What's New?

Avoiding Malicious Updates

Time: 5 minutes (3m58s + quiz time)

Points:

With a boom of companies and employees made to work from home, computer usage is at an all-time high – and cybercriminals have noticed. But while cybercriminal activity has increased, this article will show any user just how easy it is to stay safe working from home.

What is Malware?

Malware, short for malicious software, is a leading digital weapon used by cybercriminals. Whether it's malware prompting excessive advertisements, installing unwanted software, or accessing personal information, all malware is malicious and should be avoided.

What are Malicious Updates?

To infect a user's device with malware, cybercriminals have become fairly creative in how they disguise the malicious software. While this article will only discuss malware in the form of updates, it's important that users familiarize themselves with other ways in which cybercriminals utilize malware – such as email phishing or infected USB's.

Malicious updates can disguise themselves in numerous ways, such as updates for:

- Web browsers
- Software
- Operating systems
- Programs

Types of Malicious Updates

With dozens of various programs and software installed on our devices, it feels like at least one of them needs updated at any given moment. But when notified about an available software or program update, how can users differentiate an authentic update from a malicious one?

Malicious updates most commonly take on two forms: pop-up and embedded. But while cybercriminals have learned to effectively disguise their malicious updates, a basic understanding of how they work will be enough to identify red flags and avoid any potential harm.

Pop-Updates

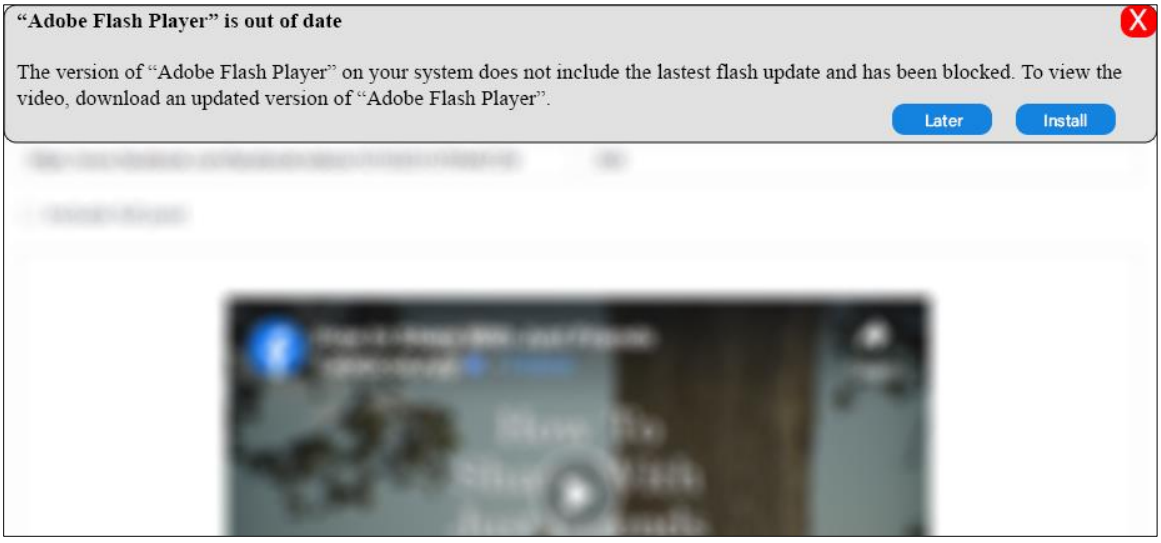
Malicious pop-up updates, or pop-updates, work similarly to the infamously annoying pop-up advertisement. Typically found on insecure or poorly maintained websites, malicious pop-updates remain hidden on the web page until they, hence their name, pop-up on screen.

Disguised as a notification for a program or software update, the malicious pop-update is meant to trick users into clicking the "update" or "install" button. But by clicking one of these options, users are actually clicking a hidden option allowing malware to be installed onto their device.

Pop-up Malicious Update Notification. Left: what the user sees, Right: what the user actually clicks

Embedded Updates

Malicious embedded updates, unlike pop-updates, are meant to look as if they are built into the website. Because these malicious updates are not shoved in front of the user, embedded updates rely on text to communicate the update's urgency and therefore trick users into downloading the malware. Like pop-updates, by clicking "update" or "install," users are actually downloading malware to their device.



Embedded Malicious Flash Update

Malicious Flash Update

While both embedded updates and pop-updates can take the form of any program or software update, users should be aware of one of the most popular formats: Adobe Flash Player update. Installed on nearly every device, Flash is a software used to view multimedia online.

Given Flash's purpose, malicious Flash updates are popularly accompanied by a message requiring users to update their Flash player in order to listen to or view multimedia on a website. And just like any other malicious update, once a user selects the update, malware will instead be installed to the device.

Red Flags

Just because malicious updates are meant to look real doesn't mean they can't be identified. In fact, there are three red flags users can keep an eye out for in order to avoid accidentally clicking a malicious update:

1. **Suspicious URL:** This is usually a giveaway. If users are asked to update a software or program while browsing the web, ensure that the website's URL (or link) is for an authentic website and is not suspicious like "freeupd.free247update."

2. **Keeps Coming Back:** When an authentic update is closed by clicking the red "x," it will remain closed. However, when malicious updates are closed, they will reappear after a few moments, if not immediately, in an attempt to get users to click "update" or "install."

3. **Won't Close:** In addition to the red "x," authentic updates typically have a "later" option to close the update notification. But when either are selected on a malicious update, the notification will remain open – a way of urging users to click "update" or "install."

Staying Safe

Say you're walking down the street and a stranger comes up and says "Here, drink this." Would you drink it? No way! So, when a strange update pops up on screen, users should act no different. Therefore, the best way to avoid malicious updates is by avoiding interaction all together. By simply avoiding clicking on the update and instead closing the webpage entirely, users are safe from accidentally installing the hidden malware.

In addition to simply avoiding suspicious update notifications when browsing online, anti-virus/anti-malware software can reduce any additional risk of becoming compromised. Norton AntiVirus software, Malwarebytes anti-malware software and Norton 360 can be earned by reaching tiers three, four and five respectively in this platform.

References:

"Can You Tell the Difference Between Fake and Legitimate Software Updates?" InvisionKC. Published: 9/12/2019. Accessed: 4/6/2020.

"Remove fake Adobe Flash Player update virus from Mac" MacSecurity. Published: 3/4/2020. Accessed: 4/6/2020.

"This fake software update tries to download malware onto your PC even when you click 'later'" ZDNet. Published: 11/21/2019. Accessed: 4/6/2020.

Quiz Questions (correct answer marked with * and answer feedback provided after the dash):

Q1: "Malware" is short for:

A1: Mail Software- "Malware" is actually short for "malicious software." Whether it's malware prompting excessive advertisements, installing unwanted software, or accessing personal information, all malware is malicious and should be avoided.

*A2: Malicious Software- Correct! Whether it's malware prompting excessive advertisements, installing unwanted software, or accessing personal information, all malware is malicious and should be avoided.

A3: It's not short for anything- "Malware" is actually short for "malicious software." Whether it's malware prompting excessive advertisements, installing unwanted software, or accessing personal information, all malware is malicious and should be avoided.

Q2: What users see on screen is always exactly what is actually on the screen?

A1: True- This is not always the case. Pop-updates are disguised as a notification for a program or software update and are meant to trick users into clicking the "update" or "install" button. But by clicking one of these options, users are actually selecting a hidden option – allowing the malware to be installed onto their device.

*A2: False- Correct! Pop-updates are disguised as a notification for a program or software update and are meant to trick users into clicking the "update" or "install" button. But by clicking one of these options, users are actually selecting a hidden option – allowing the malware to be installed onto their device.

Q3: An update notification that will not remain closed:

A1: Is likely an important update that should be installed immediately- When an authentic update is closed by clicking the red "x," it will remain closed. However, when malicious updates are closed, they will reappear after a few moments, if not immediately, in an attempt to get users to click "update" or "install."

A2: Is likely a glitched update, meaning users should install the update immediately- When an authentic update is closed by clicking the red "x," it will remain closed. However, when malicious updates are closed, they will reappear after a few moments, if not immediately, in an attempt to get users to click "update" or "install."

*A3: Is likely a malicious update and should be avoided entirely- Correct! When an authentic update is closed by clicking the red “x,” it will remain closed. However, when malicious updates are closed, they will reappear after a few moments, if not immediately, in an attempt to get users to click “update” or “install.”