Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them

To understand how modern ransomware actors use targeted techniques and discover which organizations are at the crosshairs of modern ransomware attacks, we present an in-depth case study of the Nefilim ransomware family. We also show how enterprises can formulate a defense strategy that can help prevent and mitigate the effects of modern ransomware attacks within the corporate network.

KEY FINDINGS

Nefilim gets into the network through weak credentials on exposed Remote Desktop Protocol (RDP) services and other externally facing HTTP services, and exploiting critical vulnerabilities on services such as a vulnerability in the Citrix Application Delivery Controller (CVE-2019-19781).

Nefilim is the evolved form of the Nemty ransomware. Based on the code similarities between Nemty and Nefilim, as well as similar business models, we believe that Nemty Revenue 3.1. was the first version of Nefilim. We believe that the actors behind both ransomware families are a group under the intrusion set we track as "Water Roc."

Modern ransomware actors, such as those behind Nefilim, perform lateral movement like advanced persistent threat (APT) actors. They perform lateral movement to try and find important systems, which are more likely to contain sensitive data to steal and encrypt, in the victim network.

Covert online collaboration among cybercriminal groups. Our investigation points to distinct cybercriminal groups that handle the various stages of modern ransomware attacks. This is the byproduct of a recent evolution in cybercriminal business operations: hackers are now partnering up with ransomware actors to monetize hacking-related breaches.

Double extortion replaces mere encryption techniques. To put further pressure on their victims, ransomware actors often threaten to leak sensitive data that has been stolen before deploying ransomware in their compromised networks.

HOW TO DEFEND CORPORATE NETWORKS AGAINST MODERN RANSOMWARE

The shift in the ransomware business model has allowed modern ransomware to become even more effective and destructive. Our research provides security recommendations — including the use of cross-layered detection and response tools and technologies — to help organizations formulate a strategy that will help prevent and mitigate the effects of modern ransomware attacks within the corporate network.

Read more about modern ransomware in our research paper at http://bit.ly/modernransomware.

TREND MICRO | research