Current Security Solutions and User Training are Not Solving Your Phishing Problem

Learn why moving web browsing activity from your endpoints to the cloud eliminates phishing risks, and should be your next security move

Introduction

Cyberattacks are continuing to increase dramatically in both number and severity. Reports of successful attacks using sophisticated new malware strains seem to appear weekly, with vendors like Microsoft and Google scrambling to get patches into the market to address vulnerabilities, and IT staff rushing to get updates onto exposed systems.

Phishing is the initial access channel in over 41% of all cyber incidents. Malicious attachments were deployed in 62% of those phishing attacks and malicious links in an additional 33%.

With sophisticated multipurpose phishing kits, cybercriminals can chose from a menu of top technology brands to spoof.

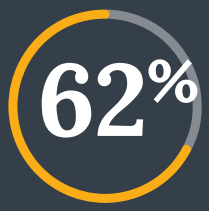
IBM X-Force Threat Intelligence Index 2023

Table of Contents

Why Haven't Current Solutions Slowed the Rising Tide of Phishing Attacks?

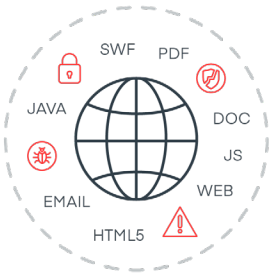
Current cybersecurity defences have proven to be ineffective at preventing browsing based exploits such as phishing attacks. Advanced malware, including drive-by browser exploits, amazingly realistic spoofed phishing sites, weaponised web downloads, and spear phishing attachments all frequently evade existing endpoint protection solutions and network security stacks. Once malicious code from websites or attachments gets onto a device's local browser, the battle has effectively been lost. Traditional web and email security techniques are unable to stem this tide. Let's look at why this is true.

Spear phishing attachments are used in



of phishing incidents.

The majority of malicious sites use encryption to hide threats. For example, 72% of phishing links send users to sites that use encryption to mask the malware they contain[1]. Most organizations do not decrypt traffic before inspection because of the significant performance impact it creates, so they are "flying blind" as far as encrypted traffic goes. In addition, many organizations lack visibility into applications and endpoints that are exposed through identity access management and single sign-on (SSO) portals. Even knowing the risk, most realize that their threat scanning technology, which works by matching traffic scans to known malware variants, would not catch zero days anyhow.



1. Phishing website with embedded malware

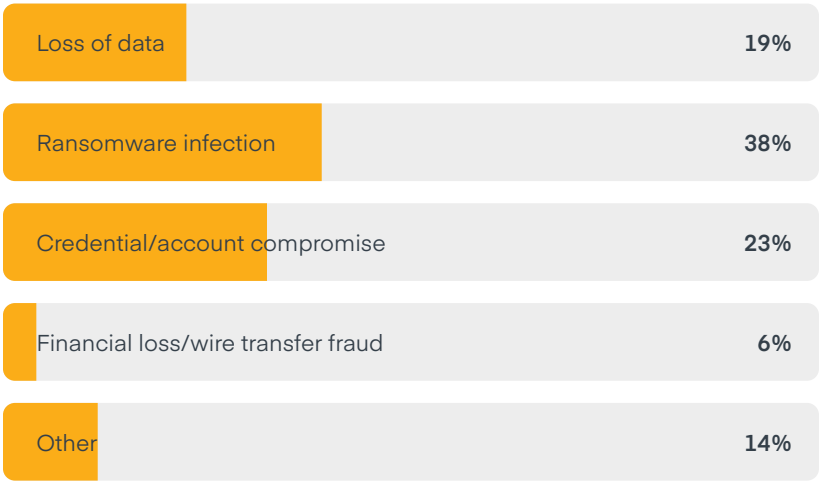
2. Bypasses security, enters local device's browser, compromises system

[1] ***Gartner*** *2020 Security and Risk Management Summit*

Instead, they choose either to dramatically limit web access ("Block all sites that are uncategorized because of limited reputational history") or to just accept the fact that they will be successfully attacked and deploy resources to try to contain breaches after an initial incident.

Of course, either approach is a losing proposition. Talk to any CIO and you will hear how preventing internet access ("over-blocking") in the name of security is a constant source of significant tension with the business lines they support. On the flip side, opening internet access, under pressure from business lines, leaves the door open to ransomware and other sophisticated threats that evade legacy protections, compromise endpoints, and then move laterally across the network.

What was the impact of the last successful phishing attack on your organization?



Gartner Peer Community Survey

In this scenario, security professionals are basically depending on end-users themselves to be part of the security stack, hoping that training and good sense will keep them out of trouble. Unfortunately, history has shown that end-users are often a weak link. An average user receives over 500 phishing emails per year. Even if training is 98% effective (and even training providers do not claim figures that high), each user in your organization is likely to click 10 phishing emails each year. Yet one single click is enough to take down a business. Today, instructing users not to open emails without checking them first should not be the strongest defensive strategy that corporations rely on.

Security professionals are basically depending on end-users to be part of the security stack, hoping that training and good sense will keep them out of trouble. Unfortunately, even security professionals fall for brilliant social engineering appeals.

RBI: A Game Changer for Eliminating Phishing Attacks and Other Common Browser Exploits

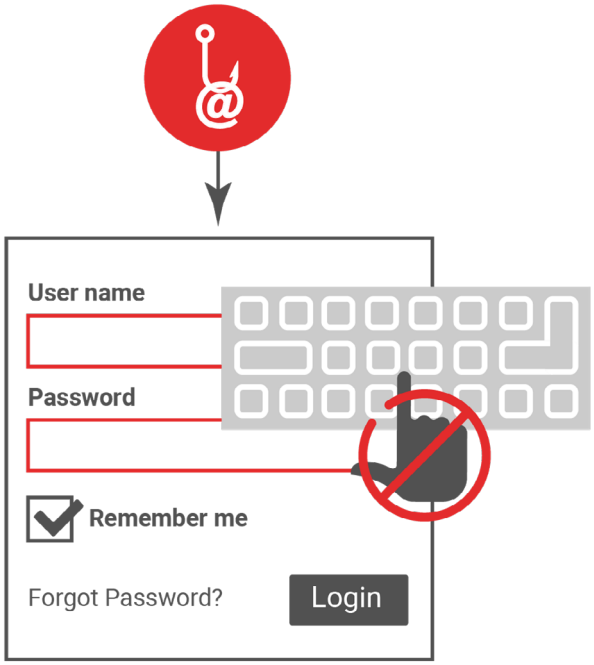
Fortunately, now there is an answer. It is called Remote Browser Isolation, or RBI and it offers a fundamentally different approach to securing the use of the web and email. RBI dramatically changes the playing field in the ongoing cyber cat-and-mouse game, taking the user out of the security equation and opening up web access so employees can stay both productive and secure. Based on the military concept of 'air-gapping' sensitive systems from the internet, RBI can be easily deployed using Ericom Web Isolation.

Think of Remote Browser Isolation as a Zero Trust security approach for the web. RBI is a way to "take the concept of Zero Trust ("trust nothing, always verify") and apply it to user interactions outside of an organisation… ensuring that all of the potentially bad stuff stays isolated on the other side of your network fence."[2] RBI moves browsing activity (e.g. the mechanics of rendering a webpage) away from the endpoint, isolating it in cloud instead. This approach air-gaps endpoints from the internet, ensuring they stay completely protected.

Ericom's innovative agentless approach allows users to access the web as they normally would using their native browser. The local browser application, however, unbeknownst to the user, is communicating with an Ericom cloud-based browser, which actually renders (e.g. executes) the webpage's code. Each browser session runs in a secured isolated cloud container that is destroyed after the browsing session. Only safe rendering information is streamed to the device, not the potentially dangerous web code. Endpoints (and the networks and applications they are attached to) are air-gapped from 100% of the malware hidden on websites, even the most sophisticated zero-day threats targeting web browser vulnerabilities. Yet users can interact with the websites they use, just as they do when browsing directly from their local browser — only without risk.

Organizations can choose to prevent users from downloading web documents and email attachments, electing instead to permit them to be viewed only within an isolated environment. Alternatively, Ericom Web Isolation integrated Content Disarm and Reconstruction (CDR) can scan files for viruses and remove any risky active content, delivering them to users with desired native file functionality intact.

[2] *https://www.csoonline.com/article/3534716/review-ericom-shield-extends-zero-trust-to-websites-with-browser-isolation.html*



On the email front, organizations can set policies that effectively eliminate the risk of phishing malware and credential theft. Phishing sites, by their nature, are almost always short lived and "new" to the internet, spun up and down in order to avoid being identified as malicious sites. As a result, they get classified by URL engines as "uncategorized." Ericom Web Isolation renders all uncategorized websites launched from URLs embedded in emails in "read-only" mode, thereby preventing users from being tricked into entering their credentials for websites, cloud applications, databases and so on.

Realize the Benefits of Zero Trust Browsing

Ericom Web Isolation truly delivers a "trust nothing, always verify" Zero Trust approach to web access. By moving the mechanics of web browsing off the endpoint and to the remote isolation cloud, organizations are taking the approach that no website is secure enough to bring its content directly onto the local device's browser. This approach eliminates zero-day exploits, even encrypted ones, targeting local browser vulnerabilities through phishing, social engineering, drive-bys, weaponized downloads, and other sophisticated attacks. And since RBI protects organizations from users that click on links in phishing emails (e.g. the unmanageable "human factor" in cybersecurity), it solves the phishing problem that has challenged CISOs and CIOs for so many years.

Organizations can use the Ericom Cloud Service with existing NGFW and Web Gateway solutions to apply isolation to specific categories of websites (e.g. uncategorized sites, social media, webmail), or to set policies to isolate all web traffic of select users, such as IT teams, C-levels and others who are frequent targets of hackers who want access to the sensitive data and credentials on their devices. And for organizations needing a higher security risk posture, all web browsing, including traffic to "trusted" allow-listed websites which could potentially contain malware as well, can as an option be isolated by Ericom Web Isolation.

The solution brings operational benefits to IT and Security departments as well. For example, by eliminating threats targeting organizations through web and email vectors, RBI reduces the numbers of network threats to which SOC analysts and threat hunters need to respond, allowing them to be more efficient and effective. Additionally, Network Operations and Help Desk personnel no longer need to waste time and effort responding to trouble tickets from users requesting policy changes to allow them to access websites from which they have been blocked. A final benefit is seen in the Risk and Privacy Compliance area. RBI provides a solution to the challenge of cookie management and privacy settings for corporate users. As a user closes a browser session, the content of the isolated cloud-based container is deleted, ensuring unwelcome cookies, changes to privacy settings, and website code never reaches the corporate infrastructure.

Simple to Deploy and Integrate with Existing Systems

Adding new security solutions is typically complex and takes time. They need to be integrated with other systems and support cloud, on-premise and remote access architectures. Ericom was developed with easy integration in-mind, allowing it to be easily deployed, regardless of the number of users in your organization. They are security gateway (SWG, NGFW, or CASB) agnostic, and work with existing DLP and web filtering solutions. As a cloud-based solution, it does not require any complicated "rip-and-replace" efforts. And because it is a cloud service, no servers, desktop agents or client-side software are required.

Summary

Eliminates common exploits targeting browsers (phishing, ransomware, etc.)

Moves browsing to a remote cloud container, keeping threats off your endpoints, networks and applications

Removes "human factor" risks, enabling IT to give users productive broad web access

Flexible policy controls to intelligently target the use of web isolation

Works with all leading firewall and web filtering gateways; hybrid deployment options available

Scalable cloud service is simple to activate and quickly delivers the value organizations expect

As many organizations' first foray into implementing Zero Trust security, replacing VPNs with Zero Trust Network Access is exciting but also daunting. Careful preparation — including choosing a partner to assist in the process, choosing a solution that meets both immediate and long-term needs, and developing granular policies that allow the organization to reap maximum benefits from the new solution — is the key to a smooth and successful transition.

Contact us today for a personalized demo or to learn more about our cloud-delivered cybersecurity service at **ericom.com/contact-us.**

