Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Bringing it all together

Zero trust isn’t a collection of technologies. Zero trust is a mindset. It swings security’s attention away from building high walls and refocuses it on an organisation’s users, their devices, and the data, resources and applications they access. This means that enterprises can approach zero trust in a variety of ways.

One way that enterprises are looking at is the software defined perimeter (SDP). It can provide a central authority for policy enforcement and the authentication of users, devices and applications. Moreover, it can segment a network on a granular level basing restriction or permission on an application-by-application, user-by-user, or device-by-device basis.

Before an entity wants to connect to the network it must first be authorised. No part of the infrastructure is revealed until the user has been properly authenticated. By making resources ‘dark’, SDP denies attackers the intelligence they could normally rely on – such as seeing their target’s DNS, internal IP address or port information – and stops the lateral movement that attackers need to get closer to critical systems and data.

Such an asset only adds to an already impressive array of security enhancements. Zero trust promises much. It’s secure access at its best: providing the access that an enterprise and its staff and users want, with the security that they need. Many are rightly anticipating the architectures that can bring that data protection, trust and continuous authentication. Most of the respondents to the 2019 survey will be embarking upon their own path to zero trust within the next year or so. Nearly half (41%) are considering SDP as a way to do that. With the right secure access choices, they’ll get there.

About the author

A veteran of numerous Silicon Valley firms, Bryan Embrey brings more than 20 years networking and security industry experience to Pulse Secure (www.pulsesecure.net). He has been a product manager, analyst and technical writer, having worked on leading-edge technologies from Nokia, Nortel, Blue Coat and Fortinet.

Reference

1. ‘State of Enterprise Secure Access’. Pulse Secure. Accessed Aug 2020. www.pulsesecure.net/resource/state-of-enterprise-secure-access/.

Why is phishing still successful?

Dr Akashdeep Bhardwaj, Varun Sapra, Aman Kumar, Naman Kumar and Arthi S, University of Petroleum & Energy Studies, Dehradun, India

In recent times, there has been a dramatic shift from bulk spam emails to targeted email phishing campaigns. Such attacks have started to cause huge brand, financial and operational damage to organisations globally. Phishing attacks involve simple, straightforward, masquerading methodology. The aim is to lure and trick an unsuspecting victim in order to elicit as much information as possible, using SMS, email, WhatsApp and other messaging services, or phone calls that have been spoofed to appear as if they are from known, reliable friends or colleagues.

The intent is to get the victims to click and log into cloned web portals such as company intranet or bank sites and social networking sites such as Facebook, Instagram, Twitter or even Yahoo and Gmail sites. Once the unsuspecting victims click on the URL sent by the attacker, instead of the original site they are directed to the attacker’s fake site. On trying to log in or submitting information on that website, victims provide the attacker with sensitive information. This can include user ID, email, password, address, mobile number, date of birth and payment card details, among other things.

Cyber attackers have enhanced their methodologies to include personalised attacks. Targeting senior-level, high-value personnel such as the head of HR, C-level executives such as CISO, CTO,
CFO or board members is an advanced form of phishing attack against individuals, known as whaling.7 Spear-phishing attacks, on the other hand, target specific individuals within the organisation, and are highly personalised.6 Such individuals include finance team members, IT security team members or even new hires. Apart from using cloned web portals, attackers also target two-factor authentication by cloning one-time passwords (OTPs) as well as creating fake QR codes which, if scanned by mobile phones, respond by offering huge discounts at restaurants, grocery stores or household service stores in return for online payment, which obviously goes to the attacker’s account.

“Although many organisations provide cyber awareness training for their staff, attackers are able to bypass human defences in various ways. This has to do with employee workloads and expectations, which have become complex and ever greater”

Such new age phishing attacks are effective and difficult to detect, as the malicious email or message is convincing and impersonates a trusted source known to the target. Although many organisations provide cyber awareness training for their staff, attackers are able to bypass human defences in various ways. This has to do with employee workloads and expectations, which have become ever greater and more complex. Due to this, employees – even experienced staff – make mistakes and can be deceived. No amount of training will be able to change this. Traditional email security systems are unable to detect spam and stop only the most basic level of phishing attacks. For cyber criminals, whaling and spear-phishing are the perfect means for performing a broad array of damaging attacks.

Alarming trends

As per the latest phishing statistics from Security Boulevard, by mid-2020 the trends have become alarming as phishing attacks have become highly creative, exploiting the Covid-19 global pandemic.7 The phishing stats indicate that targeted victims are phished on a regular basis. A few disturbing highlights of the report are:

• Verizon’s ‘Data Beach Investigations Report’ claimed that attacks involving only phishing showed an increase of 32%, and this covered nearly a third of all data breaches.8
• Some 86% of email attacks involved ‘malwareless’ emails; in place of malware, they increasingly used new sophisticated attacks such as spear-phishing, whaling, CEO fraud or impersonation tactics.9
• Over 88% of organisations across verticals reported facing spear-phishing attacks in 2019, which resulted in 46% receiving ransomware demands and 25% of small and medium-size businesses (SMBs) suffering phishing attacks.
• Around 60% of enterprises reported mobile phishing attacks via SMS and WhatsApp (Smishing) as well as voice phone calls (Vishing) using messaging, social media and even gaming apps.
• Every 20 seconds a new phishing portal is registered and launched, which now also includes Covid-19 related phishing attacks. Between January and March 2020, 51,000 coronavirus-themed domains were registered globally.
• Nearly three-quarters (74%) of phishing attacks involved the HTTPS protocol, using SSL/TLS certificates, as compared to 51% in 2019. Of these, webmail or software-as-a-service were involved in 31% of phishing attacks.
• In April 2020, cyber criminals sent 18 million phishing mails related to Covid-19. Google reported blocking over 250 million Covid-19 spam and phishing emails.
• Nearly 60% of the data breaches are due mainly to human error. These include trained and untrained insiders who fell prey to phishing attacks. This resulted in $3.5m in losses in 2019 alone.
• Overall phishing is down by 42% compared to 2019, yet the success rate of whaling and spear-phishing is higher than ever before, suggesting that attackers are going for quality over quantity.
• An alarming 40% of employees with little or no phishing awareness training regularly failed during simulated phishing campaign and assessment tests.
• Most (90%) phishing emails were actually caught and verified by email security gateways, yet the 10% that remained accounted for over 170,000 incidents inside organisations’ premises. This caused losses of over $26bn in the period July 2016 to July 2019 in the US alone.
• Apple is the most imitated commercial organisation for cloned and phishing websites, while Facebook is the number one emulated portal among social networking sites.
• Microsoft Office and Adobe Acrobat files represented 94% of malware attachments in emails; this is up from just 15% in 2018 or 25% in 2019.
• Venezuela had the dubious honour of having 31.6% of phishing victims in 2019, followed by Brazil at 30.5%, Greece at 25% and Australia at 20%.
• The biggest source of spammers came from China (over 22%), followed by the US at 15% and Russia at 6%.
• In Brazil, phishing attacks increased by 232% in just 10 months in 2019. Although the overall number of phishing attacks is on the decline, it is important to look beyond the phishing statistics. Cyber attackers are not giving up. In fact attackers keep coming up with new attack tactics, focusing on effectiveness, higher success percentage and attack qual-
ity, instead of blasting out bulk phishing messages with the hope that one in 1,000 might work. This is the core difference in targeting victims with a laser-guided rifle instead of a machine gun.

**Phishing taxonomy**

The authors classified phishing attacks based on new and upcoming tactics adopted by cyber attackers while luring victims and performing fraudulent activities to obtain personal and sensitive information. Tactical and social engineering techniques are detailed in Figure 1.

Cyber criminals perform phishing activities for money, and to ensure that their scheme is effective and evades detection, they do not make rational or ethical decisions. To combat phishing, this research presents the phisher’s mindset and methodology of attack. The authors designed and developed a phishing toolkit using Kali Linux and Python. As shown in Figure 2, the attacker’s toolkit has options to choose from, including using cloned social media sites, gathering two-factor authentication OTP code or using a QR code in the form of pre-designed templates. To generate the cloned forged Twitter link, the authors set up a reverse tunnel using an Ngrok proxy on the attacker’s command and control (C&C) server. This proxy application launches multiple virtual tunnels as local network services. These capture the network traffic for detailed inspection. This helps gather the victim’s sensitive details, using one unique phishing method from three options to maximise success.

If the attacker starts with the social media sites option, this is followed with options to choose between cloned Instagram, Facebook, Snapchat or Twitter sites, as illustrated in Figure 3.

Assuming the attacker chooses the Twitter social media template (option 4), a reverse proxy server is started on the attacker’s system. This generates a forged Twitter link and presents the spoofed social media website to the victim. In our attack, the forged link is [https://e89c09404a68.ngrok.io](https://e89c09404a68.ngrok.io) as shown in Figure 4.

Trained and aware employees can detect this link as an incorrect URL or forged link. The motivation for this research is to increase phishing awareness and not actual phishing, so DNS spoofing is not applied here. That would easily provide a legitimate link or a similar one to those used by Twitter. The attacker disguises the Ngrok link as shown in Figure 5 and then sends it to the victim using social engineering attacks.

When the disguised link is clicked, the attacker’s command and control system starts to gather the victim’s details. These include hostname, location, IP address, ISP, country and currency, as shown in Figure 6.

The attacker’s C&C server waits for the victim to log in and enter the email address and credentials on the forged Twitter login page. These details are also captured by the attacker’s C&C server, as illustrated in Figure 7.

These credentials are saved in the /sites/Twitter/Saved.IP.txt file for advanced future attacks such as identity spoofing and lateral movement on the victim’s network and other systems. More victims can be trapped as and when they click the disguised link, as illustrated in Figure 8.

The attacker has options to use enhanced phishing methods, a two-factor authentication attack to grab the victim’s OTP or even lure the victim...
to send Paytm, Google or WhatsApp money by scanning a QR Code, as illustrated in Figure 9.

Features for phishing detection

Creating phishing awareness generally involves having end users attend a course, read documents related to ‘good practices’ and ‘Dos & Don’ts’. However, it is human nature to forget and focus on the micro task when going about daily chores. The authors reviewed over 300 phishing mails received by Gmail and Yahoo. The top 15 unique tactics and phishing features adopted by cyber attackers are presented in Table 1. The authors propose creating anti-phishing rules by IT security teams to check and validate these phishing features. These can easily help detect and block phishing attacks.

The Internet of Things

Bio-wearable, body sensors, Internet of Things (IoT) devices or smart systems in our homes, offices and buildings have changed our lives for the better. These devices have become an intrinsic part of our work and lives, found everywhere in our offices, houses, schools, vehicles, hospitals, manufacturing industries and even on our bodies.

However, each IoT device communicates and connects via the insecure Internet and this is a major concern when we consider the increasing development of smart cities, integrated with multiple automation systems, IoT devices and ‘things’ inside homes. Such ‘things’ include televisions, webcams, music systems, washing machines and air conditioners, among other devices, and all this adds up to an insecure environment. Every connected device increases the threat surface and probability of an attack on our privacy.

“These ‘things on the Internet’ are actually inside our houses, controlled and connected remotely by the user’s smartphone or user systems. Malware deployed via phishing is capable of controlling these devices, which may well cause more harm than benefit”

This gets amplified more as these ‘things on the Internet’ are actually inside our houses, controlled and connected remotely by the user’s smartphone or user systems. Malware deployed via phishing is capable of controlling these devices, which may well cause more harm than benefit. IoT devices and sensors usually collect data and are mostly connected to various networks and the Internet. This leads to an individual’s personally identifiable information (PII), location and voice being stored in these devices. This PII can range from personal details such as name, age, location, email password credentials or even health data. Thus for any cyber attacker, there are easy, low-hanging assets with value information, making any individual – not just high-value executives – potential targets.

Conclusion

Phishing attacks are the number one threat vector against untrained and unaware employees. Cyber attackers continue to evolve malicious attacks that are becoming difficult to differentiate from real emails and authentic communication. Cyber attackers carrying out phishing attacks, whaling or spear-phishing are difficult to track. Only by increasing employee awareness and proper training can we hope to add proactive mechanisms to detect and block phishing.

The innovative and increasing use of the Internet of Things (IoT), wearable devices and smart cities have also presented huge opportunities to cyber criminals. It has become imperative to balance the use of the insecure Internet in our daily lives with new age devices if we are to securely communicate with others and realise the benefits of these technologies without being exploited by phishing attacks.
About the authors

Dr Akashdeep Bhardwaj is a professor (cyber security & digital forensics) at the University of Petroleum & Energy Studies (UPES), Dehradun, India. He is an eminent IT industry expert with over 25 years of experience in cyber security, digital forensics and IT management operations. He mentors graduate, masters and doctoral students as well as leading several projects. He has a PhD in computer science, has published several research papers at conferences and in international journals, and co-authored books and a patent. He has worked as technology leader and head for various multinational organisations.

Varun Sapra is an assistant professor senior scale working at the University of Petroleum & Energy Studies. His area of specialisation is machine learning and web applications and he is currently pursuing his PhD in computer science. He has published several research papers at conferences and in international journals, and co-authored books and a patent.

Aman Kumar, Naman Kumar and Arthi S are third-year students pursuing their bachelors of technology in computer science, specialising in cyber security and digital forensics at the University of Petroleum & Energy Studies. They are budding cyber security enthusiasts and have won and participated in several cyber security hackathons and competitions.

References
1. ‘What is a phishing attack?’ Imperva, 15 Jan 2020. Accessed Aug 2020. www.imperva.com/learn/application-security/phishing-attack-scam/.
2. ‘What is phishing? Phishing attacks and prevention explored’. Forecepoint. Accessed Aug 2020. www.forcepoint.com/cyber-edu/phishing-attack.
3. Grimes, RA. (2020, April 9). ‘14 real world phishing examples & how to recognise them’. CSO, 9 Apr 2020. Accessed Aug 2020. www.csoonline.com/article/3235520/15-real-world-phishing-examples-and-how-to-recognise-them.html.
4. ‘Phishing’. KnowBe4. Accessed Aug 2020. www.knowbe4.com/phishing.
5. ‘What is a whaling attack?’. Kaspersky. Accessed Aug 2020. www.kaspersky.com/resource-centre/definitions/what-is-a-whaling-attack.
6. Swinhoe, D. ‘What is spear-phishing? Why targeted email attacks are so difficult to stop’. CSO 21 Jan 2019. Accessed Aug 2020. www.csoonline.com/article/3334617/what-is-spear-phishing-why-targeted-email-attacks-are-so-difficult-to-stop.html.
7. Crane, C; Anderson, B; Jennings, R; Vizard, M. ‘Phishing Statistics: The 29 latest phishing stats to know in 2020’. Security Boulevard, 22 Apr 2020. Accessed Aug 2020. https://securityboulevard.com/2020/04/phishing-statistics-the-29-latest-phishing-stats-to-know-in-2020/.
8. ‘2020 Data Breach Investigations Report’. Verizon, 26 Feb 2020. Accessed Aug 2020. https://enterprise.verizon.com/resources/reports/dbir/.
9. ‘The 3Ts of Email Attacks: Tactics, Techniques, Targets’. FireEye. Accessed Aug 2020. https://content.fiereye.com/one-email/ig-the-3-ts-of-email-attacks.