The MobilityHub
SECURING DATA & APPS.

John Edwards

Ransomware on the Rise

John Edwards, Technology Journalist, 2/22/2013

Kidnappers used to create ransom notes by painstakingly cutting letters out of magazines. Now, such messages simply appear on a display, demanding cold cash for supposedly stolen data.

Welcome to ransomware, a type of malware that, once installed, allows thieves to lock an end-user device from a remote location, effectively holding its data hostage. Ransomware typically generates a pop-up window, webpage, or email warning that appears to come from an official authority, such as the FBI. The message states that the user's system has been locked due to its suspected use in illegal activities. The message then demands payment before the user can again access his or her files and programs.

Various forms of ransomware have circulated on the Internet for several years, creating a great deal of aggravation, not to mention significant financial losses to gullible users. Over the past few months, however, a new ransomware variant has raised the stakes by claiming that it will wipe the user's hard drives clean of data unless money is handed over within a specified period of time.

This new ransomware, which anti-malware software provider Symantec classifies as Trojan.Ransomlock.G, and several other anti-malware vendors refer to as Reveton, claims that any move to circumvent the lockdown will trigger complete and irrevocable data loss. "An attempt to unlock the computer by yourself will lead to the full formatting of the operating system. All the files, videos, photos, documents on your computer will be deleted," the on-screen message reads.

The message is bogus, of course, but it's terrifying enough to cause many recipients to fork over significant amounts of cash -- typically $300 to unlock the system within a fake deadline of 48 hours (tracked by an on-screen countdown timer).

Enterprises threatened

Ransomware poses a threat to enterprises as well as consumers. Any employee using a mobile device containing enterprise information could potentially be intimidated into meeting the thieves' demands, using either personal or business funds to retrieve the hijacked data. The chances of getting any of this money back are close to nil, of course.

Ransomware is installed when the user opens a malevolent email attachment or clicks on a malicious link contained in an email message, an instant message, or a social network post. In some cases, the ransomware can even be installed simply by visiting a malicious website. Virtually all current ransomware variations are designed to attack Windows systems, making

users with Windows-based mobile systems the most likely victims.

So far there have been no reported widespread ransomware breakouts on Apple OSX or iOS systems. Android-based devices also appear to be unaffected for the time being. This situation could soon change, however, as thieves begin looking for fresh targets.

Ransomware shows no signs of going away soon, so it's important to alert employees, particularly Windows notebook users, to the threat. Urge users not to panic if they receive a ransomware message on their device and, mostly importantly, advise them to never attempt resolving the problem on their own.

Related posts:

- Mobile Malware Outlook 2013
- How Safe Is Your Mobile Network?
- QR Codes: The Latest Hacker Entry Point