MEMCYCO

Authenticity Goes Both Ways

White Paper

How to protect your brand, organizations & end users against impostors using Proof of Source Authenticity (PoSA™)

TABLE OF CONTENTS

INTRODUCTION

Since the creation of the internet, businesses have been focused on authenticating the users who request access to the company's digital assets. Many existing solutions allow companies to better authenticate their users and this area of security continues to evolve. But, while this side of the trust relationship between customers and organizations in the digital realm has been addressed, the customer side has been neglected. How can a user authenticate a company's digital presence and communications? How can a company help keep its users from falling into imposter traps that use the company's brand and logo as bait?

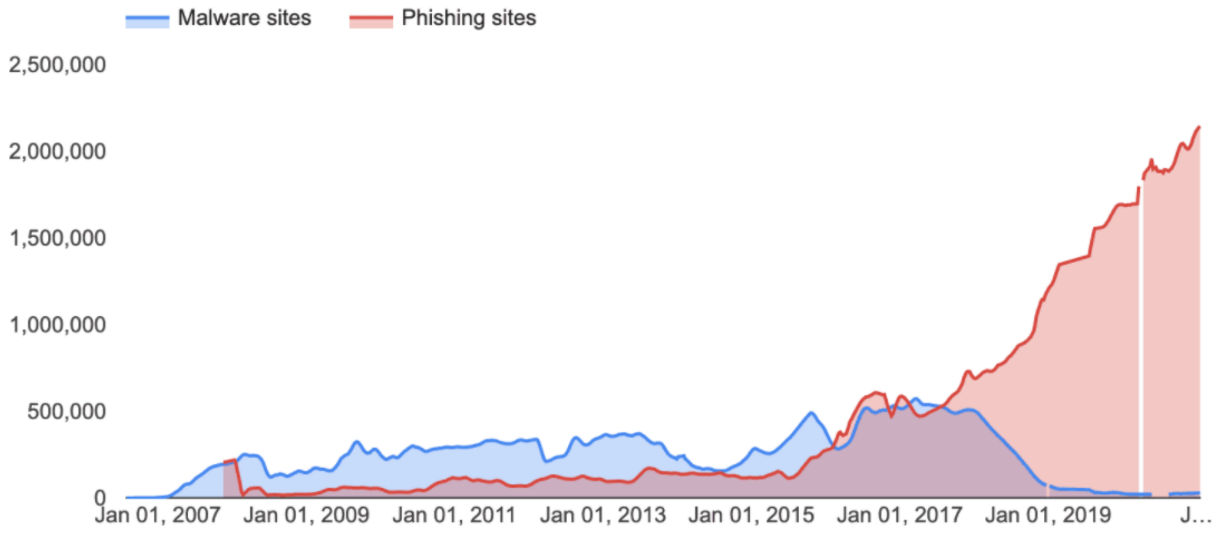
Until recent years customers were usually safe in assuming the web page they were visiting was indeed authentic. But with the dramatic rise in cyber-attacks, specifically the booming ”phishing racket,” customers are fast becoming wary of engaging with emails and other messages and hesitate to transact online because they are constantly hearing of impostor sites, counterfeit brands and phishing scams. Users receive emails and text messages that look and feel completely legitimate but contain URLs that, when clicked on, send the user to fraudulent websites where her account is taken over, her identity is stolen, her money is taken, or she is tricked into buying counterfeit goods.

In the last few years, the digital world is facing a growing problem of cyber attacks using impostor websites and fraudulent communications. According to AARP, 50% of American adults were exposed to these attacks. While it has become imperative for brands to take notice of this trend, these attacks occur beyond their security perimeters and there is no way for brands to know about these attacks, unless their customers inform them about being attacked. Worse, brands often hear about attacks when their customers post the story on social media and target their frustration toward the brand. This leaves both the brands and their end-users exposed to significant damage.

This phenomenon has become so prevalent because the brands do not have an effective solution that can detect the attack as it occurs and alert the user in real-time before damage can be done, or an effective shield to protect their users from falling into the traps.

Currently, the only approach to alleviating some of the problems is based on technology that scans for impostor domains. This is a constant “Cat and Mouse” chase and the brands are always one step behind the attackers. The end users are left exposed, as they have no real way to confirm that they have accessed a genuine website and not a fake one. The only confirmation of website authenticity is the website's certificate, shown as the tiny lock icon in the browser next to the URL, which goes completely unnoticed by the typical user. Even worse, the certificate provides no real proof that the user is communicating with the correct and legitimate website. The vast majority of impostor sites will also show such certificates on their sites.

The lack of advanced solutions that will detect and alert in real-time on these attacks, and will protect the end users from falling into the traps in the first place, leaves the door wide open for hackers to impersonate legitimate sites through various methods such as spoofing, cloning, or re-engineering the target. Hackers use these methods not only to launch phishing campaigns but also for good old-fashioned crimes such as stealing innocent user data or selling counterfeit goods.



This chart - pulled from Google Safe Browsing - shows the steep increase in the number of websites deemed unsafe between January 2016 and January 2021.

Another factor that must now be considered is the use of remote and online web services, which has risen dramatically due to the COVID19 pandemic and is increasingly here to stay. This trend has increased the need for a higher level of all forms of cybersecurity.

It is now abundantly clear that there is a need to allow users to safely open emails, visit websites, and transact digitally - being assured they are engaging with real authenticated entities. This paper describes such a Proof of Source Authenticity approach.

BRAND EXPLOITATION AND THE DIGITAL TRUST ISSUE

Impersonating sites (phishing, counterfeit or fake sites) is a type of cybercrime where an attacker imitates a genuine familiar website to trick a human victim into revealing sensitive information to the attacker, falsely transact with them, or deploy malicious software on the victim's infrastructure. The most popular techniques for attackers to imitate genuine sites are Spoofing, Cloning, or iFraming genuine websites.

These attacks are on the rise: Reports suggest that 75% of organizations around the world experienced a phishing attack in 2020, and 74% of attacks targeting US businesses were successful.
How are these attacks carried out? 96% of social engineering attacks are delivered by email, while 3% arrive through a website, and 1% are associated with phone or SMS communications and malicious documents respectively.
How is this affecting users? According to an AARP 2020 survey, “half of US adults have been targeted by impostor scams”.
What happens when scams succeed? FBI 2020 annual report suggests that brand impersonation represents 50% of cyber crime, $2 billion in the USA

No matter what technique the hackers use, their main target is to make a user click on an allegedly legitimate link, which then takes them to an impersonating site or page. There, they will do anything ranging from stealing user credentials, gaining access to account information, selling counterfeit goods, or scamming users into transferring money to criminals. These attacks occur every day in every industry: retail, health, financial, educational services, and more.

What does it take to launch such attacks? Nowadays, the ability to impersonate a website using spoofing or cloning techniques has become a common skill in the hacker community. Toolkits that automate the process are easily available for criminals to use.

How is the market responding to these attacks? Specifically for employees who are targets of such attacks, some protection is offered via a variety of solutions that try to filter out attacks by scanning email traffic arriving at company-controlled email accounts to identify blacklisted links or otherwise suspicious content. Organizations also invest in computer-based security awareness training - educating employees to identify risks and attacks and simulating them to see how well they have been trained. Solutions are also available that scan for impostors and phishing sites - to allow legitimate site owners to take steps to ask authorities for their removal. These solutions are far from effective in finding fake sites and even when such sites are found - taking them down is a lengthy process.

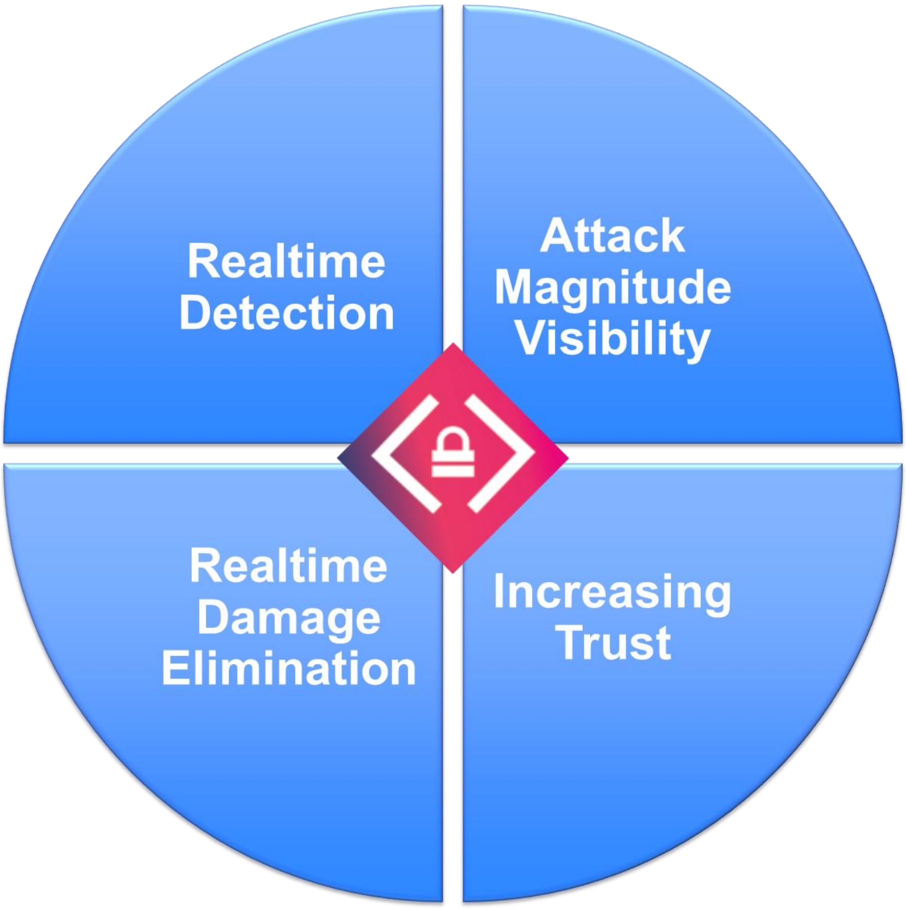
What about non-employee users? Attacks on customers, partners, and other users of the company's online services occur outside of the security perimeter of the company. These users might get an email every once in a while informing them of the risks relating to phishing campaigns, counterfeit sites, and scams. Some companies also put a "fraud notification warning" on their websites. But educating users in this manner is always too little and often too late, and the damage from the attacks to the general consumer is far reaching (see Phishing Fear Syndrome). The time has come for a proactive solution that alerts in real-time and protects the end-users from falling into the traps, that also provides users with the kind of trust they need to be sure the emails they read and the sites they visit are legitimate.

Phishing Fear Syndrome: Is a phenomenon whereby a user hesitates to engage with an organization because he or she is afraid of being attacked, even though the attack has not happened. To them, the slightest possibility of such an attack perversely affects their decisions online, hurting the organization in the process. For example, 60% of UK consumers are likely to apply checks before interacting with an organization's communications, including checking the spelling of the sender's email address and body of text.

CREATING USER TRUST IN ONLINE SITES AND CORRESPONDENCE

WHAT IS NEEDED

A solution that can tackle this phenomenon must provide these four critical pillars:



SOLUTION OVERVIEW

MEMCYCO has created a Proof of Source Authenticity (PoSA™) solution which provides a holistic solution to address the four pillars listed above. It is designed to provide organizations with real-time detection and alerting platform for impostor attacks, that issues real-time fake site alerts to attacked end-users, provides complete visibility on the attackers and the list of all exposed end-users, as well as allows organizations to provide positive confirmation to their end-users that web pages they visit and messages they receive are authentic.

Regarding the positive authenticity confirmation, PoSA™ applies a similar approach and has similar significance to that of watermarks on currency bills, but is also different in one critical aspect: the PoSA™ watermark can include a text code or a picture and animation that are unique to the specific user - much like a personal passphrase - that users can set themselves.

For real-time detection and alerts, PoSA™ is placed at the point of impact, where the attacker is attempting to carry out the scam. It detects and provides alerts on all types of impostor site attacks that use Spoofing, Cloning, iFraming, and Click Jacking techniques as well as any attempt of a hacker to investigate the website in order to create a fake one.

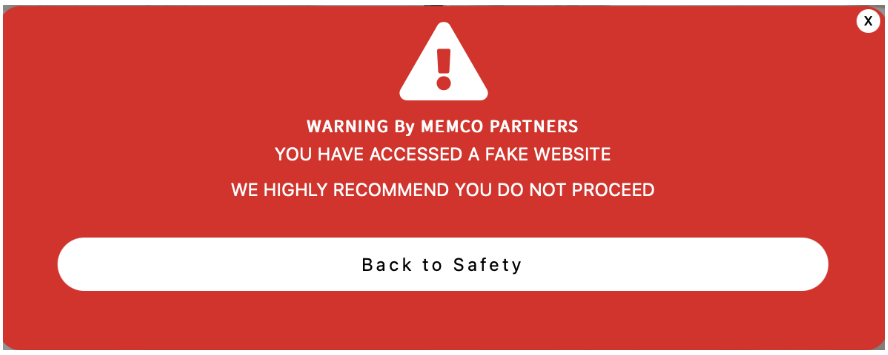
PoSA™ applies to websites, emails, and SMS messages using very quick and simple integration to the site/sender and no installation on the user's devices.

CAPABILITIES

FOR WEBSITES

The solution provides four layers of protection that can be activated together or separately:

Real-time detection and alerts to end-users (avoiding the damage) - The solution monitors activity on the website as well as at its end-users and alerts the end-users on attempted attacks using most kinds of impostor sites. In such cases, the end-users will be alerted in real-time by a prominent fake site alert appearing on their screens.



WARNING By MEMCO PARTNERS
YOU HAVE ACCESSED A FAKE WEBSITE
WE HIGHLY RECOMMEND YOU DO NOT PROCEED

This capability is achieved without requiring users to install software on their devices or register to the service - as will be explained later.

Alerts security teams in real-time on:

- Spoofing/Cloning/ iFraming/Click-Jacking attempts
- Redirects end-user from the phishing page to the real page after entering credentials
- Reverse-Engineering attempts - whenever an unauthorized user attempts to open developer tools on the website code, or uses a malicious browser extension
- Attempts to sign in from a previously unknown device
- Repeated frequent login attempts
- Abnormal behavior of users
- Password brute force attempts
- Code injection attempts
- Page modification - changes made to content after it was sent to the user device
- Impossible login attempts - Same time / Different location
- Debugger attempts
- VPN use detection

Real-time and historical reports:

- List and details of all attacked end-users in case of an impostor attack (Magnitude of the attack)
- User profiles and topology
- Device fingerprinting
- Details of the attacking domains
- Integration to SEIM and SOC platforms

- Central management

Personal digital watermark - a unique visual element on the website page that users can easily identify, to allow them to be certain that they are indeed accessing the authentic website and not an impersonating one. The watermark is stored in the user's local protected storage - thus blocking possible attempts to forge it.

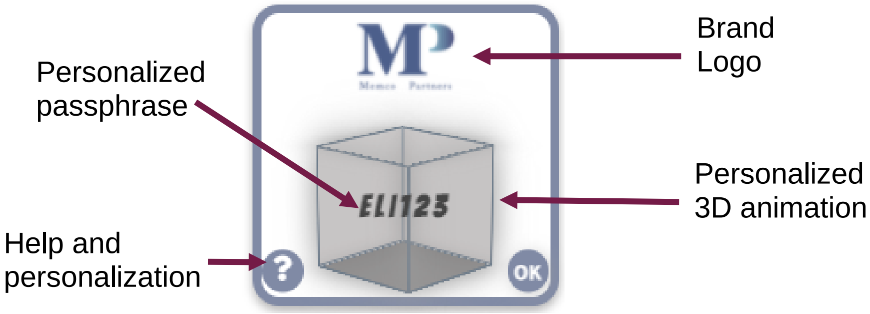


Fig 1- The Digital Watermark

With this mark appearing on a legitimate website and a little education about its significance, users become accustomed to its appearance and then can avoid fake sites when it does not appear or appears without their personal passphrase.

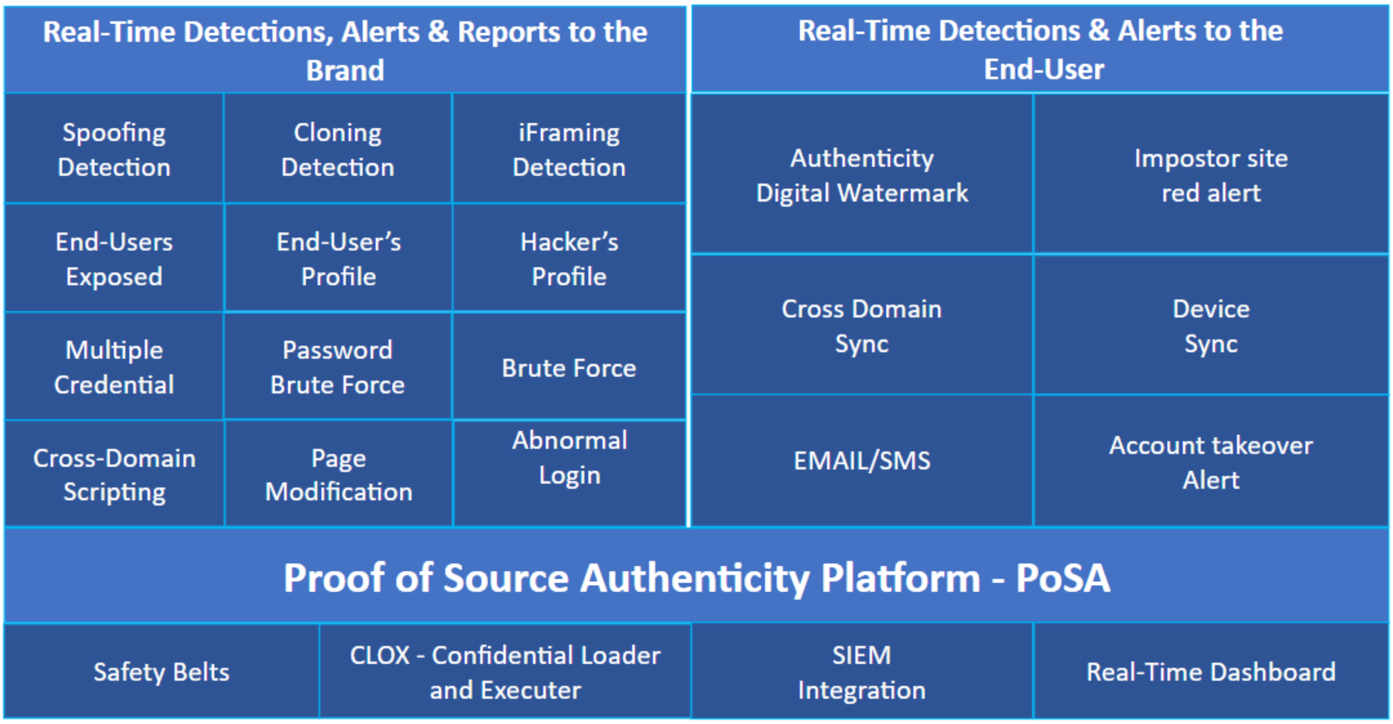
In addition, to further simplify the adoption of the watermark the solution allows:

- Cross-domain watermark consistency: allowing users to see the same personal passphrase in their watermark across the websites of multiple providers they work with
- Smart syncing across user-registered devices (PC, Tablet, Mobile)

PoSA™ platform safeguarding:

The platform is protected through several safeguard techniques (some of which are patent pending), these include an invisible Confidential Loader Executer (CLOX), "PoSA Tamper Protection ” scripts, Debugger attempts protection, High availability services and data encryption.

Platform building blocks



Real-Time Detections, Alerts & Reports to the Brand

Spoofing Detection

Cloning Detection

iFraming Detection

End-Users Exposed

End-User's Profile

Hacker's Profile

Multiple Credential

Password Brute Force

Brute Force

Cross-Domain Scripting

Page Modification

Abnormal Login

Real-Time Detections & Alerts to the End-User

Authenticity Digital Watermark

Impostor site red alert

Cross Domain Sync

Device Sync

EMAIL/SMS

Account takeover Alert

Proof of Source Authenticity Platform - PoSA

Safety Belts

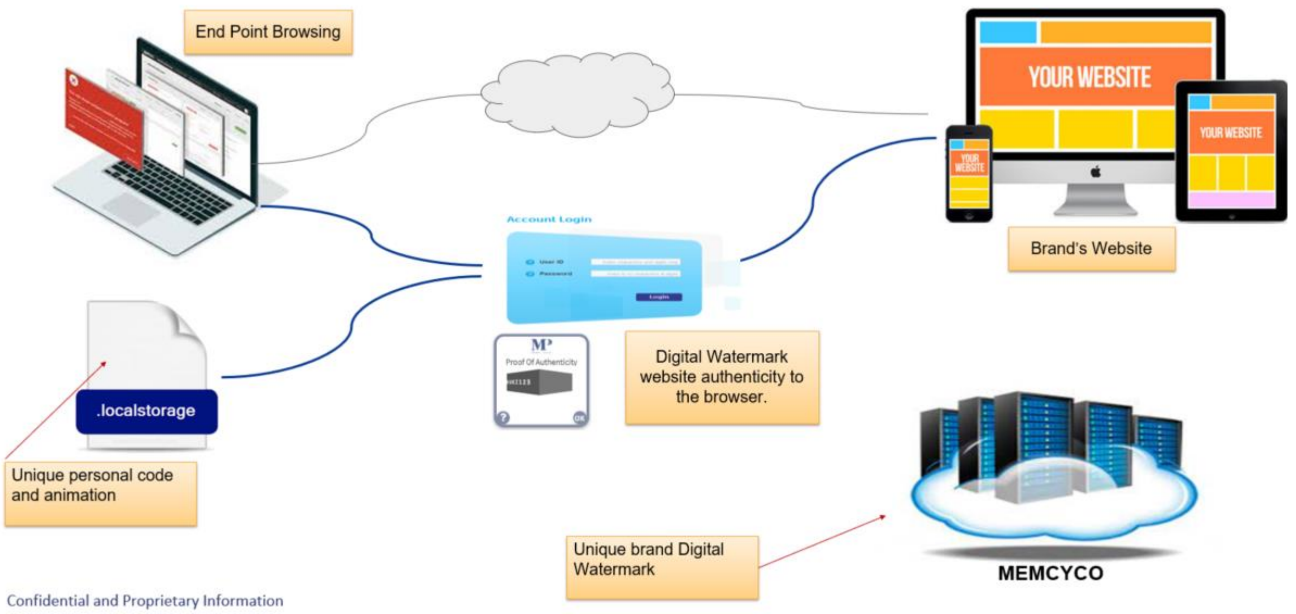
CLOX - Confidential Loader and Executer

SIEM Integration

Real-Time Dashboard

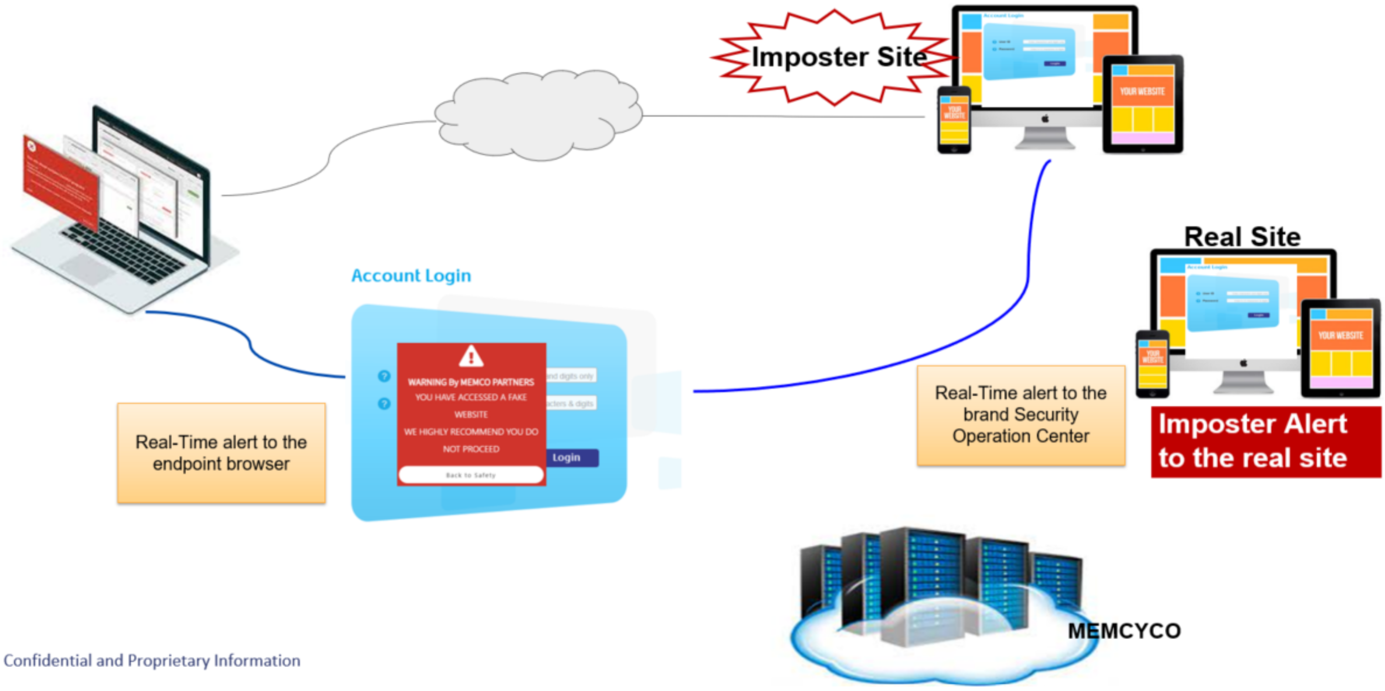
How it works:

WEB DIGITAL WATERMARK



Confidential and Proprietary Information

IMPOSTER SITE DETECTION & ALERT


Imposter Site
YOUR WEBSITE
Real Site
Account Login
WARNING By MEMCO PARTNERS
YOU HAVE ACCESSED A FAKE WEBSITE
WE HIGHLY RECOMMEND YOU DO NOT PROCEED
Back to Safety
Login
Real-Time alert to the endpoint browser
Real-Time alert to the brand Security Operation Center
Imposter Alert to the real site
MEMCYCO

Confidential and Proprietary Information

For Emails and SMS

Similar to website protection, the solution integrates with bulk email and SMS distribution systems to provide a sign of authenticity to brand communications. The solution allows:

- Seamlessly adding a unique secret code for each user, included with email content
- API integration with Mail merge servers/SaaS mail
- Users can set the watermark secret via a self-service interface

Deployment

Installation of PoSA™ requires inserting one line of JS code into the site HTML file.

After installation, MEMCYCO automatically enters "detection mode" which enables real-time detection alerts and real-time and historical reports. This allows the administrator to immediately receive alerts and automatically map out the user devices, and user identifications. The PoSA™ watermark can be activated gradually, allowing the organizations to provide proof of authenticity to end-users at their discretion. Using a provided educational template, the organization informs users of the introduction of the PoSA™ watermark and how to leverage it to ensure they do not fall for scams.

Conclusion and Benefits

MEMCYCO’s Proof of Source Authenticity (PoSA™) solution is a paradigm shift in digital authentication. MEMCYCO allows brands to protect themselves and their users from brand exploits using a unique per-user watermark that authenticates websites and emails and cannot be forged and point of impact technology that keeps users from entering impostor traps and informs the organization of the specifics and magnitude of attacks.

The unique benefits of this approach include

- Immediate protection after installation
- Protects users from falling into the attacker’s traps - customers who arrive at phishing / counterfeit sites can immediately see they’re not in the right place
- Increases trust in all brand communication - improves online communication effectiveness for emails, SMS, and website interactions
- Enable security teams to stop attacks immediately (spoofing, cloning, iFrame and clickjacking) with automatic alerts
- Enables the organizations to understand the magnitude of attacks in order to prioritize their actions
- Eliminates the damage that would have been caused by the impostor attack
- Minimal effort to install, deploy and maintain, requiring no professional services
- Zero user effort - just watch for the PoSA™ watermark
- Reduces user education costs

Appendix

PoSA™ - Proof of Source Authenticity

Attack scenarios and alerts

- **Website Spoofing / Cloning / iFraming / ClickJacking**
    - **Attack scenario** - An imposter site is being created based on cloning, spoofing, or iFrame technique on a targeted website.
    - **Detection and Alert** - A website with a different or similar *domain name* has tried to execute the code of the protected website where the *domain name* is not listed as one of the Allowed-Domains in the settings of PoSA™. This event will trigger an alert in the PoSA™ admin dashboard and to the SIEM of the organization SOC. At the same time, it will trigger a red-alert to the victim who has been exposed to the imposter page.

- Credentials Stuffing
    - **Attack Scenario** - The user is suspected to own a list of many user/password combinations. The user has entered more than (X=6, definable by the admin) different user/password combinations in a short period of time (T=10 minutes definable by the admin).
    - **Detection and Alert** - This event will trigger an alert in the PoSA™ admin dashboard and to the SIEM of the organization SOC.

- **Low Reputation Referral**
    - **Attack Scenario -** For cases where phishing attacks are carried out with a primitive HTML form asking the user for her credit card or user/password (without cloning or spoofing anything from the authentic website). Once the attackers have phished the information, they will (in most cases) make a referral (redirect) of the end user to the original website so that no suspicion gets triggered. In such cases, PoSA™ with the help of an AI-equipped engine investigates the referring domain through the following checks:
        - The domain was recently registered
        - Domain has no SSL certificate or low reputation SSL certificate.
        - Domain has a low backlinks footprint (i.e. small number of backlinks pointing back to it)
        - A domain is added to the deny list by other tools
        - Domain has very low traffic
        - Domain uses images similar to the authentic logo

- **Detection and Alert** - This event will trigger an alert in the PoSA™ admin dashboard and to the SIEM of the organization SOC. Also, can issue an alert to the end-user exposed.

- **Unknown Devices**
  - **Attack Scenario** - A user has signed in from a station he/she has never used before.
  - **Detection and Alert** - This will trigger a notification message to the end-user.

- **Password Brute Force**
  - **Attack Scenario** - A user has tried many different passwords (6, definable by the admin) in a short period of time (5 minutes).
  - **Detection and Alert** - This event will trigger an alert in the PoSA™ admin dashboard and to the SIEM of the organization SOC.

- Abnormal User Behavior
  - **Attack Scenario** - PoSA™ is configured to collect user behavioral profiles and a user has demonstrated abnormal behavior such as login-in from a country he never was in before or in a time of day he never used before, etc.
  - **Detection and Alert** - This event will trigger an alert in the PoSA™ admin dashboard and to the SIEM of the organization SOC.

- Website Reconnaissance
  - **Attack Scenario -** The user is excessively using browser dev tools (more than 90 seconds) or using a browser extension that is known to do reverse engineering or trying to directly download the source code of PoSA™ outside of any referral domain or has set a debugger breakpoint, or is trying to directly issue AJAX calls outside of any referral domain. (Website legitimate developers should be allowed in the settings of the product and so are the IP ranges of the development lab.)
  - **Detection and Alert** - This event will trigger an alert in the PoSA™ admin dashboard and to the SIEM of the organization SOC.

- **Unauthorized Domain**
  - **Attack Scenario -** While spoofing the website, the attacker has set a debugger breakpoint (or disconnect the cable) after the initial load of the website/page to avoid his discovery.
  - **Detection and Alert** - This event will trigger an alert in the PoSA™ admin dashboard and to the SIEM of the organization SOC.

- Code Injection Attempts
  - **Attack Scenario -** Cross-Site-Scripting is triggered when a user is attempting to fill in fields of an HTML form with content that is most likely targeted to inject executable code into another tab of the attacked site.

  - **Detection and Alert** - This event will trigger an alert in the PoSA™ admin dashboard and to the SIEM of the organization SOC.

- **Content Modifications**
  - **Attack Scenario --** PoSA™ can be configured to observe certain sensitive HTML elements and detect client-side modifications of these elements. For example, a user locally changes his account balance. The log record is triggered when a user did change the value of an observed element and displays the old and the new value after modification.
  - **Detection and Alert** - This event will trigger an alert in the PoSA™ admin dashboard and to the SIEM of the organization SOC.

- **Impossible Travel**
  - **Attack Scenario** - Someone has logged in with the user credentials from a location that is too distant from the last location the user has logged in from. Perhaps the user has given away his password to someone else.
  - **Detection and Alert** - This event will trigger an alert to the PoSA™ Admin dashboard and to the SIEM of the organization.

A few real-life examples of attacks that PoSA™ would protect against:

https://www.bleepingcomputer.com/news/security/microsoft-365-phishing-attacks-impersonate-us-govt-agencies/

https://www.mckinsey.com/careers/interviewing/getting-ready-for-your-interviews

https://www.tripwire.com/state-of-security/featured/10000-organisations-targeted-by-phishing-attack-that-bypasses-multi-factor-authentication