Volume 7, Issue 2
[State of the Internet]

Phishing for Finance

Akamai Intelligent Security Starts at the Edge

Table of Contents

Letter from the Editor

Welcome to the second State of the Internet / Security report of 2021. Whether you're a new reader or someone who's been reading for years, we're glad you're reading this issue. As always, we continuously strive to improve our work and bring you something new with every effort.

You may remember our gaming security issue from 2020, where we partnered with the digital events company DreamHack. We supplemented our data and research with information on the views and opinions, based on a survey of more than 1,000 gamers. This was the first time we'd gone beyond the data Akamai was able to gather to learn more about the problems we're facing.

In this issue, we're going even further. While we have access to some of the largest security data sets in the world, our viewpoint is limited to the traffic that traverses our networks and is seen by our tools. Even the hundreds of terabytes we serve every second are only a part of the global story. This is why we're partnering with threat intelligence company WMC Global for this report.

A significant part of what makes the security industry effective is the number of partnerships that go on quietly behind the scenes.

The researchers at WMC Global are experts at understanding SMS phishing (smishing) and the toolkits that criminals devise to make their attacks possible. Working together, we were able to not only look at the global contours of attack traffic, but also pick apart a specific toolset. Our desire is to provide you with both a wide view of the threat and a deep dive into a specific threat.

A significant part of what makes the security industry effective is the number of partnerships that go on quietly behind the scenes. Whether it's various global law enforcement agencies cooperating with each other, security organizations cooperating with law enforcement, or the partnerships that happen daily between individuals and companies, much of this work goes unseen by the average security professional.

But that doesn't always have to be the case. We believe that organizations should be working together publicly to share intelligence with you. Verizon's Data Breach Investigations Report (DBIR) is the best-known and longest-standing example of shared intelligence, which Akamai has been contributing to for over half a decade (seven reports, if you want to be exact). We'd like to see more, which is why we're leading by example. Or following the example set by others, depending upon your point of view.

We appreciate having partners like the team at WMC Global who are willing to take the time to develop research with us. This type of work makes us more knowledgeable and better able to protect our organizations and our end users, which should be a goal for every security professional.

Martin McKeay
Editorial Director

GUEST ESSAY

Why Is SMS Phishing Effective?

Ian Matthews
CEO, WMC Global

SMS is one type of messaging that users respond to almost instantly and with great consistency. Unfortunately, threat actors are increasingly exploiting users' trust, inundating their phones with phishing messages impersonating banks, entertainment channels, package delivery services, online retailers, and more.

SMS phishing (or smishing, as it's commonly known) is a global problem, and each malicious message undermines users' trust in messaging platforms. If left unchecked, smishing could cause a rapid decline in audience engagement and brand trust, meaning all stakeholders have a reason to protect SMS from progressively problematic attacks.

While the telecommunications industry is working hard to combat the problem, SMS phishing continues to be a lucrative enterprise for many threat actors, with escalating costs and consequences for both users and the telecommunications industry.

Why is SMS phishing so effective? SMS messaging is ubiquitous in today's smartphone-saturated communications environment. Each day, mobile users send billions of text messages, opening them quickly and frequently at a reported rate of 98%.

At the same time, SMS phishing attacks are inexpensive to develop and deploy. There is free infrastructure around domains and hosting and readily available methods of sending. To target mobile users, phishing attacks are primarily delivered over regular phone numbers, email to SMS, and (outside the United States) alpha tags, which are all easily accessible. Using burner phone numbers and fake information, many threat actors can quickly and affordably implement expansive SMS phishing campaigns with little risk of capture or prosecution.

While mobile users are progressively more aware of malicious messages on email and social networks, many inherently trust texts, and threat actors have ample opportunity to exploit this dynamic.

To preserve the integrity of the text message medium and to protect the user experience, everyone needs to understand this growing threat while working to guard against its proliferation.

The telecommunications industry is continually updating its defensive posture to prevent phishing messages from reaching their customers. While filtering agents adjust their strategies to block spam, threat actors counter their efforts with updated code and novel obfuscation techniques. Threat actors know they can deploy typosquatting techniques, for example changing the letter "O" to the number "0," or alter a URL to enhance the text message's complexity, to allow their malicious messages to avoid detection. Additional techniques, such as including a major brand – like UPS – in the message content, make it difficult for firewalls to differentiate legitimate messages from phishing messages.

Similarly, threat actors establish a URL phishing page that they masquerade using cheap or free short domains that redirect to the attack page. In this way, threat actors can send short URLs in a text message — perfectly crafted to appear legitimate to the unknowing recipient — without being blocked by filters.

Additionally, threat actors use multiple delivery methods to reach mobile users. They can effectively harness the idiosyncrasies of each delivery method (be it using a regular phone number or an email address) to avoid detection and increase overall effectiveness.

So, what is the solution?

Text messaging is a foundational element of today's mobile experience for over 5 billion people globally. Everyone, from carriers to cybersecurity companies to consumers, has motivation to participate in mitigating phishing on wireless platforms. The telecommunications industry is heavily invested in reducing SMS phishing on their networks, but they won't be successful alone.

To do so will require an all-in data-sharing effort from the entire value chain. Carriers, messaging platforms, firewalls, and threat intelligence vendors must replace today's siloed defensive strategy with a collaborative effort to prevent threat actors from using SMS phishing to steal customer data, compromise internal systems, erode user experience, and corrode brand integrity.

SMS messaging is thriving, and phishing attacks are a global issue that threaten to undermine its long-term consumer trust. If we don't work together to curb the scope, frequency, and effectiveness of phishing attacks, we risk devaluing text messaging as a trusted communication channel.

TL;DR

- *In 2020, there were 193 billion credential stuffing attacks globally, with 3.4 billion of them in the financial services space, representing a 45% growth over 2019.*
- *The number of web attacks targeting the financial services industry grew by 62%. Akamai observed 736,071,428 web attacks recorded against financial services in 2020. What was the number one web attack type targeting financial services? Local File Inclusion (52%), followed by SQL Injection (33%) and Cross-Site Scripting (9%).*
- *The Kr3pto phishing kit, which targets financial institutions and their customers via SMS, has been observed spoofing 11 brands across more than 8,000 domains since May 2020. Akamai and WMC Global have tracked Kr3pto campaigns across more than 80 different hosts (ASNs), including one host that housed more than 6,000 Kr3pto domains.*
- *An API used by the Ex-Robotos phishing kit, which targets corporate credentials, logged more than 220,000 hits over 43 days, with peaks in the first week of February 2021 reaching tens of thousands per day.*

Introduction

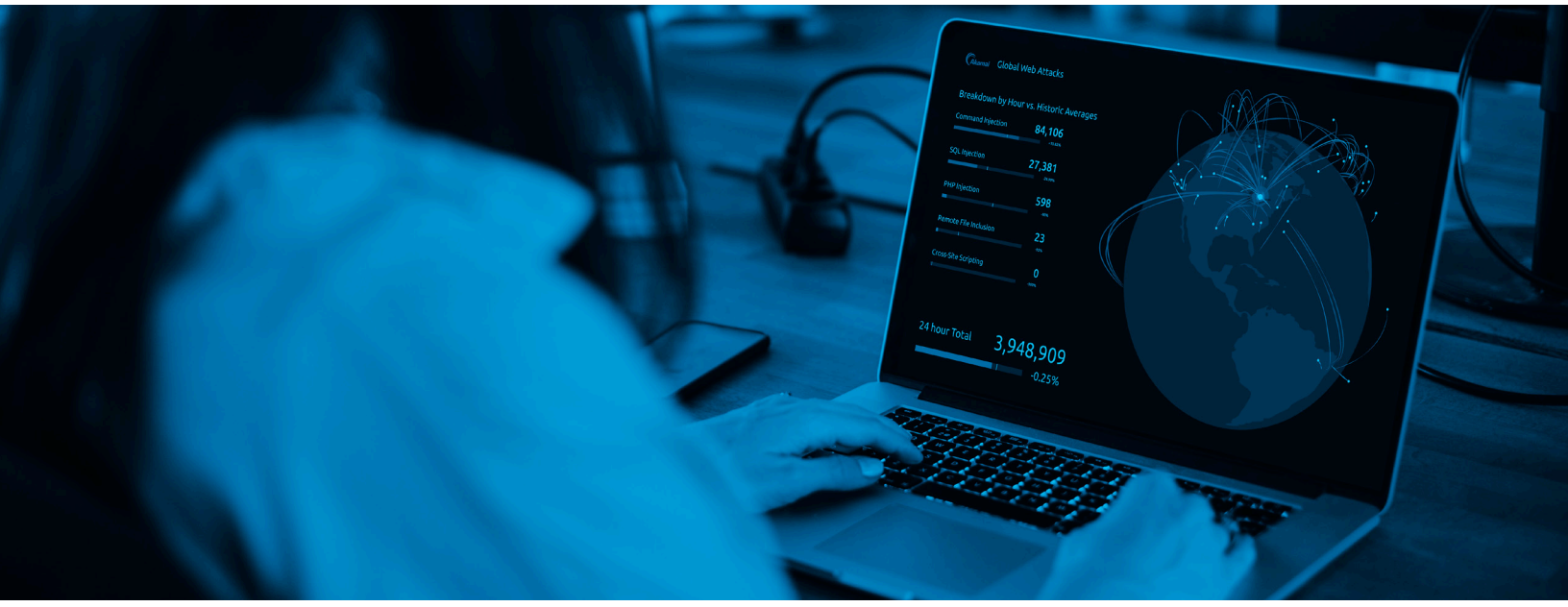
Over the past two years, Akamai's State of the Internet / Security report has evolved. Sometimes this change has been represented by new data, and the stories related to it. Other times, that evolution was represented by the inclusion of guest essays, outside research, additional threat intelligence, or a mix of all three. Already in 2021, we published our first SOTI Research report, which examined the impact of COVID-19 at Akamai and the types of attacks we faced as a company in 2020 because of it.

This report is another evolution. It includes research from WMC Global, a threat intelligence company that operates in a variety of business sectors, including financial services. For this edition of the State of the Internet / Security report, we felt that by examining WMC Global's phishing data, as well as our own, we could offer a more rounded picture of how these threats impacted the financial sector in 2020. But phishing is just part of the story. In addition to that data, we also looked at the distributed denial-of-service (DDoS), credential abuse, and web attack data collected by Akamai's sensors throughout the year.

What did we learn? Credential abuse, which is a byproduct of phishing, often with a goal of account takeover, remains one of the top attack vectors in a criminal's arsenal.

In 2020, there were 193 billion credential stuffing attacks globally, with 3.4 billion of them in the financial services space. Throughout 2020, criminals leveraged COVID-19 and the promise of financial assistance, or the stress of financial hardship, to target people across the globe via phishing. These attacks, in turn, fueled the credential stuffing boom, as newly collected credentials, newly sorted data breaches, and old collections were combined, tested, traded, and sold.

Akamai observed 6.3 billion web attacks globally in 2020, with 736 million of them in the financial services sector alone. SQL Injection was the top web attack, followed by Local File Inclusion, but these roles were reversed within the financial services industry.



Big Picture

In 2020, as shown in Figure 1, Akamai witnessed 193,519,712,070 credential stuffing attacks globally, with 3,452,192,348 in the financial sector alone, representing a 45% increase over 2019.

While some of this growth can be directly attributed to new visibility acquired by Akamai after onboarding new customers, it's still growth, even without the new attack insights. Passwords have always been a weak link in the security chain, and criminals won't hesitate to exploit that weakness.

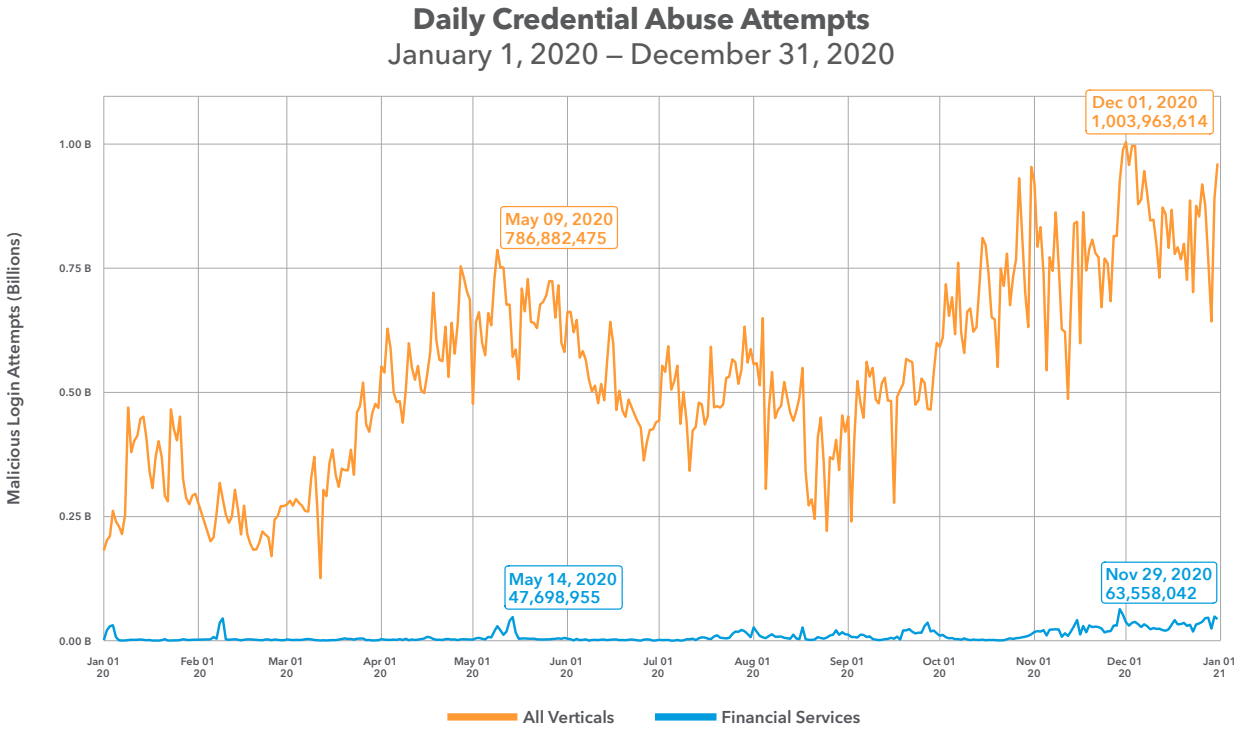


Fig. 1: Financial services experienced tens of millions of credential stuffing attacks each day in 2020, peaking at 63 million in November

Credential Abuse and Web Attacks Over Time

By adding more customers in 2020 and increasing our visibility, Akamai was able to see an increase of more than 360% for credential stuffing attacks and 150% while monitoring web attacks over the past three years.

2018
2,450,790,188 web attacks — 41,892,781,464 credential stuffing attacks

2019
6,153,098,198 web attacks — 46,959,228,610 credential stuffing attacks

2020
6,287,291,470 web attacks — 193,519,712,070 credential stuffing attacks

In May 2020, there were two dates that stood out. On May 9, credential abuse hit a peak of 786,882,475 attacks globally. Five days later, on May 14, the financial services sector saw its own record peak – 47,698,955 attacks. Later in the year, global credential abuse spiked again, reaching a peak of 1,003,963,614 attacks. The financial services sector also set a new record of 63,558,042 credential abuse attacks.

Looking back at the year, all of these instances can be linked to events happening in the criminal economy at the time. Millions of new usernames and passwords, tied to several notable incidents in Q1 and Q2 of 2020, as well as some in Q3, started circulating among criminals on several forums. Once these compromised credentials were in circulation, they were sorted and tested against brands across the internet, including several financial institutions.

> ***The financial services sector also set a new record of 63,558,042 credential abuse attacks.***

Web-based attacks and application attacks remained high in 2020 and show no indication of slowing anytime soon. Akamai observed 6,287,291,470 web attacks globally, with 736,071,428 of them in the financial services sector alone.

Many Aspects of Credential Abuse

There is a method to the madness, and chaos, that drives the credential abuse coming from the criminal economy. While a lot of the focus is on usernames and passwords, there are other elements at play. Passive attacks focus entirely on username and password combinations, targeting services large and small just to see how many accounts can be compromised.

The more focused aspect of credential abuse, however, is rather complex. For example, when a combination list doesn't produce results, a targeted effort refines the combination list with various sources to generate new passwords. The public witnessed smaller-scale efforts on this front when criminals targeted Zoom in early 2020 and unemployment agencies throughout the year. Larger-scale efforts include refining combination lists using sources such as derivatives of the original password or data enrichment, with the goal of leveraging the targeted marketing data in phishing campaigns and repeating the process until the original goal of account takeover is met.

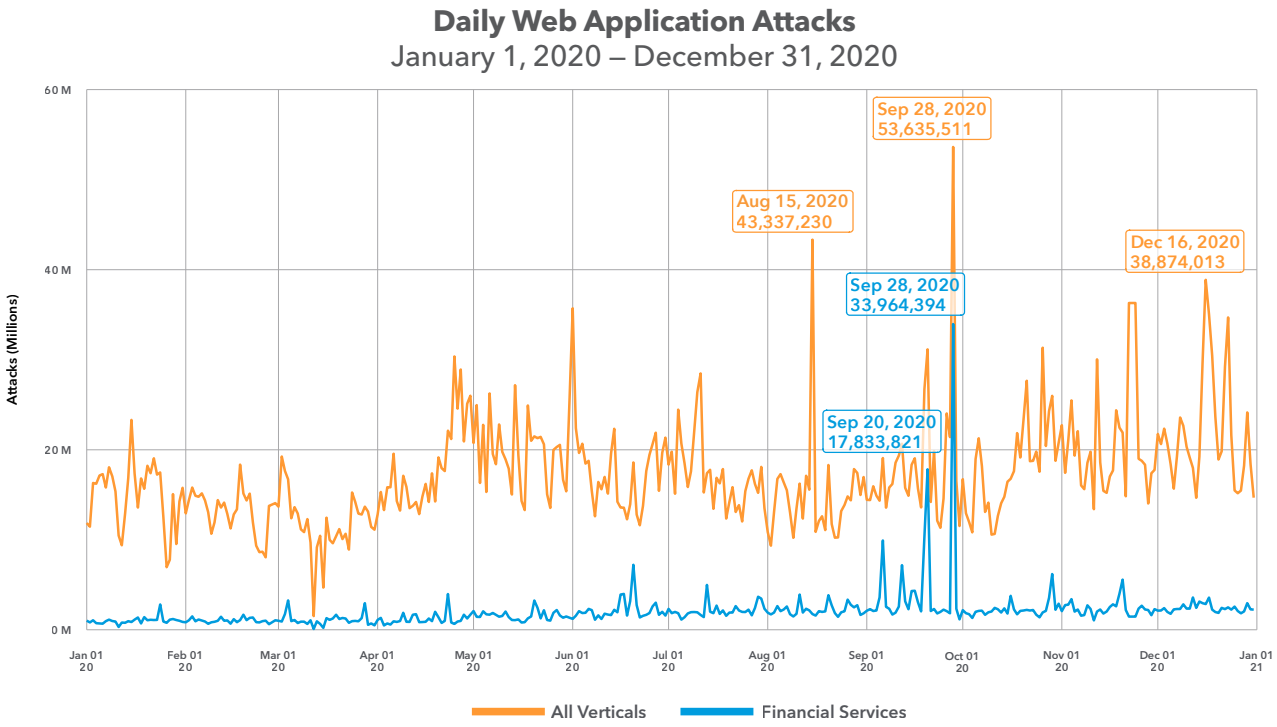


Fig. 2: Web attacks reached five notable peaks in 2020, all in Q3 and Q4

There were five notable peaks in 2020 (Figure 2), all of them taking place in Q3 and Q4. This correlates to a number of events, including the holiday shopping season, as well as additional criminal processing of freshly sorted compromised usernames and passwords. The first major peak happened in August, when global web attacks spiked to 43,337,230, followed by another jump to 53,635,511 in September. Around the same time, on September 20 and 28, the financial services industry experienced spikes reaching 17,833,821 and 33,964,394 attacks, respectively.

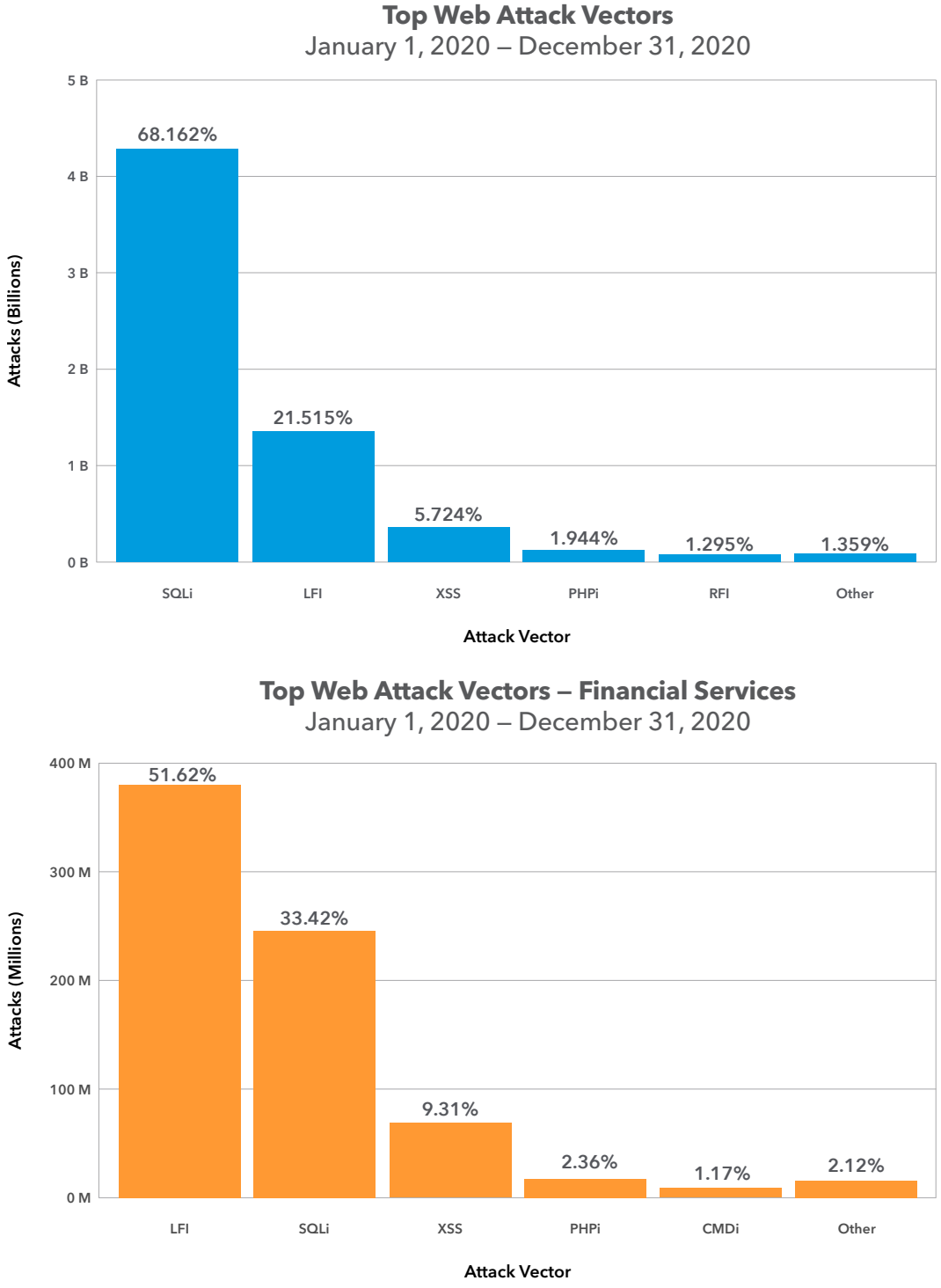


Fig. 3: LFI surpassed SQLi as the top attack type against the financial services industry in 2020, suggesting that criminals are still targeting APIs and applications

Globally, SQL Injection (SQLi) was the top attack vector, followed by Local File Inclusion (LFI), Cross-Site Scripting (XSS), PHP Injection (PHPi), and Remote File Inclusion (RFI). However, in the financial services industry, those attack vectors shift some, where LFI replaces SQLi as the top vector, swapping places entirely, followed by XSS, PHPi, and Command Injection (CMDi).

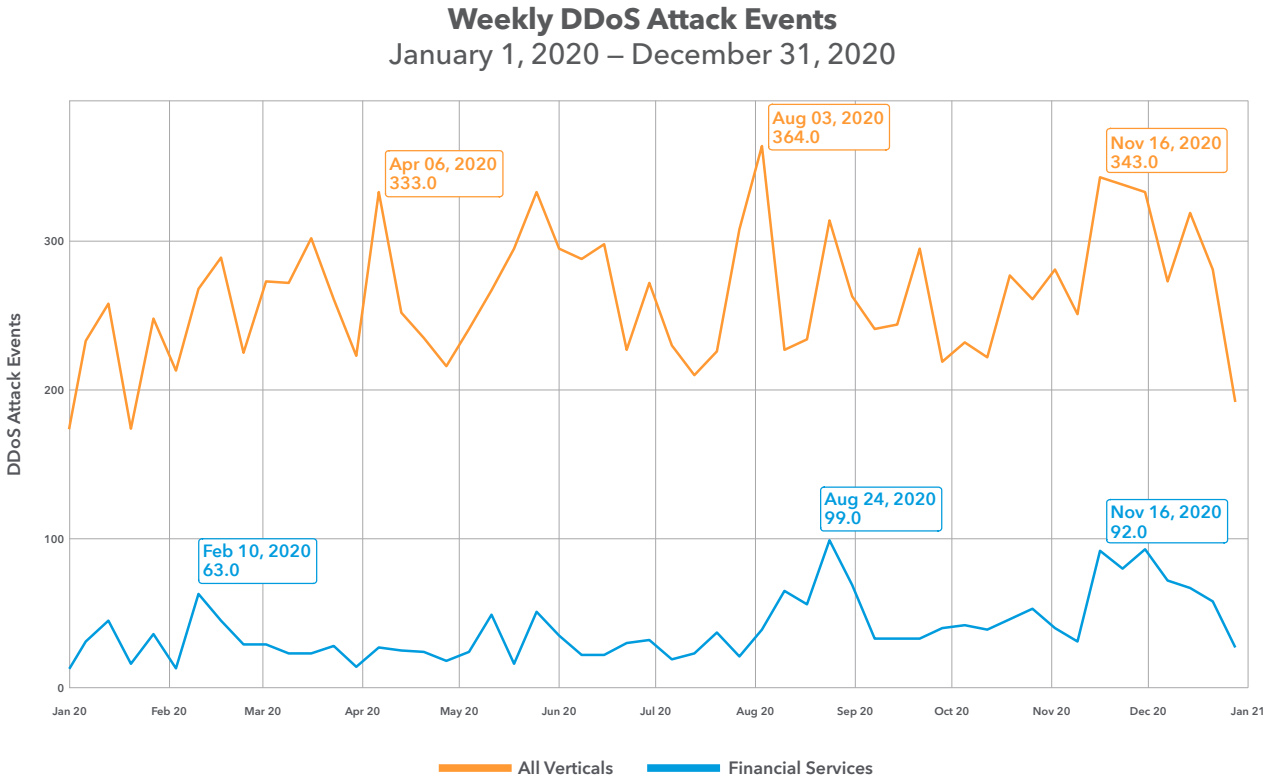


Fig. 4: DDoS attack volume has continued to grow in 2020 with a 110% increase in the financial services sector

DDoS attacks increased by 110% in 2020 over the previous year's totals in the financial services sector. Over the past three years (2018–2020), DDoS attacks against the financial services sector grew by 93%, proving that systemic disruption is always an option for criminals, who target services and applications required for daily business. In Figure 4, we see that DDoS attacks as a whole are consistent throughout 2020, with notable spikes in February, August, and November.

> ***DDoS attacks increased by 110% in 2020 over the previous year's totals in the financial services sector.***

Financial Phishing

To examine the scope and scale of the phishing attacks against the financial services industry, WMC Global and Akamai worked together to develop our research. As a threat intelligence company, and one with extensive insight into these sorts of attacks and the threat actors responsible, WMC Global was uniquely suited to help us develop the research needed for this report.

Over the past several years, phishing has remained a constant variable in many of the data breaches and security incidents that have dominated the headlines. Criminals have dedicated a good deal of energy and resources toward advancing the phishing economy on a regular basis. Gone are the days of basic cloned websites. Today, phishing is a turnkey business, even offered as a hosted solution for criminals who wish to leverage phishing-as-a-service developments.

As phishing attacks and kit development started to advance, defenders realized that usernames and passwords alone were not enough. To combat the phishing onslaught and other password-based attacks, defenders turned toward multi-factor authentication (MFA) and two-factor authentication (2FA) to help augment basic passwords. While 2FA is a subset of MFA, both provide the means of a second type of authentication, such as a PIN or one-time password (OTP). Often, 2FA is associated with SMS-based OTPs, whereas MFA is associated with authenticators, like Google Authenticator.

Fast-forward to today – the criminals have evolved. This change includes elements that target 2FA and MFA protections, where victims are tricked into filling out their OTP or revealing it to the threat actor during a conversation.

In this report, WMC Global and Akamai present research related to threat actors and the phishing kits being used to target the financial services industry, or people within it. One relatively new threat actor poses a serious threat to the financial services industry in the UK, with the development of dynamic phishing kits that effectively bypass secondary methods of authentication.

In addition, we'll examine another threat actor targeting corporate users and their credentials. The phishing kit used by this threat actor isn't overly complex, but there are a large number of websites hosting this particular Office 365 kit, which has been copied by other criminals and spread around.

Phishing as a Service

The concept of phishing as a service has been around for a few years now. Skilled website developers create complex phishing kits, which in some cases are near-flawless replicas of the targeted brand or financial institution. These kits come complete with back-end operational support and functionality, and all the developer needs to do is sell their creations to lesser skilled criminals who will, in turn, unleash them on the public.

Examples of these types of phishing kits can be seen in the coverage of 16Shop by Akamai and the Cazanova kits by WMC Global.

Busted!

In a way, those managing a phishing-as-a-service operation might feel as if they are bulletproof: allowed to create and sell their phishing kits and platforms with impunity, while someone else takes all the risk. However, this imagined immunity never lasts.

A case in point is U-Admin. This was a phishing-as-a-service platform that enabled a number of features, including phishing page generation plug-ins, victim tracking, and more, according to detailed analysis published by researcher Fred HK (@fr3dhk). One of the key elements in U-Admin was the ability to intercept MFA/2FA codes via web inject. In addition to phishing, U-Admin was also reported to have been leveraged as part of various malware-based attacks, such as Qbot.

On February 4, 2021, Ukrainian police – working with the FBI and Australian Federal Police (AFP) – arrested a 39-year-old man from the Ternopil region of Ukraine. This unnamed individual is said to be the creator and main distributor of U-Admin. According to the AFP, U-Admin was responsible for 50% of all the phishing attacks in Australia in 2019.

Enter Kr3pto

A threat actor going by the alias "Kr3pto" has made a name for itself selling phishing kits targeting many companies, including major financial institutions across the UK. Given the number of kits attributed to the Kr3pto brand, it appears that it also makes custom phishing kits based on customer requests.

Kr3pto gained the attention of WMC Global and Akamai after releasing phishing kits targeting eleven different banks in the UK. Given the scale and rapid progression of the attacks targeting the banks, Akamai and WMC Global were eager to investigate the source.

Kr3pto phishing kits target victim usernames and passwords, as well as any secondary authentication method being used, such as security questions and answers, and SMS-based PINs. The workflow used by the kits are seamless and dynamically adapt to the victim's login experience at their bank.

Research by Akamai's Or Katz shows that Kr3pto kits have been observed on 8,344 domains as of February 17, going back as far as May 2020. Deployment of the kit hit a peak of 800 domains in November 2020. This kit is so widespread, Katz tracked it to more than 80 different hosts via autonomous system numbers (ASNs). Just one of those ASNs was responsible for more than 6,000 Kr3pto domains.

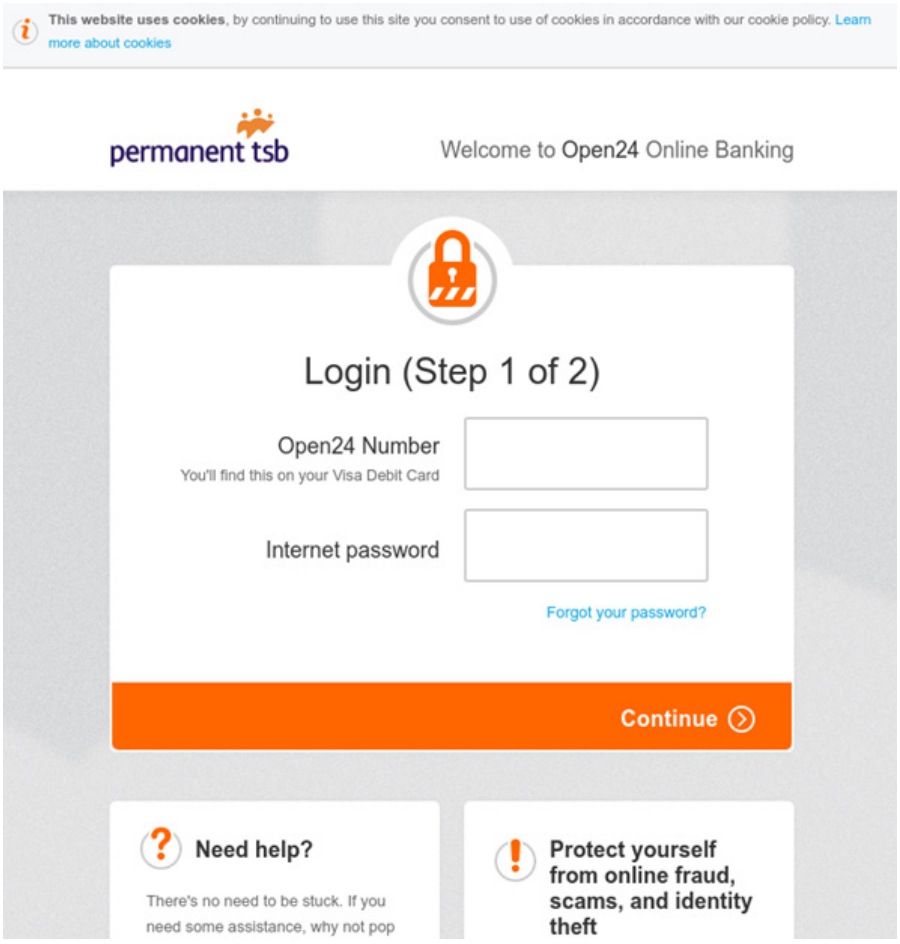


Fig. 5: A Kr3pto phishing page victimizing customers of Permanent TSB

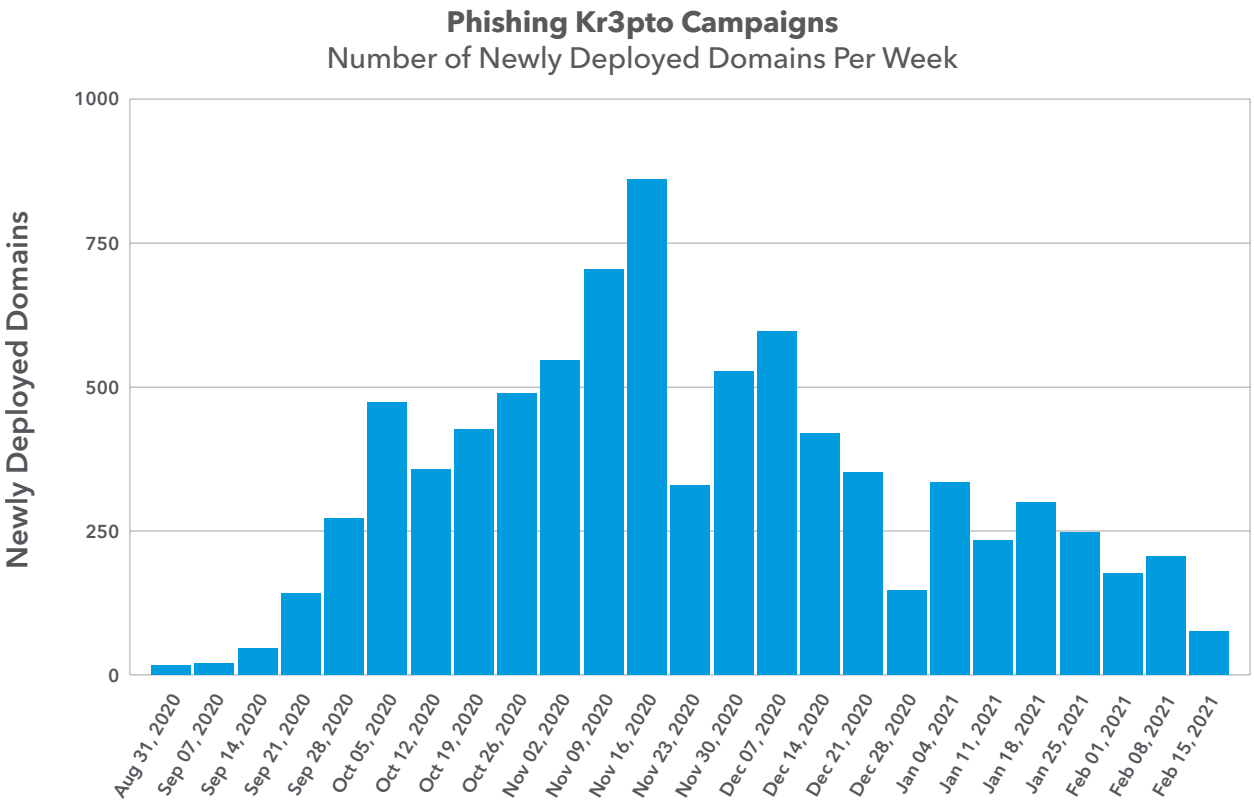


Fig. 6: A weekly breakdown of Kr3pto campaigns operating over time shows steady growth

Kr3pto Attack Workflow

Kr3pto starts its attack by sending lures to victims via SMS, reporting a locked account or a new payee being set up. Between January 12 and February 12, 2021, WMC Global tracked more than 4,000 campaigns linked to Kr3pto going out across SMS. The lures themselves change often, as do the numbers the SMS are delivered from, suggesting the threat actors running the attacks have access to a large pool of bulk SMS sending services, and automate the sending of the lures and phishing URLs.

The reason the lures are sent via SMS is obfuscation. Most enterprise operations, as well as home endpoint security offerings and general email accounts, will prevent malicious emails from hitting the victim's inbox. These protections aren't perfect, but they do prevent a majority of the attacks. Therefore, criminals have turned to SMS, and even social media, to deliver their lures.

Another thing that Kr3pto does is leverage dedicated hosting. Some phishing kits will look to compromise an existing website to leverage the reputation of the domain, but Kr3pto doesn't do that. Instead, threat actors running Kr3pto will register new domains and hosting. This is a weakness they can't avoid, since the records related to domain registration are easily tracked.

In fact, Akamai researcher Steve Ragan uses newly registered domain and certificate records as a method of tracking phishing campaigns and kit source code during his day-to-day research efforts. By monitoring the registrations of domains and SSL/TLS certificates via the certificate transparency logs provided by certificate authorities (CAs), the domains that criminals register certificates for are easily observed and reported.

There is a human element at play during these attacks as well, given that the lures are designed to cause panic, and no small amount of anxiety. These factors are what causes the victim to click the link in the SMS. The landing pages used by Kr3pto are responsive, meaning they will adjust to any screen size, including mobile devices. The URLs used by Kr3pto actors often include the target brand's name somewhere in the address, or a reference to the lure itself. Yet, when rendered on a mobile browser, the complete address is hidden, so victims see the name they were expecting, as well as the HTTPS they've been trained to watch for over the years.

Kr3pto kits require the threat actor maintaining them to manually work though the attack. What this means is that the person running the attack will log in to the admin panel on the phishing kit and wait. This creates complications, exposing another weakness, as whoever manages the attack must deal with scheduling and ensure there is coverage to monitor the admin panel. If an alert goes unnoticed, then the victim might become wise to the scam and report it.

Attack Structure

Once the victim is on the landing page, the phishing attack starts immediately. When the victim attempts to log in, their username and password are compromised. However, as this happens, the threat actor behind the attack is alerted to a new victim (the kit has text-based and audio-based alerts for the threat actor). Once the alert comes in, the threat actor will use the compromised credentials to log in to the real bank's website.

If the bank requires an SMS-based OTP, for example, the bank will send the victim the code, and the threat actor will generate a corresponding form (in real time) on the phishing website to obtain the OTP from the victim. Once the OTP is obtained, the threat actor running the attack will have all they need to access the victim's bank account and drain it. Researchers and industry sources estimate typical losses for each successful attack at $500 to $1,000.

Copycats and Clones

Kr3pto has become a popular kit in the phishing economy – so popular that other criminals have started ripping the code, or copying it wholesale, and using it in their projects. These kits have the same structure, functionality, and basic features, but the branding has been altered. If anything, their actions prove there is no honor among thieves. It is doubtful they are paying the real Kr3pto creator any sort of commission when they sell the ripped kits.

Cracked kits are an interesting research line to follow. Some rippers might alter the functionality of the original kit, or even add backdoors. Sometimes, the rippers cracking a kit will do so to remove backdoors.

Did you know?

In the phishing economy, rippers are those who steal or copy the code of phishing kit developers and rebrand it or resell it as their own. When this happens, the process is called "ripping." Also, it is common for ripped kits to be known as cracked kits, because the rippers have removed the protections that were intended to prevent ripping.

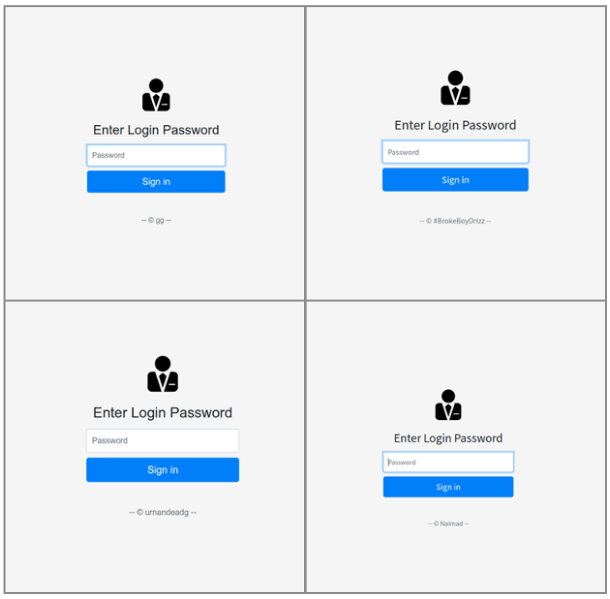


Fig. 7: Cracked copies of Kr3pto are easily discovered when looking at the admin panel

Dynamic kits such as Kr3pto are looking to take advantage of the lack of strong 2FA options, not only in the financial services space, but globally. The process used by Kr3pto to achieve this isn't new, but the fact it is becoming so widespread means there is a risk of it becoming commonplace in the near future. This means that financial institutions, as well as other critical consumer brands, need to adopt stronger 2FA/MFA alternatives as a means of protection and mitigation.

Robotos Targeting Corporate Users

We've just explored a phishing kit targeting banking, but what about the phishing kits that target corporate accounts? The types of phishing attacks commonly seen online can usually be split into two main categories: consumer and corporate. These are then subdivided. The subdivisions include social media, streaming media, gaming, etc. under the "consumer category," while kits targeting corporate accounts go after known corporate brands such as Dropbox, Office 365, OneDrive, and SharePoint.

Kr3pto is a consumer phishing kit, while the kit we're examining now, Ex-Robotos, is a corporate phishing kit.

The phishing kits targeting corporate accounts bring particularly high risk, because they expose access that extends beyond what they're targeting. Credentials compromised by corporate phishing kits instantly expose the account in question, such as office email or document storage. Unfortunately, most office workers reuse their passwords across multiple enterprise services and applications, and because of this, a single successful corporate phishing attack can place other assets at risk too, such as VPNs, payroll and human resources applications, and servers.

Making MFA Harder to Crack

With stronger types of MFA, it really comes down to moving away from SMS-based authentication and leveraging authenticators. For example, Google Authenticator offers time-based OTP (TOTP) and avoids SMS entirely as an OTP delivery channel. There is also Universal 2nd Factor (U2F), which is a challenge-response mechanism using standard public key cryptography techniques. YubiKey is the most commonly known option for U2F at present. More information about U2F is available at the FIDO Alliance website.

Ex-Robotos is the moniker chosen by a threat actor who has been developing and publishing a number of corporate phishing kits over the past few months. Like Kr3pto, their original code has been ripped and stolen by other threat actors who go by the names G66K, I.K. ZeuS, and EDBY-G66K-GOV. There are likely other rippers online using the Ex-Robotos code, but these are some of the more visible names circulating online.

```
<?php
/*
OFF365 V4 2020 by ExRobotos
CrackedBy: G66K
ICQ: [redacted]

NOTE: Sorry ExRobotos, Your Page Was Easy TO Cracked.
*/
error_reporting(0);include('blocker.php');include
function rndString($length=10){return substr(str_
$rndString1=rndString(7);$rndString2=rndString(8)
```

Fig. 8: G66K leaves a taunting message in the source code for Ex-Robotos

Not only do these rippers steal the code, they also leave taunts. G66K left comments in the source code of one kit, telling Ex-Robotos that his code was "easy" to crack. The reason the rippers targeted Ex-Robotos is ultimately unknown. However, Ex-Robotos used an API system to manage customers and validate kit activation, so it is likely the rippers cracked the kit to avoid paying for it.

The API management was supposed to ensure only the kits that were properly purchased could function, but there were clear flaws in the API design at one point, judging by the number of cracked copies in circulation.

Rise of the Ex-Robotos

Data from Akamai logs show that traffic to the Ex-Robotos phishing kit hit a strong surge in early February 2021.

January 31, 2021 –
15,978 hits to Ex-Robotos API

February 01, 2021 –
14,696 hits to Ex-Robotos API

February 02, 2021 –
10,861 hits to Ex-Robotos API

February 03, 2021 –
10,882 hits to Ex-Robotos API

February 04, 2021 –
8,388 hits to Ex-Robotos API

February 05, 2021 –
12,381 hits to Ex-Robotos API

155,240 hits
Jan 1–31, 2021

69,566 hits
Feb 1-12, 2021

Cracked or not, the danger that Ex-Robotos represents is hard to understate. Every day, thousands of victims globally are interacting with Ex-Robotos phishing kits in some form. According to data from the Akamai Intelligent Edge Platform, there were more than 220,000 hits to the API IP address used for Ex-Robotos over a span for 43 days. In fact, traffic to that address hit tens of thousands of hits per day on average between January 31 and February 5, 2021.

Fig. 9: A lure used by Ex-Robotos tells the victim they have received a new file

Crafting Lures and Launching Attacks

There are two distinct Ex-Robotos kits targeting corporate users. Both kits use basic but unique anti-detection techniques, demonstrating that the threat actor behind development put some effort into this. However, like most phishing-as-a-service offerings, Ex-Robotos just creates and sells the phishing kits, while their customers actually perform the attacks. As such, it is really hard to tell which campaigns are linked.

There are two lures being used by Ex-Robotos. One is a voicemail lure, and the other is centered on protected documents. Both kits, no matter what the lure is, will follow the same process of requesting the victim's password. Their username (email address), by function of the kit, is already populated in the login field.

Again, because of the lures used and the theming of the Ex-Robotos kits, the majority of the victims are corporate users, who release their corporate password into the threat actor's hands. Ex-Robotos targets organizations of all types and sizes, and the threat actors are mostly using known lists of targeted emails, which can be obtained for little to no cost on various criminal forums and legitimate marketing services.

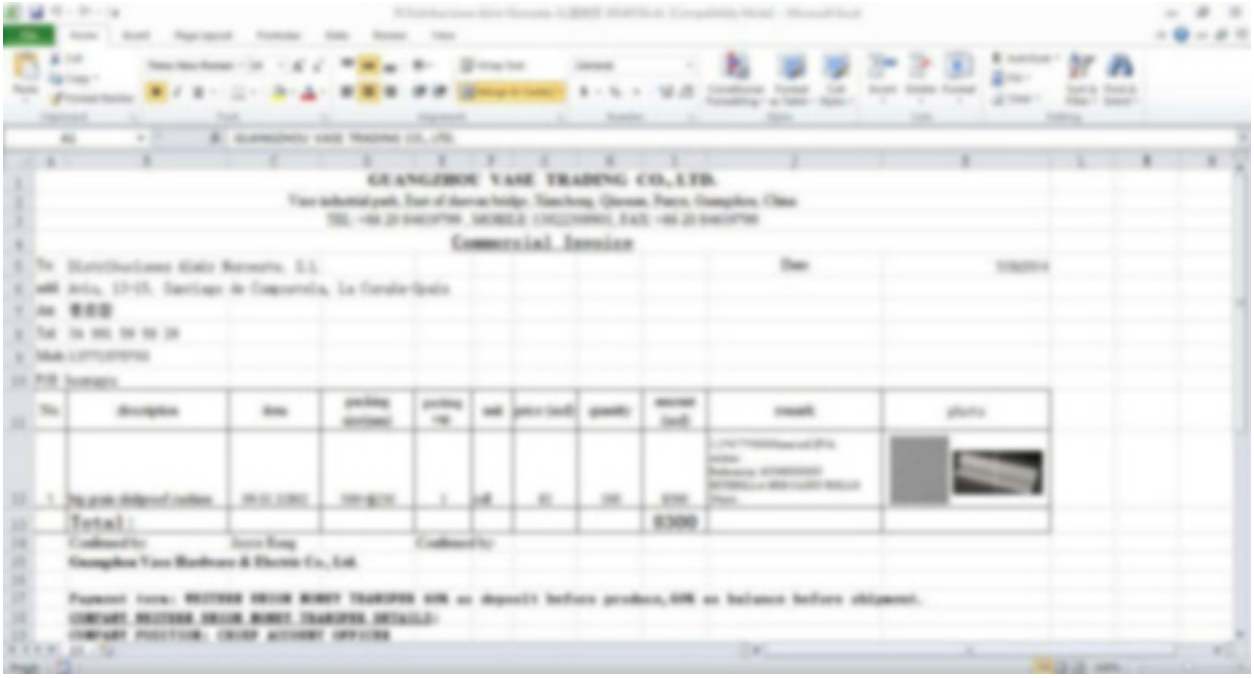


Fig. 10: The landing page of an Ex-Robotos attack, where the victim is presented with a password-protected corporate document

Another element of Ex-Robotos is the control mechanism. This allows the threat actor to limit who is able to view the landing page, by creating a pass list for email addresses. Thus, only addresses that appear on the list are able to engage with the landing page used for the attack. What this does is make the Ex-Robotos kits perfect for spear-phishing attacks, where victims are targeted directly and often repeatedly, using various lures.

```
$Resetlogs = true;
//clears all logs
$ResetAllow = false;
//reset list of blocked ips and emails and regions (allow all except bot)
$onlylistemails = false;
//allow only a list of emails (put emails in EMAILS.txt. Each email in line)
$onlyonetimeuse = false;
//true will make page become died after the user put all passwords
$limitedarea = false;//"[redacted]";
//for limited ip or country--
//put here your allowed ips and ip ranges
//exemple:"[redacted]"
$base64encodeData = true;
//true OR false(using base64encoded email value in link or not)
```

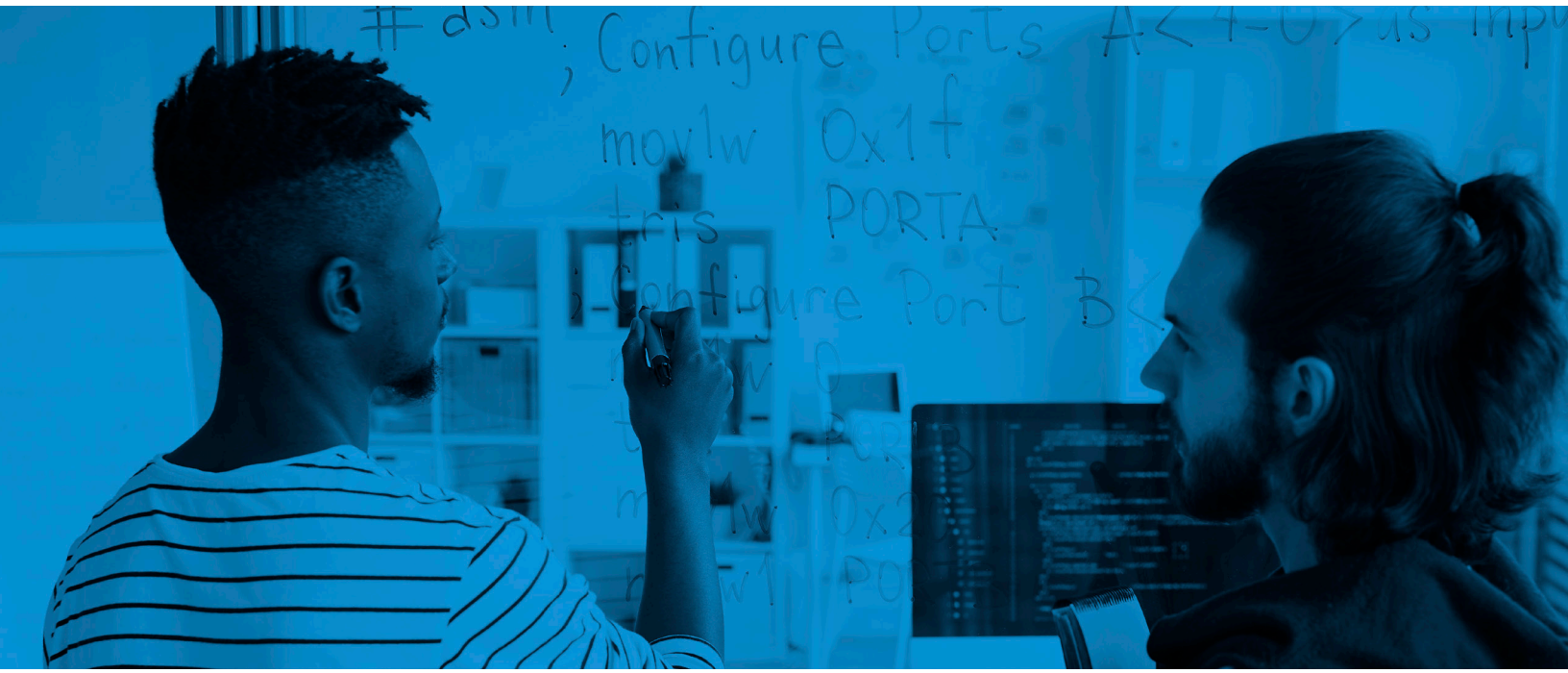
Fig. 11: The configuration file for Ex-Robotos has several options that are geared toward spear phishing

```
";
    $logs           = "
+ ------------OFFICE365 Scmpage V2 2019 by Ex-Robotos----------+
|OFFICE365 V2 by Ex-Robotos
|Information: New Logs
|Email : $email - Password : $password
|IP Address: $remoteIP
|Country: $Ex_country Country Code: $Ex_countrycode
|Region: $Ex_state City: $Ex_city Postal Code: $Ex_postal
|Date: $date Browser: $browser
+ ------------------------------------------------------------+
";
```

Fig. 12: Ex-Robotos source code showing the data collection function

In addition to password collection, Ex-Robotos kits will do some data enrichment, such as collection of country, region, city, state, postal codes, and browser details, as well as IP information. This is so the threat actor can choose proxy connections that are close to, if not directly located near, the victim. Most organizations do geolocation checking and will block login attempts if there is any suspect behavior, such as an employee from the U.S. logging into the network from an IP out of France.

Once the compromised data is collected, it needs to be offloaded somewhere so that the threat actor can access it. Ex-Robotos kits offer the ability to email the data, as well as store it locally on the web server in a text file.



Credential Poisoning

While investigating logs related to Ex-Robotos attacks, WMC Global discovered an extensive credential poisoning campaign. Credential poisoning is frequently carried out by online vigilante groups. These groups attempt to flood a phishing website with fake usernames and passwords in an attempt to dilute the logs with garbage, making it nearly impossible for the threat actor to work through all the data to find real victims.

However, threat actors know this activity occurs and use several methods to prevent it from happening. Some will use IP blocks, which kick in after data is submitted to the phishing page, preventing repeat visits from the same source. More advanced threat actors leverage a live check on the credentials. Some kits will not record if validation fails, prompting the victim to re-enter their data instead, or the kit will add a line to the logs confirming whether the credentials passed or failed the automated login attempt.

In the case of Ex-Robotos, there is no credential validation function, but there is an option to block victims after data submission. The ongoing poisoning campaign is being operated by an unknown group, and it uses legitimate emails from several known companies, often submitting addresses belonging to executives or high-profile users such as HR leadership, finance staff, and corporate directors.

Those responsible for the poisoning campaign have made some errors, which we will not disclose here — but needless to say, their methods are easily detected, enabling threat actors to filter the junk data.

The threat posed by corporate phishing kits, as mentioned previously, cannot be minimized. Once the criminals have access to verified corporate credentials, the number of attacks and additional scams they can run is boundless. Often, corporate phishing attacks are the lead-up to larger, more devastating attacks, such as business email compromise (BEC), ransomware, and data breaches. Organizations can lower the attack surface by ensuring that staff use MFA whenever possible, such as Google Authenticator or Duo Security, and that phishing awareness campaigns happen regularly.

> ***Often, corporate phishing attacks are the lead-up to larger, more devastating attacks...***

Looking Forward

2020 was a challenging year, but just because it's 2021 doesn't mean that criminals will slow down. Phishing kits like Ex-Robotos and Kr3pto are just the tip of the iceberg — hundreds of kits are developed and circulated daily. The attacks are relentless. The phishing economy as a whole has been growing exponentially year over year, as developers leverage the same web technologies and techniques that enable businesses to remain agile and ahead of the curve.

Consider this: 193 billion credential stuffing attacks and 6 billion web attacks aren't just big numbers or a testament to Akamai's increased visibility. They represent the hard fact that criminals are only going to keep targeting organizations that don't leverage authentication defenses, such as MFA and 2FA. The reason criminals are going after those organizations in the first place? Targeting organizations that do leverage 2FA and MFA isn't worth the energy or effort for most low-level, opportunistic attackers.

Again, layered defenses and segmentation make web attacks costly for opportunistic attackers, which causes them to move on. While many view it as simply a marketing term, the concepts behind what makes Zero Trust "Zero Trust" are practical concepts that have existed within the security industry for years. Limit and control access, enforce multiple layers of authentication, and layer defenses so that incident detection is as quick as possible. Because the faster you can detect a problem, the sooner it can be resolved.

Stay safe!

Methodologies

Web Application Attacks

This data describes application-layer alerts generated by Kona Site Defender and Web Application Protector. The products trigger these alerts when they detect a malicious payload within a request to a protected website or application. The alerts do not indicate a successful compromise. While these products allow a high level of customization, we collected the data presented here in a manner that does not consider custom configurations of the protected properties.

The data was drawn from Cloud Security Intelligence (CSI), an internal tool for storage and analysis of security events detected on the Akamai Intelligent Edge Platform. This is a network of approximately 300,000 servers in 4,000 locations on 1,400 networks in 135 countries. Our security teams use this data, measured in petabytes per month, to research attacks, flag malicious behavior, and feed additional intelligence into Akamai's solutions.

DDoS

Prolexic defends organizations against DDoS attacks by redirecting network traffic through Akamai scrubbing centers, and only allowing the clean traffic forward. Experts in the Akamai security operations center (SOC) tailor proactive mitigation controls to detect and stop attacks instantly, and conduct live analysis of the remaining traffic to determine further mitigation as needed.

DDoS attack events are detected either by the SOC or the targeted organization itself, depending on the chosen deployment model – always-on or on demand – but the SOC records data for all attacks mitigated. Similar to web application traffic, the source is determined by the source of the IP traffic prior to Akamai's network.

Credential Abuse

Credential abuse attempts were identified as unsuccessful login attempts for accounts using an email address as a username. We use two algorithms to distinguish between abuse attempts and real users who can't type. The first is a simple volumetric rule that counts the number of login errors to a specific address. This differs from what a single organization might be able to detect because Akamai is correlating data across hundreds of organizations.

The second algorithm uses data from our bot detection services to identify credential abuse from known botnets and tools. A well-configured botnet can avoid volumetric detection by distributing its traffic among many targets, using a large number of systems in its scan, or spreading out the traffic over time, just to name a few evasion examples.

This data was also drawn from the CSI repository. One customer with significant attack volume was removed from this data set prior to 2020, due to not having a full year of data.

Phishing URL Data

WMC Global used its proprietary data to assist in the production of this report. Data originated from multiple unique sources such as email data, mobile SMS data, and active threat hunting to detect, analyze, and tag millions of URLs a day. WMC Global also uses a link scanning and attribution system called UrSULA, which enables it to scan tens of millions of URLs every second and assert whether the URL is malicious or not. Given the range of data sources available to WMC Global; the fast, automated, and accurate capabilities of UrSULA; and the skilled threat hunting team; WMC Global is able to offer in-depth knowledge on credential phishing campaigns, enabling organizations to understand the threats posed by threat actors and giving them the ability to block and remediate an attack before there is impact to their clients.

Phishing Kit Data

WMC Global has access to the largest private collection of phishing kits, enabling it to have the deepest understanding of credential phishing sites. Using its unique KIT Intelligence Platform, it is able to process, analyze, and cluster phishing kits to enable its analysts to dive deep into the data more efficiently. The KIT Intelligence Platform is able to take a phishing kit and break it apart into each element, allowing for a safe way for an analyst to read the code and assess the threat. The system also allows for searching through all the phishing kits, which enables a simple way to view code overlaps – meaning threat actors can be tracked down with ease.

Credits

Akamai

Martin McKeay
Editorial Director

Steve Ragan
Senior Technical Writer, Editor

Amanda Goedde
Senior Technical Writer, Managing Editor

Chelsea Tuttle
Senior Data Scientist

Georgina Morales Hampe
Project Management, Creative

Shivangi Sahu
Program Management, Marketing

WMC Global

Ian Matthews
CEO

Elizabeth Snead
Senior Product Manager

Jake Sloane
Senior Threat Hunter

More State of the Internet / Security

Read back issues and watch for upcoming releases of Akamai's acclaimed State of the Internet / Security reports. akamai.com/soti

More Akamai Threat Research

Stay updated with the latest threat intelligence analyses, security reports, and cybersecurity research. akamai.com/threatresearch

Access Data from This Report

View high-quality versions of the graphs and charts referenced in this report. These images are free to use and reference, provided Akamai is duly credited as a source and the Akamai logo is retained. akamai.com/sotidata

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 05/21.