UNDERSTANDING A GROWING THREAT: CREDENTIAL PHISHING

WHITE PAPER

INTRODUCTION

Credential phishing, uniquely targeting individuals with access to valuable data and systems

Credential phishing is a rapidly growing form of cyberattack. While the most notorious credential phishing campaign was the attack on John Podesta, the chairman of the Hillary Clinton presidential campaign during the 2016 election, enterprises are increasingly finding themselves the target of malicious actors who seek to gain access into business systems and steal critical information.

But what is credential phishing? What are the risks to my organization? What can I do to stop them?

Enterprise security professionals need to better understand these increasingly common and destructive forms of cyberattacks and how they can infiltrate and impact their organization.

This white paper will explore:

- What is credential phishing
- Why credential phishing is so effective
- The anatomy of a real credential phishing attack
- How isolation can stop these types of attacks
- The Menlo Security Isolation Platform

Attack Profile Card

Menlo Security

ATTACK NAME

Credential Phishing

TARGETS

Public agencies, political organizations and enterprises (essentially anyone with valuable information)

ATTACKERS

- Nation-state sponsored groups
- Advanced Persistent Threats (APTs)
- Cyber criminals
- Hacktivists

METHODS

- Mimic an authentic-looking login website
- Hijack an existing login page

BOTTOM LINE

Credential phishing attacks are often the beginning of a much larger and more destructive attack. Phishing emails are simply the way a threat actor gains access to the network before stealing information, making a ransom demand or simply creating havoc.

What is Credential Phishing?

Credential phishing is an attempt by malicious individuals to steal user credentials and personally identifiable information (PII) by tricking users into voluntarily giving up their login information through a phony or compromised login page.

In many cases, phishing websites have been found and taken down. Many others, though, continue to steal user credentials and information, hiding in plain sight—acting with impunity and without detection—continuing to pose a threat to organizations and individuals around the world.

The common form of a credential phishing attack is where attackers create a very authentic-looking login website, mimicking an established website from a well-known or used brand.

Why is Credential Theft so Effective?

Both tactics are extremely effective, because they play on the weakest link in any organization's security posture: the user. Human nature is trusting. It's curious. It's willing to follow directions from a seemingly authoritative figure.

- When an email from Bank of America tells you to click on a link to check the accuracy of your account balance, you do it.
- When your CEO sends you a glowing email about the great work you're doing and asks you to click on a link to choose a bonus gift, you do it.
- When Google tells you that your gmail account has been compromised and you need to immediately click on a link to change your password, you do it.

Attackers know very well how to manipulate human nature and emotions to steal or infiltrate what they want. They use email messages that induce fear, a sense of urgency, curiosity, reward and validation, an emotionally charged response by their victims or simply something that is entertaining and a distraction to convince, cajole or concern even seasoned users into opening a phishing email. In fact, 12 percent of users will open a phishing email while 4 percent will always click a link in a phishing email.[1] Enterprise users are little more discerning, but not by much. According to threat intelligence from Menlo Labs, 1.3 percent of the URLs in received emails were clicked across our customer base over the past 30 days.

1. 2018 Data Breach Investigations Report (11th Edition), Verizon

Lax enforcement of security policies is another reason credential phishing attempts are so successful. For instance, many organizations may try to enforce a mandatory policy for all users to employ and enable multi-factor authentication (MFA) for account login and access. However, enforcement and adoption of MFA mandates can take time, and they can be circumvented by users who are reluctant to change their existing workflow.

For instance, in a presentation in early 2018, Google pointed out that more than 90 percent of Gmail users do not use the free two-factor authentication (2FA) that is offered to them by Google.[2] In addition, a survey compiled by Duo Security (now part of Cisco) showed that only 28 percent of users have deployed two-factor authentication and nearly one-third of these users are using 2FA because they have been mandated to use it by their employer.[3] The same can be said for adoption of security technologies. Users will resist and, in many cases, simply ignore security mandates if they interfere with their existing user experience or if they feel that the new mandate will inhibit their productivity.

➔ **That is a problem.**

Who Does Credential Phishing Impact?

Nation-state sponsored groups and Advanced Persistent Threats (APTs), such as Fancy Bear (APT28), Cozy Bear (APT29), Comment Panda (APT1), Deep Panda (APT19), Ricochet Chollima (APT37), Helix Kitten (APT 34)—among others, have employed credential phishing to launch attacks against high-profile targets, including political campaign websites, think tanks, political national committees and more. However, phishing and spear-phishing attacks are also on the rise in nearly every enterprise segment.

According to the latest Verizon Data Breach Digest, 72 percent of enterprise data breaches originate from phishing attacks.[4] The report describes in great detail how a financial services industry (FSI) organization had someone gain access to wire transfer credentials. A manufacturer discovered that a competitor gained access to their network to steal product designs and other intellectual property. A public utility was under attack from amateur hacktivists who tried to create havoc on their industrial systems. And a movie studio had to deal with a ransom demand to prevent the early release of some creative content. While anecdotal rather than statistical, the report confirms that credential phishing is increasingly being used as the avenue threat actors prefer to gain access to corporate networks.

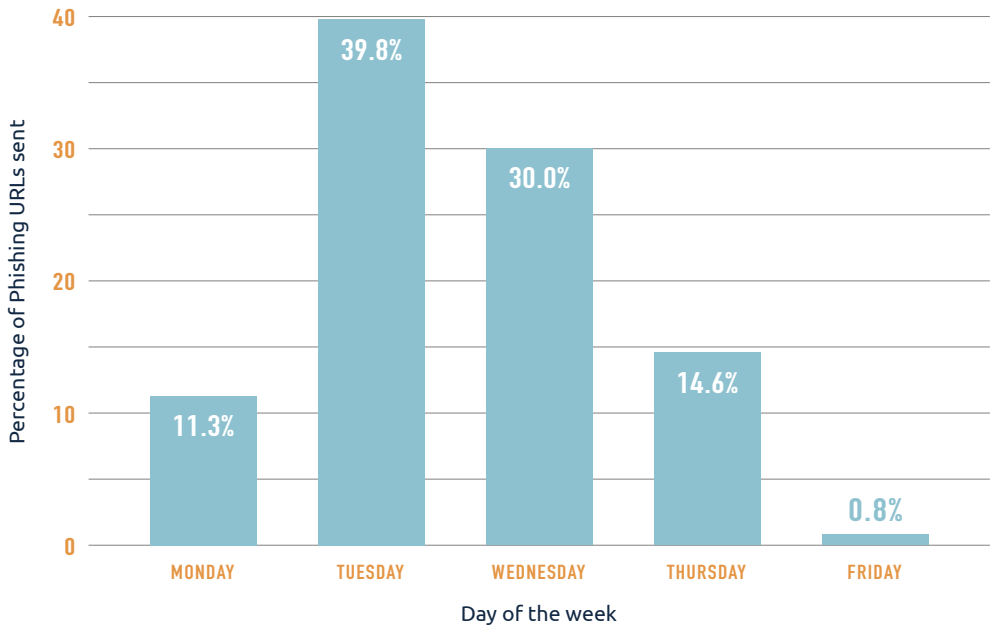
2. "Who's using 2FA? Sweet FA. Less than 10% of Gmail users enable two-factor authentication," Iain Thomson, January 17, 2018, https://www.theregister.co.uk/2018/01/17/no_one_uses_two_factor_authentication/
3. "State of the Auth: Experiences and Perceptions of Multi-Factor Authentication," Olabode Anise and Kyle Lady, November 7, 2017, https://duo.com/blog/state-of-the-auth-experiences-and-perceptions-of-multi-factor-authentication
4. Verizon. Data Breach Digest. 2016.

Menlo Labs Insight

Menlo Labs provides more insight into how threat actors target enterprises. From August 14–September 1:

- The most popular phishing themes across our entire customer base included OneDrive, LinkedIn, and Office365 logins—all work productivity tools that people would likely click from a work computer.
- Tuesday was the most popular day for attackers to send emails while Friday was the least popular.
- Interestingly, the largest campaign that we observed this month was 31 phishing URLs sent to 31 unique users at the same enterprise—a rare spray and pray approach when most attacks are targeted to one or two people who are known to have access to specific information or enterprise systems.

PERCENTAGE OF PHISHING URLS SENT vs. DAY OF THE WEEK



Most fascinating, perhaps, is that in every industry, the attack setup, deployment and results are exactly the same: A user's secure credentials and possibly other PII is stolen, and an attacker is able to access that user's email account, banking and financial accounts, healthcare information, and more.

What Does a Credential Phishing Attack Look Like?

Recently an executive at a technology company received eight credential phishing attempts over the course of a week. The emails changed slightly—different subject lines, variations of logos—and the attacker tweaked the emotional tug that they hoped would entice a click.

SUBJECT	THEME	TYPE OF LINK
Email Verification (see Fig. 1)	Fear of loss of productivity	Typosquatting (msonlineservce.com)
Payment Ref: #78291145 (see Fig. 1)	Urgent action required	Typosquatting (msonlineservce.com)
(4) messages rejected August 14, 2018, 08:59 AM		
ACH Payment August 15, 2018, 07:29 AM		
Attn: Accounts Payable (see Fig.1)	Urgent action required	Typosquatting (msonlineservce.com)
Payment August 16, 2018, 12:33 AM		
ATK-Payment Receipt August 17, 2018, 09:13 AM		
Syncing failed - action required		

As you can see, the attacker used a variety of different themes to get the user to click on a malicious link—from an expiring password and a fear of being locked out of Office 365 to an urgent action item to open and view an accounts payable receipt. Each action item led to phishing websites with phony login webforms. This attack used typosquatting, with both the email domains surreptitiously eliminating the 'i' in service to make it seem that the email was valid and the victim would be clicking on a legitimate, well-known website.

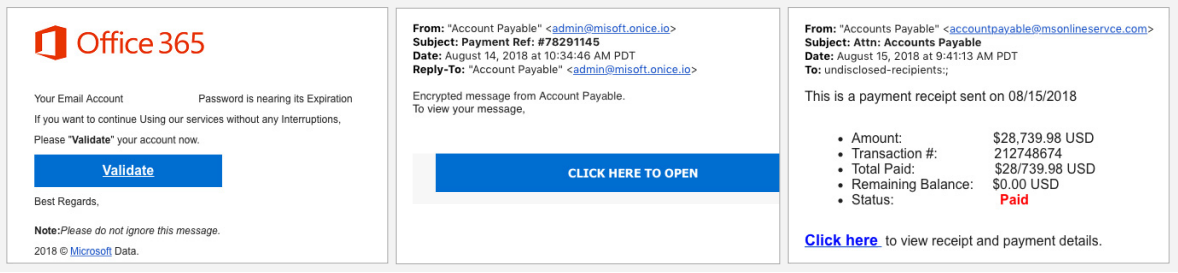


FIGURE 1: Credential phishing emails masquerading as (left to right) an Office 365 password expiration notice, an accounts payable notice, and an accounts payable receipt.

The URLs and tactics, techniques, and procedures (TTPs) employed by the attackers in this case were not extraordinary. Even so, VirusTotal—a popular free service that analyzes files and URLs for viruses, worms, trojans, and other types of malicious content—had either very low or no detection for the URLs used in these attacks. And that's the rub. Credential phishing attacks are not intended for mass delivery. Instead, they are typically targeted to a specific individual who the attackers know has the required credentials to access the information they want. These attacks do not use a cookie-cutter approach since the TTPs are often tailor-made to target a specific organization, group, or individual. Therefore, generic threat intelligence solutions have a low detection rate for credential phishing as the surgical specificity of credential phishing attacks means that there is little or no reputational information available to reference.

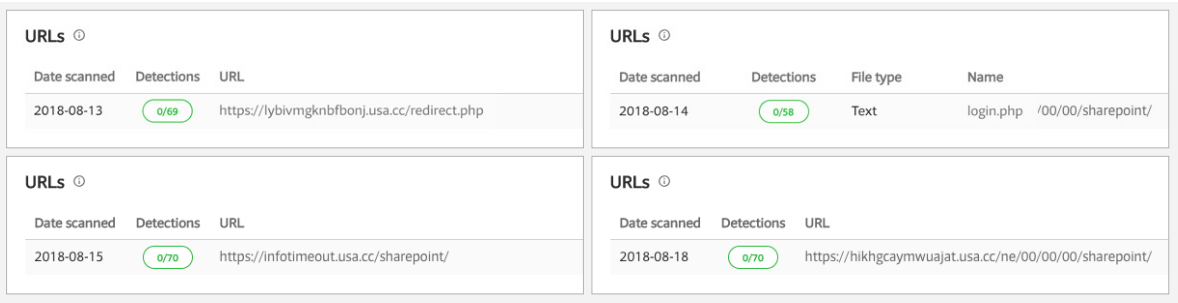


FIGURE 2: Screenshots of VirusTotal scans showing "0" detections for exploited URLs.

The difficulty of detecting credential phishing attacks shows that while the TTPs of a credential phishing attack may be simple, the technology needed to detect and protect enterprises and their users from these attacks—and to provide visibility into such attacks—must be intelligent, impenetrable, and advanced.

What Security Technologies Can Stop Credential Phishing?

Web isolation prevents all credential phishing attacks. While traditional security solutions rely on detection—and then blocking access to the malicious link—web isolation physically prevents users from entering their credentials into a bogus web form. It does this by rendering sign-in pages in read-only mode. This is the only way to 100 percent prevent users from entering their credentials into a fake form. The isolation solution should also include the ability to set policies that determine if or when web input field restrictions may be relaxed.

How Does Menlo Security Protect Enterprises from Credential Phishing?

The Menlo Security Isolation Platform (MSIP) eliminates credential theft and drive-by exploits caused by email attacks. By integrating the cloud-based MSIP with existing mail server infrastructure—such as Microsoft Exchange and Office 365, Google Gmail, or other webmail—all email links are transformed to pass through the Menlo Security Isolation Platform, without the need for any appliances or endpoint client, agent, or plug-in. When users click an email link, they are completely isolated from all malware threats, including keyloggers. At the same time, Menlo Security renders sign in pages in read only mode, preventing users from entering sensitive information into malicious webforms by policy.

Most importantly, there is no change in the user experience or workflow, and everything is transparent and seamless to the user. In fact, most will not even know that their web content is being isolated in the cloud on their behalf.

Menlo also allows administrators to define workflow policies for groups or individual users. While users are safely isolated, their behavior statistics can also be monitored, and they can be provided with customizable time-of-click messages to help reinforce anti-phishing awareness training. With zero dependency on error-prone threat-detection methods, such as data analytics, Menlo Security's Phishing Isolation solution is the only email security solution that protects every enterprise and every email user the instant it's deployed.

Conclusion

Credential phishing attacks are increasingly targeting enterprises—and it's easy to see why. Threat actors are experts at manipulating users' emotions and human nature to get them to click on a malicious link. Traditional detection-based solutions aren't catching these attacks in time—largely due to the fact that they are highly-targeted, specific attacks that are not intended for mass infection. Web isolation is the only security technology that can stop all credential phishing attacks. It does this by isolating all traffic in a secure, trusted environment, preventing malware from reaching users' devices and by rendering login pages in read-only mode.

➔ **Credential phishing attacks don't stand a chance.**

Menlo Security

About Menlo Security

Menlo Security protects organizations from cyber-attacks by seeking to eliminate the threat of malware from the web, documents, and email. Menlo Security's cloud-based Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and financial services institutions, and backed by General Catalyst, Sutter Hill Ventures, Engineering Capital, Osage University Partners, American Express Ventures, Ericsson Ventures, HSBC, and JP Morgan Chase. Menlo Security is headquartered in Palo Alto, California.

2300 Geng Rd., Ste. 200

Palo Alto, CA 94303

Tel: 650 614 1705

info@menlosecurity.com

menlosecurity.com