websense®

FIVE MOST COMMON TYPES OF MALICIOUS HACKERS

5 MAIN ARCHETYPES

HACKER TYPES

FIVE MOST COMMON TYPES OF MALICIOUS HACKERS

A few years ago, we looked at the five main archetypes of a hacker. While in many circles “hacker” has become a catchall name for ‘bad guys’ perpetrating cybercrimes, it’s important to note that not all hackers wear black hats and commit criminal acts.

Some hack to test product vulnerabilities and improve overall security. Hacking encompasses a whole culture and not all hacking is done with computers. However, there are different types of hackers with varying motivations. Knowing more about malicious hacker archetypes and their particular intent can help security solution providers tailor their tools more effectively and can help an organization plan a more advantageous defence.

We took a look at the world of malicious hackers to see if the five main archetypes we previously identified remain the same in 2014, or if the world of illicit hackers has changed (and how) over the past few years. We found an evolution of hackers with similar designs, as well as new and sophisticated tools. Present-day hackers fall into the following current categories.

01 THE ARMS DEALER

02 THE BANKER

03 THE CONTRACTOR (A.K.A. HACKERS FOR HIRE)

04 THE ONLINE ANARCHIST (A.K.A. HACKTIVISTS OR ‘SCRIPT KIDDIES’)

05 THE SPECIAL AGENT

THE ARMS DEALER

01

THE ARMS DEALER

WHO: The “Arms Dealer” is a hacker who develops and sells malware and other hacking tools and exploit kits to other cybercriminals. They can include those who rent out massive botnets or sell Trojan toolkits, keyloggers and other malware on the black market. Also under this category, we include those hackers who specialize in “ransomware” – when a cybercriminal has taken control over a person’s computer and demands money in order to give back control or not delete important files.

WHY: Arms Dealers can make good money on underground markets simply by selling their tool kits or renting out access to zombie computers (so called for performing malicious tasks under remote direction). They can quickly and easily modify their malware and sell new versions when antivirus and antimalware security tools shut down the old versions.

EXAMPLE: The infamous Zeus Trojan is an example of malware that has been sold on the black market for several years now. Periodically, we see it modified and adapted to create a new type of threat, and then this new variant is sold on the black market as well. First there was the original Zeus Trojan for sale, then Zeus-in-the-mobile (or Zitmo), and now the Zeus Game Over variant is being sold online, although temporarily downed. The Register recently reported that a Trojan dubbed the “Father of Zeus” is being sold on cybercriminal marketplaces for $7000.

Perhaps the most successful Arms Dealer of all time is the noted criminal “Paunch” who created the Black Hole exploit kit. This kit changed the face of the cybercriminal arms industry by offering frequently updated packages, hosted services and criminal infrastructure, including obfuscation modules, as a service.

After Paunch’s arrest, Black Hole infections took a nose dive, but there is no doubt that another Arms Dealer will soon develop the next big exploit kit.

Nature abhors a vacuum, and right now the throne of King of the Arms Dealers is for the taking - awaiting a new claimant.

THE BANKER

02

THE BANKER

WHO: "The Banker" is highly focused on stealing credit and other financial information, including username and password credentials or other personally identifiable information that can be easily sold and traded on the black market. These hackers are often based in China, Russia or Eastern Europe and can be individual actors or part of an organized crime group. They may use phishing attacks to capture user credentials, or employ more advanced malware to steal valuable data from an organization's network.

WHY: Once these hackers steal credit card information or other valuable data, they treat it like any other commodity that can be sold or traded. Rather than use the data to commit identity theft or make fraudulent purchases themselves, they sell the information on online underground markets for a tidy profit. The information is then used by many more hackers and crooks in a variety of crimes.

EXAMPLE: The massive breach at Target Corporation where hackers stole information of more than 40 million credit and debit cards in late 2013 is a well-known example.

Hackers used malware to compromise Target's point-of-sale registers and capture the card information when customers made their purchases. It's reported that as many as 3 million stolen cards were sold on the black market in the days after the breach, before banks started cancelling and replacing the cards.

The hackers are estimated to have made more than $53 million from the sale of the credit card information.

THE CONTRACTOR

03

THE CONTRACTOR (A.K.A. HACKERS FOR HIRE)

WHO: Teams of hackers who rent out their services. Often considered to reside in China, Russia or Eastern Europe, these hackers for hire can be a “small business” of one to two individuals; or part of a larger, organized crime syndicate capable of running multiple operations at once. They possess a variety of skills necessary for breaching networks and stealing data, often using phishing attacks and Trojans within their bag of tricks. Unfortunately, the hacker for hire is a well-established industry and their services can often start at just a few hundred dollars.

It is important to differentiate the Contractor from the Arms Dealer. While the lines are continually blurring as the malware-as-a-service market continues to develop, the Contractor is different from the Arms Dealer in that he has been paid for a specific target and gets his own hands dirty in the efforts to infiltrate. There is an entire ecosystem of role players and actors that perpetuate the cybercriminal underground. Almost every aspect of normal service has a counterpart in this dark economy.

WHY: These contractors are often hired to target specific organizations or to steal specific types of information such as credit card information or passwords. They are sometimes even hired for state-sponsored espionage. Hackers for hire are in it for the money and they will target organizations of all sizes and in all industries, depending upon what they’ve been hired to do.

EXAMPLE: In early 2014, the FBI arrested five individuals for running the “hackers for hire” website needapassword.com, which promised to provide paying clients with stolen passwords. The group charged customers anywhere from $50 to $350 for passwords.

There is an entire ecosystem of role players and actors that perpetuate the cybercriminal underground.

Almost every aspect of normal service has a counterpart in this dark economy.

THE ONLINE ANARCHIST

04

THE ONLINE ANARCHIST (A.K.A. HACKTIVISTS OR 'SCRIPT KIDDIES')

WHO: A loosely organized group of underground hackers and pranksters, mostly seeking to cause chaos for organizations or people they dislike, or provide support for the causes they follow. These are the hackers who often launch distributed denial of service attacks (DDOS) or deface a company's website to cause embarrassment or disrupt the company's activities.

The group calling itself Anonymous and its subgroups LulzSec and AntiSec are the most well known examples. These groups gained notoriety from 2008 – 2012 with a series of high-profile attacks, but have quieted down some in the past few years after one of the main leaders was arrested and turned informant. Most of their current activity centers on a series of loosely connected social causes, often using "doxing" (the gathering and release of private information of a target) as their primary weapon. But don't expect these groups to maintain a low profile or to go away completely.

WHY: Many hackers in this group started off as independent script-kiddies testing their skills in one-off battles, public forums and image boards, such as reddit and 4chan. This allowed them to find a sympathetic ear and a cause to unite around. While some of these anarchy-loving hackers do it just for the fun of causing trouble, others consider themselves to be "hacktivists," claiming to seek political change or supporting particular causes rather than hacking for financial gain. They use their hacking skills to either cause chaos for organizations and people they have deemed the enemy, or to rally the masses in support of causes they like (such as Net Neutrality). As a loosely-defined group, this hacker archetype comprises individuals with varying motives, from those conducting online political protests to those simply acting as hooligans out to cause mischief.

EXAMPLE: The agendas of Anarchist hackers are as varied as their individual members. Earlier this year, the Syrian Electronic Army (SEA) took over the homepages of eBay and PayPal in the UK, France and Israel. Instead of targeting account information of the users, the SEA displayed its own logo on the homepages of the ecommerce companies in those countries, saying it is a "hacktivist operation" and "we didn't do it to hack people's accounts." The SEA said the attack was in retaliation to eBay's and PayPal's lack of presence in Syria.

Regardless of the agenda or your personal or professional sympathies on each, these groups do represent a threat to businesses, especially as they refine their tactics to include the intrusion of private networks and theft of information.

They still have all of the same blunt tools available from their early days (including the incredibly simple, but powerful Low Orbit Ion Cannon for DDOS).

During the last few years, they have also begun to accrue a series of more surgical tools and methods in their increasing reliance on information stolen from the computers and networks of businesses, government and citizens.

THE SPECIAL AGENT

05

THE SPECIAL AGENT

WHO: These individuals deal in highly-targeted, advanced persistent threats (APT) and cyber espionage. They may be a state-sponsored agent of a foreign government or even a source within an organization working as a double agent. These types of attacks are costly, sophisticated and time-consuming. Therefore, the hacker typically focuses on very high-value targets such as large corporations in the finance, IT, defence and energy sectors. Most come from China and Russia, and are either members of large criminal organizations or hackers working for foreign governments.

WHY: The Agent is in it for cash, creed or country. They typically are looking to steal trade secrets, financial data or strategically important information on energy and defence systems. They may conduct covert, on-going spying campaigns, or they may overtly disrupt business and sabotage organizations or public infrastructure.

EXAMPLE: Just last year, federal agents notified more than 3,000 US companies across a variety of industries that their computer systems had been hacked in cyber espionage campaigns. The estimated cost of these types of targeted attacks against US companies is up to $100 billion annually. This year, a group of attackers known as Dragonfly made headlines for targeting the energy sector and industrial control systems in the US. A hacking organization called Hidden Lynx was recently uncovered in China and is alleged to have been commissioned by the Chinese military for cyber espionage campaigns. Hidden Lynx has been linked to several notorious attacks against US companies in the past, including Operation Aurora which targeted Google and Adobe among other tech companies.

While all of this discussion of hacker types and sorting out the bad apples can make for an interesting read, it will provide no solace if you or your organization becomes a victim. However, by understanding the most common motivations and archetypes of the cybercriminal underground, we can better defend ourselves from their attacks.

So it is said that if you know your enemies and know yourself, you can win a hundred battles without a single loss.

If you only know yourself, but not your opponent, you may win or may lose.

If you know neither yourself nor your enemy, you will always endanger yourself.

- Sun Tzu

ABOUT WEBSENSE

Websense®, Inc. is a global leader in protecting organizations from the latest cyber-attacks and data theft. Websense TRITON® comprehensive security solutions unify web security, email security, mobile security and data loss prevention (DLP) at the lowest total cost of ownership. More than 11,000 enterprises rely on Websense TRITON security intelligence to stop advanced persistent threats, targeted attacks and evolving malware. Websense prevents data breaches, intellectual property theft and enforces security compliance and best practices. A global network of channel partners distributes scalable, unified appliance and cloud-based Websense TRITON solutions.

To access the latest Websense security insights and connect through social media, please visit www.websense.com/smc.

For more information, visit www.websense.com.

websense®

www.websense.com