INFORMASIETEGNOLOGIE

INFORMATION TECHNOLOGY

THE HISTORY OF MALWARE,TROJANS AND WORMS (PART 3)

Two weeks ago we explored lesser known malware, Trojans and worms, after 1985. This time around, we look at more recent threats, starting with zombies...

2003 Zombie, Phishing
The Sobig worm gave control of the PC to hackers, so that it became a "zombie," which could be used to send spam. The Mimail worm posed as an email from Paypal, asking users to confirm credit card information.

2004 IRC bots
Malicious IRC (Internet Relay Chat) bots were developed. Trojans could place the bot on a computer, where it would connect to an IRC channel without the user's knowledge and give control of the computer to hackers.

2005 Rootkits
Sony's DRM copy protection system, included on music CDs, installed a "rootkit" on users' PCs, hiding files so that they could not be duplicated. Hackers wrote Trojans to exploit this security weakness and installed a hidden "back door."

2006 Share price scams
Spam mail hyping shares in small companies ("pump-and-dump" spam) became common.

2006 Ransomware
The Zippo and Archiveus Trojan horse programs, which encrypted users' files and demanded payment in exchange for the password, were early examples of ransomware.

2006 First advanced persistent threat (APT) identified
First coined by the U.S. Air Force in 2006 and functionally defined by Alexandria, Virginia security firm Mandiant in 2008 as a group of sophisticated, determined and coordinated attackers. APTs are equipped with both the capability and the intent to persistently and effectively target a specific entity. Recognized attack vectors include infected media, supply chain compromise and social engineering.

2008 Fake antivirus software
Scaremongering tactics encourage people to hand over credit card details for fake antivirus products like AntiVirus 2008.

2008 First iPhone malware
The US Computer Emergency Response Team (US-CERT) issues a warning that a fraudulent iPhone upgrade, "iPhone firmware 1.1.3 prep," is making its way around the Internet and users should not be fooled into installing it. When a user installs the Trojan, other application components are altered. If the Trojan is uninstalled, the affected applications may also be removed.

2009 Conficker hits the headlines
Conficker, a worm that initially infects via unpatched machines, creates a media storm across the world.

2009 Polymorphic viruses rise again
Complex viruses return with a vengeance, including Scribble, a virus which mutates its appearance on each infection and used multiple vectors of attack.

2009 First Android malware
Android FakePlayerAndroid/FakePlayer.A is a Trojan that sends SMS messages to premium rate phone numbers. The Trojan penetrates Android-based smartphones disguised as an ordinary application. Users are prompted to install a small file of around 13 KB that has the standard Android extension .APK. But once the "app" is installed on the device, the Trojan bundled with it begins texting premium rate phone numbers (those that charge). The criminals are the ones operating these numbers, so they end up collecting charges to the victims' accounts.

2010 Stuxnet
Discovered in June 2010 the Stuxnet worm initially spreads indiscriminately, but is later found to contain a highly specialized malware payload that is designed to target only Siemens supervisory control and data acquisition (SCADA) systems configured to control and monitor specific industrial processes. Stuxnet's most prominent target is widely believed to be uranium enrichment infrastructure in Iran.

2012 First drive-by Android malware
The first Android drive-by malware is discovered, a Trojan called NotCompatible that poses as a system update but acts as a proxy redirect. The site checks the victim's browser's user-agent string to confirm that it is an Android visiting, then automatically installs the Trojan. A device infected with NotCompatible could potentially be used to gain access to normally protected information or systems, such as those maintained by enterprise or government.

2013 Ransomware is back
Ransomware emerges as one of the top malware threats. With some variants using advanced encryption that makes recovering locked files nearly impossible, ransomware replaces fake antivirus as malicious actors' money-soliciting threat of choice.

Take note that information below is an extract from the Sophos Threatsaurus, compiled by Sophos, a security software and hardware company.

Posted in:E-mail,Security | Tagged:Ransomware,Trojan,Virus | With 2 comments