SECURITY A TO Z THE MOST IMPORTANT TERMS

Part 2: E to R

F-Secure

UNDERSTAND THE OFFICIAL TERMINOLOGY.

This is F-Secure Labs.

Learn more about the most important security terms with our official explanations from F-Secure Labs.

Part 2: E to R

ENCRYPTION

The use of a cipher or algorithm to transform data, such as a program's code, into an unintelligible form. There are many different ways to perform encryption, based on the algorithm or cipher used. Some examples of encryption algorithms include ROT13 and the Vigenere cipher. Encryption usually requires a specific piece of information (a 'key') in order to transform the encrypted information back to a usable state when necessary. The simplest form of encryption uses a static unchanging key; more sophisticated encryption may involve changes in the key itself as well as the code to be transformed. Virus writers use encryption to create encrypted viruses, which are harder for antivirus programs to detect. Once installed, the encrypted virus uses the key to decrypt its own code and execute it.

E

EXPLOIT VS EXPLOIT KIT

Exploit: An object - a program, a section of code, even a string of characters - that takes advantage of a vulnerability in a program or operating system to perform various actions. An exploit is almost always used in a malicious context. If successfully used, exploits can provide an attacker with a wide range of possible actions, from viewing data on a restricted-user database to almost complete control of a compromised system. Exploit kit: A server which has a selection of exploits targeting vulnerabilities in several softwares or versions, and a capability to analyze the client and select proper exploit. Typical exploit kit has a selection of exploits for different web browsers and plugins.

HACKING

Act of breaking into workstations, servers or mobile phones through a network or other connection. A typical example of hacking would be someone finding a vulnerability in a server and then using an exploit against that vulnerability to access the system.

HACKTIVISM

Type of activism which uses hacking in order to push some agenda. Most typical cases of hacktivism involve website defacement in which attackers gain control of a web page and change it to show political or other messages. Twitter, Facebook and other social media accounts are often seized for hacktivism purposes.

H

HARDENING

Improving the security of a server or workstation by modifying security, server or application settings. A typical example of hardening would be to reduce an attack surface by disabling features that are not needed by a client or server application. For example, disabling JavaScript from a PDF reader will break most PDF exploits.

HEURISTICS

Reasoning based automation that is used to detect malware or other attacks. Both clients and servers in security clouds use heuristics. Basically, heuristics model human decisions for computer programs, allowing those programs to automate decision making processes. F-Secure uses heuristics to detect malware and other types of attacks.

K

KEYLOGGER

A program or hardware component that surreptitiously monitors and stores all the strokes typed into a device's keyboard. Some keylogger programs will also forward the stored information to an external server for easier retrieval by the attacker. Keyloggers are typically used by attackers to steal vital information such as personal details, credit card details, online account login credentials, and so on. The stolen information can then be used to perpetrate crimes such as identity theft, online fraud, monetary theft, and so on. Keylogger programs are typically installed on a device by other malware, though they may also be manually installed by an attacker with physical access to a device. Hardware components must be manually installed.

L

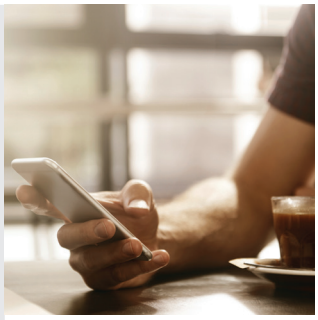
LAYERED PROTECTION

A protection principle in which multiple methods are used to protect against attacks. Layered protection is based on the reality that it is almost impossible to make one security solution that can stop 100% of attacks. Providing layered protection requires the use of multiple technologies in security solutions.

M

MAN-IN-THE-MIDDLE ATTACK

A type of attack that involves an undetected third-party actively eavesdropping and controlling communications between two systems. The specific technical details of how the attack is performed depends on the type of communication being intercepted (wireless, Internet, mail, etc.), but for it to be successful, the attacker must be able to impersonate each side of the dialogue and convince them that the communication is private and authentic. MITM attacks are usually done in order to intercept or modify messages sent between the two systems, or to inject false information.



O

ONLINE SCAMS = PHISHING

A type of social engineering attack in which fraudulent communications are used to trick the user into giving out sensitive information, such as passwords, account information, and other details. Phishing is a criminal activity in many jurisdictions. A phishing attack usually involves a fake communication, often supposedly from a trusted corporation or institution that requires some kind of response from the user. Usually, the subject matter is enticing or alarming, to motivate the user into complying. Victims are then directed to a specific (usually fraudulent) website in order to trick them into providing information to the attackers. Phishing attempts are most commonly done via email, but attempts made by instant messages, SMS messages, and even voicemail are also known. Malware may also drop phishing communications as part of their payload. Phishing can often be executed using spam emails, but targeted phishing attacks can also occur. The information stolen can have considerable value to a criminal, but its loss can be even more significant to the victim. Such information theft is rapidly becoming a major concern for law enforcement agencies and web service operators worldwide.

P

PATCHING

A program or piece of code issued by a program vendor to fix issues in a program or operating system. Patches are usually issued to fix bugs, vulnerabilities or usability issues. A good security practice is to install patches as soon as possible after they are released. Unfortunately, for many businesses and home users, there may be a significant delay between the time a patch is released and when it is installed on an affected application or machine, leaving them vulnerable to attacks.

R

RANSOMWARE

A malicious application that steals or encrypts a user's data or system, then demands a ransom payment to restore the data or normal system access. Ransomware programs typically encrypt files on a computer or device, then displays a message stating that the user needs to pay a certain sum in a specified manner. The specifics of how the encryption is done, the kind of message displayed, and the payment method to be used usually differ based on the ransomware family involved. This form of extortion works on the assumption that the user values the data enough to pay for its recovery. However, there is no guarantee of actual recovery, even after a payment is made. As encryption is usually extremely difficult to break, the best safeguard against losing access to critical data this way is to keep up-to-date backups of your files in a separate, unconnected location or device. Up-to-date antivirus protection and user caution are also key in avoiding unintentional contact with ransomware.

REMOTE CODE EXECUTION

In computer security, remote code execution means that an outside party being able to run arbitrary commands on a target machine or in a target process, almost always with malicious intent. Remote code execution is usually the goal of a system or program exploit, as it essentially means an attacker can take complete control of the compromised machine.

REPUTATION

Information about whether an application, URL or some object is malicious, known to be clean, or unknown. Reputation is the information that is used for whitelisting or blacklisting applications.

LEARN MORE ABOUT F-SECURE LABS ON OUR WEBSITE.

BUSINESS SECURITY INSIDER BY F-SECURE
Your information source for the latest news and insights into cyber security and IT security for businesses.

WEBLOG - LATEST FROM THE LABS
Updates on research done by F-Secure Labs, and views on the latest developments in information security and digital technology.

GET SOLUTIONS & GET INFORMED
Find a solution for a security concern with one of our free tools, or learn more about threats and products in our descriptions and advisories.

1

REMOVAL TOOLS
Use these free tools to scan and remove malicious programs.

2

THREAT DESCRIPTIONS
Details of threats identified by F-Secure Labs.

3

SECURITY ADVISORIES
Details and fixes of all the vulnerabilities affecting F-Secure products.

F-Secure