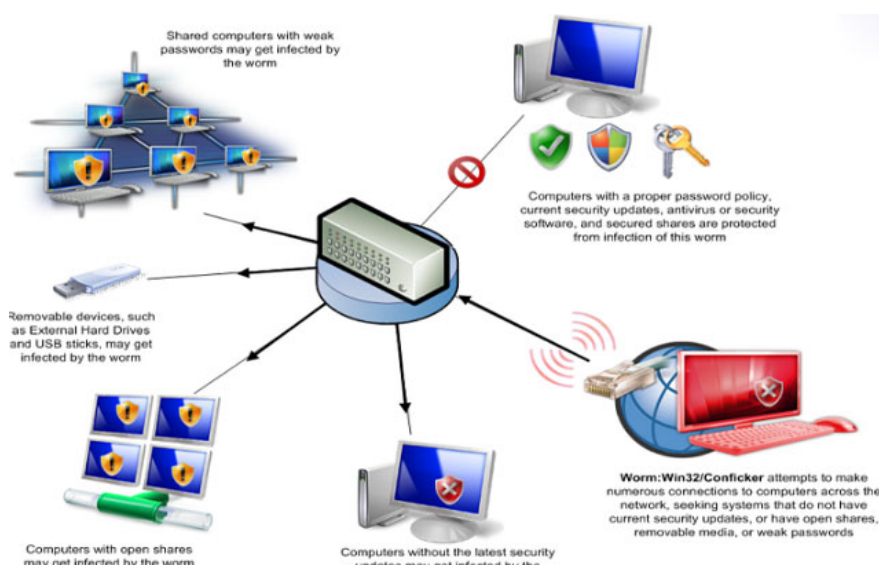


2011: malware transferred from computer to ... pocket pants

Predictably spike mobile malware is becoming a reality due to the widespread use of new generation smartphones running advanced operating systems.

Predictably spike mobile malware is becoming a reality due to the widespread use of new generation smartphones running advanced operating systems.

Although the predictions have been quite popular for the past 6 years and even though they are not expected to become reality, it seems that new malicious applications will still "disrupt" next year. Users, despite their awareness of the threat of attacking their computers, have yet to envision the attack on mobile phones.



In the third quarter of this year, more than 80 million smartphones were sold worldwide, accounting for about 20% of the total number of handsets sold, according to last month's statistics firm Gartner. Smartphone has the ability to connect to the Internet and is therefore more vulnerable to attack than other mobile devices.

Threats to these devices may appear in the following ways:

Phishing application

Online application stores for mobile are increasingly popular for platforms from Apple iOS, Android from Google to Windows Phone 7 from Microsoft and Symbian. Apple 'managed' to tighten the App Store should minimize phishing applications from dishonest developers. But bad apps for other platforms have appeared.

In September, researchers from security firm Fortinet discovered a mobile variant of Zeus - a famous malware for stealing bank account information. This application targets Symbian Series 60 and BlackBerry devices, blocking the one-time password checking process used to authenticate transactions.

This mobile application has a legal registration certificate, which allows downloading and installing on devices. This will have a strong impact on the authentication method of banks. Banks have long used mobile phones to send disposable password SMS, only a few banks using specialized devices can generate random, disposable codes.

Stealthy phishing applications aren't that much, but ordinary users should be careful about downloading programs, especially with tightly controlled applications platforms.

Traditional malware

While computer operating systems such as Windows are often infected with malware, so far malware is less targeted at mobile devices. But the researchers found that applications such as fake dialers would send SMS messages to scammers' switchboards. Other threats include worms spreading through communication protocols such as Bluetooth.

With the increasing use of mobile OS tablets, these devices will also be subject to similar types of attacks. According to Bradley Anstis - vice president of technology strategy for security company M86 (USA), that will happen within a year.

Privacy data collection issue

Mobile applications also have other privacy-related hazards such as collecting, transmitting and saving data. Ad networks and mobile app developers are often very interested in the data around how and where users are using their applications. Data may include information identifying a specific device while users are unaware that they are being monitored. Apple also allows application developers to collect location information, however only when the user is notified.

Social engineering

Like on desktops and laptops, phishing involves not only technical tricks. Phishing tricks (tricking users into accessing fake websites and disclosing their sensitive information) is a major threat to mobile devices. People often trust mobile devices rather than their computers, so they are more easily fooled.

If a person is on the corporate network, phishing sites are often blocked, Anstis said. But if someone uses a mobile device that works on a 3G network, but does not connect through an enterprise gateway, harmful pages may not be blocked.

According to experts, threats to computers will move to the mobile world next year. And many security companies are seeing new service business opportunities for mobile devices.

You finished reading the article "**2011: malware transferred from computer to ... pocket pants**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.