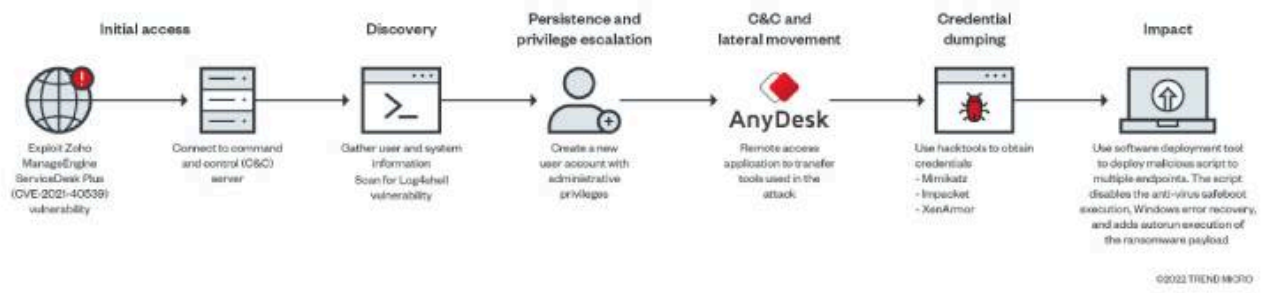
AvosLocker Ransomware Variant Using New Trick to Disable Antivirus Protection

By The Hacker News

Published: 2022-05-03 · Archived: 2026-04-05 15:48:46 UTC




```
reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\EPProtectedService /f &
reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\epredline /f &
reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\CylanceSvc /f &
reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\SAVService /f &
reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\klnagent /f &
reg delete "HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\Sophos File Scanner Service" /f &
reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\SntpService /f &
reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\EPSecurityService /f &
reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\EPUpdateService /f &
reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\EPIntegrationService /f &
reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\TmCCSF /f &
reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\TmWSCSvc /f &
reg delete HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\McAfeeFramework /f &
```

Cybersecurity researchers have disclosed a new variant of the AvosLocker ransomware that disables antivirus solutions to evade detection after breaching target networks by taking advantage of unpatched security flaws.

"This is the first sample we observed from the U.S. with the capability to disable a defense solution using a legitimate Avast Anti-Rootkit Driver file (asWarPot.sys)," Trend Micro researchers, Christoper Ordonez and Alvin Nieto, said in a Monday analysis.

"In addition, the ransomware is also capable of scanning multiple endpoints for the Log4j vulnerability (Log4shell) using Nmap NSE script."

AvosLocker, one of the newer ransomware families to fill the vacuum left by REvil, has been linked to a number of attacks that targeted critical infrastructure in the U.S., including financial services and government facilities.

A ransomware-as-a-service (RaaS) affiliate-based group first spotted in July 2021, AvosLocker goes beyond double extortion by auctioning data stolen from victims should the targeted entities refuse to pay the ransom.

Other targeted victims claimed by the ransomware cartel are said to be located in Syria, Saudi Arabia, Germany, Spain, Belgium, Turkey, the U.A.E., the U.K., Canada, China, and Taiwan, according to an advisory released by the U.S. Federal Bureau of Investigation (FBI) in March 2022.

Telemetry data gathered by Trend Micro shows that the food and beverage sector was the most hit industry between July 1, 2021 and February 28, 2022, followed by technology, finance, telecom, and media verticals.

The entry point for the attack is believed to have been facilitated by leveraging an exploit for a remote code execution flaw in Zoho's ManageEngine ADSelfService Plus software (CVE-2021-40539) to run an HTML application (HTA) hosted on a remote server.

"The HTA executed an obfuscated PowerShell script that contains a shellcode, capable of connecting back to the [command-and-control] server to execute arbitrary commands," the researchers explained.

This includes retrieving an ASPX web shell from the server as well as an installer for the AnyDesk remote desktop software, the latter of which is used to deploy additional tools to scan the local network, terminate security software, and drop the ransomware payload.

Some of the components copied to the infected endpoint are a Nmap script to scan the network for the Log4Shell remote code execution flaw (CVE-2021-44228) and a mass deployment tool called PDQ to deliver a malicious batch script to multiple endpoints.

The batch script, for its part, is equipped with a wide range of capabilities that allows it to disable Windows Update, Windows Defender, and Windows Error Recovery, in addition to preventing safe boot execution of security products, creating a new admin account, and launching the ransomware binary.

Also used is aswArPot.sys, a legitimate Avast anti-rootkit driver, to kill processes associated with different security solutions by weaponizing a now-fixed vulnerability in the driver the Czech company resolved in June 2021.

"The decision to choose the specific rootkit driver file is for its capability to execute in kernel mode (therefore operating at a high privilege)," the researchers pointed out. "This variant is also capable of modifying other details of the installed security solutions, such as disabling the legal notice."

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
