LemonDuck Trojan Delivers Cryptominers and Other Malware

Author: James Barnett

Overview

On July 29, Microsoft reported a series of ongoing malware campaigns that involve LemonDuck: a trojan botnet that installs cryptominers and other malware.[1]

Customer Impact

The majority of LemonDuck's targets are businesses in the manufacturing and IoT industries, and it has been seen across the world including the United States, Russia, China, Germany, the United Kingdom, and more. LemonDuck is one of the few known botnets that target Linux as well as Windows systems, and its capabilities have been expanding rapidly in recent months.

Campaign Analysis

LemonDuck uses a variety of distribution methods, including but not limited to, malspam, server exploits, infected USB devices, and brute-force attacks. When distributed via exploits and brute-force attacks, LemonDuck is usually controlled by a human actor during the initial stages of the infection. When distributed through other vectors, LemonDuck is operated by a series of automated scripts and servers.

LemonDuck's malspam campaigns have reused the same email subjects, body content, and attachment names since mid-2020.[2] Its most typical email subjects are "The Truth of COVID-19" and "broken file," and its email attachments are DOC, JavaScript (JS), and ZIP files that contain JS files. All three types of files use "readme" as the filenames.

Attack Chain

When the victim opens the malicious LemonDuck attachment *readme.js*, the script executes an obfuscated PowerShell command that retrieves malicious scripts from a command and control (C&C) server. After retrieving these scripts, LemonDuck tries to expand its capabilities, establish persistence, and spread to other systems.

Once it has a foothold on a system, LemonDuck creates scheduled tasks that rerun the aforementioned PowerShell script at regular intervals, to ensure that its components remain on the system. It also creates a backup persistence mechanism that uses Windows Management Instrumentation (WMI) Event Consumers to execute that PowerShell script.

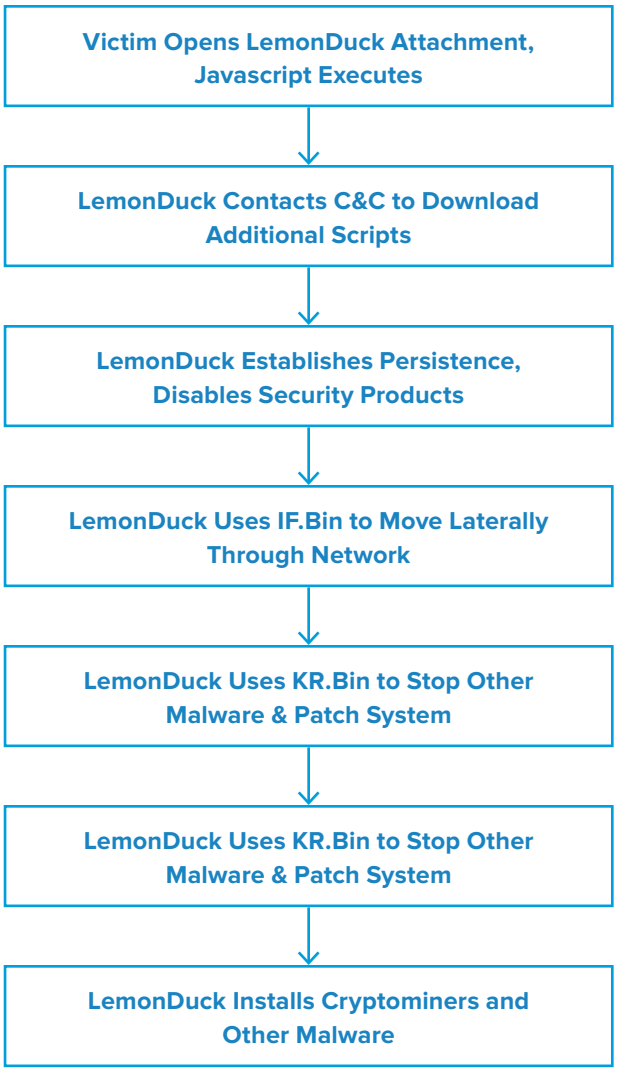
After establishing persistence, LemonDuck attempts to disable Microsoft Defender for Endpoint and to add all contents of the *C:* drive to Microsoft Defender's exclusion list; the goal is to make Microsoft Defender stop scanning for malware. It then tries to uninstall other security products by using *CMD.EXE* to call *WMIC.EXE*.

During this process, LemonDuck runs its infection script, commonly named *IF.Bin*, to scan the network for vulnerable systems and devices. This script includes a wide array of exploits that can allow LemonDuck to move laterally through the network, via SMB, SQL, and other services.

LemonDuck's *IF.Bin* also contains code that allows it to infect USB storage devices, as well as an embedded copy of Mimikatz, which allows it to steal credentials from infected systems. *IF.Bin* also contains a function that can locate Microsoft Outlook mailboxes on the infected system, so that it can send a copy of its initial malspam attack to every address in the compromised mailbox's address book.

Another notable LemonDuck script that runs throughout the infection process is *KR.Bin*. This script (1) scans the system for indicators of competing malware and (2) attempts to terminate them, so that LemonDuck and its associated payloads are the only malware running on the system. In addition, to preserve system resources, *KR.Bin* closes commonly used cryptomining ports and shuts down known mining services. In some cases, the threat actors behind LemonDuck will manually patch the security exploits they initially used; presumably, to make system administrators believe the system is not vulnerable to the exploit and has not been infected.

After LemonDuck has thoroughly established itself on the system and spread through the network, it downloads additional malware payloads that allow the actors to monetize the infection. LemonDuck's most commonly delivered payload has been the XMRig cryptominer but it has also delivered Ramnit and other secondary payloads. Regardless of the payload, LemonDuck will remain on the system and communicate with its C&C servers to transmit stolen information and any cryptocurrency generated by its cryptominer.



Vulnerabilities & Mitigation

Infoblox recommends the following mitigations for preventing and reducing the impact of an infection by LemonDuck:

- Monitor for patterns and unusual protocols running on the network. Cryptocurrency-mining network traffic occurs at regularly repeating intervals.
- Sanitize attachments to remove potentially harmful or active content, such as macros, JavaScript, and links to executable downloads.
- Use a packet-level access filter that enforces a tight set of rules for how interfaces on a USB device can interact with the host operating system. Disable AutoRun for removable media.
- If removable media has seen limited usage, consider deploying an endpoint security solution to enforce policies for removable media usage, such as blocking executables from running off of a USB device.

Endnotes

1. https://www.microsoft.com/security/blog/2021/07/29/when-coin-miners-evolve-part-2-hunting-down-lemonduck-and-lemoncat-attacks/
2. https://www.microsoft.com/security/blog/2021/07/22/when-coin-miners-evolve-part-1-exposing-lemonduck-and-lemoncat-modern-mining-malware-infrastructure/

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com