REvil ransomware now changes password to auto-login in Safe Mode

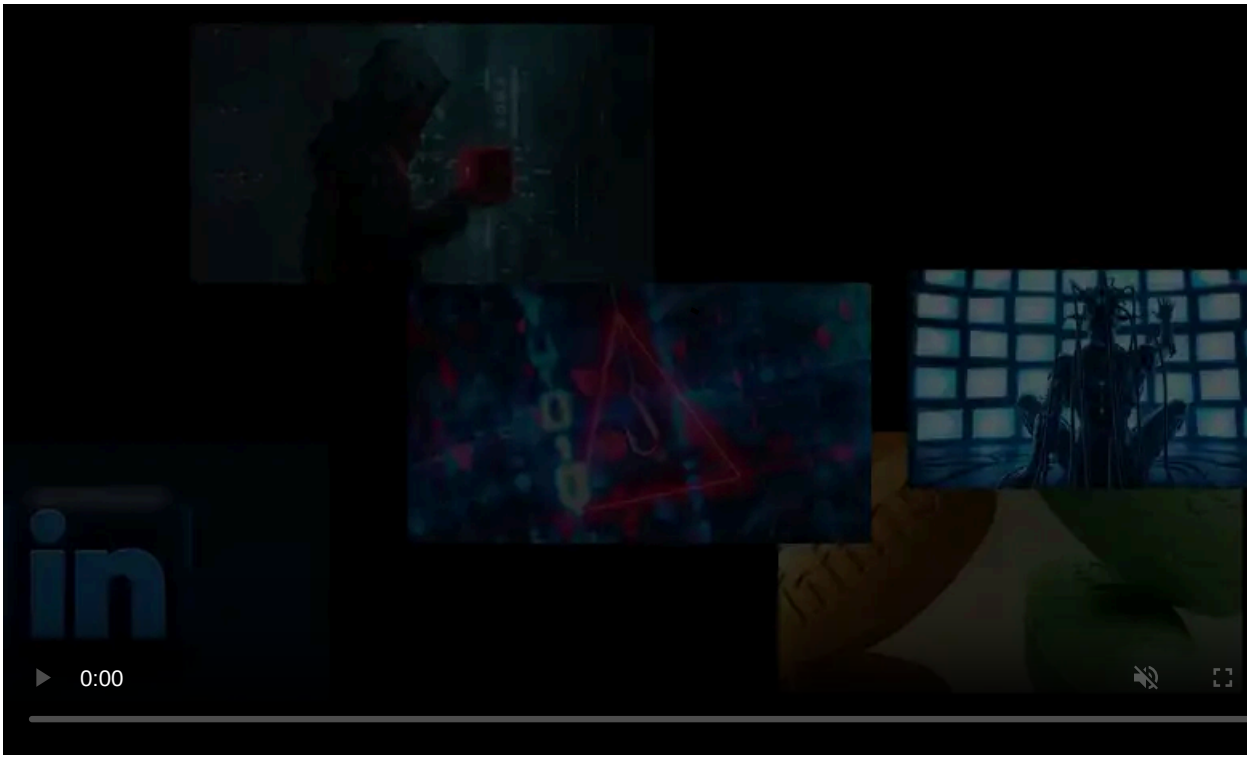
By Lawrence Abrams

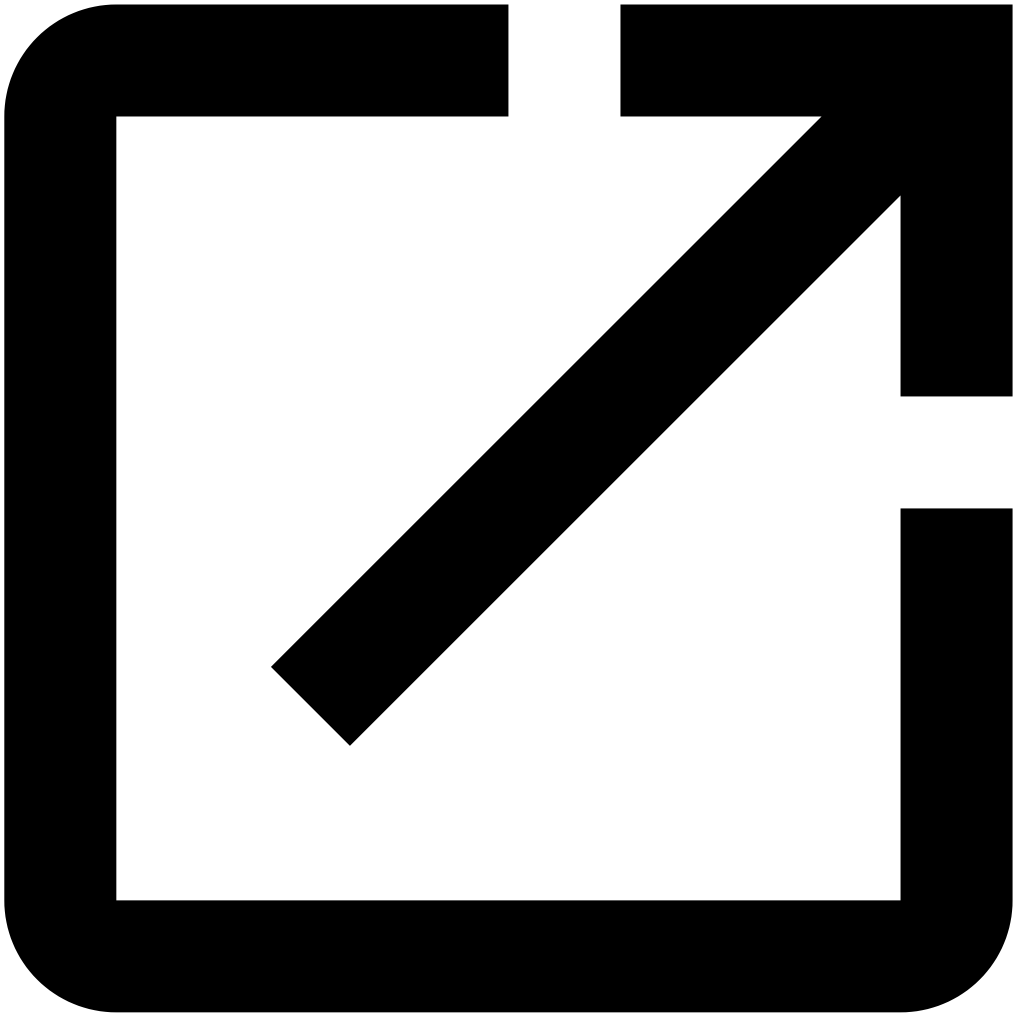
Published: 2021-04-07 · Archived: 2026-04-05 16:37:57 UTC

A recent change to the REvil ransomware allows the threat actors to automate file encryption via Safe Mode after changing Windows passwords.

In March, we reported on a new Windows Safe Mode encryption mode added to the REvil/Sodinokibi ransomware. This mode can be enabled using the -smode command-line argument, which would reboot the device into Safe Mode, where it would perform the encryption of files.

It is believed that this mode was added as a way to evade detection by security software and to shut down backup software, database servers, or mail servers to have greater success when encrypting files.


0:00



However, at the time of our reporting, the ransomware required someone to manually login to Windows Safe mode before the encryption would start, which could raise red flags.

New version automatically logs Windows into Safe Mode

At the end of March, a new sample of the REvil ransomware was discovered by security researcher R3MRUM that refines the new Safe Mode encryption method by changing the logged-on user's password and configuring Windows to automatically login on reboot.

With this new sample, when the -smode argument is used, the ransomware will change the user's password to '**DTrump4ever**.'

The ransomware then configures the following Registry values so that Windows will automatically login with the new account information.

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"AutoAdminLogon"="1"
"DefaultUserName"="[account_name]"
"DefaultPassword"="DTrump4ever"

While it unknown if new samples of the REvil ransomware encryptor continue to use the 'DTrump4ever' password, at least two samples uploaded to VirusTotal in the past two days continue to do so.

These changes illustrate how ransomware gangs continuously evolve their tactics to successfully encrypt victims' devices and force a ransom payment.

REvil also recently warned that they would perform DDoS attacks on victims and email victims' business partners about stolen data if a ransom is not paid.

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.
