OCTOBER 2018

Cyber Security Awareness Month

INFOSEC NEWSBYTES OF THE WEEK | ISSUE 3

BDO
WE SUPPORT CYBER SECURITY AWARENESS MONTH 2018

Fake Adobe Flash Updates Hide Malicious Crypto Miners

The good news: A recent scourge of fake Adobe installers does provide an update to the latest version of Flash. The bad news: It places cryptomining malware on your machine too.

Security-savvy computer users have not found such attacks difficult to spot and know to only get updates to Adobe Flash Player from the company's website.

A new wave of attacks, however, has added a twist to the traditional malware attack disguised as an update to Adobe Flash Player by actually updating Adobe Flash… for real!

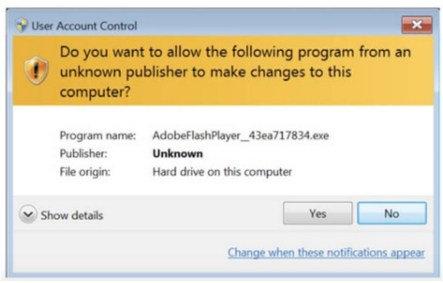
Have malicious hackers had a surprising change of heart? Have online criminals replaced avarice with altruism?

Sadly not, because although a fake Adobe update is updating Adobe Flash, it is also sneakily installing cryptomining code onto the Windows computers of its unsuspecting victims.

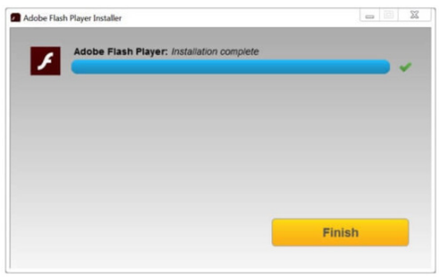
Security researchers at Palo Alto Networks published details of how XMRig cryptomining code has been installed under the cover of fake Adobe Flash updates. Fake Flash updates that borrow genuine pop-up notifications from the official Adobe installer do indeed update their victim's Flash Player installation.

Of course, a user is less likely to suspect that an Adobe Flash update was bogus if their installation of Adobe Flash really is brought up-to-date. But that's not to say there are no clues that the installer is not the one approved by Adobe.

One warning sign, for instance, is that the bogus installer has not been digitally signed by Adobe, which causes Windows to pop up a warning that the user is about to run code from an unknown publisher.



Unfortunately, many users may ignore the warning and grant permission for the program to execute regardless, causing the Adobe Flash installation to be updated and XMRig cryptomining code to be installed.



In tests conducted by Palo Alto's Brad Duncan, an infected Windows computer soon began to generate network traffic over TCP port 14444 associated with XMRig mining code in an apparent attempt to cryptomine Monero, a digital currency that has been widely adopted by cybercriminals.

The observant may also notice that their computer's performance has become sluggish after the cryptomining code has been installed, although, in practice, this can be difficult for many users to spot.

At BDO, we have the expertise and experience in a range of cybersecurity services and solutions. Please feel free to contact us and let us know how we can assist you.

FOR MORE INFORMATION

CECIL SU
+65 6829 9628
cecilsu@bdo.com.sg

www.bdo.com.sg

BDO

BDO TRA Recommendations:

- *Use web and email filtering to protect your organisation from malicious URLs.*
- *Run an up-to-date anti-virus solution.*
- *Educate staff about the risks of running programs from unknown sources and help them understand the implications of ignoring security prompts that warn software is from an unknown publisher.*
- *Only trust Adobe updates that come directly from Adobe's website, and perhaps consider uninstalling Flash altogether if you don't need it!*

Multiple unauthorised log-in attempts detected on HealthHub portal: HPB

Multiple unauthorised log-in attempts were detected on the Singapore Health Promotion Board's (HPB) HealthHub portal over four days, the statutory board said on Thursday (Oct 18).

HPB said it conducted an investigation after it received feedback from a user who suspected that her email account had been used without her authorisation to log in to the portal.

It found a "higher than usual" number of attempted log-ins on four days - Sep 28, Oct 3, Oct 8 and Oct 9. The attempts were made with more than 27,000 unique IDs and emails.

Although 98 per cent of the email addresses used were not related to existing HealthHub accounts and the log-in attempts were unsuccessful, 72 accounts were successfully logged in during those time periods.

"Based on the suspicious volume of email addresses not related to HealthHub account IDs and the repeated attempts, it is likely that the volume of email addresses used had been obtained from external sources," HPB said in its statement.

Investigations on the HealthHub system is still on-going.

Meet GreyEnergy, the newest hacking group hitting Ukraine's power grid

Ever since the seminal cyberattacks on the Ukrainian power grid in 2015 and 2016, researchers have traced the evolution of the broad set of hackers behind the attacks in an effort to warn organisations the hackers might strike next. Early October 2018, analysts from cybersecurity company ESET added to that body of knowledge in revealing a quieter subgroup of those hackers that has targeted energy companies in Ukraine and Poland.

ESET has dubbed the group GreyEnergy, a derivative of the original group of hackers, which have been known as BlackEnergy. Whereas BlackEnergy is known for the disruptive 2015 attack on the Ukrainian grid that cut power for roughly 225,000 people, GreyEnergy has to date preferred reconnaissance and espionage, according to ESET. The group has taken screenshots of its possible targets, stolen credentials, and exfiltrated files.

"Clearly, they want to fly under the radar," said Anton Cherepanov, the company's lead researcher on the case. ESET suspects that BlackEnergy morphed to GreyEnergy at the end of 2015 after the group grabbed the world's attention in the first known cyberattack to cause a blackout.

Other cybersecurity companies refer to the group behind BlackEnergy as "Sandworm," an outfit that Western governments have attributed to Russian's military intelligence directorate. Last week, ESET researchers published evidence - in the form of custom remote access tools - that links 2015 and 2016 hacking operations against the Ukrainian grid with last year's NotPetya malware outbreak.

Can your flight be hacked?

It took Robert Hickey and his team of researchers just two days to do what the aerospace industry had insisted was nearly impossible.

On 21st September 2016, the US Department of Homeland Security official hacked into the systems of a Boeing 757 passenger aircraft parked in the airport in Atlantic City, New Jersey. It was, he said last year, "a remote, non-co-operative penetration" without insider help or being onboard, using "typical stuff that could get through security".

Mr Hickey waited more than a year to drop his bombshell at a cybersecurity conference in Virginia, and even then he gave scant detail about what had been accessed and how -- for obvious security reasons.

But his revelation has raised serious questions about aviation's exposure to cyber attack as aircraft, airports and air traffic control systems become increasingly reliant on digital systems.

WHAT ARE ROOTKITS?

Cybercriminals use rootkits to hide and protect malware on a computer. The rootkit itself is not necessarily harmful; what is dangerous is the various forms of malware inside them.

Malware in a rootkit can steal data and take over a system for malicious purposes, all while remaining undetected.

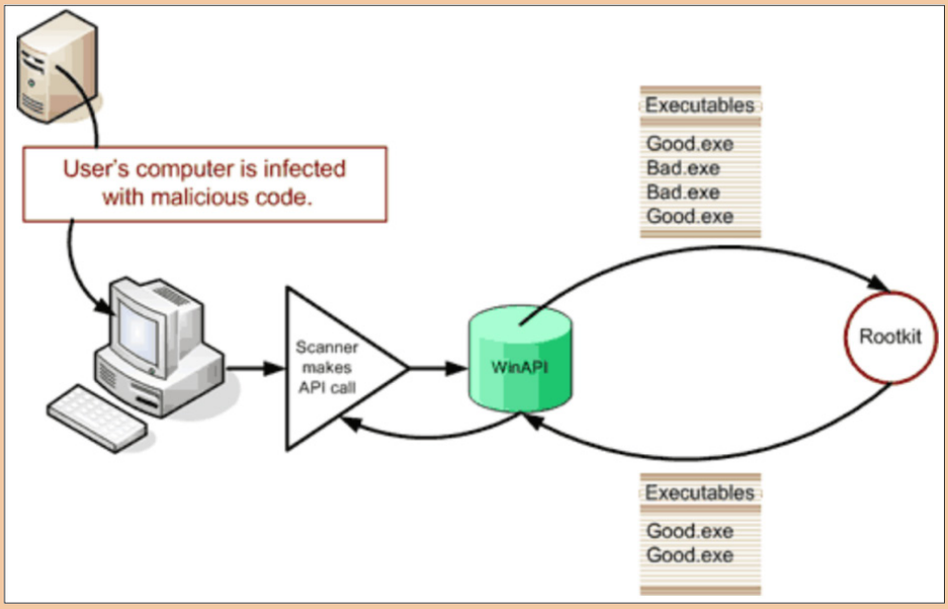
Installed in the core operating system of a computer, rootkits are difficult to detect and potentially harmful to a system. They can block some antivirus and antimalware software, rendering them ineffective, in part because rootkits activate before an operating system boots up.

Rootkits could remain in place for years. Their core role is to hide any trail of their existence. They can even alter data reports from a system to avoid detection.

The Alureon and Sinowal Trojans and Sirefef, Rustock and Cutwail, are all well-known malware associated with rootkits.

Windows operating systems have some built-in technologies to help protect them from rootkits, but they are not perfect. Criminal programmers can design a rootkit virus to change how an operating system processes information and commands, including login protocols.

Rootkit installation can be automated, or an attacker can install it after having obtained root or Administrator access. Obtaining this access is a result of direct attack on a system, i.e. exploiting a known vulnerability (such as privilege escalation) or a password (obtained by cracking or social engineering tactics like "phishing"). Once installed, it becomes possible to hide the intrusion as well as to maintain privileged access. The key is the root or administrator access. Full control over a system means that existing software can be modified, including software that might otherwise be used to detect or circumvent it.



Source: http://wiki.cas.mcmaster.ca/index.php/Rootkits

Rootkit detection is difficult because a rootkit may be able to subvert the software that is intended to find it. Detection methods include using an alternative and trusted operating system, behavioural-based methods, signature scanning, difference scanning, and memory dump analysis. Removal can be complicated or practically impossible, especially in cases where the rootkit resides in the kernel; reinstallation of the operating system may be the only available solution to the problem. When dealing with firmware rootkits, removal may require hardware replacement or specialised equipment.