Acronis

WHITE PAPER

Cyberattack techniques and what they mean for your business

What is a cyberattack and how does it work

Introduction

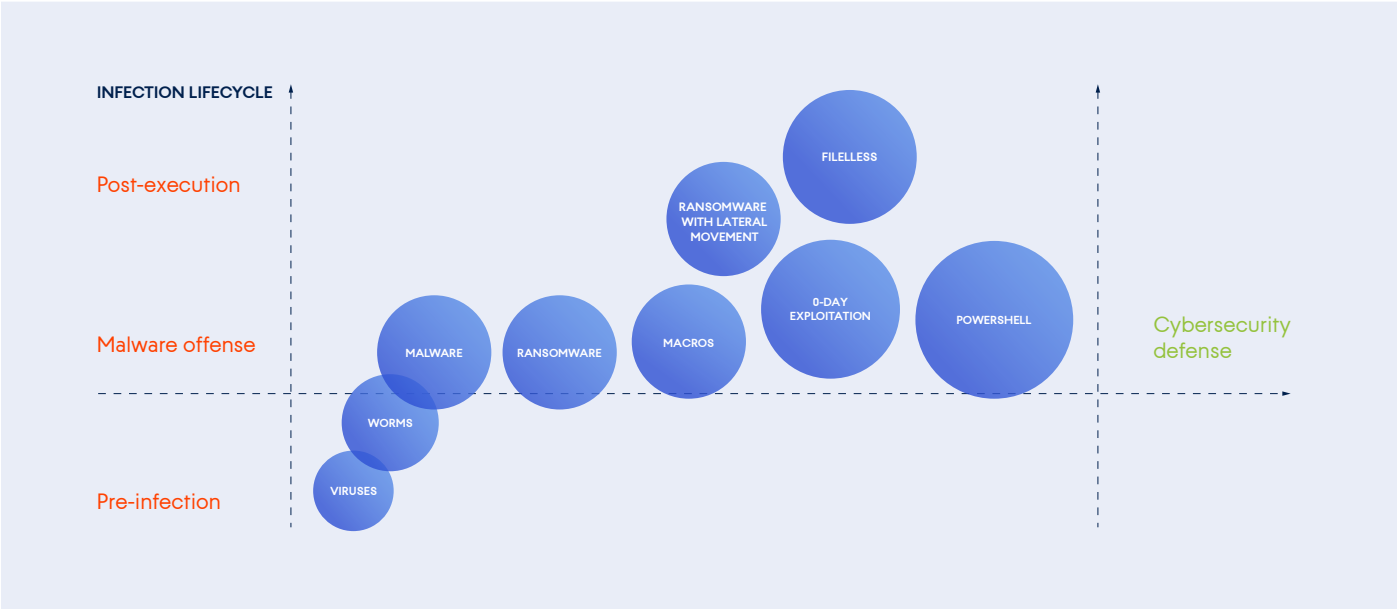
There are a lot of cyberthreats out there: different attack types and vectors designed to penetrate companies and home users cybersecurity. While cybercriminals usually pursue specific goals like money, data, or disruption, they use a wide array of malware and vectors of infection to achieve these goals. Good cyber protection and cybersecurity solutions should be able to deal with all of these. In this whitepaper, we will explain the different kinds of threats out there, the difference between cyber protection and cybersecurity in this regard, and how Acronis Cyber Protection Solutions are able to defend against all attack vectors to provide the ultimate end-to-end cyber protection.

WHAT IS A CYBERATTACK?

A cyberattack, on a high level, is a digital assault on a computer, smart device, or network. Cybercriminals use a variety of attack vectors and techniques to compromise and infect the system, and finally achieve their malicious goal.

It is important to distinguish mass and targeted attacks. Mass attacks are usually done via campaigns and involve an "as-a-service" scheme with a broad spectrum of victims. Campaigns can be spam, phishing, mass infection of legitimate sites, and so on. These kinds of attacks are automated and everyone can be a victim. On the other hand, targeted attacks are when the victim was specifically chosen and profiled in advance and such attacks are often performed manually. The most sophisticated targeted attacks are called advanced persistent threats (APTs) and these attacks usually involve many stages, can last for months, and are hard to detect.

All attacks include basic stages: preparation, infection, and post-execution. As you can imagine, if your security solution can't react to some of these stages, there's a high risk that the threat will be missed or detected too late.



Vectors of attack

There are several vectors of attacks and it is important to cover all of them with your security defense strategy.

THE MOST COMMON ATTACK VECTORS ARE:

- Email e.g. malicious attachments
- Drive-by compromise e.g. websites with browser exploits
- Exposed services e.g. vulnerable RDP servers
- Valid accounts e.g. account takeover
- Supply chain e.g. software update hijacking
- Hardware e.g. USB sticks

First, a key one, is over email. Attacks can come through both web and app email clients. The threat comes through email and can come in a variety of forms: malicious link, malicious attachment, social engineering, and so on. We will discuss all these options later.

Threats can also come via the exploitation of vulnerabilities in software, services, and more. Vulnerabilities are always bad but they're not dangerous until they're exploited. Unfortuately, whether you're a user or admin, you won't know if it was exploited or not. That's why you need to patch all known vulnerabilities and be ready for zero-day, unknown vulnerabilities without a patch available. Vulnerabililities can reside in an exposed server service, such as the Microsoft DNS server, which had a remote code execution vulnerability (CVE-2020-1350) fixed in July. However vulnerabilities also exist in client applications such as web browsers, and can get exploited when you visit a maliciously-crafted website, which is called a drive-by download attack.

You can be infected via an account takeover: a cybercriminal gains control over a legitimate account and performs malicious actions from it. For example, if cybercriminals guess a password and corrupt an admin account they can delete backups and copy confidential information.

Another vector of attack, somewhat similar to an account takeover, is called a trusted relationship or supply chain attack. It involves your partner or service provider getting compromised. If the software vendor of an application that you use is compromised, you might automatically download a malicious update from their site. This happened to ASUS early in 2019 when they got compromised and started unknowingly distributing an infected driver update.

Sometimes attackers make use of physical devices, such as a USB stick with malware on it, that is deliberately placed in public places or near a targeted business in the hopes that someone will be curious enough to plug it into their computer.

It's worth noting that with each of these attack vectors different attack techniques may be used. These are what people usually think of when we talk about security threats.

Cyberattack techniques

For all the different attack vectors, there are different methods and techniques that can be applied. Some are concepts that apply to various groups (such as social engineering) while other techniques (like sniffing) allow criminals to find useful information for further attacks.

SOCIAL ENGINEERING

Social engineering is all about the human element. The attacker creates a convincing story that will trick the user into performing certain actions. This is the most dangerous and effective cyberattack technique today. People are always the weakest link in security, because if you're creative enough you can convince people of doing practically anything.

Social engineering can be combined with an account takeover and impersonation attack, making it very difficult to discover. For example, if your boss's account is compromised, it will be difficult to verify that an email with instructions to open an attachment, was not sent by your boss. That is why even if you properly train your personnel regarding phishing scams, you still need to have a proper cybersecurity solution in place.

PASSWORD ATTACKS

A password attack is an attempt to obtain or use a user's password with illegal intentions. Cybercriminals can use password sniffers, dictionary attacks, and cracking programs to get a user's password. While largely useless with two-factor authentification in place, in some cases password attacks can be enough to get bad guys what they want. Password attacks can be prevented by simple common sense (do not tell anyone your password, do not write it down, do not use the same password on multiple services, etc.) and the usage of strong, long passwords or password managers.

PHISHING AND SPEAR-PHISHING ATTACKS

Phishing is a technique that employs fraudulent communications (emails, messages, SMS, and websites) that appear to come from a reputable source. The attacker impersonates legitimate service brands in other to use that inherent trust to trick people into sharing their credentials. For example, by creating a page that looks like the Office 365 web portal cybercriminals can steal user credentials in the background. It is a very popular attack technique and often goes hand-in-hand with social engineering. Phishing can lead you to disclose your confidential data (PII, financial data like credit card numbers, etc.), make you install malware, or visit an infected or malicious site.

Spear-phishing has the same goal but is specifically targeted to a person who is typically profiled over social networks in real-life before the attack. Spear-phishing is typically very convincing and hard to recognize unless detected by cybersecurity products.

DRIVE-BY ATTACKS

A drive-by attack is a stealthy and dangerous method of distributing malware. It's also a good example you can point to with friends who argue against needing cybersecurity by saying "I don't click on any links and don't visit any shady sites".

Typically drive-by works this way: cybercriminals utilize poorly configured or unpatched websites and inject malicious script into one of the pages. Once a user visits the website, this script will exploit a vulnerability in the browser or a plug-in and install malware into the computer. In most cases, these scripts are obfuscated and not easy to detect. These attacks are called drive-by because they don't require any action on the victim's part except visiting the compromised website.

EXPLOITATION OF A ZERO-DAY VULNERABILITY

A zero-day vulnerability is a software vulnerability that was not yet known to the vendor when it appeared in the wild and therefore has no patch available. Because of this, there are zero days available to protect yourself by patching. A zero-day vulnerability often comes with a zero-day exploit that can abuse the flaw. It is not easy to detect with average cybersecurity solutions as it requires deep system knowledge and constant monitoring of all applications. Eventually, every vulnerability becomes known, and the hole will be closed with a security patch. The problem is that sometimes it can take months, if not years.

SQL INJECTION ATTACKS

The Structured Query Language (SQL) is very often used in a servers, including web servers. SQL injection means that an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. For example, an attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box and receive all user accounts for this web application.

CROSS-SITE SCRIPTING (XSS) ATTACKS

Similar to SQL injection, cross-site scripting (XSS) is a kind of injection breach where the attacker sends malicious scripts into content from otherwise reputable websites. It happens because poor configuration or vulnerabilities make it possible to attach code into web applications, the malicious code is bundled together with dynamic content that is then sent to the victim's browser. The exploits can include malicious scripts in many languages including JavaScript, Flash, HTML, Java, and Ajax.

MALWARE ATTACKS

A lot of cyberattacks involve malicious software (malware for short). As we already explained, malware can get into the system in a variety of ways: downloaded and launched by a user, silently installed through a drive-by, silently downloaded and executed via a vulnerability, and so on.

MAN-IN-THE-MIDDLE (MITM) ATTACKS

Man-in-the-middle (MitM) attacks occur when attackers intercept traffic in order to steal or modify transmitted data: namely login information, passwords, financial data, and so on. The attackers pose as a legitimate service and will pass all traffic like a proxy. These attacks typically take place on unsecured public Wi-Fi networks, where attackers easily can insert themselves between a visitor's device and the network. Doing so they can install malware or redirect users to a malicious website. HTTPS is believed to help prevent these attacks but this is not true. Simple HTTPS encryption only secures the traffic to the server end, but does not verify the authenticity of the server endpoint.

Types of malware

Trojans

Sometimes called trojan horses, Trojans are the most prevalent type of malicious program. Trojans can't replicate like viruses but can do a lot of damage. Trojans not only launch an attack but also can create a backdoor for future attacks.

Ransomware

A very popular type of malware that prevents access to the system's data. Ransomware usually encrypts data through a very strong encryption algorithm so that there is no way to decrypt the data yourself. Instead, it demands a ransom in cryptocurrency to decrypt it. The attacker may also threaten to publish or delete sensitive information if the ransom is not paid.

Viruses

A malicious program that most media outlets and end-users incorrectly label every malware program. A digital virus modifies other legitimate host files (or pointers to them) in such a way that when a victim's file is executed, the virus is also executed. Pure viruses can replicate and are uncommon today.

Adware and PUA (Potentially Unwanted Applications)

Not that dangerous, but very annoying, software programs used by dodgy businesses as part of their marketing efforts. They usually manifest as advertisements or banners displayed while applications are running.

Worms

The distinctive trait of the worm is that it's self-replicating and spread over networks. Worms are dangerous because they can spread without end-user interaction.

Root and Boot kits

Sophisticated malicious programs that hide themselves in a master boot record on hard disks or hide their presence in the operating system. Originally, a rootkit was a collection of tools that enabled administrator-level access to a computer or network. Today rootkits are rare and generally associated with malware – such as Trojans, worms, and viruses – that hide their presence and actions from users and other system processes.

Spyware

This type of malware is designed to collect information on the victim's machine. Spyware tracks everything you do without your consent or knowledge and delivers the information directly to a remote cybercriminal. It can also install other malicious applications onto your system via the internet.

Scripted malware or malicious scripts

These were previously known as macro viruses. But in general, they're any kind of script executed by a legitimate program to perform malicious activity. In recent years they've been wrongly associated with fileless attacks. But if you think of the term, the script is still a file in a hard drive or any other storage source.

Botnets

Your machine will be controlled by someone to perform malicious activities like spreading malware, Denial-of-Service, and Distributed Denial-of-Service attacks. A bot alone is relatively harmless, especially when it's not connected to the Command and Control server. That's why bots are combined into botnets and a botnet can do significant harm like completely disrupting business operations.

Fileless attacks

Fileless attacks are a type of cyberthreat that's often associated with malware and exploits. There are many definitions with slight variations for fileless attacks. To put it simply, fileless attacks are attacks without a specific malicious file on disk.

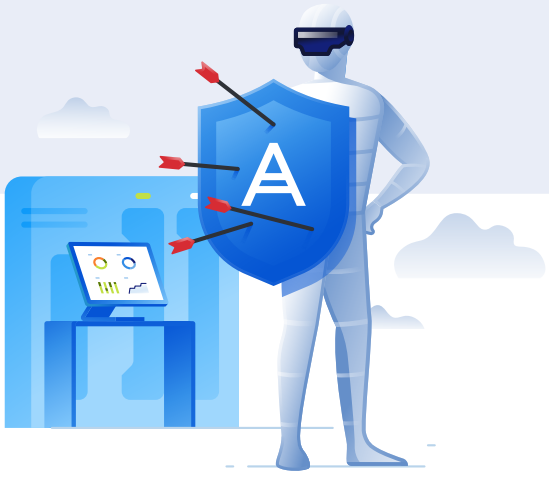
A fileless attack leverages legitimate apps and processes to perform malicious activities like privilege escalations, payload deliveries, data gathering, and so on. This technique, when preinstalled legitimate software is used in a fileless attack is often called living-off-the-land. Very often we see that only some phases of an attack chain use fileless techniques, thus making the whole attack technically not fileless.

All this can happen in random access memory (RAM) only and leave no traces after a machine reboot. That means when one of these attacks strikes nothing related to malicious activity should be written to the target hard drive, meaning that fileless attacks are very much resistant to existing security detection technologies like file-based whitelisting, signature detection, hardware verification, etc. because they leave practically no evidence that could be used by digital forensic investigators to identify and understand the attack later on.

HOW ACRONIS CYBER PROTECTION SOLUTIONS DEAL WITH THESE ATTACK TECHNIQUES

It's important to use cybersecurity and cyber protection solutions like Acronis Cyber Protect Cloud or the on-premises solution Acronis Cyber Protect to stop these potential cyberattacks and keep systems and data safe. The problem facing the modern cybersecurity industry is that it's very hard to find a product that can protect you from all of these types of threats and quite often business have to use multiple solutions or compromise and leave some holes in their security perimeter, which is both dangerous and ill-advised. Typical cybersecurity solutions can't protect data and deliver quick recovery and good business continuity.

Acronis Cyber Protection Solutions, which combine cybersecurity and data protection, is the closest to the ideal solution to address all of these threats. It provides innovative integrated multilayered protection with well-tuned technologies inside each solution that work to stop the threats explained in this white paper. This is what we call the Acronis Cyber Protection approach. Let's take a look at the following table which covers all the vectors and techniques explained before and corresponding Acronis security technologies.



ACRONIS SECURITY TECHNOLOGY			
ATTACK VECTOR OR TECHNIQUE	**PROACTIVE STAGE**	**ACTIVE STAGE**	**REACTIVE STAGE**
Attack over email		URL filtering	URL filtering, Behavioral engine, Static AI-analyzer, Cloud detection, Exploit prevention
Usage of vulnerability, including Zero-Day vulnerabilities	Vulnerability assessment, Patch management	Exploit prevention	
Account takeover			URL filtering, Behavioral engine, Static AI-analyzer, Cloud detection, Exploit prevention
Trusted relationship or supply chain attack			URL filtering, Behavioral engine, Static AI-analyzer, Cloud detection, Exploit prevention
Social Engineering		URL filtering	URL filtering, Behavioral engine, Static AI-analyzer, Cloud detection, Exploit prevention
Phishing and spear-phishing attacks		URL filtering	URL filtering
Fileless attacks	Vulnerability assessment, Patch management	URL filtering, Behavioral engine, Cloud detection, Exploit prevention	Static AI-analyzer
Drive-by attacks		URL filtering, Behavioral engine, Exploit prevention	
Malware attacks		Behavioral engine, Cloud detection, Exploit prevention, Acronis Active Protection, Static AI-analyzer	Static AI-analyzer
Man-in-the-middle (MitM) attacks		Behavioral engine, Cloud detection, URL filtering	Static AI-analyzer
Password attacks	2FA	Brute-force detection	
Botnet inclusion		Behavioral engine, Cloud detection	Static AI-analyzer
Tampering			Acronis Notary (via blockchain)
SQL injection attack		URL filtering	
Cross-site scripting (XSS) attacks		URL filtering	

PROACTIVE (OR PREVENTIVE) STAGE

You get ready for threats in advance, patch systems, use authentification, etc.

ACTIVE STAGE

Security technology detects an active threat or attack which executes in the system right now.

REACTIVE STAGE

A threat may be in the system already, or the first stage of the attack is executed. For example, you received a phishing email. It is important to understand, that even if a threat is in the system it doesn't mean the system received any damage, as the actual payload can be downloaded much later. And in this stage it will be detected.

AS YOU CAN SEE, ACRONIS SOLUTIONS WITH THEIR INTEGRATIONS AND MULTILAYERED SECURITY STACK CAN DEFEAT ALL OF THESE TECHNIQUES AND KEEP YOUR SYSTEMS AND DATA SAFE.

Acronis

Learn more at
www.acronis.com