Help protect your business against ongoing email threats

ADT Cybersecurity

Overview

From 1988, when CompuServe was the first major commercial online email service provider in the United States[1], to the digital economy of 2019, email has become the go-to form of business communication. Given the universal nature of email, and the simple fact that its form, content and trafficking is almost entirely shaped by the "Human Element," there are no signs that email won't continue to be the best, most efficient method to compromise a network with both known and new varieties of malware.

Email usage continues to increase

Regardless of the proliferation of text and social media, email communication is still growing strong. The total volume of worldwide emails sent and received reached 205 billion per day, with this volume projected to increase by at least 5% every year.[2]

This fact isn't lost upon hackers, who are constantly seeking opportunities to exploit organizations, and are now focusing on smaller organizations due to the perception that they don't have the proper resources. In fact, 43% of all cyberattacks will be launched at smaller businesses in 2019.[3]

205B

total volume of worldwide emails sent and received reached per day

43%

of all cyberattacks will be launched at smaller businesses in 2019.[3]

[1] Peter H. Lewis (29 November 1994). ("The CompuServe Edge: Delicate Data Balance". The New York Times).
[2] Radicati Group,
[3] Ponemon Research Institute, The State of SMB Cybersecurity, 2018.

Email threats organizations face today

Emails offer hackers a vehicle to deliver a variety of vulnerabilities to an organization. Some of the more common email-borne threats include:

Malware: The most efficient way to introduce malware into a network is through email—either through an attached malicious file, or a link to a compromised or "spoofed" website. With a single click, the attachment or "bad URL" deploys an executable file, a download or other mechanism, which sets the intruder on its mission—to compromise the network in some way, disabling defenses and either overtly (Ransomware) or to covertly steal data and credentials, enslave endpoints into a botnet (Trojans, Spyware, Botnet) or any number of other harmful activities.

Ransomware: The most dramatic and high-profile strain of malware. The email attachment is opened, and the file injects code that typically encrypts or removes user access to critical files and operational systems. The criminals then extort a fee, payable in an untraceable Bitcoin (or other) digital currency transaction, which may, or in many cases, may not allow them to regain access.

Phishing: Widely disseminated email "spam" is used to garner gullible readers to open messages and click on links. When the victims visit these sites, they're enticed to enter PII (Personably Identifiable Information), which then leads to identity theft, stolen credentials, financial loss and compromised systems.

A classic attack scenario

- Threat actor researches company controller. They locate their email address, full name and the CEO's name.

- Threat actor will spoof the CEO's email address.

- Threat actor will send a semi-casual or informal email, without any links or attachments, opening a dialogue.

- The victim responds directly to the email.

- Threat actor creates urgency, says they're busy or in a meeting, and asks for immediate wiring of money... Sometimes in the form of gift cards.

- Victim noting this as not entirely abnormal doesn't double and triple check the ask and wires the threat actor money.

Other scenarios

- An employee with administrative rights to key systems receives an urgent email from IT to update their network password. They disclose their password to cybercriminals.

- An employee receives an email to read an important attachment about their benefits provider. When they open the attachment, they unknowingly activate hidden Trojan malware.

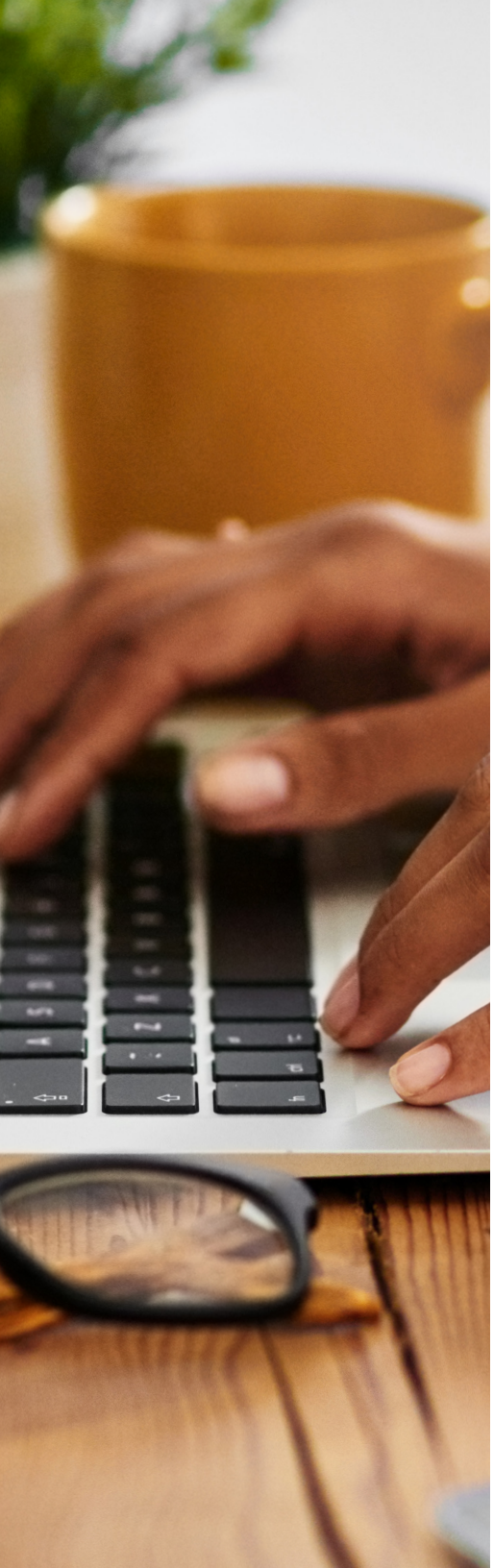
Spear Phishing / Whaling: in this variant of phishing, key IT/networking individuals or company execs are targeted using malware-laced emails appearing to come from a trusted source, in efforts to gain access to internal systems and data.

Business Email Compromise / CEO Fraud / Impostor email: Over the past two years, Business Email Compromise (BEC) schemes have caused at least $3.1 billion in total losses to approximately 22,000 enterprises around the world, according to the latest figures from the FBI.[4] Business Email Compromise is a term that refers to attempts to compromise systems of companies that engage in high-volume wire transfers of funds internationally.

Spam: High-volume unsolicited messaging or "Junk email" has been around almost as long as email itself. While spam isn't as top of mind as much due to the various filtering software available, these solutions must keep pace with the evolving spammer technology. Maintaining spam filters, managing junk email rules, "hold for verdict" junk mailboxes all put a drain on network capacity and employee productivity.

Outbound Email Hijacking: Corporations are also subject to corporate policies and government regulations, which hold businesses accountable for their outgoing emails and ensure they protect their customer's PII. Zombie attacks and IP hijacking can disseminate customer PII, ruining the reputation of a business.

[4] (www.ic3.gov/media/2016/160614.aspx)



A multi-pronged defense-in-depth

Training and testing

Organizations of all sizes have adopted training that instructs employees on how to recognize the dangers that may be lurking in their daily in-box. This is a necessary first step in any defense, especially considering the fact that one out of every five employees opened a phishing email in 2018.[5] And to reinforce these lessons, many organizations regularly test employee retention and resilience through phishing their own employees. Some cybersecurity professionals believe that by staging mock phishing drills on a constant basis, companies can maintain a high degree of discipline among their team members and prevent phishing attacks.But, there's a downside to this approach:

Reduced productivity

Some employees, such as salespeople and customer service personnel, must open emails and attachments from strangers as part of their daily routine. Any time spent by employees deciding whether a message is dangerous or not affects customer experience and productivity.

Less legitimate communication

Excessive security training could spur a chilling effect on doing business if employees err on the safe side and delete legitimate unopened email. This can lead to missed opportunities, errors of omissions, reduced productivity and non-action to time-sensitive issues.

Employee alienation

Employees who fail the mock-phishing test are often reprimanded and given compulsory re-training. A punitive stance might be deemed appropriate given the high stakes involved - but often this will only reduce the reporting of real phishing emails.

Reduced trust

Mock-phishing undermines the foundation of trust that your company and its employees share with one another. Constantly probing for employee weaknesses and pretending to be fellow employees or vendors could alienate employees to some degree.

Email threat awareness training and recognition of potential threats in email communications is the first necessary step. But given the negative factors associated with aggressive phishing simulation as a compliance method, companies need to realize that other tactics should be employed, especially when these techniques will never be 100% effective.

[5] Widup, Suzanne & Spitler, Marc & Hylender, David & Bassett, Gabriel. (2018). 2018 Verizon Data Breach Investigations Report.

Sandboxing

is rapidly being recognized as a required element in the defense against email-borne threats. The inherent danger posed comes in two forms — attachments and links embedded in the message text. Most email filtering systems will spot and strip out executable files that are recognized as malware by global threat networks. These "known" threats don't include very recent releases of new malware, or "Zero Day" threats, i.e. threats that are less than 24 hours old. Before defenses have a chance to identify and block these new releases, they can slip through a great many standard email filtering systems.

Sandboxing is a technique that specifically addresses this scenario by routing all email with suspicious attachments to the cloud to be opened in a virtual environment. Not all sandboxing services are the same, however. Some minimize delivery delays through the use of AI to be more selective and can identify malicious files masquerading as benign to further limit risk. These services also recognize "bad" URLs identified as spreading malware within 20 minutes of their appearance.

Conclusion

Email communications have been essential to organizations for over three decades and will continue to be for the foreseeable future. Cybercriminals realize this and are constantly changing up the nature and form of their attacks to find, entice and exploit "the weaker links in the network user chain." The innovative and sophisticated approach adopted by today's cybercriminals demands a suitable response — an effective, up-to-date security solution that includes dedicated, leading-edge email protection consisting of recognition of the threat, training to recognize potential phishing messages, and AI (Artificial Intelligence) to recognize Zero-Day threats.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. ADT Cybersecurity products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective in ensuring network security and regulatory compliance. ADT Cybersecurity does not warrant that its products and services are immune from the malicious or illegal conduct of any party. ADT Cybersecurity products and services are designed to protect your information from the average computer user