**The Risks of Email Phishing Attacks in 2022**

Email-based attacks have been a primary form of compromise for enterprises since email became widely used. While it initially started as just a way to deliver malware to sabotage or deface corporate assets, attackers quickly realized that there is more to gain. So, email-based attacks morphed into phishing attacks. Phishing is best defined as attempting to gain access to information or credentials from end users by posing as a potentially legitimate source of email or call. When it comes to email phishing, this is often accomplished by mimicking, spoofing, or domain squatting to make an email origination address appear to be from a legitimate source, like Microsoft or AWS. From there, the hope is that the user will click on a link provided in the email and either provide credentials or download the attached malware. Now that the attacker has a small foothold in the network, they will continue to escalate, pivot, or move through the network to attain the information they need or to deploy something much more nefarious, like ransomware.

So, this is something that has been around for a while, so the assumption is that it is becoming less of a threat. Well, that is not the case. Like anything else in cybersecurity, this is a cat and mouse game where the defenders are almost always reacting to the attackers. As cybersecurity teams, tools, and research groups identify patterns to help defend an organization, the attackers will pivot to evade that defense. Many tools, including G-suite and O365, offer up resources to help mitigate the risk of a phishing attack but the only real way is to make sure that end users are fully educated and paying close attention to every email coming in. These tools are great at catching low-tech, mass phishing campaigns through machine learning and herd knowledge, but they are not bulletproof. Attackers have become very sophisticated and have technics that can evade initial detection from these tools leaving employees on the front line to help defend the enterprise.

There has been a bit of a resurgence in phishing attacks in the last few years. As organizations have been able to improve security posture and prevention capabilities, it has become harder for attackers to gain access. Because of this, the attackers have pivoted back to utilizing phishing as the primary mode of entry into organizations. According to the Ponemon 2021 Phishing Study, the average cost of phishing has increased nearly 5x since 2015 for organizations. Further, loss of productivity has doubled in that same time for employees. Productivity loss could be a result of credentials being locked, systems needing to be reimaged, or users not being able to work during the investigation. With the largest cost associated with the work to reimage and redeploy assets to affected users, this is increasing in cost as employees move to a more remote posture.

This is a large problem that is not going away. How can individuals and companies protect themselves from phishing attacks? Well, there is no easy solution. It is a multi-prong approach. Enterprises need to implement tools to help detect and remove phishing attacks that are easily identified from inboxes as the starting point. The next prong is to implement a robust training and education program to educate employees on how to identify and report phishing attacks. This should not only involve training presentations but also hands-on training through simulation. It is extremely critical that organizations explain that the simulated phishing training is not meant to catch an individual but to help an individual understand how to identify phishing and to continue to hone their security skills. Lastly, an organization should look to implement additional monitoring and response tools and protocols that involve monitoring user activity and end-point security tools.

As organizations continue to improve tools, prevention, and detection capabilities, we will continue to see attackers evolve. We can expect to continue to see low-tech, shotgun approach phishing campaigns from organizations hoping to slip through detection and catch just one individual. However, it is more likely that attackers are going to pivot to meet the new wave of working and technology. This evolution is happening now. More and more phishing attacks are coming in via SMS text (Smishing), in attempts to bypass corporate controls. Further, we will see higher utilization of open-source intelligence to mimic trusted vendors or to even compromise that vendor to allow for attacks to be launched against their clients. No matter the current trend of attacks, it can be assumed that phishing will remain one of the largest initial compromise vectors for attackers

**The State of Ransomware Attacks in 2022**

Ransomware is still a relatively new form of attack that enterprises and government entities are currently faced with. In short, it is the act of loading malware that will, in some way, restrict access to data or systems until the organization is willing to pay a ransom to the attacking group. The attacking group may or may not release the data, computer systems, or assets from the malware. In the early stages, it was extremely likely that the ransomware will be reversed, however with groups that are mimicking the well-known gangs, it has become less common. There has been a new wave of ransomware-based attacks. One is destructionware, where the malware imitates ransomware but in reality, the attackers will never reverse the encryption or damage done as their goal was to destroy the data and cause as much damage as possible. The second is the evolution of ransomware that involves not only encrypting data or locking up systems but also exfiltrating data from the organization. Once the data is removed from the organization, the attackers will not only demand a ransom to reverse their encryption but also to prevent the release of the data.

Since its introduction, ransomware has not slowed down. The reality is, that these attacks are extremely successful because it just takes one employee to slip up and download the malware, the impact is quite large, and these attacks have been successful so more attackers are utilizing them. It has become one of the biggest and most expensive types of data breaches or security events. This has become such a large issue that many cybersecurity insurance policies have separate underwriting writers to address the potential cost and impact of ransomware attacks on an organization. While the likelihood of an organization paying the ransom has gone down, this has not decreased the number of attackers utilizing ransomware as a mode of attack. With ransoms of multiple million being paid, it is a highly lucrative attack strategy and as more large-scale attacks are successful, it will only embolden attackers.

Ransomware attacks are extremely destructive for organizations. The ransom is often the lowest cost of the event. A ransom event will often entail a months-long recovery effort that may see hundreds of thousands of hours of lost productivity for employees, lost production or operation, and lost revenue from systems being down. This just covers the impact directly on the business, there are additional costs that will add up quickly related to fines and consumer class action lawsuits. Further, the impact on reputation and future revenue is not easily able to be calculated for many organizations. In fact, with all of these things considered, ransom attacks can be considered an organization killer type of event without insurance.

An attack is extremely destructive, so what can organizations do? Taking a risk-based approach is the best way to plan and address potential ransom attacks. Some key areas to focus on are related to access. Keeping domain admin accounts to a minimum and deploying a privileged access management system is a great way to help prevent the spread as most ransomware will attempt to elevate to admin credentials. Another great step is to implement robust segmentation within the network as this will help to limit the scope of an attack and not fully impact the business. Other controls to implement are endpoint detection and response tools, robust logging that involves behavior analytics, and strong email-based controls to help prevent phishing attacks. While all of these can help prevent or limit the impact of a ransom attack, none of them will fully immunize an organization from ransomware.

As better controls are implemented, attackers will continue to evolve to evade these controls. This is something that is actively happening every month. We have seen attackers move to nullify the security measures implemented to protect backups by exfiltrating data from the network before encrypting. We then saw some attacks move to destroy the organization’s data after exfiltrating to increase the likelihood of paying. We will likely see attacks continue to focus on exfiltrating data or proof of attack to extort payment to save a company’s reputation. Further, cloud-based backups will likely be a primary focus going forward with vendors being included in the attack. One thing that is almost guaranteed is that attackers will continue to focus on getting data and implementing attack techniques that will increase the likelihood of payment.