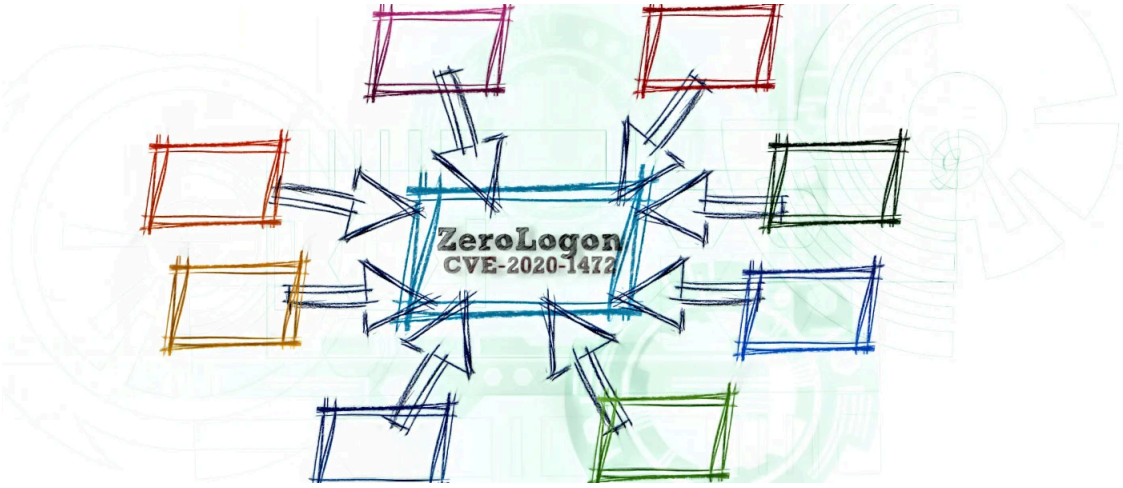
Ransomware gang now using critical Windows flaw in attacks

By Ionut Ilascu

Published: 2020-10-09 · Archived: 2026-04-05 12:36:27 UTC

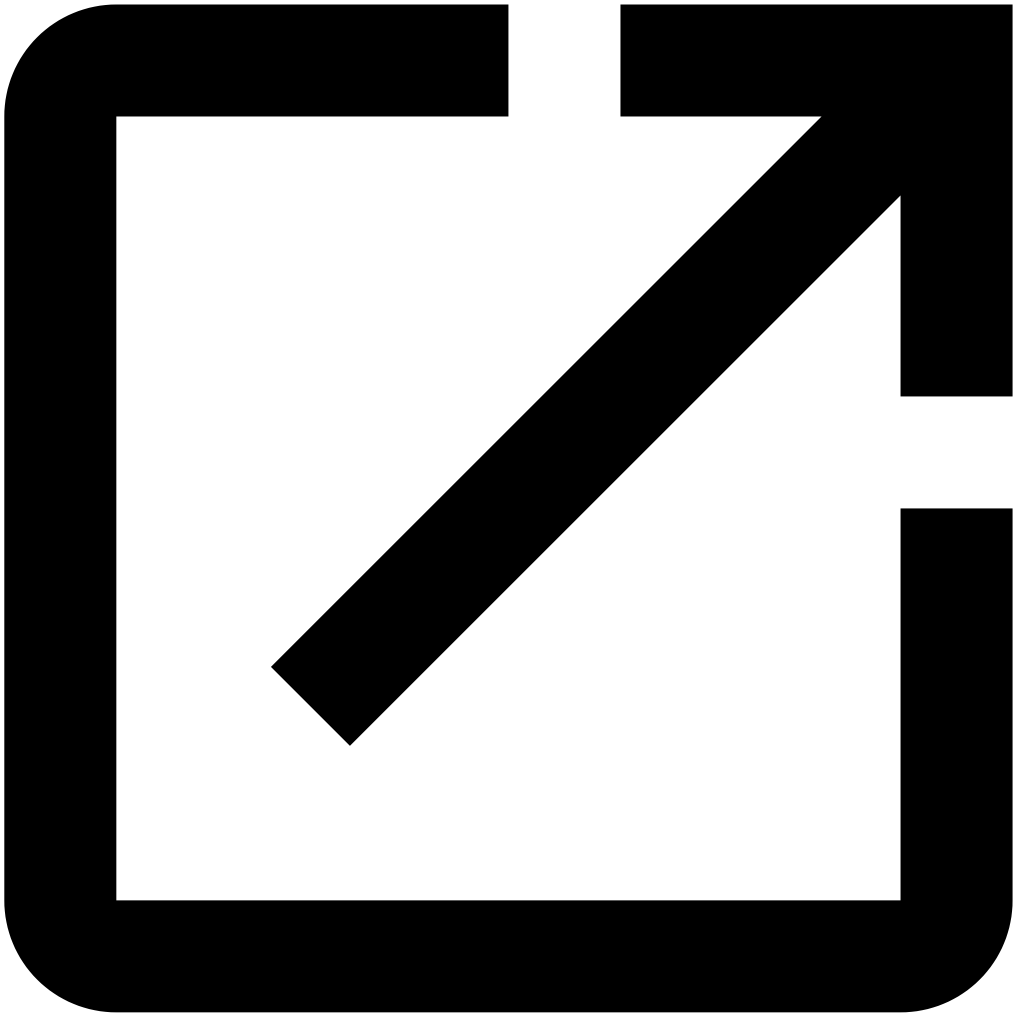


Microsoft is warning that cybercriminals have started to incorporate exploit code for the ZeroLogon vulnerability in their attacks. The alert comes after the company noticed ongoing attacks from cyber-espionage group MuddyWater (SeedWorm) in the second half of September.

This time, the threat actor is TA505, an adversary who is indiscriminate about the victims it attacks, with a history starting with the distribution of Dridex banking trojan in 2014.

Over the years, the actor has been in attacks delivering a wide variety of malware, from backdoors to ransomware.


DIE LINKE.
0:00



Recently, intrusions from this group are followed by the deployment of Clop ransomware, as in the attack on Maastricht University last year that resulted in paying a 30 bitcoin (about $220,000) ransom.

Fake updates and legit tools

Microsoft says that TA505, which it tracks as Chimborazo, deployed a campaign with fake software updates that connect to the threat actor's command and control (C2) infrastructure.

The purpose of the malicious updates is to give hackers increased privileges (User Account Control bypass) on the target system and run malicious scripts.

For the second part, TA505 uses Windows Script Host (WScript.Exe), which allows executing scripts in various programming languages, including VBScript, Python, Ruby, PHP, JavaScript, and Perl.

Microsoft says that the attackers compile a version of the Mimikatz post-exploitation tool using the Microsoft Build Engine (MSBuild.Exe)n for building applications.

The version of Mimikatz obtained this way includes exploit code for the ZeroLogon vulnerability (CVE-2020-1472). Over the past month, numerous researchers released proof–of–concept exploits for this flaw.

What Microsoft described in a short thread is a classic domain takeover attack, where ZeroLogon is a perfect fit. It offers direct access to the domain controller, so the attacker no longer needs to spend time getting the admin credentials.

With TA505 involved in big-money ransomware business, organizations should prioritize applying security patches for this vulnerability as attacks similar to what Microsoft described are likely to occur with increased frequency.

ZeroLogon details available

Discovered by Tom Tervoort of Secura, ZeroLogon allows intruders on a domain network to increase permissions to administrator level without needing to authenticate.

Tervoort found that he could force the connection to a domain controller through the Netlogon Remote Protocol in an unencrypted state (non-secure RPC communication).

Next, by leveraging a flaw in the Netlogon crypto algorithm, it is possible to spoof a domain administrator login. A technical write-up is available from Secura.

Microsoft addressed this vulnerability partially for now, by preventing Windows Active Domain controller communication over non-secure RPC. This update is available since August 11.

On February 9, though, a new update will enforce the same secure communication to all devices on the network.

Warnings released

Network admins received repeated warnings about the severity of the ZeroLogon vulnerability (maximum critical score 10/10) and urged to apply the current patch.

With exploit code that (domain admin privilege obtained in seconds) released since mid-September, threat actors moved quickly to incorporating it in their attacks.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on September 18 required the Federal Civilian Executive Branch to treat fixing the flaw as an emergency.

Microsoft first sounded the alarm on September 23, when it saw ZeroLogon actively exploited in attacks. Next came the alert about MuddyWater leveraging the exploit.

Now it's cybercriminals wielding it, a clear sign that ZeroLogon is on the way of being adopted by a wide range of threat groups targeting organizations in both the public and private sectors.
