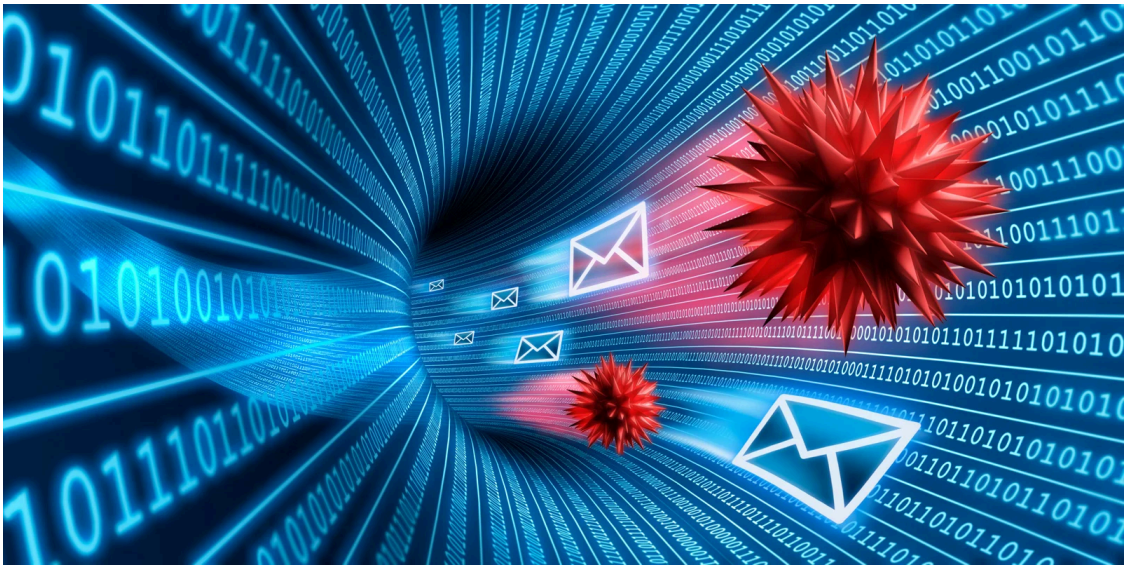
New Latrodectus malware attacks use Microsoft, Cloudflare themes

By Lawrence Abrams

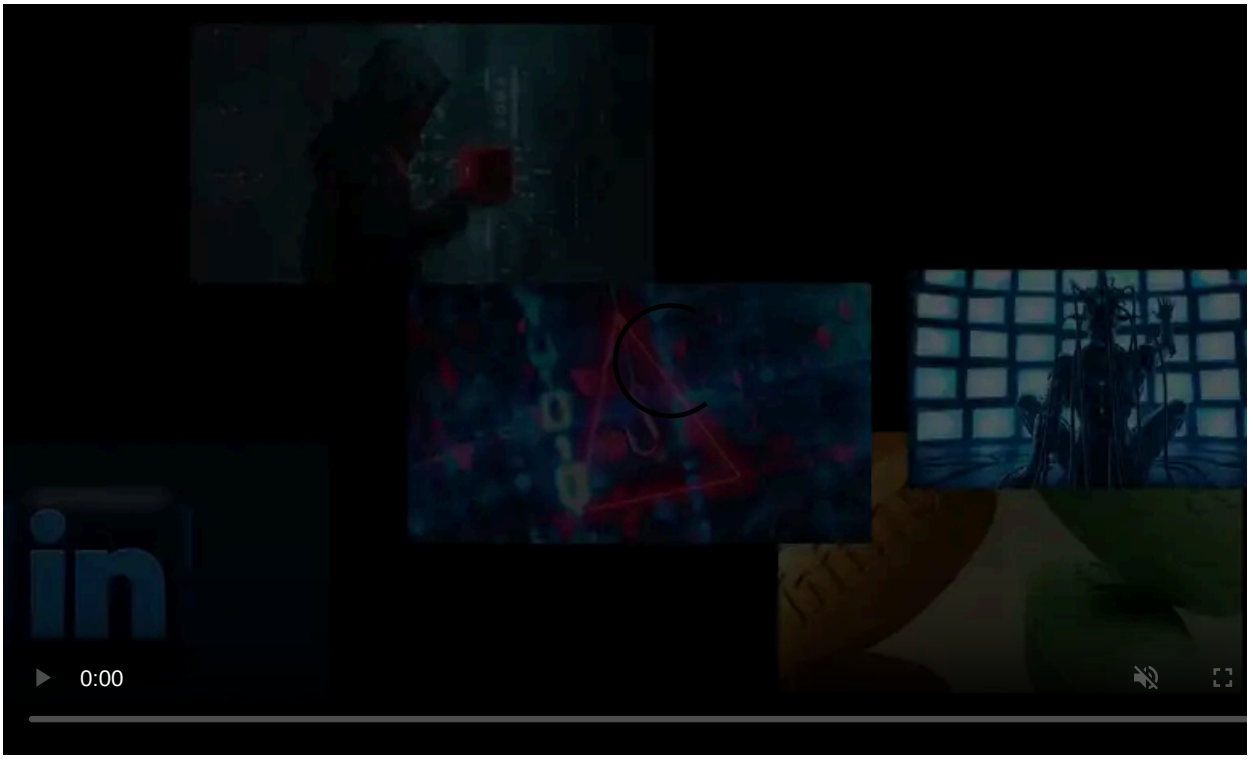
Published: 2024-04-30 · Archived: 2026-04-05 18:32:54 UTC

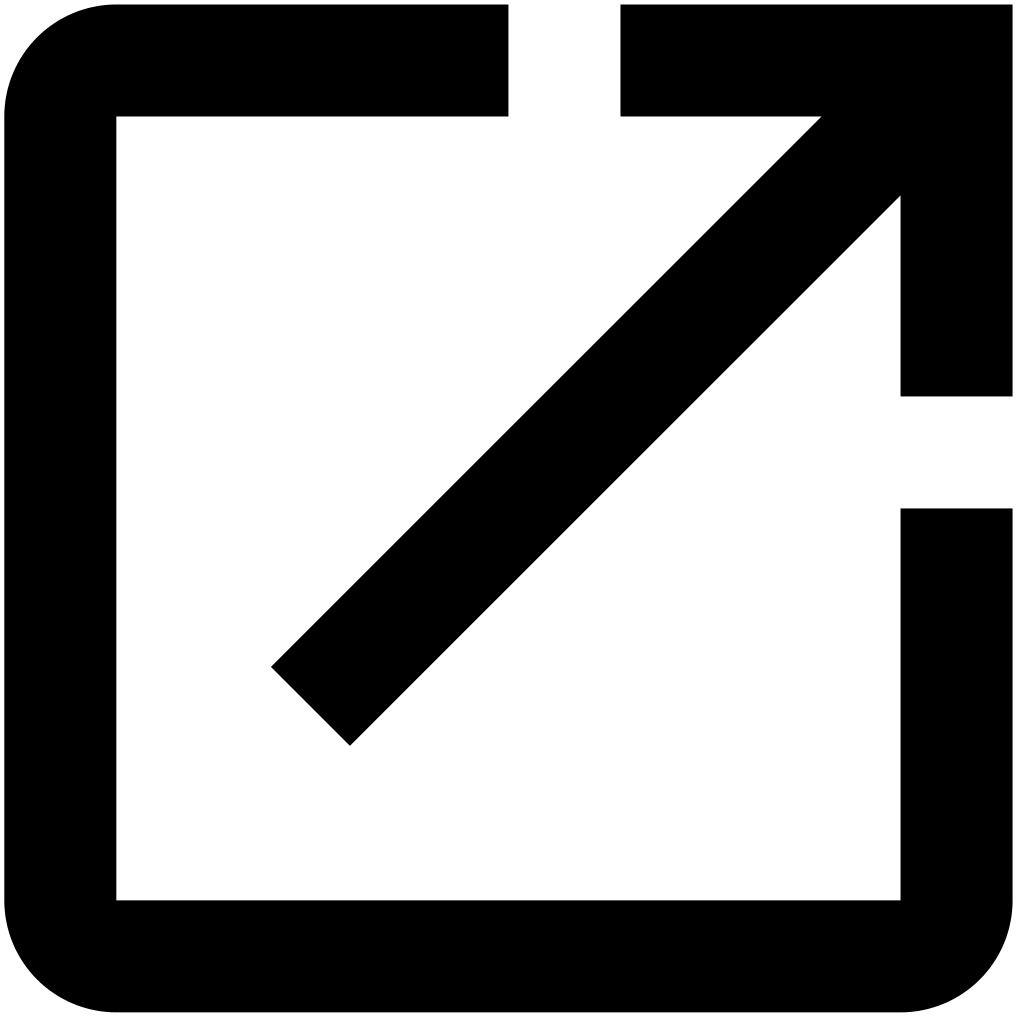


Latrodectus malware is now being distributed in phishing campaigns using Microsoft Azure and Cloudflare lures to appear legitimate while making it harder for email security platforms to detect the emails as malicious.

Latrodectus (aka Unidentified 111 and IceNova) is an increasingly distributed Windows malware downloader first discovered by Walmart's security team and later analyzed by ProofPoint and Team Cymru that acts as a backdoor, downloading additional EXE and DLL payloads or executing commands.

Based on the distribution and infrastructure, researchers have linked the malware to the developers of the widely-distributed IcedID modular malware loader.


0:00



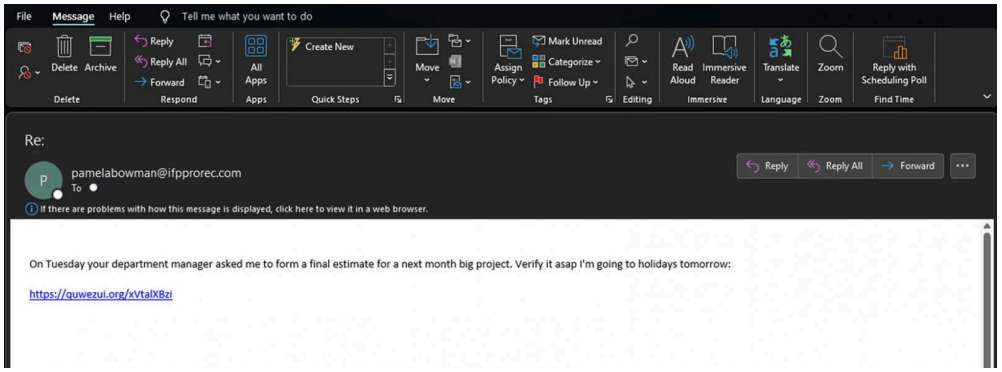
While it is not known at this time if they plan on phasing out IcedID in favor of Latrodectus, the newer malware is increasingly being used in phishing campaigns and contact form spam to gain initial access to corporate networks.

Security researcher ProxyLife and the Cryptolaemus group have been chronicling Latrodectus's use of various PDF lures and themes, with the latest campaign utilizing a fake Cloudflare captcha to evade security software.

Starts with an email

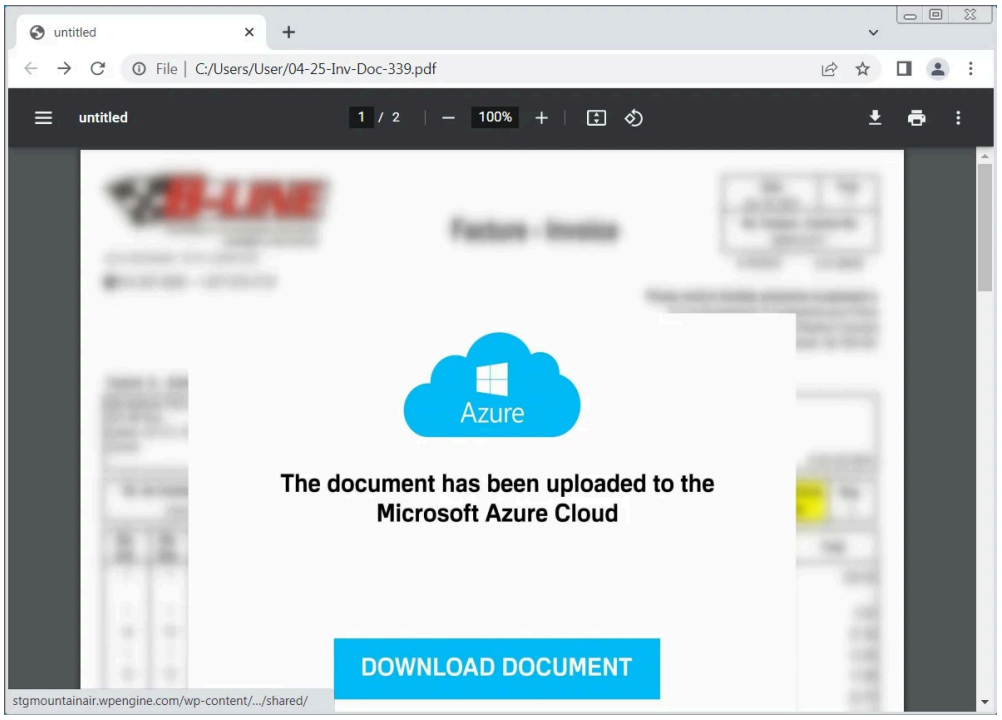
Latrodectus is currently being distributed through reply-chain phishing emails, which is when threat actors use stolen email exchanges and then reply to them with links to malware or malicious attachments.

ProxyLife told BleepingComputer that this campaign uses either PDF attachments or embedded URLs to start an attack chain that eventually leads to installing the Latrodectus malware.



Latrodectus phishing email
Source: BleepingComputer

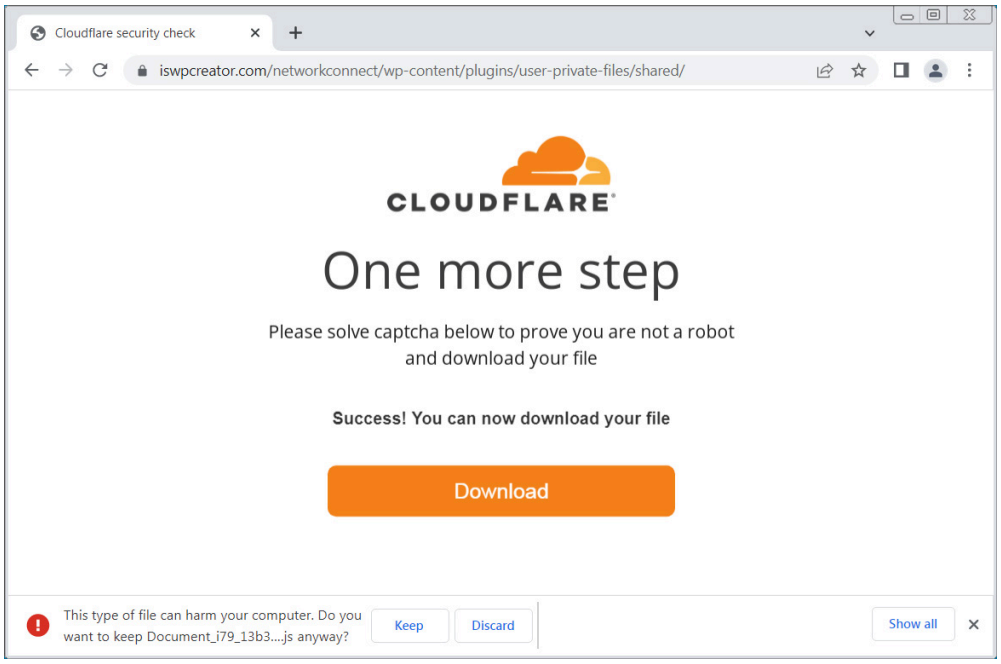
The PDFs will use generic names like '04-25-Inv-Doc-339.pdf' and pretend to be a document hosted in Microsoft Azure cloud, which must first be downloaded to be viewed.



PDF document pretending to be hosted in Microsoft Azure Cloud
Source: BleepingComputer

Clicking on the 'Download Document' button will bring users to a fake 'Cloudflare security check' that asks you to solve an easy math question. This captcha is likely to prevent email security scanners and sandboxes from easily following the attack chain and only delivering the payload to a legitimate user.

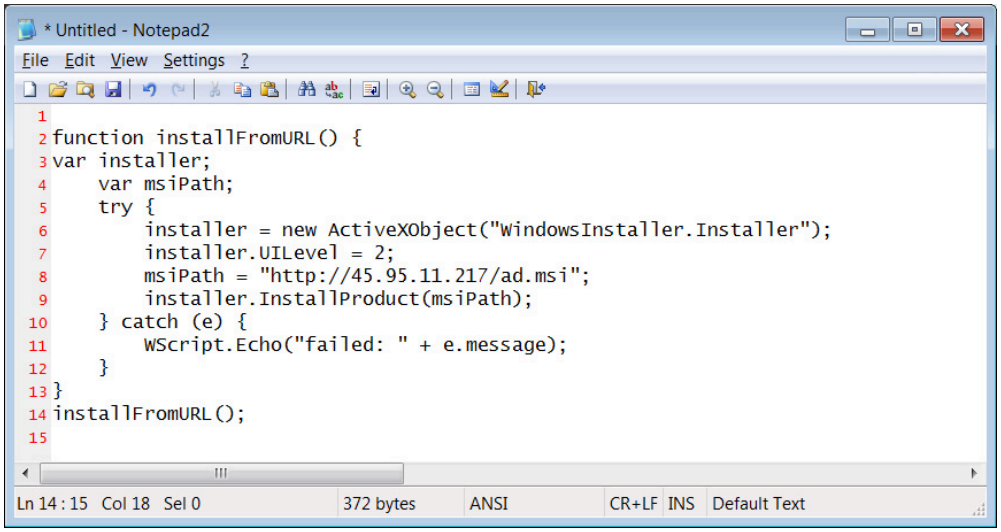
When the correct answer is entered into the field, the fake Cloudflare captcha will automatically download a JavaScript file pretending to be a document named similar to "Document_i79_13b364058-83054409r0449-8089z4.js".



Solving a fake Cloudflare captcha to download payload

Source: BleepingComputer

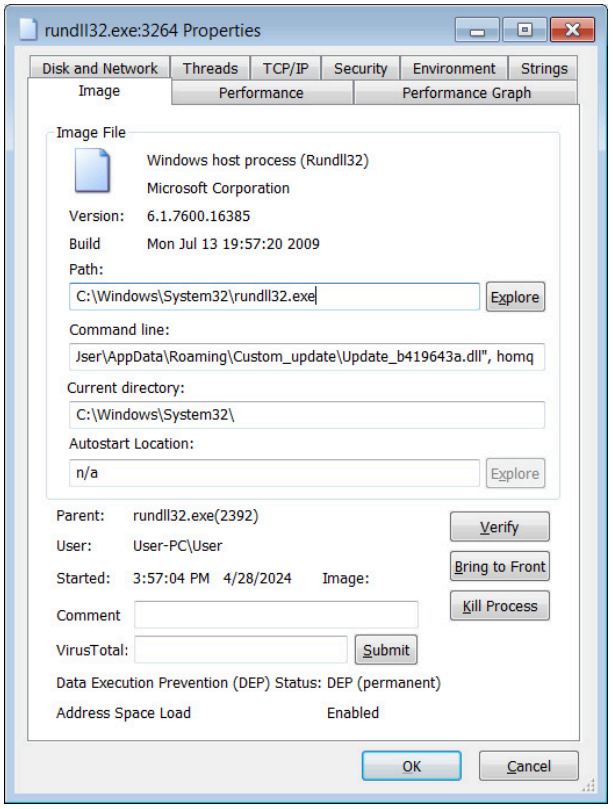
The downloaded JavaScript script is heavily obfuscated with comments that include a hidden function that extracts text from comments that start with '////' and then executes the script to download an MSI from a hardcoded URL, as shown in the deobfuscated script below.



Deobfuscated script that downloads MSI file

Source: BleepingComputer

When the MSI file is installed, it drops a DLL in the %AppData%\Custom_update folder named Update _b419643a.dll, which is then launched by rundll32.exe. The file names are likely random per installation.



RunDLL32 used to launch Latrodectus DLL

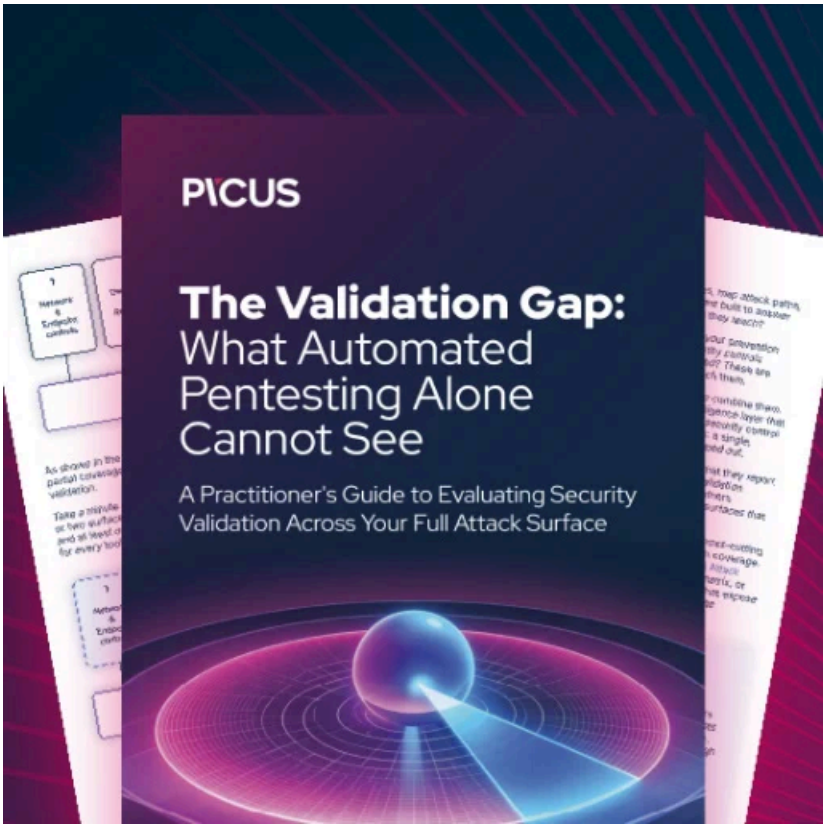
Source: BleepingComputer

This DLL is the Latrodectus malware, which will now quietly run in the background while waiting for payloads to install or commands to execute.

As Latrodectus malware infections are used to drop other malware and for initial access to corporate networks, they can lead to devastating attacks.

At this time, the malware has been observed dropping the Lumma information-stealer and Danabot. However, since Latrodectus is linked to IcedID, these attacks may lead to a wider range of malware in the future such as Cobalt Strike and we might also see partnerships with ransomware gangs.

Therefore, if a device becomes infected with Latrodectus, it is critical to take the system offline as soon as possible and evaluate the network for unusual behavior.



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/new-latrodectus-malware-attacks-use-microsoft-cloudflare-themes/