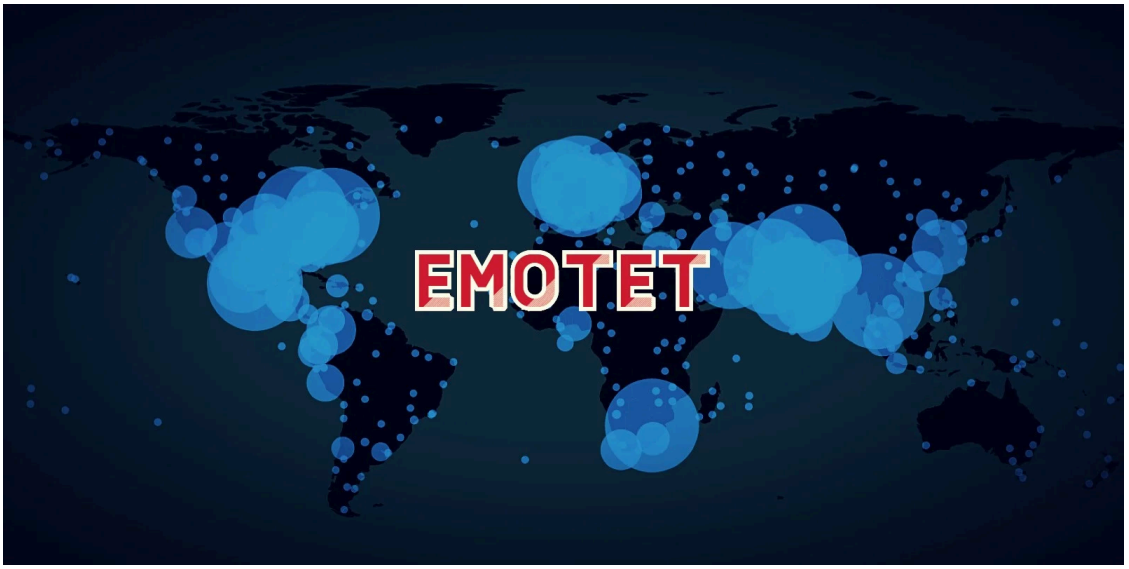
Emotet now spreads via fake Adobe Windows App Installer packages

By Lawrence Abrams

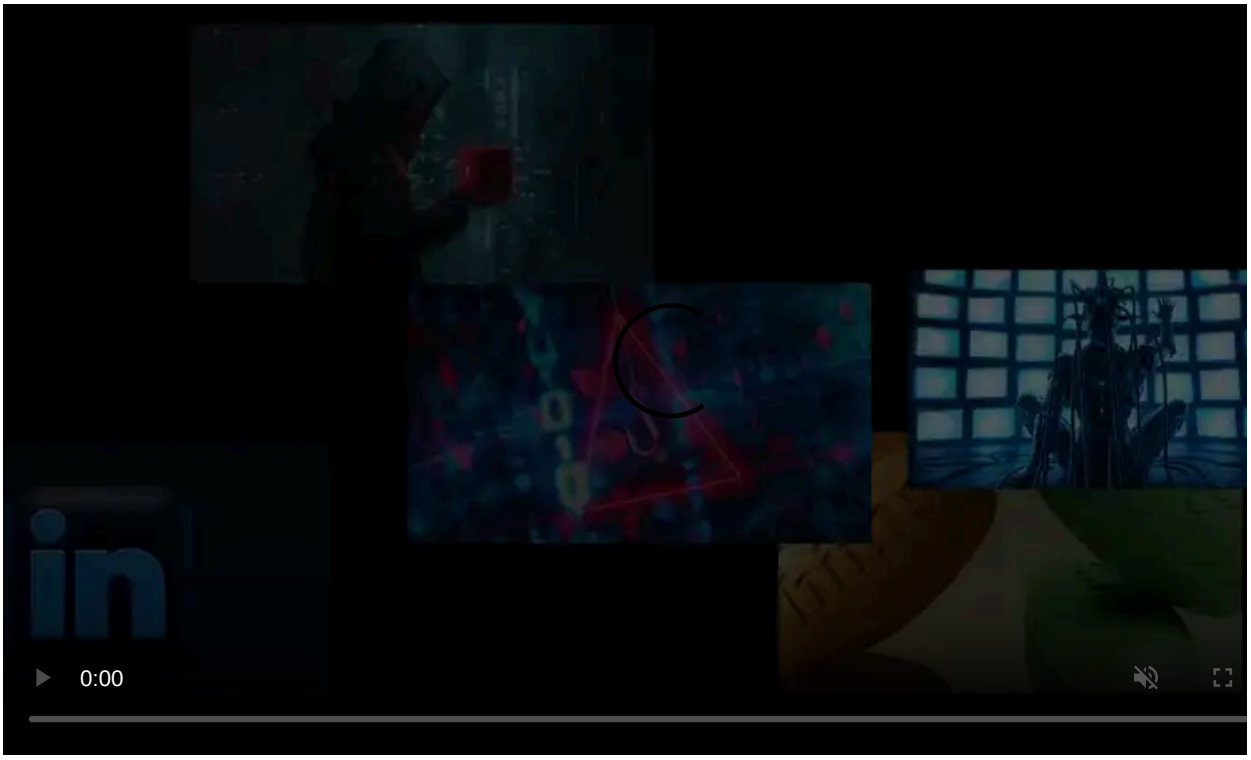
Published: 2021-12-01 · Archived: 2026-04-05 16:52:12 UTC

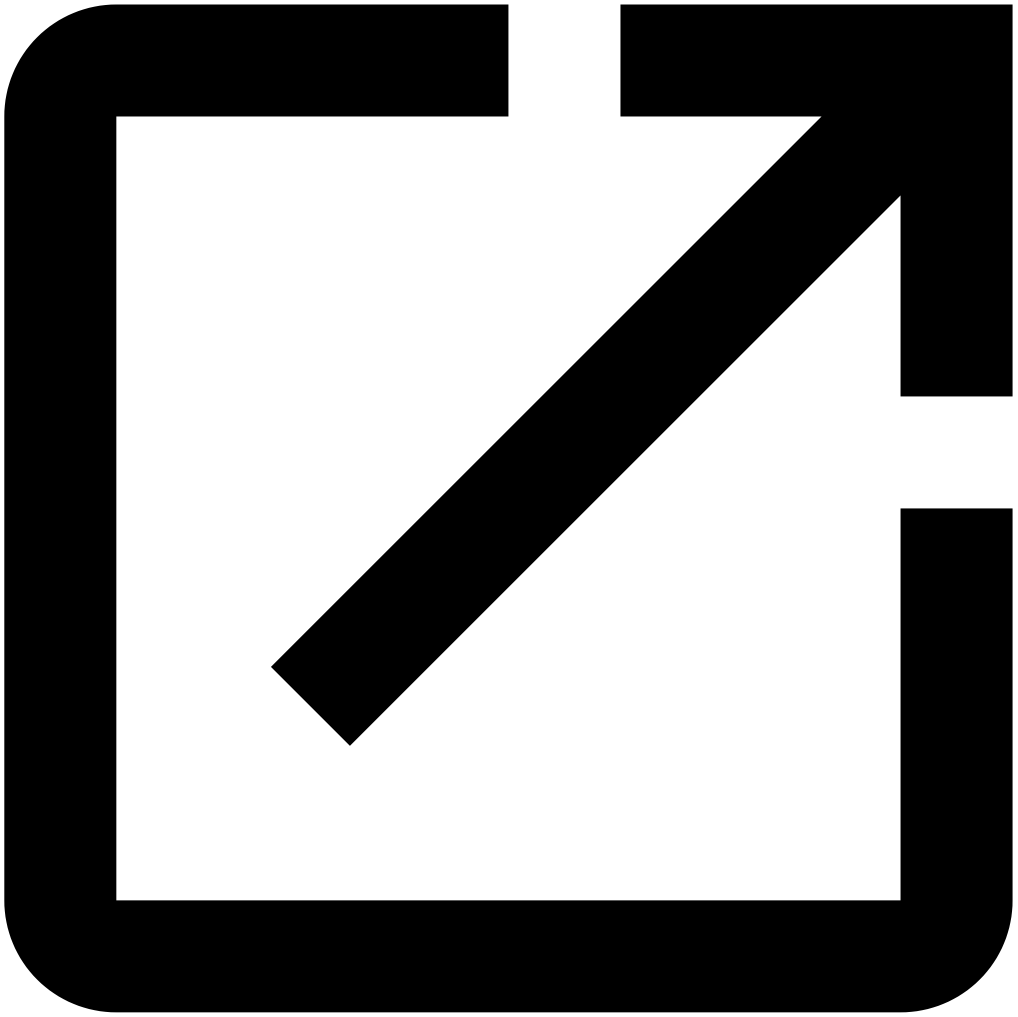


The Emotet malware is now distributed through malicious Windows App Installer packages that pretend to be Adobe PDF software.

Emotet is a notorious malware infection that spreads through phishing emails and malicious attachments. Once installed, it will steal victims' emails for other spam campaigns and deploy malware, such as TrickBot and Qbot, which commonly lead to ransomware attacks.

The threat actors behind Emotet are now infecting systems by installing malicious packages using a built-in feature of Windows 10 and Windows 11 called App Installer.


0:00



Researchers previously saw this same method being used to distribute the BazarLoader malware where it installed malicious packages hosted on Microsoft Azure.

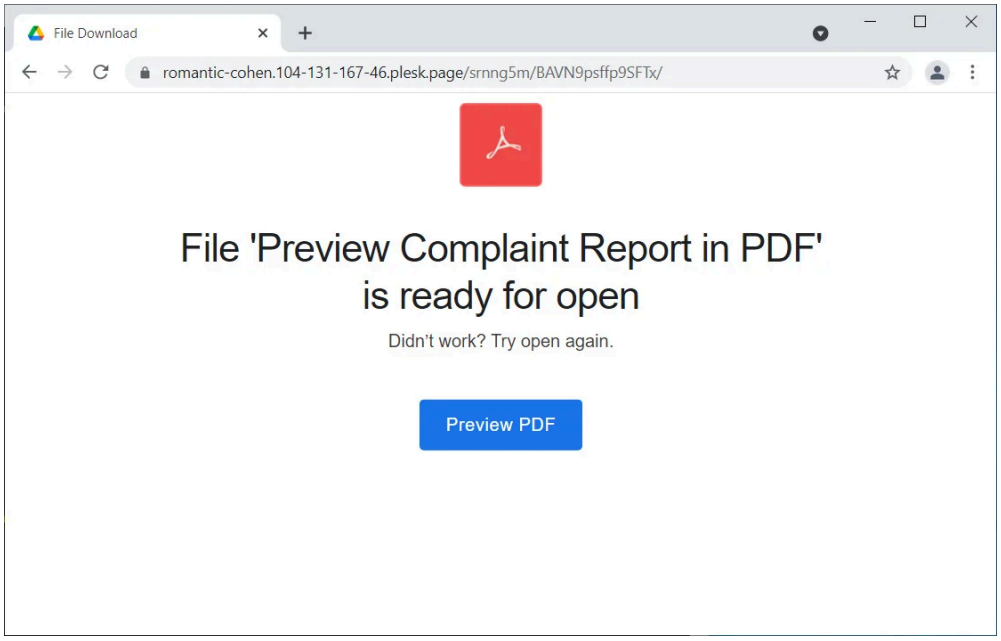
Abusing Windows App Installer

Using URLs and email samples shared by the Emotet tracking group Cryptolaemus, BleepingComputer demonstrates below the attack flow of the new phishing email campaign.

This new Emotet campaign starts with stolen reply-chain emails that appear as a reply to an existing conversation.

These replies simply tell the recipient to "Please see attached" and contain a link to an alleged PDF related to the email conversation.

When the link is clicked, the user will be brought to a fake Google Drive page that prompts them to click a button to preview the PDF document.

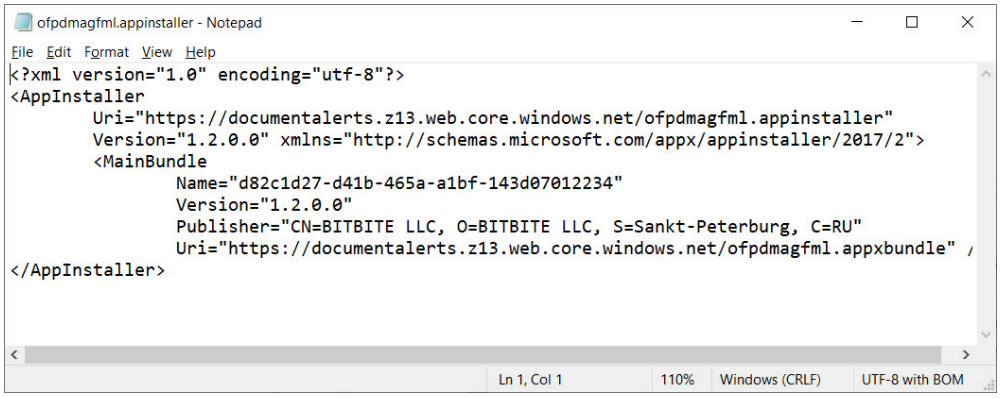


Phishing landing page prompting you to preview the PDF
Source: BleepingComputer

This 'Preview PDF' button is an ms-appinstaller URL that attempts to open an appinstaller file hosted on Microsoft Azure using URLs at *.web.core.windows.net.

For example, the above link would open an appinstaller package at the following example URL: ms-appinstaller:?source=https://xxx.z13.web.core.windows.net/abcdefghi.appinstaller.

An appinstaller file is simply an XML file containing information about the signed publisher and the URL to the appbundle that will be installed.

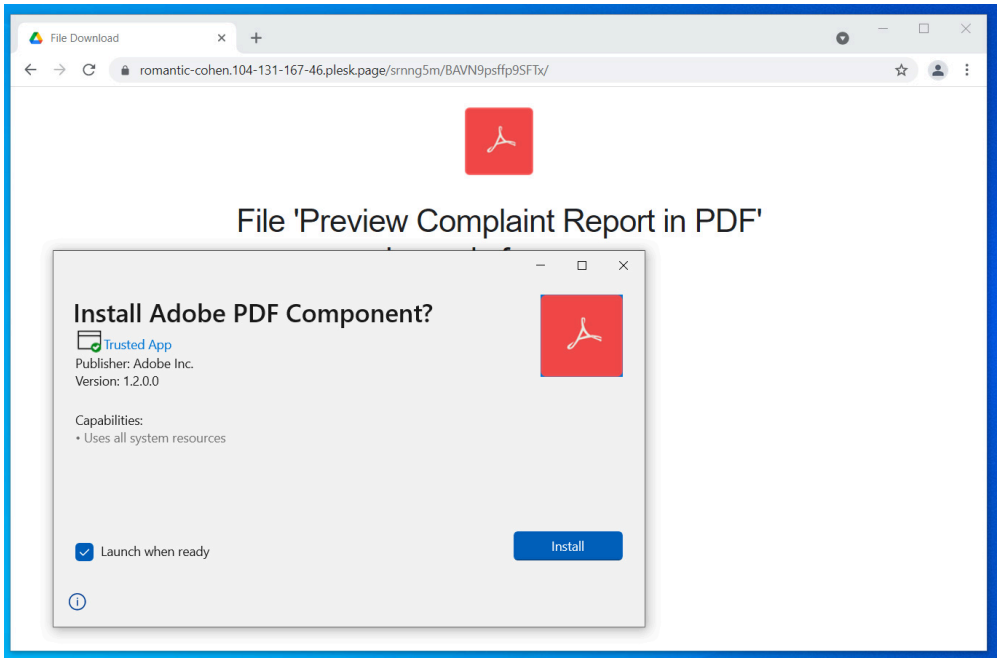


An Emotet appinstaller XML file

Source: BleepingComputer

When attempting to open an .appinstaller file, the Windows browser will prompt if you wish to open the Windows App Installer program to proceed.

Once you agree, you will be shown an App Installer window prompting you to install the 'Adobe PDF Component.'

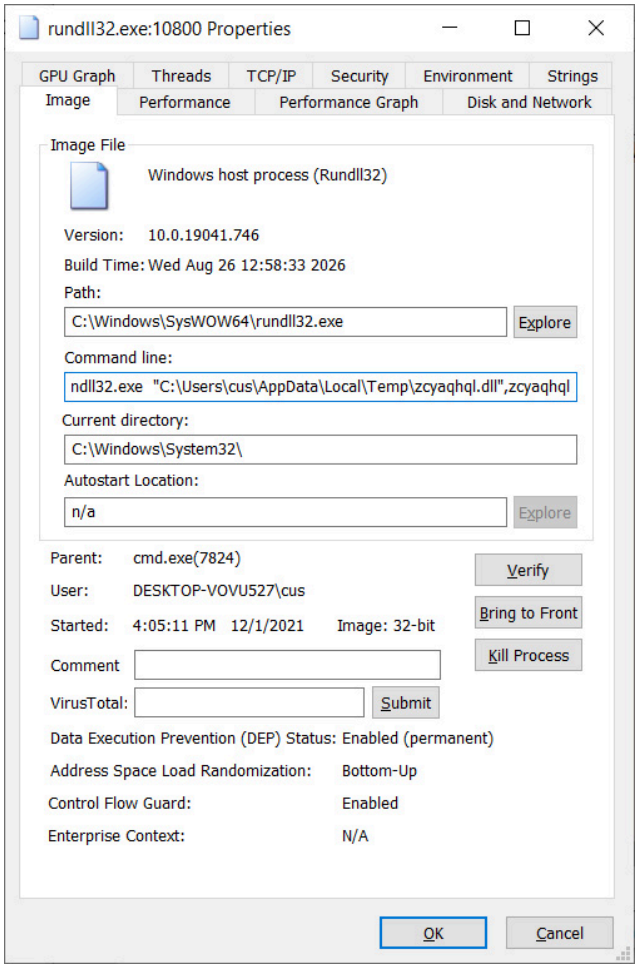


App Installer prompting to install the Fake Adobe PDF Component

Source: BleepingComputer

The malicious package looks like a legitimate Adobe application, as it has a legitimate Adobe PDF icon, a valid certificate that marks it as a 'Trusted App', and fake publisher information. This type of validation from Windows is more than enough for many users to trust the application and install it.

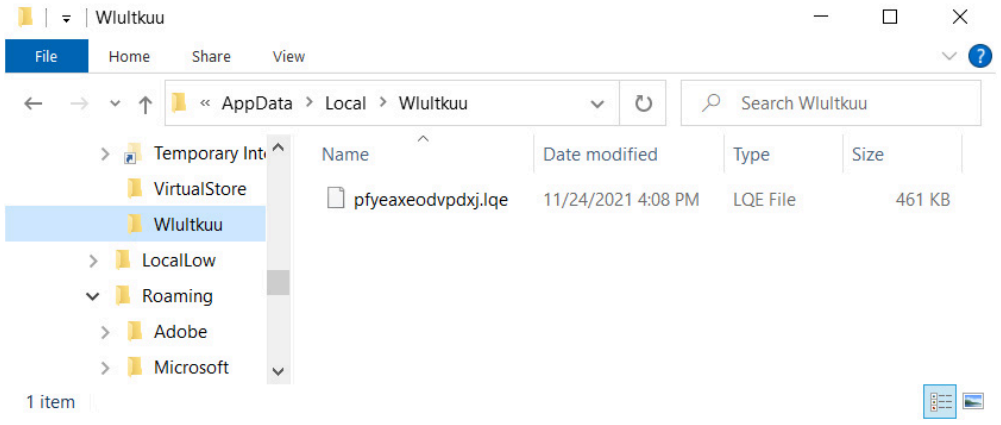
Once a user clicks on the 'Install' button, App Installer will download and install the malicious appxbundle hosted on Microsoft Azure. This appxbundle will install a DLL in the %Temp% folder and execute it with rundll32.exe, as shown below.



Installing the Emotet infection

Source: BleepingComputer

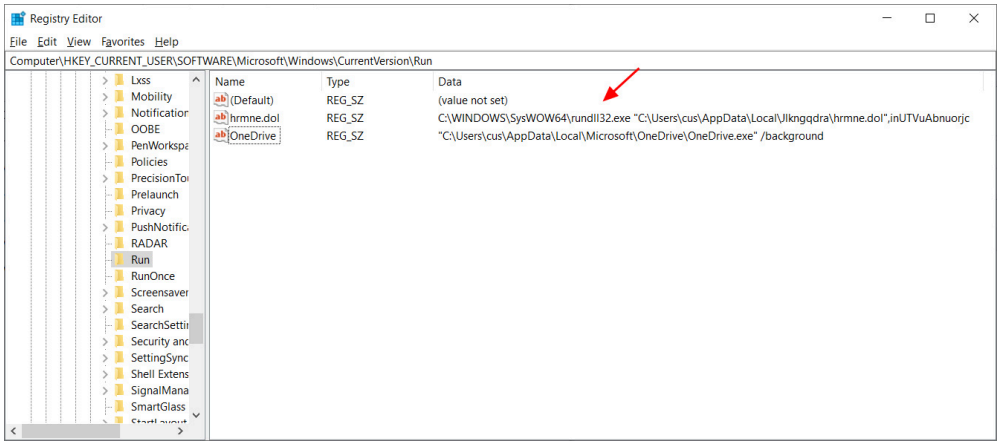
This process will also copy the DLL as a randomly named file and folder in %LocalAppData%, as shown below.



Emotet saved under a random file name

Source: BleepingComputer

Finally, an autorun will be created under **HKCU\Software\Microsoft\Windows\CurrentVersion\Run** to automatically launch the DLL when a user logs into Windows.



Registry autorun to start Emotet when Windows starts

Source: BleepingComputer

Emotet was the most highly distributed malware in the past until a law enforcement operation shut down and seized the botnet's infrastructure. Ten months later, Emotet was resurrected as it started to rebuild with the help of the TrickBot trojan.

A day later, Emotet spam campaigns began, with emails hitting users' mailboxes with various lures and malicious documents that installed the malware.

These campaigns have allowed Emotet to build its presence rapidly, and once again, perform large-scale phishing campaigns that install TrickBot and Qbot.

Emotet campaigns commonly lead to ransomware attacks. Windows admins must stay on top of the malware distribution methods and train employees to spot Emotet campaigns.

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.
