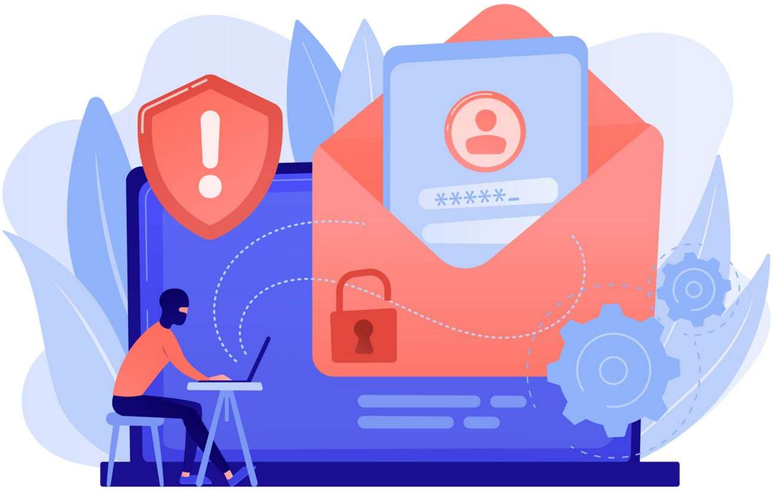
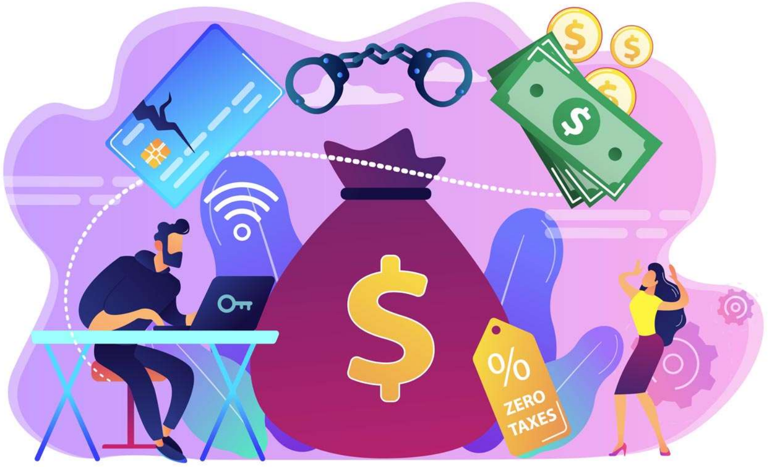
Types of Cyberattacks that Threaten Businesses, Part II: Phishing, Brute Force Logins & Denial-of-Service Breaches

By Ryan Zanoni



In this second installment of our article series exploring different types of cyberattacks that pose a danger to businesses, we'll examine three additional kinds of popular tactics employed by criminals, along with examples, and discuss how to counter them.

Over the past several years, we have witnessed hackers becoming even more bold and sophisticated in their schemes and committing more damaging attacks than ever before. It has never been more important for companies to be prepared to defend themselves and their customers against established and emerging types of cybersecurity threats. That readiness depends on learning how these breaches work and what went wrong security-wise that allowed them to happen in the cases referenced below, as well as what strategies and tools can be utilized to prevent or mitigate them in the future.



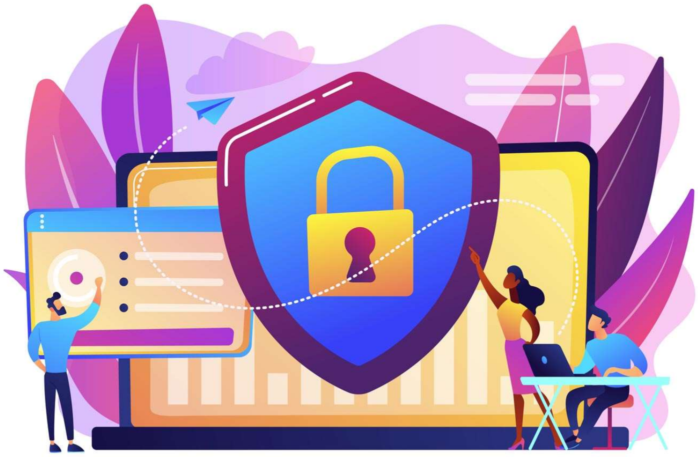
Phishing and Spear-Phishing Scams

Phishing and spear-phishing are oft-used types of cyberattacks in which hackers send authentic-looking emails and text messages to their targets in order to steal personal and financial information. The messages often ask victims to update, validate or confirm accounts. During a phishing scam, the audience is broad and indiscriminate; in spear-phishing, hackers target specific individuals.

Although people talk about them often and enterprise IT pros continue to work hard to stop them, phishing scams still work and are relatively inexpensive and easy to run, which is why they persist. According to tracking by IBM X-Force Incident Response and Intelligence Services (IRIS), in 2018 and 2019, offenders used phishing as an entry point for 33 percent of cyberattacks.

Phishers prey on recipients' emotions with their words, drawing them in right away. Criminals' ability to generate genuine-looking emails with plausible logos, letterheads and language, as well as topics of interest to the target audience, enables them to deceive even the most security-savvy users. And they often use phishing as a vehicle to launch other attacks, such as malware.

Additionally, people — especially those working from home — are often inundated with emails, while environmental pressures like public health crises, economic recession and civil unrest add more stress to their personal and work lives. Hackers exploit the confluence of these two factors to take advantage of these folks by sending fraudulent communications, and unfortunately, this has resulted in more people falling for phishing attacks.



Real-World Examples:

2013 and 2014 Yahoo Hacks

In 2013, Yahoo fell prey to a phishing scam and malware attack that was the largest cyber breach in history, ultimately compromising all three billion user accounts that were active at the time. The culprits, who are believed to be Russian and may have been working for the Kremlin, sent emails with malicious links; once recipients clicked, the hackers were able to steal their personal information, including names, email addresses, phone numbers and dates of birth, along with passwords and security questions and answers. While the passwords were not visible in clear text, they were protected by outdated encryption that was easy to crack.

The very next year, Yahoo was hit again with a spear-phishing attack by criminals affiliated with the Russian government, who gained access to the emails and private information of up to five hundred million users. As stated by the FBI, Aleksey Belan, a Latvian hacker recruited by the Russian state security service, initiated the attack with an email sent to a single Yahoo employee. The total numbers of employees targeted and emails deployed were unknown, but the criminals' scheme only required one recipient to click on a link in order to be successful.

Once Belan had access, he located Yahoo's user database and the Account Management Tool with which to edit it. He also installed a backdoor into the server to avoid losing access and stole a backup copy of the database, which he transferred to his personal computer.

COVID-19 Relief Fraud

The coronavirus pandemic of 2020-21 brought on a new wave of digital attacks. Unscrupulous lawbreakers have exploited business owners' struggles and dependence on government relief loans from the CARES Act, impersonating federal workers and contacting these owners to deceive them into divulging their personal information.

According to the FTC, there were numerous reports of business owners receiving emails that appeared to be related to government-sponsored loan programs but were actually phishing messages from criminals. The emails, which featured the logos and branding of the U.S. Small

Business Administration (SBA) as well as spoofed sender addresses that seemed to be from the agency, stated that the recipients were eligible for loans up to $250,000 and asked them to input their names, addresses, cell phone numbers, birth dates and Social Security numbers. Some of the messages directed people to the login page of a phony SBA website. There were three phases of these emails sent to business owners during the pandemic in 2020, the last of which instructed recipients to enter their bank account information.

Lessons and Solutions

Knowledge is Power

Business owners, executives and IT directors can protect their companies against phishing by educating their employees in how to recognize the signs and avoid risky behavior online. This might include directives to refrain from filling out forms embedded within emails or providing sensitive information digitally, as well as instructions to ignore generic-looking requests for personal data.

As a way of testing employees and assessing their companies' overall risk levels, IT teams can also run phishing simulations by sending emails that mimic such attacks but are not actually malicious. There are even tools that can track which employees opened the test email and which ones clicked the link therein.

When it Comes to Passwords, Less Isn't More

After the Yahoo hacks, cybersecurity experts warned that these attacks were likely to lead to further cases of email fraud and account hijacking, because many of the three billion Yahoo users impacted were utilizing the same passwords for different sites and services.

This highlights the importance of diversifying passwords as much as possible across sites and platforms, as well as the risks of saving passwords in convenient digital keychains on one's computer. Some cybersecurity experts have cautioned against the use of such keychains, which have been hacked before, thus giving bad actors access to numerous passwords at once.

Trust Old-Fashioned Conversations Over Electronic Messages

The SBA scam during the COVID-19 pandemic underscores a great low-tech recommendation from security experts: Whenever one receives a message purporting to be from a government agency or company and asking one to provide personal information, the recipient should immediately call that agency or company directly, using the phone number listed on the organization's website, to determine whether or not the correspondence is legitimate.

Password Attacks/Brute-Force Logins

In this old type of cyberattack, hackers attempt to figure out passwords or encryption keys to gain access to databases, accounts and other sensitive digital spaces. They may obtain a list of employee names or access to a web page, then conduct trial-and-error experiments to run through as many combinations of available data as possible, until they are successful in breaching the system. The investment of time required varies based on the length and complexity of the password or key — cracking the code can take as little as several seconds or as long as several years.

Often, the hackers will use particular software programs or other tools to try to speed up the process and make it more effective. These resources can work against FTP, MySQL, SMPT and Telnet computer protocols; infiltrate wireless modems; decrypt passwords located in encrypted storage; generate and attempt all possible combinations of characters; and execute dictionary attacks (explained below).

This type of cybersecurity threat comprises the following categories:

- *Simple Brute-Force Attacks*: Hackers try to guess login info or credentials using logic, with no software or other tools to help them; this is sometimes enough to crack simple passwords.
- *Dictionary Attacks:* Hackers target a specific username and then use a dictionary to generate possible passwords based on a pre-defined list of commonly used words.
- *Hybrid Brute-Force Attacks* Perpetrators combine the simple logic-based scheme with an outside resource, e.g., a dictionary or a software program, to increase their chances of figuring out more complex passwords that blend characters and numbers.
- *Reverse Brute-Force Attacks:* Criminals start with passwords they've stolen or purchased (often from online lists leaked on the dark web after data breaches) and then search millions of usernames to find a match.
- *Credential Stuffing:* When a crook has had success breaking into one online account with a password-and-username combination they've obtained, they try that same login info on other websites.

Real-World Example:

Alibaba Attack

One of the most prominent brute-force attacks took place during the fall of 2015, when hackers in China tried to break into more than 20 million active accounts on Alibaba Group Holding Ltd.'s Taobao e-commerce website. A state media report said the perpetrators used Alibaba's own cloud computing service in the attempt, while another report from a website managed by the Ministry of Public Security stated that they acquired a database of 99 million usernames and passwords from various websites.

Next, the hackers entered the account details into Taobao, discovering that over 20 million of the Alibaba accounts were also being used on the e-commerce site. They then faked orders via some of the compromised accounts and sold others to be used for fraud. Alibaba reported the breach to police immediately upon learning of it, and the hackers were apprehended.

Thankfully, the company's systems reportedly caught and blocked the clear majority of the hackers' log-in attempts.

Lessons and Solutions

To a certain extent, warding off password attacks is fairly straightforward. Companies can encourage their employees to use passwords that are not easy to guess (e.g., Alibaba123) or made up of simple keyboard progressions (such as "qwerty"), but rather, complex and consisting of combinations of letters, numbers and special characters.

They can also remind employees not to reuse passwords for different accounts and websites and not to save them in digital keychains on their computers. Additionally, they may require passwords to be changed frequently.

If employers want to add extra layers of security — as cybersecurity experts would strongly recommend — they can require two-factor authentication for all logins, cause accounts to automatically lock after a certain number of failed login attempts, buy time by adding increasingly longer delays between these login attempts or require Captcha tests to block robots that have been programmed to hack into systems.

Another great option is to increase the level of encryption of all passwords to 256-bit for more robust protection. And there is also a technique known as "salting the hash," which involves adding a random string of characters to hashed passwords, so that hackers have to work harder to determine which letters and numbers are actually part of the password and which ones are not.

Denial of Service (DoS)/Distributed Denial of Service (DDoS)

Denial of Service (DoS) attacks are most often used against large companies and organizations. Their point is to shut down the system or website in question. The hackers exploit one system vulnerability and use it to send massive quantities of data to the rest of the network, until the system is so inundated that it becomes extremely slow or unable to function at all. In DoS attacks, hackers go through a single computer; in Distributed Denial of Service (DDoS) attacks, they use several. Perpetrators can execute these operations for various purposes, including censorship, protest and extortion.

There was a 12 percent uptick in DDoS attacks in the latter half of 2020, especially those that utilized the simple services delivery protocol (SSDP) and the simple network management protocol (SNMP). The culprits employed botnet swarms, enabling them to amplify IP requests and overpower enterprise networks, which slowed down response times in some instances and suspended services in others. SNMP exploits are even more troublesome, because this protocol connects and manages common business devices, meaning that when hackers compromise a system in this way, they're largely immune to the counterattack efforts of the network firewall.

Real-World Example:

Attack on Dyn

The Internet service company Dyn, which routes and manages traffic for major web-based services, was hit by a DDoS attack on its domain name service in the fall of 2016. The crime resulted in service interruptions and outages that prevented millions of users in various regions of the U.S. and Europe from accessing Amazon, Netflix, Twitter and Spotify, in addition to the online forum website Reddit, the crafts marketplace Etsy and the software developer site GitHub. The event also seems to have impacted other popular sites, as Gizmodo received reports of problems associated with accessing content for leading media companies, including CNN, The Guardian, Wired, HBO and People, as well as the money transfer service PayPal.

Service was first restored within a couple of hours, but just a few hours after that, Dyn suffered another cyberattack that led to more widespread outages.

Ben Johnson, a former engineer with the National Security Agency and founder of the cyber-security company Carbon Black, explained that the increasing interconnection of ordinary devices to the Internet, known as the "Internet of things," raised networks' risks of being attacked.

Lessons and Solutions

Protecting against DoS and DDoS attacks requires organizations to update software regularly. They need agile, adaptable tools with the capacity to discover, isolate and stop distributed attacks as they happen, such as IBM's QRadar Network Security IQNS (XGS) and Network IPS (GX) appliances.

Both of these applications provide the ability to quarantine DoS and DDoS attacks, and the QRadar also lets you create a Network Access Policy rule using an IP Reputation object to safeguard against these breaches.

Another helpful tactic is to monitor data flow to see if there are any unexplained spikes in traffic. Companies may buy extra bandwidth to handle traffic spiking or specific tools to detect DDoS attacks as well.

Having the right tools is half the battle, but knowing how to use them effectively is the other half. Because defending against established, emerging and future web-based attacks requires such a thorough knowledge base and advanced skill set, many professionals are finding that an online cybersecurity education is their best weapon against hackers and other criminals.

Your Future in Cybersecurity

Because computers affect nearly all aspects of modern business and government, protection against phishing, brute-force, DoS/DDoS and all other types of cyberattacks is paramount. For individuals who wish to be part of an exciting field full of opportunities, the Bachelor of Arts, Bachelor of Science or Bachelor of Applied Science in Cybersecurity degree from Eastern Oregon University provides the education and training necessary to face the challenges of today and tomorrow, featuring a curriculum taught by experienced instructors who are real-world industry professionals. Designed for ultimate flexibility, the program allows students to study on their own schedules while still giving them the ability to interact with their professors and classmates.

To learn more, fill out the form located here or call Eastern Oregon University at 855-805-5399.