Nefilim Ransomware Targets Victims with $1 Billion Revenue

Trend Micro report takes a deep dive into one of the most successful threat groups in modern ransomware

DALLAS, June 8, 2021 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today released a case study of the Nefilim ransomware group, providing insight into the inner-workings of modern ransomware attacks. The report gives valuable insight into how ransomware groups have evolved, operate under the radar and how advanced threat detection and response platforms can help stop them.

The approach of modern ransomware families makes detection and response significantly more difficult for already stretched SOC and IT security teams. This matters not only to the bottom line and corporate reputation, but also the wellbeing of SOC teams themselves.

To read the report, Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them, please visit: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransomwares-double-extortion-tactics-and-how-to-protect-enterprises-against-them.

"Modern ransomware attacks are highly targeted, adaptable and stealthy – using proven approaches perfected by APT groups in the past. By stealing data and locking key systems, groups like Nefilim look to extort highly profitable global organizations," said Bob McArdle, director of cybercrime research for Trend Micro. "Our latest report is a must-read for anyone in the industry who wants to understand this fast-growing underground economy inside-out, and how solutions like Trend Micro Vision One can help them hit back."

Of the 16 ransomware groups studied from March 2020 to January 2021, Conti, Doppelpaymer, Egregor and REvil led the way in terms of number of victims exposed—and Cl0p had the most stolen data hosted online at 5TB.

However, with its ruthless focus on organizations posting more than$1 billion in revenue, Nefilim extorted the highest median revenue.

As the report reveals, a Nefilim attack typically involves the following stages:

- Initial access that exploits weak credentials on exposed RDP services or other externally facing HTTP services.
- Once inside, legitimate admin tools are used for lateral movement to find valuable systems for data theft and encryption.
- A "call home" system is set up with Cobalt Strike and protocols that can pass through firewalls, like HTTP, HTTPS and DNS.
- Bulletproof hosting services are used for C&C servers.
- Data is exfiltrated and published on TOR-protected websites later to extort victim. Nefilim published around 2TB of data last year.
- Ransomware payload is launched manually once enough data has been exfiltrated.

Trend Micro has previously warned of the widespread use of legitimate tools such as AdFind, Cobalt Strike, Mimikatz, Process Hacker, PsExec, and MegaSync, to help ransomware attackers achieve their end goal while staying hidden. This can make it challenging for different SOC analysts looking at event logs from different parts of the environment to see the bigger picture and spot attacks.

Trend Micro Vision One monitors and correlates suspicious behavior across multiple layers—endpoints, emails, servers, and cloud workloads—to ensure there's no hiding space for threat actors. This makes for faster incident response times, and teams can often stop attacks before they've had a chance to make a serious impact on the organization.

About Trend Micro
Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

https://newsroom.trendmicro.ca/2021-06-08-Nefilim-Ransomware-Targets-Victims-with-1-Billion-Revenue