14 February 2022 Dave Kostos

Common cyberattacks and the tactics behind them

Cyber Protect
formerly Acronis Cyber Backup

Cyberattacks are common for businesses of all sizes and across all industries. Many companies work diligently to guard against cyberattacks, and over the years, they have found tried-and-true techniques to combat these attacks and minimize their impact.

But businesses aren't the only ones learning the ins and outs of cyberattacks. In fact, cybercriminals commit significant time, energy and resources to become masters of their craft. These criminals frequently fine-tune their attack tactics, and as a result, they are well-equipped to launch successful attacks.

A clear understanding of common cyberattacks and the tactics behind them is paramount for today's businesses. If you know these attacks and tactics, you can plan accordingly; but most importantly, you can optimize your security posture.

Now, let's look at three of the most common cyberattacks and their associated tactics.

1. Ransomware

Ransomware refers to malicious software that prevents users from accessing their files, systems, or networks. It ranked first among the most prolific cyberthreats for large companies and small and medium-sized businesses (SMBs) during the second half of 2021. This is due in large part to the biggest cyber ransoms paid to date are: millions of dollars in ransoms that cybercriminals can extort from victims.

CWT Global ($4.5 million)

Colonial Pipeline ($4.4 million)

Brenntag ($4.4 million)

Travelex ($2.3 million)
University of California at San Francisco ($1.14 million)
The FBI recommends victims don't pay cyber ransoms, as doing so offers no guarantees. It also does nothing to deter cybercriminals from continually launching ransomware attacks.

2. Phishing

Phishing emails are perhaps the most popular technique used to spread ransomware. They take place every day and have affected Facebook, Google and other globally recognized brands. And phishing attacks show no signs of slowing down any time soon.

A typical phishing email can look harmless at first glance. The email likely includes an engaging subject line, which leads someone to open it. Once an email recipient opens the email and clicks on the attachment contained within the message, malicious software infects the victim's device. All it takes is one phishing email to disrupt an entire organization. For example, if an employee opens a phishing email on their business device and downloads its malicious attachment, ransomware gets loaded onto their device. From there, the hacker can infect any devices and systems linked to the victim. And the hacker can potentially lock out all users across business systems until a ransom is paid.

There has been no shortage of phishing scams. Some of the largest and most notable ones include:

1. FACC

An employee at Austrian aerospace parts manufacturer FAC got an email that appeared to come from its CEO. In the email, the sender asked the employee to transfer approximately $48 million to a bank account as part of a new project. The employee fulfilled the request, despite the fact that the account belonged to a cybercriminal.

2. Crelan Bank

A cybercriminal once spoofed the email account of the CEO of Belgian firm Crelan Bank. The criminal emailed the employee and asked the worker to transfer funds into an account controlled by the attacker. This resulted in more than $86 million in losses for Crelan.

3. Sony Pictures

Acronis is no stranger to phishing emails. At one point, one of our C-level executives received a phishing email that Several Sony executives received phishing emails from someone they believed was with Apple. The executives opened the emails, which asked them to provide ID verification. When the executives complied with the request, hackers were able to capture their login credentials and caused over $100 million in damages.

The executive who received the email works with invoices on a daily basis. And the cybercriminal appeared to know this before sending the email, which was apparent in the message's theme.

Meanwhile, the phishing cyberattack included several malicious links in the email the executive received. It was easy for our executive to tell that the email and these links were dangerous, but for someone with little to no cybersecurity experience, this might have gone unnoticed. And this same individual might not have checked the email client — which did not show by default in the phishing email our C-suite executive received — either.

For phishing emails, keep an eye out for anything out of the ordinary. Shortened URLs, for instance, are common in phishing emails. Plus, in a phishing email, you may notice you can't find the actual address of a URL in an email if you hover over it.

Many organizations use web filters to prevent phishing emails from reaching their employees. Regardless, the best cybercriminals tailor their phishing emails in a way that can bypass spam filters. On the other hand, if you teach workers how to identify the signs of phishing emails, you can stop phishing hackers in their tracks.

3. Malware

Malware, aka malicious software used to damage a system or steal data, is often used for financial gain or as part of a state-sponsored attack. It comes in many forms, including:

Adware

Ransomware

Spyware

Worms

Trojans

There are many examples of malware attacks that have impacted businesses from around the world, including:

CovidLock

LockerGoga

WannaCry

Petya

CryptoLocker

Email attachments and links represent two of the most common malware attack vectors. For example, a cybercriminal can send an email that contains a malicious attachment or link. The hacker may send an email to a business employee that appears to come from a legitimate source. If the employee downloads the attachment or clicks on the link, malware is loaded onto their system. The malware can then spread across all systems linked to it.

Cybercriminals can use "fileless" malware, too. In a fileless malware attack, a cybercriminal embeds malicious code into a native scripting language or into PowerShell or a similar program. Or, a cybercriminal can leverage fileless malware to exploit a public-facing web server and use a web shell to move laterally in a user's environment.

We're all too familiar with malware and the damage it can cause. Yet we know how to handle malware, which is reflected in our work with Homebuys. HomeBuys is a discount retailer with the tagline: "The Best for Less." The retailer managed more than 1.5TB of historical data. When Homebuys needed a data protection solution, it Acronis Cyber Protect "has a lot of value and is extremely useful," a HomeBuys network administrator noted. It provides HomeBuys with one console for patch management, vulnerability assessments, backup, recovery and anti-malware. And Acronis Cyber Protect was easy to set up, install and use.

How to combat common cyberattacks and the tactics behind them

There is no one-size-fits-all approach to protect against cyberattacks and the tactics behind them. Conversely, there are several things you can do to stay safe against current and emerging cyberthreats, including:

- **Watch for suspicious email attachments and web links.** Do not download attachments or click on links from unknown senders.
- **Back up your data frequently.** Establish a system that ensures you can quickly and easily recover your data at any time.
- **Update your software regularly.** Install software patches and updates as soon as they're available.
- **Use two-factor authentication.** Require multiple methods of authentication to provide access to devices, networks, and systems.
- **Provide cybersecurity awareness training.** Offer cybersecurity awareness training to keep employees up to date on new cyberthreats and how to guard against them.

Finally, if you're ready to transform cyber protection across your business operations, Acronis Cyber Protect to learn everything you need to know about Acronis Cyber Protect. To get started with Acronis Cyber Protect, can help. Our cyber protection solution combines cybersecurity, data protection and management. You can use Acronis Cyber Protect to secure your endpoints, systems and data. In doing so, you can avoid downtime, data loss and security breaches.

About Acronis

A Swiss company founded in Singapore in 2003, Acronis has 15 offices worldwide and employees in 50+ countries. Acronis Cyber Protect Cloud is available in 26 languages in 150 countries and is used by over 20,000 service providers to protect over 750,000 businesses.

Stay up-to-date