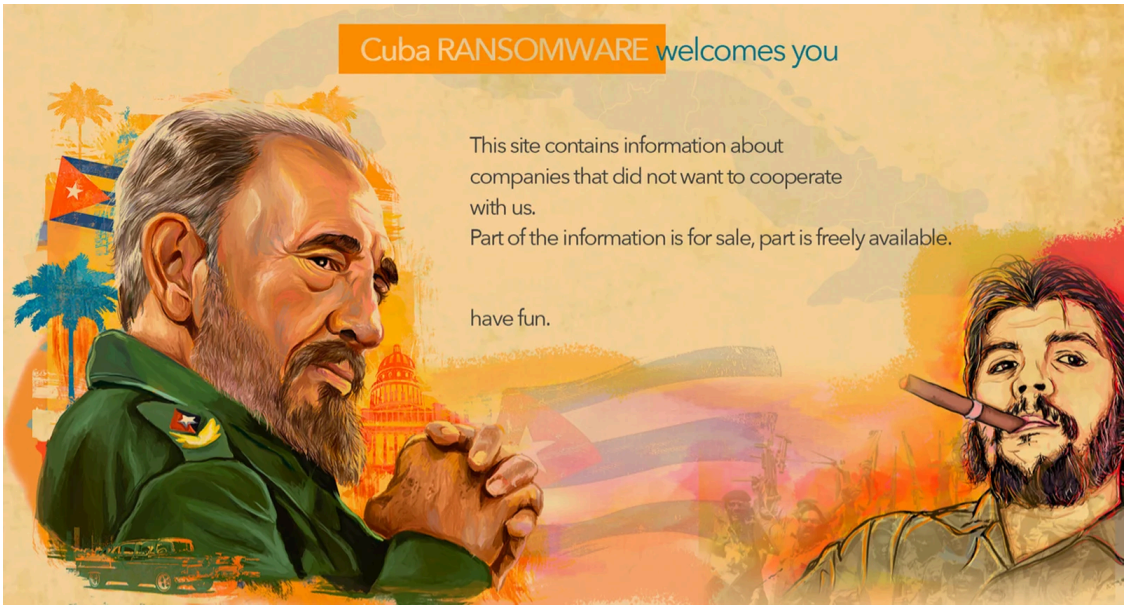
Microsoft Exchange servers hacked to deploy Cuba ransomware

By Bill Toulas

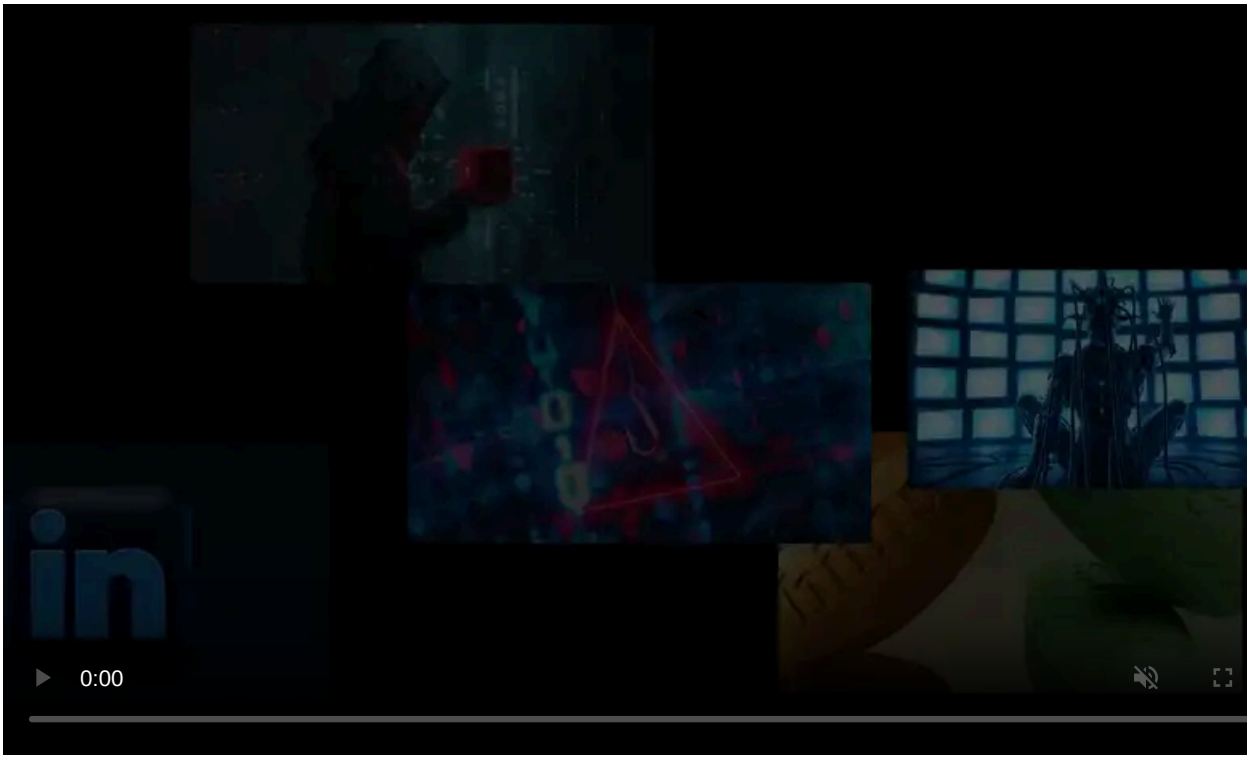
Published: 2022-02-24 · Archived: 2026-04-05 16:20:16 UTC

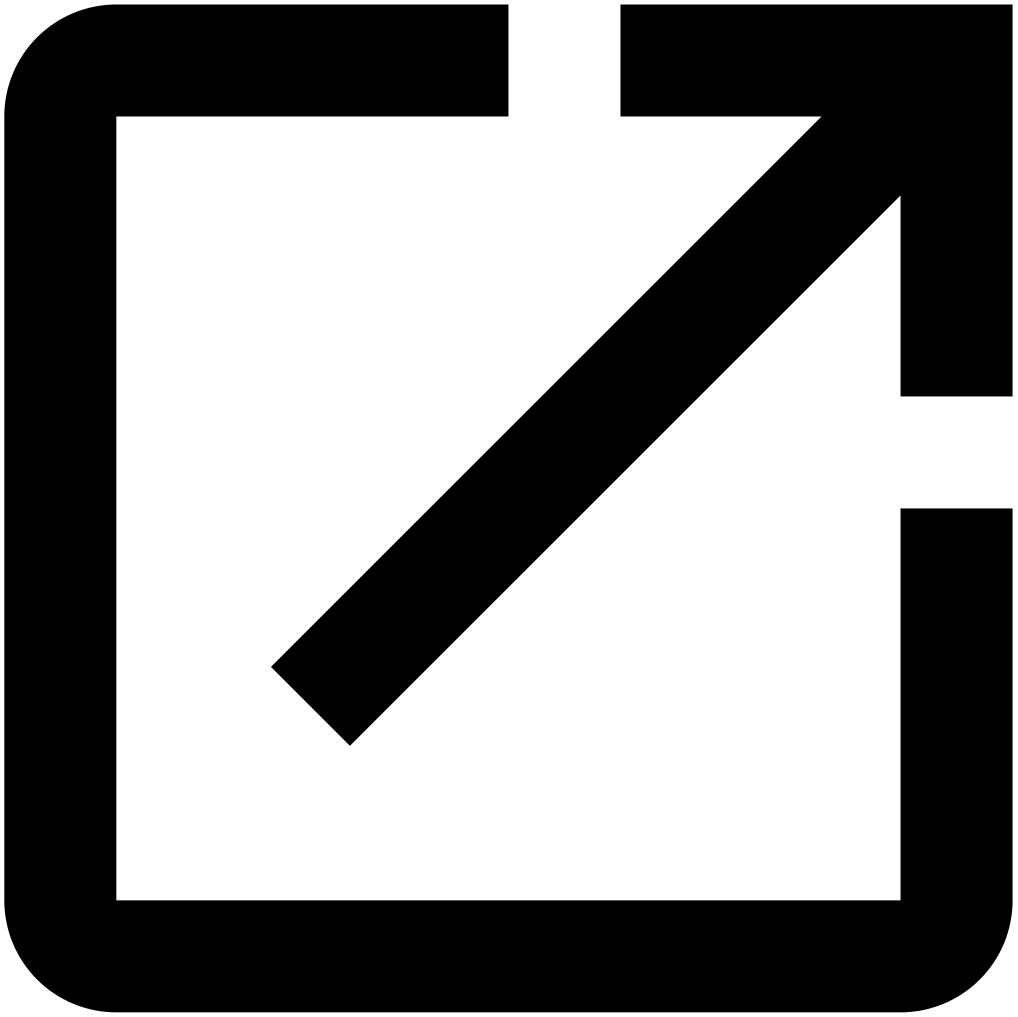


The Cuba ransomware operation is exploiting Microsoft Exchange vulnerabilities to gain initial access to corporate networks and encrypt devices.

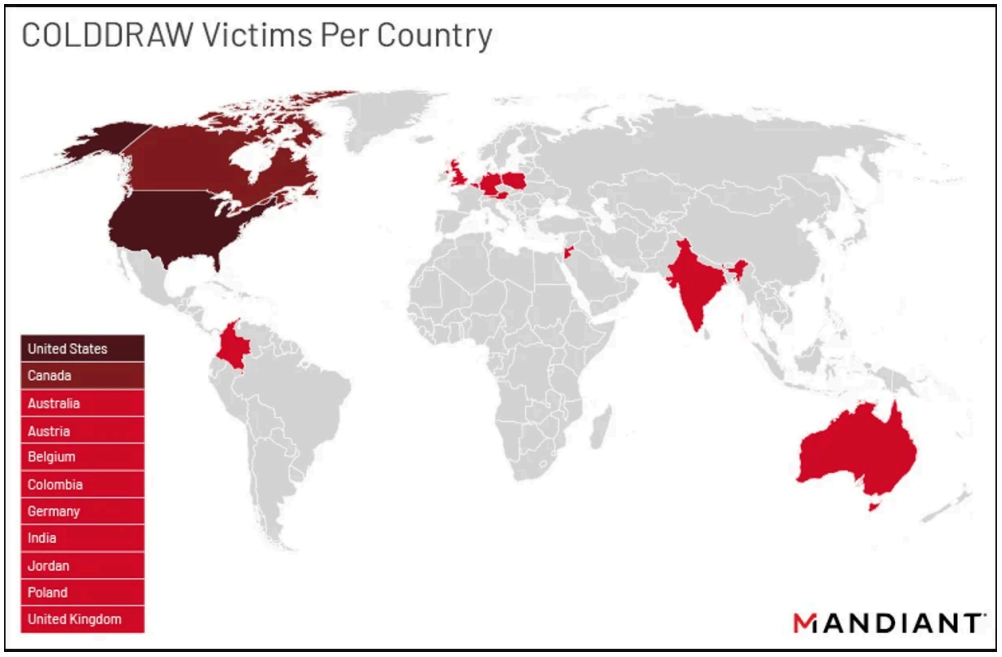
Cybersecurity firm Mandiant tracks the ransomware gang as UNC2596 and the ransomware itself as COLDDRAW. However, the ransomware is more commonly known as Cuba, which is how BleepingComputer will reference them throughout this article.

Cuba is a ransomware operation that launched at the end of 2019, and while they started slow, they began to pick up speed in 2020 and 2021. This increase in activity led to the FBI issuing a Cuba ransomware advisory in December 2021, warning that the gang breached 49 critical infrastructure organizations in the U.S.


0:00



In a new report by Mandiant, researchers show that the Cuba operation primarily targets the United States, followed by Canada.



Cuba ransomware victims heat map
Source: Mandiant

Mixing commodity and custom malware

The Cuba ransomware gang was seen leveraging Microsoft Exchange vulnerabilities to deploy web shells, RATs, and backdoors to establish their foothold on the target network since August 2021.

"Mandiant has also identified the exploitation of Microsoft Exchange vulnerabilities, including ProxyShell and ProxyLogon, as another access point leveraged by UNC2596 likely as early as August 2021," explains Mandiant in a new report.

The planted backdoors include Cobalt Strike or the NetSupport Manager remote access tool, but the group also uses their own 'Bughatch', 'Wedgecut', and 'eck.exe", and Burntcigar' tools.

Wedgecut comes in the form of an executable named "check.exe," which is a reconnaissance tool that enumerates the Active Directory through PowerShell.

Bughatch is a downloader that fetches PowerShell scripts and files from the C&C server. To evade detection, it loads in memory from a remote URL.

Burntcigar is a utility that can terminate processes at the kernel level by exploiting a flaw in an Avast driver, which is included with the tool for a "bring your own vulnerable driver" attack.

Finally, there's a memory-only dropper that fetches the above payloads and loads them, called Termite. However, this tool has been observed in campaigns of multiple threat groups, so it's not used exclusively by the Cuba threat actors.

The threat actors escalate privileges using stolen account credentials sourced through the readily available Mimikatz and Wicker tools.

Then they perform network reconnaissance with Wedgecut, and next, they move laterally with RDP, SMB, PsExec, and Cobalt Strike.

The subsequent deployment is Bughatch loaded by Termite, followed by Burntcigar, which lays the ground for data exfiltration and file encryption by deactivating security tools.

The Cuba gang doesn't use any cloud services for the exfiltration step but instead sends everything onto their own private infrastructure.

Cuba ransomware note to victims
Source: Mandiant

An evolving operation

Back in May 2021, Cuba ransomware partnered with the spam operators of the Hancitor malware to gain access to corporate networks through DocuSign phishing emails.

Since then, Cuba has evolved its operations to target public-facing services vulnerabilities, such as the Microsoft Exchange ProxyShell and ProxyLogon vulnerabilities.

This shift makes the attacks more potent but also easier to thwart, as security updates that plug the exploited issues have been available for many months now.

The Cuba operation will likely turn its attention to other vulnerabilities once there are no more valuable targets running unpatched Microsoft Exchange servers.

This means that applying the available security updates as soon as the software vendors release them is key in maintaining a robust security stance against even the most sophisticated threat actors.

Source: https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-cuba-ransomware/