Media Advisory

Fortinet Urges Consumers to Watch Out for Ransomware Targeting their Mobile Devices

Malicious software that locks mobile devices and demand payment are becoming common, and users must proactively guard against them

Fortinet® (NASDAQ: FTNT) – a global leader in high-performance network security – has advised mobile device users to be on the alert for mobile ransomware, which has seen a steady increase worldwide in recent months.

Ransomware is a type of malware that restricts usage of the device it infects, demanding payment from the end-user in order to regain control over the device. Until recently, ransomware has been targeting computers, but they are now attacking mobile phones.

"Ransomware threats have been big on mobile phones this year − from the emergence of the first variant targeting iOS devices to the first Android variant that encrypts phone data," said Ruchna Nigam, Security Researcher, FortiGuard Labs, Fortinet.

Here are the four mobile ransomware detected by FortiGuard Labs recently:

Simplocker, discovered in June 2014, comes in the form of Trojanized applications like a Flash player, for example. This is the first "real" ransomware seen on Android in the sense that it actually encrypts files (with extensions "jpeg", "jpg", "png", "bmp", "gif", "pdf", "doc", "docx", "txt", "avi", "mkv", "3gp" and "mp4") on the phone. The malware locks the infected phone, displays a screen telling the user that the phone is locked, and demands payment to unlock it. Even after uninstallation of the application in safe mode, the files need to be decrypted to be read.

Cryptolocker for mobile, discovered in May 2014, disguises itself as a fake BaDoink video downloader application. Although the malware doesn't cause any damage to phone data, it displays a locked screen claiming to originate from the local police, customized to the geo-location of the end-user. The locked screen is re-launched every five seconds, making phone operation near impossible without uninstallation of the malware.

iCloud 'Oleg Pliss', discovered in May 2014, accounted for the first reported cases of ransomware for Apple devices. These incidents can't be attributed to a particular piece of malware but to compromised iCloud accounts in combination with some social engineering. The attackers were believed to have exploited Apple's Find My iPhone, iPad, and Mac feature along with recycled passwords leaked from password breaches. The attack, however, doesn't work if the device already has a passcode (phone lock) set. The malware can potentially leak calendar and contact information, and allow the attacker to delete all information on the phone.

FakeDefend, discovered in July 2013, is a ransomware that targets Android phones. It comes disguised as a fake antivirus (AV) application prompting the end-user to pay for a full subscription of the AV after performing a fake scan and showing a list of hardcoded "infections" found on the phone. If the user decides to pay, the credit card details entered are leaked to the attacker's server in plain text. These captured credit card details may be used for rogue transactions later.

"As mobile device adoption continues to gain pace, hackers have found a new lucrative target in handsets, in addition to traditional PCs," said Nigam. "The public needs to become more security-aware, and take more measures to prevent their handsets from becoming conduits of monetary and information loss."

Here are Nigam's top three pointers to guard against mobile ransomware:

1. Have a functional anti-virus software on your phone. This should prevent or at least warn against installation of infected applications.

2. Always install applications from trusted sources and developers. If in doubt, user comments can help gauge the legitimacy of an application.

3. iPhone and iPad users should activate and set passcodes on their device. This forces the use of that passcode while activating the Find My iPhone feature, thereby rendering the iCloud ‘Oleg Pliss' ransomware attack ineffective.

######