Social media security risks

Timo Ojala, Petteri Manninen,
Jani Haippo, Ilkka Peuron

Social media security risks

- Distribution of malware through social media
- Reliability of the Social media platform itself
  - Selling customer data?
  - Security?
- Social engineering
  - Phishing

Distribution of malware through social media

- Very large userbase
  - Lots of potential victims
  - Amount of moderation?
- Links
- Malware disguised as something else

An example of malware: Keyloggers

- Keylogger is a program that records key struck on a keyboard
  - This is usually done without the person typing on the keyboard noticing it
- Can be used to record the "users" usernames and passwords
  - This can undermine a lot of security based on usernames and passwords
- Keylists are a good countermeasure against keyloggers

Hypervisor-based:

- The keylogger can theoretically reside in a malware hypervisor running underneath the operating system, which remains untouched. It effectively becomes a virtual machine. Blue Pill is a conceptual example.

Kernel-based:

- This method is difficult both to write and to combat. Such keyloggers reside at the kernel level and are thus difficult to detect, especially for user-mode applications. They are frequently implemented as rootkits that subvert the operating system kernel and gain unauthorized access to the hardware, making them very powerful. A keylogger using this method can act as a keyboard device driver for example, and thus gain access to any information typed on the keyboard as it goes to the operating system.

API-based

- These keyloggers hook keyboard APIs; the operating system then notifies the keylogger each time a key is pressed and the keylogger simply records it. Windows APIs such as GetAsyncKeyState(), GetForegroundWindow(), etc. are used to poll the state of the keyboard or to subscribe to keyboard events.

These types of keyloggers are the easiest to write, but where constant polling of each key is required, they can cause a noticeable increase in CPU usage, and can also miss the occasional key. A more recent example simply polls the BIOS for pre-boot authentication PINs that have not been cleared from memory.

Form grabbing based

- Form grabbing-based keyloggers log web form submissions by recording the web browsing onsubmit event functions. This records form data before it is passed over the Internet and bypasses HTTPS encryption.

Memory injection based

- Memory Injection (MitB)-based keyloggers alter memory tables associated with the browser and other system functions to perform their logging functions. By patching the memory tables or injecting directly into memory, this technique can be used by malware authors who are looking to bypass Windows UAC (User Account Control). The Zeus and Spyeye Trojans use this method exclusively.

Packet analyzers

- This involves capturing network traffic associated with HTTP POST events to retrieve unencrypted passwords.

Countermeasures against keyloggers

- Anti-virus and anti-spyware programs can detect some keyloggers but since some keyloggers are legitimate under some circumstances they are usually not 100% effective against all keyloggers.
- Anti keylogger programs are specifically designed to detect keyloggers and are better at detecting them than other anti virus software.

Automatic form filler programs

- Automatic form filler programs are programs which are designed for browsers, they fill in forms and login information without using a keyboard or a clipboard, thus reducing the possibility of private data being recorded.

Consequences of being keylogged

- A hacked facebook profile is not really a catastrophe for a user since it can be recovered and usually has no real monetary value.
- Problems may occur if the user has been using the same password for something like Steam or a Paypall account, which are usually goldmines for hackers because of the fact that they often have the users credit card information attached.

- https://www.youtube.com/watch?v=5xy9w9-hzrs