lastline™

Malware Primer

Table of Contents

Introduction

In The Art of War, Sun Tzu wrote, "If you know the enemy and know yourself, you need not fear the result of a hundred battles." This certainly applies to cyberwarfare. This primer will help you get to know cybercriminals by providing you with a solid foundation in one of their principle weapons: malware.

Our objective here is to provide a baseline of knowledge about the different types of malware, what malware is capable of, and how it's distributed. Because effectively protecting your network, users, data, and company from malware-based attacks requires an understanding of the various ways that the enemy is coming at you.

Keep in mind, however, that we're only able here to provide the basics. To build on this knowledge, read our **Lastline blog**, and our **Lastline Labs blog** which collectively cover a wide range of malware and cybercrime-related topics, sometimes in great depth.

Chapter 1: A Brief History of Malware—Its Evolution and Impact

A brief look at the history of malware, short for malicious software, shows us that this malicious menace has been with us since the dawn of computing itself. According to **Scientific American**, the idea of a computer virus extends back to 1949, when early computer scientist John von Neumann wrote the "**Theory and Organization of Complicated Automata**," a paper that postulates how a computer program could reproduce itself. In the 1950s, employees at Bell Labs gave life to von Neumann's idea when they created a game called "Core Wars." In the game, programmers would unleash software "organisms" that competed for control of the computer.

The earliest documented viruses began to appear in the early 1970s. Historians often credit the "**Creeper Worm**," an experimental self-replicating program written by Bob Thomas at BBN Technologies with being the first virus. Creeper gained access via the ARPANET and copied itself to remote systems where it displayed the message: "I'm the creeper, catch me if you can!"

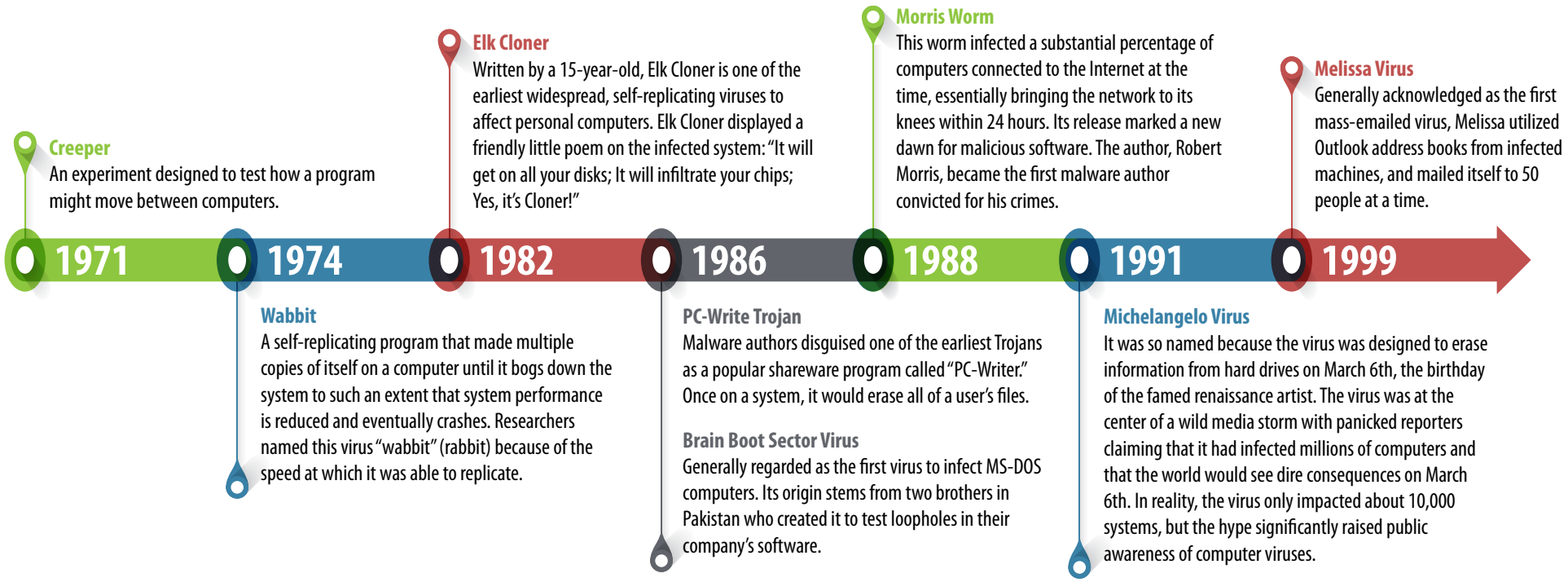
The term "virus" however, wasn't introduced until the mid-eighties. **Fred Cohen**, often considered the father of what we know today as a computer virus, coined the term in his 1986 Ph.D. thesis. He defined a "virus" in a single sentence as: "A program that can infect other programs by modifying them to include a, possibly evolved, version of itself."

From these simple and benign beginnings, a massive and diabolical industry was born. Today, according to **The Anti-Phishing Workgroup**, malware has infected one-third of the world's computers. The consequences are staggering. **Cybersecurity Ventures** reports that losses due to cybercrime, including malware, are anticipated to hit $6 trillion annually by 2021.

History of Malware—The Early Years

Early malware was primitive, often spreading entirely offline via floppy disks carried from computer to computer by human hands. As networking and the Internet matured, malware authors were quick to adapt their malicious code and take advantage of the new communication medium.

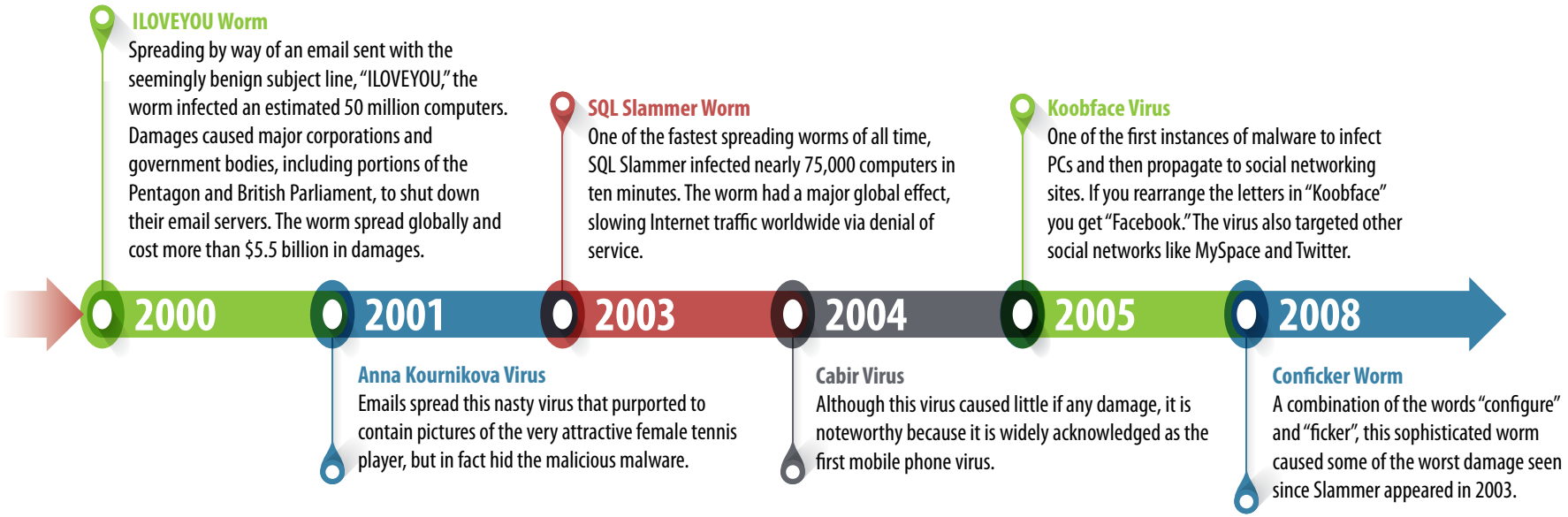
Here's a representative list of some of the significant early versions of malware and how they impacted the world:



History of Malware—Toolkits and Astonishing Rates of Infection

Between 2000 and 2010, malware grew significantly, both in number and in how fast infections spread. At the start of the new millennium, Internet and email worms were making headlines across the globe. Later, we witnessed a dramatic increase in malware toolkits, including the now infamous Sony rootkit, which was instrumental in malware authors including rootkits in most modern malware. Crimeware kits aimed specifically at websites also rose in popularity, and the number of compromised websites escalated correspondingly. SQL injection attacks became a leading threat, claiming popular victims such as IKEA.

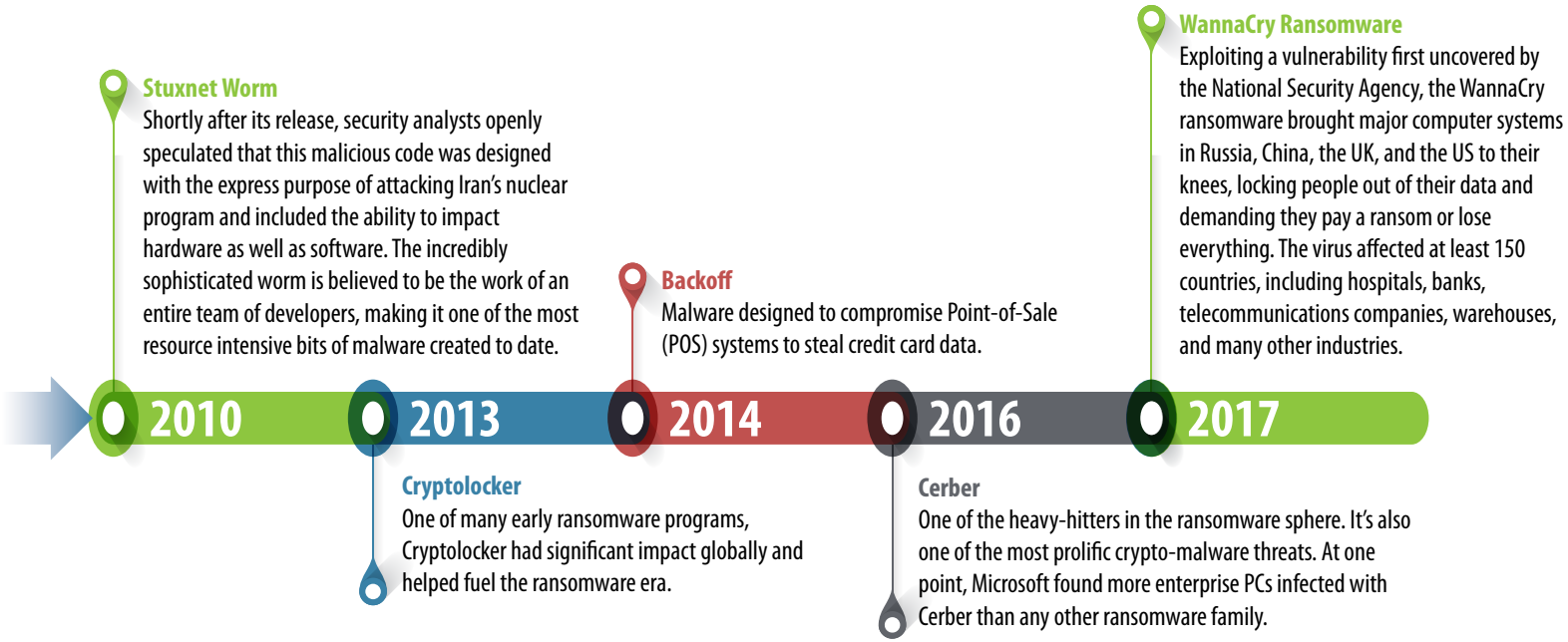
Here's a summary of some of the significant malware released between 2000 and 2010:



History of Malware—State Sponsored, Sophisticated and Profitable

Between 2010 and the present time, we've again observed significant evolution in the sophistication of malware. Organized crime and state sponsors upped the game dramatically with large, well-funded development teams. These malicious workgroups continue to evolve today, developing advanced malware with evasion tactics that outsmart many conventional anti-malware systems. Infiltrating factories and military systems became a common reality, and the monetization of malware grew rapidly with dramatic growth in ransomware and other illegal schemes.

Here are some notable varieties of malware that have had a major impact between 2010 and today.



History of Malware—From PCs to Just About Everything Electronic

Although malware gained much of its initial footing by infecting computers like PCs, today virtually anything with a microprocessor is at risk. Researchers have demonstrated how malware can infect hundreds of new targets, including **wearables** (like watches and Fitbits), **light bulbs**, **automobiles**, **water supply systems**, and even **airliners**.

Moving from research and theory to reality, cybercriminals have already successfully deployed malware that compromised everything from simple devices to complex industrial complexes, including **mobile phones**, **ATM machines**, **security cameras**, **TVs**, **e-cigarettes**, **vending machines**, and **nuclear plants**. This list is of course, just a small representation of actual malware infections.

History of Malware—Is This Just the Beginning?

Most wars involve a specific set of countries and have a defined beginning and end. Regrettably, the war with malware impacts everyone across the globe and has no end in sight. According to **CNBC**, cyberattacks are the fastest growing crime in the United States (and it's easy to speculate, the fastest growing crime in the rest of the world as well).

While the cybersecurity industry is feverishly working to control malware—and succeeding in many ways, cybercriminals show no signs of defeat, or even of slowing down. When cybercriminals are thwarted in one area, they quickly develop new tactics and attack in another. After all, it's good business for them so they're not very likely to throw in the towel and just walk away.

In all probability, most of the history of malware lies in front of us, not behind us. We can expect to see cybercrime continue to cause unprecedented damage to both private and public enterprises.

Sources:

1. Timeline of Computer Viruses and Worms, Wikipedia, Mar 30 2018
2. A Short History of Crimeware, CSO, Nov 4 2011
3. When Did the Term Computer Virus Arise? Scientific American
4. Creeper (Program), Wikipedia, Mar 30 2018
5. Report: Malware Poisons One-Third of World's Computers, TechNewsWorld
6. Cybercrime Damages Predicted to Cost $6 Trillion Annually by 2021, PRNews Wire, Oct 19, 2017
7. Protect Against the Fastest Growing Crime: Cyber Attacks, CNBC, 25 July 2017
8. Everything You Need to Know About WannaCry, CNET, May 19 2017
9. Ransomware: Security Researchers Spot Emerging New Strain of Malware, ZDNET, Oct 19 2017
10. The Story Behind The Stuxnet Virus, Forbes, Oct 17 2010
11. Cryptlocker: What You Need to Know, The Guardian, Jun 3 2014

Chapter 2: Malware Types and Classifications

Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software. Cybercriminals design malware to compromise computer functions, steal data, bypass access controls, and otherwise cause harm to the host computer, its applications or data.

Researchers classify the many types of malware in several different ways, including:

- The attack methodology. Examples include drive-by downloads that distribute malware simply by visiting a website, **phishing** emails that trick victims into divulging data, Man-in-the-Middle attacks that take over control of a computer, and **cross-site scripting** where an attacker injects malicious code into the content of a website.
- The specific type of vulnerability that the malware exploits. Examples include SQL Injection used by attackers to gain access to or modify data, and domain spoofing where bad actors seduce web visitors to click on links to their ads or websites by making them look like other legitimate sites.
- The goal or objective of the malware. For instance, **ransomware** has a purely financial goal, whereas spyware is out to capture confidential or sensitive information, and keyloggers capture user names and passwords.
- By the platform or device that the malware targets, such as mobile malware, or attacks that target a specific operating system.
- The malware's approach to stealth, or how it attempts to hide itself. Rootkits, that typically replace legitimate operating system components with malicious versions are an example.
- Specific behaviors and characteristics—like how the malware replicates and spreads, or other attributes that distinguish it from other forms of malware. This is the most common method for classifying malware.

A basic understanding of how malware is classified is sufficient for most readers. So, we'll forego a more detailed description.

However, it's essential for anyone involved with cybersecurity to have at least a fundamental knowledge of the most significant and common varieties of malware. The list below provides that overview.

The Most Significant and Common Types of Malware

Adware

Adware is the name given to programs designed to display advertisements on your computer, redirect your search requests to advertising websites and collect marketing data about you. For example, adware typically collects the types of websites that you visit so advertisers can display custom advertisements.

Many consider adware that collects data without your consent to be malicious adware. Another example of malicious adware is intrusive pop-up advertisements for supposed fixes for non-existent computer viruses or performance issues.

Spyware

Spyware is, as the name implies, software that spies on you. Designed to monitor and capture your web browsing and other activities, spyware, like adware, will often send your browsing activities to advertisers. Spyware however, includes capabilities not found in adware. It may, for example, also capture sensitive information like banking accounts, passwords, or credit card information.

While not all spyware is malicious, it is controversial because it can violate privacy and has the potential to be abused.

Computer Virus

The primary characteristic of a computer virus is malicious software that cybercriminals program to reproduce. It usually does so by attacking and infecting existing files on the target system. Viruses must execute to do their dirty work, so they target any type of file that the system can execute.

Viruses have been around, at least in concept, since the early days of computers. John von Neumann did the first academic work on the theory of self-replicating computer programs in 1949. The first examples of actual viruses appeared in the '70s.

Although their threat has diminished in recent years and other forms of malware have moved into the spotlight, viruses have been the cause of widespread destruction over the years. In addition to stealing and corrupting data, they consume system resources—often rendering the host system ineffective or even useless.

Another characteristic common to viruses is that they are covert, making them hard to detect. Viruses arrive uninvited, hide in secrecy, reproduce by infecting other files when executed, and usually work in obscurity.

Worm

Like a virus, worms are infectious and cybercriminals design them to replicate themselves. However, a worm replicates without targeting and infecting specific files that are already present on a computer. Worms carry themselves in their own containers, and often confine their activities to what they can accomplish inside the application that moves them. They use a computer network to spread, relying on security failures on the target computer to access it, and steal or delete data.

Many worms are designed only to spread, and do not attempt to change the systems that they pass through.

Trojan

A Trojan is a malicious program that misrepresents itself to appear useful. Cybercriminals deliver Trojans in the guise of routine software that persuade a victim to install it on their computer. The term is derived from the ancient Greek story of the wooden horse used to invade the city of Troy by stealth. Trojan horses are just as deadly on computers.

The payload can be anything, but is usually a form of a backdoor that allows attackers unauthorized access to the affected computer. Trojans also give cybercriminals access to the personal information of a user like IP addresses, passwords and banking details. They are often used to install keyloggers that can easily capture account names and passwords, or credit card data, and disclose the data to the malware actor. Most ransomware attacks are carried out using a Trojan horse, by housing the harmful code inside an apparently harmless piece of data.

Security experts consider Trojans to be among the most dangerous types of malware today, particularly Trojans designed to steal financial information from users. Some insidious types of Trojans actually claim to remove any viruses from a computer, but instead introduce viruses.

Keylogger

A keystroke logger, or keylogger, records every keystroke entry made on a computer, often without the permission or knowledge of the user. Keyloggers have legitimate uses as a professional IT monitoring tool. However, keystroke logging is commonly used for criminal purposes, capturing sensitive information like user names, passwords, answers to security questions, and financial information. (See chapter 5 for more information about keyloggers and other password stealing malware.)

Rootkit

A rootkit is a set of software tools, typically malicious, that gives an unauthorized user privileged access to a computer. Once a rootkit has been installed, the controller of the rootkit has the ability to remotely execute files and change system configurations on the host machine.

Rootkits cannot self-propagate or replicate. They must be installed on a device. Because of where they operate (in the lower layers of the operating system's application layer, the operating system kernel, or in the device basic input/output system (BIOS) with privileged access permissions), they are very difficult to detect and even more difficult to remove.

When a rootkit is discovered, some experts recommend completely wiping your hard drive and reinstalling everything from scratch. (See chapter 8 for a more in-depth discussion of rootkits.)

Bots and Botnets

Also known as robots, bots are malicious programs designed to infiltrate a computer and automatically respond to and carry out instructions received from a central command and control server. Bots can self-replicate (like worms) or replicate via user action (like viruses and Trojans).

An entire network of compromised devices is known as a botnet. One of the most common uses of a botnet is to launch distributed denial of service (DDoS) attack in an attempt to make a machine or an entire domain unavailable.

Ransomware

Ransomware is a type of malware that locks the data on a victim's computer, typically by encryption. The cybercriminal behind the malware demands payment before decrypting the ransomed data and returning access to the victim.

The motive for ransomware attacks is nearly always monetary, and unlike other types of attacks, the victim is usually notified that an exploit has occurred and is given instructions for making payment to have the data restored to normal.

Payment is often demanded in a virtual currency, such as Bitcoin, so that the cybercriminal's identity remains hidden.

Many More Types of Malware

The above list describes only the most common types of malware in use today. In reality, there are many additional types and variations of malware, and cybercriminals are continually developing more, although most are simply new techniques to carry out one of the objectives described above.

At some point in the future, there will no-doubt be new malware that doesn't look anything like the above categorizations. That means that those of us responsible for network security need to be forever diligent in looking for new types of malware that don't fit the mold. We can never let our guard down.

Chapter 3: How Malware Works – Malicious Strategies and Tactics

Understanding how malware works, and in particular, the strategies and tactics most often used by malware authors, is vitally important for cybersecurity professionals. Now that we've provided a brief history of malware and basic malware types, we'll look at some of the common methods that malware authors use to distribute, control, and hide malicious code.

How Malware is Distributed

AV-Test, one of the most renowned institutions for testing Anti-Malware products, reports that cybercriminals push 250,000 new malicious programs into the wild every day. So, what tactics do cybercriminals use to distribute this massive amount of malware? Although new methods are constantly emerging, most malware is delivered in the following ways.

- Malicious Email Attachments: Emails often include attachments that install malware when opened by the victim. According to **Verizon's 2017 Data Breach Investigations Report**, in 2016 hackers delivered two-thirds of all successful malware (penetrated the victim's network) via malicious email attachments.
- Malicious Email Links: Contained in either an attachment or in the body of the email, links to malicious web pages also account for a significant number of data breaches. **ZDNet** reported that almost a quarter of users will click what turns out to be a malicious link if they believe the email is from a friend. See **Protection from Malicious Links** to learn more.
- Social Engineering: Cybercriminals use social engineering to build trust before stealing user logon credentials or confidential data. In a social engineering attack, a computer criminal poses as a trusted individual (IT support, human resource, outside contractor, etc.) and entices the victim to either verbally divulge their login credentials, or more often, open a malicious attachment or visit a malicious web page that captures their credentials.
- Phishing: phishing is a broad category of social engineering attack that uses psychological manipulation to bait victims into divulging sensitive information. Targets are contacted by telephone, text message, or email by someone posing as a legitimate institution, delivering a convincing, socially engineered message. The criminal's goal is to lure the victim into providing sensitive data, such as personally identifiable information, banking and credit card details, and passwords.

  While some attacks are designed to trick victims into divulging sensitive information, email and some text-based phishing attacks are designed to deliver malware. Many recipients believe the message is from a trusted individual or organization, and will open infected attachments or click on malicious links.

  Spear phishing refers to an attack that is targeting a specific individual or set of individuals, such as the CFO of a corporation to gain access to sensitive financial data.

  To learn more, see **Cybercriminals, A Bad Day of Phishing is Still a Good Day**.
- Business Email Compromise (BEC): Another social engineering attack where the attacker sends an email to someone in the organization that has the ability to execute a financial transaction. Although sent by the attacker, the email looks like it's from the CEO, CFO, or another empowered individual. It authorizes and requests an immediate financial transaction such as a vendor payment, direct deposit, or wire transfer. This **$5 billion-dollar problem** is sometimes referred to as "**whaling**" since it specifically targets or impersonates an organization's biggest fish. For additional information, see **Preventing Business Email Compromise** and **Don't be a Whale—How to Detect the Business Email Compromise Scam**.
- Drive-by Downloads: Cybercriminals compromise a website, often a legitimate one, by embedding or injecting malicious objects within the site's web pages. When a user visits an infected page, the user's browser automatically loads the malicious code. See **Drive-By Downloads and How to Prevent Them** for more information.

- Watering Hole Attacks: The phrase **watering hole attack** comes from predators in the natural world who lurk near watering holes, waiting for their desired prey to come have a drink. In a network watering hole attack, cybercriminals set traps in websites that their target victims are known to frequent. Often the booby-trapped websites are smaller, niche sites that tend to have limited security.
- Malvertising: Cybercriminals purchase advertising space on legitimate websites and insert malicious code into the ad. Simply viewing the add injects malicious code into an unprotected device. These are similar to a drive-by-download, however there is no interaction needed on the users' part to download the malware. For more information about malvertising, see **The Malicious 1% of Ads Served**.
- Scamware: Malicious programs disguised as malware protection or other legitimate products. This delivery technique is not new, but cybercriminals are developing new and more sophisticated techniques to this old scam.
- Mouse Hovering: A fairly new technique, mouse hovering takes advantage of vulnerabilities in PowerPoint and other document readers. When a user hovers over a link, the reader executes a malicious shell script. See **Malware Analysis—Mouse Hovering Can Cause Infection** to learn more.

Command and Control—How Cybercriminals Manage Malware

To be useful, most malware must communicate with the cybercriminals that own and control it. The malware must transmit stolen data. Perpetrators behind the crimes need to coordinate how and when sophisticated attacks are launched, propagated, and in some cases, how the malware terminates and remains undetected.

Command-and-control servers established by the cybercriminals generally handle this necessary communication. Attackers use these command-and-control servers, also called C&Cs or C2s, to communicate with compromised computers, websites, smart phones, routers, IoT devices, and other networking equipment.

Cybercriminals use C&C servers to instruct and manage individual instances of malware or entire botnets of compromised systems. Most malware is designed to respond to specific instructions received from one or more C&C servers. Using the associated C&C server(s), the attackers direct the malware to perform a number of malicious actions, including:

- Upload reports regarding the malware's status and results of C&C commands
- Install upgrades to the malware or new pieces of malware to expand the attack
- Install keyloggers used to collect sensitive information such as credit card numbers or logon credentials
- Transmit spam or phishing emails
- Launch coordinated DDoS attacks
- Transmit back to the criminal stolen data such as logon credentials, sensitive user data, payment card numbers, corporate intellectual property or financial data, etc.

Advanced malware detection products monitor network traffic for connections to known C&Cs, and for traffic that contains C&C communications. When these tools discover malicious traffic, administrators can block the connections and, in some cases, identify and remove the responsible malware.

Malware authors use several strategies for hiding their C&C communications from malware detection systems. For example, cybercriminals often use covert channels such as **Internet Relay Chat** (IRC), peer-to-peer technology (P2P), and social networks like Facebook and Twitter to hide their communications. The most advanced methods have the ability to quickly switch C&C servers to avoid detection. Some C&C servers have a lifespan of just minutes before another server replaces them.

How Malware Hides—Evasion Tactics

Malware authors are very creative. They use countless tactics to lessen the likelihood that security tools will detect their malware. Earlier in this chapter when we discussed malware distribution, we covered how cybercriminals hide malware in websites, attachments, and advertisements during the initial delivery phase of an attack.

When an attempt is made to download a malicious object, either by a user or their browser, sandboxes are often used to test the object for malicious capabilities. To counter this, malware authors deploy numerous tactics to try to hide from sandboxes. If malware does find its way to an endpoint, malware designers use additional strategies to maintain their stealth.

Sandbox Evasion Tactics

- Fragmentation: A technology that splits malware into several components that only execute when the targeted system reassembles the code.
- Time Delays: The malware remains idle for an extended period, avoiding all malicious activity until (the criminal hopes) the file is released to the intended user.
- User Action Delays: Some malware avoids doing anything malicious until a user performs a specific action (e.g. a mouse click, pressing a key, opening or closing a file, exiting the program).
- Return-Oriented Programming (ROP): A technique where malware injects functionality into another process without modifying the code of that process. To accomplish this, malware alters the contents of the stack (the set of memory addresses that tells the system which segment of code to execute next).
- Rootkits: A rootkit is an application (or set of applications) that hides malicious code in the lower layers of the operating system.
- Polymorphism: Polymorphic malware is so named because it morphs, or mutates, into many forms, and does so very quickly—constantly creating new variations of itself, which makes it nearly impossible to detect using signature-based malware detection tools.

To learn more about sandbox evasion tactics, see Lastline's paper **An Introduction to Advanced Malware and How it Avoids Detection**.

Endpoint Evasion Tactics

In addition to using covert C&C communication channels as discussed earlier, malware authors use a number of tactics to avoid having their malware detected after installation. Here are just a few of those tactics:

- Unique Signatures: Most malware today is a one-of-a-kind. To avoid detection by signature-based anti-virus solutions, cybercriminals have developed automated systems that create a unique malicious object for each installation.
- Critical System Files: Malware often masquerades as a legitimate system file. By replacing original system files with compromised versions of the same, endpoint malware detection systems have difficulty spotting the malicious code.
- Disabling Endpoint Security: Some malware is able to evade certain endpoint antivirus tools by disabling the tool or adding an exception.
- Windows Registry: Hiding malicious code within the Windows registry is a common malware tactic because no additional files are installed.
- Temporary Files, Folders or Directories: Malware scans are often configured to analyze a specific set of files and folders. So, malware authors use or create temporary or uncommon files and folders that aren't typically scanned in which to hide their code.
- In Shortcuts: Commonly known as shortcuts, malware writers have used Shell Link Binary Files for years to hide and launch malware. Recently, we've seen a resurgence of their usage.
- Within Macros: Inserting malicious macros inside of otherwise legitimate-looking documents like Microsoft Excel files has reemerged as a popular technique to hide malware.

To learn more about malware's evasive capabilities, you might want to read **An Introduction to Advanced Malware and How to Avoid Detection**.

Chapter 4: Polymorphic Malware—Real Life Transformers

Polymorphic malware has been around since the early 1990s, but it's still wreaking havoc in our computers and networks. **SC Magazine** recently reported on a particularly nasty strain of polymorphic malware that, according to the article, "is able to evade over 75 percent of antivirus engines tested." That's a very disturbing statistic.

What is Polymorphic Malware?

So, what is this strange type of malware that is so adept at evading detection, and why is it so dangerous? Polymorphic malware is so named because it morphs, or mutates, into many forms, and does so very quickly—constantly creating new variations of itself. Because polymorphic malware can change so rapidly, it is very difficult for conventional, signature-based antimalware tools to detect it. Each new iteration of the malware alters its own attributes in some way. Changes include a different filename, new encryption keys, or a unique compression signature. These changes, or any change to the code, alter the malware's signature, making it very difficult or even impossible for antimalware tools that rely on signatures–and most do–to effectively detect advanced polymorphic malware.

Why Polymorphic Malware is Especially Dangerous

When writing polymorphic malware, cybercriminals typically take an existing malicious code base and apply polymorphism to it. The basic malicious functionality of the code usually remains the same. However, the packaging is different, so it generates an entirely different signature—one that antimalware products have not yet blacklisted.

Because it's relatively easy to modify an object's packaging through polymorphism, malware authors can rapidly create new versions, typically automating the entire process. Cybercriminals are churning out new versions at an unbelievable pace. Lastline's research indicates that most modern versions of polymorphic malware will transform within seconds. Often, and perhaps most of the time, cybercriminals release only a single instance of a particular malware version into the wild. The majority of these single-use malicious objects will never be seen by antimalware researchers, and if they are, their signatures are already obsolete and useless.

Polymorphic malware has become so successful that most malware today employs at least some level of polymorphism.

Notable Examples of Polymorphic Malware

Here are some of the more significant and well-known polymorphic malware families.

Emotet Trojan: This is the polymorphic malware family referenced in the introduction that evaded 75% of antimalware products. By the way, I'm happy to report that Lastline wasn't among those that failed to detect this malicious malware.

Emotet is notable because recent versions have shown additional levels of polymorphism. Typically, malware authors will add polymorphism by simply changing the packaging of the distribution container or method (like moving from a Microsoft Word document to a PDF formatted document). However, in addition to rewrapping the documents used to distribute the malware, some recent Emotet strains continuously rewrap their packed executables as well. This makes it even more difficult for signature-based tools to detect the malware.

Storm Worm: Named from the portentous subject line, "230 dead as storm batters Europe," Storm Worm surfaced in 2007. This malicious email attachment installed wincom32 service and a Trojan, effectively turning the victim's computer into a bot. The compromised computer spewed out a new version of Storm Worm every 30 minutes. At the time, researchers deemed Storm Worm responsible for up to 8 percent of all global malware infections.

CryptoWall: As one of the most infamous ransomware families, CryptoWall has done a lot of damage. In 2015, researchers found more than 4,000 versions of the malware as it spread through phishing email campaigns. Reportedly, in 2015 alone CryptoWall 3.0 cost ransomware victims $325 million dollars paid in Bitcoin.

Virlock: Notable because its ransomware payload arrives encrypted, and the malware only decrypts a small portion of the payload at a time, and then immediately re-encrypts it using a different encryption key. The ongoing cycle of decryption and re-encryption means the malware in memory will constantly look different than the original version. This makes it extremely difficult and time-consuming for researchers to fully analyze the code.

Effective Protection from Polymorphic Malware

Since traditional signature-based antimalware tools are unable to reliably detect polymorphic malware, it's obvious that organizations require more advanced detection techniques.

Behavior analysis and **Deep Content Inspection™** are proven methods for detecting polymorphic malware and organizations are encouraged to augment their signature-based antimalware tools with these advanced products.

It's important to point out that not all sandboxes or behavior-based antimalware products are the same. Some are significantly more effective than others at detecting polymorphic and other types of advanced malware. To learn more about different sandbox technologies, read **Limited Visibility of a Conventional Sandbox**.

Chapter 5: Keyloggers and Other Password Snatching Malware

Cybercriminals are motivated by several things, including fun, fame, ideology, revenge, and especially monetary gain. They use many techniques in their quest to achieve these goals, and keylogging malware (aka keyloggers), and other password-snatching techniques are among their primary tools.

Understanding the Why of Malware is as Important as Knowing How it Works

Experts often classify malware by how a particular strain works—it's a virus, Trojan, worm, or uses a rootkit. These technically oriented taxonomies are of course very important, but it's also useful to categorize malware by its intent. This helps answer why a cybercriminal wrote a particular piece of malware, and what the ultimate, or even the preliminary, objectives are.

Understanding the goal of the malware provides an insight into the criminals' objectives, but equally importantly, it helps researchers and network defenders anticipate where and how the malware may attack. That added intelligence is critical when trying to protect valuable data.

The focus of this chapter is on the set of malicious software that is specifically designed to steal user credentials.

Stealing Login Credentials is Key to Cybercriminals

Password-snatching malware is extremely important to cybercriminals. The vast majority of data breaches involve the use of stolen passwords, especially passwords to privileged accounts. In fact, **research shows** that hackers use stolen login credentials in 81% all of significant data breaches. A detailed discussion about the frequency of password theft is beyond the scope of this ebook, but for those who want a deeper dive, see **Password-Stealing Malware Remains Key Tool for Cybercriminals**.

Hackers typically obtain IDs and passwords in the following ways:

Guessing. Since weak passwords are still commonly used, this approach is alarmingly successful. Automated password-guessing tools are readily available to criminals, and effective.

Social Engineering. Tricking users into revealing their passwords through a **phishing attack or other form of social engineering**. Phishing remains one of the most prolific ways to launch a cyberattack of any kind.

Malware. Code specifically written to do one thing—steal user names and passwords.

Types of Password Snatching Malware

There are several types of malware specifically designed to steal user credentials. Here are some of the more common varieties.

Keylogging Malware: Keystroke loggers ("keyloggers") capture user data as it's entered into the keyboard. Not all keystroke logging software is malicious. Employers use legitimate keylogging software or hardware to oversee the use of their computers and to monitor employee activity. **Windows 10 has a built-in keylogger** in its final version. According to Microsoft, the keylogger is there to "improve typing and writing services." Unfortunately, keyloggers are often used by cybercriminals to capture user IDs, passwords, and other sensitive information. Network defenders need to understand the basics of keyloggers, how criminals use them, and how to detect them.

Ramscrapers: Sometimes referred to as memory scraping malware, these malicious programs find their way into the heart of the system and monitor its memory looking for IDs, passwords, account numbers, and other valuable data. Even though this type of sensitive data is often encrypted in storage, ramscapers capitalize on the fact that at some point the system needs to decrypt that data and hold it in memory in order to use it. Ramscrapers are readily found in the underground market. Popular versions include Dexter, Soraya, ChewBacca, Mimikatz, and BlackPOS.

Password File and System Grabbers: Some malware is specifically designed to access or steal your system's password repository or files. If successful, the malware may obtain all passwords for all users on the system, or all of the passwords belonging to a particular user. For example, Keydnap is a MacOS X-based program that steals passwords from the Keychain password

management system of the infected Apple device. Researchers have discovered a number of malware families designed to compromise an entire password file, including malicious programs that specifically target third-party password managers like Password Safe and KeePass.

Password Crackers: Password cracking tools take many forms. Some try to login with every possible combination of words, numbers, and characters. Other tools aim to break the decryption of captured password files that contain the login credentials for all authorized users. Cybercriminals also plant malware that captures and breaks passwords transmitted over wireless or physical networks. Common password cracking tools include Brutus, RainbowCrack, Cain and Abel, John the Ripper, Medusa, Aircrack-NG, and Wfuzz.

Man-In-the-Browser: This form of malware infects the victim's browser, and captures IDs, passwords, and other data as it travels between the browser and the Internet. The malware frequently injects authentic looking dialog boxes or forms for the user to complete, such as a request for the user's ID and password.

Password Snatching is a Huge Problem

Organizations lose billions of dollars to password stealing malware. Both the Target and Home Depot data breaches were reportedly caused by the ramscraping BlackPOS malware, which successfully stole user IDs and passwords. In the staggering **Yahoo data breach**, where cybercriminals stole 3 billion user accounts, the hackers gained initial access through login credentials obtained via a phishing scheme. But the real damage apparently came when the hackers were able to access the giant's entire password file.

More recently, both NotPetya and BadRabbit ransomware strains leveraged Mimikatz ramscaping malware. **NotPetya** alone crippled thousands of computers at companies like Maersk, Merck, and FedEx, and caused well over a billion dollars in damages.

Hope for Organizations—Using Behavior Analysis to Safeguard Credentials

Given the amount of damage inflicted by stolen IDs and passwords, it's critical that enterprises take immediate and effective steps to protect themselves, their employees, and their customers. Fortunately, there are a number of things an organization can do to dramatically cut their risk of password theft and resulting data loss.

In addition to policies requiring strong passwords and appropriate user training about phishing and other social engineering attacks, organizations need to deploy tools specifically designed to detect and stop today's advanced malware that's intentionally created to steal user credentials. Because malware is constantly growing in sophistication, companies must make sure the system they implement uses the very latest in malware detection techniques.

A good quality and up-to-date malware detection system can identify all forms of password-stealing code—primarily through advanced sandbox technologies. By performing both **static analysis** and **dynamic analysis**, these systems analyze and execute the code in a carefully controlled environment—evaluating the program for malicious capabilities and behaviors. This **Deep Content Inspection** identifies specific malicious behaviors engineered into a piece of malware, and analyzes it for potential risks—including but not limited to the following behaviors:

- Credential stealing capabilities, such as seeking out and capturing user names and passwords for network access, financial accounts, and VPN access, including privileged access
- Evasion attempts or capabilities
- Attempts to establish unauthorized persistence
- Specific password decryption or cracking features
- Attempted access to privileged system files

- Lateral movement, looking for password files, especially privileged credentials, or other assets or other systems that may lead to added password and ID information
- Attempted communications with the malware's command and control server to exfiltrate stolen credentials
- Other related events, that individually don't appear threatening, but when evaluated as a whole, reveal malicious intent

With the right policies, culture, and advanced malware detection tools in place, organizations will dramatically reduce the risk of a data breach or other security incident due to keyloggers and other forms of malware that's specifically designed to steal user IDs and passwords.

Chapter 6: Account and Identity Theft Malware

The prior chapter focused specifically on malware that is designed to capture account credentials. But malware is capable of stealing so much more, which is the focus of this chapter. Identity theft involves capturing extensive details about an individual needed to impersonate that person for the purpose of filing a tax return, opening a new credit card account, acquiring healthcare services and prescriptions, and numerous other purposes.

Identity theft continues to be a challenging and expensive risk for consumers, and malware that's specifically designed to steal users' identities is often used to commit the crime.

The reason for this persistent threat? Simple, identity theft is a very lucrative business for cybercriminals. The **2017 Identity Fraud Study**, recently released by Javelin Strategy & Research, found that cybercriminals stole $16 billion dollars from 15.4 million U.S. consumers in 2016 alone. That's a substantial amount of money. It also represents nearly a billion dollar increase over 2015 identity theft losses. In the past six years identity thieves have stolen over $107 billion dollars from victims in the U.S. alone.

Somewhere around 100 million Americans have personally identifiable information (PII) stored in databases managed by government agencies and numerous businesses. With the current onslaught of data breaches and user account theft, private, sensitive information is constantly at risk of account and identity theft.

Malware is a Major Factor in Identity Theft

There are a number of methods used to commit identity theft, including physical theft of wallets, purses, and personnel records, as well as simply bribing or colluding with employees who have access to bank, credit card, tax data, or other types of PII. But the most dangerous form of identity theft involves cybercrime, including malware. According to the **2012 Verizon Data Breach Investigative Report**, malware was found to contribute to 69% of data breaches, and there's no reason to believe that the situation has improved since then.

The sophistication level of professional identity thieves continues to grow, and so does the methods they develop. With individually tailored phishing and spear phishing scams and elaborate networks of botnets designed to hijack millions of computers without leaving a trace, cybercriminals are constantly developing and deploying new malware in an attempt to steal user accounts and identities.

One example of identity stealing malware is a nasty bit of code called **MEDJACK**, designed specifically to target medical devices. Security researchers found new versions of this malicious code designed to exploit hospital equipment like x-ray machines and MRI scanners. The malware executes a sophisticated zero-day attack that allows cybercriminals to steal patient data from the devices, including PII that the thieves use to commit identity theft.

Keyloggers are another type of dangerous malware. They are often used to capture user IDs, passwords, account numbers, and other sensitive data that cybercriminals leverage to commit identity theft. Criminals used keyloggers in many of the largest and most notable breaches, including TJX, Citibank, Sony, RSA/EMC, World Bank, Lockheed Martin, NBC, Google, and Heartland Payment Systems, as well as breaches of scores of medical clinics and small business the world over. According to the afore mentioned Verizon report, of those breaches where criminals used malware to steal data, 98% of the time the malware included keylogging functionality.

The number of malicious smartphone apps used for identity theft is also on the rise. We've recently seen sophisticated Android apps designed to secretly steal your credit card data and other sensitive information. Victims are unlikely to know about the malware until they learn of the fraudulent use of their identities.

Chapter 7: How Cybercriminals Use Malware to Steal Intellectual Property from Your Company

Stealing intellectual property (IP) is big business for cybercriminals, and they often use malware to do it. Many cyberthieves have turned to IP theft as their primary focus because it's often easier than stealing credit card numbers or other forms of digital currency. IP thieves can operate from anywhere in relative anonymity, and armed with the latest malware, they pose a major threat to the world's IP.

Theft of IP Has Major Impact

IP is the very lifeblood of many enterprises. It fuels growth, innovation, and differentiation, and its theft is often catastrophic—leading to a loss of revenue, damaged customer relationships, and a devaluation of the company's brand and reputation. IP theft not only hurts the victim organization, but the entire economy.

A recently updated report on the **Theft of American Intellectual Property** puts the annual cost to the U.S. economy at over $225 billion in counterfeit goods, pirated software, and theft of trade secrets. The estimated low-end cost of trade secret theft to U.S. firms is $180 billion, or 1% of U.S. GDP. The high-end estimate is $600 billion, amounting to 3% of the nations' GDP and over $1.2 trillion dollars in economic damage over the last three years.

By stealing IP, or purchasing stolen IP, organizations can bring products to market much faster and cheaper than if they designed those products on their own. When IP theft occurs, an organization that invested in the creation, innovation, and design of a related product may find themselves competing with copies of their own merchandise—on sale at half the price.

Cybercriminals target trade secrets and proprietary business information that they can quickly monetize. The opportunities for thieves are endless, but examples include merger plans, new drug formulas, manufacturing processes, schematics, unique product designs, geological surveys showing mining deposits, sophisticated software, and all forms of copyrighted data.

With this broad array of valuable information, IP theft is an issue for virtually every industry and sector.

Significant Examples of IP Loss

IP theft occurs every day, and the number is increasing—and so is the impact. Here are just a few of the more notable cases that have been publicly disclosed.

LOCKHEED MARTIN

Thieves stole terabytes of technical data about the F-36 Joint Strike Fighter Jet, including radar designs and engine schematics. The subsequent unveiling of the copycat Chinese J-31 fighter indicate that the attackers were in fact able to steal sensitive schematics that enabled foreign nations to piggyback off U.S. taxpayers' investment in advanced weaponry.

Coca-Cola

Attackers used spear-phishing tactics to exploit employee systems, upload keyloggers, steal passwords from an executive, and gain access to extremely sensitive data pertaining to Coca-Cola's plans to acquire China Huiyuan Juice Group. The multi-billion-dollar deal fell apart just days after the FBI let Coke executives know about the intrusion.

RSA

Cybercriminals stole data related to the company's sensitive SecurID two-factor authentication technology, forcing RSA to reissue authentication tokens to 40 million users, costing the company over $66 million.

SONY

Attackers stole an enormous amount of IP, including copies of yet-to-be-released movies and TV episodes, employee salaries and data, embarrassing executive emails, and details regarding the company's IT infrastructure. The criminals also deployed wiper software that caused a major disruption to Sony's systems and operations.

amsc

American Superconductors Corporation (AMSC) lost over a billion dollars in share value when cybercriminals stole all of its IP and a rival company allegedly used the data to create and sell competing products.

Malware Designed to Steal Intellectual Property

Cybercriminals use a variety of malware types to help them commit their crimes. Some of these malicious tools use modern state-of-the-art technologies. Other tools are older, but still effective—especially when used repeatedly and in mass. Here's a short list of some of the more common types of malware and malicious techniques cyberthieves use to steal IP.

Keyloggers: Malicious software that captures data as it's entered. When it comes to IP theft, criminals typically use a keylogger to first capture credentials, and then log into an account to steal the intellectual property. (See Chapter 5 for more information about Keyloggers and other credential stealing malware.)

Cross-Site Scripting: A type of injection attack where cybercriminals deliver malicious script or code to a client browser, often via a vulnerable web application. In this type of attack, cybercriminals trick a users' browser into executing malicious code. A classic example is causing a browser to display a popup with a link to a website that installs additional malware which cybercriminals use to steal IP. In other cases, a cross-site scripting attack will cause a victim's browser to send confidential data or cookies containing login credentials to the attacker. Read **Lastline's blog Malware Detection—Discovering Cross-Site Scripting Attacks** to learn more about cross-site scripting.

Drive-by Downloads: Criminals compromise a website, often a legitimate one, by embedding or injecting malicious objects inside the web pages. The infections are invisible to the user, and range from malicious JavaScript code to iFrames, links, redirects, malvertisements, cross-site scripting, and other malicious elements. Cybercriminals frequently use drive-by downloads to steal IP. See **Drive-By Downloads and How to Prevent Them** to learn more.

Ramscraping: Some malware is designed specifically to read and capture data from an infected machine's RAM. This approach to IP theft is effective even when sensitive data is encrypted while it is stored on disk. To use encrypted data, a system must first decrypt that data. That typically occurs in RAM. Ramscraping malware copies the data while it's in RAM and unencrypted.

Man-in-the-Browser: This malware sits in the browser, between the user interface and the connected website or application. From this vantage point, **Man-in-the-Browser** malware can view and capture everything the user enters or sees.

File Hosting Service Exploits: This type of man-in-the-cloud malware is specifically designed to copy cloud-based files. It often abuses vulnerabilities in a hosting service's file synchronization features, capturing and copying IP and other sensitive data during the update process. Such exploits are increasingly dangerous to businesses as they escalate the use cloud-based services to share sensitive customer and corporate data.

Economic Espionage as a Service: Dishonest organizations and cybercriminals can easily find tools and services they need to spy on and exfiltrate highly confidential IP from competitors or other entities. It's even possible to hire hackers to do the actual spying. Espionage-as-a-Service makes it relatively easy for not only state-sponsored cybercriminals to steal IP, but much less sophisticated and funded entities as well.

Companies Must Protect Their IP

There is no letup in attempts to steal IP. Whether state sponsored or at the hands of organized crime, IP theft is here to stay and it's important that companies take a proactive stance to protect their intellectual property. Since cybercriminals will target any trade secret of value, virtually every innovative organization is at risk.

Sadly, unless sophisticated security controls are in place, including advanced malware protection, organizations are often unaware that they've been victims of IP theft until it's too late. Fortunately, enterprises can dramatically reduce their odds of becoming a victim of IP theft by diligently and continuously implementing the very latest malware detection technologies.

Chapter 8: Rootkits and the Role They Play in Malware Attacks

If your data center tells you they need to re-install the operating system onto one of your servers, there's a good chance it's due to a rootkit. Malicious rootkits are one of the most dangerous tools that cybercriminals use. They enable malware authors to easily add stealth, persistence, and privilege escalation to already malicious programs. Once infected by a rootkit, it's very difficult for even the most skilled security experts to remove them, and completely re-installing the OS is often the only way to get rid of them.

Rootkits are not only challenging to remove, they are also very difficult to even spot, and require advanced malware detection technologies to do so.

Rootkit prevention—understanding rootkits, how they operate, and what they're intended to do—is key to detecting malicious attempts to install them. While not all rootkits are malicious, most are, and it's these malicious ones that we'll focus on in this chapter.

Origin and Mission of Rootkits

Rootkits have been around since the 1990s, and they have continued to evolve in sophistication and numbers. Today, they are readily available on the black market to help even novice authors dramatically strengthen their malware.

The term rootkit originates from "root" in UNIX-based operating systems, which is the most privileged administration account in the system. With root-level access, uses can do virtually anything on the system. As for the "kit" in rootkit, it's just an abbreviation of the word "toolkit."

Although the term was instigated in UNIX environments, it now applies to all operating systems, including Windows and Mac OS X. The majority of rootkits in circulation today are Windows-based.

In most cases, apart from modifying the operating system, a rootkit by itself doesn't do any damage. Instead, a rootkit's main function is to keep the malware that it's linked to from being detected. The malware does the actual damage.

Rootkits are primarily used to:

- Establish or enhance stealth, making it very difficult for security analysts and most antimalware products to detect the malware the rootkit is designed to protect
- Conceal other malware that cybercriminals may subsequently install as part of a sustained attack
- Enable persistence, allowing the malware to survive reboots and removal attempts by antimalware and other tools
- Provide an attacker with ongoing full access, often via backdoors
- In some cases, escalate the privilege level in which the malware operates
- Appropriate the compromised machine as a zombie computer or member of a bot

In a nutshell, a rootkit is a toolkit used to add privileged access, stealth, and persistence to a malicious program. Rootkits are typically used to hide malware like keyloggers, spyware, adware, data exfiltration, spam distribution, or to provide privileged access to unauthorized individuals.

Multiple Types of Rootkits

Rootkits are available for every major operating system, including UNIX, Windows, Android, Mac OS X, and iOS. While most rootkits today target Microsoft Windows operating systems, security administrators need to diligently defend all systems from these malicious toolkits.

Experts often classify rootkits by what part of the system they inhabit, such as the kernel, user space, hypervisor, firmware, and even the hardware. Most rootkits will target either the kernel, or the user application space.

User-mode rootkits—These are rootkits operating in user space, also known as "ring 3." This is where applications typically run.

Kernel-mode rootkits—These rootkits reside in kernel space, also known as "ring zero." Kernel mode rootkits are more dangerous than user mode rootkits because they have the highest level of privileges in the system.

How Rootkits are Installed

Attackers want unlimited access, so one of their primary goals is to gain control over processes that execute with top-level privileges. Since loadable kernel modules in UNIX/Linux systems, and device drivers in Windows environments generally execute with the same privileges as the operating system itself, it's common for rootkits to replace these legitimate modules and drivers with malicious versions. This class of rootkit provides the attackers with unrestricted privileges and access.

Rootkit infections are frequently due to **insecure passwords** on root or administrator accounts. Rootkits generally breach the system by utilizing root or administrator account privileges long enough to upload and replace core system files with modified versions. Backdoor access is then established, ensuring that the perpetrators will have access even if the security staff changes the root or administrator password. All traces of the invasion and system modifications are then removed, including log file entries, temporary caches, name changes, etc.

Machines and devices are also commonly infected with rootkits via **drive-by downloads** while browsing the web, or by clicking on **malicious email links** or on **malicious attachments**.

How Rootkits Hide Themselves

Once installed, rootkits are difficult to detect because they try to remove all evidence of their presence. The only visible symptoms typically are an unusually slow system, and strange network traffic. Unfortunately, with today's high-speed CPU's and high bandwidth networks, users or administrators may not even notice the additional CPU or network activity.

Rootkits establish stealth by erasing artifacts that programs normally generate when they're installed, or when they execute. When any program, including malware, is installed, monitoring tools can usually detect its existence by the presence of multiple indicators, like:

- New files
- Additional services or processes
- New or modified registry keys
- Unexpected changes in disk or storage utilization
- New user accounts, or changes to account privileges
- User applications or processes running with root or administrator privileges
- Entries in system logs

Antimalware tools monitor the above and many other entities for anomalies. If found, it's a good indicator that there's malware present. The rootkit's aim is to modify the system components that show these indicators so the malware remains undetected. For example, a rootkit may hide the malware's files, processes, and in the Windows environments, even its registry keys. Another common practice is for the rootkit to create a hidden, encrypted file system where it hides other malware or original copies of the files it has encrypted. The rootkit may even restore the original files when the malware is not active.

IAT and SSDT Hooking to Hide Malicious Software

In Windows machines, IAT Hooking is one technique that user-mode rootkits use to hide malicious software. The IAT, or Import Address Table, is a table where applications look up the addresses of functions they need to run. IAT Hooking occurs when a rootkit alters the addresses in the table so it points to malicious code instead of the legitimate function.

Cybercriminals use IAT hooking in various ways, one of which is to fool antimalware tools. For example, consider an antimalware program that calls a function that normally returns a list of all running services. A sophisticated rootkit will alter the table so it points to a function that's part of the rootkit itself. However, this version of the function removes all malicious processes from the list. As a result, the antimalware program won't see the malware that is in fact executing.

Kernel-mode rootkits employ similar methods, altering what's known as the SSDT, or System Service Dispatch Table. Here again, calls to legitimate software are replaced with calls to rootkit code that hides the presence of the malware.

Notable Rootkits

There are a number of rootkits available in the wild—too many to enumerate here. But to provide a general idea of what's out there, here's a brief description of three notable ones.

TDSS: At one time, experts believed TDSS to be responsible for the second largest botnet in the world. The malware, enabled by TDSS targeted personal data like credit card numbers, online bank accounts, passwords, social security numbers, and other personal information. Law enforcement successfully took down much of the botnet. However, it is still available and actively used.

ZeroAccess rootkit: Responsible for the **ZeroAccess botnet**. This malicious code consumed the CPU and other resources of infected machines while it mined for bitcoins and committed click fraud—spamming the machine's owner with ads. Researchers estimated that the ZeroAccess botnet had compromised up to 2 million PCs. Microsoft took down much of the botnet in 2013, unfortunately, ZeroAccess resurfaced shortly thereafter.

Necurs: This rootkit is behind one of the biggest malicious networks in the world—the Necurs botnet. It has more than 6 million zombie machines tied to it, and is responsible for spreading massive amounts of Locky ransomware spam as well as the Dridex financial malware. The Necurs rootkit protects the malware that enslaves a PC to the botnet, making sure the infection cannot be removed. Necurs is an active botnet, and the cybercriminals behind it are still actively trying to grow it.

Preventing Rootkit Infections

Rootkits pose a very high level of risk to enterprises everywhere. As such, information security professionals need to understand rootkit-related risks, and implement effective defense mechanisms.

As with most things, the best way to counter rootkits is through prevention rather than detection and remediation.

A successful risk management strategy includes putting multiple systems in place to combat the threats, including appropriate system configuration, strong authentication, patch and configuration management, and the latest malware detection solutions. Because rootkits are so proficient at hiding themselves, organizations need to implement extremely strong antimalware technologies.

Conclusion

If you weren't already wary of malware and its extensive capabilities, perhaps now you are. Cybercriminals continually reinvent and improve the malware they're developing to escape detection and complete the task for which it's designed, be it demanding a ransom from an individual or stealing valuable IP from a multinational corporation.

And what's clear about how malware is designed, and the various ways in which it's distributed, is that conventional signature-based detection tools are ineffective. The industry largely has accepted this fact, although many organizations continue to rely on static (i.e. signature-based) analysis.

What's needed today is the ability to conduct dynamic analysis that identifies all of the behaviors engineered into a piece of malware. Then it's clear which files and which network anomalies are benign and which are malicious. Behaviors tell security teams what to block, and what to deliver, what is a benign activity that happens to be anomalous, and what is a malware file that is not anomalous, without wasting time on investigating alerts that falsely identify a benign file as a malicious one.

About Lastline

Lastline, Inc. provides breach protection products that are innovating the way companies defend against advanced malware with fewer resources and at lower cost. We deliver the visibility, context, analysis, and integrations enterprise security teams need to quickly and completely eradicate malware-based threats before damaging and costly data breaches occur. Headquartered in Redwood City, California with offices throughout North America, Europe and Asia, Lastline's technology is used by Global 5000 enterprises, is offered directly and through resellers and security service providers, and is integrated into leading third-party security technologies worldwide. **http://www.lastline.com**