Cyber Security

SECURITY ALERT! PEGASUS IS COPYING YOUR PERSONAL DATA…

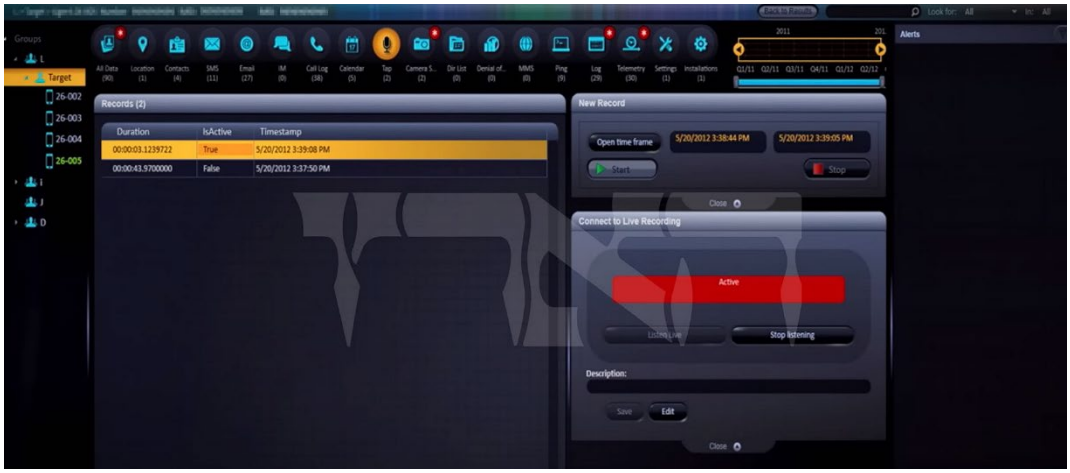
'T'was the night before Songkran, and all through the house, not a creature was stirring, except …" the Pegasus spyware working quietly and invisibly in the background on your devices and copying all your personal information and data to a computer server in some foreign country… while your sleep soundly in your bed, completely unaware of this silent thief!

But how can that happen? … I mean, phones and laptops, etc., have security built-in, don't they? My personal information can't just be stolen like that… can it? I mean, without me knowing?

The answer is YES. It can.

Pegasus is the name for the most powerful piece of spyware ever developed. An Israeli private company, the NSO Group, developed it and it is so powerful and more lethal that even the Israel Ministry of Defense declares it a military cyber weapon and only allows government agencies to own it.

It was the Pegasus spyware which penetrated all the security of the most secure Blackberry devices in 2014 during Barack Obama's second term. And, in a recent cybersecurity detection, it was found to be lurking in the background on the mobile phones of many political activists. Clearly, Pegasus is now targeting iPhones and Android devices.

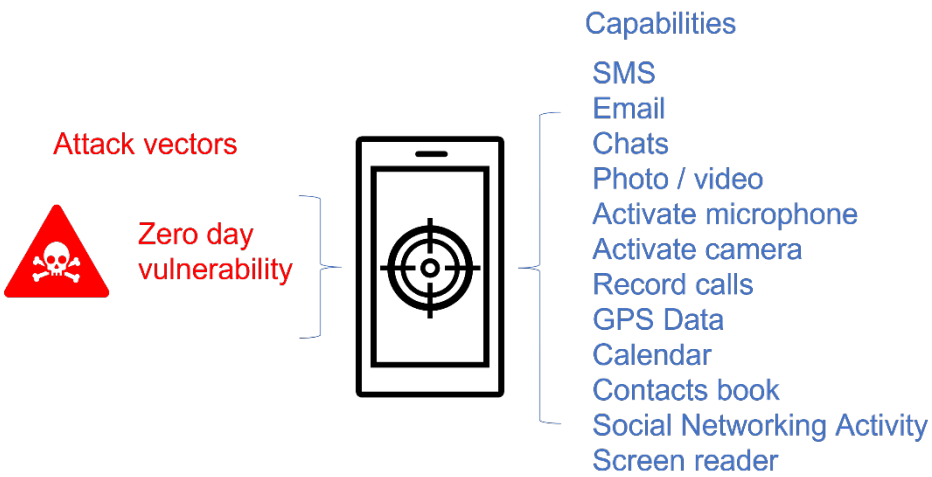


Cyber Security

So how does it do it? Well, the earliest version of Pegasus used what's called ' one-click attack vulnerability' using spear-phishing. This is when a phone is sent an email or text message and tricks the user into clicking on a malicious link. The problem for Pegasus in its earlier incarnations was that it was easily detectable because it was active in the core of the target devices operating system and forensic software could detect it.

The latest versions however have improved its stealth and it no longer requires a smartphone's operating system to perform its actions. An attacker just needs to find a vulnerable application on the device or the operating system of the device where a patch is not yet available (a patch is a software update which addresses security vulnerabilities within a program or product – if security vulnerabilities exist in program or product, Pegasus can exploit this. This type of attack is also referred to as a zero-click attack.

After exploiting a mobile phone's vulnerability with a zero-click attack, Pegasus can theoretically harvest any data from the penetrated device and transmit it back to NSO's server in Israel. In fact, Pegasus can do a lot more than what the owner of the device can do!

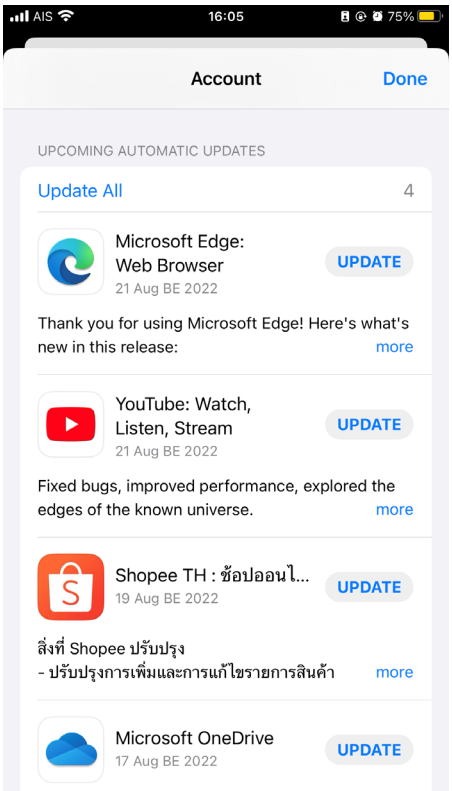


PKF Thailand

Cyber Security

Mobile phones are not the only device Pegasus targets, and it could also have penetrated other devices you own such as your notebook, CCTV, etc. Potentially, it could be in any device where a security vulnerability exists and where a 'patch' wasn't installed or hasn't been installed to 'plug' the security hole.

But all is not lost – there are things you can do to help dissuade Pegasus and other potential malware from building a home in your devices and these include:



- Ensuring that your applications are up to date and have the latest updates installed;
- Ensuring that the operating system on your device is up to date;
- Never click on any links or download any attachments sent in email messages or text messages from unknown senders;
- Avoid the use of public Wi-Fi; and,
- Always encrypt the data on your device and enable remote-wipe features if possible so that if, for some reason, your device is lost or stolen - you know that your data is safe.

Good luck and keep your devices safe from invisible spyware thieves!