Cyberint

Argos™ Phishing Beacon

Identify Emerging Threats, Before They Damage Your Brand

HERE TO STAY: PHISHING & BRAND-ABUSE THREATS

AN AVERAGE OF 200,000 NEW PHISHING SITES ARE CREATED EACH MONTH – THAT'S ALMOST QUADRUPLED OVER THE LAST YEAR

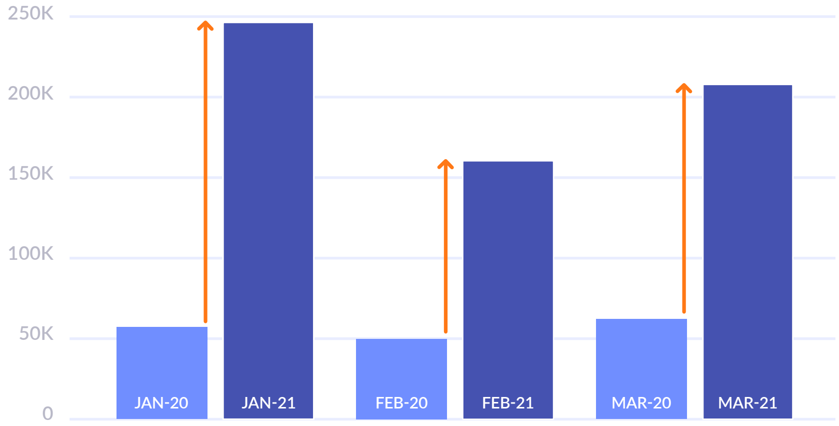


Figure 1: Phishing Sites Q1 2020 vs Q1 2021
(APWG Phishing Activity Trends Report Q1 2021)

Year-on-year, phishing attacks are becoming more sophisticated, and more targeted. Gone are the days where attackers cast a wide net, hoping that if they targeted enough businesses, a substantial number of users would take the bait. Today, threat actors spend months planning their attacks, and launch phishing scams that target a specific organization directly, including both customers and employees. By impersonating the organization's website (e.g. its login page), threat actors are seeing a growing amount of success from phishing techniques, successfully stealing credentials or sensitive data, and using this for financial gain, or to establish a foothold inside your organizational ecosystem.

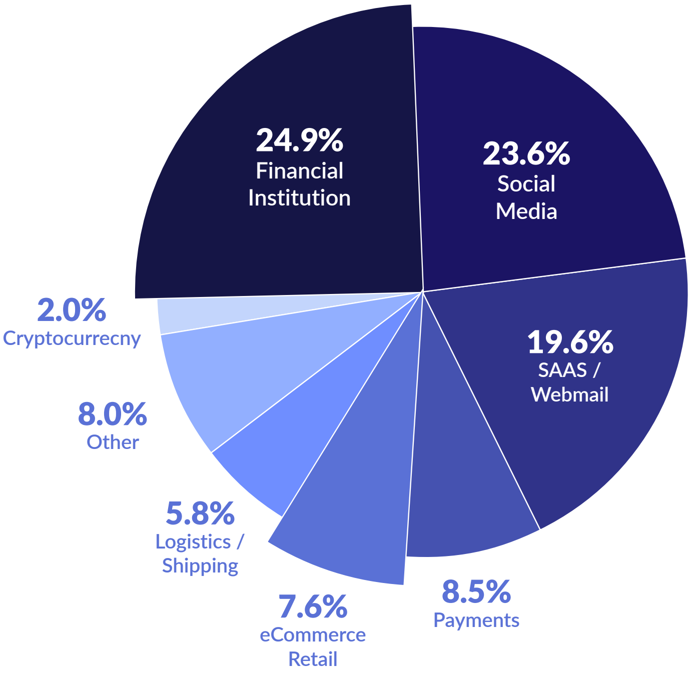


Figure 2: Most targeted industry sectors, Q1 2021
(taken from APWG Phishing Activity Trends Report Q1 2021)

The potential damage of a successful phishing attack to an organization is huge, influencing security operations, brand reputation, and both data privacy and compliance. In fact, the average cost of a phishing attack to a mid-size company is 1.6 million dollars, while for larger companies, this cost increases to 14.8 million dollars[1]. As shown in figure 2, these threats span any and all industries.

[1] https://www.scmagazine.com/news/phishing/study-phishing-scams-cost-large-us-companies-about-15-million-a-year

HOW ARE THE ATTACKERS LAUNCHING PHISHING SCAMS?

To understand how to address this threat, organizations need to get into the mind of today's threat actors, and see how easy it is to launch phishing websites and evade detection. Here are some of the top methods the attackers use, and how traditional cybersecurity solutions alone, fail to measure up.

PHISHING-AS-A-SERVICE

In many cases phishing sites target an organization are the result of a "phishing kit" execution. A phishing kit is a collection of software tools that makes it easier for people with little or no technical skills to launch a phishing exploit. This type of crimeware is sold for as little as $50 on the Dark Web, and can be launched in hours, leaving very little time for digital risk platforms to locate the threat before your brand is already under attack.

REGISTERING FALSE DOMAINS

Every phishing website needs to be registered, and so scanning newly registered domains, or domains with new certificates, can help to reduce the amount of successful phishing websites that go live. However, intelligent attackers have found workarounds, including hosting the malicious website on a subdomain of a valid website that has no connection to the brand under attack. In these cases, organizations may not realize that there is a malicious website mimicking their own, until their customers report identity theft or until a data breach is uncovered. By this point of course, it's too late.

CLONING WEB PAGES

In the majority of cases, the approach of the attacker is to copy the HTML code of the target website and create a malicious clone. In fact, Cyberint's Data Science Team have discovered that at least 66% of phishing sites that put our customers at risk, are actually 1:1 clones of legitimate login pages. Unfortunately, traditional cybersecurity solutions are ill-equipped to manage this threat. Some may provide a web-browser plugin, to detect active live phishing URLs. However, many cloned content pages won't have malicious attributes to pick up on. Even where they do – by the time a browser plugin picks it up, the threat is already in the wild, and your organization won't know how much damage has already been done.

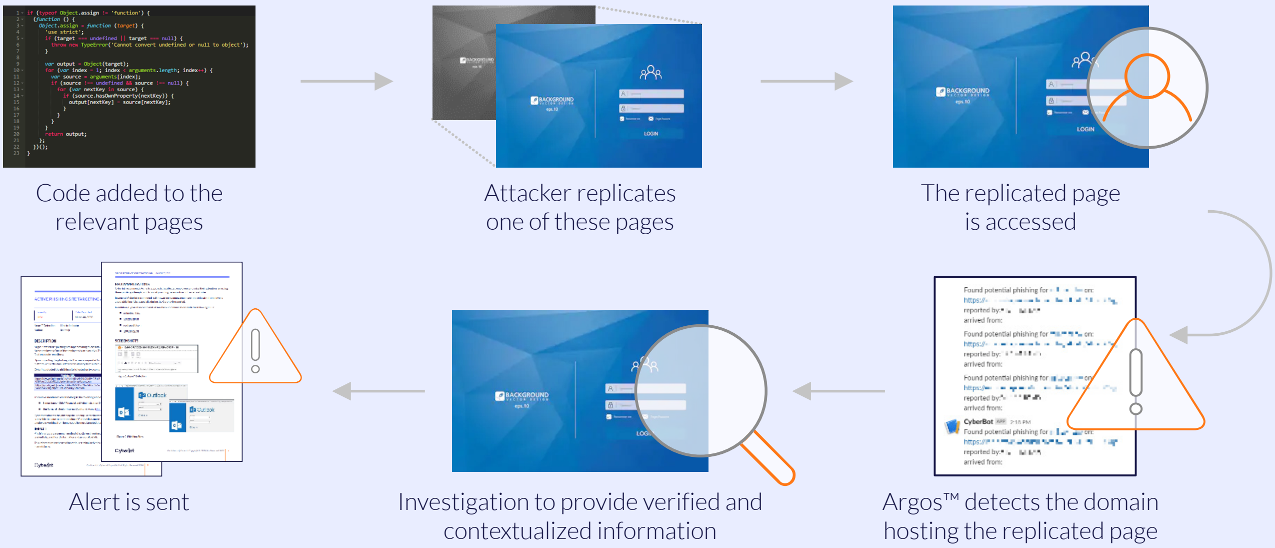
THE BOTTOM LINE? TRADITIONAL CYBERSECURITY SOLUTIONS OFFER PARTIAL DETECTION, OR LATE MITIGATION, AND THAT'S JUST NOT GOOD ENOUGH FOR THE SCALE OF TODAY'S THREAT.

CYBERINT'S PHISHING BEACON – AUGMENTING PHISHING DETECTION FOR DIGITAL BUSINESSES

Cyberint's Phishing Beacon takes a proactive approach. Our goal is to detect the phishing site before it has any effect. We do this by adding an obfuscated script to your organization's original website, on top of ensuring that we are best-in-class at the traditional anti-phishing defenses listed above. This code is extremely lightweight, and so it doesn't interfere with the regular operation of the website, and of course, is invisible to any user. However, once the site's code is cloned by an attacker to serve the creation of a phishing site, the Phishing Beacon identifies that it is being run on an invalid hosting domain. This automatically generates an alert, notifying the organization of the malicious intent, and enabling quick mitigation before the phishing website is launched.

HOW IT WORKS

1. **Add the Phishing Beacon code to vulnerable web pages –** The customer adds a single line of code provided by Cyberint to the web pages it wishes to protect.
2. **Threat Actor clones the page –** The threat actor clones the web page for malicious intent (I.e. phishing or brand abuse as part of a one-time activity or to add to a phishing kit).
3. **The cloned page is rendered for the 1st time –** The 1st time the cloned page is rendered (typically by the attacker testing the new phishing site) the Phishing Beacon is activated, automatically alerting Cyberint.
4. **Alert is generated –** Cyberint's analyst team investigates the page. If determined that the cloned page is a malicious phishing page, an alert is sent to the customer.
5. **Phishing site takedown –** Upon request from the customer, Cyberint contacts the hosting provider or registrar to take down the infringing content under DMCA law.



```
if (typeof Object.assign != 'function') {
  (function () {
    Object.assign = function (target) {
      'use strict';
      if (target === undefined || target === null) {
        throw new TypeError('Cannot convert undefined or null to object');
      }

      var output = Object(target);
      for (var index = 1; index < arguments.length; index++) {
        var source = arguments[index];
        if (source !== undefined && source !== null) {
          for (var nextKey in source) {
            if (source.hasOwnProperty(nextKey)) {
              output[nextKey] = source[nextKey];
            }
          }
        }
      }
      return output;
    };
  })();
}
```

Code added to the relevant pages

Attacker replicates one of these pages

The replicated page is accessed

Argos™ detects the domain hosting the replicated page

Investigation to provide verified and contextualized information

Alert is sent

Figure 3: Phishing Beacon - Advanced Phishing Detection for Digital Businesses

CASE STUDY: 4X AS MANY PHISHING SITES UNCOVERED USING PHISHING BEACON

THE CHALLENGE

This major digital media company in North America experienced constant cloning of their content pages. As the nature of its business as a media company is to promote content, the impact of cloned sites on their business and on their brand reputation, is high. The cloned pages siphon traffic that was intended for the company's legitimate web pages towards content promoted by the attackers. These pages abuse the company's brand, and in the worst-case, steal sensitive data from end-users.
Prior to implementing the Phishing Beacon, the organization was responding reactively to phishing websites, two steps behind the attackers, waiting for a live threat to come to their attention before they could act.

THE SOLUTION

By implementing the Phishing Beacon effectively, through a single line of code on its website, this digital media company heavily reduced the impact of cloned websites on their business and brand. This capability enabled Cyberint to detect, and take down phishing and brand-abuse websites on the customer's behalf intelligently, proactively and much faster.

BY THE NUMBERS

5 Months

The amount of time it took to get phishing websites completely under control

More than 400%

The increase in detected URLs related to the customer

62%

The increase in attacks detected by the Phishing Beacon, over traditional security methods

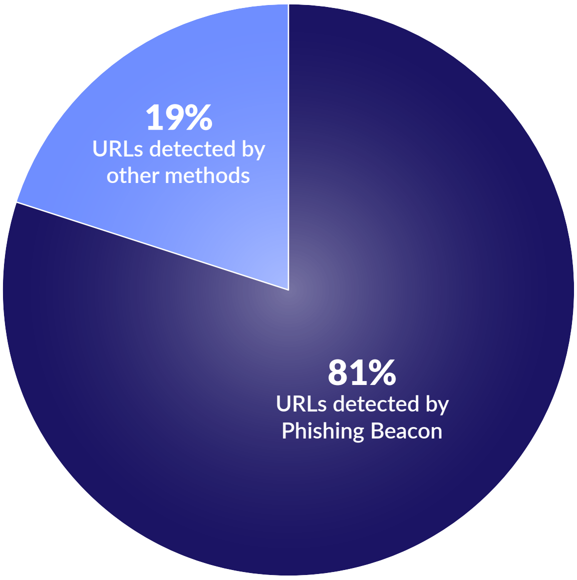


Figure 4:
Phishing & Brand Abuse URLs - Detection Methods

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA
368 9th Ave, Suite 09-123
New York, NY 10001
Tel: +1-646-568-7813

ISRAEL
17 Ha-Mefalsim St.
4951447 Petah Tikva
Tel: +972-3-7286-777

UNITED KINGDOM
14 Grays Inn Rd., Holborn
WC1X 8HN, London
Tel: +44-203-514-1515

SINGAPORE
135 Cecil St. #10-01 MYP
PLAZA 069536
Tel: +65-3163-5760

FRANCE
67 Avenue de Wagram
75008 Paris
+33 1 77 50 58 91

Cyberint