SLASHNEXT

REPORT

Defending Against Zero-Hour Social Engineering Threats with Modern Threat Intelligence

OVERVIEW

Threat actors are going after the human attack surface with new kinds of phishing and social engineering techniques, tactics, and procedures. While credential stealing remains popular, new types of phishing and direct-to-browser attack vectors are evading existing multi-level security controls. The introduction of next-gen antivirus and other similar technologies are making it harder for bad actors to deliver malware successfully, so they have become more sophisticated in delivering phishing and social engineering attacks.

Threat intelligence that covers new types of phishing threats is essential for understanding and defending against previously unknown zero-hour threats.

In this report you'll learn about:

- How the phishing threat landscape has changed
- Techniques, tactics, and procedures for the new generation of evasive phishing threats
- What existing phishing threat intelligence feeds are missing
- What is required for modern phishing threat detection
- Benefits and use cases for real-time phishing threat intelligence

PHISHING OVERTAKES MALWARE

Since 2015 phishing sites have been growing, while malware sites have been decreasing to the point that phishing has taken over the threat landscape. Data sourced by Google from millions of Chrome users from 2009 to 2018, clearly demonstrates the overall threat landscape is shifting towards phishing (Exhibit 1).

Number of Unsafe Websites Detected Per Week

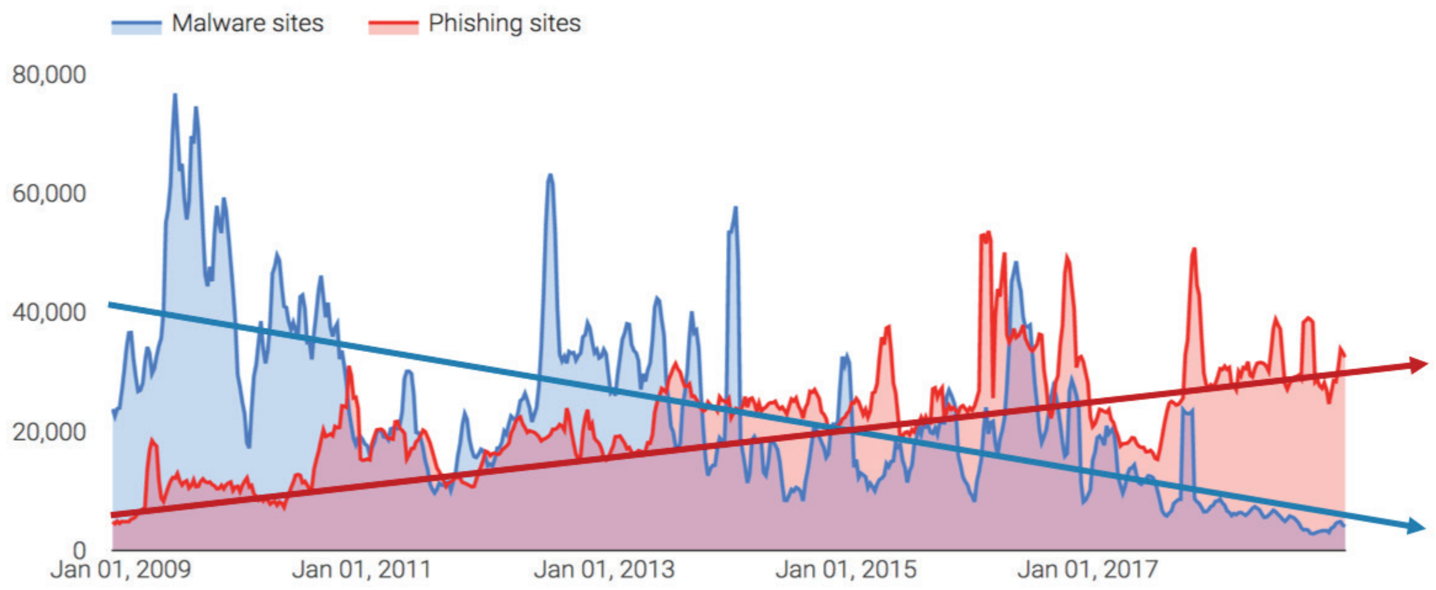


Exhibit 1: Chart indicating how the weekly number of unsafe malware sites has declined while unsafe phishing sites have increased over the last nine years.

Back in 2009, you can see that malware was a prominent attack vector for internet users. Phishing was present, but it was not the number one attack vector, and over the years there has been a transition from malware to phishing. Now malware is a minority player and phishing is favored because when it comes to infiltrating an organization's assets, personal data phishing has become the first choice for bad actors.

One of the main reasons for the reduction of malware over the years can be traced to the introduction of next-gen antivirus, commercial antivirus, sandboxing, EDR and other similar technologies that are making it a lot harder for the bad actors to deliver malware successfully.

With the knowledge that most antivirus and similar existing technologies are focused on malware, and not designed to catch phishing or social engineering attacks, bad actors have evolved. They have become more sophisticated in their approach, by targeting human nature and this is why there has been a rise in phishing.

At SlashNext, we see this trend across our networks as well. Three to four years ago, we were catching a lot more malware. During the last two years, 90% of the infections that we see across our customer base are predominantly phishing and social engineering attacks. The total number of phishing detections that Google now reports are approximately 30,000 - 40,000 per week. This trend is real, and it's happening right in front of our eyes.

BAD ACTORS HAVE REINVENTED THE PHISHING LANDSCAPE

Now that bad actors have shifted their tactics to phishing, another trend is happening at the same time -- they're reinventing the phishing landscape. The classical phishing paradigm was you'll get an email with a link to a fake log-in page. That's no longer the case—There are new attack vectors and phishing categories. Email phishing is still out there, but there are more attacks vector happening under the umbrella of phishing. Phishing has spread beyond email to social media, advertisements, search engines, browser extensions, chat apps and mobile (Exhibit 2).

Email Phishing Protection No Longer Enough

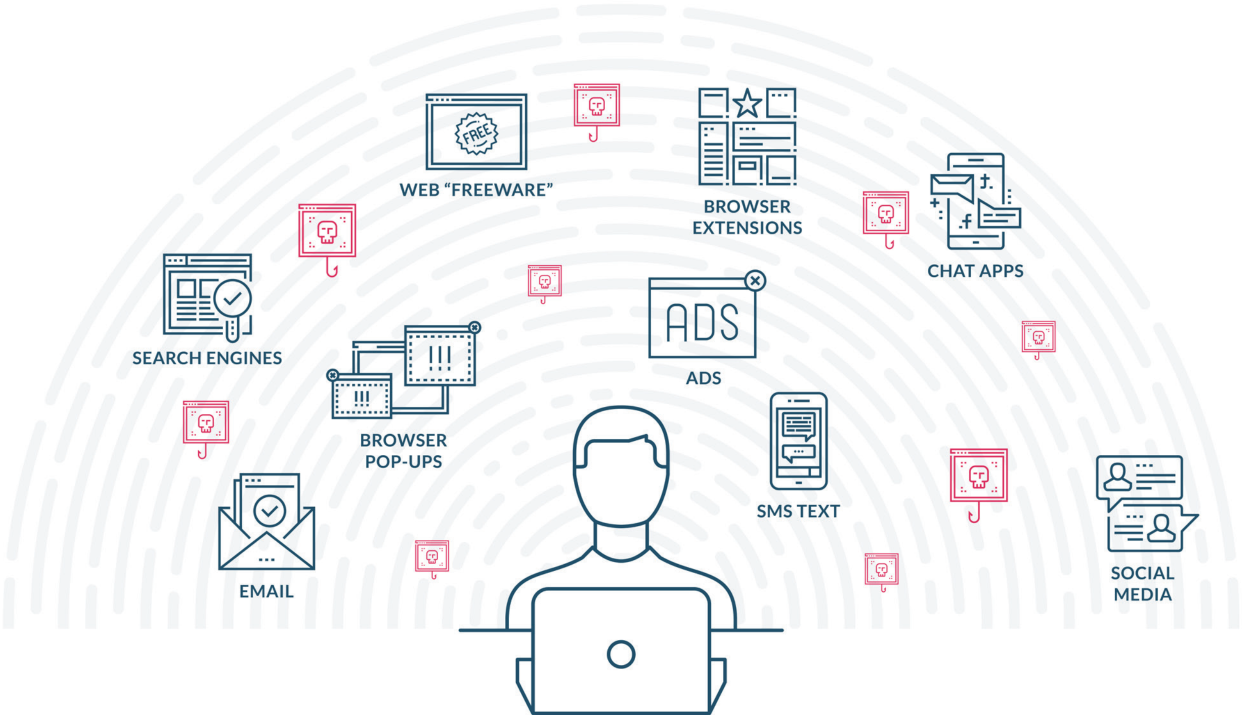


Exhibit 2: The phishing landscape has changed to include new attack vectors and phishing categories beyond email.

Fake login pages are no longer the only game in town. HTML phishing can be delivered straight into browsers and apps, bypassing infrastructure (SEG, NGAV, AEP), evading URL inspection, and domain reputation analysis methods. Bad actors have become sophisticated, employees can't spot the fakes, and traditional defenses that rely on domain reputation and blacklists are not enough. It's not surprising that Verizon's 2018 Data Breach Incident Report found that 93% of breaches involve phishing.

ATTACKS ARE MOVE FASTER THAN DEFENSES

The life-span of a phishing URL has decreased significantly since 2016 (Exhibit 3). Today bad actors are gathering valuable personal information and moving on within 40-45 minutes to evade detection. SlashNext Real-Time Phishing Threat Intelligence feeds are seeing an average URL life-span of 40 to 50 minutes.

Timeline of a Phishing URL

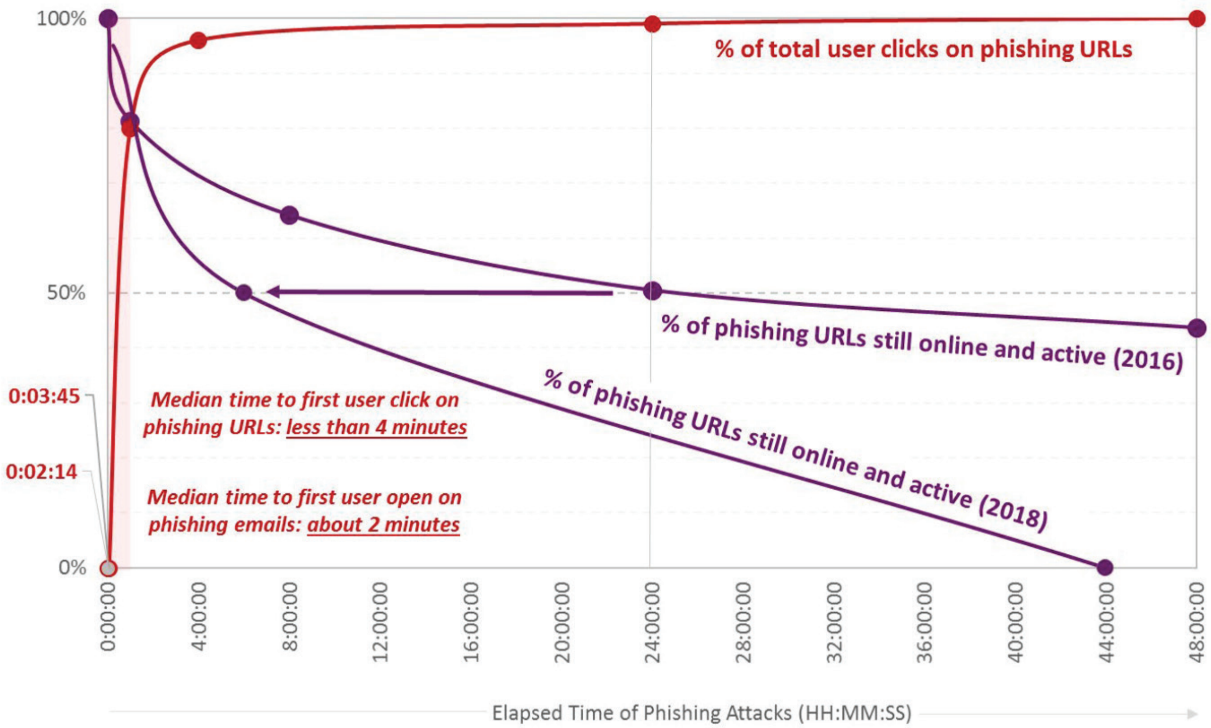


Exhibit 3: 80% of victims are hooked within first hour and most sites disappear in 4-8 hours, before they become known or blacklisted. Source: Reducing the Risk of Phishing Attacks: The Race is On (Aberdeen Group, Dec. 2018)

Bad actors are aware of how current technologies are trying to catch them, and they see perfect opportunities to evade detection. They change domains and URLs fast enough so the blacklist-based engines cannot keep up. For example, malicious URLs might be hosted on compromised sites that have good domain reputation. People click and within a few minutes the bad actors have collected all the data they need, so they move on to the next site. By the time the security teams have caught up, that cool attack is already gone and hosted somewhere else. It's no surprise at this speed that old legacy methods of chasing URLs and using domain reputation are no longer enough. Of the tens of thousands of new phishing sites that go live each day, the majority are hosted on compromised, but otherwise legitimate domains. These sites would pass a domain reputation test, but they're still hosting the malicious pages.

At SlashNext, approximately 90% of the phishing URLs detected by our feeds are either hosted on a compromised domain, or hosted on legitimate cloud services like SharePoint, GoDaddy, and Amazon AWS. Bad actors know blacklisting Amazon or SharePoint isn't feasible, so any online services that provide HTML hosting are prey for these types of attacks, as bad actors attempt to evade domain reputation engines.

PHISHING BEYOND FAKE LOG-IN PAGES

The phishing type that everyone is familiar with, fake login pages to various business applications, PayPal, SharePoint, and Office 365, are all popular targets. The threat research team at SlashNext sees many phishing attacks that do not involve fake log-ins including malicious browser extensions, rogue apps, social engineering scams, post-infection phishing C2s and tech support scams leading to remote backdoor access.

Malicious Browser Extensions

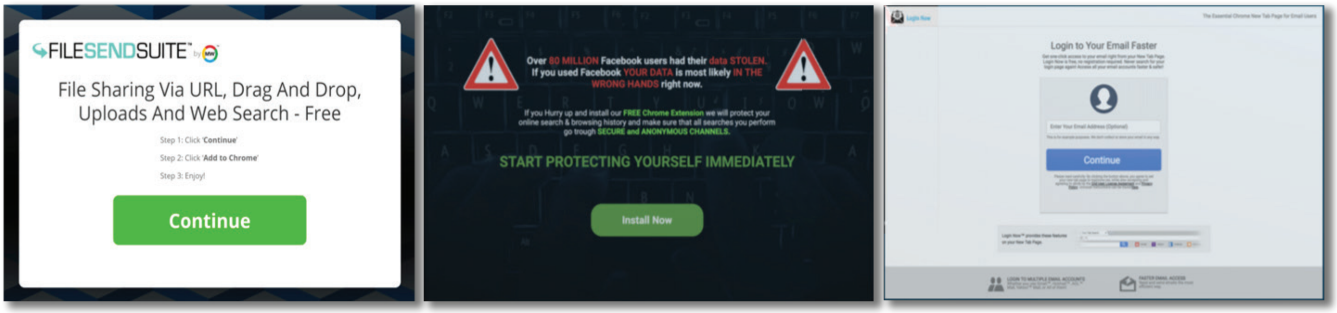
There is a lot at stake with all types of phishing, but malicious browser extensions can be particularly sophisticated. Google runs security checks on Chrome extensions before they are available in the store, but bad actors know this, and by design, these browser extensions have legitimate functionalities. They are capable of updating or downloading JavaScript on the fly and once installed; the malicious script is downloaded from the web. Using a runtime code, once the browser is closed, it goes away, but when you launch the browser, it's active, because the code is living inside the browser memory with JavaScript. JavaScript is the most common thing you can find inside a browser, so there's no way you can distinguish the malicious JavaScript that is scraping data from JavaScript that's being rendered by a legitimate page.

Now we see more phishing attempts that can bypass two-factor authentication (2FA) or multi-factor authentication, with Man-in-the-Browser attacks. Many with 2FA believe they're protected from phishing because the birth of 2FA grew from the knowledge that anti-phishing defense systems were no longer working. Users think it's ok to use extensions that make their life easier, like logging into email faster or using a PDF Converter. These extensions have legitimate functionality, but they have a side business, and that's the reason why they are free. Their exact functionality is the Man-in-the-Middle that is scraping and selling their data.

At SlashNext, we see malicious browser extensions that merely wait for the 2FA to complete. A browser extension offers bad actors the perfect workaround for organizations that rely heavily on 2FA. By design, once a browser extension is installed, it has access to the complete canvas of the browser. Once logged in, they hijack the session and capture whatever is being rendered on the computer screen. These extensions have the full power to do whatever the user is doing and seeing whatever is within that browser window.

For example, a user logs into a Service Now Management Portal, once 2FA is complete, the browser extension starts collecting data—leaving the organization's cloud infrastructure wholly open and vulnerable. With bad actors waiting for the user to log-in legitimately before they start scraping data from the browser, 2FA or multi-factor authentication ceases to be a viable security option to protect organizations.

Examples of Malicious Browser Extensions



File Sharing Via URL, Drag And Drop, Uploads And Web Search - Free

Step 1: Click 'Continue'
Step 2: Click 'Add to Chrome'
Step 3: Enjoy!

Over 80 MILLION Facebook users had their data STOLEN. If you used Facebook YOUR DATA is most likely IN THE WRONG HANDS right now.

If you Hurry up and install our FREE Chrome Extension we will protect your online search & browsing history and make sure that all searches you perform go trough SECURE and ANONYMOUS CHANNELS.

START PROTECTING YOURSELF IMMEDIATELY

Login to Your Email Faster

Get one-click access to your email right from your New Tab Page. Login Now is free, no registration required. Never search for your login page again! Access all your email accounts faster & safer!

FILESENDSUITE
Continue
Install Now
Login Now
The Essential Chrome New Tab Page for Email Users
Enter Your Email Address (Optional)
Continue
LOGIN TO MULTIPLE EMAIL ACCOUNTS
FASTER EMAIL ACCESS

Exhibit 4: Despite going through a rigorous review, some browser extensions available in the Chrome store start benign, but with an update become malicious.

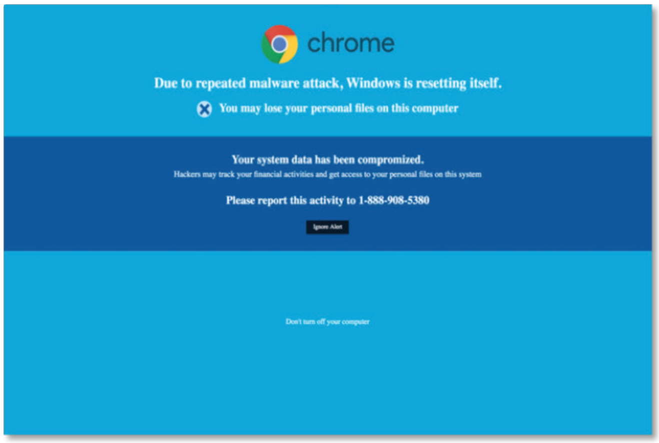
Technical Support Scams

At the same time, you have the technical support scam that asks you to install a TeamViewer or some other LogMeIn software, that can log in remotely. A fake scan is then performed and the TeamViewer session is left open so it can be sold on the black market. In this case a scammer has stored a legitimate backdoor, which is not malware, but it provides full backdoor capability. These credentials are sold on the Dark Web, and the best-of-the-breed antivirus will not find them. There are many other examples, like phishing C2s, and none of these attacks can be prevented through 2FA or security dongles.

Scareware

Scareware is something that many phishing threat intelligence and antivirus detection systems cannot detect. These scams are designed to fool the user. There is nothing inherently wrong that an antivirus threat analysis would catch—there are no exploits or malware. A scammer is just trying to scare the user into giving them remote access, and then the real damage happens. They asked you to install a legitimate remote support software like TeamViewer or LogMeIn, and once it's installed, the credentials and license are sold on the dark web. Now, whoever wants to attack your organization doesn't have to send a phishing email; they can go to the dark web and buy the credentials.

Examples of Scareware, Tech Support Scams



Due to repeated malware attack, Windows is resetting itself.

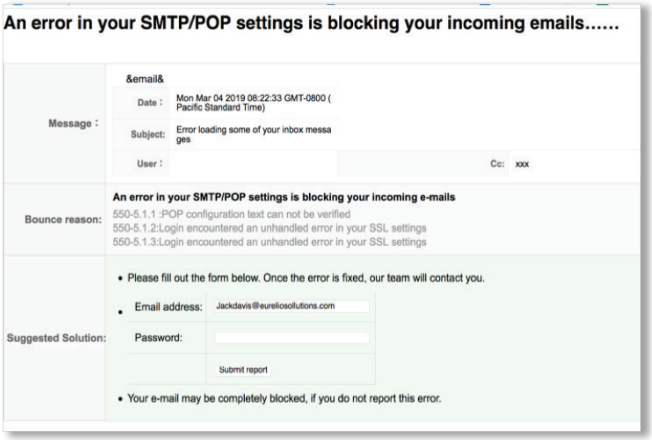
You may lose your personal files on this computer

Your system data has been compromized.

Hackers may track your financial activities and get access to your personal files on this system

Please report this activity to 1-888-908-5380

Don't turn off your computer



An error in your SMTP/POP settings is blocking your incoming emails......

Message : &email&

Date : Mon Mar 04 2019 08:22:33 GMT-0800 (Pacific Standard Time)

Subject: Error loading some of your inbox messa ges

User :

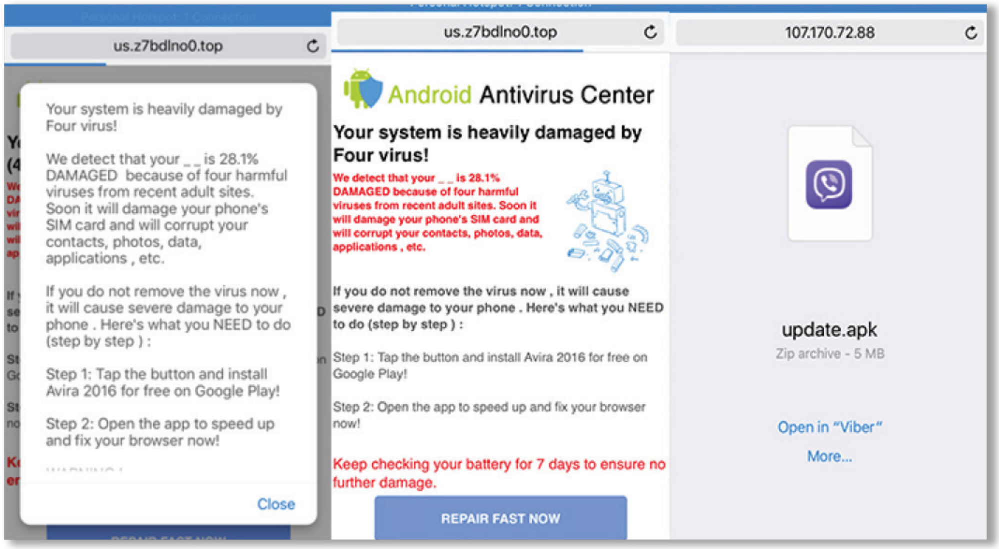
Cc: xxx

Bounce reason: An error in your SMTP/POP settings is blocking your incoming e-mails

550-5.1.1 :POP configuration text can not be verified
550-5.1.2:Login encountered an unhandled error in your SSL settings
550-5.1.3:Login encountered an unhandled error in your SSL settings

Suggested Solution:

- Please fill out the form below. Once the error is fixed, our team will contact you.
- Email address: Jackdavis@eureliosollutions.com
  Password:
  Submit report
- Your e-mail may be completely blocked, if you do not report this error.



Your system is heavily damaged by Four virus!

We detect that your _ _ is 28.1% DAMAGED because of four harmful viruses from recent adult sites. Soon it will damage your phone's SIM card and will corrupt your contacts, photos, data, applications , etc.

If you do not remove the virus now , it will cause severe damage to your phone . Here's what you NEED to do (step by step) :

Step 1: Tap the button and install Avira 2016 for free on Google Play!

Step 2: Open the app to speed up and fix your browser now!

Your system is heavily damaged by Four virus!

We detect that your _ _ is 28.1% DAMAGED because of four harmful viruses from recent adult sites. Soon it will damage your phone's SIM card and will corrupt your contacts, photos, data, applications , etc.

If you do not remove the virus now , it will cause severe damage to your phone . Here's what you NEED to do (step by step) :

Step 1: Tap the button and install Avira 2016 for free on Google Play!

Step 2: Open the app to speed up and fix your browser now!

Keep checking your battery for 7 days to ensure no further damage.

update.apk

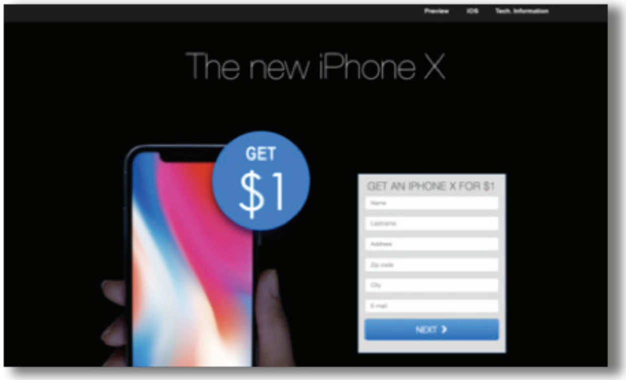
Zip archive - 5 MB

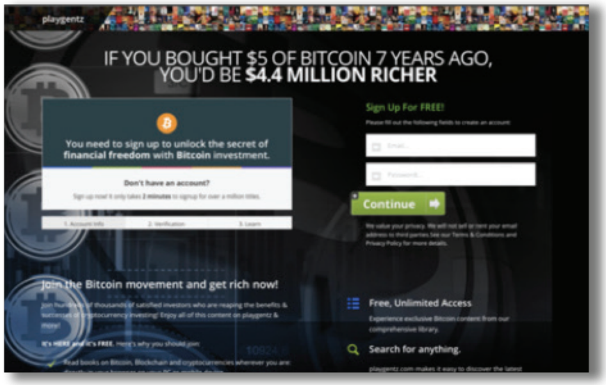
Exhibit 5: Tech Support Scams and Scareware are designed to scare the user into creating a backdoor that can be sold on the dark web

Social Engineering Scams

The bad actor's motives are the same with social engineering scams as with tech support scams. The goal is to get a user to install something to get information. One example is an iPhone giveaway, which starts asking a series of questions on the first page. When the user is 20% done, there is a new questionnaire and then another questionnaire, until they have collected all the user's confidential information and now the user is just 10% away from getting an iPhone. There's nothing inherently wrong with these ads because they are legitimate rewards. There is no way to distinguish between legitimate and malicious ads because they are intermingled within the very fabric of internet advertising. One out of 10 ads are malicious, but they are precisely the same as legitimate one, there are no files or malware to detect.

Examples of Social Engineering Scams





You need to sign up to unlock the secret of financial freedom with Bitcoin investment.

Don't have an account?

Sign up now! It only takes 2 minutes to signup for over a million titles.

Please fill out the following fields to create an account

We value your privacy. We will not sell or rent your email address to third parties See our Terms & Conditions and Privacy Policy for more details.

Join the Bitcoin movement and get rich now!

Join hundreds of thousands of satisfied investors who are reaping the benefits & successes of cryptocurrency investing! Enjoy all of this content on playgentz & more!

It's HERE and it's FREE. Here's why you should join:

Read books on Bitcoin, Blockchain and cryptocurrencies wherever you are:

Experience exclusive Bitcoin content from our comprehensive library.

playgentz.com makes it easy to discover the latest

Exhibit 6: Screen shots of iPhone and Bitcoin frauds that are part of social engineering scams .

With all of these phishing threat vectors, the purpose is precisely the same, to install a backdoor or scrape confidential information to sell on the dark web. The methods are different—They play on human desires and fears. Sometimes they scare, sometimes they pretend to be legitimate or they merely create excitement.

PHISHING IS A BUSINESS, BUILT TO MAKE MONEY

Most targeted attacks are happening when bad actors buy data from the dark web. Gone are the days where hackers or nation states would actually send a phishing email and work hard to penetrate an organization. Today a bad actor can go to the dark web to buy infected machines from the organization of their choice. Every organization has infected features and employees. Information is compromised. All hackers have to do is pay a middleman for access. They don't have to go to lengths to try to scam you, because the compromised machines with malicious browser extensions or TeamViewer are already available for sale.

We currently see tens of thousands of new phishing sites per day, but it varies day-to-day depending on the activity of bad actors. For instance, on weekends we might see volume decrease by 50% because the bad actors take weekends off too. By Sunday morning (PST) we see volume pick up again, by Monday and Tuesday it's at full volume. Phishing is a business, much like any other, built to make money.

A DIFFERENT APPROACH IS NEEDED

Even a tech-savvy user could miss phishing from different attack vectors. It's not possible to remember the millions of blacklisted URLs or take the time to cross verify the origins of a site. Most employees are not tech savvy users, they are not trained to detect these types of sophisticated phishing attacks, and they merely fall victim. Human vulnerability, human-vetted threat intelligence and traditional blacklists are no match for today's fast-moving phishing threats.

Most of the industry is examining phishing URLs and domains. That data is often not accurate or fast enough to detect new and fast-moving phishing attacks. Slashnext's approach for detecting phishing centers on the behavioral analysis of the content. If something looks suspicious, it's loaded into a virtual browser session and renders the whole page, so SlashNext's Session Emulation and Environment Reconnaissance™ (SEER) threat detection technology can detect threats missed by URL inspection and domain reputation analysis.

Real-Time Site Analysis with SEER

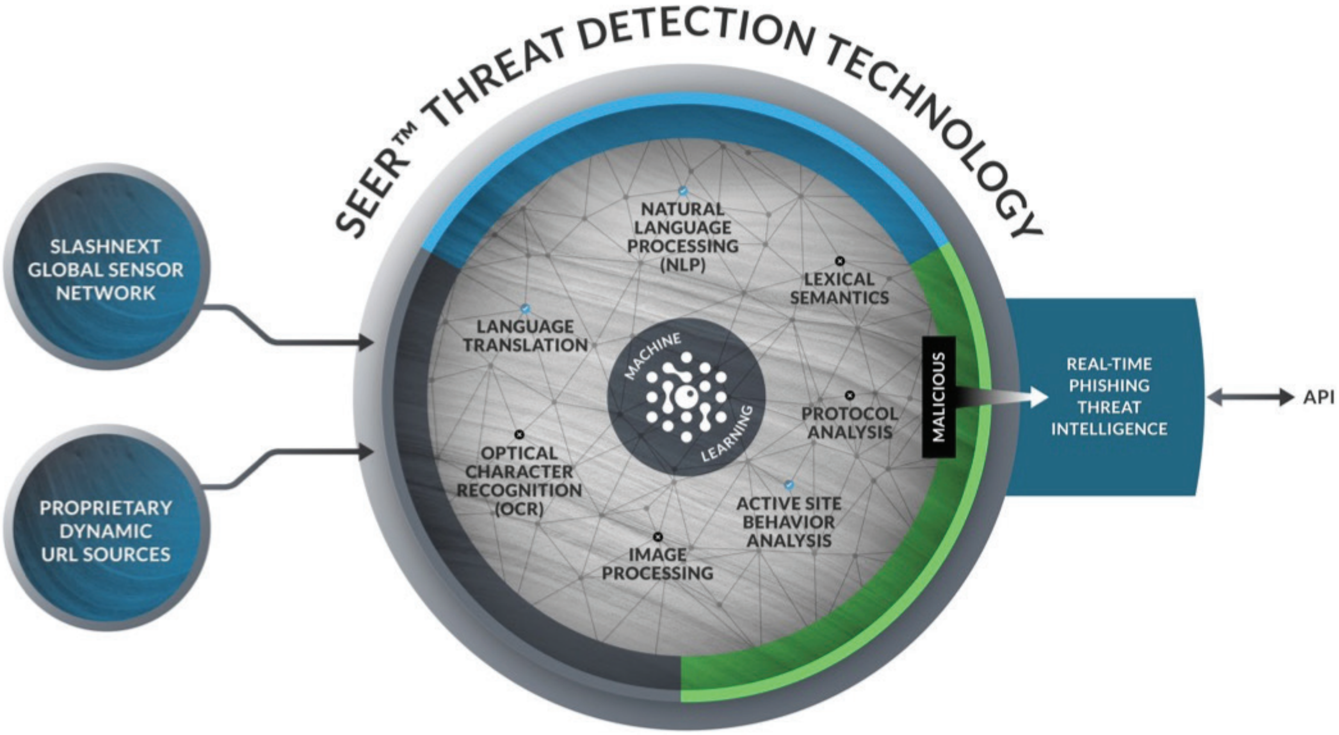

SEER™ THREAT DETECTION TECHNOLOGY
SLASHNEXT GLOBAL SENSOR NETWORK
PROPRIETARY DYNAMIC URL SOURCES
NATURAL LANGUAGE PROCESSING (NLP)
LEXICAL SEMANTICS
LANGUAGE TRANSLATION
MACHINE LEARNING
PROTOCOL ANALYSIS
OPTICAL CHARACTER RECOGNITION (OCR)
ACTIVE SITE BEHAVIOR ANALYSIS
IMAGE PROCESSING
MALICIOUS
REAL-TIME PHISHING THREAT INTELLIGENCE
API

Exhibit 7: SEER analyzes page content using natural language processing and image recognition to see exactly how it looks and understand the context of the page.

A SMARTER, CLOUD-POWERED APPROACH TO REAL-TIME THREAT DETECTION

Through multiple live sources, SlashNext proactively scans billions of global internet transactions and millions of suspicious URLs daily. Suspect URLs are rendered with millions of virtual browsers in the SlashNext threat detection cloud. SEER technology inspects the site with advanced computer vision, OCR, NLP, and active site behavior analysis. SEER analysis features are fed into machine learning algorithms which deliver a single definitive verdict: malicious or benign. There are no inconclusive threat scores and near zero false positives. Malicious URLs, Domains, and IPs are continuously added to the SlashNext Real-Time Phishing Threat Intelligence feed and available in multiple machine-readable formats via Web APIs.

Real-Time Site Analysis with SEER

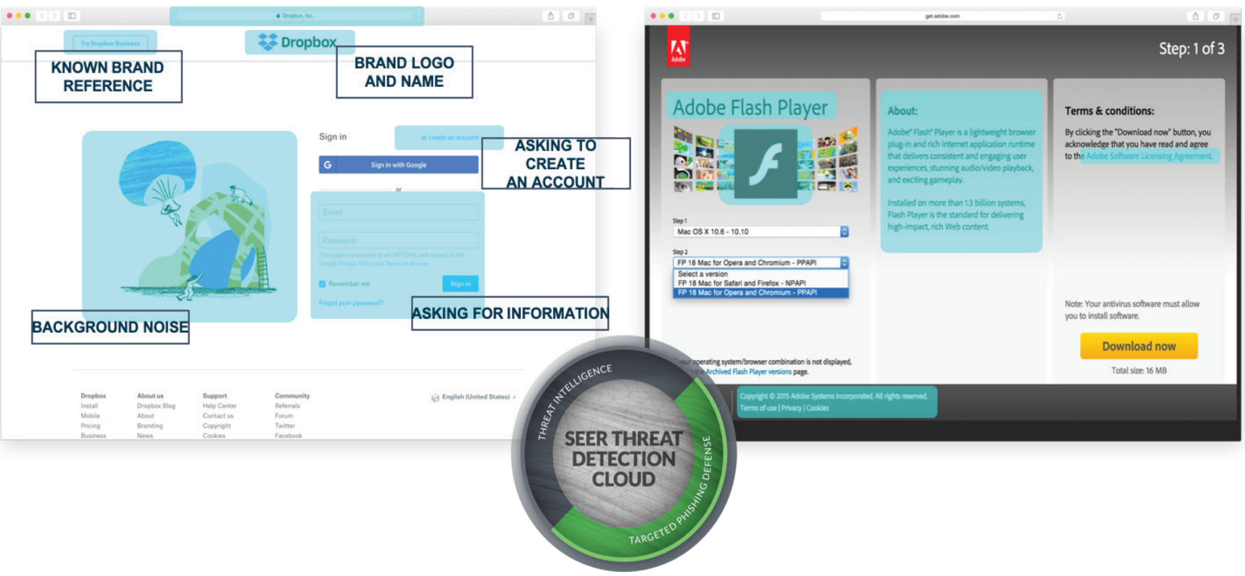


Exhibit 8: The area highlighted in blue demonstrate how SEER is analyzing the URL. .

SEER has viewed millions of websites that have been written historically for phishing or for benign purposes. And just like a security education company that trains employees, SEER is trained to recognize a phishing site. It doesn't matter if the malicious URL is hosted on a legitimate site like Dropbox or SharePoint, SEER will use real-time behavioral analysis rather than URL reputation to see, read and behave like an actual user. All enabling it to make a definitive determination if the site is malicious or benign (Exhibit 8).

GET AHEAD OF ZERO-HOUR PHISHING THREATS WITH REAL-TIME PHISHING THREAT INTELLIGENCE

Phishing attacks are coming and going so quickly, and many are hosted on compromised websites that pass URL inspection. The bad actors are sophisticated and creating new methods to evade detection. A much more automated approach is needed. SlashNext's Real-Time Phishing Threat Intelligence produces threat intelligence that is more automated and offers higher levels of accuracy, because it's evaluating many more characteristics of the site, it's able to renders a definitive verdict, malicious or benign.

Continuously Updated List of Zero-Hour Phishing URLs, Domains, IPs

This approach is entirely different than other threat feed products that offer a probability of being malicious and suspicious. With a binary approach, we can offer our feed for blocking purposes. It's a continuously updated list of zero-hour phishing URLs, domains, IPs with IOCs that can stop an attack before it happens. Most threat feeds are not even suitable for blocking purposes and are usually used in research. We are marketing our threat feed for instant blocking because there are near-zero false positives, which offers little fear of blacklisting legitimate websites.

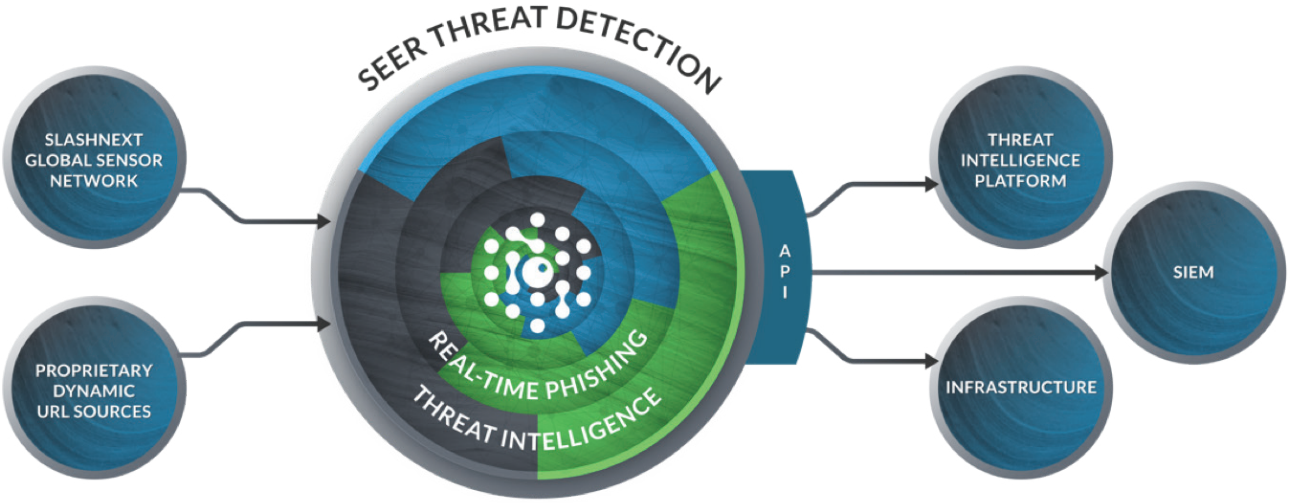

SEER THREAT DETECTION
SLASHNEXT GLOBAL SENSOR NETWORK
PROPRIETARY DYNAMIC URL SOURCES
REAL-TIME PHISHING THREAT INTELLIGENCE
API
THREAT INTELLIGENCE PLATFORM
SIEM
INFRASTRUCTURE

Exhibit 9: Real-Time Phishing Threat Intelligence detects tens of thousands of new phishing site per day, delivering a continuously updated list of zero-hour phishing URLs, domains, IPs.

Dynamic Data Collection, Multiple Proprietary Sources, Proactive Threat Hunting

SlashNext's Real-Time Phishing Threat Intelligence feed is taking dynamic data collected from multiple proprietary sources, and proactive threat hunting. This data is fed into the SEER engine, and within minutes, it is available for blacklisting if it's malicious. The live input to the system, outputs real-time, because speed matters. If a feed is 45 minutes late, the attack is already gone. That is what differentiates SlashNext from other vendors who have semi-manual processing. Our approach takes live data streams, without any manual intervention to provide the speed that is needed to protect your organization. Otherwise, detecting phishing URLs after two hours becomes useless because the attack has already moved.

Covers All Major Phishing Categories

Real-Time Phishing Threat Intelligence is very easy to integrate, it's generated in real-time and available through a REST API, covering all six-types of phishing:

- Credential Stealing
- Scareware
- Rogue Software
- Phishing Exploits
- Social Engineering Scams
- Phishing Callbacks (C2s)

The threat feed is available in multi-formats (JSON, CSV, plaintext). It can be feed it to your SIEM for correlation, or firewalls to see how many infected machines exist in your organization. It can be used in your blocking infrastructure and integrated into a Threat Intelligence Platform (TIP) to become part of a unified blocking feed.

Fully-Automated URL Re-checking and Retirement

With a combination of six threat feeds to deal with all ranges of phishing attacks, tens of thousands of new phishing site are detected each day. Real-Time Phishing Threat Intelligence offers a very robust retirement mechanism that is dynamically rechecking phishing sites in the background. The moment a site is no longer malicious, we take the URL out of the feed. The advantage is that only the dynamic list of active phishing sites is accessible, so an organization will have the confidence of knowing when using this feed for blocking purposes, it will not jam firewalls with millions of dead domains, and it will not block legitimate websites that are no longer compromised.

ABOUT SLASHNEXT

We are a team of cybersecurity professionals changing how companies protect themselves from today's—and tomorrow's—phishing threats. Our mission: to protect organizations from the growing number of phishing attacks occurring outside of email throughout the Web.

Founded by Atif Mushtaq, lead architect of FireEye's core malware detectiontechnology, we are focused on the biggest vulnerability in cybersecurity: human fallibility. While OS emulation (sandboxing) addressed the .exe malware problem, SlashNext has pioneered the concept of Session Emulation to solve the HTML Attack problem presented by Web-based phishing.

Over 90% of breaches begin with phishing. And while email phishing still occurs, secure email gateways and employee training have forced hackers to employ phishing tactics beyond the inbox via techniques that evade existing cybersecurity defenses by design. Thus, phishing is shifting to the Web with browser pop-ups, ads, search results, browser extensions, chat, and social media. The problem is big. And getting bigger.

SEE WHAT PHISHING THREATS YOU'RE MISSING—TRY SLASHNEXT REAL-TIME PHISHING THREAT INTELLIGENCE FREE FOR 15 DAYS.

LEARN MORE AT HTTPS://WWW.SLASHNEXT.COM/FREE-TRIAL/

4301 Hacienda Drive, Pleasanton, CA 94588 | slashnext.com | info@slashnext.com | 800.930.6843