MEMCYCO

Authenticity Goes Both Ways

How to protect your brand and customers against impostors using Proof of Source Authenticity (PoSA)

A White Paper

Table of contents

Introduction

Since the creation of the internet, businesses have been focused on authenticating their users to ensure they are indeed communicating and transacting with who they need to. Many solutions have been introduced and implemented in order to 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 users authenticate companies' digital presence and communications? Until recent years the customers were usually safe in assuming the web page they are visiting is indeed authentic. But with the explosive rise in cyber attacks, specifically the booming ״phishing racket”, customers are fast becoming wary of engaging with emails and other messages and are held back in many cases from transacting online as 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 their accounts are taken over or their identities stolen, their money taken and more .

While it has become imperative for brands to take notice of this trend, currently the only real effort to address the question of website authenticity is the website’s certificate, shown as the little lock in the browser next to the URL, which is almost invisible to the human eye. Even worse, the certificate provides no real proof that the user is communicating with the correct and legitimate website. And since customers do not accept the “lock”as a trusted indicator - companies are left with the only available measure of damage containment - educating their customers to be suspicious on the web and scanning for impostor sites and working to take them down when they are discovered.

The lack of a visible Proof of Source Authenticity (PoSA) on websites and emails leaves the door wide open for hackers to impersonate legitimate sites through methods such as spoofing, cloning or re-engineering of the target. Hackers use these methods mainly to launch Phishing campaigns, but also for good old-fashioned crimes such as stealing innocent user data or selling counterfeit goods. In 2016, phishing leapfrogged malware to become the leading type of internet crime. Prior to that year, there were two malware sites per phishing site. In 2022, there will be nearly 75 phishing websites per one malware site.

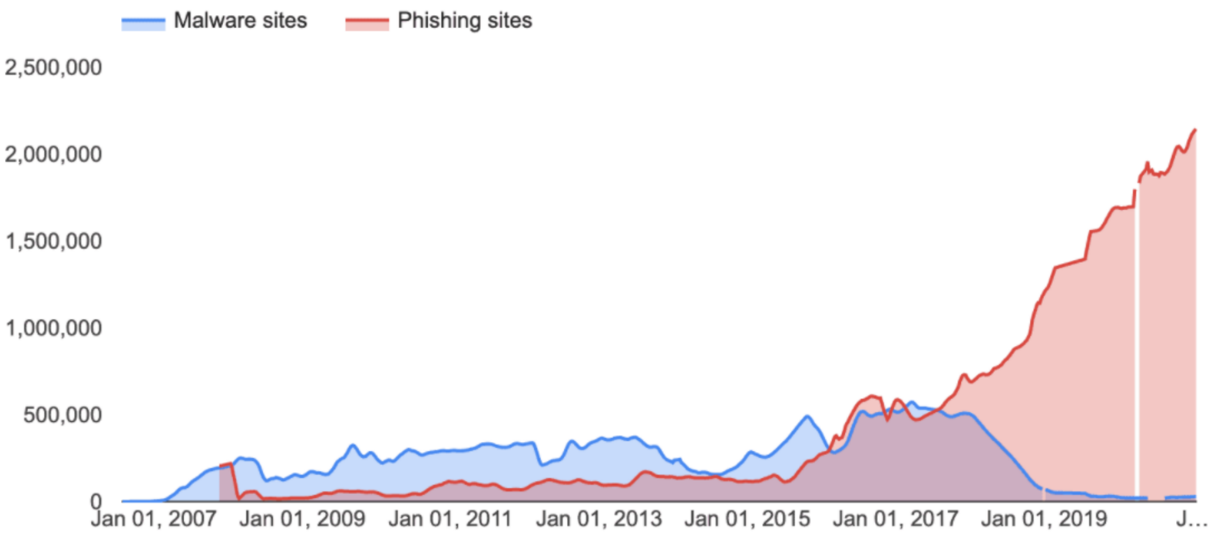
Another factor that must now be considered is the use of remote and online web services, which has risen dramatically due to the COVID19 pandemic and is increasingly here to stay. This trend has increased the need for a higher level of all forms of cybersecurity.

It is now abundantly clear that there is a need to allow users to safely open emails, visit websites, and transact digitally - being clearly 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) are a type of cyber crime where an attacker imitates a genuine familiar website in order to trick a human victim into revealing sensitive information to the attacker, to falsely transact with them or to deploy malicious software on the victim's infrastructure.

As of 2021, phishing sites are by far the most common attack performed by cyber-criminals, with the FBI's Internet Crime Complaint Center recording over twice as many incidents of phishing than any other type of computer crime.



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

These attacks are on the rise : 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 just 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"[1].

What happens when scams succeed? IBM found that customers' personally identifiable information (PII) was the most commonly compromised type of data and the most costly. 80% of breached organizations reported a loss of customer PII in 2020.

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, and there do anything ranging from stealing their credentials, gaining access to account information, selling them counterfeit goods or scamming them into transferring money to criminals. These attacks occur 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 practice among the hackers' community. Toolkits that automate the process are easily available for criminals to use.

How is the market responding to these attacks? Employees as targets of such attacks are offered some protection via a variety of solutions that try to filter out attacks by scanning emails arriving at company-controlled emails 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 impostor and phishing sites - to allow the 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? Customers, partners, and other users of company online services might get an email every once in a while informing them of the risks relating to phishing campaigns, counterfeit sites, and scams. But educating users in this manner can only go so far. The

[1] https://states.aarp.org/georgia/half-of-u-s-adults-have-been-targeted-by-impostor-scams-says-aarp-survey

time has come for a proactive solution that would actually provide users with the kind of trust they need to be sure the emails they read and the sites they visit are legitimate.

Creating user trust in online sites and correspondence

Solution Overview

Memcyco has created a Proof of Source Authenticity (PoSA) solution to address the challenges listed above. It is designed to allow organizations to provide positive confirmation to their users that web pages they visit and messages they receive are authentic.

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 and visual elements that are unique to the specific user - much like a personal passphrase - that they can set themselves. PoSA applies to websites, emails, and SMS messages using very simple integration to the site/sender and no installation on the user’s devices. It also provides monitoring and visibility to actually attempted attacks.

Capabilities

For websites

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

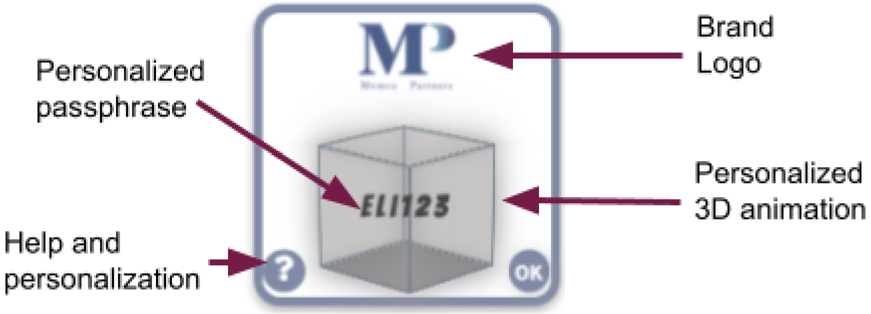


Fig 1- The Digital Watermark

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

The solution is capable of running in “silent mode”, without activating the watermark. At silent mode phase, the solution will also monitor activity at the user endpoints on the site and will alert on attempted attacks, including alerts when users visit most kinds of impostor sites. In such cases, the end users will see a red alert appearing on their screens.

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

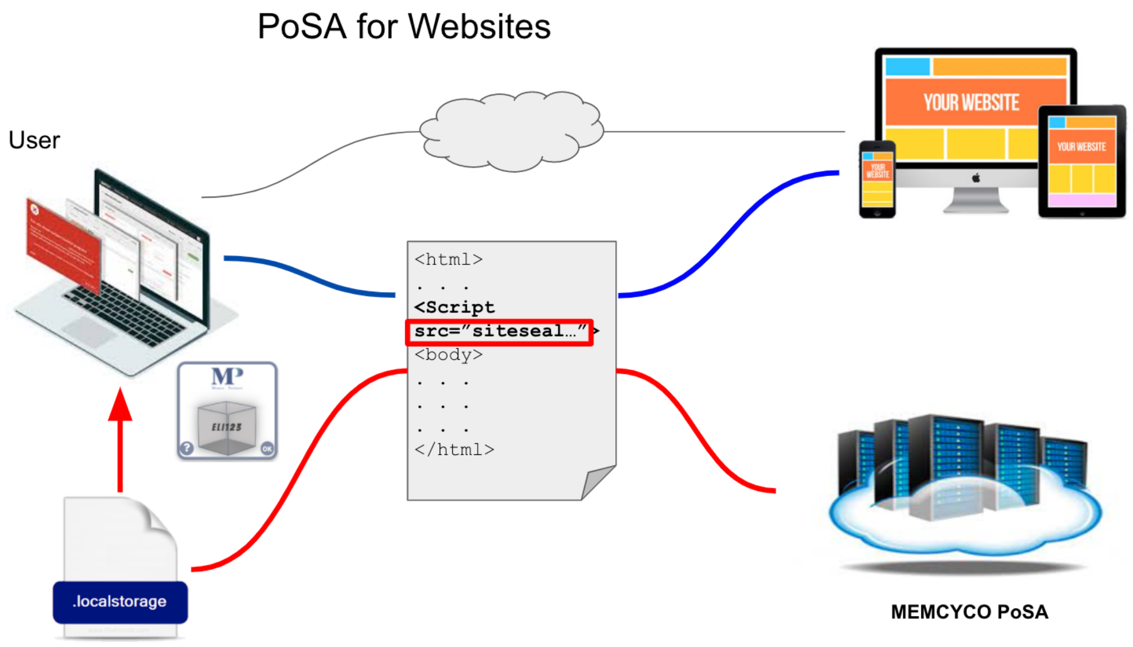
- Cross-domain watermark consistency - allowing users to see the same personal passphrase in their watermark across the websites of multiple providers they work with
- Smart syncing across user registered devices (PC, Tablet, Mobile), after receiving user consent

The product also alerts security teams to:

- Spoofing/Cloning attempts
- Reverse-Engineering attempts - whenever a user attempts to open developer-tools on the website code
- Attempts to sign in from a previously unknown device
- Repeated frequent login attempts

And offers them key capabilities such as:

- Hide all client-code/logic from the eye of the user by encrypting it.
- User behavior integration with Google Analytics events sent on any user interaction with the product.
- Central management including operation in silent mode and gradual deployment to users



```
<html>
. . .
<Script
src="siteseal…">
<body>
. . .
. . .
. . .
</html>
```

Fig 2. - How it works

For emails and SMS

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

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

Deployment

In order to install the Memcyco PoSA solution, the organization is required to insert one single line of JS code to the site HTML file or configure the email/SMS service integration.

After installation, Memcyco automatically enters "silent mode" to allow the administrator to map out the desired user devices, and to generate user identifications. This is done to support the gradual deployment of the watermark. Using a provided educational template the organization informs users of the introduction of the 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 provides brands the ability to protect themselves and their users from brand exploits using a unique per-user watermark that authenticates websites and emails and cannot be forged.

The advantages of this approach include:

- Protects users from falling into the attacker's traps - customers who arrive at phishing / counterfeit sites can 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, and iFrame) with automatic alerts
- Minimal effort to install, deploy and maintain
- Zero user effort - just watch for the watermark
- Reduces user education efforts