2018 National Seminar

Hacking & Phishing Glossary:
2018 Annual National Seminar

Adware - Adware can mean the software that automatically generates advertisements in a program that is otherwise free, such as an online video game. But in this context it more commonly means a kind of spyware that tracks your browsing habits covertly to generate those ads.

Anonymous - A non-hierarchical hacktivist collective, Anonymous uses hacking (and arguably cracking) techniques to register political protest in campaigns known as "#ops." Best known for their distributed denial of services (DDoS) attacks, past activities have included attacks against the Church of Scientology; Visa, Paypal, and others who withdrew their services from WikiLeaks' Julian Assange after that group began releasing war documents; #OpTunisia and others purporting to support the Arab Spring; and a campaign that brought down the website of the Westboro Baptist Church. #Ops are usually marked with the release of a video of a reader in a Guy Fawkes mask using a computer generated voice. Offshoot groups include AntiSec and LulzSec.

AntiSec - An Anonymous splinter group, AntiSec was best known for the hack of security firm Stratfor, publishing credit card numbers and email addresses taken from the company's site. Jeremy Hammond was arrested for alleged Anti-Sec activities under the alias sup_g.

Back Door - A back door, or trap door, is a hidden entry to a computing device or software that bypasses security measures, such as logins and password protections. Some have alleged that manufacturers have worked with government intelligence to build backdoors into their products. Malware is often designed to exploit back doors.

Black hat - Black hat hackers are those who engage in hacking for illegal purposes, often for financial gain, though also for notoriety. Their hacks (and cracks) result in inconvenience and loss for both the owners of the system they hack and the users.

Bot - A program that automates a usually simple action so that it can be done repeatedly at a much higher rate for a more sustained period than a human operator could do it. Like most things in the world of hacking, bots are, in themselves, benign and used for a host of legitimate purposes, like online content delivery. However, they are often used in conjunction with cracking, and that's where their public notoriety comes from. Bots can be used, for instance, to make the content calls that make up denial of service attacks. Bot is also a term used to refer to the individual hijacked computers that make up a botnet.

Botnet - A botnet is a group of computers controlled without their owners' knowledge and used to send spam or make denial of service attacks. Malware is used to hijack the individual computers, also known as "zombies," and send directions through them. They are best known in terms of large spam networks, frequently based in the former Soviet Union.

Brute Force Attack - Also known as an exhaustive key search, a brute force attack is an automated search for every possible password to a system. It is an inefficient method of hacking compared to others like phishing. It's used usually when there is no alternative. The process can be made shorter by focusing the attack on password elements likely to be used by a specific system.

Clone Phishing - Clone phishing is the modification of an existing, legitimate email with a false link to trick the recipient into providing personal information.

Code - Code is the machine-readable, usually text-based instructions that govern a device or program. Changing the code can change the behavior of the device or program.

Compiler - A compiler is a program that translates high-level language (source code in a programming language) into executable machine language. Compilers are sometimes rewritten to create a back door without changing a program's source code.

Cookie - Cookies are text files sent from your Web browser to a server, usually to customize information from a website.

Cracking - To break into a secure computer system, frequently to do damage or gain financially, though sometimes in political protest.

Hacking & Phishing Glossary:
2018 Annual National Seminar

Denial of Service Attack (DoS) - DoS is used against a website or computer network to make it temporarily unresponsive. This is often achieved by sending so many content requests to the site that the server overloads. Content requests are the instructions sent, for instance, from your browser to a website that enables you to see the website in question. Some have described such attacks as the Internet equivalent of street protests and some groups, such as Anonymous frequently use it as a protest tool.

Distributed Denial of Service Attack (DDoS) - A DoS using a number of separate machines. This can be accomplished by seeding machines with a Trojan and creating a botnet or, as is the case with a number of Anonymous attacks, by using the machines of volunteers.

Doxing - Discovering and publishing the identity of an otherwise anonymous Internet user by tracing their online publically available accounts, metadata, and documents like email accounts, as well as by hacking, stalking, and harassing.

Firewall - A system using hardware, software, or both to prevent unauthorized access to a system or machine.

Gray Hat - Just like the rest of life, hacking is often less black or white than it is gray. The term gray hat hacker reflects that reality. A gray hat hacker will break the law in the pursuit of a hack, but does not do so maliciously or for personal gain. Many would argue Anonymous are gray hats.

Hacking - Hacking is the creative manipulation of code, distinguished, albeit amorphously, from programming by focusing on the manipulation of already written code in the devices or software for which that code was already written. Metaphorically it extends to social engineering in its manipulation of social code to effect change. Many prefer to use the term cracking to describe hacking into a machine or program without permission. Hackers are sometimes divided into white hat, black hat, and gray hat hackers.

Hacktivist - A hacker whose goals are social or political. Examples range from reporting online anonymously from a country that attacks free speech to launching a DDoS campaign against a company whose CEO has issued objectionable statements. Not to be confused with slacktivism, which refers to push-button activism in which a supporter of a social or political campaign's goals does nothing but register their support online, for instance by "liking" a Facebook page.

Hash - A hash is a number generated by an algorithm from a string of characters in a message or other string. In a communications system using hashes, the sender of a message or file can generate a hash, encrypt the hash, and send it with the message. On decryption, the recipient generates another hash. If the included and the generated hash are the same, the message or file has almost certainly not been tampered with.

IP - Internet protocol address. It's the distinctive numeral fingerprint that each device carries that's connected to a network using Internet Protocol. If you have a device's IP you can often identify the person using it, track its activity, and discover its location. These addresses are apportioned by the regional Internet registries of the IANA (the Internet Assigned Numbers Authority). Crackers can use knowledge of your IP address to your computer via one of its ports, the points that regulate information traffic flow.

IRC - Internet relay chat is a protocol used by groups and for one-on-one conversations, often utilized by hackers to communicate or share files. Because they are usually unencrypted, hackers sometimes use packet sniffers to steal personal information from them.

Keystroke Logging / Keylogger - Keystroke logging is the tracking of which keys are pressed on a computer (and which touchscreen points are used). It is, simply, the map of a computer/human interface. It is used by gray and black hat hackers to record login IDs and passwords. Keyloggers are usually secreted onto a device using a Trojan delivered by a phishing email.

Logic Bomb - A virus secreted into a system that triggers a malicious action when certain conditions are met. The most common version is the time bomb.

LulzSec - LulzSec is an Anonymous offshoot. It's best-known actions were hacking user information from the website of Sony Pictures and for allegedly shutting down the CIA website with a DDoS attack. LulzSec's best known, however, for Hector Xavier Monsegur, a.k.a. "Sabu," a hacker turned FBI informant, whose intel led to the arrest of four other LulzSec members. He faces the possibility of a long prison term despite his cooperation.

Malware - A software program designed to hijack, damage, or steal information from a device or system. Examples include spyware, adware, rootkits, viruses, keyloggers, and many more. The software can be delivered in a number of ways, from decoy websites and spam to USB drives.

Hacking & Phishing Glossary:
2018 Annual National Seminar

Master - The computer in a botnet that controls, but is not controlled by, all the other devices in the network. It's also the computer to which all other devices report, sending information, such as credit card numbers, to be processed. Control by the master of the bots is usually via IRC.

NSA - The National Security Agency is the U.S. intelligence group dedicated to intercepting and analyzing data, specifically electronic data.

Payload - The cargo of a data transmission is called the payload. In black hat hacking, it refers to the part of the virus that accomplishes the action, such as destroying data, harvesting information, or hijacking the computer.

Packet Sniffer - Sniffers are programs designed to detect and capture certain types of data. Packet sniffers are designed to detect packets traveling online. Packets are packages of information traveling on the Internet that contain the destination address in addition to content. Packets can be used to capture login information and passwords for a device or computer network.

Phishing - Tricking someone into giving you their personal information, including login information and passwords, credit card numbers, and so on by imitating legitimate companies, organizations, or people online. Phishing's often done via fake emails or links to fraudulent websites.

Remote access - Remote control is the process of getting a target computer to recognize your keystrokes as its own, like changing a TV with a remote control. Gaining remote access allows you to run the target machine completely by using your own, allowing for the transfer of files between the target and the host.

Rootkit - A rootkit is a set of software programs used to gain administrator-level access to a system and set up malware, while simultaneously camouflaging the takeover.

Script Kiddie - A pejorative term for a would-be cracker without technical skills. Script kiddies use prefab cracking tools to attack systems and deface them, often in an attempt to score points with their peers.

Social Engineering - Social engineering is conning people into giving you confidential information, such as passwords to their accounts. Given the difficulty of breaking, 128-bit encryption with brute force, for example, social engineering is an integral element of cracking. Examples include phishing and spear-phishing.

Spam - Unwanted and unsolicited email and other electronic messages that attempt to convince the receiver to either purchase a product or service, or use that prospect to defraud the recipient. The largest and most profitable spamming organizations often use botnets to increase the amount of spam they send (and therefore the amount of money they make).

Spear-phishing - A more focused type of phishing, targeting a smaller group of targets, from a department within a company or organization down to an individual.

Spoofing - Email spoofing is altering the header of an email so that it appears to come from elsewhere. A black hat hacker, for instance, might alter his email header so it appears to come from your bank. IP spoofing is the computer version, in which a packet is sent to a computer with the IP altered to imitate a trusted host in the hope that the packet will be accepted and allow the sender access to the target machine.

Spyware - Spyware is a type of malware that is programmed to hide on a target computer or server and send back information to the master server, including login and password information, bank account information, and credit card numbers.

Syrian Electronic Army - The SEA is a pro-government hacking group, best known for defacing high-profile publications like the New York Times and National Public Radio (and the Daily Dot). Recently, Vice and Krebs on Security have doxed several alleged members of the group. Some have accused them of being less hackers than script kiddies.

Time Bomb - A virus whose payload is deployed at or after a certain time.

Trojan Horse - A Trojan is a type of malware that masquerades as a desirable piece of software. Under this camouflage, it delivers its payload and usually installs a back door in the infected machine.

Virus - Self-replicating malware that injects copies of itself in the infected machine. A virus can destroy a hard drive, steal information, log keystrokes, and many other malicious activities.

Vulnerability - A weak spot hackers can exploit to gain access to a machine.

Hacking & Phishing Glossary:
2018 Annual National Seminar

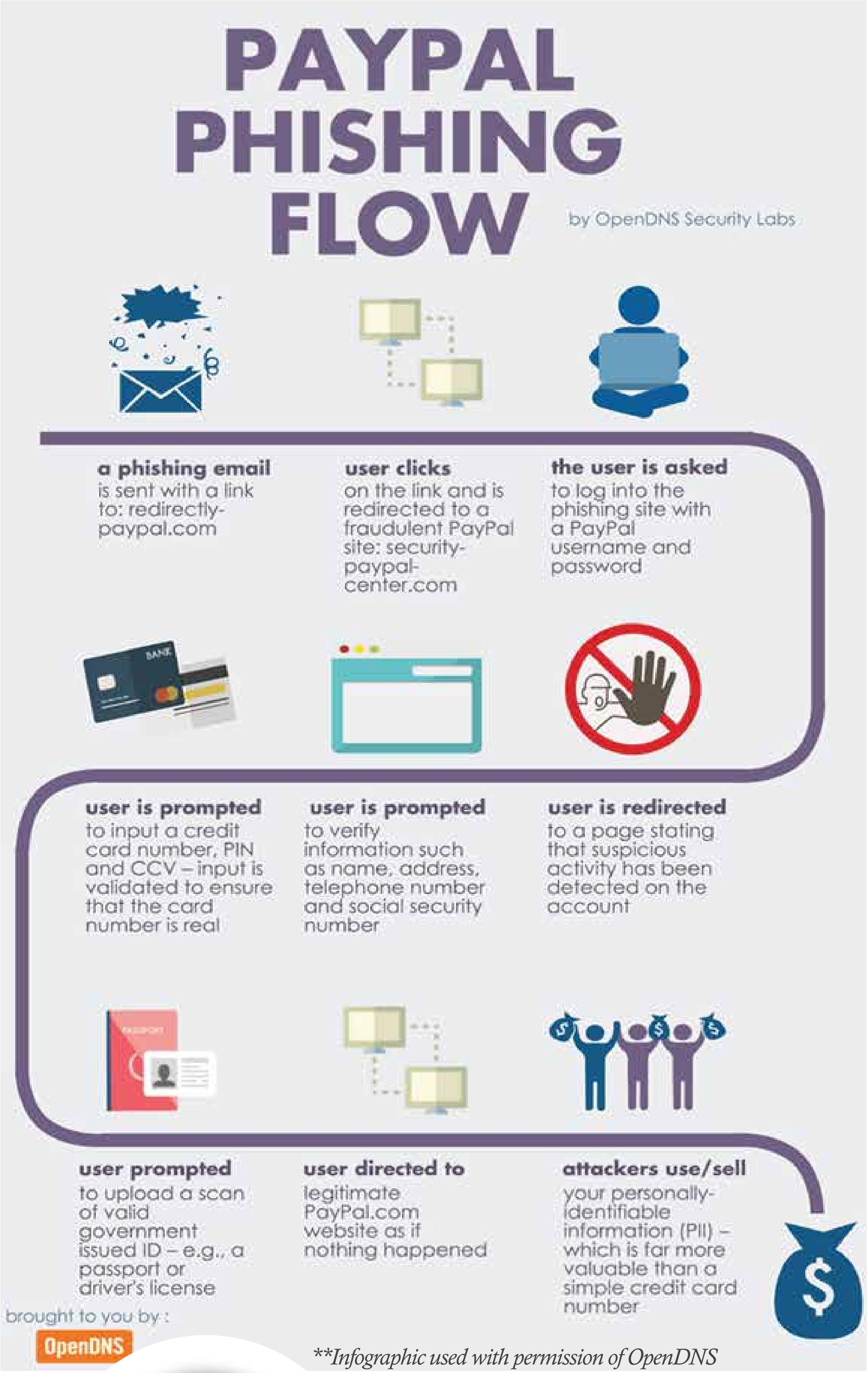
2018 National Seminar

Whaling - Spear-phishing that targets the upper management of for-profit companies, presumably in the hope that their higher net worth will result in either more profit, if the cracker is after financial gain, or that their higher profile will ensure the gray hat hacker more exposure for his or her cause.

White Hat - An ethical hacker who uses his skills in the service of social good. The term may also be applied to a hacker who helps a company or organization, or users in general, by exposing vulnerabilities before black hat hackers do.

Worm - Self-replicating, standalone malware. As a standalone it does not report back to a master, and unlike a virus it does not need to attach itself to an existing program. It often does no more than damage or ruin the computers it is transmitted to. But it's sometimes equipped with a payload, usually one that installs back doors on the infected machine to make a botnet.

Zero Day Exploit - A zero day attack is a previously unknown vulnerability in a system. A zero day attack is the first such use of the exploit by a cracker.



PAYPAL PHISHING FLOW

by OpenDNS Security Labs

a phishing email is sent with a link to: redirectly-paypal.com

user clicks on the link and is redirected to a fraudulent PayPal site: security-paypal-center.com

the user is asked to log into the phishing site with a PayPal username and password

user is redirected to a page stating that suspicious activity has been detected on the account

user is prompted to verify information such as name, address, telephone number and social security number

user is prompted to input a credit card number, PIN and CCV – input is validated to ensure that the card number is real

user prompted to upload a scan of valid government issued ID – e.g., a passport or driver's license

user directed to legitimate PayPal.com website as if nothing happened

attackers use/sell your personally-identifiable information (PII) – which is far more valuable than a simple credit card number

brought to you by : OpenDNS

***Infographic used with permission of OpenDNS*

**This glossary contains terminology and explanations of concepts relevant to various emerging technologies. The purpose of the glossary is to inform the reader of the most commonly used vocabulary terms in the cyber world. This glossary was compiled from various sources readily available on the Internet.*

To receive updates on future events and other Commission activities, visit us on Twitter @TheUSSCgov, or subscribe to e-mail updates through our website at www.ussc.gov. For guidelines questions, call our Helpline at 202.502.4545, and to request training, email us at training@ussc.gov.

UNITED STATES SENTENCING COMMISSION

The United States Sentencing Commission, an independent agency in the judicial branch of the federal government, was organized in 1985 to develop a national sentencing policy for the federal courts. The resulting sentencing guidelines provide structure for the courts' sentencing discretion to help ensure that similar offenders who commit similar offenses receive similar sentences.