Glupteba Backdoor Trojan

Author: Christopher Kim

Overview

From 20 to 26 September, Infoblox detected communications between malicious Glupteba bots and command and control (C2) servers in customer DNS traffic. This activity was identified by our Threat Insight[1] (TI) security solution, which employs machine learning models to detect and block certain types of malicious behavior, in this case data exfiltration.[2]

Customer Impact

Glupteba is a backdoor trojan that was first discovered in 2014.[3] What sets it apart from other backdoors is its sophisticated functionality for stealthily controlling remote bots. The malware can also use modules to perform the following tasks:

- Install a rootkit to control the bot and hide malware files and processes from the system administrator.
- Turn off antivirus and security monitoring programs.
- Propagate across the victim's network using EternalBlue variant exploits.
- Compromise unpatched ethernet routers and use them as network proxies for future attacks.
- Steal data from local browser files.
- Secretly run cryptominers.

In late 2019, the malware authors applied a significant update that allows Glupteba to fetch C2 information by querying Bitcoin transaction IDs hardcoded into the binary.[4]

Campaign Analysis

Threat Insight detected 28 unique second-level domains (SLDs) in customer DNS traffic that were used for C2 communications. The domains are all inherently malicious and were registered between March and May 2020. The threat actor registered most of the domains with companies such as GoDaddy, Namecheap, or 101domain. The threat actor set all the nameservers to Cloudflare, a network provider often used by miscreants for its Dynamic DNS services.

Domain names may have been generated with a dictionary-based domain generation algorithm (DGA). Each domain name is alphanumeric and consists of two or more words. Each bot submitted hundreds of DNS requests to fully qualified domain names (FQDNs) that contained a patterned global unique identifier (GUID).

Historic queries in customer DNS traffic indicated that some devices were infected as early as May 2020.

Attack Chain

In one recent campaign, the actor distributed Glupteba using a fake YouTube video download site.[5] When a visitor submits the URL of a YouTube video into the site's input field, they are prompted to download an executable file hosted at another site. The filename of the executable includes the individual words of the video title, delimited by underscores.

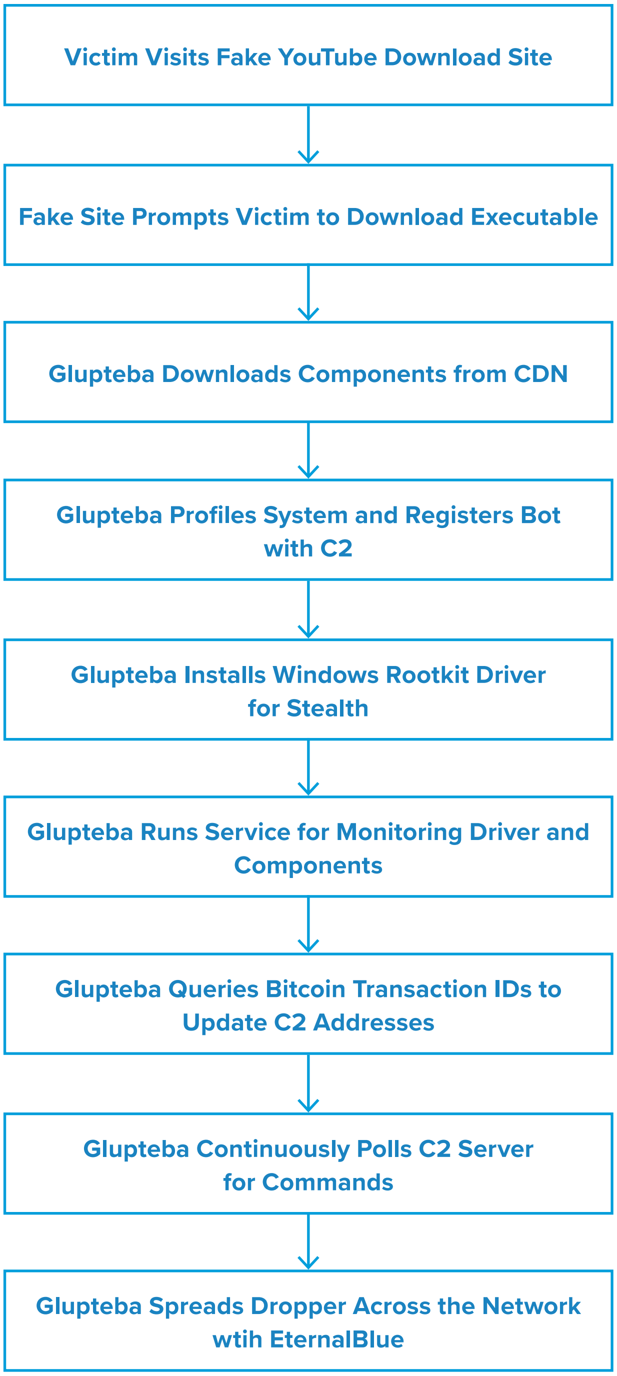
After the victim executes the file, the malware downloads components that extend its capabilities from the actor-controlled content distribution network (CDN) server.

Next, the malware profiles the infected machine and establishes a connection with the C2 to submit system information, as well as register the bot within the Glupteba botnet. Additionally, Glupteba identifies and shuts down antivirus and security monitoring applications that are running in the system.

The malware then installs a Windows kernel rootkit driver to protect certain directories and components that it dropped into the system.

Glupteba achieves persistence using the *watchdog.exe* process that reinitializes any failed driver or components of the malware. This process also updates the C2 address configuration by querying Bitcoin transaction IDs hardcoded in the binary. Throughout the process, the malware continuously polls the C2 server to obtain commands, configuration information, and other instructions.

Finally, Glupteba spreads itself laterally across the network after it identifies vulnerable machines using the EternalBlue exploit.


Victim Visits Fake YouTube Download Site
Fake Site Prompts Victim to Download Executable
Glupteba Downloads Components from CDN
Glupteba Profiles System and Registers Bot with C2
Glupteba Installs Windows Rootkit Driver for Stealth
Glupteba Runs Service for Monitoring Driver and Components
Glupteba Queries Bitcoin Transaction IDs to Update C2 Addresses
Glupteba Continuously Polls C2 Server for Commands
Glupteba Spreads Dropper Across the Network wtih EternalBlue

Vulnerabilities & Mitigation

Infoblox recommends the following actions to reduce the risk of this type of infection:

- Subscribe to Infoblox Threat Insight, which detects and can block data exfiltration activities over DNS.
- Frequently patch software; Glupteba propagates by exploiting vulnerable Microsoft Windows Server Message Block (SMB) hosts via EternalBlue.
- Use strong antivirus software and web filtering tools to combat drive-by download attacks.
- Only download software and applications from trusted sources.
- Devices infected by rootkit frequently send TCP/IP packets. Examine unusual patterns or volume of outbound connections in your firewall logs.

Endnotes

1. https://www.infoblox.com/products/threat-insight/
2. https://www.infoblox.com/glossary/dns-tunneling/
3. https://labs.bitdefender.com/2019/12/revisiting-glupteba-still-relevant-five-years-after-debut/
4. https://news.sophos.com/en-us/2020/06/24/glupteba-report/
5. https://twitter.com/James_inthe_box/status/1293305070491074560

Infoblox
NEXT LEVEL NETWORKING

Infoblox enables next-level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. Infoblox has over 8,000 customers, including 350 of the Fortune 500, and is recognized as the industry leader in the DDI networking market.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com