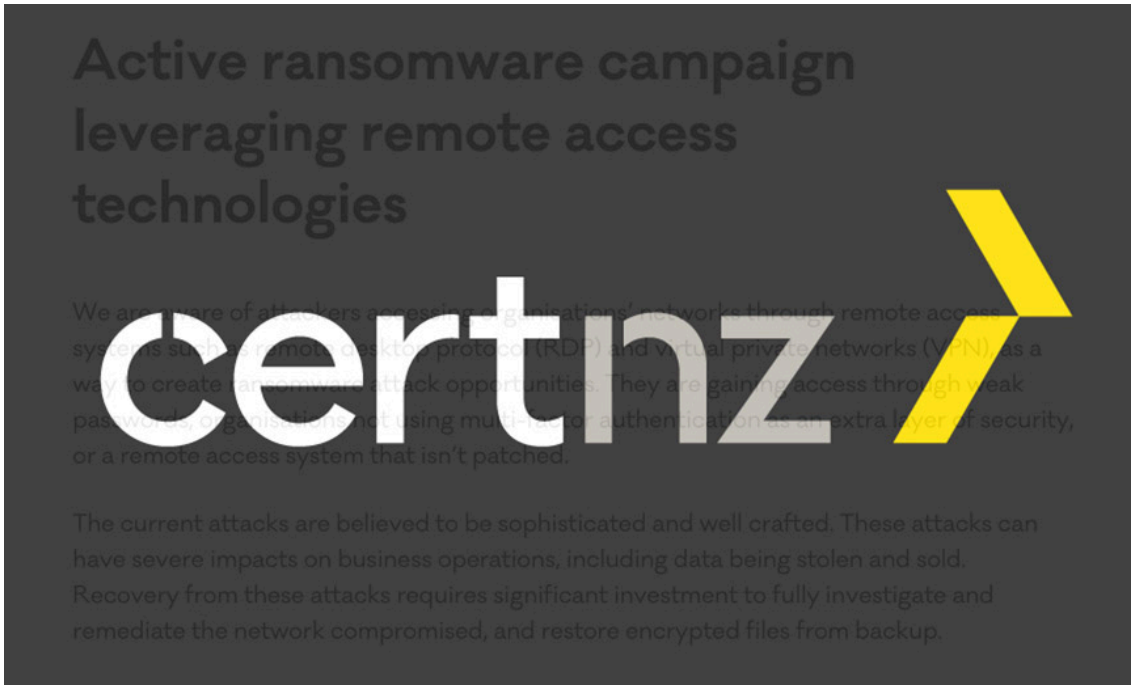
Nefilim Ransomware Gang Tied to Citrix Gateway Hacks

By Mathew J. Schwartz

Archived: 2026-04-05 12:59:39 UTC

Cybercrime , Fraud Management & Cybercrime , Governance & Risk Management

Campaign Targets Unpatched Software and Weak Authentication, Defenders Warn (euroinfosec) • June 22, 2020



CERT New Zealand issued an alert

A crime gang seeking "ransomware attack opportunities" is targeting organizations that use unpatched or poorly secured Citrix remote-access technology, then stealing data, unleashing crypto-locking malware and using the threat of exfiltrated data being publicly dumped to try to force payment, New Zealand's national computer emergency response team warns.

In an alert issued last week, and subsequently amplified by the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, CERT NZ says that a "sophisticated and well-crafted" attack campaign has been hitting unprepared organizations with Nefilim - aka Nephilim - ransomware.

"We are aware of attackers accessing organizations' networks through remote access systems, such as remote desktop protocol and virtual private networks, as a way to create ransomware attack opportunities," CERT NZ's security alert says. "They are gaining access through weak passwords, organizations not using multifactor authentication as an extra layer of security, or a remote access system that isn’t patched."

After this group of attackers gains access to a network, security researchers say they often practice living-off-the-land tactics, which refers to using legitimate tools to try to better evade detection. Once an attacker gains a foothold through the remote access system, they then use tools such as Mimikatz, PsExec and Cobalt Strike to elevate privileges, move laterally across a network and establish persistence on the network," CERT NZ says.

Mimikatz is a credential-stealing tool, PsExec is a command-line tool and Cobalt Strike is a legitimate penetration testing framework, which is similar to Metasploit. Experts say these tools and tactics are used by a number of more sophisticated attackers (see: *10 Ransomware Strains Being Used in Advanced Attacks*).

Data Exfiltration, Then Ransomware

After gaining entry to a network, the attackers in this campaign have been searching for sensitive data and exfiltrating it, after which they install crypto-locking malware on as many network-connected systems as possible, CERT NZ says. While this has included Nefilim ransomware, it notes that "other ransomware can also be used."

In terms of vulnerable software being targeted by hackers, CERT NZ says that weak RDP credentials, and especially RDP or other remote-access environments not protected by MFA, are at risk (see: *Why Are We So Stupid About RDP Passwords?*). But it also notes that "Citrix remote access technologies have been reported as a common way for attackers to gain access," referencing a Citrix vulnerability, CVE-2019-19781, which came to light last December and was patched in January amid reports that it was being widely exploited.

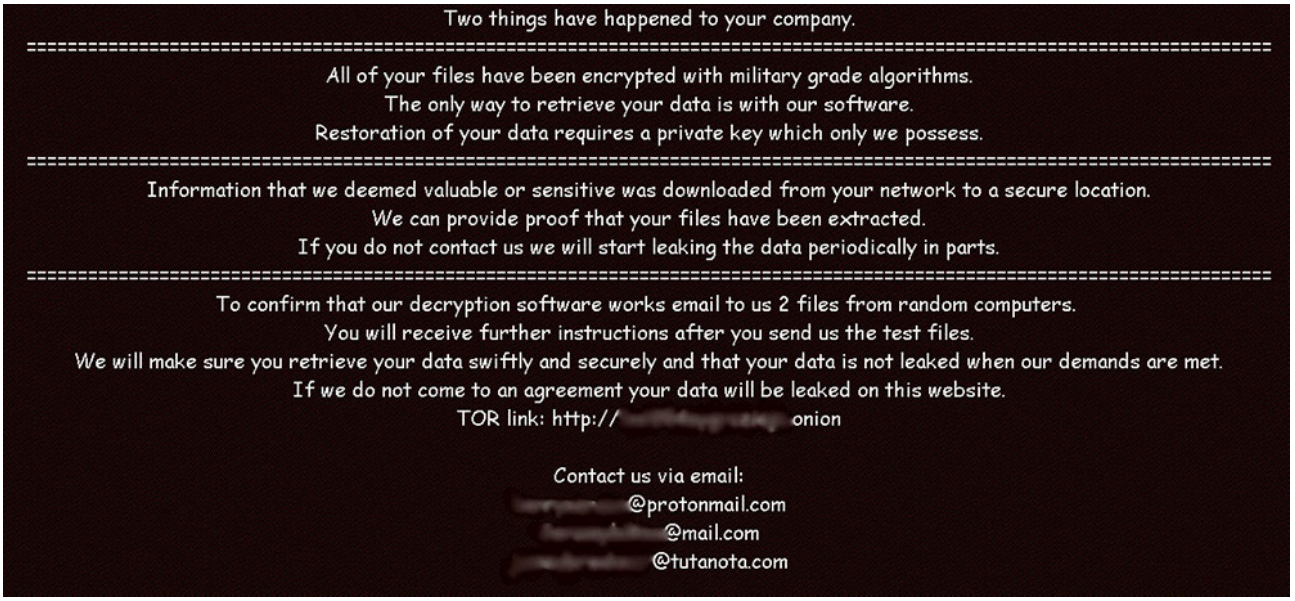
On Thursday, CISA published its own threat advisory about the Nefilim ransomware campaign, linking to the New Zealand alert, as well as referencing CISA's best practices for protecting against ransomware.

Nefilim: Closed Shop

Security experts say that unlike ransomware-as-a-service operations such as REvil, aka Sodinokibi, in which operators provide ransomware code to affiliates and split profits, Nefilim appears to be run as a closed shop by a single gang.

"Nefilim emerged in March 2020 and shares a substantial portion of code with another ransomware family, Nemty," security firm AlienVault notes. "Nefilim is another family which has very quickly risen to prominence with multiple damaging campaigns that threaten to publish victims' sensitive information in the event they fail to 'cooperate' with the attacker's demands."

Exfiltrating data and using it to try to force victims to pay was pioneered by the Maze gang last November. Since then, about a dozen other RaaS operators and ransomware gangs have followed suit (see: *Crypto-Lock and Tell: Ransomware Gangs Double Down on Leaks*).



Nefilim ransom note (Source: SentinelLabs)

One of the most high-profile attacks to date by Nefilim was against Australian shipping giant Toll Group, which first publicized the attack on May 5. Six weeks earlier, Toll Group fell victim to a Mailto - aka Netwalker - ransomware attack, which had disrupted operations for weeks. In both cases, Toll Group refused to pay a ransom. In response, Nefilim began leaking stolen Toll Group data and said on its dedicated leaks site that Toll Group had failed to fully shore up defenses following the Mailto hit (see: *Toll Group Data Leaked Following Second Ransomware Incident*).

Watch for Lateral Movement

To ascertain if an organization has been hit by Nefilim, "check your remote-access systems for any sign of unauthorized access," CERT NZ advises. "If any unauthorized access is detected, further investigation will be required to determine any lateral movement across the network."

Trend Micro, in an analysis of an attempted attack by the Nefilim gang against one of its customers in March, noted that among the various tricks and tactics used by attackers, they relied on PsExec to try to remotely execute commands in the victim's network. In addition, attackers attempted to move around the network well in advance of attempting to deploy ransomware.

"What can be observed from this incident is that the threat actors behind it are not just relying on Nefilim alone," Trend Micro said in its analysis. "They might already have exfiltrated the data even before they launched a full-on ransomware attack."

That's why detecting these types of attackers as quickly as possible is imperative, and one way to spot these types of attacks is to watch not just for attack code, but also "any evidence of lateral movement and data exfiltration within the environment," Trend Micro said. "An attack's point of entry may not be where the important data is found; therefore, threat actors would need to be able to move around within the environment (host-to-host) to get to the parts of the system where the juicier data is stored. Being able to identify unusual outbound traffic patterns for hosts (host-to-external) is equally important, as this represents potential data exfiltration."

Data Breach Risk

As with other ransomware gangs that now practice data exfiltration, Nefilim attackers' focus on stealing data before encrypting systems means that organizations typically don't just need to recover from a ransomware outbreak, but also ascertain what data was stolen.

Per breach-notification rules in place in numerous countries, including across the U.S. as well as in Europe under the EU's General Data Protection Regulation, if certain types of personal or financial information get accessed by attackers, the organization may need to report the breach to authorities and potentially also send breach notifications to affected individuals.

Researchers at SentinelLabs, the research division of SentinelOne, say the Nefilim gang threatens to leak stolen data unless victims cooperate, and it historically has viewed any attempt to negotiate down the size of the demanded ransom payment as failing to cooperate.

"While Maze, DoppelPaymer and REvil [aka Sodinokibi] tend to get the bulk of media coverage, Nephilim is another family which has very quickly risen to prominence with multiple, damaging campaigns that threaten to publish victims' sensitive information in the event they fail to 'cooperate' with the attacker's demands," SentinelLabs notes.

Patch or Perish

The Nefilim gang isn't the first to try and target vulnerabilities in Citrix gateway devices, which were identified last December and patched in January. Upon their release, both the U.K.'s National Cyber Security Agency and CISA issued alerts to all Citrix users to install security updates to mitigate exploitable flaws.

"The NCSC and CISA have observed actors scanning for publicly known vulnerabilities in Citrix ... and [we] continue to investigate multiple instances of this vulnerability's exploitation," the agencies said in a joint alert issued in April.

In May, CISA and the NCSC issued another joint alert, warning that APT attackers were targeting the websites of multiple organizations - including in the healthcare sector and other organizations providing essential services - in search of known vulnerabilities in as-yet-unpatched software. "Actors are known to take advantage of Citrix vulnerability CVE-2019-19781 and vulnerabilities in virtual private network products from Pulse Secure, Fortinet and Palo Alto," the alert said (see: *Alert: APT Groups Targeting COVID-19 Researchers*).

U.S. and U.K. security and intelligence agencies issued a similar alert for users of Pulse Secure, Fortinet and Palo Alto products in October 2019, warning that months after patches had been released to fix easily exploitable flaws in remote tools, many organizations had yet to apply the security updates and that the flaws were being actively exploited by both crime gangs and nation-state attackers (see: *Unpatched VPN Servers Hit by Apparent Iranian APT Groups*).
