Phishing in the Age of SaaS

AN ESSENTIAL GUIDE
FOR BUSINESSES AND USERS

AVANAN
The Cloud Security Platform

Q3 2017

intro

Phishing attacks have become the primary hacking method used against organizations. In the past, there was a tendency to blame the user, but attacks have evolved to appear so genuine that even the most security-savvy recipient can be fooled. Phishing attacks have recently experienced newfound success with the proliferation of SaaS in the workplace.

What is phishing?

Phishing is a hacking method in which the attacker sends a malicious message, usually an email, but sometimes a text message, Skype, or Slack message. The attacker impersonates a trusted entity with the intention of convincing the recipient to share sensitive information, transfer funds, or connect to a fraudulent website.

Phishing continues to be a very effective hacking method for a number of reasons.

1 By leveraging the standard communication channels, hackers have direct access to all users in the organization.

2 Computer-based filters eventually fail because hackers constantly reverse engineer the algorithm until they find a way through.

Phishing attacks can spread like a computer worm.

Once one account is compromised, the attack can send messages to all the account holder's contacts so that further attack emails are coming from a trusted source and their legitimate account..

Who are they impersonating?

In general, hackers will try to impersonate a trusted person or legitimate service. To appear genuine, the format and timing of the message often resonates with the intended victim. For example:

Impersonating someone in the organization:

A. The CEO asking the CFO to wire funds
B. HR asking for personal info, especially around end-of-year or tax season
C. A 'new' employee at a distant branch asking questions

Forging an automated message impersonating a trusted service

A. A link to a shared Google Doc file
B. A Citibank bank deposit receipt
C. A Fedex shipping message

What are they after?

Ultimately, hackers are looking for monetization. They are well funded groups with 'investors' that expect a return on their investment.

Direct Monetization

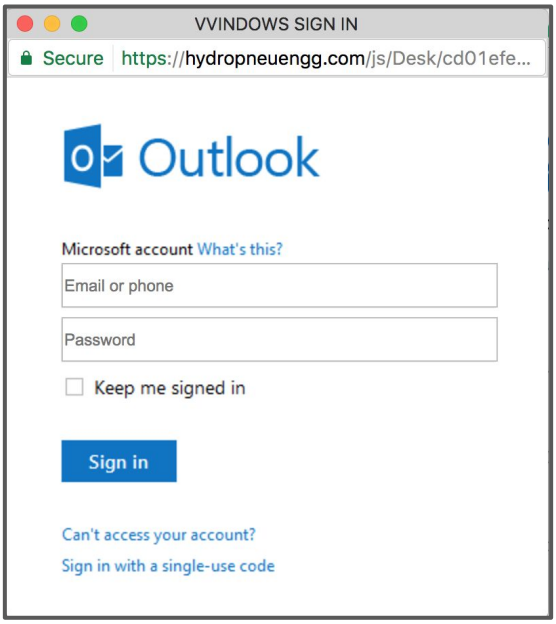
For example, fake wire transfers or ransomware that demands a payment to decrypt encrypted data.

Indirect Monetization

Selling credentials to compromised accounts, credit card numbers, personal data, etc. on the darknet to other entities that will monetize them.

Why is Phishing Easier on SaaS Platforms?

While the roots of phishing attacks trace back to the beginning of email adoption, the proliferation of SaaS has lead to a resurgence in this hacking method. SaaS applications are especially prone to these violations because they can be used in every form of phishing attack.



Fake Office 365 login: URL sent in email to O365 Email Users

Access

Impersonation is easier when the SaaS is the trusted communication channel and login can be from anywhere. If hackers manage to steal credentials, they have immediate access to the account.

Behavior

SaaS applications are an easy target for credential theft because **end users are continuously being asked to reauthenticate** and commonly receive messages with links that require a login. A rogue request for login credentials does not raise much suspicion.

Uniformity

Another aspect of SaaS that increases its vulnerability to phishing attacks is its **uniformity**. Hackers can open an account and test their methods until they are able to bypass the default filters. Once they have unfettered access to the inbox, the only barrier is an inattentive end user.

Previous Defense Measures

Solving the anti-phishing problem requires additional security layers on top of the SaaS default protection. Until recently, most solutions were deployed externally--either as a proxy for incoming messages (MTA) or as a gateway between the end user and the service (forward or reverse proxy). Because these solutions were deployed at the perimeter, they were typically blind to internal threats —compromised accounts or employee-to-employee messages.

What Can You Do?

The Avanan Cloud Security Platform was designed to defend against all forms of SaaS phishing attacks and overcome the weaknesses of earlier perimeter-based protection.

The Avanan Anti-Phishing package offers the security layers necessary to combat the rise of SaaS phishing attacks within all forms of SaaS communication, from email to chat message.

Solutions

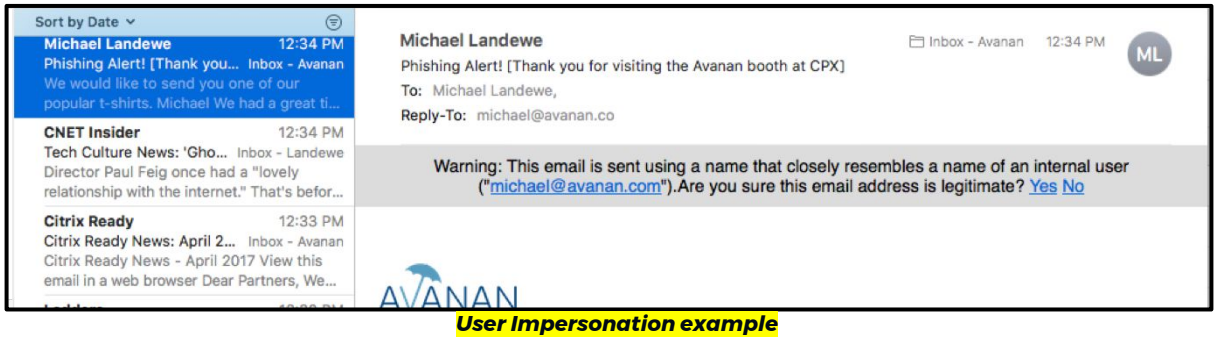
Impersonation Analysis

(Leveraging Big-Data analytics)
Both sender and message content are scanned for impersonation. The AI algorithms deployed for detecting and protecting from impersonation look for:

User impersonation
Avanan looks to see if a similar sender exists in the organization with a different email address. We identify the sender by cross referencing several fields in the email such as the sender, the signature at the bottom, etc.

Domain impersonation
Avanan checks if the sender is sending from a domain similar to a known domain but with a different mail-flow path, different source IP, etc.

Brand impersonation
Avanan detects if the email appears to be coming from a trusted brand (Fedex, Microsoft, etc) but mail-flow path does not fit that sender



User Impersonation example

Real user is "Michael Landewe <michael@avanan.com>" but this email comes from same user with email michael@avanna.co

URL and File Analysis

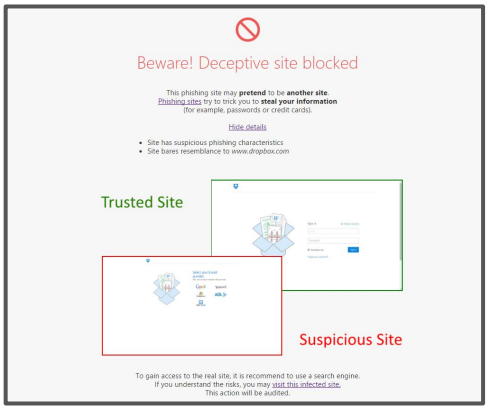
As many phishing attacks propagate through a malicious URL or contain a malicious file, it is important to scan this type of content before it reaches the end user. The two main methods of analysis conducted by this scan are:

Static analysis
Tools that perform static analysis of the content vary in technology but all analyze the content as displayed in the email. Some examples include Antivirus scanning, predictive malware analysis of files, URL reputation filtering, and more.

Dynamic analysis
Tools that perform dynamic analysis emulate the action of the file or link in a sandbox environment and compare the result to known malware activities. Some examples include following a URL and comparing the rendered image result to that of a known login page or opening a file in a sandbox environment to test the actions it takes.

Solutions

To circumvent the SaaS default security, hackers have created attacks intended to evade standard detection. Therefore, it is important to test and emulate such combinations recursively, for example, by finding a URL within a file, following the link, and then scanning the file that might be downloaded.



Example of a report from an attack blocked by Avanan

AI Baselining for Suspicious Email Activity

By looking at an array of indicators from the age of the linked domains or by verifying the sender, Avanan can present a message to the end user asking if they know or trust this sender without blocking traffic. This interaction allows the algorithm to learn what is legitimate and what is malicious based on end user interaction.

Dynamic Quarantine and Message Control

Avanan's API-based approach allows it to quarantine suspicious emails even after they have already arrived in a user's inbox. While most security solutions can only quarantine emails in transit, the ability to do so after delivery allows the Avanan solution to incorporate real-time information such as previously benign URLs that later become malicious.

Monitoring for Compromised Accounts

Some email attacks attempt to spread from a compromised account to the rest of the organization. Therefore, it is important to truncate the internal distribution of the attack. Avanan does this with two security layers. First, it monitors for compromised accounts by baselining each user's behavior and flagging anomalous activity. Second, the Avanan solution scans for malicious attachments and phishing links within all emails - including those originating from internal users.

summary

The proliferation of phishing attacks has been correlated with the growth in SaaS adoption. Avanan leverages its multi-layer, multi-vendor approach for SaaS security to create the most advanced anti-phishing protection with several technologies and multiple vendors working in sync. We ensure that any organization is protected from even the most sophisticated of attacks.

Want to protect your organization from phishing attacks?

Schedule a demo

Start your free trial