eBook

datto

How Hackers Plan Their Attacks and How to Defend Against Them

Introduction

The costs of cybercrime reach far beyond the ransoms paid. It encompasses the costs of the damage and destruction of data, lost productivity, theft of intellectual property, theft of personal and financial data, and not to mention reputational harm. With cybercrime costing businesses roughly $6 trillion a year and the average payout estimated to be $200,000 for each attack, it is easy to understand why the business of being a hacker has become so appealing and lucrative.

That is why now more than ever, to protect your business from hackers, you must understand how they work.

How attacks are planned

Just like many things, there is a formula, and the same holds for cyber attacks. They are planned from who is targeted to how access will be gained, what tools will be used, and what will happen once access is attained.

A typical cyber attack plan looks like this:

1. **Planning:** The hacker decides what kind of attack and how the attack is executed. In the case of this e-book, we will focus on a common delivery of malware - mainly ransomware and phishing attacks.
2. **Dropper:** They borrow or create a dropper – a simple piece of code that is disguised to trick you into inadvertently placing it onto your computer. It's usually triggered by clicking on a hyperlink or concealed in an innocent-looking file, so you don't even know it's there. When run, the dropper fetches and installs a malicious payload onto your computer.
3. **Payload:** A high-precision piece of innovative malware created and hidden somewhere in cyberspace. It's poised to cause the victim significant damage upon command.
4. **C2:** Command & Control (C2) Center is just a fancy name for the hacker's tools and techniques that enables the whole exercise.
5. **Execution:** Ransomware execution is unique. Once the dropper delivers the payload and it executes, a computer, server systems and files become locked (encrypted) forcing the business to pay a ransom to the hacker to unlock (unencrypt) files and/or servers.

Hackers look for easy-to-penetrate endpoints. As endpoints are connected to the Internet 24/7, even when nobody is working on them, they are stagnant. They provide a place where hackers can take their time to see what kinds of security mechanisms are installed and what is the best way to gain access. The easiest way to gain access is to penetrate endpoints, finding a person who already has access, and tricking them into letting the hacker in. Once they have access to one endpoint, it becomes quite easy to jump to another and another before you catch onto what they are doing.

Creating a dropper

Malware can be sent directly, so why bother with a dropper?

A dropper is lightweight and camouflaged in a file; a file one would be intrigued to open. It could look like a calendar invitation, a purchase order, or a CV from a friend. The dropper lies low, it is the element that penetrates your computer once you click on an email attachment, and a dropper executes its malware payload that can stealthily be sitting on your drive. Even more startling, a company's Antivirus is unlikely to find it.

The dropper's job is to fetch a malicious payload and is done in several ways by:

- Exploiting an unknown or **new vulnerability**, a Zero-Day, which takes advantage of an unfound weakness in an operating system or application that can be manipulated to run the hacker's code. This is VERY difficult and time-consuming. Such a vulnerability can be purchased, but that will be very expensive (could be millions of dollars). It will be discovered quickly, and the cybersecurity companies will provide patches for it right away.
- Using a **known vulnerability**, an N-Day, and exploiting the fact that many organizations tend not to deploy patches so often, so it might still be effective. Many EMOTET droppers that went this path were able to gain access to the personal data of hundreds of thousands of US healthcare patients and bank account holders.
- Writing a **malicious VBA macro**, a scripting language for MS Office files, to hide true intentions.

Many IT departments struggle to keep up with security patches in a timely manner, so the second option of abusing a known vulnerability works in enough cases to make a hacker successful in their attack.

To answer our question of why use a dropper? First, because droppers are cheap, easy, and readily available, and second because many droppers can evade antivirus software, firewalls, and other security safeguards.

Those labeled “CV” are even more likely to be opened, as studies show that people tend to open CVs even from contacts they don’t know in person.

Dropping the Payload Successfully

A few things from both a practical and technical standpoint that attackers need to look at when deciphering how to deliver the payload successfully. This includes various ways to hide the true nature of the email and website in question to ensure the delivery of the malware.

- **Attachments**
  Because most people trust MS-Word files without hesitation, hiding a dropper in a docx file attachment to an email with a catchy name that people like to click on works quite well, and it doesn’t have to be just a docx file. A dropper can be hidden in pdf, excel, ppt, and even images or calendar invitations just as easily as long as the end result equals successful delivery. If 100,000 emails are sent, then the law of averages means that some significant number of recipients will click on the attachment. After all, 1% of 100,000 equals 1,000 “conversions” - or computers that the dropper can infect.

- **Email delivery obstacles**
  Other challenges include deciding how the email will be delivered

  - Anonymity - Anonymity is the key to the success of the operation. Sending attachments from free email vendors like Gmail and Yahoo requires validation most hackers set up fake or “spoofed” email accounts, or use email accounts that have already been compromised for sending malicious email.

  - Flagged as Spam - if the email is flagged, it will reduce conversion rates. To prevent this, a variety of outgoing mailboxes will be needed. Previously hacked email addresses and passwords and personal identifiers are perfect for higher credibility and diversity, making it harder for spam filters to catch.

Remain untraceable

For a hacker, the goal is to get paid and not get caught. Different IPs, software that cloaks IP addresses, and hacked routers make it challenging to trace them, and plenty exists to complete this step efficiently. There is also the creation of a Command and Control (C2) Center far away from the reach of those targeted. The C2 can use cloud-based services, such as webmail and file-sharing, to blend in with average traffic and avoid detection.

If the malware payload is designed to extract data, it delivers it to the C2. The malware will encrypt the files on the target computer until a ransom is paid.

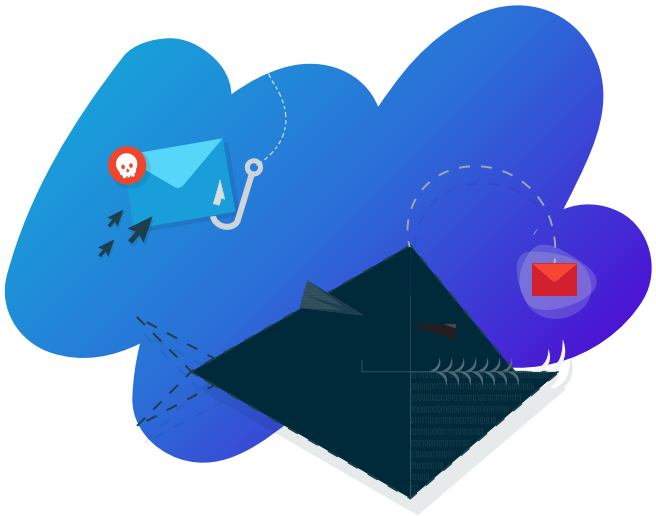
You've got mail - Phishing for access

Phishing is a fraudulent attempt to obtain sensitive information or data, such as usernames, passwords, and credit card details. This is done by disguising oneself as a trustworthy entity in an electronic communication and using "social engineering" tactics to psychologically manipulate a person into performing actions or divulging confidential information. Malicious actors will use every trick in the book to get people to take action. Email is the most common way hackers gain access to network data because it is ubiquitous, it's anonymous, and most hackers can spoof an address and send thousands of them from anywhere.

96% of attacks are delivered this way, as it's easy to obtain volumes of authentic email addresses. Lists are abundant, and they're virtually free to get, allowing a download of 100,000 emails in a few seconds.

96% of phishing attempts use email as the primary delivery vector.

— Source:
Verizon's 2021 Data Breach Investigations Report



Common types of phishing attacks

The days of bad phishing email attempts are gone. Many phishing attempts can look surprisingly legitimate. There are many types of phishing attacks, and they continue to grow. Some of the most common are:

1. **Mass campaigns**
   Wide net phishing emails are sent to the masses from a knock-off corporate entity asking them to enter their credentials or credit card details. Attacks that rely on email spoofing appear as if a trusted sender sent them, but there are few telltale signs to look for:

2. **Spear phishing**
   Directly targets a specific organization or person with tailored phishing emails.

3. **Whaling**
   Whaling refers to spear-phishing attacks directed specifically at senior executives and other high-profile targets in an attempt to gain access to company platforms or financial information.

4. **Clone phishing**
   The attacker copies a legitimate email message sent from a trusted organization and replaces a link that redirects to a malicious/fake website.

5. **Pretexting**
   Pretexting involves an attacker doing something via a non-email channel (e.g., voicemail) to set an expectation that they'll be sending something seemingly legitimate shortly only to send an email that contains malicious links.

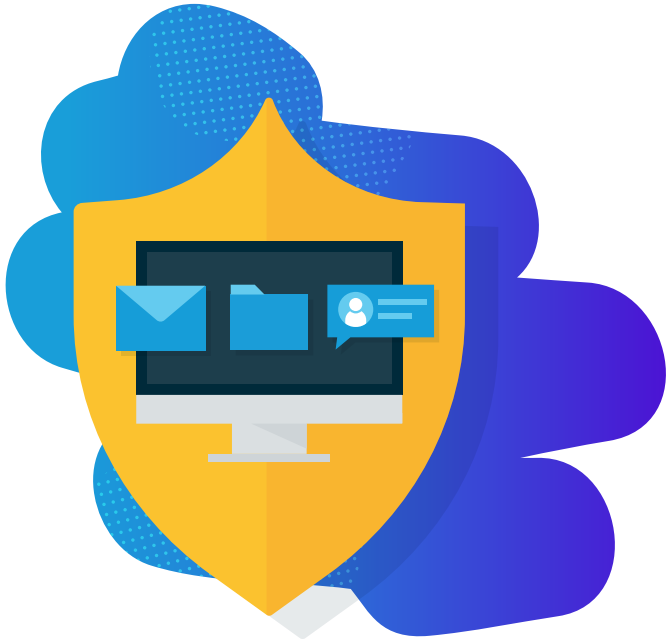
The phishing landscape

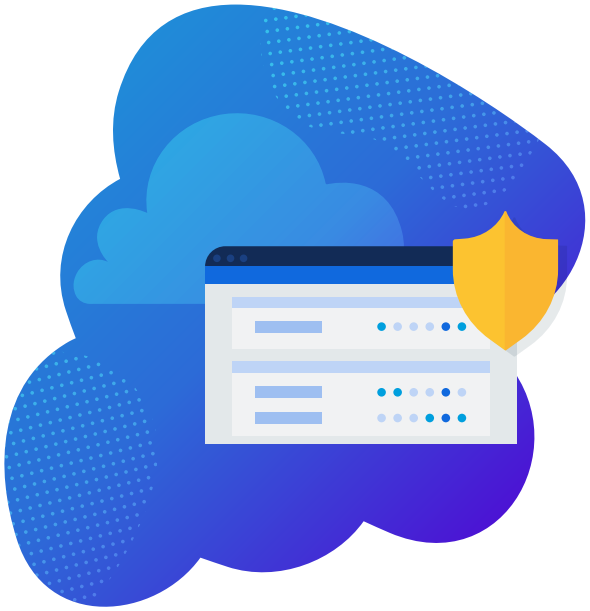
While email is likely to be the primary way attackers deliver phishing attacks for a long time to come. Increasingly attackers are leveraging collaboration platforms such as Zoom, MicrosoftTeams, LinkedIn, and Facebook to perpetrate phishing attacks. As more people work remotely and need to collaborate quickly and effectively, these types of attacks are likely to skyrocket. Some solutions address the threats and help MSPs combat them.

SaaS Defense:
Advanced threat protection against phishing attacks

Phishing messages are crafted with the end goal of capturing sensitive data. If your clients fall prey to phishing scams, it can affect both company networks, yours and theirs, by transferring malware and viruses over internet connections. It can also affect additional third-party vendors, customers, and partners. Why? because if their email was compromised, the hackers can take control over the compromised email and use it to send malicious emails to other organizations they work with.

Protect and defend your clients' critical cloud data against both known and unknown cyber threats and common data loss scenarios with comprehensive detection, protection, and recovery from a single, channel-focused vendor. SaaS Defense provides MSPs with an advanced threat protection, and spam filtering solution for Microsoft 365. SaaS Defense closes detection gaps by proactively monitoring, detecting, and eliminating unknown cyber threats such as ransomware, that other solutions miss with data-independent technology designed to analyze the composition of safe email, OneDrive files, SharePoint sites, and Teams chat. This first encounter detection eliminates the time needed to detect an intrusion by detecting at the first encounter instead of days later, with a data-independent solution.





Proven Patented Technology and Comprehensive threat protection

- SaaS Defense detects malware at the dropper stage, therefore stopping malicious payloads before they can execute.
- SaaS Defense detects either the malicious email or the malicious webpage before the user clicks the phishing link.
- SaaS Defense's advanced threat protection goes beyond just email and proactively defends against malware and phishing threats that target Exchange Mail, SharePoint sites, OneDrive folders, and Teams chats.
- Direct access to Datto security experts with a single-vendor solution saves time, eliminates confusion, and provides an extra level of confidence when deploying new technology.

Learn more about
Datto SaaS Defense

datto