Cyberint

The Phishing Protection Handbook

The purpose of this eBook is to provide valuable insight into the emergence of phishing attacks and the steps taken by threat actors to set up and launch a successful phishing attack.

More importantly, these observations are intended to help determine what layers of protection are needed in order to maximize the efficiency of a phishing protection suite, and the return on security investment.

CONTENTS

OVERVIEW

Phishing is still one of the top 3 successful attack vectors.
The reason for its success is twofold:
A. It could be relatively simple for a novice threat actor to set up a phishing campaign
B. It's designed to trick your brain to trust it - which can be achieved fairly easily, especially in the hectic digital life we are living.

THE GOAL OF A PHISHING CAMPAIGN IS USUALLY ONE OF THREE:

COLLECT DATA

such as fresh credentials, credit card number, bank account details that can be used in a future attack.

FRAUDULENTLY

get the victim to process payment (for example tax for newly coming package)

DOWNLOAD

a malicious payload (malware) to his\herdevice: allowing the threat actor to continue further steps with this payload.

Whatever the goal of a threat actor, every campaign requires setting up a legitimate-looking page, to trick the victim into taking the desired action.
In many cases, these campaigns rely on a combination of elements:

The email looks legitimate

as it resembles something the reader would recognize from the past, or includes details that only a legitimate sender would have.

Evokes a sense of urgency

in order to lower the defenses of the reader with immediate actions required for immediate gain.

No alarms have been set

by the recipient organization security system. As users want to believe that the security system will detect all phishing emails.

ANATOMY OF A PHISHING CAMPAIGN

CHOOSING A TARGET

Phishing campaigns can be launched against any organization, but usually targets can be categorized as follows:

with the final goal of gaining access to user accounts and transfer funds into their own.

either to conduct fraud, such as using one person's payment details in order to place an order for someone else, or to collect personal information including payment method and details.

to collect employee credentials which would then be used for further information collection and launch ransomware attacks.

Whereas financial and e-commerce attacks require a perfect clone of a company's web page, targeting enterprise organizations requires different assets:

A login page of a 3rd Party application

used by the enterprise –such as office 365, Salesforce, SAP, etc. In these cases the phishing will be used to collect fresh credentials including the ability to overcome multi-factor authentication (MFA) techniques.

A web page

usually an email sending setup that resembles a supplier, customer or business partner organization – supporting an operation with the goal to conduct fraud, for example by changing bank account details of a supplier and receiving intended payments.

PHISHING CAMPAIGN PREPARATIONS

Once a target has been selected the threat actors need to build their email list and set up the infrastructure:

Make or buy

The threat actors that go through the trouble of setting up their own infrastructure and develop a perfect clone of the target organization web page, or buy from a specialized threat actor which sells phishing kits for a living. Phishing kit-building is a thriving business with specialized tech-savvy actors who invest a lot of effort to create out-of-the-box phishing kits that could be utilized hundreds of times by the same actor in different places or by different actors. These actors must stay on top of the defenders and continuously improve the phishing kit to bypass new security controls.

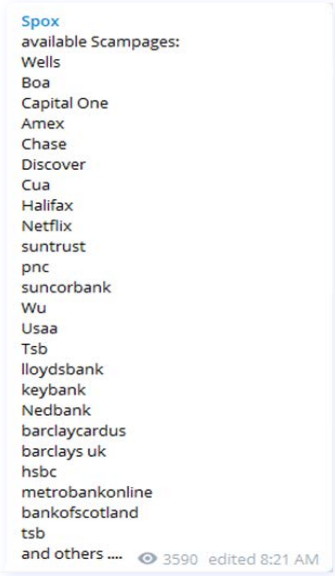

Figure 1: Example of a threat actor named SPOX which offers phishing kits for different banks

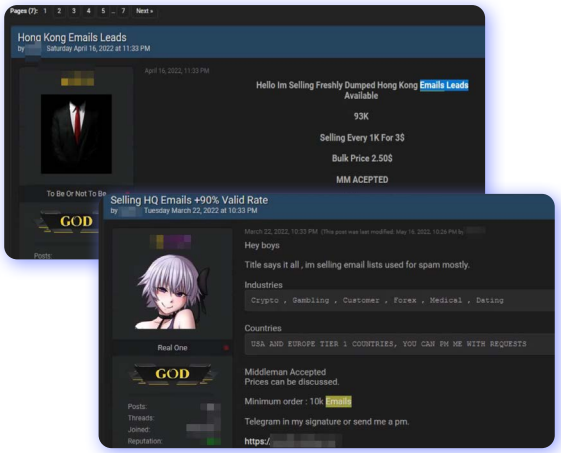

Figure 2: An email list for sale on the darknet

Create the email list

Once a phishing site is ready, the operator would need to send phishing emails to the potential victims. In order to achieve high efficiency and reduce risk of being detected and blocked, the threat actor must use an accurate list that is relevant to the phishing campaign. For instance, there is no value in sending a link to a fake bank login page to someone who is not a customer of that bank. Similarly, there is no point sending malicious business emails (for example with the organization logo) to users who are not part of that business. A common shortcut in this labor-intensive stage is purchasing email lists, either from legitimate companies who collect data for marketing purposes, or utilize the billions of email addresses being leaked from countless attacks which result in data leakage.

Campaign Setup

Once the target is chosen and the threat actor has been built (or bought) and the target organization web pages cloned, it needs to go into the stage of setting up the campaign.

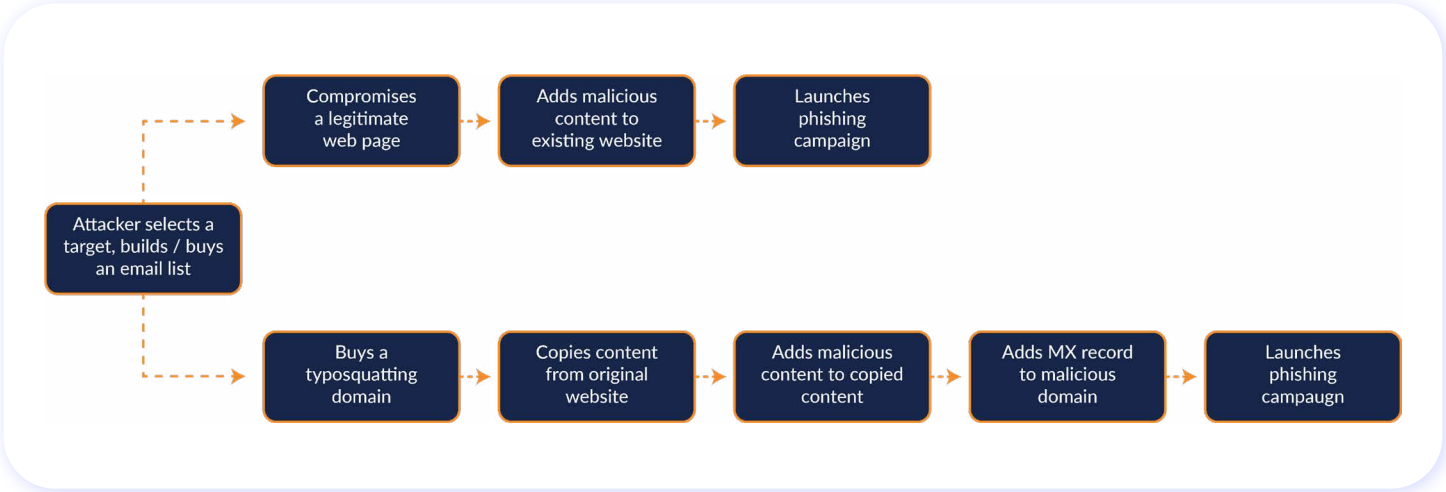

Figure 3: Typical processes employed by actors to execute a phishing campaign

The following description is a simplified illustration of the steps actors take to execute a phishing campaign. In broad strokes, phishing campaigns observed are mostly executed in one of two ways. Either compromising a legitimate website and adding malicious content to newly created pages, or by purchasing a new domain similar to the legitimate source via a method called 'typosquatting' domain, www.amz0n.com or www.microfost.com for example, copy legitimate-looking content that includes the information collection or payload distribution.

Scenario 1
SETTING UP A NEW PHISHING SITE

Scenario 2
USING AN EXISTING LEGITIMATE WEBSITE

PHISHING AS A SERVICE

SCENARIO 1 – SETTING UP A NEW PHISHING SITE

In this scenario the threat actor sets up its own infrastructure. This includes these steps:

1. Attacker selects a target

2. Attacker purchases a domain

that would be used for the phishing infrastructure. For high efficiency, threat actors usually select a domain which resembles the target organization's main domain, or includes its name. This is done either by creatively searching for a domain permutation or using automated permutation engines to get names and purchase the domain. This is generally referred to as the 'typosquatting domain'.

3. Attacker populates content

that resembles the original website – Text, CSS, logo, and any other element that would help to trick the victims into believing they are on a legitimate page. This could be done by their own development or by using a phishing kit available for purchase on the deep and dark web.

4. Attacker adds the malicious content

to the page after creating the appearance of a legitimate page. This could include a credential harvesting tool or a login box in a credential collection campaign, or by other means, such as dropping the malicious payload into the victim's machine.

5. Attacker sets up email sending infrastructure

In many cases the domain will be used to send emails from. This technically requires adding a 'mail exchange' (MX) record, the DNS records that will allow email servers to communicate with this email sender and verify that the email delivery will be successful.

6. Attacker launches the campaign

A carefully crafted phishing email using the names and addresses from the obtained email list is then being sent to the entire list.

Figure 4: In this scenario the threat actor sets up its own infrastructure

SCENARIO 2 – USING AN EXISTING LEGITIMATE WEBSITE

In this scenario, the attacker is not setting up a new infrastructure, but rather tries to leverage the credibility of an existing website that can be hacked, allowing them to add their own malicious content to it. Unfortunately, it is quite common to identify a non-patched or misconfigured WordPress website, which enables hackers to gain administrator access and add their malicious content unbeknownst to the owner and without disrupting the website operation.
This includes these steps:

1. Attacker selects a target

Either by buying a target or a combo list. A combo list is a text file containing a list of usernames, email addresses and passwords. Those lists are curated by cybercriminals over data breaches or other security incidents then sold or leaked on the dark web so cybercriminals could use them to commit identity theft or other crimes.

2. Attacker adds content to an existing website

whether through a phishing exploit kit bought on the deep and dark web or, if they are more advanced, through cross-site scripting (XSS).

3. Attacker launches the campaign

A carefully crafted phishing email using the names and addresses from the list is then being blasted to the entire list.

Figure 5: In this scenario the threat actor compromises legitimate infrastructure.

PHISHING AS A SERVICE

A method that is quickly gaining popularity is Phishing-as-a-service (PHAAS). As cybercrime going through commercialization and digital transformation, phishing has been commoditized – there's a whole eco-system where some threat actors have become service providers to other threat actors, offering a range of phishing related products and services in exchange for payment.

To perform a successful attack, an attacker should deploy an up-to-date interface with reliable infrastructure, those requirements are not an easy task to maintain daily, the service providers offer their own products, designed to help with the continuation of the attack. Another reason for purchasing the service is that a threat actor needs an infrastructure that might be deployed for a one-time use.

The PHAAS service provides all of the above. It even might include additional features such as MFA bypass. The threat actor purchasing the service will be required to specify the target list and choose the workflow they would like to activate. This allows threat actors launch ophisticated campaigns along high authenticity, increasing their chances to successfully lure their targets into the trap.

CYBERINT'S END-TO-END PHISHING PROTECTION

In order to maximize protection against phishing attacks, Cyberint's Argos is designed to cover each and every step in both of the attack scenarios illustrated above. Argos' algorithm combines automatic generation of domain permutations with open source and advanced DNS intelligence to predict in high confidence, an imminent phishing attack. Together with the phishing beacon, which proactively protects against phishing hosted on domains that aren't flagged as suspicious, Cyberint is able to provide the broadest protection against phishing attacks.

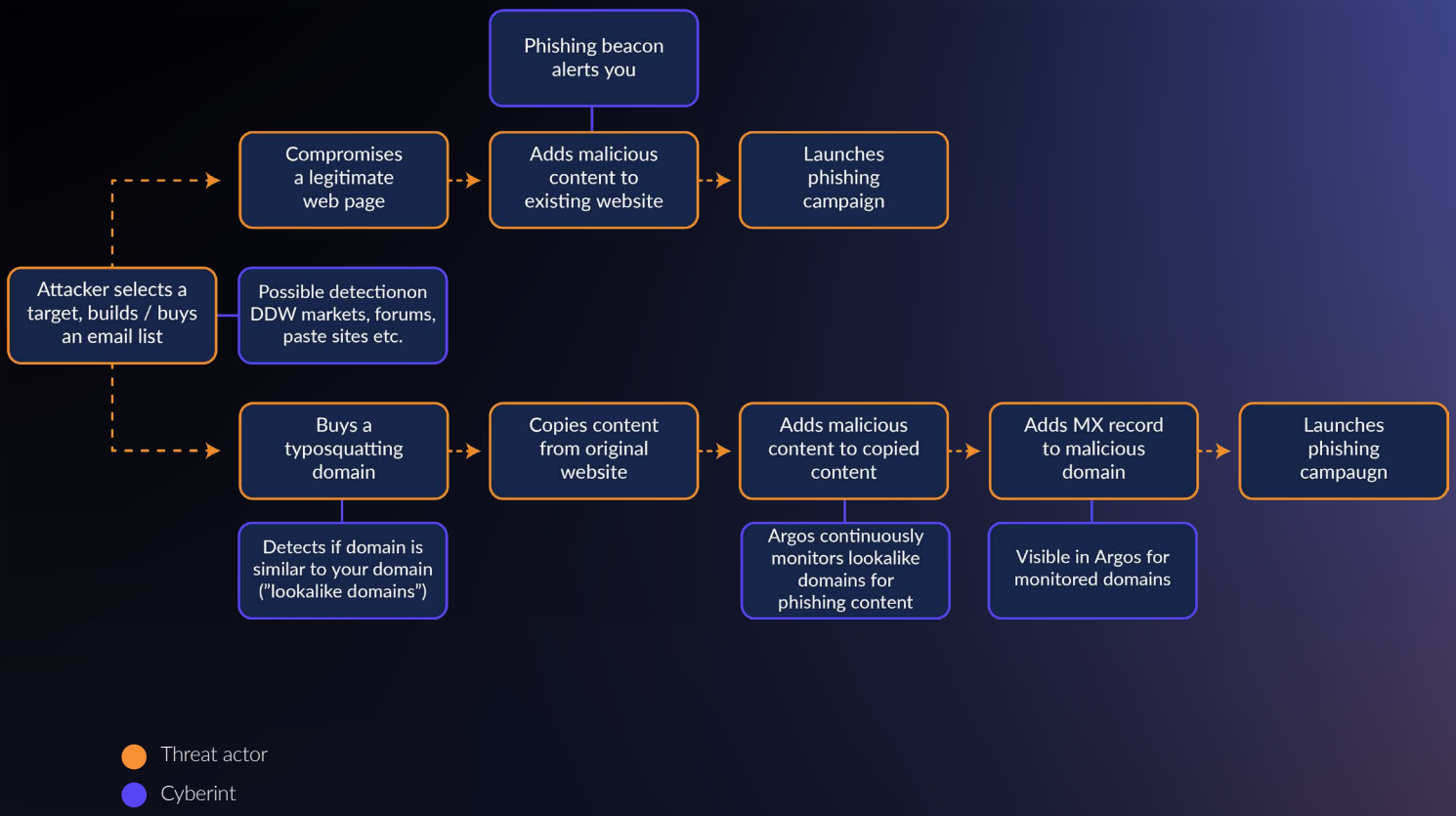

Figure 6: How Cyberint prevents phishing in every phase of the campaign

CAPABILITIES

Identifying typosquatting domains

Cyberint continuously monitors for similarities between your domains and the newly registered candidates to provide a level of indication of malicious intent, and alerts you of suspicious, newly registered lookalike domains.

Alerting on new phishing sites and dark web chatter

Mentions of your name, domain/s, logos, and digital assets within the website source code as well as the URL – all from a pool of external and proprietary sources that surface suspicious candidates.

Tracking leaked credentials, combo lists, and phishing kits in open, deep, and dark web sources including Virtual HUMINT activity

Cyberint's threat intelligence sources offer intelligence on the trends and phishing options in various deep and dark web markets. This includes detecting indicators from dark web sources, both for targeting a specific organization as well as the new phishing technologies, toolkits, and services offered. In addition, Cyberint's analysts interact with threat actors to stay on top of new phishing technologies, and Tactics, Techniques, and Procedures (TTPs).

Identifying spear phishing emails (from AV repositories)

As a spear phishing campaign emerges, some threat actors will test their emails against a company's Antivirus software. Cyberint collects emails flagged as phishing email, investigates further and notifies the relevant personnel in order to take the right actions to prevent further phishing attempts.

Phishing IOCs

As a phishing campaign emerges, there are specific IOCs that are expected: domain parking, creating a mail exchanger (MX) record to send phishing email, absence of DMARC records and more. Argos constantly monitors for those specific IOCs in order to determine whether or not a domain is malicious and a phishing campaign is emerging.

PHISHING BEACON:
CATCHING PHISHING AS EARLY AS IN STAGING PHASE

66% of phishing URLs are created by cloning the original page, typically the public facing login page of the organization, rendering traditional phishing prevention methods –typo-squat discovery methods, brand reconnaissance – irrelevant. Cyberint's groundbreaking, patented technology allows organizations to effectively detect this type of phishing campaign by injecting a small code ("the beacon") into their main web pages or public facing login pages. Once implemented and configured, the beacon alerts Cyberint if the page is copied and hosted on any other domain. The Phishing Beacon allows cybersecurity teams to know about an emerging campaign as early as the staging phase, where attackers test their page.

66%
of phishing URLs are created by cloning the original page

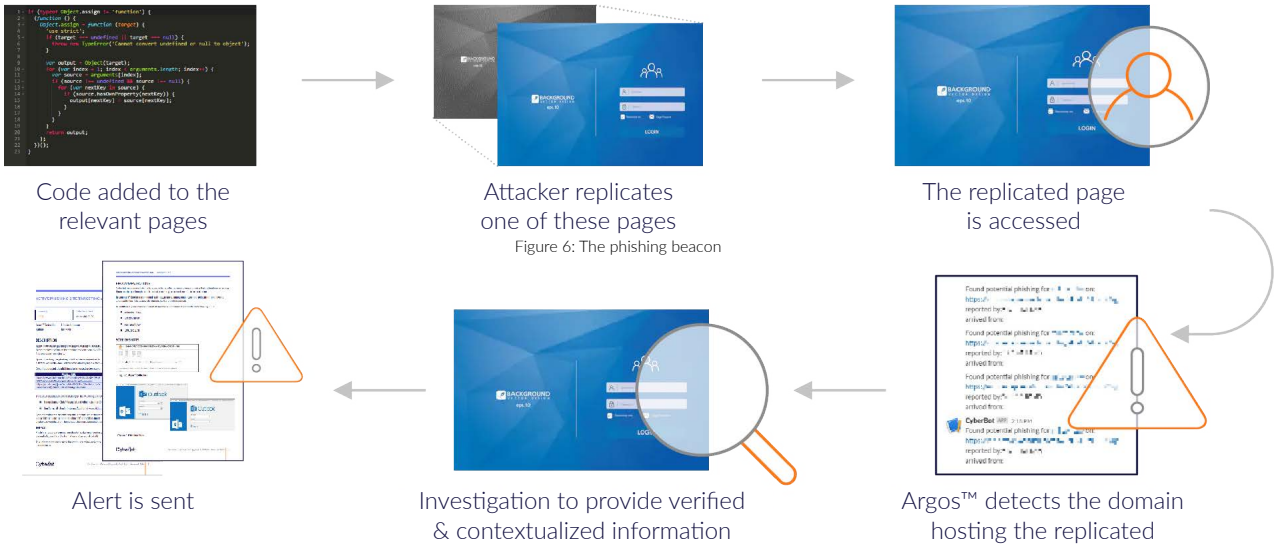

Figure 6: The phishing beacon

TAKEDOWNS

Upon detection of a malicious phishing site, Argos alerts and provides the option to initiate a takedown process that involves, as necessary, a notification to the relevant providers to remove misleading content, block domains, and update public blacklists.

Cyberint handles hundreds of takedown requests per week from various customers and can influence providers to act quickly.

Upon receiving the request for the removal of illegitimate content that is infringing the customers' trademark or used for malicious purposes.

SUMMARY

Cyberint's anti-phishing technologies have demonstrated dramatic results in pre-empting phishing attacks, better detecting the emergence of phishing campaigns, and accelerating mitigation or takedowns. Due to its impressive track-record in phishing takedowns, the company is recognized by governments CERTs and anti-phishing groups as a leader, resulting in an accelerated processing of its takedown requests - which leads to a significant reduction in Mean-Time-to-Remediate (MTTR).

ABOUT CYBERINT

Cyberint fuses threat intelligence with attack surface management, providing organizations with extensive integrated visibility into their external risk exposure. Leveraging autonomous discovery of all external-facing assets, coupled with open, deep and dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities and more, ensuring continuous external protection from cyber threats.

For more information visit www.cyberint.com

