Michigan State University network breached in ransomware attack

bleepingcomputer.com/news/security/michigan-state-university-network-breached-in-ransomware-attack/

Ionut Ilascu

By
Ionut Ilascu

- May 28, 2020
- 01:02 PM
- 0

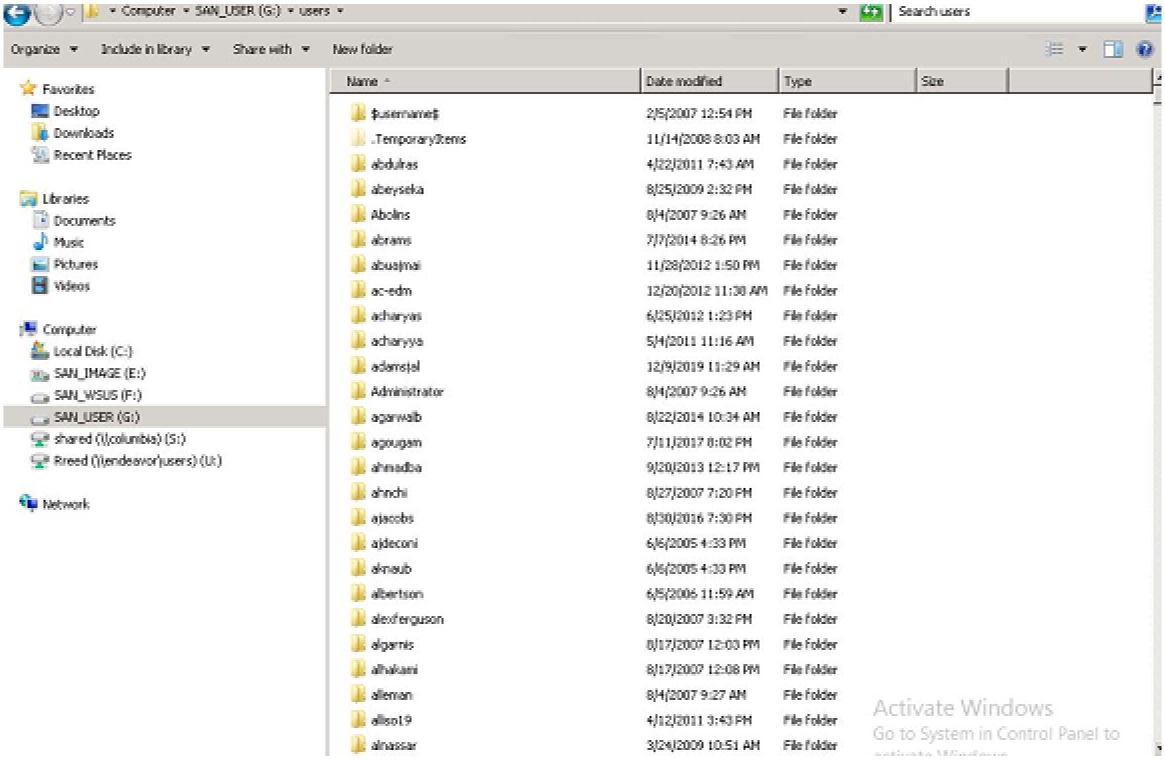
Michigan State University received a deadline to pay ransomware attackers under the threat that files stolen from the institution's network will be leaked to the public.

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.

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.



Name	Date modified	Type	Size
$username$	2/5/2007 12:54 PM	File folder	
.TemporaryItems	11/14/2008 8:03 AM	File folder	
abdulras	4/22/2011 7:43 AM	File folder	
abeyseka	8/25/2009 2:32 PM	File folder	
Abolins	8/4/2007 9:26 AM	File folder	
abrams	7/7/2014 8:26 PM	File folder	
abuajmai	11/28/2012 1:50 PM	File folder	
ac-edm	12/20/2012 11:38 AM	File folder	
acharyas	6/25/2012 1:23 PM	File folder	
acharyya	5/4/2011 11:16 AM	File folder	
adamsjal	12/9/2019 11:29 AM	File folder	
Administrator	8/4/2007 9:26 AM	File folder	
agarwalb	8/22/2014 10:34 AM	File folder	
agougam	7/11/2017 8:02 PM	File folder	
ahmadba	9/20/2013 12:17 PM	File folder	
ahnchi	8/27/2007 7:20 PM	File folder	
ajacobs	8/30/2016 7:30 PM	File folder	
ajdeconi	6/6/2005 4:33 PM	File folder	
aknaub	6/6/2005 4:33 PM	File folder	
albertson	6/5/2006 11:59 AM	File folder	
alexferguson	8/20/2007 3:32 PM	File folder	
algarnis	8/17/2007 12:03 PM	File folder	
alhakami	8/17/2007 12:08 PM	File folder	
alleman	8/4/2007 9:27 AM	File folder	
allso19	4/12/2011 3:43 PM	File folder	
alnassar	3/24/2009 10:51 AM	File folder	

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.

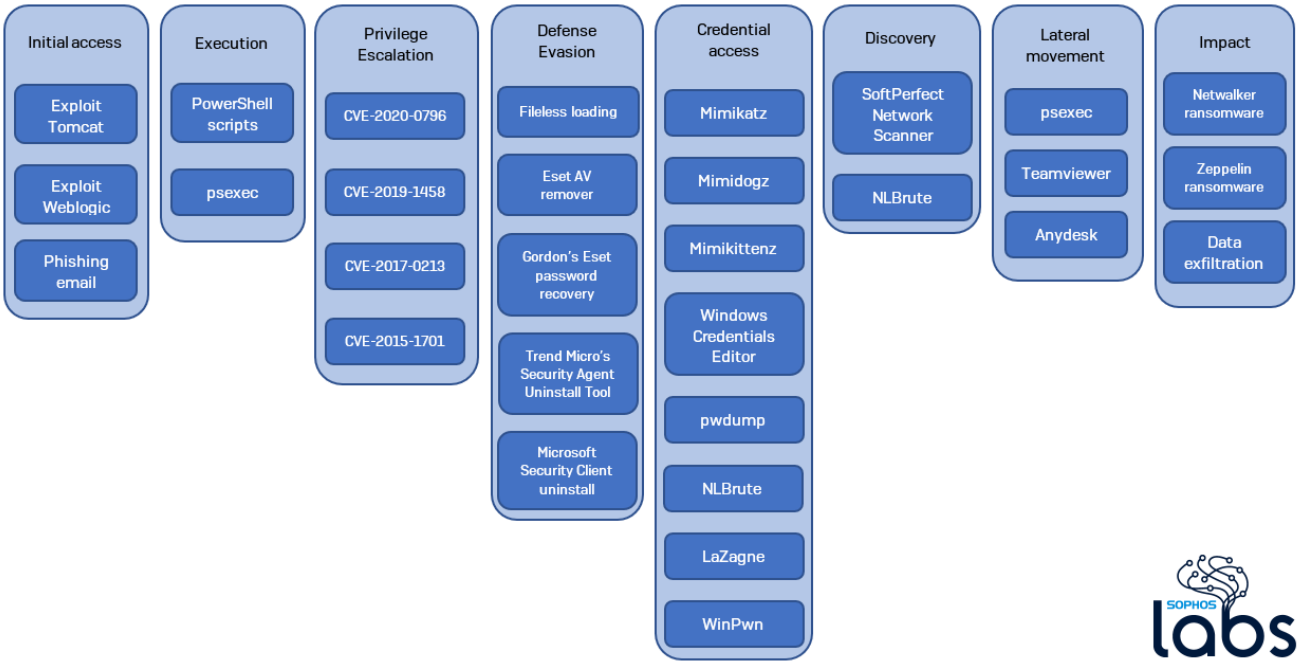
Researchers at Sophos security software and hardware company shared in a report yesterday that the threat actor also used legitimate removal tools for ESET antivirus, Trend Micro's Security Agent, and Microsoft Security Client that is part of Microsoft Security Essentials.

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



Initial access	Execution	Privilege Escalation	Defense Evasion	Credential access	Discovery	Lateral movement	Impact
Exploit Tomcat	PowerShell scripts	CVE-2020-0796	Fileless loading	Mimikatz	SoftPerfect Network Scanner	psexec	Netwalker ransomware
Exploit Weblogic	psexec	CVE-2019-1458	Eset AV remover	Mimidogz	NLBrute	Teamviewer	Zeppelin ransomware
Phishing email		CVE-2017-0213	Gordon's Eset password recovery	Mimikittenz		Anydesk	Data exfiltration
		CVE-2015-1701	Trend Micro's Security Agent Uninstall Tool	Windows Credentials Editor			
			Microsoft Security Client uninstall	pwdump			
				NLBrute			
				LaZagne			
				WinPwn			

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.

Related Articles:

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.