LemonDuck botnet evolves to allow hands-on-keyboard intrusions

By Catalin Cimpanu

Published: 2023-01-18 · Archived: 2026-04-06 00:45:15 UTC

Over the past two years, a once-tiny crypto-mining malware strain has evolved into a massive botnet and is now experimenting with hands-on-keyboard intrusions into hacked networks, signaling a dangerous turn that could see the group's operators deliver ransomware or more dangerous threats in the coming future.

Tracked as **LemonDuck**, the botnet was first spotted by Israeli security firm Guardicore in the first half of 2019.

> #Campaign in tweets - @Guardicore Labs in a new tradition; we find the attacks, you get to know them and learn the attackers' tricks and techniques. This time, let's get familiarized with "Lemon_Duck", a #cryptomining campaign involving a sophisticated #propagation tool. pic.twitter.com/sUBND697af
>
> — Ophir Harpaz (@OphirHarpaz) July 3, 2019

Initially, the botnet was a small-time operation that relied on classic email spam to distribute malicious files that would infect users with its malware.

The first iterations of LemonDuck were simplistic. They infected systems, disabled security software, expanded into internal networks, and then deployed a Monero-mining app to generate profits using a hacked organization's computer resources.

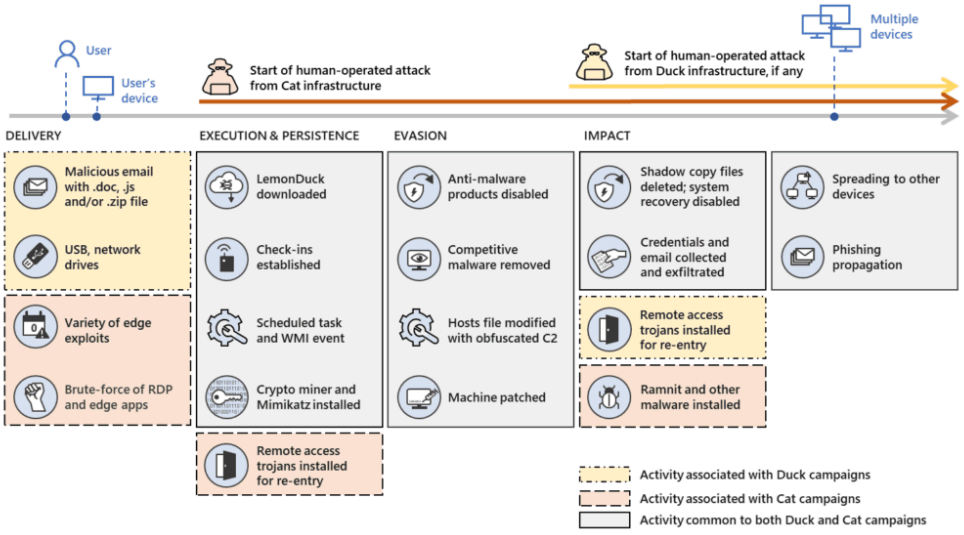
However, while some botnets would be happy with this type of access and operational model, LemonDuck was one of the rare botnet crews that did not content themselves with meager profits.

Over the past two years, the malware has seen one of the most impressive expansions among any botnet operation today. It constantly received new features, and in 2020 its creators took a rare step to add a new infection mechanism to the botnet by adding support for web-based attacks.

This included the botnet attacking unpatched web servers using exploit code and brute-force (password-guessing) attacks against systems like Microsoft Exchange email servers, SQL databases, Hadoop and Redis servers, and systems running internet-exposed SMB and RDP services.

This saw the botnet grow in size and sophistication far beyond most of its crypto-mining rivals. Today, the botnet can infect both Windows and Linux systems and comes equipped with a trove of features that allow it to remove competing malware from the same infected hosts, patch infected servers to avoid attacks from rivals, and collect credentials from local systems to ensure future and more persistent access.

LemonDuck has grown so much that it recently also drew the attention of the Microsoft security team, which dedicated a two-part series on the malware's recent upgrades.



While both Cisco Talos and Sophos previously analyzed LemonDuck operations in their own reports, Microsoft drew attention to recent developments in the LemonDuck code that had been focusing on adding the ability to carry out hands-on-keyboard attacks.

A relatively new term in the cybersecurity jargon, hands-on-keyboard attacks are when threat actors stop using automated scripts and manually log into an infected system to execute manual commands themselves.

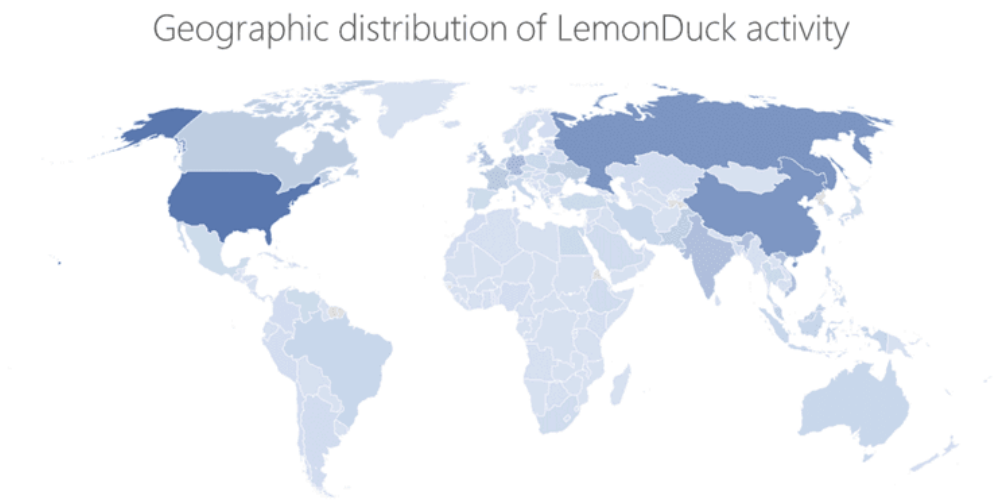
In recent years, all the botnets that have added this capability have used it primarily to ensure that expanding access into a high-profile victim's internal network succeeds by having the operator run the commands by themselves using "hands on keyboard," hence the term's origin.

Hands-on-keyboard attacks are usually associated with nation-state threat actors, ransomware gangs, and financially motivated cybercrime groups.

"Back in 2019, when Guardicore Labs discovered LemonDuck, it was the classic spray-and-pray type of campaign," Ophir Harpaz, the GuardiCore malware analyst who first spotted LemonDuck, told *The Record* in an interview last week.

"There was no sign of the hands-on-keyboard nature that future attacks would carry. However, we could tell even at that early phase that LemonDuck operators were serious about their business; their multi-stage PowerShell scripts were more complex and obfuscated than others', and they already made extensive use of open-source tools for code execution and infection," Harpaz added.

"Actually, many of the aspects that Microsoft points out as novel have been there since the beginning: credential theft, removal of security controls and lateral movement - were all there from the very start.



"What is different about the LemonDuck group is their persistence - and for once, I'm not talking about persistence on infected machines, but persistence in the landscape of botnet campaigns," the GuardiCore researcher said.

"They started in March 2019 and literally never stopped since. There was not a single month where we didn't observe a LemonDuck attack hitting our threat sensors," Harpaz told *The Record*.

"With such consistent campaigns, threat actors must up their game to stay powerful. It is, therefore, no surprise that LemonDuck, which has been running for more than two years, evolves into a much more aggressive campaign with multiple variants and infrastructures."

No connections to ransomware attacks yet

Right now, even if there's been an increase of incidents where a LemonDuck infection has evolved into a hands-on-keyboard attack, there is no evidence to support a theory that LemonDuck has shifted from its primary purpose of illicit crypto-mining.

However, Microsoft has also noted that LemonDuck operators have also begun deploying other malware strains on systems they infected, such as the Ramnit family and others.

With LemonDuck showing signs that it may evolve into a Malware-as-a-Service operation that rents access to other cybercrime gangs, the ability to carry out hands-on-keyboards attacks may soon be abused for more dangerous intrusions, such as economic espionage, BEC scams, or even ransomware.

Until then, IT security teams will need to re-assess and prioritize LemonDuck detections before this new botnet catches them off guard.

No previous article

No new articles

Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.
