SOC Threat Advisory

Threat Level – Minor

Pegasus Spyware – CVE-2016-4655, CVE-2016-4656, CVE-2016-4657

Synopsis

A sophisticated attack has been uncovered by security researchers targeting Apple mobile phone software. The attack in effect is a phishing scam where by a victim is socially engineered into clicking on a link within a SMS message. The link points the user to a web page that then installs malicious software.

Technical Threat

The Pegasus spyware attack contains three separate vulnerabilities:

- CVE-2016-4655: which allows attackers to calculate the iOS kernels location in memory.
- CVE-2016-4656: which is Kernel memory corruption which allows the attacker to silently jailbreak the device and install surveillance software.
- CVE-2016-4657: which is a memory corruption webkit that allows the attacker to compromise the device when the user clicks on a specially crafted link.

Researchers believe the spyware is highly configurable and can gather information from multiple applications that are installed on a specific device. The malware was also capable of restricting automatic updates from Apple from being delivered to compromised devices.

For more information, please contact:
Fujitsu Managed Security Services
fapl.askMSS@sg.fujitsu.com

Affected Platforms

Versions lower than iOS 9.3.5

Mitigation

Apple have released a software update which mitigates the threat. Advice is to update to the latest version of iOS. An Apple mobile device user can check their device’s version of Software by checking Settings > General > About > Version.

Further Reading

https://blog.lookout.com/blog/2016/08/25/trident-pegasus/

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-4655

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2016-4656

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4657

https://support.apple.com/en-gb/HT207107