SONICWALL®

PHISHING IN THE AGE OF SAAS

An Essential Guide for Businesses and Users

Introduction

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

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

Forging an automated message impersonating a trusted service

1. A link to a shared Google Doc file
2. A Citibank bank deposit receipt
3. 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.

Forging an automated message impersonating a trusted service

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.

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

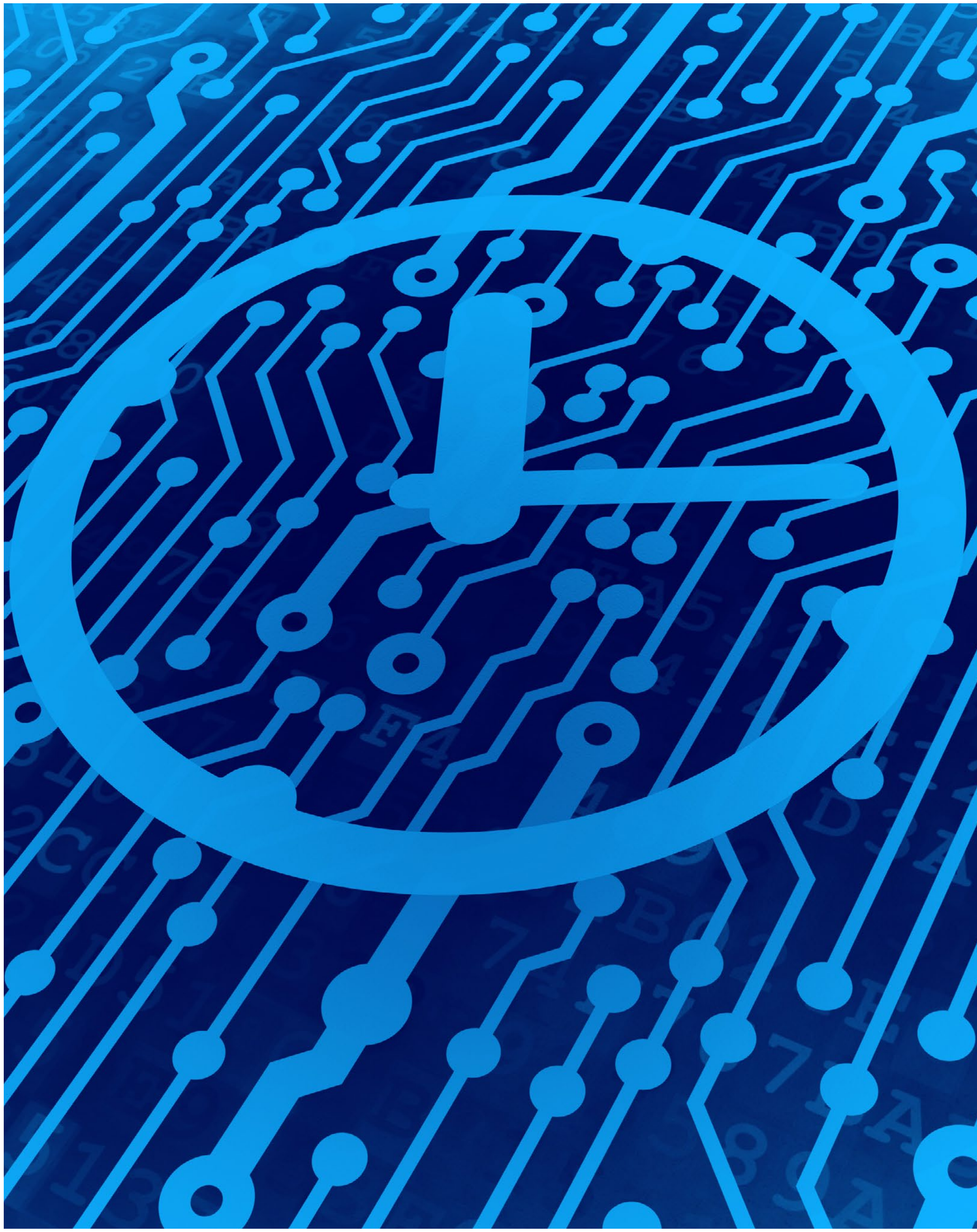
SaaS applications are an easy target for credential theft because **end users are continuously being asked to reauthenticate** and commonly receive messages with links that require a login. A rogue request for login credentials does not raise much suspicion.

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

The built-in anti-phishing technology 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

Cloud App Security 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

Cloud App Security 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

Cloud App Security detects if the email appears to be coming from a trusted brand (FedEx, Microsoft, etc) but mail-flow path does not fit that sender.

Solutions

URL and File Analysis – Leveraging Capture ATP

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. Cloud App Security utilizes Capture ATP service to detect and block advanced threats until verdict. This service is the only advanced threat-detection offering that combines multi-layer sandboxing, including RealTime Deep Memory Inspection™ (RTDMI™), full system emulation and virtualization techniques, to analyze suspicious code behavior within emails, to protect customers against the increasing dangers of zero-day threats. The service includes advanced URL protection that dynamically analyzes embedded URLs, to block and quarantine messages with malicious URLs before so users never click on them and become compromised.

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.

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, Cloud App Security 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

Cloud App Security 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.

Monitoring for Compromised Accounts

Cloud App Security detects if the email appears to be coming from a trusted brand (FedEx, Microsoft, etc) but mail-flow path does not fit that sender.

Summary

The proliferation of phishing attacks has been correlated with the growth in SaaS adoption. SonicWall Cloud App Security leverages its multi-layer 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?

CONTACT SALES

About Us

SonicWall has been fighting the cybercriminal industry for over 27 years, defending small, medium-sized businesses and enterprises worldwide. Our combination of products and partners has enabled an automated real-time breach detection and prevention solution tuned to the specific needs of the more than 500,000 organizations in over 215 countries and territories, so you can do more business with less fear. For more information, visit **www.sonicwall.com** or follow us on Twitter, LinkedIn, Facebook and Instagram.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.