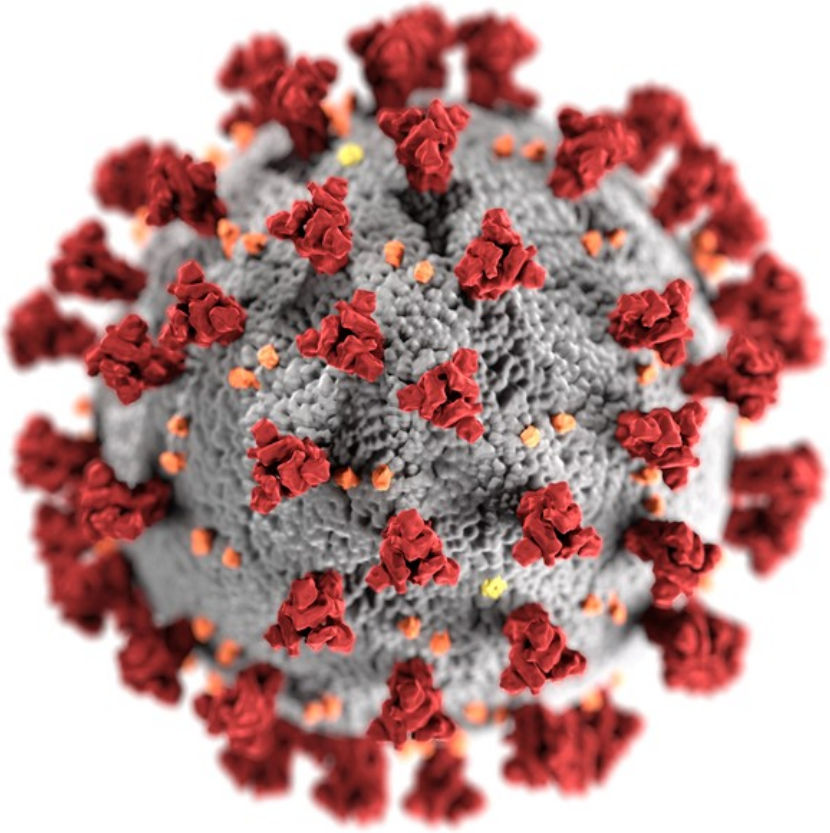
History of Hacking

Part 3: The Computer Virus

By Bruce Nikkel

Published in HISTEC Journal, a publication by the Swiss computer museum Enter (https://enter.ch).

This is part three of a four part series on the history of computer hacking. In the first two articles we covered the early hacking of global telephone switching systems and hacking with dial-up modems. This article describes the history of the computer virus.

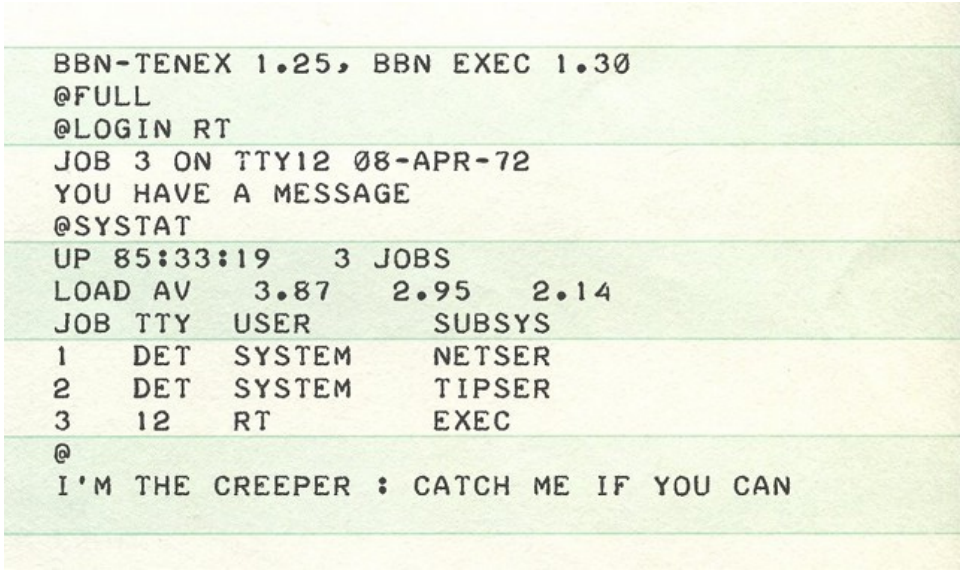


Centers for Disease Control and Prevention (CDC)

We are all tired of reading about viruses, but this article was planned long before the current health crisis started. The comparison of biological viruses with certain types of computer code was due to the similarities in behavior. A virus spreads through different forms of contact, reduces functionality in the infected body, causes unwanted symptoms, and can be difficult to cure (remove). Even virus prevention has similarities, instead of masks computers have firewalls, and instead of vaccinations computers have anti-virus software. Company IT departments even use the word *quarantine* to describe separating infected computers from a network of "healthy" computers.

The use of the word "virus" for referring to certain types of computer code was described in a paper in the mid-1980s by Fred Cohen. A *worm* is a virus that self replicates to other computers over a network. A Trojan horse is reference to Greek mythology, where a person receives something (a file or link) that appears harmless, but later executes malicious code on their computer. The word *Malware* was later proposed as a more general term for all malicious computer software. Other examples of malicious or unfriendly software are spyware, adware, ransomware, or forkbombs. The first computer viruses were developed by computer scientists, academics, and hobbyists. The purpose was to learn, experiment, and research software that could self-replicate or be malicious. Virus code was written as a proof of concept, and not intended to inflict harm.

One of the first examples of a self replicating program was the *Creeper* worm. It was created in the early 1970s and infected networked computers with the TENEX operating system. The Creeper was harmless and simply printed a message that said "I'M THE CREEPER : CATCH ME IF YOU CAN". A program called *Reaper* was later written to delete the Creeper code.



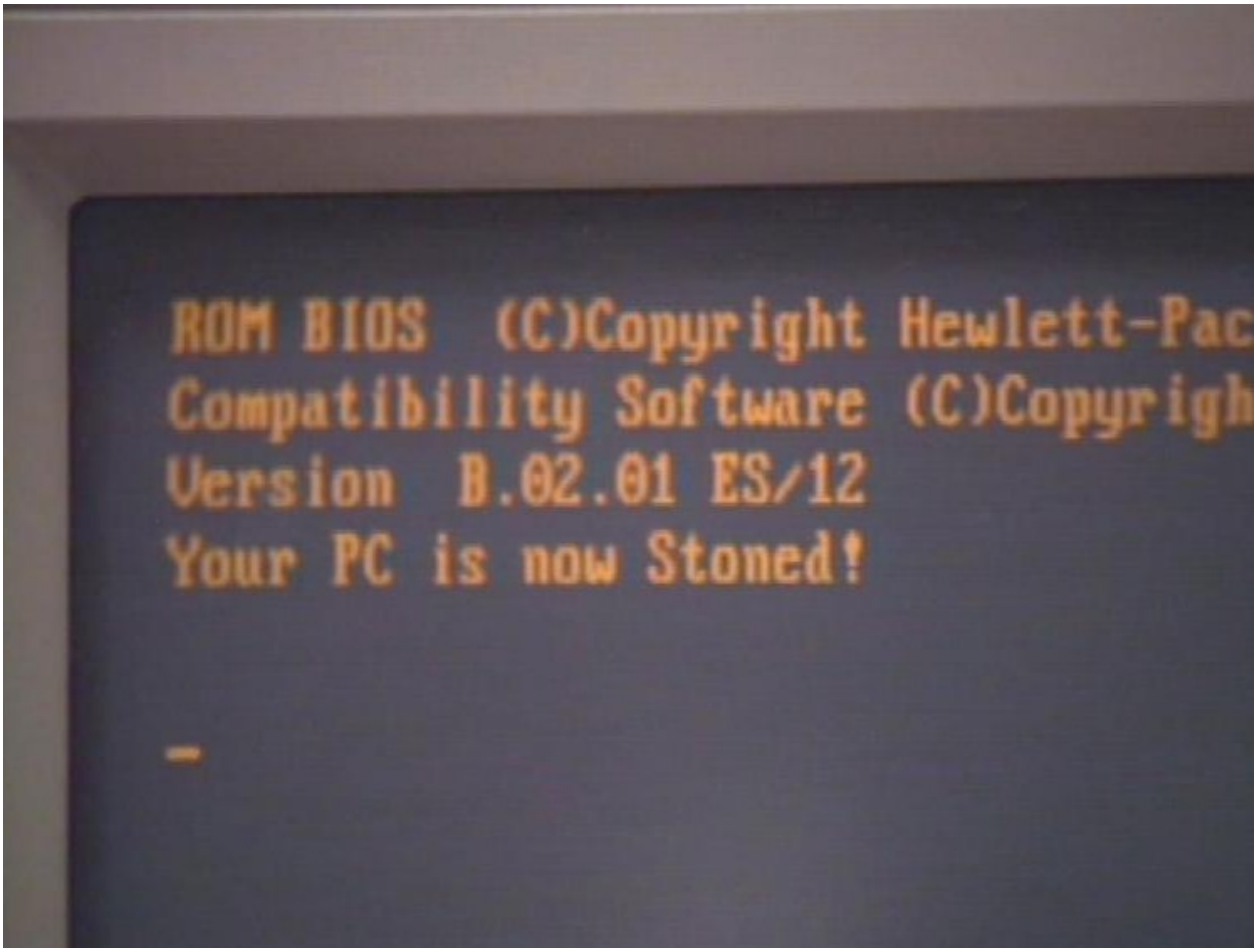
Creeper Worm Output

One of the first worms to cause widespread disruption was the *Morris Worm*, written by student Robert Tappen Morris, in 1988. This was also the first malicious code to attract high profile attention of both the news media and law enforcement (the FBI). The Morris worm used a buffer overflow vulnerability in the finger daemon and exploited debug functionality left enabled in the sendmail daemon. The code only affected BSD UNIX systems and consumed resources, it didn't delete or steal any information. Within 24 hours of being released the worm had brought the Internet to a standstill. This incident motivated the creation of CERTs (Computer Emergency Response Teams) around the world, and was the birth of the malware analysis and reverse engineering field that is still active today.

As Personal Computers grew in popularity, so did PC viruses. Initially the viruses were written by people trying to be funny or mischievous. These viruses were mostly harmless, at worst they were annoying. PC viruses typically spread by floppy diskettes or software downloaded from BBS systems (as described in my last HISTEC article). When the copied or downloaded programs ran, they would infect the new system. One example was the *Joshi* boot sector virus. On January 5th of every year, the virus became active and required the user to type "Happy Birthday Joshi" before they could continue.

Joshi Virus

The *stoned* virus is an example of a harmless but annoying virus which infected the boot sector of hard disks and floppies. The stoned virus became active at random boots, leaving the message "Your PC is now Stoned!". There were many variations of the Stoned virus following the original version.



Stoned Virus

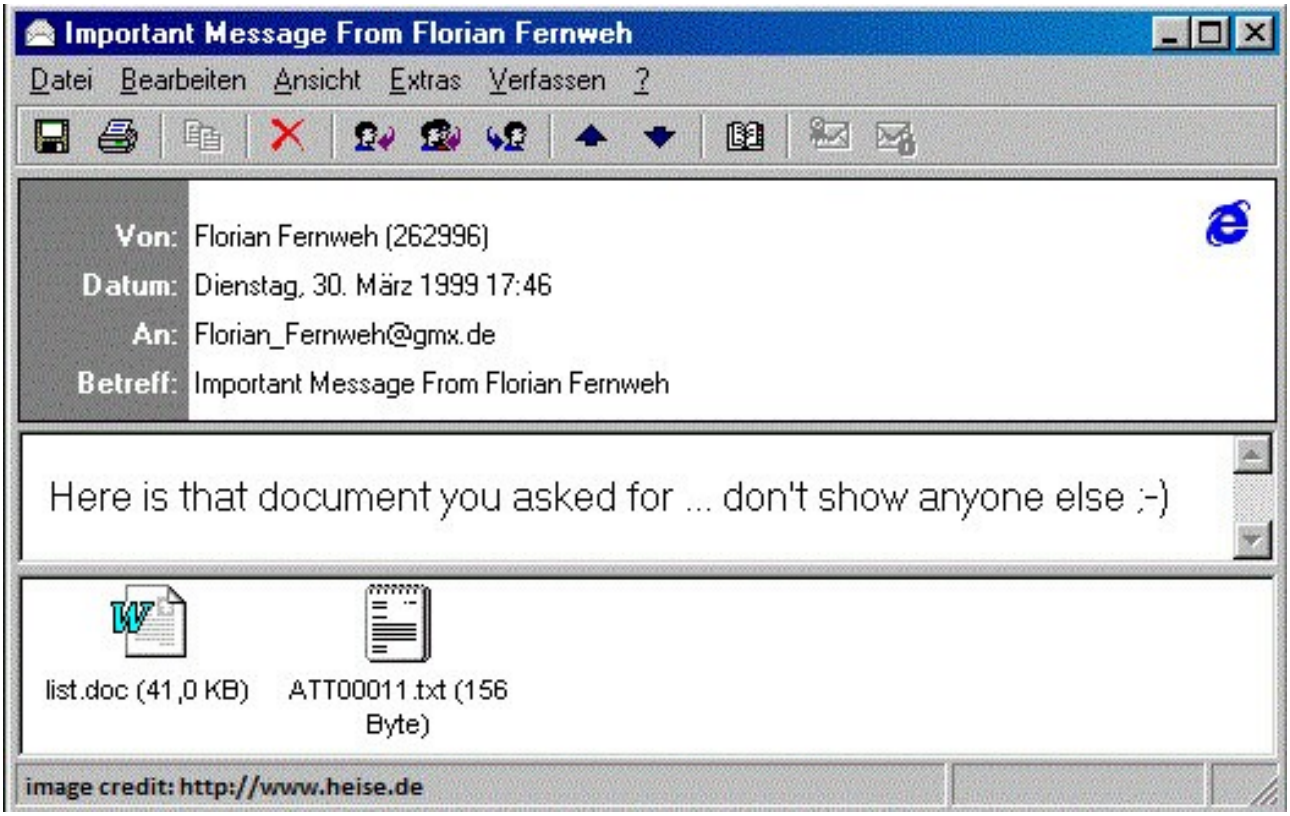
The first virus scanners and anti-virus programs were created with pattern detection to find and remove viruses. But virus writers were aware of this and looked for ways to avoid detection. A common method to avoid detection was to dynamically modify the executable binary so each infected machine would appear to have a unique version (called polymorphic viruses). This drastically reduced the chances of detection based on pattern matching.

The growth of the internet changed how viruses were distributed. It was trivial to send people emails with malicious attachments or web links to malicious executable files on websites. People who opened the attachments or clicked the links became infected. Another method of client infection is called a *drive-by* infection, where people are surfing the Internet and visit a compromised website

containing malicious code that is unwittingly downloaded to the victim. All of these methods are still in use today.

Viruses not only affected end-user clients, they also affected server infrastructure. In the early days of the Internet, servers were less protected (no firewalls), configuration was not defensive (insecure default settings), and software vulnerabilities made exposed services easy to exploit. One example is the *SQL Slammer* which exploited a bug in Microsoft SQL Server and caused widespread disruption in 2003. The SQL Slammer is an example of a virus causing Denial of Service (DoS) and used the UDP protocol to replicated itself as fast as possible.

As people started using firewalls and anti-virus programs, virus writers needed a new way to infect users. Feature rich applications and office programs were starting to provide advanced scripting and macro capability which (at the time) was not monitored by anti-virus programs. This led to the creation of the macro virus which infected office documents. A famous macro virus launched in 1999 was Melissa which used MS-Word macros to replicate itself. A person opening an attachment with a Melissa infected Word document would cause copies of the infected document to be sent to their email contacts. This overloaded email systems around the world.



Melissa Virus

One problem with typical virus distribution was that after a virus was released, there was no way to control it. The idea of a central *Command & Control* (C&C or C2) server solved this problem and allowed malware to be managed while it was in an active state. The malware on infected computers, called *bots*, stayed in contact with a C&C server which provided commands, configuration, and other instructions. Large numbers (hundreds or thousands) of infected PCs under central control is called a *botnet* and can be remotely controlled by a single person called a *bot herder*. Using a C&C also allowed malware to be updated with new versions that were less detectable by anti-virus programs. The botnet management was easy and often used comfortable web interfaces. The SpyEye botnet management panel is a good example where a hacker could steal passwords, credit cards, emails, make screenshots, a perform other botnet maintenance tasks.

Figure 1: SpyEye Botnet Management Panel with 10k bots in 2011

In the mid-2000s criminal gangs became interested in malware as a way to steal credit cards and access online bank accounts. Organized criminal gangs would create or rent botnets which used *web-injects* to manipulate a user's browser while they were logged into their bank. The malware would allow criminals to make fraudulent payments without the victim noticing.

Government intelligence agencies also had an interest in using malware for the purpose of covert monitoring, stealing information, or causing disruption. The Edward Snowden leaks of 2013 reveal the use of state sponsored malware. This is often called an APT or Advanced Persistent Threat. The most famous state sponsored malware used for disruption was *Stuxnet* which was suspected of causing damage to Iran's nuclear program.

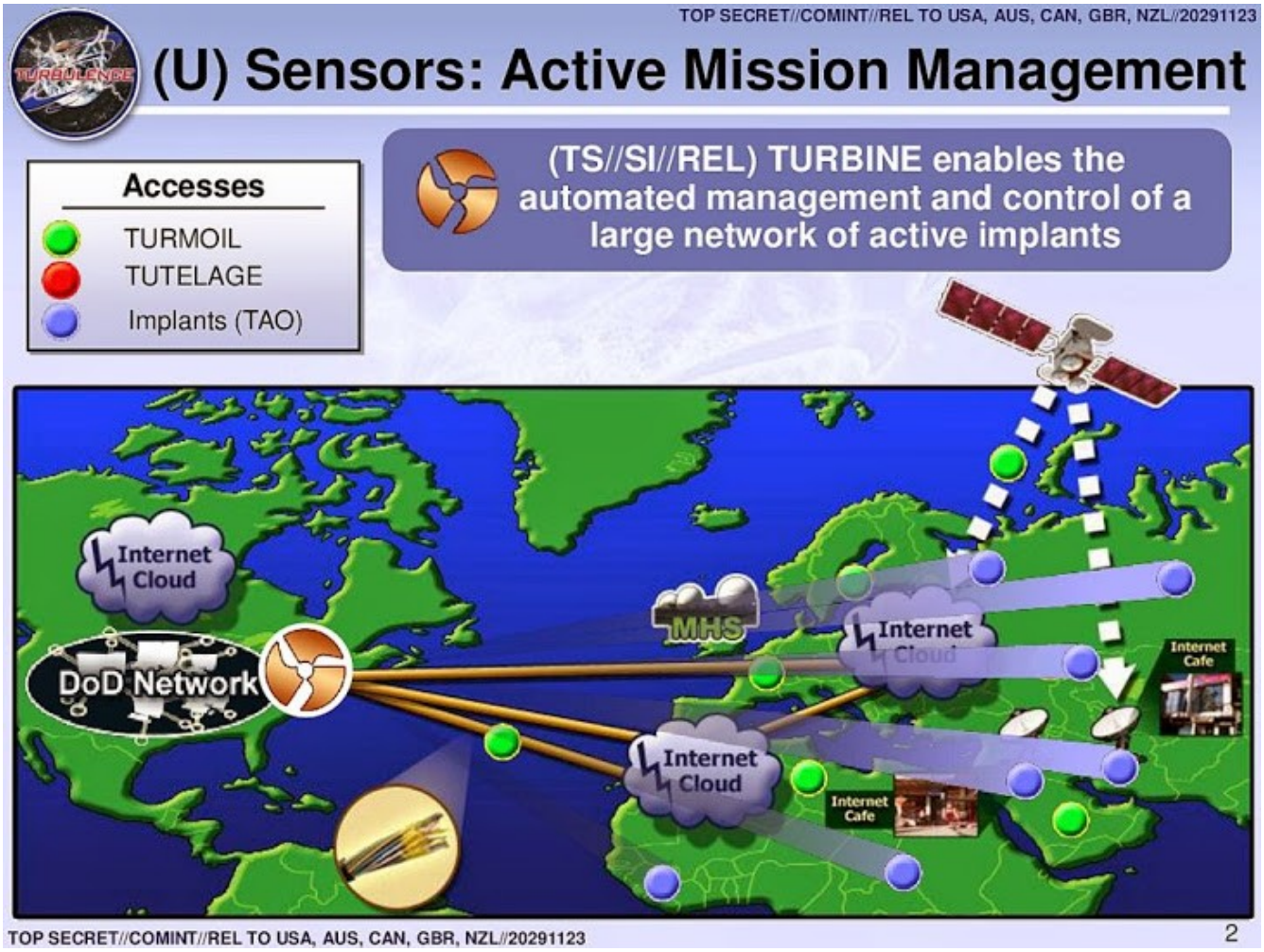
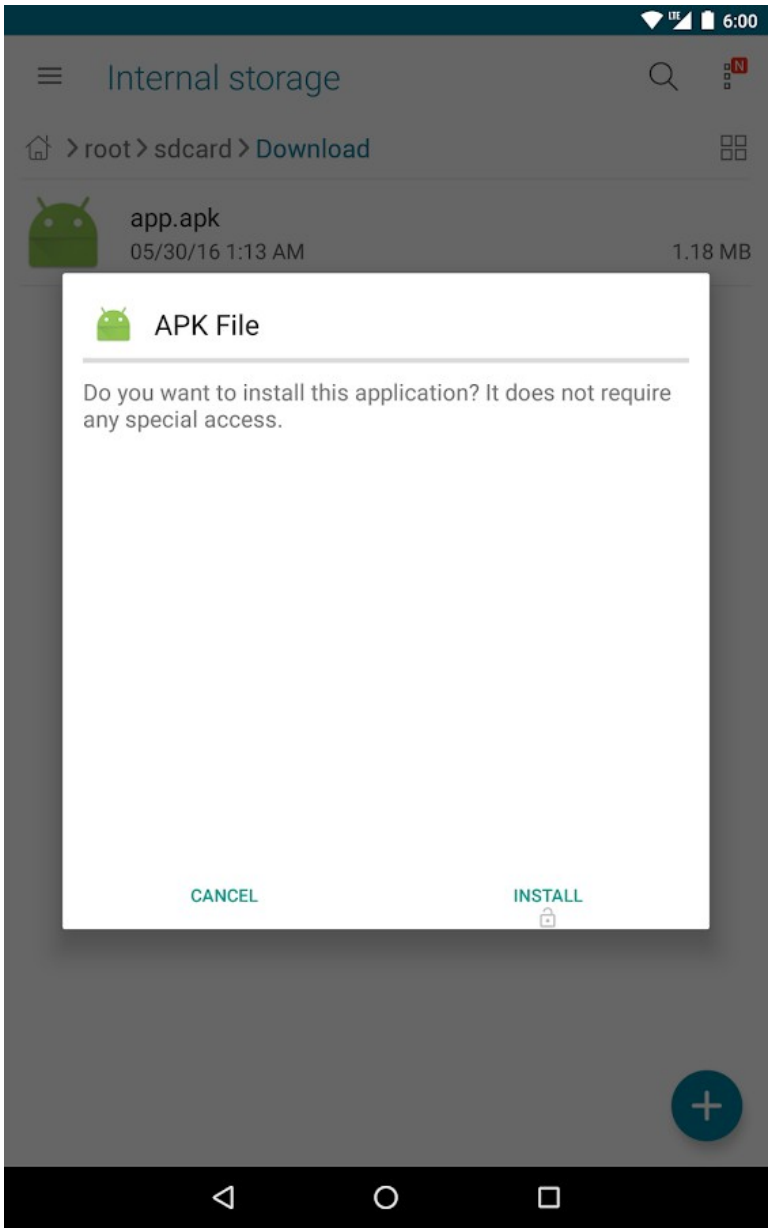


Figure 2: Snowden leak showing government malware implants

As smart phones became popular, criminals started to focus on mobile malware. Most mobile malware was written for Android (Apple was more difficult because they kept stricter control over the hardware, OS, and app stores). Popular mobile malware used an *overlay attack* which intercepted the finger tapping and presented fake screen activity. Mobile malware was used to steal passwords, PINs, intercept SMS messages, and more. This was especially interesting for criminal gangs trying to steal the MTAN for banking applications. A phone could be infected by sending the victim a link an APK, which is an Android software

package. If the user agreed to install it, the phone would become infected. These techniques are still in use today.



Google APK Install

Malware called *Ransomware* encrypts a user's files and then demands a ransom be paid (usually in Bitcoin today) to get the decryption key. Criminals expected if the user had no backups and the files were valuable enough, they would pay. One of the earliest ransomware viruses was in the late 1980s which was distributed on floppy diskette to AIDS researchers. The virus encrypted files and demanded a payment of $189 be sent to a post office box in Panama. The first popular modern ransomware attack was *CryptoLocker* in 2013.

Cryptolocker Ransomware

There are so many interesting and famous viruses, we can't possibly describe them all. For example, Brain, the ILOVEYOU virus, the Zeus banking trojan, MyDoom, Nimda (admin spelled backwards), CodeRed, and many, many others.

Viruses and malware will remain a problem in the future. Even today we are seeing not just software but also hardware vulnerabilities that can be exploited (for example, Heartbleed and Spectre). As hardware becomes more complex and poorly secured IoT devices proliferate, there will be more forms of malware created in the future.

Resources:

Computer viruses: Theory and experiments, Fred Cohen
Elsevier Computers & Security, Volume 6, Issue 1, February 1987
https://doi.org/10.1016/0167-4048(87)90122-2

The Internet Worm Program: An Analysis
Eugene H. Spafford
Purdue Technical Report CSD-TR-823, November 1988
https://spaf.cerias.purdue.edu/tech-reps/823.pdf

The Virus Information Summary List (VSUM):
(Includes 7 viruses suspected of originating in Switzerland)
Patricia Hoffman
http://wiw.org/~meta/vsum/

The Malware Museum:
Mikko Hypponen
http://archive.org/details/malwaremuseum&tab=collection

The History and Evolution of Computer Viruses
Mikko Hypponen
DEF CON 2011
https://youtu.be/yswPIwDFYDY

Der Artikel wurde von Florence Kunz übersetzt. Der englische Originalartikel befindet sich auf:
https://digitalforensics.ch/nikkel20d.pdf

Original English version can be found here:
https://digitalforensics.ch/nikkel20d.pdf