SYNCDOG

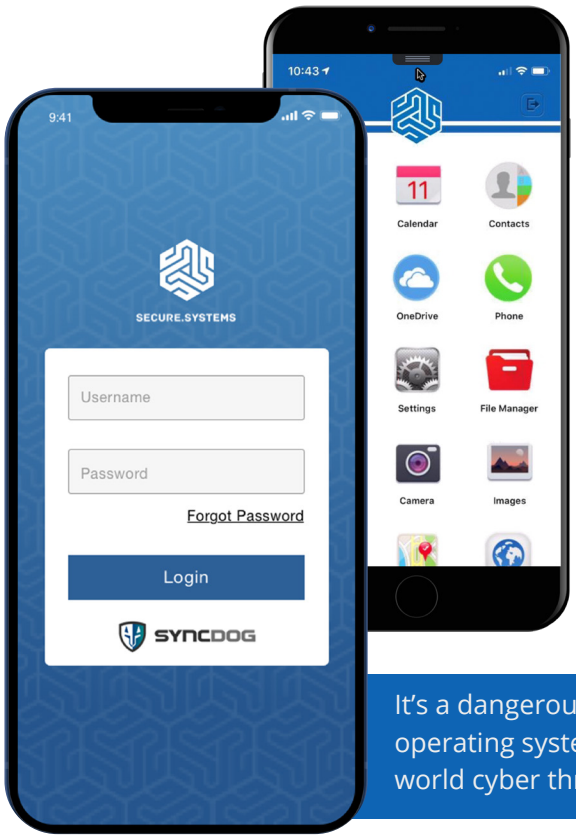
Pegasus Spyware – No Match for SyncDog

News cycles around the world have been dominated by COVID-19 stories especially related to the recent global surge of the Delta variant, a highly infectious mutation of SARS cov-2. Similarly, in the digital realm, computer viruses have also been developing, with one variant finding its way onto mobile devices around the world with surprising ease. If Delta is the highly infectious version of COVID, Pegasus is its digital equal, and then some.

Recent news regarding the Pegasus spyware – developed by the Israeli tech firm NSO – has brought to light serious vulnerabilities in mobile devices and called into question many users' assumptions about the security of their device, and if device manufacturers are providing the level of protection that they claim.

There have been countless malware and spyware attacks over the years, but perhaps what is most disturbing about the Pegasus variant is that its exploits can be delivered via zero-click distribution through innocuous methods such as receiving a text message or a WhatsApp call. This means the user doesn't have to open an attachment, click on a link, or perform any other actions to become infected. Pegasus achieves this by constantly searching for and identifying vulnerabilities in the operating system or bundled applications, such as iMessage. The ease of which it can infiltrate devices is astounding and extremely concerning, especially since the infection goes completely unnoticed by the user.

This new variant of spyware has further exposed the already crumbling notion that operating systems can provide real security, whether Android or iOS. It would be helpful to reframe our assumptions about hardware security by taking some cues from the human body. Sure, the human body has a built-in immune system that is designed to handle protection against various types of infection, but certain serious diseases can prove to be too much for the body's operating system. This is when we must implement external measures to treat and protect against these invaders.



Much the same way, a device's operating system is the first line of defense. There are some basic protections that the operating system offers against common types of malware, but as all the recent press about the Pegasus spyware shows, it certainly does not offer complete security and protection against all variants. For that, it's necessary to implement external security software that is specifically dedicated to this task. SyncDog's Secure.Systems containers are an example of this type of implementation. Our containers do not rely on the operating system to be clean and uncompromised. We provide security and protection even when, or even assuming, the operating system has been infected. All data in a Secure.Systems container is stored in its own encrypted database, separate from the operating system, and does not use built-in operating system encryption or storage mechanisms, such as the keychain. We also handle low level protocol transport encryption for all data that is sent in and out of the container, and we do not rely on the operating system to secure data in transit. More than anything, Secure.Systems containers provide peace of mind, allowing a user, corporation, government agency or the like, to be confident that their data is secure no matter what malware may exist on the device.

It's a dangerous world out there both in the physical and digital realms. Modern operating systems may provide baseline security, but for protection against real world cyber threats that let you sleep at night it has to be SyncDog.

SYNCDOG

+1.855.SYNCDOG (1-855-796-2364)
info@syncdog.com

1801 Old Reston Ave, Suite 301
Reston, VA 20190