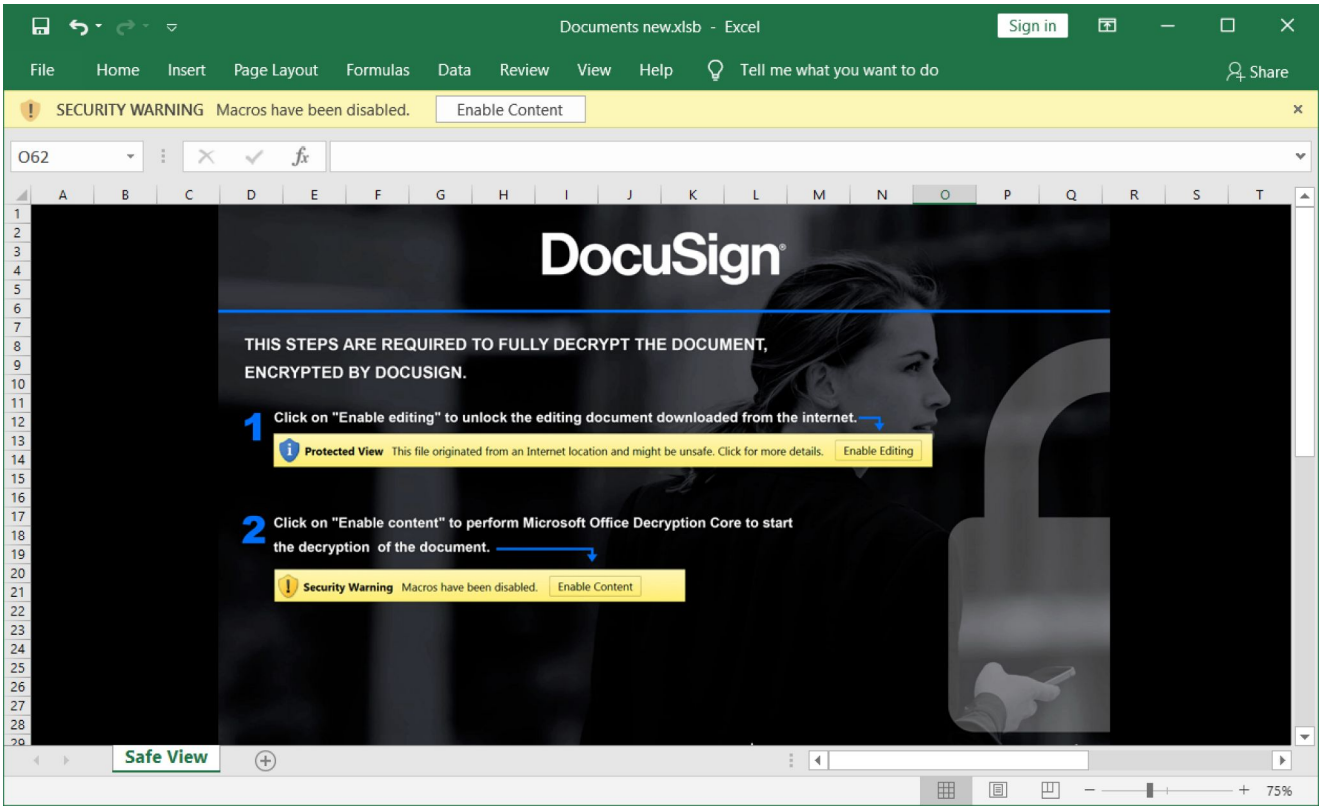


Figure 2. Screenshot of the malicious Excel spreadsheet.

After enabling malicious macros on a vulnerable Windows host, the spreadsheet presented a new tab for a page with fake invoice information, as shown below in Figure 3.

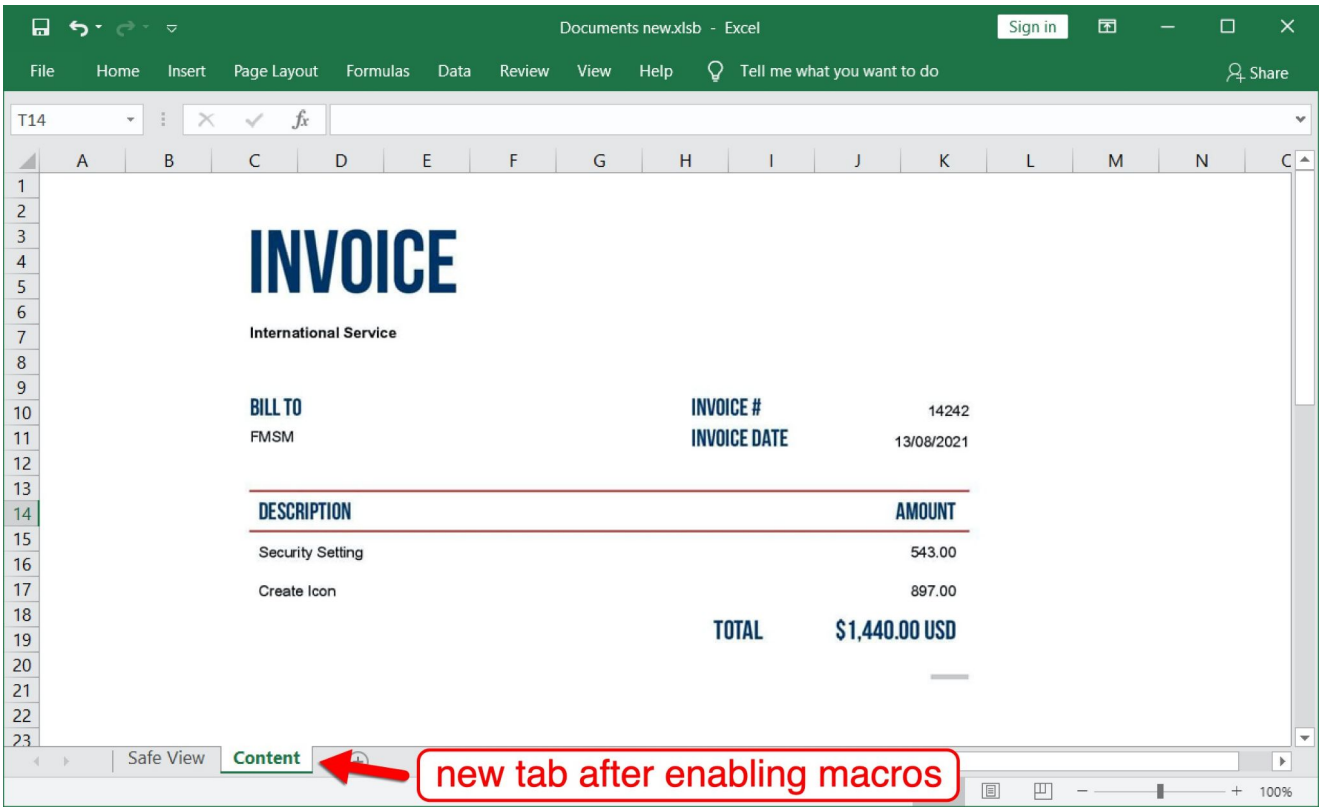


Figure 3. Excel spreadsheet presented a fake invoice after enabling macros.

As it presented the fake invoice page, the spreadsheet's macro code had already retrieved a malicious binary for BazarLoader.

BazarLoader Binary

The spreadsheet's macro code retrieved a malicious Dynamic Link Library (DLL) file for BazarLoader from the following URL:

hxxps://pawevi[.]com/lch5.dll

As shown below in Figure 4, the DLL was saved to the victim's home directory at C:\Users\[username]\tru.dll. It ran using regsvr32.exe.

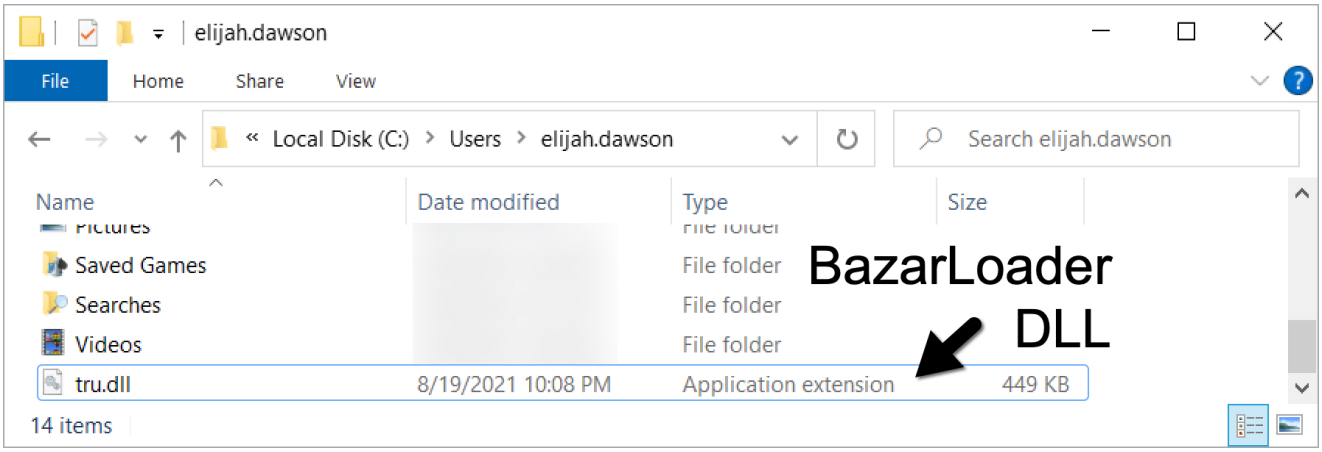


Figure 4. BazarLoader DLL saved to the infected user's home directory.

The BazarLoader DLL was immediately copied to another location and made persistent through the Windows registry, as shown below in Figure 5.

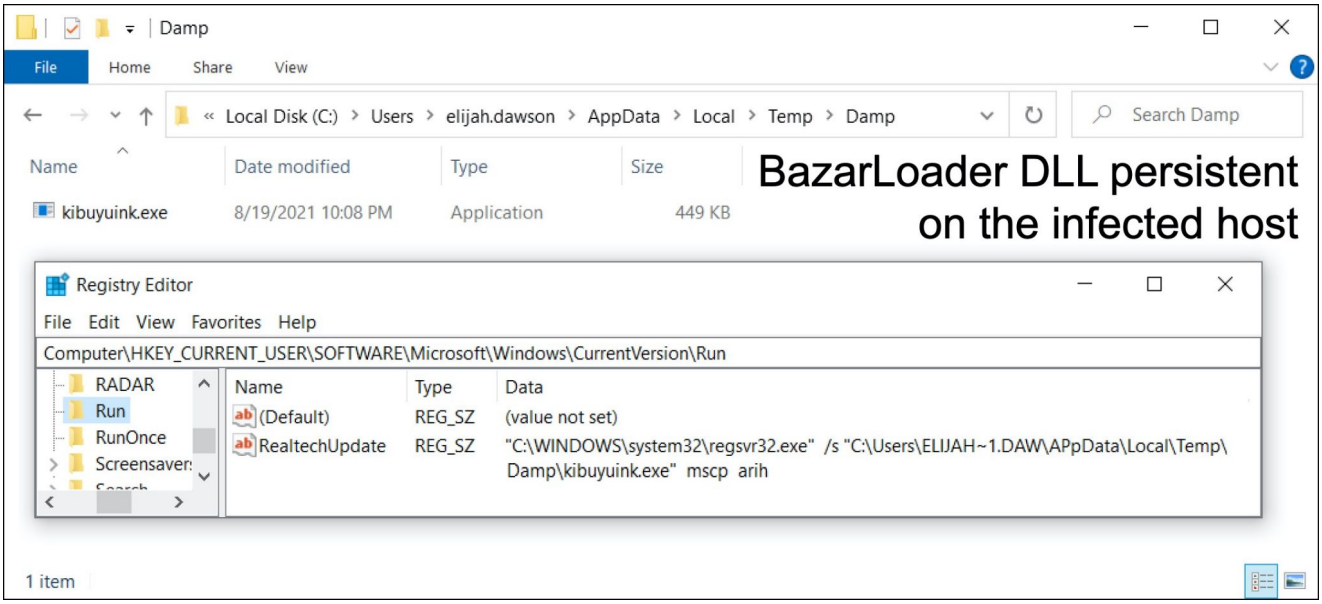
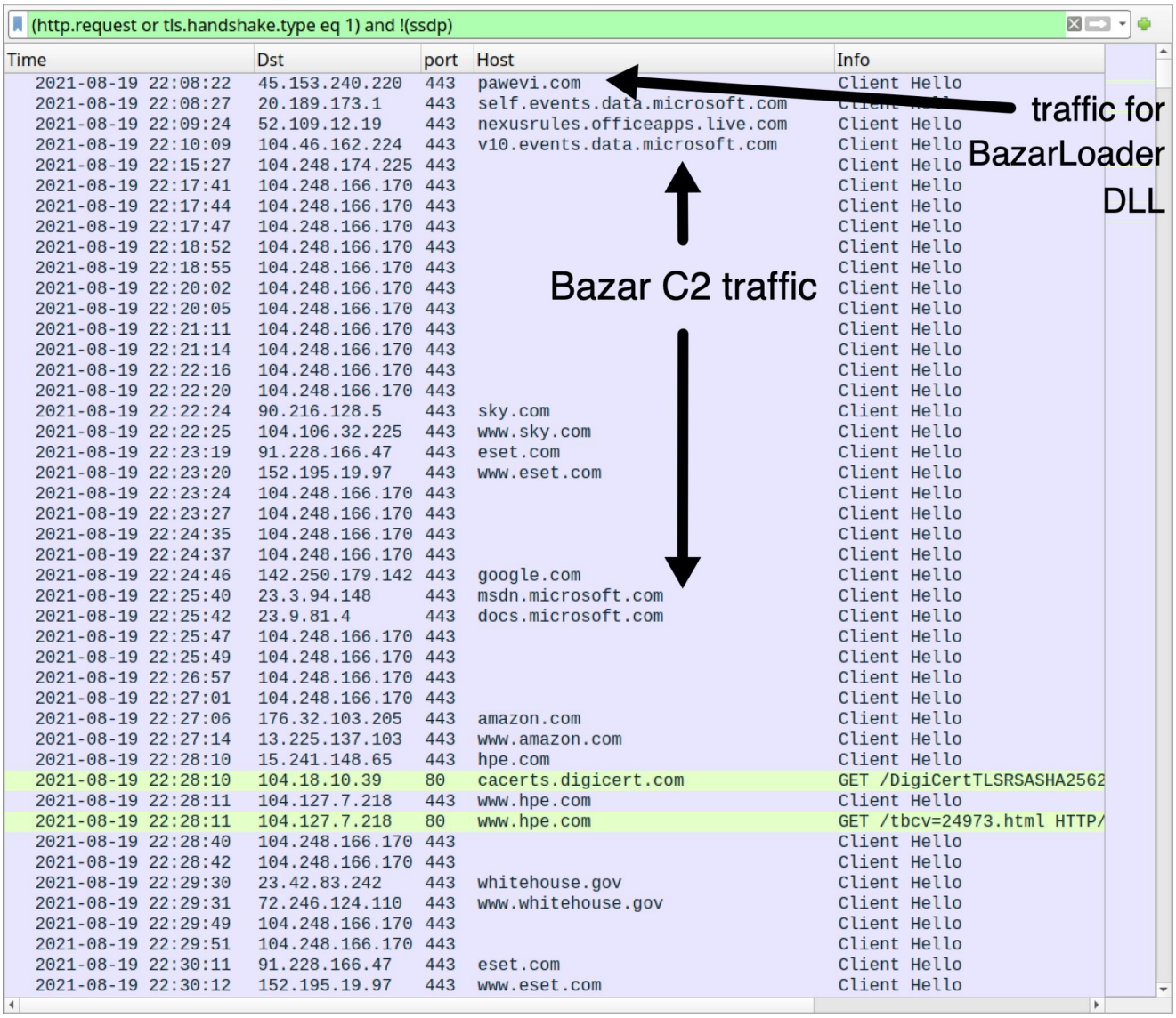


Figure 5. Location and Windows registry update for persistent BazarLoader DLL.

As seen in Figure 5, the filename changed from tru.dll to kibuyuink.exe, even though it remained a DLL and still required regsvr32.exe to run. Changing the filename extension is a common tactic seen in various malware infections.

Bazar C2 Traffic

This example of BazarLoader generated command and control (C2) activity, retrieving BazarBackdoor using HTTPS traffic from 104.248.174[.]225 over TCP port 443. Then BazarBackdoor generated C2 activity using HTTPS traffic to 104.248.166[.]170 over TCP port 443. In Figure 6, we refer to this combined C2 activity as Bazar C2 traffic.



Time	Dst	port	Host	Info
2021-08-19 22:08:22	45.153.240.220	443	pawevi.com	Client Hello
2021-08-19 22:08:27	20.189.173.1	443	self.events.data.microsoft.com	Client Hello
2021-08-19 22:09:24	52.109.12.19	443	nexusrules.officeapps.live.com	Client Hello
2021-08-19 22:10:09	104.46.162.224	443	v10.events.data.microsoft.com	Client Hello
2021-08-19 22:15:27	104.248.174.225	443		Client Hello
2021-08-19 22:17:41	104.248.166.170	443		Client Hello
2021-08-19 22:17:44	104.248.166.170	443		Client Hello
2021-08-19 22:17:47	104.248.166.170	443		Client Hello
2021-08-19 22:18:52	104.248.166.170	443		Client Hello
2021-08-19 22:18:55	104.248.166.170	443		Client Hello
2021-08-19 22:20:02	104.248.166.170	443		Client Hello
2021-08-19 22:20:05	104.248.166.170	443		Client Hello
2021-08-19 22:21:11	104.248.166.170	443		Client Hello
2021-08-19 22:21:14	104.248.166.170	443		Client Hello
2021-08-19 22:22:16	104.248.166.170	443		Client Hello
2021-08-19 22:22:20	104.248.166.170	443		Client Hello
2021-08-19 22:22:24	90.216.128.5	443	sky.com	Client Hello
2021-08-19 22:22:25	104.106.32.225	443	www.sky.com	Client Hello
2021-08-19 22:23:19	91.228.166.47	443	eset.com	Client Hello
2021-08-19 22:23:20	152.195.19.97	443	www.eset.com	Client Hello
2021-08-19 22:23:24	104.248.166.170	443		Client Hello
2021-08-19 22:23:27	104.248.166.170	443		Client Hello
2021-08-19 22:24:35	104.248.166.170	443		Client Hello
2021-08-19 22:24:37	104.248.166.170	443		Client Hello
2021-08-19 22:24:46	142.250.179.142	443	google.com	Client Hello
2021-08-19 22:25:40	23.3.94.148	443	msdn.microsoft.com	Client Hello
2021-08-19 22:25:42	23.9.81.4	443	docs.microsoft.com	Client Hello
2021-08-19 22:25:47	104.248.166.170	443		Client Hello
2021-08-19 22:25:49	104.248.166.170	443		Client Hello
2021-08-19 22:26:57	104.248.166.170	443		Client Hello
2021-08-19 22:27:01	104.248.166.170	443		Client Hello
2021-08-19 22:27:06	176.32.103.205	443	amazon.com	Client Hello
2021-08-19 22:27:14	13.225.137.103	443	www.amazon.com	Client Hello
2021-08-19 22:28:10	15.241.148.65	443	hpe.com	Client Hello
2021-08-19 22:28:10	104.18.10.39	80	cacerts.digicert.com	GET /DigiCertTLSRSASHA2562
2021-08-19 22:28:11	104.127.7.218	443	www.hpe.com	Client Hello
2021-08-19 22:28:11	104.127.7.218	80	www.hpe.com	GET /tbcv=24973.html HTTP/
2021-08-19 22:28:40	104.248.166.170	443		Client Hello
2021-08-19 22:28:42	104.248.166.170	443		Client Hello
2021-08-19 22:29:30	23.42.83.242	443	whitehouse.gov	Client Hello
2021-08-19 22:29:31	72.246.124.110	443	www.whitehouse.gov	Client Hello
2021-08-19 22:29:49	104.248.166.170	443		Client Hello
2021-08-19 22:29:51	104.248.166.170	443		Client Hello
2021-08-19 22:30:11	91.228.166.47	443	eset.com	Client Hello
2021-08-19 22:30:12	152.195.19.97	443	www.eset.com	Client Hello

Figure 6. Traffic from the infection filtered in Wireshark.

This example of Bazar C2 activity generates traffic to legitimate domains. This activity is not inherently malicious on its own. Various malware families generate similar traffic as a connectivity check or to ensure an infected Windows host has continued internet access.

Cobalt Strike Activity

Approximately 41 minutes after the initial BazarLoader infection, our infected Windows host started generating Cobalt Strike activity using HTTPS traffic to gojihu[.]com and yuxicu[.]com, as shown below in Figure 7.

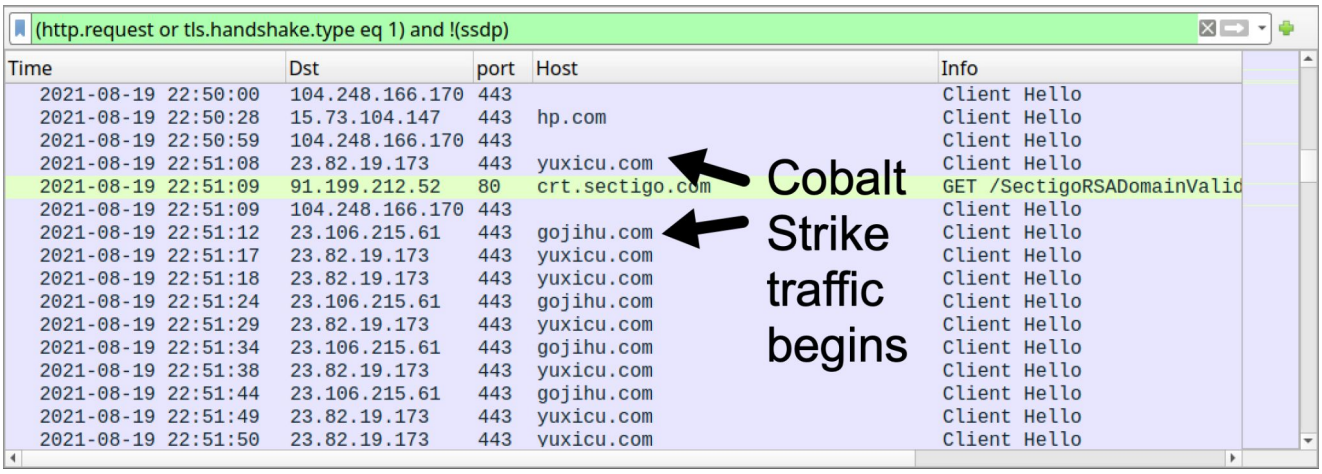


Figure 7. Wireshark showing when the Cobalt Strike activity began.

In this case, a Cobalt Strike DLL file was sent through Bazar C2 traffic and saved to the infected Windows host under the user's AppData\Roaming directory. Figure 8 shows the Cobalt Strike DLL running on the infected machine.

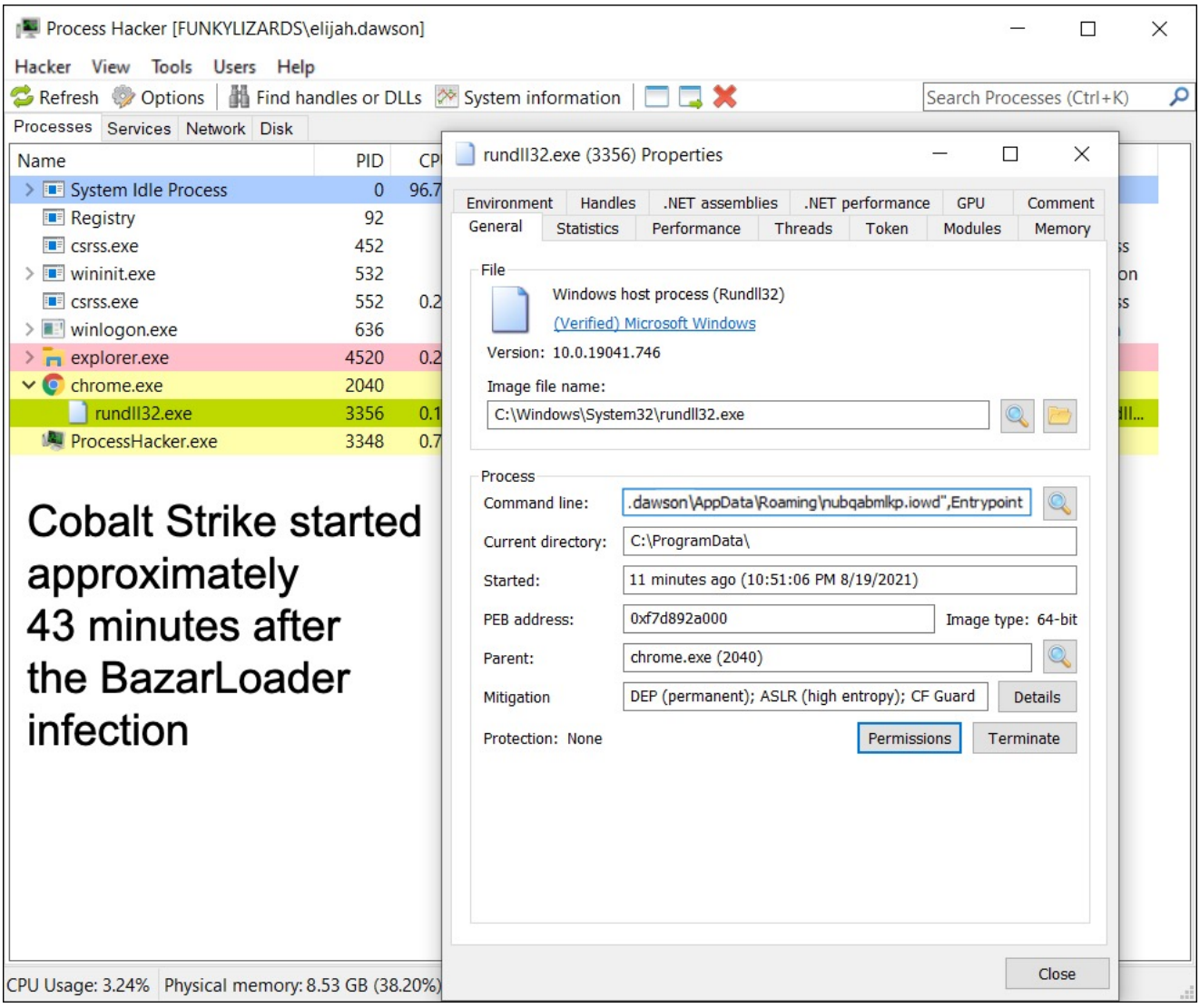


Figure 8. Cobalt Strike activity shown in Process Hacker.

Cobalt Strike leads to reconnaissance of an infected host's environment. In our lab environments, this reconnaissance activity can start within a few minutes after Cobalt Strike traffic first appears.

Reconnaissance Activity

In our case study, approximately two minutes after Cobalt Strike activity started, a tool to enumerate an AD environment appeared on the infected host at C:\ProgramData\AdFind.exe. This tool has been used by criminal groups to gather information from an AD environment. AdFind is a command line tool, and an associated batch file was used to run the tool in our case study.

Figure 9 shows the location of AdFind, the associated batch file adf.bat and the results of its search saved in seven text files.

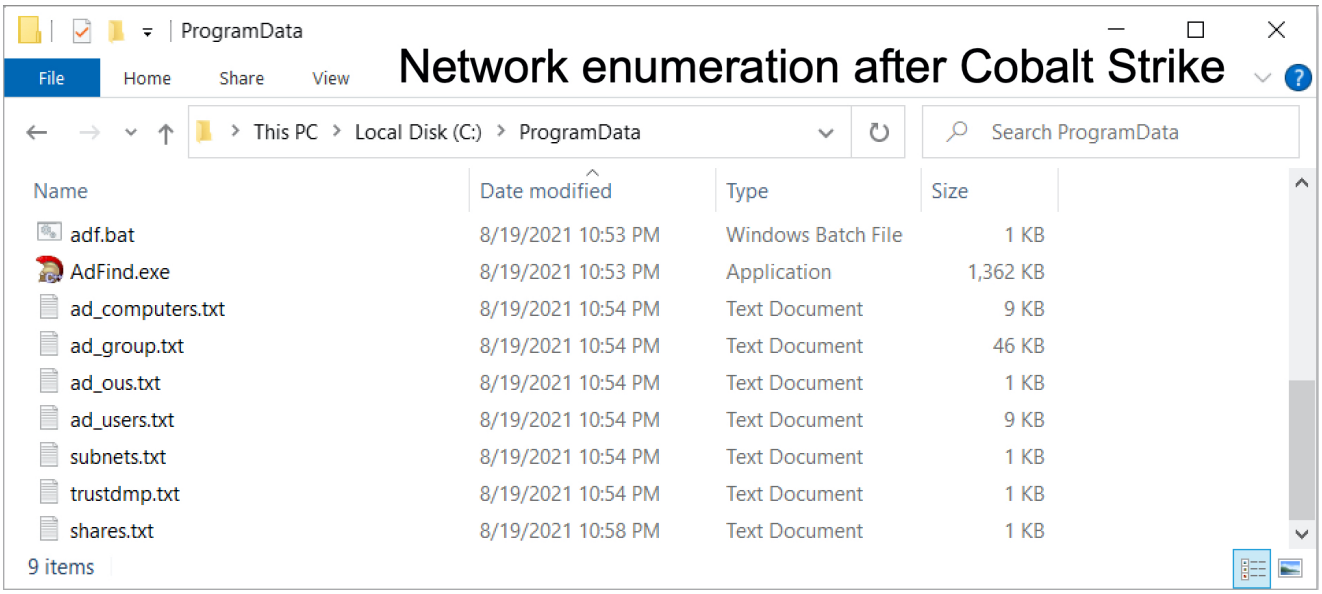


Figure 9. AdFind.exe, the batch file and search results saved to text files.
Figure 10 shows commands used in the adf.bat file that run AdFind.exe.

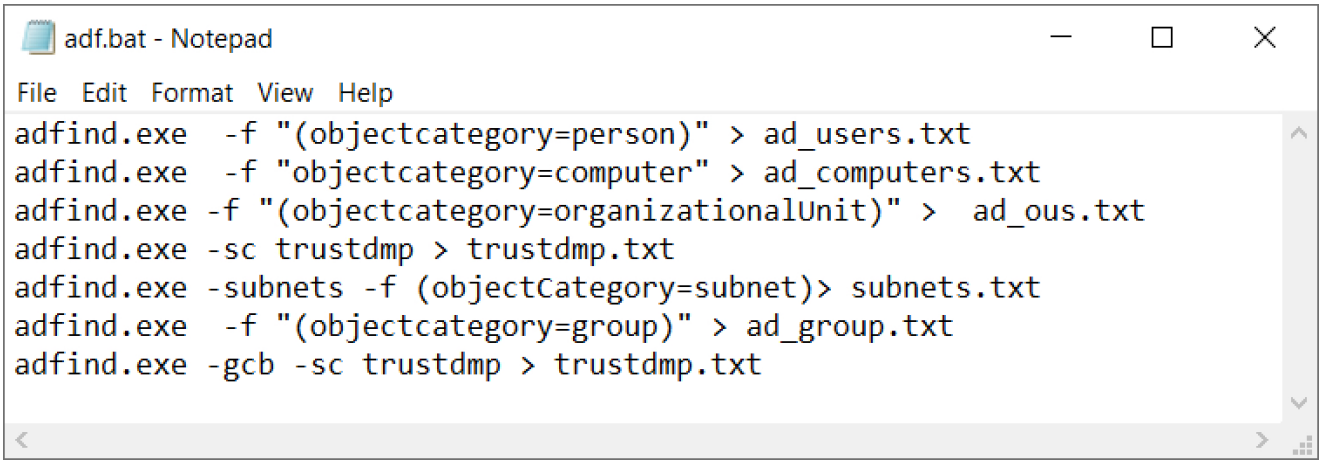


Figure 10. Commands used for AdFind.exe.

These commands reveal the users, computers, file shares and other information from a targeted AD environment.

Our example did not involve a high-value target, and the environment was wiped within two or three hours after the initial infection. In this example, no follow-up ransomware was sent after the reconnaissance.

Conclusion

This case study reveals one example of an initial malware infection moving to Cobalt Strike, followed by reconnaissance activity. When attackers use Cobalt Strike, they can also perform other types of reconnaissance in an AD environment.

If the AD environment is a high-value target, the attacker's next step is lateral movement and gaining access to the domain controller and other servers within the network.

This is a common pattern seen before attackers hit an organization with ransomware.

Organizations with decent spam filtering, proper system administration and up-to-date Windows hosts have a much lower risk of infection. Palo Alto Networks customers are further protected from this threat. Our Threat Prevention security subscription for the Next-Generation Firewall detects this and similar BazarLoader samples. Endpoint detection like Cortex XDR can prevent Cobalt Strike activity and criminal access to your network.

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

Excel file with macros for BazarLoader, SHA256 hash:
8662d511c7f1bef3a6e4f6d72965760345b57ddf0de5d3e6eae4e610216a39c1
File size: 332,087 bytes
File name: Documents new.xlsb

Malicious DLL for BazarLoader retrieved by above Excel macro, SHA256 hash:
caa03c25583ea24f566c2800986def73ca13458da6f9e888658f393d1d340ba1
File size: 459,776 bytes
Online location: hxxps://pawevi[.]com/lch5.dll
Initial saved location: C:\Users\[username]\tru.dll
Final location: C:\Users\[username]\AppData\Local\Temp\Damp\kibuyuink.exe
Run method: regsvr32.exe /s [filename]

Malicious DLL for Cobalt Strike, SHA256 hash:
73b9d1f8e2234ef0902fca1b2427cbef756f2725f288f19edbdedf03c4cadab0
File size: 443,904 bytes
File location: C:\Users\[username]\AppData\Roaming\nubqabmlkp.iowd
Run method: rundll32.exe [filename],Entrypoint

ADfind command-line tool for enumerating AD environment, SHA256 hash:
b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682
File size: 1,394,176 bytes
File location: C:\ProgramData\AdFind.exe

Batch file to run ADfind, SHA256 hash:
1e7737a57552b0b32356f5e54dd84a9ae85bb3acff05ef5d52aabaa996282dfb
File size: 385 bytes
File location: C:\ProgramData\adf.bat

Contents of adf.bat:

```
adfind.exe -f "(objectcategory=person)" > ad_users.txt
adfind.exe -f "objectcategory=computer" > ad_computers.txt
adfind.exe -f "(objectcategory=organizationalUnit)" > ad_ous.txt
adfind.exe -sc trustdmp > trustdmp.txt
adfind.exe -subnets -f (objectCategory=subnet)> subnets.txt
adfind.exe -f "(objectcategory=group)" > ad_group.txt
adfind.exe -gcb -sc trustdmp > trustdmp.txt
```

Additional Resources

BazarCall Method: Call Centers Help Spread BazarLoader Malware – Unit 42, Palo Alto Networks
TA551 BazarLoader to Cobalt Strike – Internet Storm Center
“Stolen Images Evidence” BazarLoader to Cobalt Strike – @Unit42_Intel
“Stolen Images Evidence” BazarLoader to Cobalt Strike – malware-traffic-analysis.net
Stolen Images Evidence” BazarLoader to Cobalt Strike to PrintNightmare – @Unit42_Intel
BazarLoader to Cobalt Strike – @Unit42_Intel
BazarLoader to Cobalt Strike to Anchor malware – Internet Storm Center
TA551 BazarLoader to Cobalt Strike – malware-traffic-analysis.net

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.