GLOSSARY

This glossary was made to help take some of the confusion out of the terms often used when referring to cyber crime. When dealing with crackers, black hats and hackers, what you don't know can hurt you, so please take a moment to familiarize yourself with these terms and tools of their trade.

Adware – Adware is software designed to force pre-chosen ads to display on your system. Some adware is designed to be malicious and will pop up ads with such speed and frequency that they seem to be taking over everything, slowing down your system and tying up all of your system resources. When adware is coupled with spyware, it can be a frustrating ride, to say the least.

APT: Advanced persistent threats, or APTs, are long-term targeted attacks that break into a network in multiple phases to avoid detection. There are five stages of an APT, which are reconnaissance (researching and understanding the target), incursion (delivering targeted malware), discovery (mapping the target's internal defenses), capture (acquiring data over an extended period) and exfiltration (exploiting captured information).

Back Door – A back door is a point of entry that circumvents normal security and can be used by a cracker to access a network or computer system. Usually back doors are created by system developers as shortcuts to speed access through security during the development stage and then are overlooked and never properly removed during final implementation. Sometimes crackers will create their own back door to a system by using a virus or a Trojan to set it up, thereby allowing them future access at their leisure.

Black Hat – Just like in the old westerns, these are the bad guys. A black hat is a cracker. To add insult to injury, black hats may also share information about the "break in" with other black hat crackers so they can exploit the same vulnerabilities before the victim becomes aware and takes appropriate measures… like calling Global Digital Forensics!

Bot – A bot is a software "robot" that performs an extensive set of automated tasks on its own. Search engines like Google use bots, also known as spiders, to crawl through websites in order to scan through all of your pages. In these cases bots are not meant to interfere with a user, but are employed in an effort to index sites for the purpose of ranking them accordingly for appropriate returns on search queries. But when black hats use a bot, they can perform an extensive set of destructive tasks, as well as introduce many forms of malware to your system or network. They can also be used by black hats to coordinate attacks by controlling botnets.

Botnet – A botnet is a network of zombie drones under the control of a black hat. When black hats are launching a Distributed Denial of Service attack for instance, they will use a botnet under their control to accomplish it. Most often, the users of the systems will not even know they are involved or that their system resources are being used to carry out DDOS attacks or for spamming. It not only helps cover the black hat's tracks, but increases the ferocity of the attack by using the resources of many computer systems in a coordinated effort.

Cookies – A cookie is a small packet of information from a visited webserver stored on your system by your computer's browser. It is designed to store personalized information in order to customize your next visit. For instance, if you visit a site with forms to fill out on each visit, that information can be stored on your system as a cookie so you don't have to go through the process of filling out the forms each time you visit.

Cracker – When you hear the word hacker today, in reality it is normally referring to a cracker, but the two have become synonymous. With its origin derived from "safe-cracker" as a way to differentiate from the various uses of "hacker" in the cyber world, a cracker is someone who breaks into a computer system or network without

authorization and with the intention of doing damage. A cracker may destroy files, steal personal information like credit card numbers or client data, infect the system with a virus, or undertake many others things that cause harm. These are the black hats.

Denial of Service Attack (DOS) – A Denial of Service attack is an attack designed to overwhelm a targeted website to the point of crashing it or making it inaccessible. Along with sheer numbers and frequency, sometimes the data packets that are sent are malformed to further stress the system trying to process the server requests. A successful Denial of Service attack can cripple any entity that relies on its online presence by rendering their website virtually useless.

Distributed Denial of Service Attack (DDOS) – A Distributed Denial of Service attack is done with the help of zombie drones (also known as a botnet) under the control of black hats using a master program to command them to send information and data packets to the targeted webserver from the multiple systems under their control. This obviously makes the Distributed Denial of Service attack even more devastating than a Denial of Service attack launched from a single system, flooding the target server with a speed and volume that is exponentially magnified. As is normally the case with zombie drones and botnets, this is often done without the user of the controlled system even knowing they were involved.

Dumpster Diving – The act of rummaging through the trash of an individual or business to gather information that could be useful for a cyber criminal to gain access to a system or attain personal information to aid them in identity theft or system intrusion. One person's garbage can indeed be a cyber criminal's treasure.

Easter Egg – A non-malicious surprise contained in a program or on a circuit board installed by the developer. It could be as simple as a text greeting, a signature, or an image embedded on a circuit board, or comprise a more complex routine, like a video or a small program. The criteria that must be met to be considered an Easter Egg are that it be undocumented, non-malicious, reproducible to anyone with the same device or software, not be obvious, and above all – it should be entertaining!

Firewall – A firewall is a security barrier designed to keep unwanted intruders "outside" a computer system or network while allowing safe communication between systems and users on the "inside" of the firewall. Firewalls can be physical devices or software-based, or a combination of the two. A well designed and implemented firewall is a must to ensure safe communications and network access and should be regularly checked and updated to ensure continued function. Black hats learn new tricks and exploit new techniques all the time, and what worked to keep them out yesterday may need to be adjusted or replaced over time.

Gray Hat – A gray hat, as you would imagine, is a bit of a white hat/black hat hybrid. Thankfully, like white hats, their mission is not to do damage to a system or network, but to expose flaws in system security. The black hat part of the mix is that they may very well use illegal means to gain access to the targeted system or network, but not for the purpose of damaging or destroying data: they want to expose the security weaknesses of a particular system and then notify the "victim" of their success. Often this is done with the intent of then selling their services to help correct the security failure so black hats can not gain entry and/or access for more devious and harmful purposes.

Hacker – This is the trickiest definition of the group and controversy has followed its use for decades. Originally, the term hacker had a positive connotation and it actually had nothing to do with computer systems. In 1946, the Tech Model Railroad Club of MIT coined the term to mean someone who applies ingenuity to achieve a clever result. Then, when computers came along, "hacker" took on the meaning of someone who would "hack" away on a program through the night to make it better. But in the 80s everything changed, and Hollywood was the catalyst.

When the personal computers onslaught started invading our daily lives, it didn't take long for clever screen-writers to bring the black hat villains of the cyber world to the forefront of our collective consciousness, and they haven't looked back since. They associated our deepest fears with the word hacker, making them the ones that unraveled our privacy, put our safety in jeopardy, and had the power to take everything from us, from our material possessions to our very identities. And they could do it all anonymously, by hacking away in a dark room by the dim light of a computer monitor's glow. Needless to say, right or wrong, it stuck! Even many professionals in the computing field today have finally, albeit grudgingly, given in to the mainstream meaning of the word. "Hacker" has thus become the catch-all term used when in fact it should be "cracker."

Inside attack: For this type of cyberattack, a sophisticated software program may not even be required: Someone with administrative privileges, usually from within the organization, purposely misuses his or her credentials to gain access to confidential company information. Ex-employees in particular present a threat if they left the company on bad terms, so your business should have a protocol in place to revoke all access to company data immediately upon an employee's termination. Inside attacks can also happen in the form of a hacker posing as a representative of a company your business works with to gain access to sensitive data.

Keylogger – A keylogger is a non-destructive program that is designed to log every keystroke made on a computer. The information that is collected can then be saved as a file and/or sent to another machine on the network or over the Internet, making it possible for someone else to see every keystroke that was made on a particular system. By breaking down this information, it can be easy for a black hat cracker to recreate your user names and passwords, putting all kinds of information at risk and susceptible to misuse. Just imagine your online banking login information falling into the wrong hands! Finding out you have a keylogger installed, however, does not necessarily mean you were the victim of a black hat, as some companies install them on employee computers to track usage and ensure that systems are not being used for unintended purposes. Keyloggers are, for obvious reasons, often considered to be spyware.

Logic Bomb – A logic bomb is a malicious program designed to execute when a certain criterion is met. A time bomb could be considered a logic bomb because when the target time or date is reached, it executes. But logic bombs can be much more complex. They can be designed to execute when a certain file is accessed, or when a certain key combination is pressed, or through the passing of any other event or task that is possible to be tracked on a computer. Until the trigger event the logic bomb was designed for passes, it will simply remain dormant.

Malware – Simply put, malware is a malicious program that causes damage. It includes viruses, Trojans, worms, time bombs, logic bombs, or anything else intended to cause damage upon the execution of the payload.

Master Program – A master program is the program a black hat cracker uses to remotely transmit commands to infected zombie drones, normally to carry out Denial of Service attacks or spam attacks.

Password attacks: Cracking a password is the simplest way for hackers to gain access to their target's accounts and databases. There are three main types of password attacks: brute force attack, which involves guessing at passwords until the hacker gets in; dictionary attack, which uses a program to try different combinations of dictionary words; and key logging, which tracks all of a user's keystrokes including login IDs and passwords.

Payload – The payload is the part of the malware program that actually executes its designed task.

Phishing – Phishing is a form of social engineering carried out by black hats in electronic form, usually by email, with the purpose of gathering sensitive information. Often these communications will look legitimate and sometimes they will even look like they come from a legitimate source like a social networking site, a well-known

entity like Paypal or Ebay, or even your bank. They will have a link directing you to a site that looks very convincing and ask you to verify your account information. When you log in to verify your information on the bogus site, you have just given the black hat exactly what they need to make you the next victim of cyber crime. Phishing is done in many forms – sometimes it's easy to spot, sometimes not.

Phreaker – Considered the original computer hackers, phreakers, or phone phreakers, hit the scene in the 60s and made their mark by circumventing telecommunications security systems to place calls, including long distance, for free. By using electronic recording devices, or even simply creating tones with a whistle, phreakers tricked the systems into thinking it was a valid call. One of the first to find prominence was "Captain Crunch," a phreaker who realized the toy whistle that came as a prize in a box of Captain Crunch cereal could be used to mimic the tone frequencies used by telecommunications companies to validate and route calls.

Polymorphic Virus – A polymorphic virus is a virus that will change its digital footprint every time it replicates. Antivirus software relies on a constantly updated and evolving database of virus signatures to detect any virus that may have infected a system. By changing its signature upon replication, a polymorphic virus may elude antivirus software, making it very hard to eradicate.

Ransomware is a type of malware that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a trojan, whose payload is disguised as a seemingly legitimate file; thus, ransomware is an access-denial type of attack that prevents legitimate users from accessing files.

Rootkit – Without a doubt, the biggest fear in IT security is an undetected intrusion. A rootkit is a tool that can give a black hat the means for just such a perfect heist. A rootkit is a malware program that is installed on a system through various means, including the same methods that allow viruses to be injected into a system, like email, websites designed to introduce malware, or downloading and/or copying to the system with an unsafe program. Once a rootkit is introduced, this will create a back door for a black hat that will allow remote, unauthorized entry whenever he or she chooses. What makes a rootkit particularly lethal: it is installed and functions at such low system levels that it can be designed to erase its own tracks and activity from the now vulnerable system, allowing the black hat to navigate through entire networks without being exposed. Often, black hats will use social engineering to gain physical access to particularly well protected system so the rootkit can be directly installed from CD or a tiny USB drive (it only takes a minute) in order either to circumvent a particularly troublesome firewall or gain access to a system that is not normally accessible from the outside. Once the rootkit is introduced, the black hat has free reign and even skilled IT security departments will have a lot of trouble even seeing the activity as it's happening. Rootkits are a definite 10 on the scary scale of cyber intrusions.

Script Kiddie – An individual who does not possess, or just doesn't use, their own skills and know-how to hack or crack a computer system or network, but uses a pre-written program or piece of code, a script, to do the dirty work. While they may not possess the computing talent, they can be just as dangerous!

Social Engineering – In the realm of the black hats, social engineering means to deceive someone for the purpose of acquiring sensitive and personal information, like credit card details or user names and passwords. For instance, when fictitious Mr. Smith calls from IT services to inform you of new user name and password guidelines being implemented by the company and asks you to reveal yours so he can make sure they meet the new guidelines, you have been a target of social engineering. They can be very clever and resourceful, and very, very convincing. The

only way to make sure you are not a victim of social engineering is never to give your personal and sensitive information to anyone you are not absolutely sure about. There are very few occasions that anyone legitimate would ever ask you for a password, and you should always be the one contacting them, not the other way around.

Spam – Spam is simply unsolicited email, also known as junk email. Spammers gather lists of email addresses, which they use to bombard users with this unsolicited mail. Often, the emails sent are simply advertising for a product or a service, but sometimes they can be used for phishing and/or directing you to websites or products that will introduce malware to your system. When you receive spam, the best practice is to delete it immediately. Sometimes you will see a note in a spam email that gives you instructions on how to be removed from the list – never do it! This will only confirm to the spammer that they have a valid email address and the spam will just keep coming. They could also then sell your email address to another spammer as a confirmed email address and more spam will show up in your inbox. Most mail services have spam filters and these should be employed whenever possible.

Spoofing – Spoofing is the art of misdirection. Black hat crackers will often cover their tracks by spoofing (faking) an IP address or masking/changing the sender information on an email so as to deceive the recipient as to its origin. For example, they could send you an email containing a link to a page that will infect your system with malware and make it look like it came from a safe source, such as a trusted friend or well-known organization. Most of the true sources have security measures in place to avoid tampering with sender information on their own mail servers, but as many black hat spammers will launch attacks from their own SMTP (Simple Mail Transfer Protocol), they will be able to tamper with that information. When in doubt, check with the source yourself.

Spyware – Spyware is software designed to gather information about a user's computer use without their knowledge. Sometimes spyware is simply used to track a user's Internet surfing habits for advertising purposes in an effort to match your interests with relevant ads. On the other side of the coin, spyware can also scan computer files and keystrokes, create pop-up ads, change your homepage and/or direct you to pre-chosen websites. One common use is to generate a pop-up ad informing you that your system has been infected with a virus or some other form of malware and then force you to a pre-selected page that has the solution to fix the problem. Most often, spyware is bundled with free software like screen savers, emoticons and social networking programs.

Time Bomb – A time bomb is a malicious program designed to execute at a predetermined time and/or date. Time bombs are often set to trigger on special days like holidays, or sometimes they mark things like Hitler's birthday or 9/11 to make some sort of political statement. What a time bomb does on execution could be something benign like showing a certain picture, or it could be much more damaging, like stealing, deleting, or corrupting system information. Until the trigger time is achieved, a time bomb will simply remain dormant.

Trojan – A Trojan, or Trojan Horse, is a malicious program disguised to look like a valid program, making it difficult to distinguish from programs that are supposed to be there. Once introduced, a Trojan can destroy files, alter information, steal passwords or other information, or fulfill any other sinister purpose it was designed to accomplish. Or it may stay dormant, waiting for a cracker to access it remotely and take control of the system. A Trojan is a lot like a virus, but without the ability to replicate.

Virus – A virus is a malicious program or code that attaches itself to another program file and can replicate itself and thereby infect other systems. Just like the flu virus, it can spread from one system to another when the infected program is used by another system. The more interconnected the host is, the better its chances to spread. The spread of a virus can easily occur on networked systems, or it could even be passed along on other media like a CD or memory stick when a user unwittingly copies an infected file and introduces it to a new system. A virus

could even be emailed with an attachment. “Virus” is often incorrectly used as a catch-all phrase for other malicious programs that don’t have the ability to self-replicate, like spyware and adware.

Wardriving – Wardriving is the act of driving around in a vehicle with the purpose of finding an open, unsecured Wi-Fi wireless network. Many times, the range of a wireless network will exceed the perimeter of a building and create zones in public places that can be exploited to gain entry to the network. Black hats, and even gray hats, will often use a GPS system to make maps of exploitable zones so they can be used at a later time or passed on to others. Wardriving is not the only way this task is performed – there are Warbikers and Warwalkers too. As you can see, it is imperative that your WiFi network is secure because there are entities out there looking for any opening to ply their trade.

White Hat – While black hats use their skill for malicious purposes, white hats are ethical hackers. They use their knowledge and skill to thwart the black hats and secure the integrity of computer systems or networks. If a black hat decides to target you, it’s a great thing to have a white hat around.

Worm – A worm is very similar to a virus in that it is a destructive self-contained program that can replicate itself. But unlike a virus, a worm does not need to be a part of another program or document. A worm can copy and transfer itself to other systems on a network, even without user intervention. A worm can become devastating if not isolated and removed. Even if it does not cause outright damage, a worm replicating out of control can exponentially consume system resources like memory and bandwidth until a system becomes unstable and unusable.

Zero Day Threat/Exploit – Every threat to your computer security has to start somewhere. Unfortunately, the way most of us protect ourselves from cyber threats and intrusions, is to use detection programs that are based on analyzing, comparing and matching the digital footprint of a possible threat to an internal database of threats that have been previously detected, reported and documented. That’s why we all have to go through those seemingly never-ending updates to our antivirus programs, that’s how the database is updated and the newest threats are added to the list of what the scanners look for. That inherent flaw in our scanners is what makes a Zero Day threat so dangerous. A Zero Day threat is pristine and undocumented. From the very first day a particular threat is ever deployed (zero day) until that threat is noticed, reported, documented and added to the index, it is an unknown. As far as standard protection goes, unknown means invisible – and when it comes to cyber threats, invisible can definitely mean trouble.

Zombie / Zombie Drone – A zombie is a malware program that can be used by a black hat cracker to remotely take control of a system so it can be used as a zombie drone for further attacks, like spam emails or Denial of Service attacks, without a user’s knowledge. This helps cover the black hat’s tracks and increases the magnitude of their activities by using your resources for their own devious purposes. Rarely will the user infected with a zombie even know it’s there, as zombies are normally benign and non-destructive in and of themselves. Zombies can be introduced to a system by simply opening an infected email attachment, but most often they are received through non-mainstream sites like file sharing sites, chat groups, adult websites and online casinos that force you to download their media player to have access to the content on their site, using the installed player itself as the delivery mechanism.