Menlo Security

WHITE PAPER

Is SaaS the New Trojan Horse in the Age of Cloud Computing?

Traditional security products are not designed to protect enterprises against SaaS-based attacks

Security teams need to rethink how they protect users from SaaS-based attacks.

The Internet is changing the way we work. No longer are users chained to their desks or the data center. They are more mobile, more collaborative, and more flexible than ever. They also leverage web-based apps, rich-media websites, and Software as a Service (SaaS) services to complete daily responsibilities and engage with customers.

While SaaS has made employees more productive, it's also made enterprises less secure. Once confined to gateways that guarded the data center, a company's attack surface is now unlimited and ubiquitous. The attack surface is now basically everywhere that users log in from—whether it's a remote office, their home, at a customer site, through public Wi-Fi, or while lounging at the beach. The more tools used by an enterprise, the greater the attack surface that the security team needs to track, monitor, and secure.

Attackers have noticed. Menlo Security's research has confirmed that SaaS services are increasingly being utilized to attack enterprises—essentially becoming the Trojan horse in the age of cloud computing. Traditional security solutions have become more effective at stopping malware and blocking access to suspicious sites, so attackers are now using legitimate SaaS services to dupe users into divulging their credentials or unknowingly download and install malware.

The danger to enterprises is real, since many of these services are actually whitelisted by security products because they are approved services. This means that security products that block phishing links or user access to malware are bypassed, leaving the enterprise with few or no defenses against these advanced attacks.

Enterprises Are Increasingly Moving Business Systems to SaaS Platforms

SaaS adoption, in particular, is exploding in the enterprise.

SaaS adoption, in particular, is exploding in the enterprise. Critical systems such as ERP, CRM, collaboration and communication platforms, customer-facing apps, and other business tools that were once on premises are moving to the cloud, so users can log in from anywhere and access all the information they need.

According to Blissfully, enterprises with more than 1,000 employees are adopting SaaS platforms at a rapid pace—with each employee using an average of 9.5 SaaS apps as part of their daily routines. Office 365, for example, is now used by one in five corporate employees worldwide, making it the most widely used cloud service by user count. Leading the way is the financial services industry, followed by manufacturing, healthcare, and legal services. In total, there are 155 million Office 365 business users, making up more than half of the 81 percent of total organizations that have made the shift to cloud services.

Attackers Are Increasingly Using SaaS Platforms as the Trojan Horse

Attackers are capitalizing on this trend and are using popular SaaS platforms to launch attacks.

SaaS adoption by the enterprise is no secret. Malicious actors—including cybercriminals and cyberterrorists, insider threats, industrial spies, and hacktivists—are capitalizing on this trend and are increasingly using popular SaaS platforms as an attack vector. Credential theft and malware downloads are the two most common types of attacks, and, like the original Trojan virus, these new attacks use social engineering with the intent to gather valuable data or install a back door to gain unauthorized access remotely.

Credential Phishing Example

An attacker hosts a malicious document in a cloud storage account such as OneDrive, Google Drive, Box, or iCloud. The attacker then shares the document with targeted users under the guise of a legitimate purpose. Some examples include invoices, statements of work, or another action that may be relevant to the target's occupation. Once the document is opened, users are encouraged to click on a link in the document that takes them to a fake web form, where they are prompted to provide their credentials—which are then used as another threat vector to steal information, access other business systems, or simply create havoc.

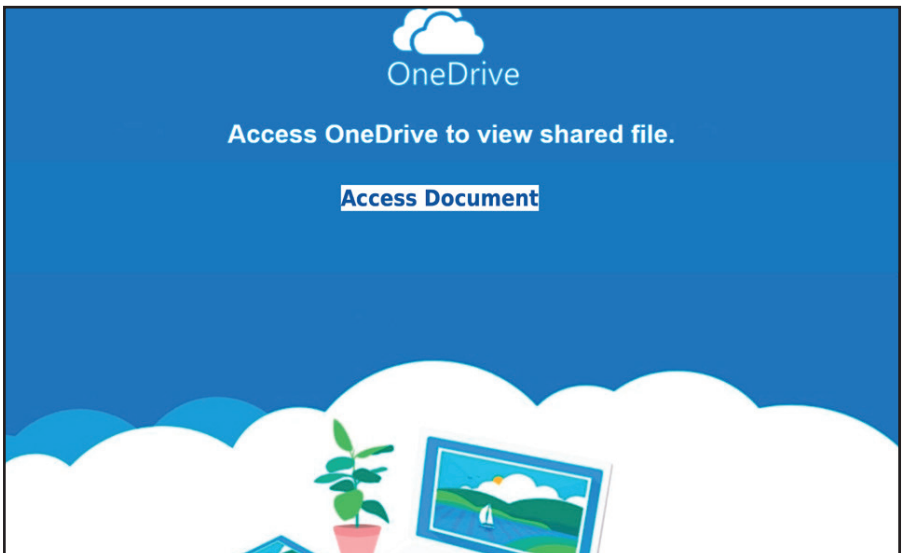


Image: A fake OneDrive page is used for credential theft

Malware Example

A piece of malware is stored in a SaaS platform as a raw or ZIP file. The attacker shares the file with a targeted user, who downloads the malware to their device. From there, the attacker is able to control the device, perhaps laying in wait for days, weeks, or months until the malware can spread to other systems.

Image: A victim is sent an email that is tied to their job responsibilities and seems legitimate.

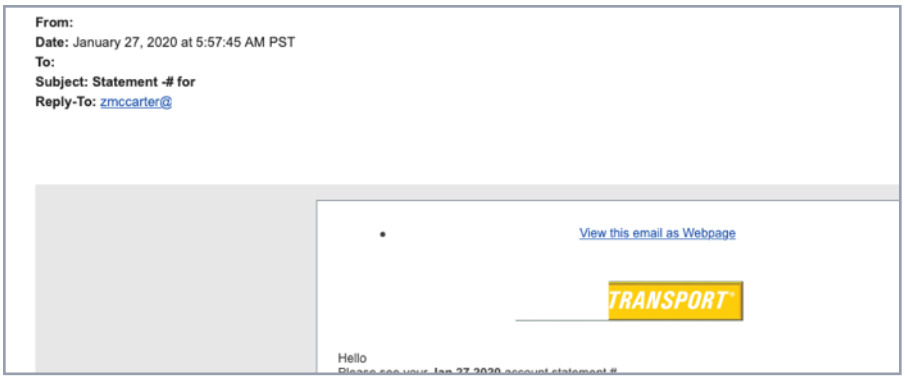
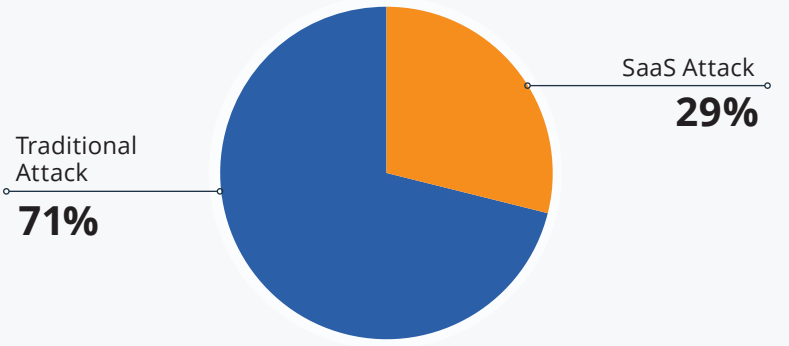


Image: The ZIP file has an embedded .exe extension that is the malicious payload. The ZIP file, however, is password protected with the password in the readme.txt file.

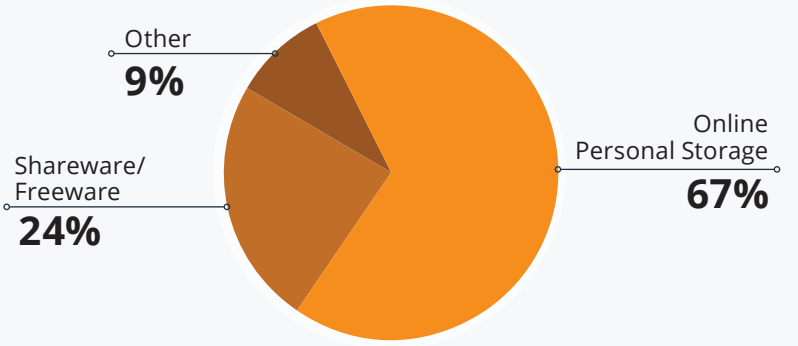
Digging into the Data

Menlo Security monitored the increase in attacks that leveraged legitimate SaaS services throughout 2019. An in-depth analysis by Menlo Security's research team showed that nearly one-third (29 percent) of all attacks leveraged a legitimate SaaS service to launch an attack.

Percent of SaaS Attacks



SaaS Services Used in Attacks



Of the attacks that used SaaS as an attack vector, two-thirds (67 percent) originated from an online personal storage platform, while one-fourth (24 percent) originated from shareware or freeware. Attackers used well-known SaaS providers to launch these attacks. The data shows that nearly all the attacks (97 percent) originated from five of the most well-known SaaS companies: Microsoft, Google, Dropbox, Box, and Amazon. Microsoft OneDrive alone accounted for 90 percent of all attacks that used online personal storage. This is not surprising given the popularity of Microsoft Office 365 in the large enterprise market, which includes OneDrive.

Isolation Protects Enterprises from SaaS Attacks

As cloud transformation continues to explode in the enterprise, security teams need to rethink how they protect users from these increasingly sophisticated types of attack. Traditional detect-and-respond approaches rely on categorization and up-to-date, real-time threat intelligence. Unfortunately, there's no way to tell legitimate requests from malicious ones in SaaS platforms. Instead, enterprises have to make a choice. They can either block all SaaS traffic, which would severely limit productivity and grind cloud transformation to a halt, or they can allow all SaaS traffic to flow unimpeded to users' devices, which doesn't do anything to protect users from these types of attacks. In addition, any insight into active attacks from threat intelligence is likely to come too late, because threat actors are able to spin up and customize out-of-the-box phishing and malware attacks from the dark web easily and cheaply with little or no coding expertise.

Delivering isolation services through the cloud allows enterprises to employ a Zero Trust Internet strategy, which assumes that all web traffic is risky.

Microsoft Office 365 (O365), probably the most widely used SaaS service in the world, provides unique challenges for enterprises when it comes to security. Because of technical issues, companies using O365 often bypass their traditional security layers, such as the proxy, and connect directly to Microsoft. Some cloud security vendors actually tout this as a benefit, meaning that enterprises are relying completely on Microsoft's ability to detect and stop attacks. However, this eliminates the security barrier for attackers, allowing them to gain entry into the enterprise. Though the user experience is improved with faster email access and attachment downloads, the enterprise is essentially creating an unguarded entry into their network.

A better approach is to take a Zero Trust Internet strategy and implement a security layer that isolates email links or attachments sent through any SaaS service. This can be done with a global cloud proxy that blocks known malicious sites and isolates everything else in the cloud. It doesn't matter if there's a known or unknown vulnerability, because no content—whether it is malicious or not—is executed on the endpoint browser where it could potentially do serious damage. So users are free to click on any link in an email, a document, or a SaaS platform. The resulting traffic is executed remotely in the cloud and has no avenue for delivering malware to users' devices.

Security without Compromise

Enterprises are undergoing cloud transformation, giving users ubiquitous access to the cloud-based tools and information they need wherever business takes them. Unfortunately, this makes SaaS platforms an enticing vector for attackers who are able to store and share malicious content and links in compromised or free accounts. Traditional hardware-based

security approaches that rely on making a detect-and-respond decision at the perimeter fail to protect users from SaaS attacks. A cloud security transformation strategy that delivers security services such as isolation through the cloud is the only approach that provides 100 percent protection to all users from SaaS attacks. In this Zero Trust Internet approach, it doesn't matter if users click on links in an email or a cloud document, they are protected. And, most importantly, isolation allows users to click with impunity—opening up more of the Internet so they can do their job effectively. It's security without compromise.

For more information on how your organization can protect users from SaaS attacks, visit menlosecurity.com or email us at ask@menlosecurity.com.

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security has helped hundreds of Global 2000 companies and major government agencies achieve Secure Cloud Transformation. The company's Cloud Security Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. The company was named a Visionary in the Gartner Magic Quadrant for the Secure Web Gateway.

Contact us
menlosecurity.com
(650) 614-1705
ask@menlosecurity.com