CYBALT

# Phishing And Ransomware Attacks

Cybalt Inc. Suite #510, 2701,
North Dallas Parkway, Plano, TX

discover@cybalt.com

## Phishing and Ransomware Attacks

The notion that ransomware attacks may be on the decline after a relatively quieter period in late 2021 have quickly been dashed in early 2022. There have been twenty-seven publicly announced ransomware attacks in January alone, ranging from a county in New Mexico to a major media outlet in Portugal. The impact has been significant. Patient care was affected in a number of Maryland healthcare organizations after the Maryland Department of Health was hit with a ransomware attack. In Saskatoon, Canada, their airport was attacked, and some exfiltrated data was posted on the Dark Web after the city did not pay the ransom.

The invasion of Ukraine by Russia has significantly heightened the risk of US attacks by Russia and other state-sponsored cyber-criminals. The Cybersecurity and Infrastructure Security Agency (CISA) issued an advisory the week of February 21, 2022: "Russia's unprovoked attack on Ukraine, which has been accompanied by cyber-attacks on Ukrainian government and critical infrastructure organizations, may have consequences for our own nation's critical infrastructure."

Ransomware attack methodology can span a wide set of vectors. The most common attack methods all focus on phishing, meaning exploiting user behaviors. They tend to fall into three categories: a.) malicious email attachments, b.) malicious email links and c.) exploit kits.

With **malicious email attachments**, the cyber-criminal creates an email from a believable source, such as the Human Resources department, and attaches a malicious file, typically a PDF, a Word document, or an .xls file. The recipient opens the attachment, assuming the email has been sent from a trusted source. When the file is opened, the ransomware payload is unknowingly downloaded, the system is infected, and from there, the cyber-criminal can potentially access sensitive data across the entire corporate environment.

**Malicious email links** are URLs in the body of the email. Similar to the malicious email attachment approach, these emails are sent from someone you believe to be a trusted source. When clicked, these URLs download malicious files, the user's system is infected and again, the cyber-criminal can potentially access sensitive data across the entire corporate environment.

**Exploit kits** are sophisticated toolkits that exploit vulnerabilities. Generally, exploit kits are executed when an unsuspecting user visits a compromised website. Malicious code hidden on the site, often in a fake advertisement, redirects you to the exploit kit landing page, unaware by the user. If the user's system is vulnerable (not containing the latest OS patch for example), a drive-by download of a malicious payload will be executed, the system will become infected, and the cyber-criminal again has free rein into a corporate environment.

Despite all the tools and controls organizations put in place today, the ease and simplicity of these attacks means any organization continues to be vulnerable. Cyber-criminals do not discriminate based on industry, size, geography or any other factors.

Cyber-attacks target government, healthcare, manufacturing, financial services, and other organizations. As a result, cybersecurity managers struggle to prioritize actions in order to combat the shifting ransomware landscape. Even the most mature cyber-savvy organizations are anxious and wary. A recent Deloitte 2021 survey indicated that 90% of the respondents (CISOs and other cyber professionals) are worried about ransomware even with a mature program in place.

Despite the significant amount of articles, white papers, frameworks and industry committees on the topic of ransomware, there is not a one-size-fits-all strategy to defend against ransomware. Based on post mortems of ransomware attacks, there is no straightforward, singular root cause. Interviews with cybersecurity professionals echo the complexity of the problem citing over twenty methods to defend against ransomware.

With that as a backdrop, the best ransomware defense is making your organization as difficult a target as possible. Here are nine specific steps an organization can take to minimize the risk of a ransomware attack:

1. **A basic, but very important first step, is the creation (or immediate update) of an Incident Response (IR) Plan.** It is critical that the entire management team and IT department are aligned and ready in the event you have a suspected ransomware or other cyber-attack. Insurers will demand a plan, but it is also important to know, prior to an event, their role and responsibilities in guiding you through the process. Also, identify your go-to legal counsel (breach coach) and preferred Incident Response partner who will lead the forensic investigation. Simulated cyber-attacks (often call IR Tabletops) are an excellent exercise to determine 'attack readiness by all key constituents within the organization, including top management, legal, IT, PR and HR.

2. A **security awareness program** is essential for every organization. Not only does it educate your users to identify potential phishing attacks, nearly every insurance company that writes cybersecurity policies will mandate a security awareness program. The program should focus on identifying attacks such as phishing through creative and interactive methods. Companies such as Wizer Training have developed curriculum that engages users at all levels of the organization.

3. Conducting a **vulnerability assessment** of your systems and networks is an important benchmark to identify potential gaps in your IT environment. Poor patch and configuration management processes are the second most prevalent vector (behind phishing) for cybercriminals to gain entry. A formal quarterly assessment is recommended along with weekly vulnerability scanning. A mature assessment program will rank vulnerabilities and prioritize areas of remediation.

4. **Multi Factor authentication (MFA)** is absolutely essential for access to every application within your environment. It is now considered the first line of defense against brute force cyber-attacks of a user's login credentials. Insurance companies are now mandating MFA as well. There are multiple tools on the market such as Duo and Microsoft Authenticator. Although cybercriminals have been able to bypass MFA in certain situations, implementing MFA will make access to your internal applications and systems very difficult for cybercriminals.

**5.** Although antivirus protection for endpoints and servers has been around for many years, a new generation of protection called **Endpoint Protection and Response** (EDR or sometimes called XDR) is now essential to protect endpoints from sophisticated cyber-attacks. The EDR 'category' was initially named by Gartner Group and is defined as a solution that "records and stores endpoint-system-level behaviors, uses various data analytics techniques to detect suspicious system behavior, provides contextual information, blocks malicious activity, and provides remediation suggestions to restore affected systems."

**6. A corollary to EDR is a proactive approach to identifying potential hidden threats in your organization through Threat Hunting**. The core notion is an assumption you've been breached and, through an ongoing set of sophisticated investigations, potential cybercriminals can be identified. Typically they are found through specific behaviors related to IPs, hashes and failed login efforts, all known as indicators of compromise (IoC).

**7. Identify all third-party systems used by every department.** Potentially one of the most difficult tasks, particularly for larger organizations, is an inventory of every relationship with partners where there is bilateral access to any part of your (and their) IT infrastructure and applications. Some of the most egregious cyber-attacks started with access via a third party vendor. This process often begins with individual departments providing basic information of the third-party relationship e.g. the outsourced maintenance department that tests your physical security system or the travel agency's portal used to upload executive's passport information.

**8. Network Access Control (NAC) is an important process to enforce policies and limit network access to approved users and applications. The three capabilities of NAC are authentication, network segmentation and integration with other security tools that will enforce policies.** But NAC is only as good as having visibility to all devices through **Asset Discovery**. Make sure your Asset Discovery solution monitors all aspects of your environment including cloud applications and those serving remote workers.

**9.** Today's network environment serving cloud applications, remote workers and global operations has dramatically impacted how to design and manage a secure network infrastructure. The notion of a simple 'edge' firewall platform is changing due to the challenges in terms of service availability, user performance, and productivity. These challenges are now addressed through a **Secure Access Service Edge (SASE)** framework. In addition to the network performance advantages, SASE delivers, specifically for security, unified threat and data protection capabilities thus minimizing cyber-attack vectors.

Ultimately, the goal is to be in a state of 'ransomware readiness.' This includes the aforementioned actions to better protect your overall corporate IT environment and make users continually aware of the types of threats they may be exposed to. There are plenty of tools available to combat cyber-attacks, but the best defense is the underlying processes and people to properly leverage those tools.