What is SquirrelWaffle malware? How to avoid?

Called dropper malware, the developers of SquirrelWaffle have gone to great lengths to keep it hard to detect and analyze.

A malware threat called SquirrelWaffle has emerged. Distributed primarily through spam email campaigns, this malware infiltrates corporate networks by injecting malicious programs into compromised systems.

Let's learn how this malware spreads and its attack vectors. At the end of the article, TipsMake will also give 5 tips to help you stay protected from malware attacks.

How is SquirelWaffle spread?

Called dropper malware, the developers of SquirrelWaffle have gone to great lengths to keep it hard to detect and analyze.

SquirrelWaffle is mainly spread through attachments of Microsoft Office documents in spam emails. At the time of writing (November 2021), two sources, a Microsoft Word document and a Microsoft Excel spreadsheet, have been found to be the source of this malware.

The infection vector begins when the victim opens a ZIP file containing a malicious Office document. The VBA macros in that file download the SquirrelWaffle DLL, which then distributes the vector to another threat known as Cobalt Strike.

It has also been observed that attackers can use the DocuSign signing platform as bait to trick recipients into enabling macros on their Microsoft Office toolkit.

How does SquirrelWaffle exploit Cobalt Strike?

Cobalt Strike is a legitimate penetration testing tool used by white hat hackers and security groups to test an organization's infrastructure for vulnerabilities and security issues.

Unfortunately, hackers got hold of Cobalt Strike and started exploiting this tool using it as a second stage payload for a variety of malware.

And the SquirrelWaffle malware exploits Cobalt Strike in a similar way. By providing the Cobalt Strike framework that contains post-infection malware, SquirrelWaffle renders exploits, such as persistent remote access to compromised devices.

5 tips to stay protected against malware attacks

Here are 5 tips that will help you stay protected against SquirrelWaffle and other potential malware attacks:

1. Be careful with attachments

The number one defense against any type of malware is caution with opening suspicious attachments.

Most well-prepared malware, such as phishing attacks, are very easy to fool victims and can take a lot of technical expertise to identify them. A phishing attack tricks people into opening a link or email that may come from a legitimate source. Once opened, the link can take victims to a fake website, prompt them to enter personal login information, or take them to a website that infects them with malware directly onto their device.

So take precautions when opening attachments and don't click on them - unless you're absolutely sure of their provenance.

2. Install anti-virus software

Investing in robust antivirus software and endpoint security is critical in mitigating malware attacks. Certain antivirus solutions can detect dangerous malware and prevent it from downloading.

These tools can also provide the ability to view compromised devices and even send alert notifications when a user stumbles upon a dangerous website. Most antivirus software these days also offer automatic updates to provide enhanced protection against newly created viruses.

3. Pay attention to IoC

Sometimes anti-virus software isn't equipped with malware detection, or the malware may be too new and difficult to detect, as is the case with SquirrelWaffle.

If you find yourself in this situation, it's best to keep an eye on the Indicators of Compromise (IoC).

IoC is your clue that your device has been infected with malware. For example, you may notice unusual behavior such as geographical differences on devices, an increase in database reads, or higher authentication rates on the network, etc.

4. Regular software updates

Software updates are released to address any security concerns, fix software bugs, remove security holes from old and outdated systems, improve hardware functionality, and provide support for newer device models.

So, in addition to installing anti-virus software, you should also update it regularly. This will prevent hackers from accessing your computer and infecting the system with malware.

5. Beware of Free Apps and Unknown Sources

Always buy and download apps from trusted sources as it reduces the risk of malware infection. Reputable brands take extra measures to ensure they don't distribute malware-infected apps.

Also, the paid versions of apps are generally more secure than the free ones.

> Note: Confirm the authenticity of the source by checking the full name, list of published apps, and contact details in the app description in Google Play or the Apple App Store.