

Michigan State University network breached in ransomware attack

By Ionut Ilascu

Published: 2020-05-28 · Archived: 2026-04-05 21:19:24 UTC

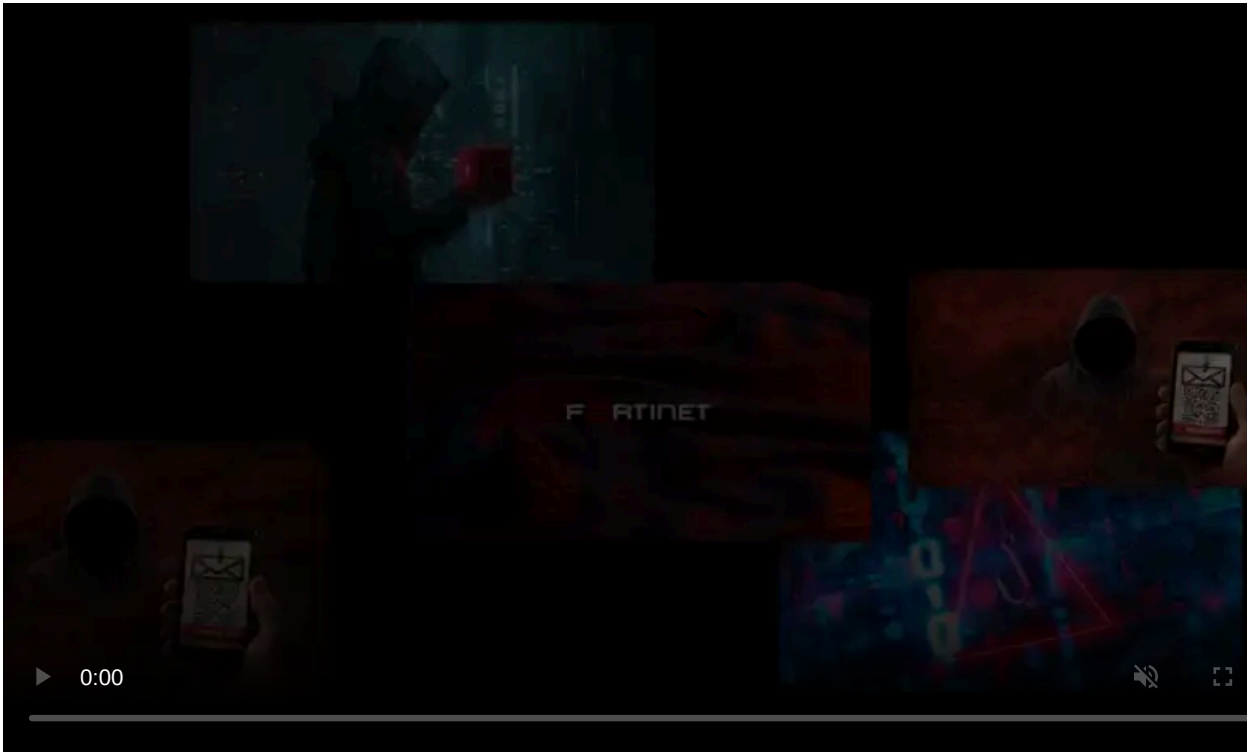


Michigan State University received a deadline to pay ransomware attackers under the threat that files stolen from the institution's network will be leaked to the public.

The demand is from Netwalker ransomware-as-a-service (RaaS) operators, a group that recently started to recruit skilled network intruders for their affiliate program.

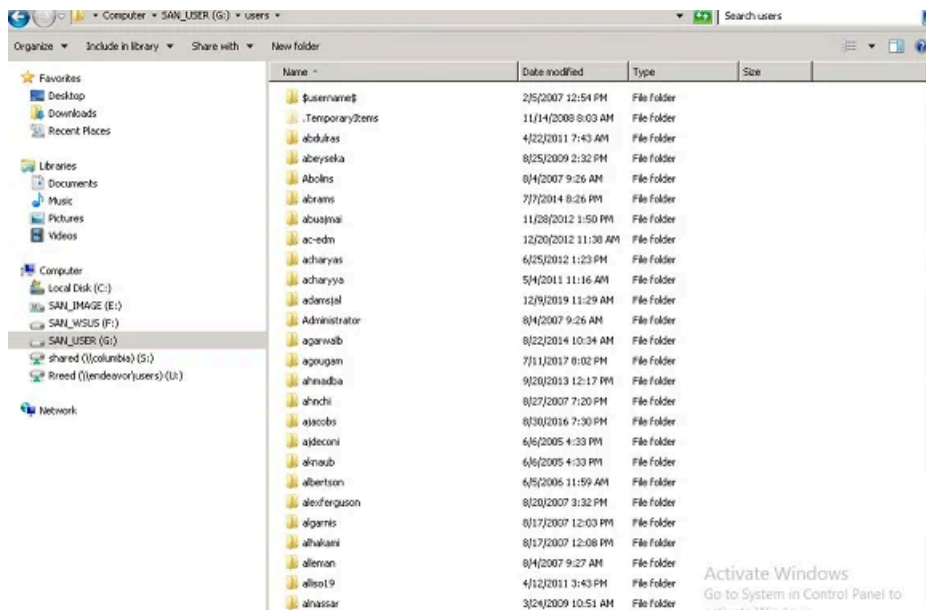
Proof of stolen data

A countdown timer on the attacker's website shows that the university has about six days to comply or "secret data" will become public.



Visit Advertiser website [GO TO PAGE](#)

The site set up by the Netwalker ransomware gang gives no details about the attack but they posted images with directories, a passport scan, and two financial documents allegedly stolen from the university's network.



BleepingComputer reached out to Michigan State University (MSU) for more details about the attack but received no reply at publishing time.

Information about how and when the attack happened, its impact on MSU, and the ransom demand remain unknown at this time.

Antivirus removers to disable defenses

Netwalker ransomware relies on multiple programs for remote access (Team Viewer, AnyDesk), files from public code repositories, and custom PowerShell scripts.

However, they also use at least three legitimate tools to uninstall security software on a compromised system.

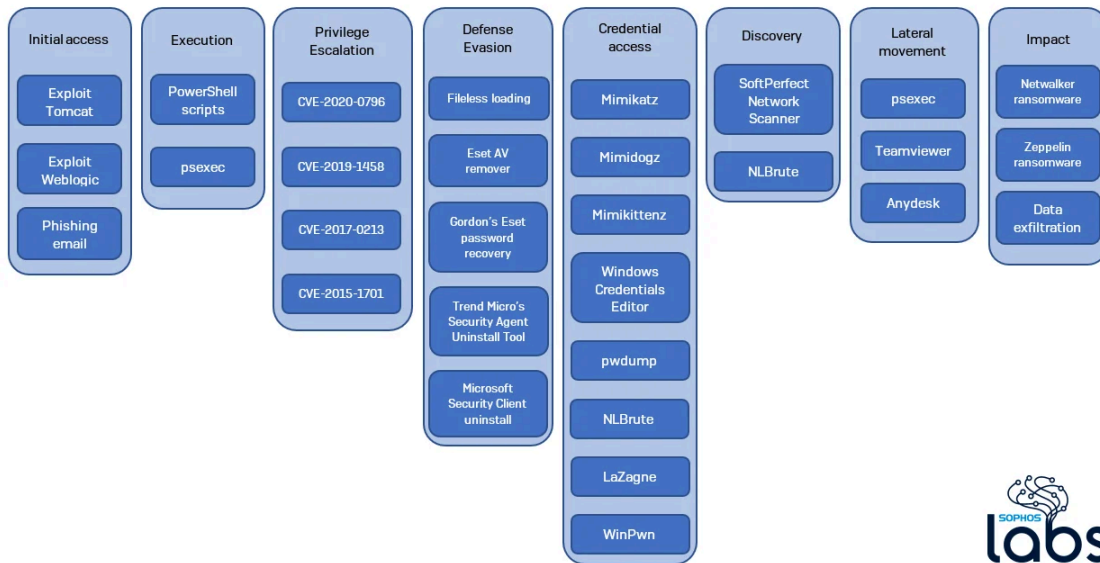
Researchers at Sophos security software and hardware company shared in a [report](#) yesterday that the threat actor also used legitimate removal tools for ESET antivirus, Trend Micro's Security Agent, and Microsoft Security Client that is part of Microsoft Security Essentials.

Apart from tools that enabled intrusion and lateral movement on the victim network, they discovered "individual samples of the Zeppelin Windows ransomware and the Smaug Linux ransomware as well."

In a trove of malicious files discovered while investigating a malware campaign from Netwalker, the researchers also found that the attacker also leveraged several vulnerabilities for privilege escalation.

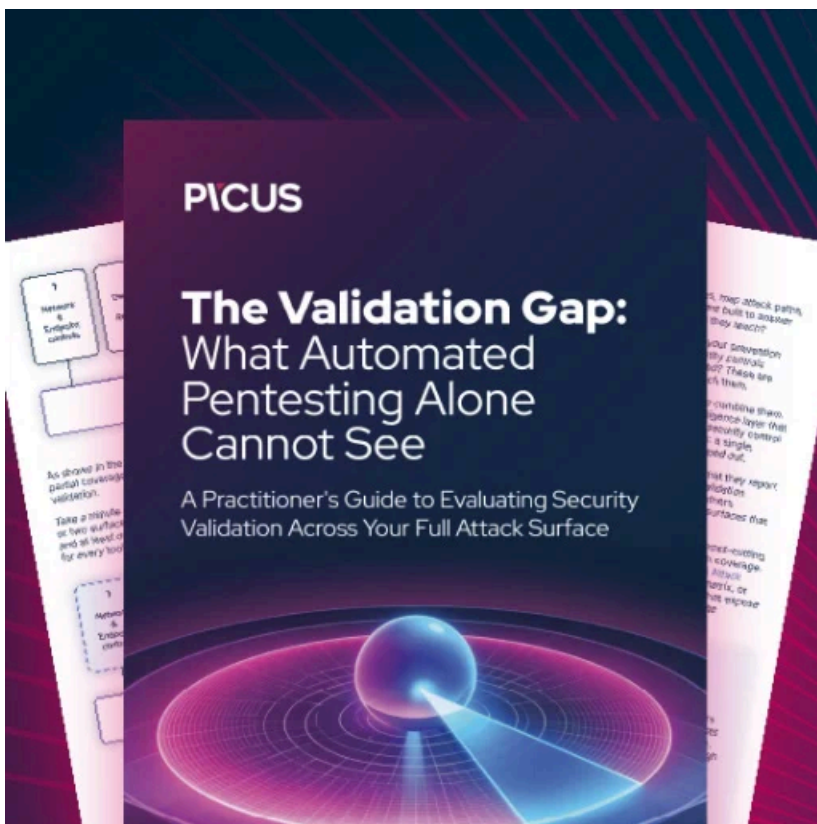
One of them is [CVE-2020-0796](#), for which there is proof-of-concept exploit code released for local privilege escalation. It can also be exploited for remote code execution, but the code for this is not currently available to the public.

Netwalker threat actor toolset on the ATT&CK matrix



Netwalker ransomware group advertised recently that they were looking for new collaborators with access to large enterprise networks. The move is meant to distance themselves from malware distribution through spam, which is a common method.

As an incentive, the group promised affiliates huge rewards, a cut between 80% and 84% from paid ransoms. Other ransomware operators typically offer up to 70% from the ransom money.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/michigan-state-university-network-breached-in-ransomware-attack/>