Cybercrime timeline – updated in 2012

Cybercrime has become a well-known security risk in recent years, but hackers have been breaching IT security since the 1970s. Don't believe it? Read the cybercrime timeline to find out more.

1970s: Rootkits

Came out of the UNIX era in the 70's but the most famous episode was in 2005 it was discovered that Sony BMG Music Entertainment had used rootkit techniques to disguise digital rights management software that installed itself on consumers' computers when they played a Sony CD.

Rootkits are software that enables continuous, privileged access to a computer while actively hiding its presence from administrators. Typically, an attacker installs a rootkit on a computer after first obtaining root-level access, either by exploiting a known vulnerability or by obtaining a password

1978: Spam

The first spam e-mail was sent in 1978 over the ARPAnet, the US Defense Department network by a Digital Equipment Corp. marketing executive. Today mass mailings are sent via a vast array of channels - email, newsgroups, instant messaging, mobile phones - to recipients who have not requested them and cannot remove themselves from the mailing list. Spam has grown more malevolent, as criminals have made it the carrier for a host of scams.

1982: Viruses

A high school student named Rich Skrenta wrote Elk Cloner for Apple II computers. Hidden on a floppy disk necessary to load the operating system on the computer, it spread when users unknowingly used an infected disk to boot up.

A computer virus is a computer program that can copy itself and infect a computer. A true virus can spread from one computer to another (in some form of executable code) when its host is taken to the target computer. Thus, viruses are spread when a user sends it over a network or the Internet, or carries it on a removable medium such as a floppy disk, CD, DVD, or USB drive.

1988: Worms

Robert T. Morris, a graduate student at Cornell University, created software that would automatically replicate itself on computers hooked up to the government's ARPAnet (the precursor to the Internet).

A computer worm is a self-replicating computer program, which sends copies of itself to other nodes over a network. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

1989: Trojan horse software

In 1989 (or '87, depending who you speak to), a diskette claiming to be a database of AIDS information was mailed to thousands of AIDS researchers and subscribers to a UK computer magazine.

A Trojan is a destructive program that masquerades as a benign application and is named after the Trojan Horse of Greek mythology. The software initially appears to perform a desirable function for the user prior to installation and/or execution, but steals information or harms the system. Unlike viruses or worms, Trojans do not replicate themselves.

1990s Crimeware

This evolved from prankware, the kind of software that would install a daft message on your computer screen if you opened an infected email. Demand from organised online criminals has created a supply of easily downloadable malware packages.

1996: Phishing

The term is coined although activity predates this. Phishing attempts to trick Internet users into divulging their personal information for use or resale by criminals. Also known as social engineering, phishing typically cons users through authentic-looking emails, which link to websites that mimic those of respected financial institutions or retailers.

Spear-phishing was coined a decade later and refers to a more sophisticated online con act that targets an individual or an organisation

1998: Man-in-the-middle attack

A man in the middle attack was reported by the National Security Agency in 1998, but more famous attacks occurred in October 2005, when global banks were targeted.

Man-in-the-middle depends on interception and has been around since espionage began. However technology has given it a whole new momentum. It can be a as simple as snooping on someone's emails over unencrypted wi-fi in an Internet cafe. More malicious attacks use sophisticated Trojans to interrupt banking deals in order to siphon off billions of dollars.

MITM has recently morphed into the more invidious man–in-the-browser. The pernicious malware lurks within the victim's browser, waits until authenticated procedures have been successfully negotiated, before redirecting funds into an illicit bank account. Zeus is the most notorious MITB used to circumvent banks' multi-factor

The 00's: Social networking sites take off

My Space launches in 2003 and Facebook in 2004, heralding a new era of social networking. The medium is also rapidly colonised by criminals and is now a primary conduit for the proliferation of malware, and also of social engineering attacks.

2000: Denial-of-service and distributed denial-of-service attacks

Canadian hacker MafiaBoy launched a distributed denial-of-service attack that took down several high-profile Web sites, including Amazon, CNN and Yahoo!

A D(D)oS attack makes a computer resource, often a website, unavailable to its intended users. A common method of attack involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable

2003: Botnets

The SoBig email worm is thought to be the first organised attempt to create large-scale botnets.

A botnet is a collection of infected computers or bots that have been taken over by hackers and are used to perform malicious tasks or functions. A computer becomes a bot when it downloads a file that has bot software embedded in it. A botnet takes action without the hackers having to log in to the client's computer.

July 2010: Stuxnet

A Microsoft Windows computer worm was discovered in July 2010 that targets industrial software and equipment. It is the first discovered malware that spies on and subverts industrial systems.

2011: Advanced persistent threat (APT)

Is the acronym on every cyber security professional's lips. APT usually refers to a group, such as a foreign nation state government, with both the capability and the intent to persistently and effectively target a specific entity. The aggressor uses every kind of malware at their disposal in a sustained attack on a target that can last months in order to achieve their criminal ends.

Sources:

A brief history of Malware
Wikipedia
First Base Technologies
Invincea
Marcus Ranum

Next….???

You will note that this article stops at 2011. Don't imagine for a moment that things stopped developing at that point. The Internet and social networks are ubiquitous. Microsoft Windows operating systems are embedded in many ATMs, and in many case are not patched with the latest security updates. There is now a great deal of focus on the Internet of Things (IoT). This is where so-called "smart" devices communicate with each other. Think of smart TV's; smart traffic lights; smart phones (of course); smart central heating or lighting, and even a smart fridge which orders up deliveries for you on direct delivery from Tesco for delivery when it knows you will be at home.

Wonder at the security of our electricity generation and transmission system, and the security of nuclear power stations. Cyber security must surely be one of our greatest concerns. But the oldest and simplest tricks are often the most effective. Look out for the next article on email security to find out more.

John Wells – Webmaster, East Grinstead U3A