2020 PHISHING AND FRAUD REPORT

Phishing During A Pandemic

AUTHORS:
David Warburton, F5 Labs

CONTRIBUTORS:
Paul Dockter, F5 SOC
Avihai Sitbon, F5 Malware Researcher
Carlos Asuncion, Shape Security

EDITOR:
Debbie Walkowski

DATA PARTNERS:
F5 SIRT
Webroot, an OpenText Company

F5 LABS

Table of Contents

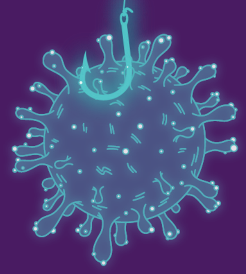
Executive Summary

Phishing remains a popular method of stealing credentials, committing fraud, and distributing malware. But what appears on the surface to be a juvenile form of cybercrime can be, in practice, a well-orchestrated, multi-faceted, and sustained attack campaign by organized crime groups. From finding victims and creating phishing sites, to harvesting and fraudulently using victims' credentials, it can be difficult to build a complete picture of the end-to-end process. We focus our report on how fraudsters are building and hosting their phishing sites, and the tactics they use to remain hidden. Using insight from Shape Security, we also show how quickly cybercriminals are making use of their stolen goods.

WE FOCUS OUR REPORT ON HOW FRAUDSTERS ARE BUILDING AND HOSTING THEIR PHISHING SITES, AND THE TACTICS THEY USE TO REMAIN HIDDEN

This year's Phishing and Fraud report examines five years' worth of phishing incidents from the F5 Security Operations Center (SOC), deep dives into active and confirmed phishing sites supplied by OpenText's Webroot® BrightCloud® Threat Intelligence, and analyzes darkweb market data from Vigilante. Together, these help build a comprehensive and consistent picture of the world of phishing.

In our 2019 Phishing and Fraud Report, we noted a significant abuse of free and automated services, such as blogging platforms and free digital certificate services. Fraudsters made heavy use of automation with very little, if any, financial outlay. We saw emerging use of encryption with just over half of all sites leveraging HTTPS, and attackers were creating lengthy and deceptive web addresses (URLs) in order to appear genuine and confuse their victims.



15%

INCREASE IN PHISHING INCIDENTS IN 2020

The past twelve months has been not a revolution in the attackers' methods but an evolution, and 2020 is on target to see a 15% increase in phishing incidents compared with last year. This year we found that phishing incidents rose by a staggering 220% compared to the yearly average during the height of global pandemic fears. Fraudsters were quick to seize upon the confusion and we saw large spikes in phishing activities that closely coincide with various lockdown rules and the increase in homeworking. Using certificate transparency logs, we found that at its peak, there were almost 15,000 active certificates using "covid" or "coronavirus" in their names. On the topic of encryption, the use of HTTPS also rose sharply across all phishing sites with an impressive 72% making use of digital certificates and TLS encryption. The dramatic increase in phishing activity at the beginning of lockdown could well be a factor in the sharp rise of stolen payment cards discovered in May and June of this year. The number of cards of seven major global banks found on darknet markets was almost double a similar peak period in 2019.

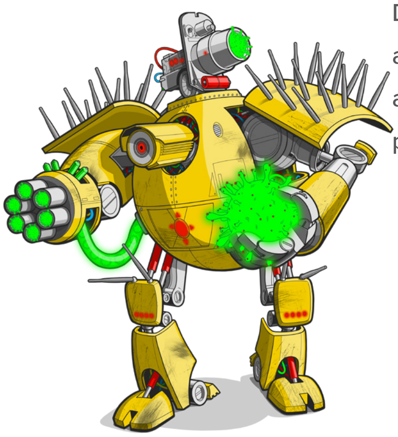
WE FOUND THAT PHISHING INCIDENTS ROSE BY A STAGGERING 220% COMPARED TO THE YEARLY AVERAGE DURING THE HEIGHT OF GLOBAL PANDEMIC

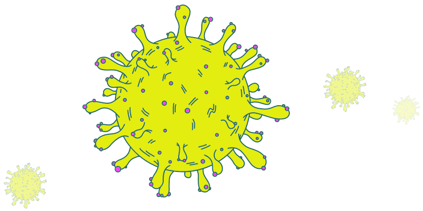
Fraudsters are becoming more creative with the names and locations of their phishing sites. Attempting to create ever more realistic website addresses, we found that 55% of phishing sites made use of target brand names and identities in their URLs. We tracked theft of credentials through to their use in active attacks and found that criminals were attempting to use them within four hours. In some cases, the attacks occurred in real time.

Vulnerable websites continue to present an opportunity for fraudsters to host their phishing pages on a reputable URL, for free. We found that WordPress sites alone accounted for 20% of generic phishing URLs.

This year we also found that Office 365 continues to present a rich and compelling target for attackers with fraudsters employing new tactics such as "consent phishing". And an increasing number of phishing sites are using evasion techniques to avoid detection and inspection by targeted businesses and security researchers.

Despite the continued growth of phishing attacks, security controls and user training are failing to adequately combat it. Fraudsters know that the way to make a quick buck isn't to spend months attempting to breach an organizations security, it's simply to ask nicely for the username and password so they can walk right in through the front door.



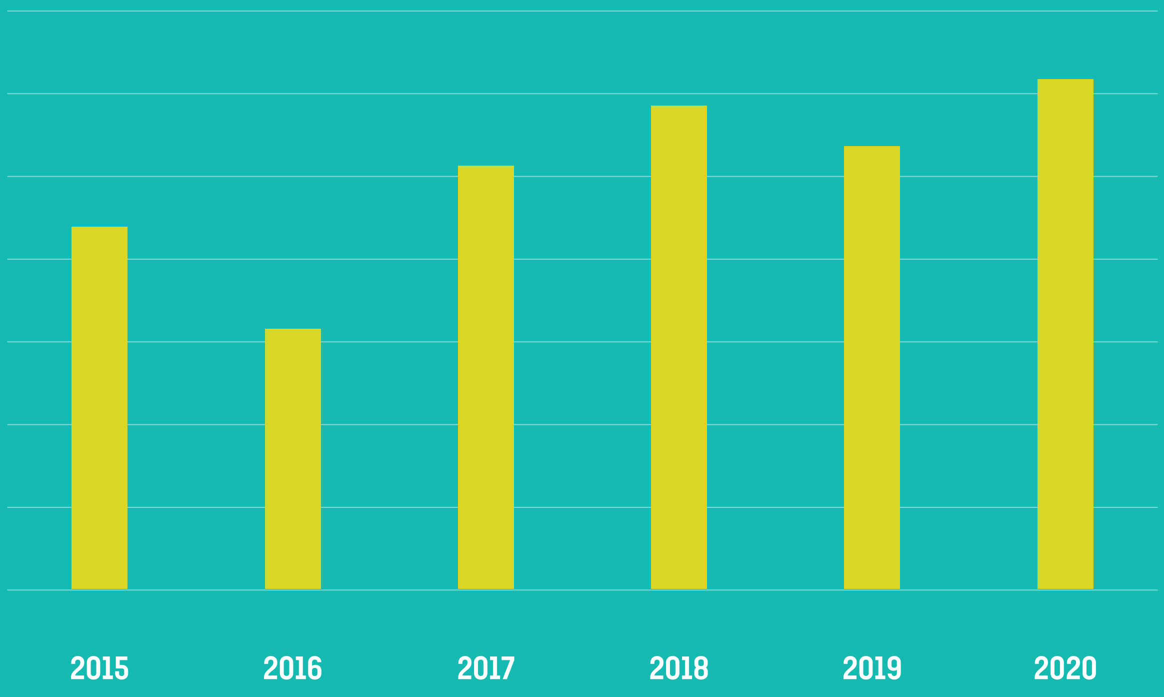


Introduction

Phishing, the email focused form of social engineering, shows no sign of abating. It remains just as popular with organized cybercrime as it is with nation states for one simple reason: it works. The number of phishing incidents in 2020 is projected to increase by 15% compared with last year, according to data from the F5 Security Operations Center (SOC) (see Figure 1). F5 Labs' 2020 Application Protection Report found that 52% of all breaches in the US were due to failures at the access control layer. These include credential theft, brute force login attempts, and phishing. Across the pond, data released by the UK's Information Commissioner's Office (ICO), showed that phishing was the number one cause of cyber related data breach for their reporting period covering April 2019 to March 2020, accounting for 28% of all cases.[i] The trend continues all over the world. Numbers from the Office of the Australian Information Commissioner (OAIC) show that phishing holds the top spot in malicious cyber incidents, accounting for 36% of all cases reported to them.[ii] Theft of credentials, one of the most common initial attack vectors for cybercriminals, is a close second and is responsible for 29% of all incidents (July 2019 to June 2020).

FIGURE 1. PHISHING INCIDENTS DEALT WITH BY F5's SECURITY OPERATIONS CENTER

To protect customer confidentiality, we do not mention specific organizations or divulge numbers. We instead compare increase levels in incident reports.



Phishing is now such a problem that the 2020 Verizon Data Breach Investigations Report (DBIR) noted the use of malware and trojans had dropped significantly and that "attackers become increasingly efficient and lean more toward attacks such as phishing and credential theft."[iii] Europol's latest Internet Organised Crime Threat Assessment (IOCTA) report stated, "Social engineering and phishing remain a key threat," and that "both demonstrate a significant increase in volume and sophistication."[iv] Yet, while the organized cybercriminal element are indeed becoming far more skilled in their use of social engineering, using multi-vector attacks and intercepting SMS tokens, phishing has dramatically increased due to the ease with which it can be conducted. Phishing kits and Phishing-as-a-Service, not to mention the ease with which personal data can be obtained, all mean that virtually anyone can start a phishing campaign with very little prior knowledge. Since likelihood is a factor in calculating risk, we must assume that our risk of being phished is now greater than ever.

PHISHING HAS DRAMATICALLY INCREASED DUE TO THE EASE WITH WHICH IT CAN BE CONDUCTED

Non-cash payment fraud, such as credit card theft, skimming, or phishing, is commonly used to enable the majority of other cyber-dependent crime, such as extortion, theft of data, and deployment of malware. Advanced persistent threat (APT) groups have long been known to conduct active cyber espionage campaigns. Social engineering of APTs' victims via email and social media phishing campaigns is commonly the first step in the attack chain. In September 2020, a new campaign by the Iranian-linked Charming Kitten APT combined targeted spear-phishing via WhatsApp with bogus LinkedIn profiles in order to create believable back stories. Their aim was to trick the victim into downloading malware or harvest the victim's credentials.[v]

SOCIAL ENGINEERING OF APTs' VICTIMS VIA EMAIL AND SOCIAL MEDIA PHISHING CAMPAIGNS IS COMMONLY THE FIRST STEP IN THE ATTACK CHAIN

Business email compromise (BEC)—spear-phishing that targets staff members who have access and the authority to transfer money—is on the rise as attackers show an increased understanding of internal business relationships and processes. The second-quarter 2020 report from the Anti-Phishing Working Group (APWG) showed that the average wire transfer attempt was more than $80,000, with one specific threat actor targeting companies for an average of $1.27 million.[vi]

Despite many advanced tools, techniques, and procedures (TTPs), many phishing attacks are simple in nature and succeed because of poor security controls and lack of awareness by users.

How Cybercriminals Capitalized on COVID-19 in 2020

Always keen to hook onto emotive topics, cybercriminals were quick to capitalize on the global outbreak of SARS-CoV-2, colloquially known as Coronavirus or COVID-19. While millions of people struggled to learn the real facts about the pandemic from world leaders, the morally absent cybercriminal community saw their opportunity. Phishing emails began hitting inboxes around mid-March with subject lines such as “Covid-19 in your area?” and “Message from the World Health Organization.”

Phishing Subject Line Examples

- Covid-19 in your area? Please confirm your address
- Click here for COVID-19 vaccinations
- Get your COVID-19 CARES Act relief check here
- Counterfeit Respirators, sanitizers, PPE
- Fake cures for COVID-19
- Message from the World Health Organization
- Message from the Centers for Disease Control and Prevention
- Click here for Coronavirus-related information
- Donate to these charitable organizations.
- Message from Local hospital— Need patient data for COVID-19 testing
- COVID 19 Preparation Guidance
- 2019-nCoV: Coronavirus outbreak in your city (Emergency)
- HIGH-RISK: New confirmed cases in your city
- Coronavirus (2019-nCoV) Safety Measures

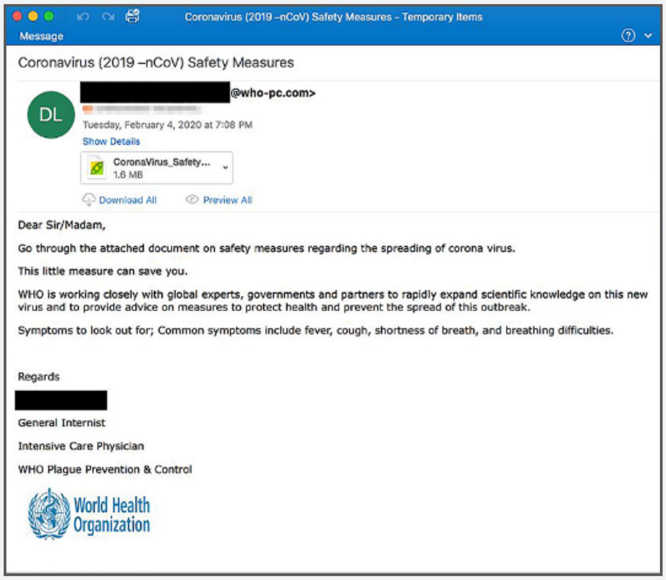
The APWG reported that targets were predominantly “workers, healthcare facilities and the recently unemployed.”[vii] Figures 2 and 3 show just two samples of many pandemic-related phishing emails F5 Labs has seen.

Three primary objectives for COVID-19 related phishing emails became apparent. Fraudsters focused their efforts on:

- Asking for donations to fake charities
- Credential harvesting
- Malware delivery

While criminals seized on the opportunity to spoof login and download pages for increasingly popular web conferencing apps, such as Zoom, Skype, and WebEx, it’s remarkable how *unremarkable* many of these attacks really were. Europol’s IOCTA 2020 report summarizes this well stating, “COVID-19 demonstrated how cybercrime—at its core—remains largely the same but criminals change the narrative.”[viii] This echoes the previous discovery by F5 Labs of a Mirai botnet lazily cloned to include references to COVID-19.

FIGURE 2. A PHISHING EMAIL THAT USED FEAR OF THE PANDEMIC TO HOOK ITS VICTIMS



Coronavirus (2019 –nCoV) Safety Measures

[redacted]@who-pc.com>

Tuesday, February 4, 2020 at 7:08 PM

CoronaVirus_Safety... 1.6 MB

Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of corona virus.

This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

[redacted]

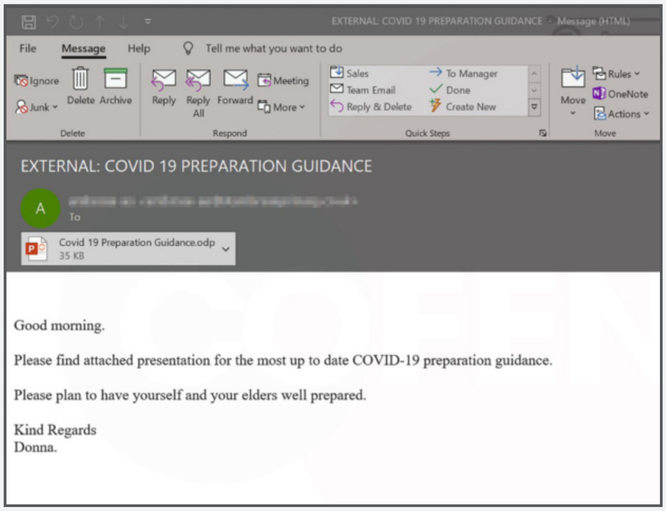
General Internist

Intensive Care Physician

WHO Plague Prevention & Control

World Health Organization

FIGURE 3. A COVID-19 RELATED PHISHING EMAIL WITH A MALICIOUS POWERPOINT PRESENTATION ATTACHED



EXTERNAL: COVID 19 PREPARATION GUIDANCE

Covid 19 Preparation Guidance.odp 35 KB

Good morning.

Please find attached presentation for the most up to date COVID-19 preparation guidance.

Please plan to have yourself and your elders well prepared.

Kind Regards
Donna.

The number of phishing incidents reported to the UK ICO for each quarter of 2019 and 2020 averaged 289, while new figures, released for the months covering April to June 2020, show a sharp decline with only 185 confirmed cases. The F5 Security Operations Center (SOC) saw a similar trend, with initial phishing statistics broadly following patterns of previous years but with a large spike around the start of 2020, a slump between March and April, and another significant rise over the spring and early summer months (see Figure 4).

Across the SOC datasets for the months of July to September, we found 320 unique malicious domains making use of the specific terms "covid" or "corona" in their URLs. Many other malicious sites used deliberate misspellings or simply used unrelated domain names for their attacks.

Using certificate transparency logs, we can also search for specific words or values within HTTPS certificates. It is no surprise that when the pandemic was headlining every news outlet in March, the number of certificates created that month with the words "covid" or "corona" peaked at 14,940 (see Figure 5).

Security practitioners are generally well aware of how phishers bait and hook their victims by using provocative topics, but if these trends tell us anything, it's that end users—our staff and our customers—need to know this. Phishing awareness training must drive home the message that attackers are quick to jump onto new trends. Users need to be extra vigilant watching for email, voicemails, and text messages that appear to be related to widely discussed topics in the media or popular culture.

PHISHING AWARENESS TRAINING MUST DRIVE HOME THE MESSAGE THAT ATTACKERS ARE QUICK TO JUMP ONTO NEW TRENDS

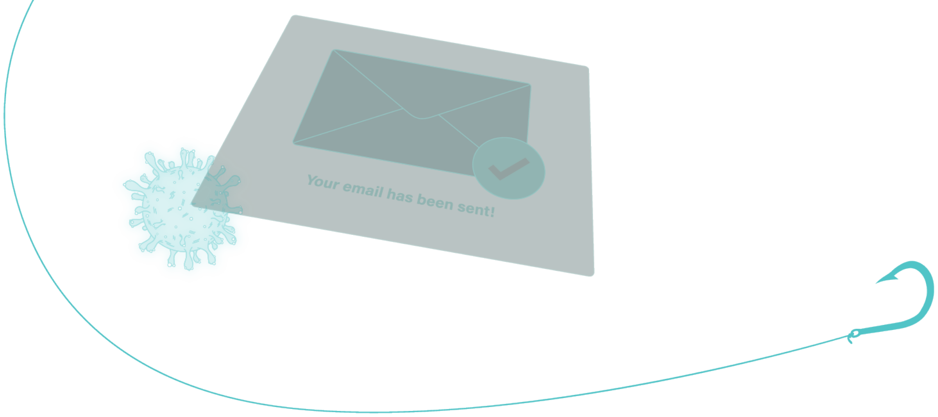


FIGURE 4. PHISHING INCIDENTS DEALT WITH BY F5 SOC

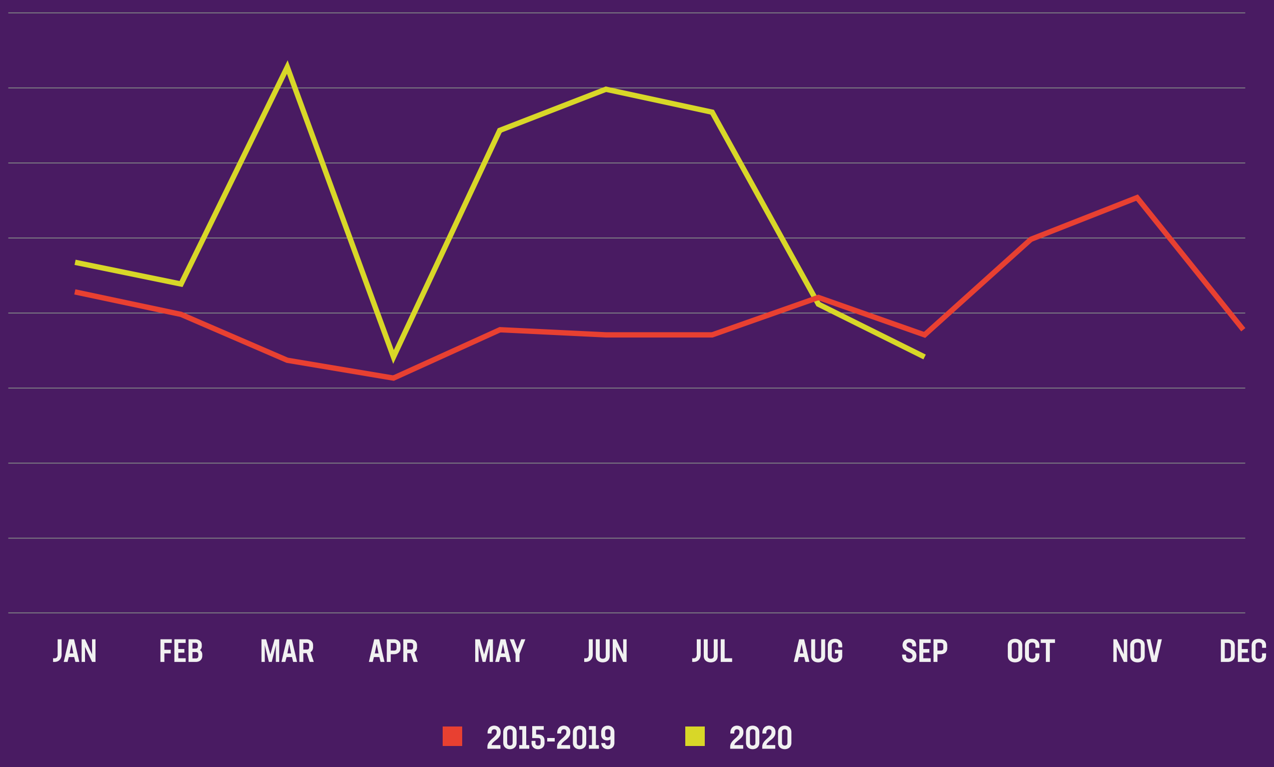
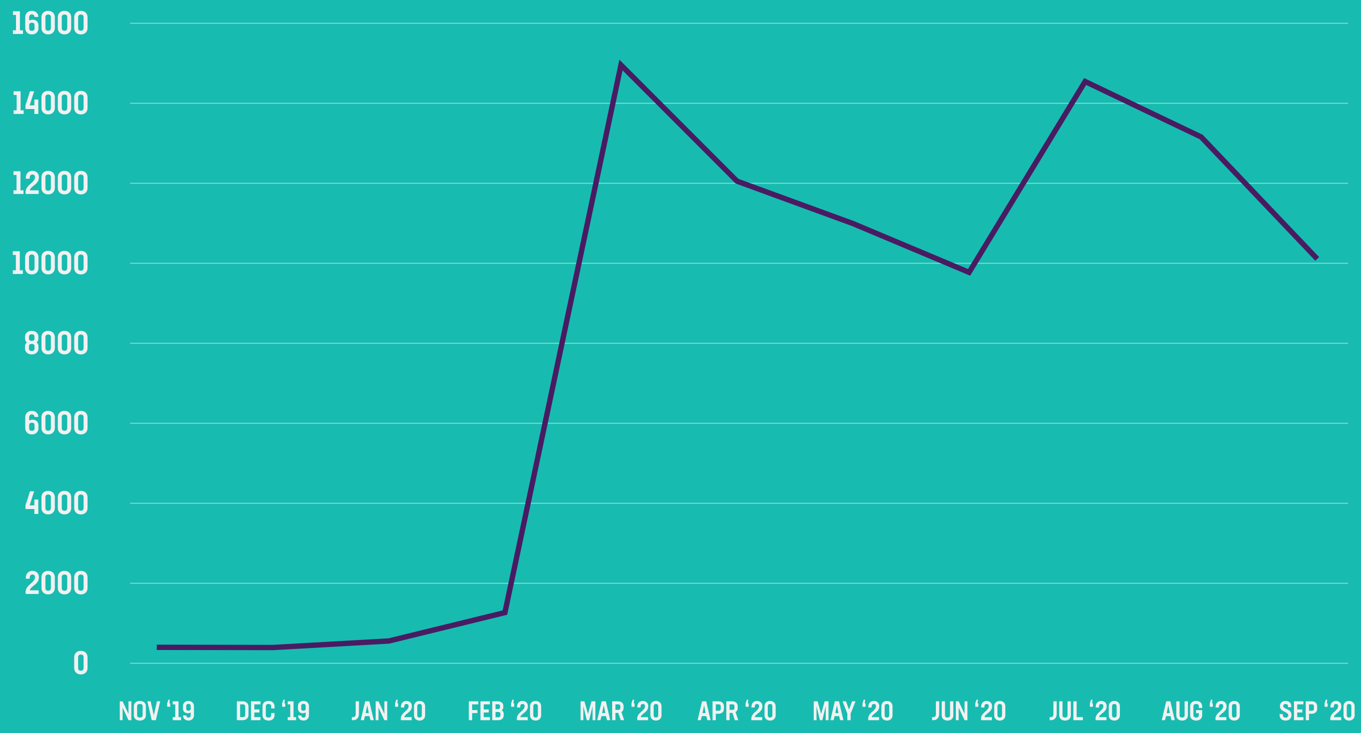
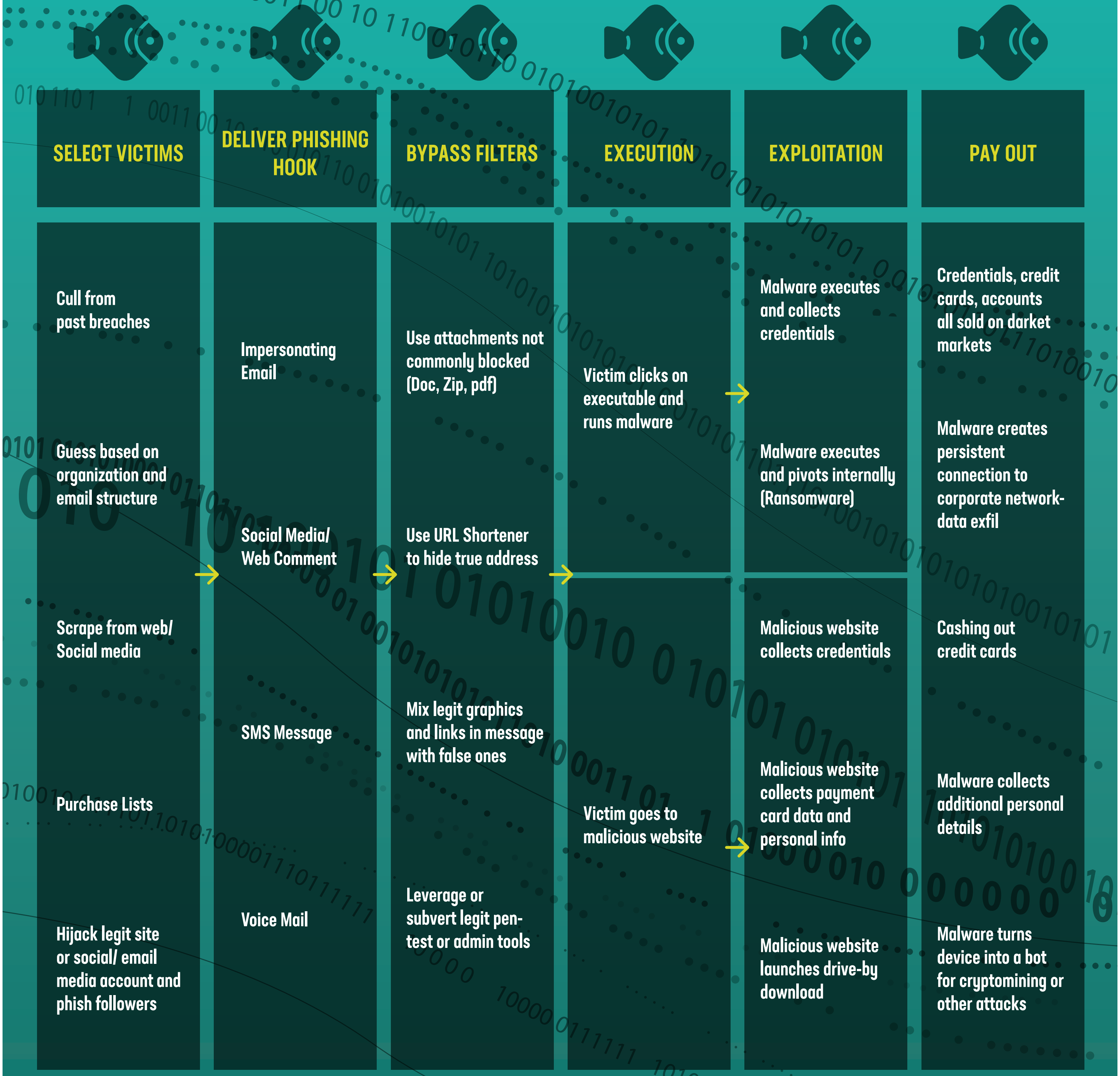


FIGURE 5. RATE OF NEW CERTIFICATES CONTAINING “COVID” OR “CORONA.”

DATA OBTAINED FROM CENSYS.IO



STEPS IN A PHISHING ATTACK



SELECT VICTIMS

- Cull from past breaches
- Guess based on organization and email structure
- Scrape from web/ Social media
- Purchase Lists
- Hijack legit site or social/ email media account and phish followers

DELIVER PHISHING HOOK

- Impersonating Email
- Social Media/ Web Comment
- SMS Message
- Voice Mail

BYPASS FILTERS

- Use attachments not commonly blocked (Doc, Zip, pdf)
- Use URL Shortener to hide true address
- Mix legit graphics and links in message with false ones
- Leverage or subvert legit pen-test or admin tools

EXECUTION

- Victim clicks on executable and runs malware
- Victim goes to malicious website

EXPLOITATION

- Malware executes and collects credentials
- Malware executes and pivots internally (Ransomware)
- Malicious website collects credentials
- Malicious website collects payment card data and personal info
- Malicious website launches drive-by download

PAY OUT

- Credentials, credit cards, accounts all sold on darket markets
- Malware creates persistent connection to corporate network- data exfil
- Cashing out credit cards
- Malware collects additional personal details
- Malware turns device into a bot for cryptomining or other attacks

The Business of Phishing

There are many ways to phish, and the tools and tactics required are often determined by what the attacker is aiming to catch. As we covered in F5 Labs' 2019 Phishing and Fraud Report, the three broad methods of phishing are:

- General, indiscriminate, in which the attacker targets many unrelated victims knowing that they are likely to get a few bites
- Semi-targeted, in which attacks are focused against a specific organization or group
- Spear phishing, in which a specific individual (often C-level or IT administrator) is directly targeted.

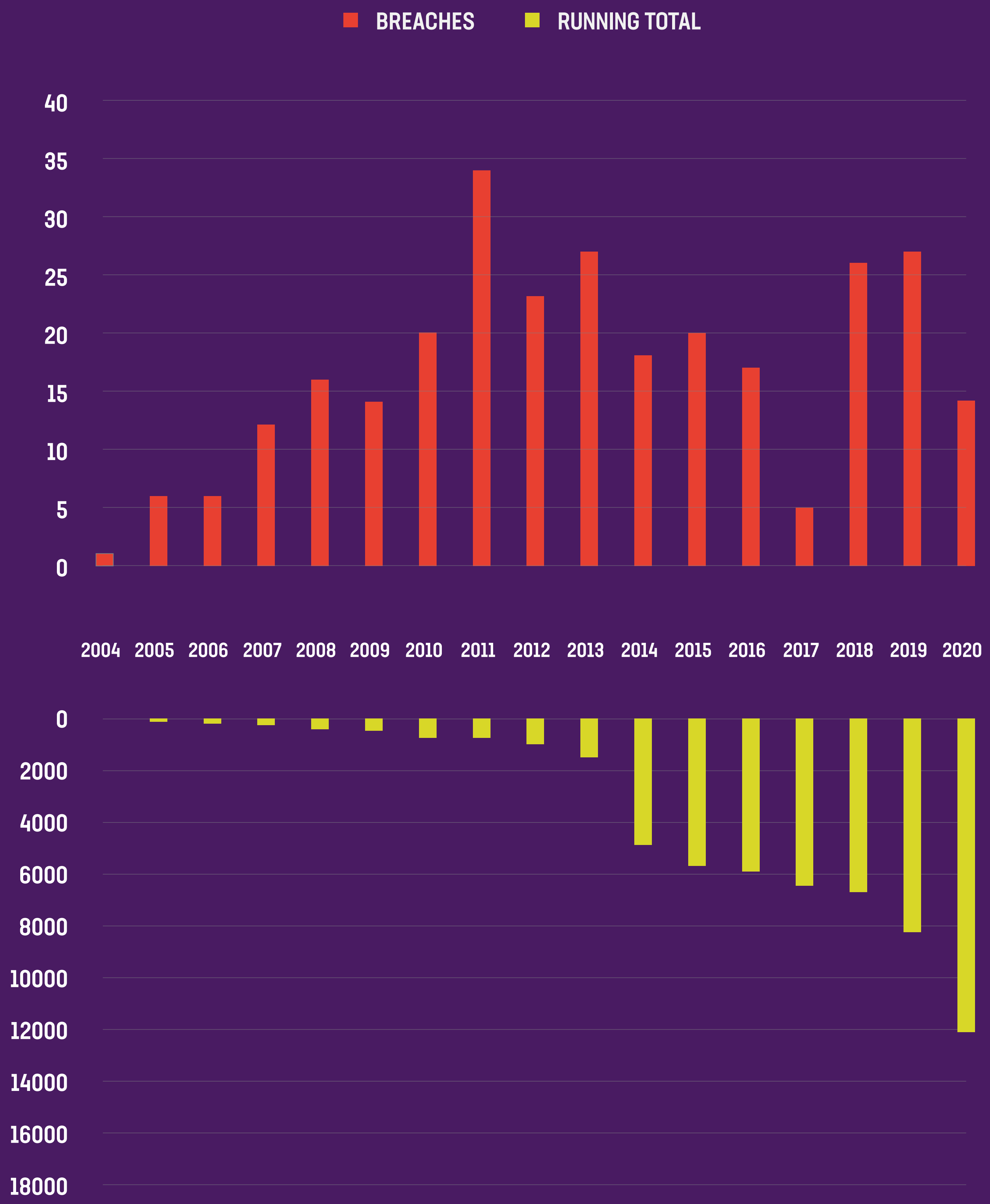
While the catch (the pay-out) might be different between phishing campaigns (some attackers are looking to harvest credentials while others want to distribute malware), the commonality is that fraudsters use one or more social engineering tactics to circumvent a victim's critical thinking. In a 2013 paper, *A Study of Social Engineering in Online Frauds*, the authors found the five most common methods of persuasion used were authority, urgency, fear/threat, politeness, and formality.[ix] In 100% of those cases, the cybercriminal used authority, and 71% of phishing emails added a sense of urgency. Whether it be a missed package delivery, a deadline for a competition, or threat of imminent "legal action," fraudsters know that persuading us to rush increases the likelihood that we will not logically evaluate the request. This year we've very much seen this to hold true with the huge jump in phishing traffic around the periods of national pandemic lockdowns and many examples of emails claiming to have information about the virus.

Phishing Objectives

Social engineering, and primarily phishing, is often used as an enabler of both newer cyber-dependent crime (for example, ransomware and website compromise) as well as cyber-enabled crime (such as fraud and theft). Here, we focus on two of the most common objectives for fraudsters: credential harvesting and financial fraud.

FIGURE 6. COUNT OF DATA BREACH INCIDENTS PER YEAR OVERLAYING THE NUMBER OF CUMULATIVE DATA RECORDS BREACHED

(displaying only incidents with known number of records breached)



Credential Harvesting

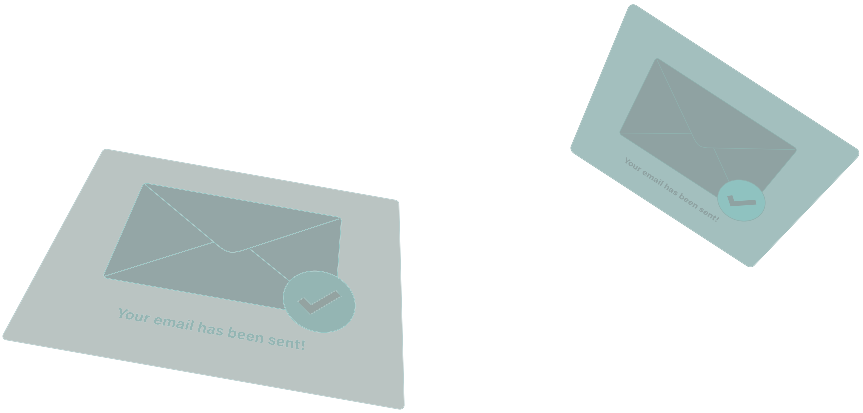
Usernames, email addresses, and passwords can often be the actual target of the fraudster, with stolen credentials commonly selling in bulk on darknet markets. These data sets of stolen credentials are purchased by other organized crime groups to enable others to carry out activities such as credential stuffing attacks.

More often, however, credentials are used to accomplish further objectives such as the theft of intellectual property or committing financial fraud. Attackers rarely have a problem obtaining usable credentials. Shape Security's 2018 Credential Spill Report found that 2.3 billion credentials were breached in 2017.[x] And 2017 was, according to Wikipedia, a quiet year for data breaches.[xi] Figure 6 shows the number of data breach incidents per year compared with the cumulative number of records breached. Despite a fluctuating number of incidents from year to year, the total number of records lost or stolen appears to be growing almost exponentially.

Office 365 Provides a Rich Target

Microsoft's incredibly popular email, productivity, and collaboration platform, Office 365, is a prime target for attackers. Once credentials have been captured, attackers have a multitude of options open to them. They might choose to send more fraudulent emails, now with the benefit of having them appear to come from a genuine corporate account. This same Office 365 account is likely to have access to SharePoint and OneDrive, which could provide direct access to intellectual property and sensitive data. The worst-case scenario might involve the compromised account being a member of a privileged access group, which then gives the attacker the ability to modify access privileges for the Office 365 platform itself.

A common tactic to phish for Office 365 credentials is to send a victim an email claiming that a Word or Excel document has been shared with them. To retrieve it, the victim must authenticate to the (spoofed) Office 365 website.



Consent Phishing

Now that businesses are starting to better secure their credentials (by federating user accounts, performing device posture checks, and applying MFA), fraudsters are beginning to shift their targets. With credentials becoming harder to steal, fraudsters are asking the victim for direct access to their account in an attack called *consent phishing*.

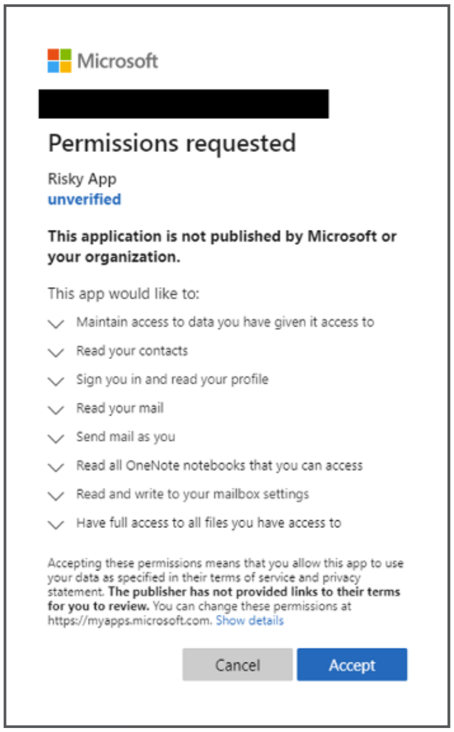
There are hundreds of mobile and desktops apps that promise to tidy your inbox, organize your contacts, or provide some incredibly useful new productivity feature. To use these apps, all you have to do is download it to your phone or laptop and authorize it to connect to your Gmail or Office 365 account.

The process for authorizing apps to your email or productivity platform is as follows:

1. Tell your new app of choice what platform you use, for example, Office 365
2. Your app then directs you to a login page for your Microsoft account
3. You authenticate to Microsoft by entering your credentials
4. Finally, you see a page, such as the one shown in Figure 7, in which you accept the permissions being requested by the app

FIGURE 7. GRANTING AN APP PERMISSION TO ACCESS YOUR MICROSOFT ACCOUNT.

Image credit: Microsoft



[redacted]

Permissions requested

Risky App
unverified

This application is not published by Microsoft or your organization.

This app would like to:

- Maintain access to data you have given it access to
- Read your contacts
- Sign you in and read your profile
- Read your mail
- Send mail as you
- Read all OneNote notebooks that you can access
- Read and write to your mailbox settings
- Have full access to all files you have access to

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

You might assume you've just provided your credentials to your newly downloaded app. You haven't. Instead, you've told Microsoft to hand the app a special token that grants it (often) indefinite and (commonly) unlimited access to your email as well as your entire Office 365 or Google account. Not surprisingly, criminals are abusing this to gain fraudulent access to Office 365 and Gmail accounts. Fraudsters correctly assume that many everyday users of these platforms don't fully read the permissions or, very likely, have no idea what they really mean and, since so many people now use these platforms, the fraudster's net can be cast far and wide.

Financial Fraud

Generic phishing campaigns often ask victims to hand over cash in order to claim a prize or to donate money to a charity. Often these scams trick visitors into making a one-time donation to a non-existent charity or by getting them to sign up for regular direct debits. Semi-targeted phishing attacks, however, will go after customers of a specific bank or service and aim to steal their payment card details for later use. These campaigns frequently ask victims for payment card details as well as login credentials. Not only can the card details help authenticate the criminal to the victims' online accounts, they can also be resold on dark web markets.

Using information supplied by threat intelligence firm Vigilante, we analyzed stolen payment card details found over the past four years. The data represents over 44,000 debit and credit cards supplied by seven of the world's largest banks some with headquarters in America, UK, Singapore, Hong Kong, and Australia. We compared the dates on which these stolen cards were discovered with their expiration dates and other associated personal information.

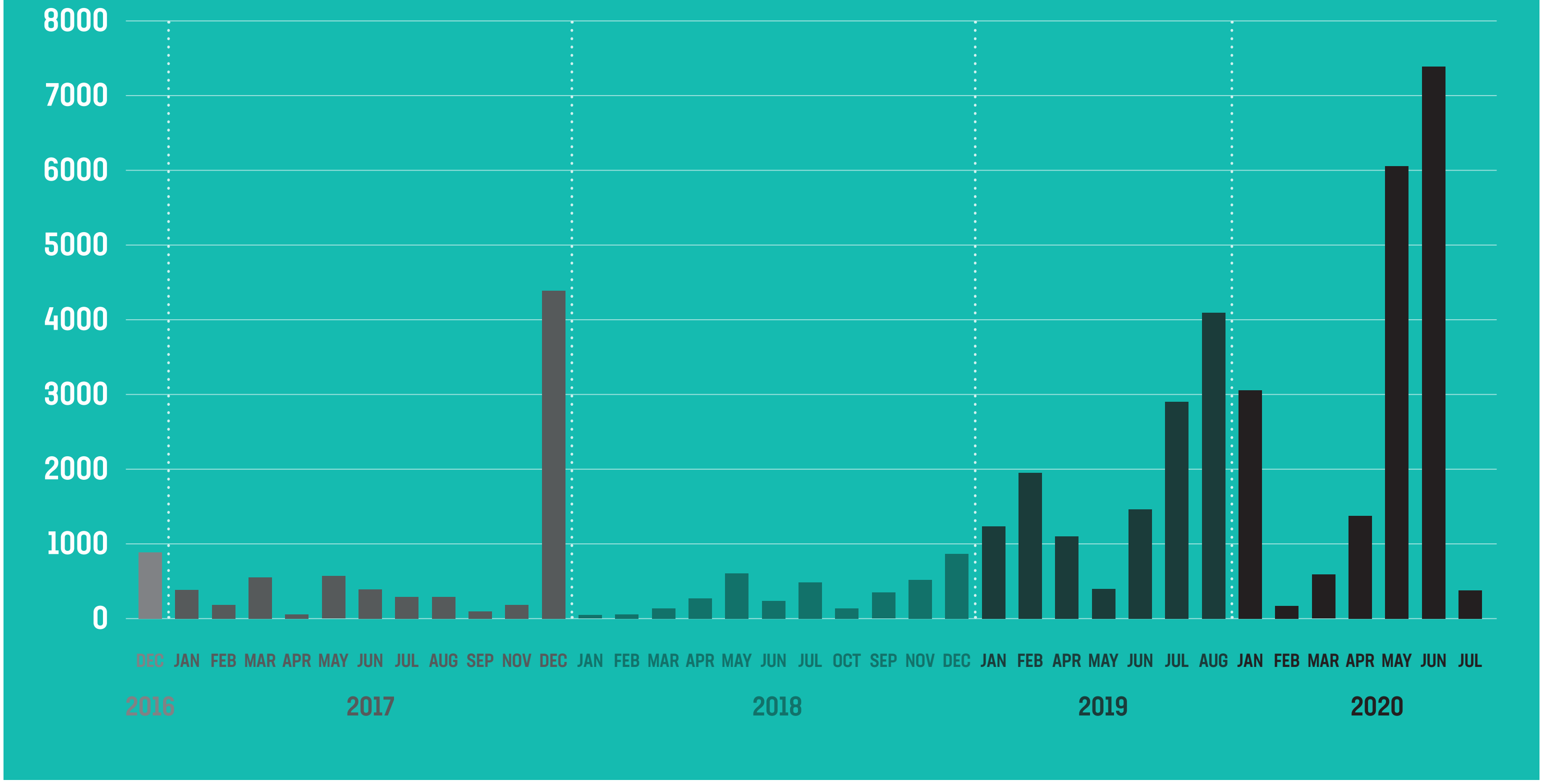
Looking at a near four-year average, from late 2016 through mid-2020, almost half of all cards, 42%, were found to be in-date at the time of discovery. An impressive 98% cards had some personal data associated with them. In most cases, this included names and addresses, but some also contained phone numbers and email addresses.

SINCE 2016, 98% OF STOLEN PAYMENT CARDS HAD SOME PERSONAL DATA ASSOCIATED WITH THEM

Thankfully, across the seven multinational banks we analyzed, we have found that these numbers have been declining. At the peak in 2016, 97.2% of all cards had full names associated with them. In 2020 this number has dropped to 84.9%. Likewise, card validity has also fallen. At its worst in 2017, 76% of cards were in date at the time of discovery. This had dropped to just 32.8% in 2020.

FIGURE 8. QUANTITY OF STOLEN PAYMENT CARDS FROM SEVEN GLOBAL BANKS DISCOVERED ON DARKNET MARKETS

No data was available for Sept-Dec 2019



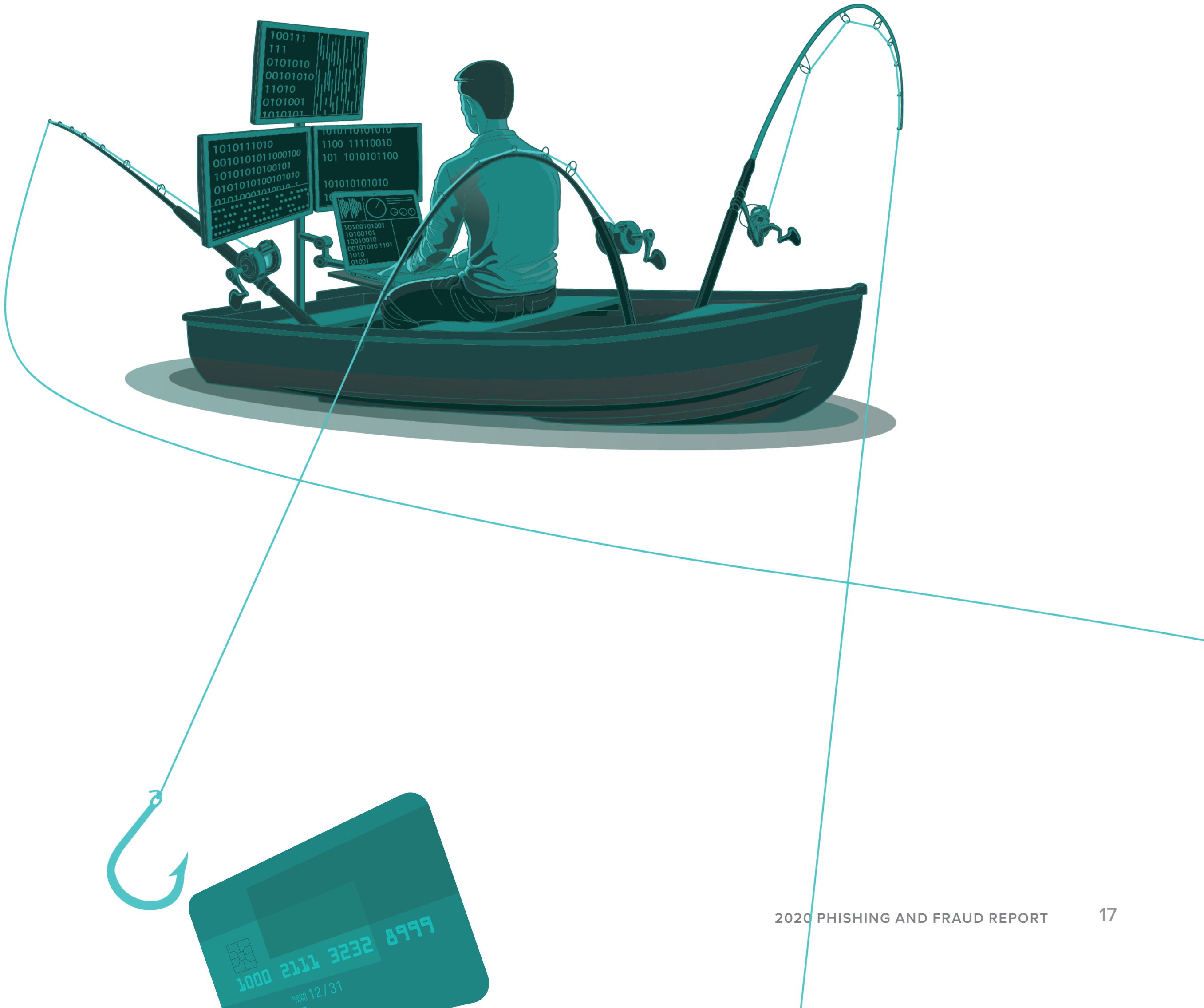
Physical card skimming is still commonplace within the organized crime world, but this process typically only captures a victim's card number. Payment card data with associated personal information is significantly more valuable to the cybercriminal. Having access to a victim's name, physical address, and email address allows the criminal to create fraudulent accounts in the victim's name. Additionally, physical addresses allow them to pay for goods using the correct billing address while sending goods to a different location.

The large amount of personal data associated with payment card numbers points to several possible sources:

- Breached databases storing payment card details
- Formjacking (a form of cyber card skimming)
- Simple scams asking users to enter payment details to claim a prize
- Phishing pages designed to imitate real banking websites

Cybercriminals are quick to act. They understand that once they have tricked the victim into handing over their payment card details or banking credentials, the quicker they act the more likely they are to successfully steal the victim's money. Shape Security, now part of F5, frequently investigates phishing sites that imitate real banking login pages. By tracking the known payment card details entered into the phishing site and detecting when an attempt was made to use that card, we were able to build a comprehensive picture of the phishing campaign. The average time between a victim entering payment card details into a phishing site and a cybercriminal fraudulently using those credentials was just four hours. In many cases, a repeated login was attempted another seven hours later.

4 HOURS: THE AVERAGE TIME BETWEEN A VICTIM ENTERING PAYMENT CARD DETAILS INTO A PHISHING SITE AND A CYBERCRIMINAL FRAUDULENTLY USING THOSE CREDENTIALS IN AN ATTACK



Modern Phishing Practices

Phishing is slowly evolving. While there is rarely a radical shift in how phishing attacks are carried out, fraudsters are certainly adapting to security controls and improving their level of sophistication. In this section we look at how attackers build and host their phishing sites and what methods they use to avoid detection.

Building a Phishing Site

Cybercriminals have a number of ways to build their phishing sites. Although creating a fake site completely from scratch is possible, it is rarely worth the phisher's time. Instead, they use one of two methods: clone the real site or purchase a phishing kit.

Cloning a Site

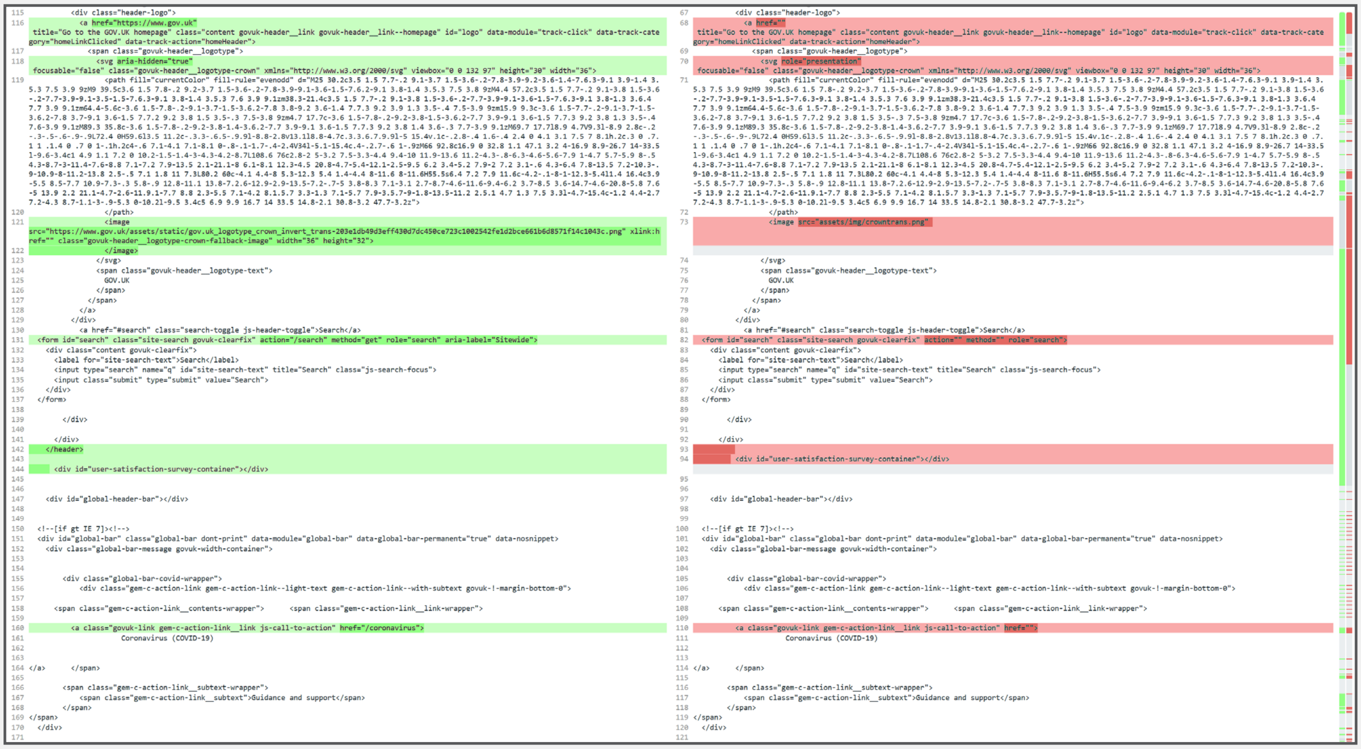
Cloning a real webpage can be a simple three-step process:

1. Visit the genuine website

2. Right-click and select **Save Page As...**

3. Take the HTML, CSS, and images just saved and host them on a rented server

FIGURE 9. COMPARISON OF LEGITIMATE UK GOVERNMENT SITE (LEFT) AND SPOOFED SITE (RIGHT)



```
        <div class="header-logo">
          <a href="https://www.gov.uk"
 title="Go to the GOV.UK homepage" class="content govuk-header__link govuk-header__link--homepage" id="logo" data-module="track-click" data-track-cate
gory="homeLinkClicked" data-track-action="homeHeader">
            <span class="govuk-header__logotype">
              <svg aria-hidden="true"
 focusable="false" class="govuk-header__logotype-crown" xmlns="http://www.w3.org/2000/svg" viewbox="0 0 132 97" height="30" width="36">
                <path fill="currentColor" fill-rule="evenodd" d="M25 30.2c3.5 1.5 7.7-.2 9.1-3.7 1.5-3.6-.2-7.8-3.9-9.2-3.6-1.4-7.6.3-9.1 3.9-1.4 3.
5.3 7.5 3.9 9zM9 39.5c3.6 1.5 7.8-.2 9.2-3.7 1.5-3.6-.2-7.8-3.9-9.1-3.6-1.5-7.6.2-9.1 3.8-1.4 3.5.3 7.5 3.8 9zM4.4 57.2c3.5 1.5 7.7-.2 9.1-3.8 1.5-3.6
-.2-7.7-3.9-9.1-3.5-1.5-7.6.3-9.1 3.8-1.4 3.5.3 7.6 3.9 9.1zm38.3-21.4c3.5 1.5 7.7-.2 9.1-3.8 1.5-3.6-.2-7.7-3.9-9.1-3.6-1.5-7.6.3-9.1 3.8-1.3 3.6.4
7.7 3.9 9.1zm64.4-5.6c-3.6 1.5-7.8-.2-9.1-3.7-1.5-3.6.2-7.8 3.8-9.2 3.6-1.4 7.7.3 9.2 3.9 1.3 3.5-.4 7.5-3.9 9zm15.9 9.3c-3.6 1.5-7.7-.2-9.1-3.7-1.5-
3.6.2-7.8 3.7-9.1 3.6-1.5 7.7.2 9.2 3.8 1.5 3.5-.3 7.5-3.8 9zm4.7 17.7c-3.6 1.5-7.8-.2-9.2-3.8-1.5-3.6.2-7.7 3.9-9.1 3.6-1.5 7.7.3 9.2 3.8 1.3 3.5-.4
7.6-3.9 9.1zM89.3 35.8c-3.6 1.5-7.8-.2-9.2-3.8-1.4-3.6.2-7.7 3.9-9.1 3.6-1.5 7.7.3 9.2 3.8 1.4 3.6-.3 7.7-3.9 9.1zM69.7 17.7l8.9 4.7V9.3l-8.9 2.8c-.2
-.3-.5-.6-.9-.9L72.4 0H59.6l3.5 11.2c-.3.3-.6.5-.9.9l-8.8-2.8v13.1l8.8-4.7c.3.3.6.7.9.9l-5 15.4v.1c-.2.8-.4 1.6-.4 2.4 0 4.1 3.1 7.5 7 8.1h.2c.3 0 .7.
1 1 .1.4 0 .7 0 1-.1h.2c4-.6 7.1-4.1 7.1-8.1 0-.8-.1-1.7-.4-2.4V34l-5.1-15.4c.4-.2.7-.6 1-.9zM66 92.8c16.9 0 32.8 1.1 47.1 3.2 4-16.9 8.9-26.7 14-33.5
l-9.6-3.4c1 4.9 1.1 7.2 0 10.2-1.5-1.4-3-4.3-4.2-8.7L108.6 76c2.8-2 5-3.2 7.5-3.3-4.4 9.4-10 11.9-13.6 11.2-4.3-.8-6.3-4.6-5.6-7.9 1-4.7 5.7-5.9 8-.5
4.3-8.7-3-11.4-7.6-8.8 7.1-7.2 7.9-13.5 2.1-21.1-8 6.1-8.1 12.3-4.5 20.8-4.7-5.4-12.1-2.5-9.5 6.2 3.4-5.2 7.9-2 7.2 3.1-.6 4.3-6.4 7.8-13.5 7.2-10.3-.
9-10.9-8-11.2-13.8 2.5-.5 7.1 1.8 11 7.3L80.2 60c-4.1 4.4-8 5.3-12.3 5.4 1.4-4.4 8-11.6 8-11.6H55.5s6.4 7.2 7.9 11.6c-4.2-.1-8-1-12.3-5.4l1.4 16.4c3.9
-5.5 8.5-7.7 10.9-7.3-.3 5.8-.9 12.8-11.1 13.8-7.2.6-12.9-2.9-13.5-7.2-.7-5 3.8-8.3 7.1-3.1 2.7-8.7-4.6-11.6-9.4-6.2 3.7-8.5 3.6-14.7-4.6-20.8-5.8 7.6
-5 13.9 2.2 21.1-4.7-2.6-11.9.1-7.7 8.8 2.3-5.5 7.1-4.2 8.1.5.7 3.3-1.3 7.1-5.7 7.9-3.5.7-9-1.8-13.5-11.2 2.5.1 4.7 1.3 7.5 3.3l-4.7-15.4c-1.2 4.4-2.7
7.2-4.3 8.7-1.1-3-.9-5.3 0-10.2l-9.5 3.4c5 6.9 9.9 16.7 14 33.5 14.8-2.1 30.8-3.2 47.7-3.2z">
                </path>
                <image
src="https://www.gov.uk/assets/static/gov.uk_logotype_crown_invert_trans-203e1db49d3eff430d7dc450ce723c1002542fe1d2bce661b6d8571f14c1043c.png" xlink:h
ref="" class="govuk-header__logotype-crown-fallback-image" width="36" height="32">
                </image>
              </svg>
              <span class="govuk-header__logotype-text">
                GOV.UK
              </span>
            </span>
          </a>
        </div>
          <a href="#search" class="search-toggle js-header-toggle">Search</a>
  <form id="search" class="site-search govuk-clearfix" action="/search" method="get" role="search" aria-label="Sitewide">
    <div class="content govuk-clearfix">
      <label for="site-search-text">Search</label>
      <input type="search" name="q" id="site-search-text" title="Search" class="js-search-focus">
      <input class="submit" type="submit" value="Search">
    </div>
  </form>

        </div>

      </div>
    </header>

      <div id="user-satisfaction-survey-container"></div>


    <div id="global-header-bar"></div>


  <!--[if gt IE 7]><!-->
  <div id="global-bar" class="global-bar dont-print" data-module="global-bar" data-global-bar-permanent="true" data-nosnippet>
    <div class="global-bar-message govuk-width-container">


        <div class="global-bar-covid-wrapper">
            <div class="gem-c-action-link gem-c-action-link--light-text gem-c-action-link--with-subtext govuk-!-margin-bottom-0">

      <span class="gem-c-action-link__contents-wrapper">      <span class="gem-c-action-link__link-wrapper">

          <a class="govuk-link gem-c-action-link__link js-call-to-action" href="/coronavirus">
                      Coronavirus (COVID-19)


</a>      </span>

        <span class="gem-c-action-link__subtext-wrapper">
            <span class="gem-c-action-link__subtext">Guidance and support</span>
        </span>
</span>
  </div>

```

```
        <div class="header-logo">
          <a href=""
 title="Go to the GOV.UK homepage" class="content govuk-header__link govuk-header__link--homepage" id="logo" data-module="track-click" data-track-cate
gory="homeLinkClicked" data-track-action="homeHeader">
            <span class="govuk-header__logotype">
              <svg role="presentation"
 focusable="false" class="govuk-header__logotype-crown" xmlns="http://www.w3.org/2000/svg" viewbox="0 0 132 97" height="30" width="36">
                <path fill="currentColor" fill-rule="evenodd" d="M25 30.2c3.5 1.5 7.7-.2 9.1-3.7 1.5-3.6-.2-7.8-3.9-9.2-3.6-1.4-7.6.3-9.1 3.9-1.4 3.
5.3 7.5 3.9 9zM9 39.5c3.6 1.5 7.8-.2 9.2-3.7 1.5-3.6-.2-7.8-3.9-9.1-3.6-1.5-7.6.2-9.1 3.8-1.4 3.5.3 7.5 3.8 9zM4.4 57.2c3.5 1.5 7.7-.2 9.1-3.8 1.5-3.6
-.2-7.7-3.9-9.1-3.5-1.5-7.6.3-9.1 3.8-1.4 3.5.3 7.6 3.9 9.1zm38.3-21.4c3.5 1.5 7.7-.2 9.1-3.8 1.5-3.6-.2-7.7-3.9-9.1-3.6-1.5-7.6.3-9.1 3.8-1.3 3.6.4
7.7 3.9 9.1zm64.4-5.6c-3.6 1.5-7.8-.2-9.1-3.7-1.5-3.6.2-7.8 3.8-9.2 3.6-1.4 7.7.3 9.2 3.9 1.3 3.5-.4 7.5-3.9 9zm15.9 9.3c-3.6 1.5-7.7-.2-9.1-3.7-1.5-
3.6.2-7.8 3.7-9.1 3.6-1.5 7.7.2 9.2 3.8 1.5 3.5-.3 7.5-3.8 9zm4.7 17.7c-3.6 1.5-7.8-.2-9.2-3.8-1.5-3.6.2-7.7 3.9-9.1 3.6-1.5 7.7.3 9.2 3.8 1.3 3.5-.4
7.6-3.9 9.1zM89.3 35.8c-3.6 1.5-7.8-.2-9.2-3.8-1.4-3.6.2-7.7 3.9-9.1 3.6-1.5 7.7.3 9.2 3.8 1.4 3.6-.3 7.7-3.9 9.1zM69.7 17.7l8.9 4.7V9.3l-8.9 2.8c-.2
-.3-.5-.6-.9-.9L72.4 0H59.6l3.5 11.2c-.3.3-.6.5-.9.9l-8.8-2.8v13.1l8.8-4.7c.3.3.6.7.9.9l-5 15.4v.1c-.2.8-.4 1.6-.4 2.4 0 4.1 3.1 7.5 7 8.1h.2c.3 0 .7.
1 1 .1.4 0 .7 0 1-.1h.2c4-.6 7.1-4.1 7.1-8.1 0-.8-.1-1.7-.4-2.4V34l-5.1-15.4c.4-.2.7-.6 1-.9zM66 92.8c16.9 0 32.8 1.1 47.1 3.2 4-16.9 8.9-26.7 14-33.5
l-9.6-3.4c1 4.9 1.1 7.2 0 10.2-1.5-1.4-3-4.3-4.2-8.7L108.6 76c2.8-2 5-3.2 7.5-3.3-4.4 9.4-10 11.9-13.6 11.2-4.3-.8-6.3-4.6-5.6-7.9 1-4.7 5.7-5.9 8-.5
4.3-8.7-3-11.4-7.6-8.8 7.1-7.2 7.9-13.5 2.1-21.1-8 6.1-8.1 12.3-4.5 20.8-4.7-5.4-12.1-2.5-9.5 6.2 3.4-5.2 7.9-2 7.2 3.1-.6 4.3-6.4 7.8-13.5 7.2-10.3-.
9-10.9-8-11.2-13.8 2.5-.5 7.1 1.8 11 7.3L80.2 60c-4.1 4.4-8 5.3-12.3 5.4 1.4-4.4 8-11.6 8-11.6H55.5s6.4 7.2 7.9 11.6c-4.2-.1-8-1-12.3-5.4l1.4 16.4c3.9
-5.5 8.5-7.7 10.9-7.3-.3 5.8-.9 12.8-11.1 13.8-7.2.6-12.9-2.9-13.5-7.2-.7-5 3.8-8.3 7.1-3.1 2.7-8.7-4.6-11.6-9.4-6.2 3.7-8.5 3.6-14.7-4.6-20.8-5.8 7.6
-5 13.9 2.2 21.1-4.7-2.6-11.9.1-7.7 8.8 2.3-5.5 7.1-4.2 8.1.5.7 3.3-1.3 7.1-5.7 7.9-3.5.7-9-1.8-13.5-11.2 2.5.1 4.7 1.3 7.5 3.3l-4.7-15.4c-1.2 4.4-2.7
7.2-4.3 8.7-1.1-3-.9-5.3 0-10.2l-9.5 3.4c5 6.9 9.9 16.7 14 33.5 14.8-2.1 30.8-3.2 47.7-3.2z">
                </path>
                <image src="assets/img/crowntrans.png"

              </svg>
              <span class="govuk-header__logotype-text">
                GOV.UK
              </span>
            </span>
          </a>
        </div>
          <a href="#search" class="search-toggle js-header-toggle">Search</a>
  <form id="search" class="site-search govuk-clearfix" action="" method="" role="search">
    <div class="content govuk-clearfix">
      <label for="site-search-text">Search</label>
      <input type="search" name="q" id="site-search-text" title="Search" class="js-search-focus">
      <input class="submit" type="submit" value="Search">
    </div>
  </form>

        </div>

      </div>

      <div id="user-satisfaction-survey-container"></div>


    <div id="global-header-bar"></div>


  <!--[if gt IE 7]><!-->
  <div id="global-bar" class="global-bar dont-print" data-module="global-bar" data-global-bar-permanent="true" data-nosnippet>
    <div class="global-bar-message govuk-width-container">


        <div class="global-bar-covid-wrapper">
            <div class="gem-c-action-link gem-c-action-link--light-text gem-c-action-link--with-subtext govuk-!-margin-bottom-0">

      <span class="gem-c-action-link__contents-wrapper">      <span class="gem-c-action-link__link-wrapper">

          <a class="govuk-link gem-c-action-link__link js-call-to-action" href="">
                      Coronavirus (COVID-19)


</a>      </span>

        <span class="gem-c-action-link__subtext-wrapper">
            <span class="gem-c-action-link__subtext">Guidance and support</span>
        </span>
</span>
  </div>

```

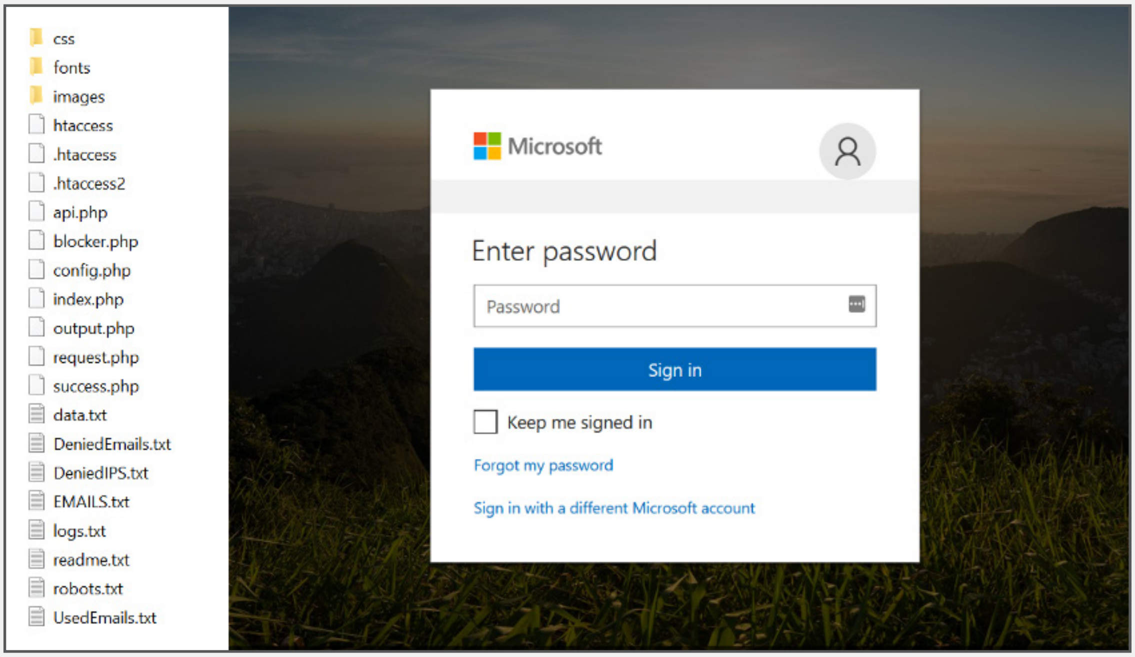
While these steps are somewhat over-simplified, the principle is entirely valid. The F5 SOC is often involved in phishing site takedowns in which the malicious site was a simple clone of the genuine one. The benefit of site cloning is that the phisher captures all the elements of the real web page, including CSS and images. They need only alter a few components of the site, such as where the credentials are sent, and they're good to go.

Figure 9 compares the source code from a phishing campaign spotted in August 2020. The code on the left shows the legitimate UK Government website HTML and the code from the malicious site is shown on the right. Only small changes have been made to the code; it uses as much of the original source as possible.

Phishing Kits

The alternative—and arguably an even easier method than cloning a site—is to acquire a phishing kit. These are turnkey phishing solutions that come packaged with all the HTML, images, and code needed to create a fraudulent site (see Figure 10).

FIGURE 10. LEFT: THE COMPONENTS OF A PHISHING KIT.
RIGHT: HOW THE PHISHING SITE APPEARS TO VISITORS



```
css
fonts
images
htaccess
.htaccess
.htaccess2
api.php
blocker.php
config.php
index.php
output.php
request.php
success.php
data.txt
DeniedEmails.txt
DeniedIPS.txt
EMAILS.txt
logs.txt
readme.txt
robots.txt
UsedEmails.txt
```

Kits are developed to target a specific organization or brand. For example, kits for logistics firm DHL attempt to trick victims into paying a fee to deliver their (non-existent) parcels. Banking kits are designed to steal credentials, payment card details, and answers to security questions. One of the most popular targets for generic phishing is the Microsoft Office 365 login page. The productivity and collaboration platform enjoys widespread global usage with many businesses often moving their entire back office systems onto the platform. Attackers know that stealing Office 365 credentials can grant them access not only to email but also corporate documents, finance, HR, and many other critical business functions.

Phishing kits vary in complexity, but the more advanced ones require an active license from the author and employ numerous tricks to avoid detection by researchers and casual observers. One such recent example is the *OfficeV4* kit, which, not surprisingly, targets users of Office 365.

OfficeV4 fraudsters must have an active license in order to use the kit. Figure 12 shows a portion of the configuration file, which is dynamically included in every page of the kit, meaning that every page load requires a lookup for an active license.

Stealth and Evasion

Where and how phishers decide to host their fraudulent site will depend on how frugal they are and what they want their website address to look like. While some attackers leech off a vulnerable website, many choose to register their own domain names. Fraudsters are also keen to avoid detection by security researchers, so they employ a number of techniques in an attempt to remain hidden.

Spoofing Brands by Using Similar URLs

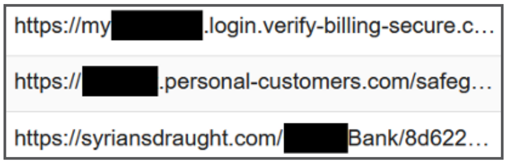
Attackers use a combination of tactics to make their phishing URLs appear genuine. From making use of target brands in the domain to the implementing genuine HTTPS certificates, their goal is to minimize the risk of victims being suspicious about the site they are visiting.

Using Custom Domain Names

In targeted campaigns attackers often include the name of the target organization somewhere in the URL. Analyzing the fraudulent domain names of phishing sites detected by the F5 SOC shows that, in 2020, 52% of malicious links contain the brand name either in the domain name or the path.

FIGURE 11. ATTACKERS USE TARGET NAMES IN THE DOMAIN OR PATH OF THE URL

(Source: F5 SOC)



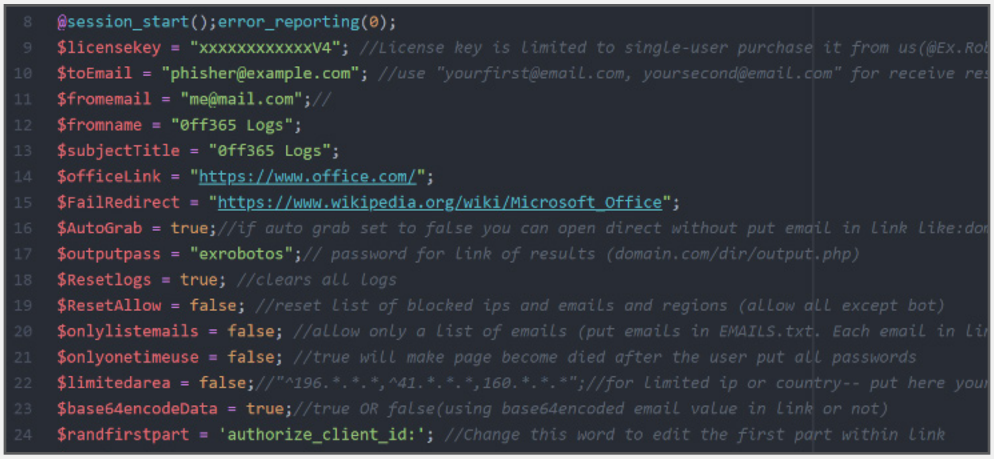
https://my[redacted].login.verify-billing-secure.c…

https://[redacted].personal-customers.com/safeg…

https://syriansdraught.com/[redacted]Bank/8d622…

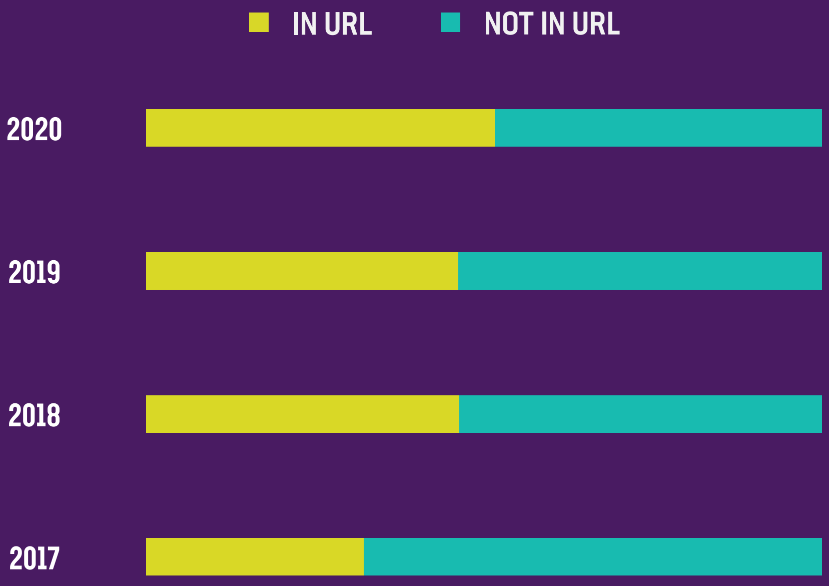
Attackers often choose a subdomain that makes use of the target name. Victims—not paying close attention or simply unaware of the rules that govern the web and how URLs function—will see a genuine looking part of the domain name and may assume it is an authentic site (see Figure 11).

FIGURE 12. THE CONFIGURATION FILE FOR THE “OFFICEV4” PHISHING KIT, WHICH REQUIRES USERS TO ENTER THEIR LICENSE KEY



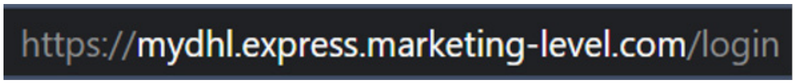
```
@session_start();error_reporting(0);
$licensekey = "xxxxxxxxxxxxV4"; //License key is limited to single-user purchase it from us(@Ex.Rob
$toEmail = "phisher@example.com"; //use "yourfirst@email.com, yoursecond@email.com" for receive res
$fromemail = "me@mail.com";//
$fromname = "0ff365 Logs";
$subjectTitle = "0ff365 Logs";
$officeLink = "https://www.office.com/";
$FailRedirect = "https://www.wikipedia.org/wiki/Microsoft_Office";
$AutoGrab = true;//if auto grab set to false you can open direct without put email in link like:dom
$outputpass = "exrobotos";// password for link of results (domain.com/dir/output.php)
$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 lin
$onlyonetimeuse = false; //true will make page become died after the user put all passwords
$limitedarea = false;//"^196.*.*.*,^41.*.*.*,160.*.*.*";//for limited ip or country-- put here your
$base64encodeData = true;//true OR false(using base64encoded email value in link or not)
$randfirstpart = 'authorize_client_id:'; //Change this word to edit the first part within link
```

FIGURE 13. PERCENTAGE OF PHISHING SITES SEEN BY THE F5 SOC THAT MAKE USE OF THE TARGET BRAND NAME SOMEWHERE IN THE URL



Some browser vendors, aware that this is now a common practice, attempt to highlight to true domain, but there is much inconsistency among them. Google's Chrome browser, for example, shades the path of the website in gray and highlights both the domain name and also any subdomain.

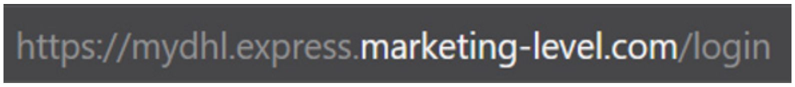
FIGURE 14. CHROME HIGHLIGHTING THE FULL DOMAIN OF A PHISHING SITE



https://mydhl.express.marketing-level.com/login

Firefox, however, recognizing that phishers often use subdomains to trick their victims, grays all parts of the URL, apart from the base domain.

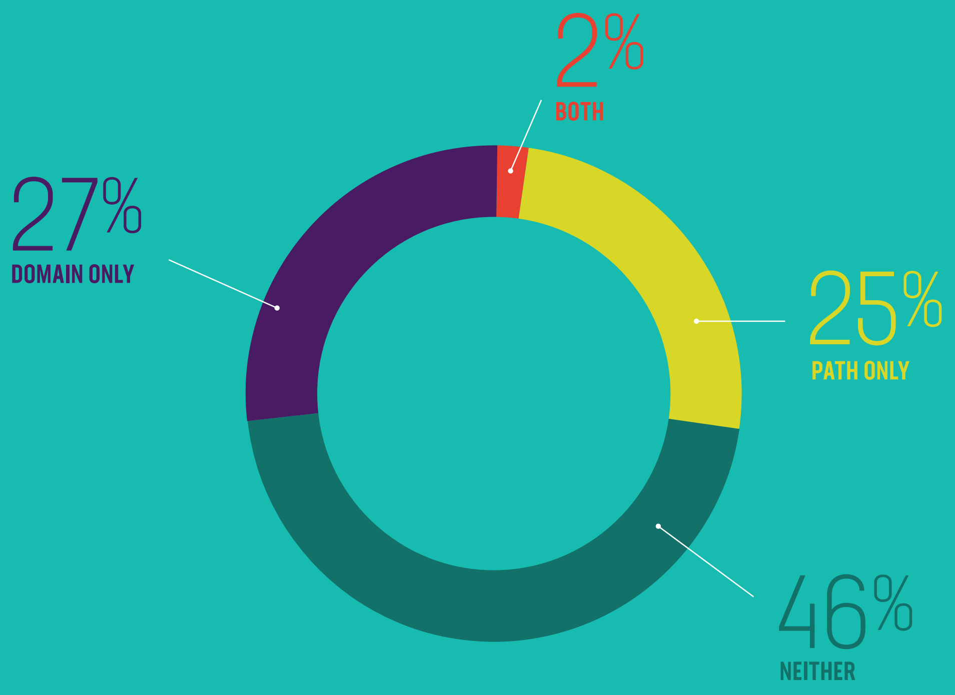
FIGURE 15. FIREFOX HIGHLIGHTING ONLY THE BASE DOMAIN OF THE URL



https://mydhl.express.marketing-level.com/login

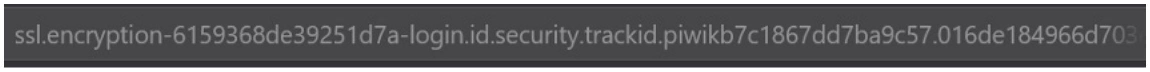
Is domain highlighting a big enough move, however? We found that almost 30% of phishing sites made use of the target brand in the domain portion of the URL while only 25% used that brand name in the path only.

FIGURE 16. PROPORTION OF PHISHING SITES USING BRAND NAMES IN THE HOSTNAME, PATH, OR BOTH



In addition to creating genuine looking URLs, fraudsters often create subdomains so long that the true base domain is hidden from view off the end of the address bar. Despite graying the subdomain, all the victim can see is the start of the address, which includes some authentic looking words such as *ssl, encryption, and security*.

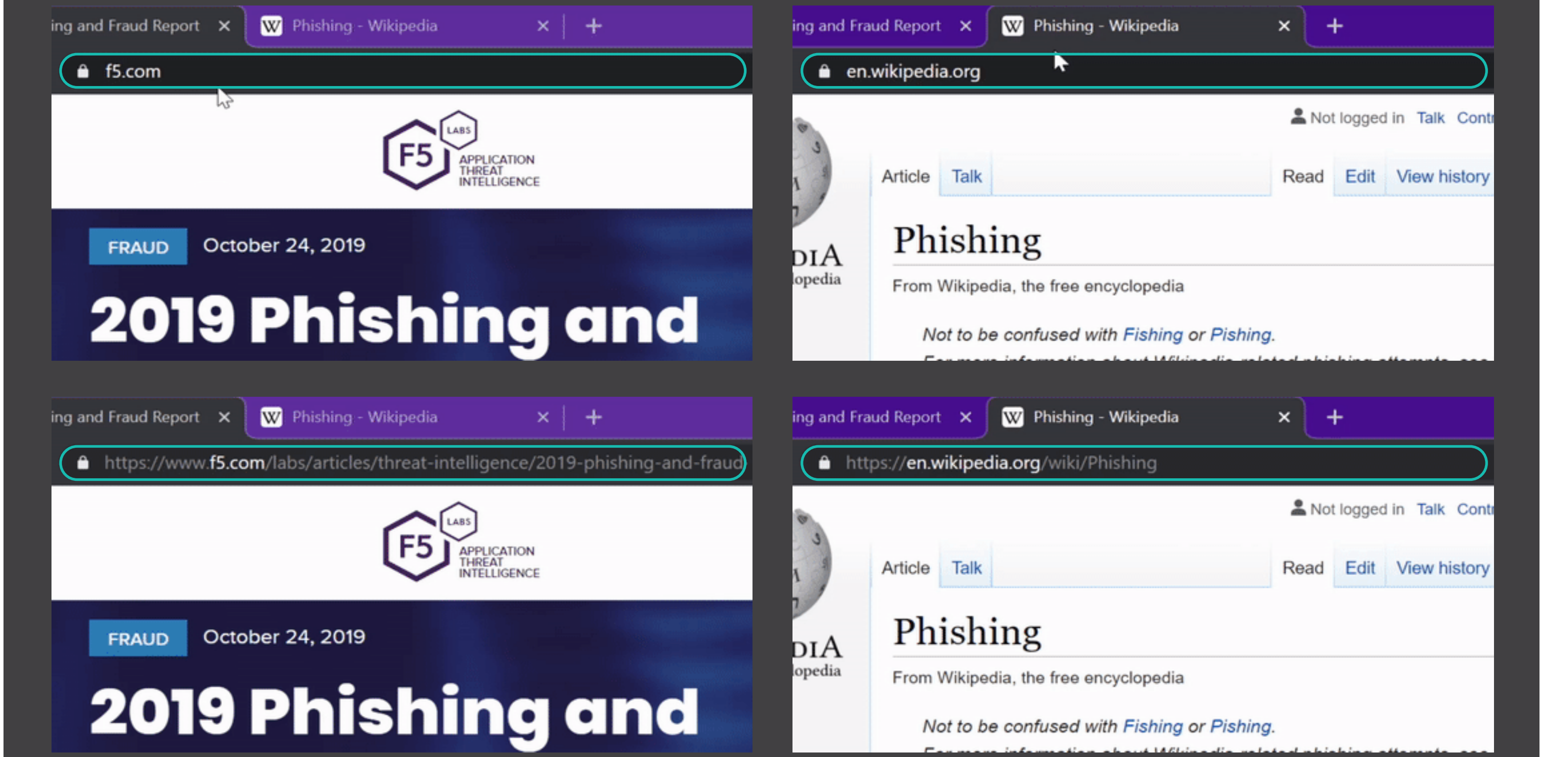
FIGURE 17. PHISHING SITE URL MAKING USE OF DECEPTION TECHNIQUES TO HIDE THE TRUE ADDRESS



ssl.encryption-6159368de39251d7a-login.id.security.trackid.piwikb7c1867dd7ba9c57.016de184966d703

In an attempt to fully address this, the Chrome browser is now testing a feature to auto-hide the path of a website until a user clicks in the address bar (see Figure 18). This is similar to way that Apple's Safari browser displays URLs (so long as the "Show full website address" option is unchecked). For the majority of web users who know or care little about the difference between domains, subdomains, paths, and query strings, this is a positive move. It allows them to focus their attention on the full domain of the site they are visiting.

FIGURE 18. CHROME 86 IS TESTING A FEATURE TO AUTOMATICALLY HIDE WEBSITE PATHS UNTIL THEY ARE NEEDED



f5.com

en.wikipedia.org

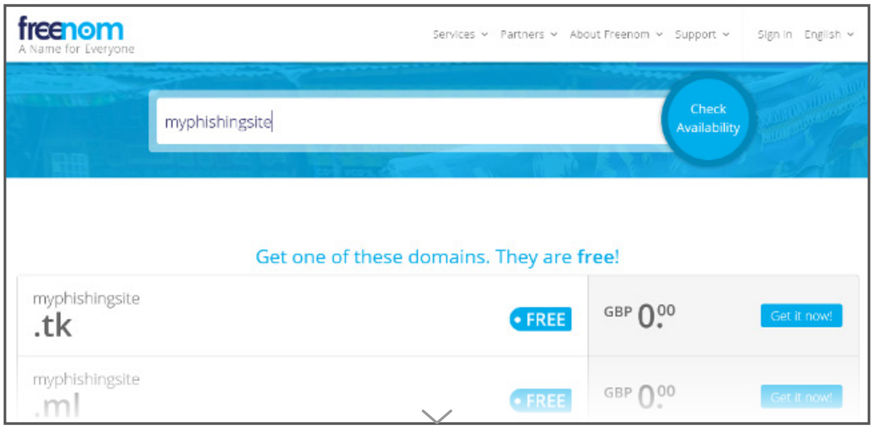
https://www.f5.com/labs/articles/threat-intelligence/2019-phishing-and-fraud

https://en.wikipedia.org/wiki/Phishing

Abusing Free Top-Level Domains

Registering a domain such as myphishingdomain.com (or something slightly less obvious, such as secure-site-login.com) brings with it a cost charged by the registrar. This can range from a few dollars a year to many thousands of dollars if the domain name contains popular or trademarked keywords. However, we are now seeing increased use of free registrars (such as Freenom) for certain country code top-level domains (ccTLDs) such as .tk, .ml, .ga, .cf, and .gq (see Figure 19).

FIGURE 19. FREENOM IS THE REGISTRAR IN CHARGE OF .TK COUNTRY CODE TLDs AND OFFERS THEM FOR FREE



myphishingsite

Get one of these domains. They are free!

myphishingsite .tk	• FREE	GBP 0.00
myphishingsite .ml	• FREE	GBP 0.00

This allows both legitimate and fraudulent users to register domains entirely for free, once again lowering the financial cost to the attacker. In fact, these free domains have become so popular that .tk is now the fifth most popular TLD by number of registered domains (see Figure 20).[xii]

The F5 SOC has observed numerous attack campaigns in which a crime group created almost 1,000 custom domains that all contained short strings followed by the suffix “-71”. The same domain was registered for each of the free TLDs, as shown in Figure 22.

These nearly 1,000 domains resolved to just under thirty IP addresses that were hosted on various public clouds, predominantly Alibaba, Amazon AWS, and Microsoft Azure. These IP addresses also hosted many other non-malicious websites. It’s likely that the short length and numbering of these domains made it simple for the attackers to identify and automate the deployment of malicious sites through the use of scripts that called out to web shells, instead of managing them via cloud-native tools that differ among the providers.

FIGURE 20. DISTRIBUTION OF ALL TOP-LEVEL DOMAINS IN OCTOBER 2020

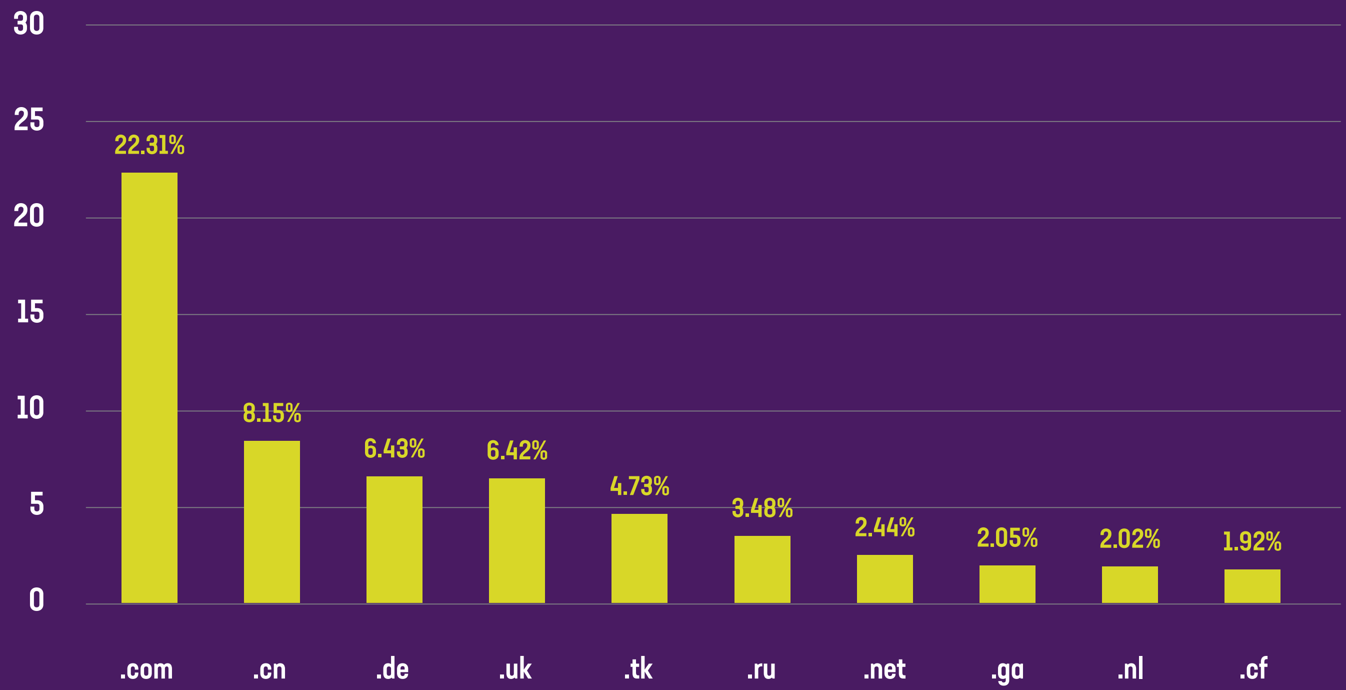


FIGURE 21. DISTRIBUTION OF TLDS USED BY PHISHING SITES IN SEPTEMBER 2020; .COM REMAINS THE MOST POPULAR

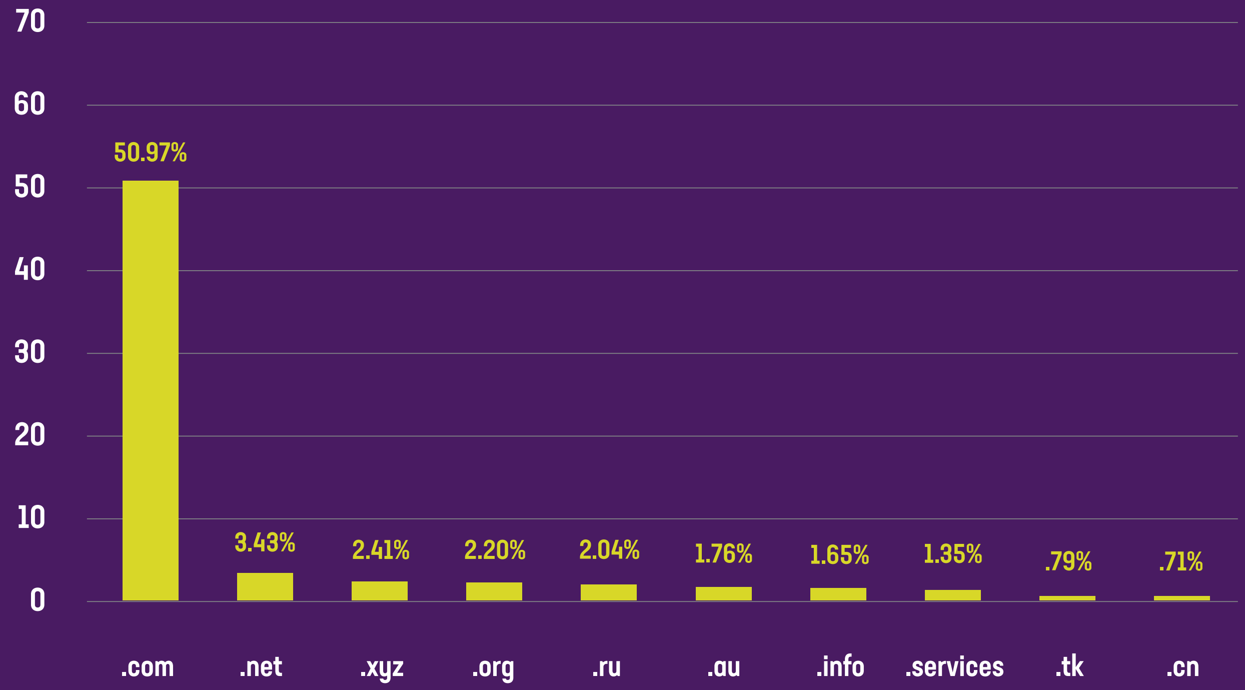
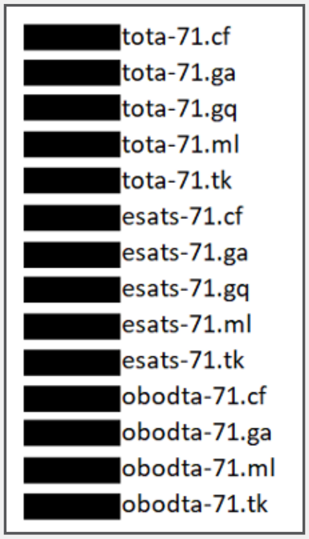


FIGURE 22. A REDACTED SAMPLE OF THE NEARLY 1,000 MALICIOUS "-71" DOMAINS CREATED BY CYBERCRIMINALS



[redacted]tota-71.cf
[redacted]tota-71.ga
[redacted]tota-71.gq
[redacted]tota-71.ml
[redacted]tota-71.tk
[redacted]esats-71.cf
[redacted]esats-71.ga
[redacted]esats-71.gq
[redacted]esats-71.ml
[redacted]esats-71.tk
[redacted]obodta-71.cf
[redacted]obodta-71.ga
[redacted]obodta-71.ml
[redacted]obodta-71.tk

Despite the growing use of free top-level domains, the ubiquitous .com TLD remains a clear favorite for phishers. While global TLD statistics show overall use of .com at just over 22% (see Figure 20), the average value we see from our combined datasets show phishing sites using .com at over 50% (see Figure 21).

Phishers are also getting creative and having fun with their domain names. Punycode, the ASCII translation of domain names using non-English character sets, has long been popular with phishers looking to trick their victims. One of the malicious domains found in our dataset this year, for example, was shop.dev.xn--blockchin-c2d.com which, when displayed in Punycode, displays as shop.dev.blockchain.com in the browser address bar. This is known as an IDN homograph attack, and virtually all modern browsers mitigate it by displaying domains with mixed character sets entirely in ASCII, making the Punycode visible. For this reason, the number of phishing domains we see attempting to exploit this attack vector is low, only 0.25%.

While mixed character sets are generally not displayed in browsers, domains made up entirely of Punycode are indeed visible. Fraudsters have become playful with their domains, using Emoji's to give some indication of what might wait for the visitor if they follow the link (see Figure 23).

FIGURE 23. EMOJI-BASED DOMAIN NAMES USED BY PHISHERS

💯👙🆓.tk

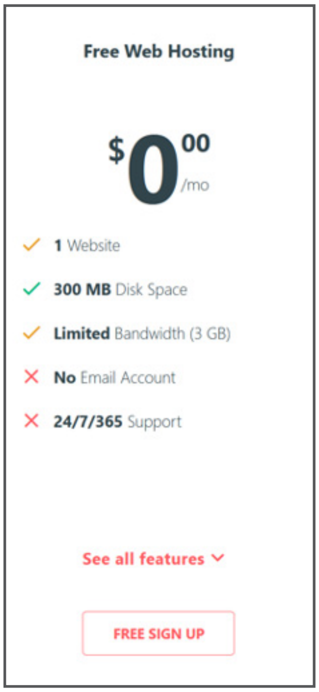
Once the domain name is registered, the phishing site needs to be placed onto a website. This year, like last, we saw extensive use of free and cheap cloud hosting services. Table 1 shows the most common web hosting platforms used by phishers and, for the second year running, 000webhostapp.com is the most popular.

TABLE 1. THE HOSTING PLATFORMS MOST COMMONLY USED BY PHISHING SITES

000webhostapp.com	bludomain6.com
appspot.com	srsdatuksimonfung.edu.my
arcseam.com.au	ca-oo.com
zarmuzik.com	shopnsmiles.com
shadetreetechnology.com	hdlxw.com

With free hosting for small web sites, it is easy to understand why attackers are using these platforms (Figure 24).

FIGURE 24. FREE WEB HOSTING FROM 000WEBHOSTAPP.COM



Free Web Hosting

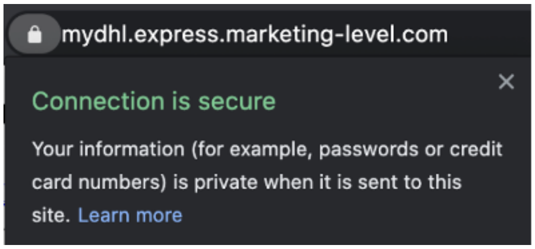
$0.00 /mo

- ✓ 1 Website
- ✓ 300 MB Disk Space
- ✓ Limited Bandwidth (3 GB)
- ✕ No Email Account
- ✕ 24/7/365 Support

Hiding in Plain Sight

Phishers use whatever means they have at their disposal to make their fraudulent site appear as genuine as possible. In today's online world, using TLS certificates so that websites appear secure is a virtual necessity. Despite domain names that have nothing to do with the brand the site is impersonating, unwitting victims often see the padlock and phrases such as "Connection is secure" and believe the site is trustworthy (see Figure 25).

FIGURE 25. PHISHING SITE MAKING USE OF A VALID CERTIFICATE



mydhl.express.marketing-level.com

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

F5 SOC statistics (see Figure 26) show that a rapidly growing number of phishing sites are using encryption. The majority, 71.2% of phishing links, make use of valid HTTPS certificates in order to present credible looking links to their victims. Corroborating our own data, we found that:

- Scans of phishing sites from BrightCloud Threat Intelligence showed that 72% used HTTPS
- The APWG's recent Phishing Activity Trends report similarly found that 78% of phishing sites now use SSL/TLS, up from 75% at the start of the year[xiii]

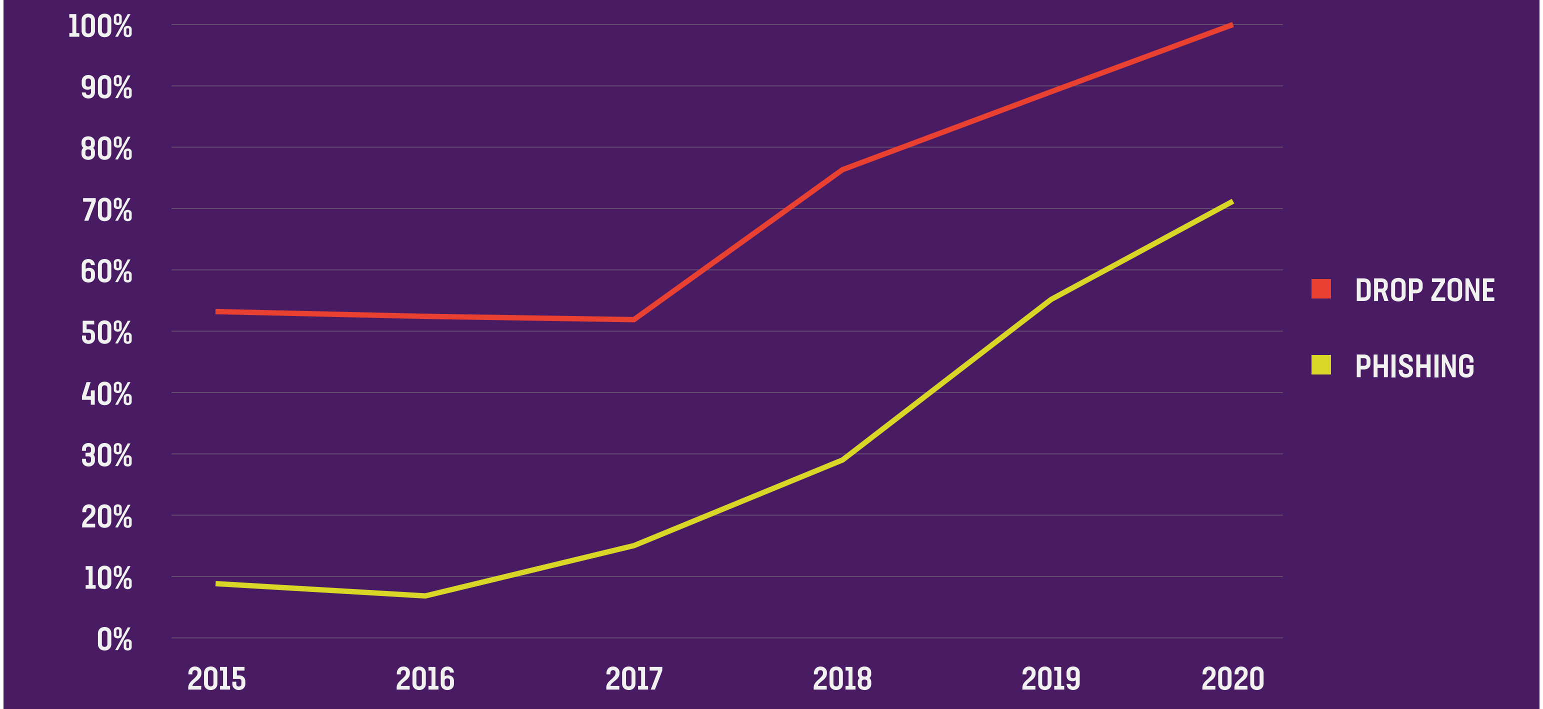
72% OF ALL PHISHING SITES SECURE THEIR SITE WITH SSL/TLS

Drop zones, destinations to which malware sends stolen data, make use of TLS encryption in 100% of incidents the F5 SOC investigated during 2020. Combining incidents from 2019 and 2020, we found that 55.3% of drop zones use a non-standard SSL/TLS port. In all but one of these cases, port 446 was used. Almost all phishing sites, 98.2%, used standard ports: 80 for cleartext HTTP traffic and 443 for encrypted SSL/TLS traffic. A non-trivial number of incidents, 1.5%, featured sites hosted port 32000.

Compromising Vulnerable Websites

Newly registered domains can be detected and blocked by corporate web proxies. The more discerning phisher might, instead, choose to avoid the costs and worries of domain name registration altogether by exploiting a vulnerability in someone else's website. By compromising a vulnerable website, they can not only host their phishing pages for free but also benefit from an existing and likely trusted domain name.

FIGURE 26. PERCENTAGE OF F5 SOC PHISHING AND DROP ZONE SITES MAKING USE OF ENCRYPTION



Across all our datasets, we found an average of almost 10% of all phishing incidents involved victims being sent to malicious pages built using WordPress. Examining data from the F5 SOC, we see that figure rise as high as 20% when we focus on phishing sites that do not make use of the target brand name anywhere in the URL. This suggests that vulnerable WordPress sites are being used opportunistically. Attackers recognize that they may not have such a strong hook (since they cannot customize the URL), but WordPress sites can represent a low-effort platform upon which to host their fraudulent pages. Exploitation of vulnerable websites appears to be trending up. Focusing on WordPress, we saw only 4.7% of phishing sites use the platform in 2017. This rose to 9% in 2018 and peaked in 2019 at just over 21%.

Compromising Third Parties

A trend closely followed by F5 Labs has been one in which attackers are increasingly breaching third-party services in an effort to massively scale their attacks and bypass security controls. In the past few years, we saw huge formjacking (web card skimming) campaigns that stole personal information and payment card data. Many of these attacks, such as those by the Magecart threat groups, compromised and modified scripts hosted on third party websites. Anyone using those compromised scripts by dynamically linking to it in their code was immediately affected.

Similarly, in August 2020, a large email marketing service found that several of its users had their credentials stolen. Attackers were then using their accounts to send spam and phishing emails. Organizations that had previously added the email provider to an allowlist found that they were suddenly receiving hundreds of phishing emails despite their email filter initially marking it as suspect.

The lesson here is simple. Adding entries to an allowlist should only be used as a last resort and done with limited scope. Entire domains should rarely be allowed without inspection. Instead, create allowlists that are as restricted as possible and clearly document the business justification for doing so.

ADDING ENTRIES TO AN ALLOWLIST SHOULD ONLY BE USED AS A LAST RESORT AND DONE WITH LIMITED SCOPE

Evading Prying Eyes

Threat actors are keen to prevent curious victims or determined security researchers from investigating their fraudulent sites. To this end, they employ a number of methods to block anyone that might not be a genuine victim.

Blocking Security Researchers

A common tactic to hide from prying eyes is to perform geolocation of the IP address to identify which country the connection is coming from. Russian scammers, for example, commonly block IP addresses from their home country so that they do not draw the eyes of Russian law enforcement. For this same reason, Tor exit nodes are also prevented from viewing the real phishing site. Additionally, victim IP addresses are logged and, once visited, repeat visitors are blocked and either shown a benign page or redirected elsewhere on the web, such as to Wikipedia.

Phishing kits, such as ‘OfficeV4’ as described in the Phishing Kits section, uses the.htaccess web server configuration file to block access from certain locations. The OfficeV4 kit contained over 1,000 lines of IP ranges, headers, and referring domains, such as google.com and firefox.com. The code sharing website Pastebin has many sample .htaccess files with preconfigured IP ranges and domains that other phishers can use to get started.

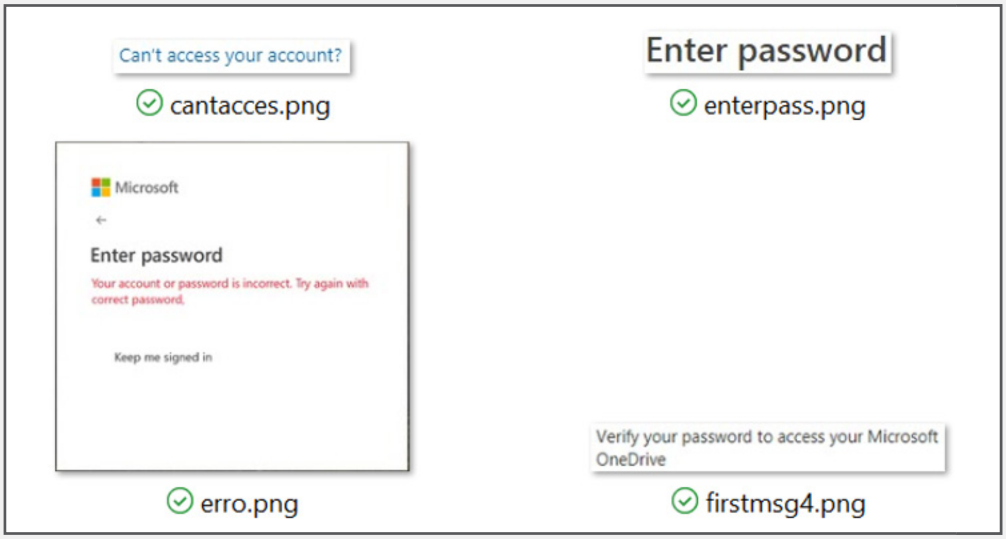
Many phishing kits examine the user-agent header of the client browser. Researchers often use scripts or tools to view malicious websites. Phishing pages attempt to detect what tool or browser is requesting access by examining this header and will block everything other than standard web browsers, such as Chrome and Safari. Mobile phishing scams follow the same pattern by blocking access to any device that does not appear to be an Android or iOS phone.

Attackers know how and where their links were distributed. If the referer header is blank or comes from a site they were not expecting, there's a good chance a security researcher is investigating the site and the connection is blocked.

Use Images Not Text

Security controls, such as web proxies, attempt to detect when a staff member is visiting a potential phishing site by examining the content of the incoming web page. By detecting the use of certain phrases, such as "failed login" or "password is incorrect," a proxy can determine the risk a site poses. Knowing this, phishers avoid being detected by using images to display text whenever possible. Figure 27 shows images used by the OfficeV4 phishing kit. It uses PNG images to display text such as "Enter password" instead of using raw text within the HTML page itself.

FIGURE 27. A PHISHING KIT THAT TARGETS OFFICE 365 AND USES IMAGES TO DISPLAY BASIC TEXT



Can't access your account?

✓ cantacces.png

Enter password

✓ enterpass.png

Microsoft

←

Enter password

Your account or password is incorrect. Try again with correct password.

Keep me signed in

✓ erro.png

Verify your password to access your Microsoft OneDrive

✓ firstmsg4.png

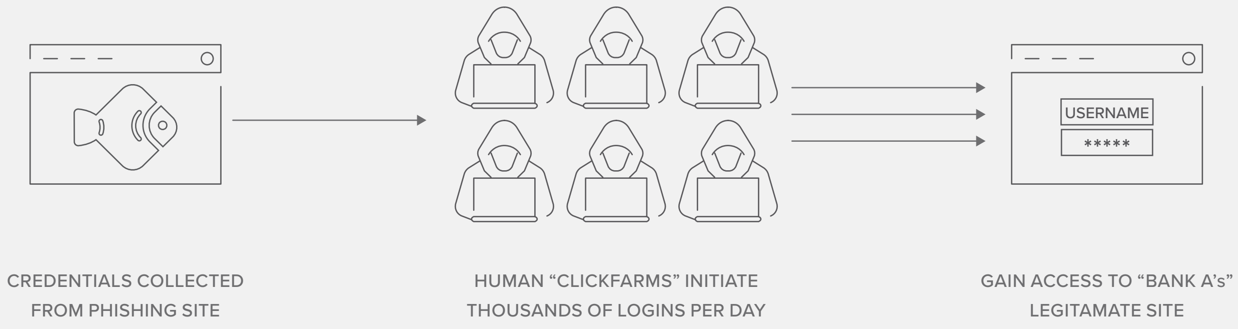
The Future of Phishing

Phishing is a lucrative business, and organized crime organizations operate much like any traditional organization. Under the leadership team are skilled individuals who specialize in different areas of phishing and fraud. Experts in human psychology and social engineering devise new lures to hook victims, web developers clone and host the fake sites, while others recruit unsuspecting members of the public to function as money mules. Since late 2018, Shape Security researchers have identified two growing trends in phishing attacks.

Where Botnets Fail, Click Farms Succeed

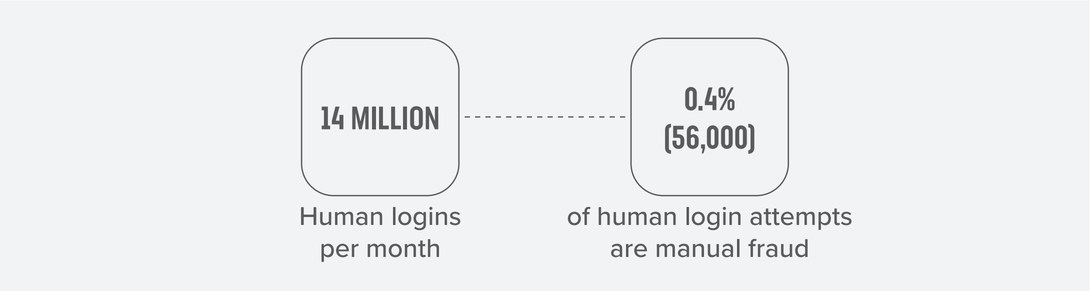
As the success of phishing continues to grow, so too does the need for the criminal organization to scale their operation. Botnets, a collection of compromised servers, home routers, and Internet of Thing (IoT) devices, allow the criminal organization to rapidly validate harvested credentials and automate fraudulent financial transactions. Over the past few years, however, security controls such as web application firewalls and fraud detection engines have become adept at detecting automated bot traffic. Aware of this, attackers are increasingly making use of click farms (see Figure 28). Dozens of remote "workers" systematically attempt to log onto the target website using recently harvested credentials. Since the connection is coming from a real human using a standard web browser, the fraudulent activity can be harder to detect than bot traffic.

FIGURE 28. CLICK FARMS ARE VIRTUAL TEAMS OF ATTACKERS MANUALLY LOGGING ONTO TARGET WEBSITES USING PHISHED CREDENTIALS


USERNAME
*****
CREDENTIALS COLLECTED
FROM PHISHING SITE
HUMAN "CLICKFARMS" INITIATE
THOUSANDS OF LOGINS PER DAY
GAIN ACCESS TO "BANK A's"
LEGITAMATE SITE

Figures from Shape Security show that, from a sample of 14 million human logins per month for one financial services customer, 0.4% were detected as humans attempting manual fraud. While this sounds like a tiny proportion of traffic, this still equates to 56,000 fraudulent login attempts.

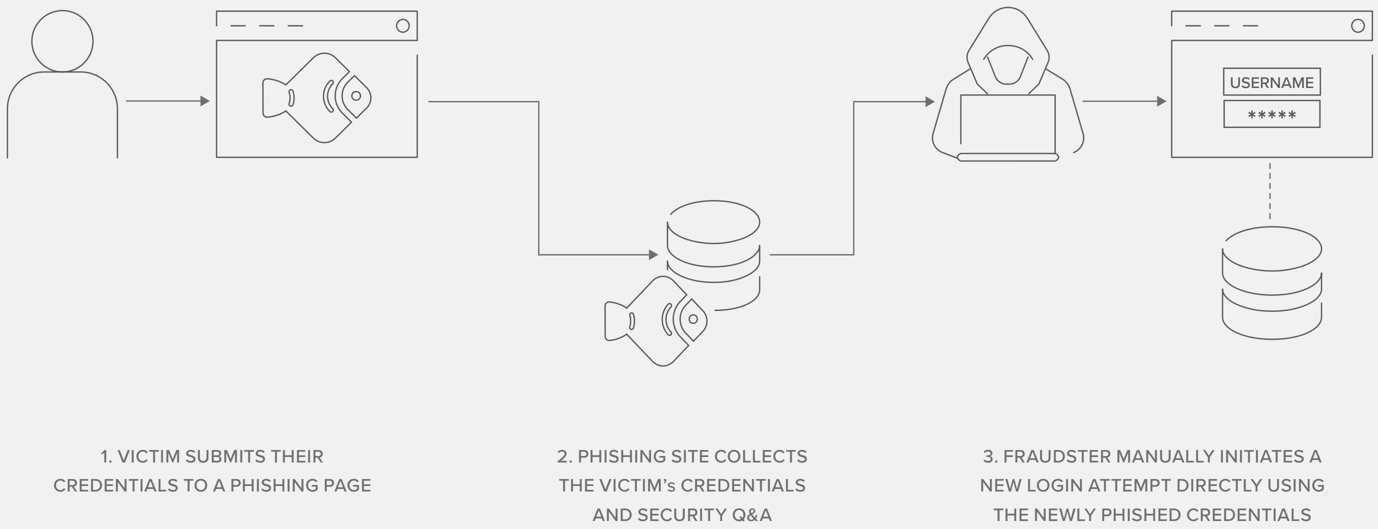
FIGURE 29. COMPARING THE TOTAL NUMBER OF HUMAN LOGINS PER MONTH TO DETECTED MANUAL FRAUD ATTEMPTS FOR A LARGE FINANCIAL SERVICES CUSTOMER



The Emergence of Real-Time Phishing Proxies

Phishing is typically an asynchronous attack in which the attacker does not need to be active at the same time a victim is using their phishing site. Fraudsters craft an email, SMS, or voicemail, wait for victims to log onto the fake site and then, at some time in the future, collect the stolen credentials and attempt to log onto the target website (see Figure 30).

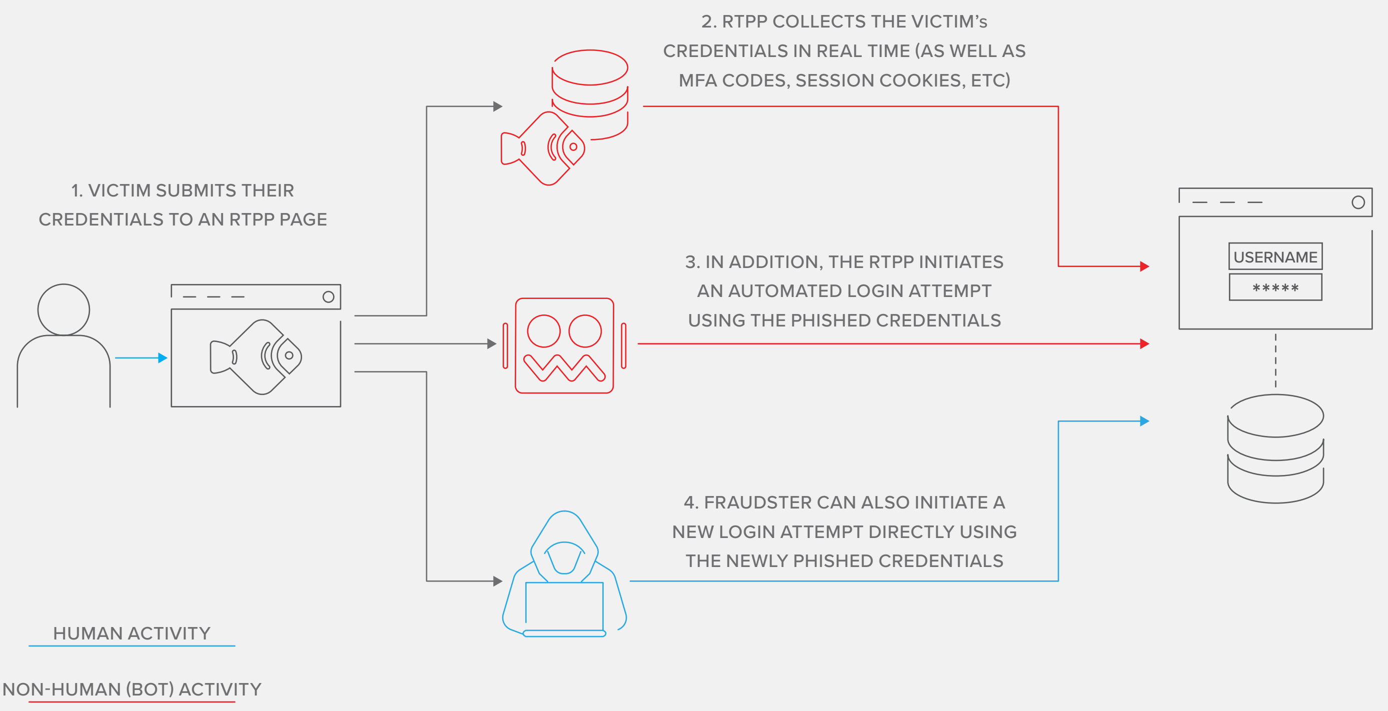
FIGURE 30. STEPS IN A TRADITIONAL ASYNCHRONOUS PHISHING ATTACK


USERNAME
*****
1. VICTIM SUBMITS THEIR CREDENTIALS TO A PHISHING PAGE
2. PHISHING SITE COLLECTS THE VICTIM's CREDENTIALS AND SECURITY Q&A
3. FRAUDSTER MANUALLY INITIATES A NEW LOGIN ATTEMPT DIRECTLY USING THE NEWLY PHISHED CREDENTIALS

This traditional model has several disadvantages. The longer the attacker waits to collect harvested credentials, the more likely the victim is to have reported the attack or changed their password. The model also struggles to contend with time-based authentication systems, such as multi-factor authentication (MFA) schemes. Standard phishing pages commonly ask the victim to enter far more information than simply their username and password. Often, they will ask for additional data such as mother's maiden name, credit card number, postal address, and so on. These are all data that can be replayed at any point in the future. Since MFA codes—typically 6- or 8-digit numbers—change every 30 to 60 seconds, it is not possible for an attacker to capture one and reuse it hours or days later.

Shape Security researchers have recently found an increase in the number of real-time phishing proxies (RTPP) that can capture and use MFA codes. Instead of setting up a phishing site and directing users to it, the RTPP acts as a person-in-the-middle and intercepts the victim's transactions with the real website. Since the attack occurs in real time, the malicious website can automate the process of capturing and replaying time-based authentication such as MFA codes and can even steal and reuse session cookies.

FIGURE 31. REAL-TIME PHISHING PROXIES (RTPP) REUSING A VICTIM'S DATA IN REAL TIME



1. VICTIM SUBMITS THEIR CREDENTIALS TO AN RTPP PAGE

2. RTPP COLLECTS THE VICTIM's CREDENTIALS IN REAL TIME (AS WELL AS MFA CODES, SESSION COOKIES, ETC)

3. IN ADDITION, THE RTPP INITIATES AN AUTOMATED LOGIN ATTEMPT USING THE PHISHED CREDENTIALS

4. FRAUDSTER CAN ALSO INITIATE A NEW LOGIN ATTEMPT DIRECTLY USING THE NEWLY PHISHED CREDENTIALS

TABLE 2. THE PROS AND CONS OF TRADITIONAL AND REAL-TIME PHISHING MODELS

Table 2 compares characteristics of traditional phishing with the use of real-time phishing proxies.

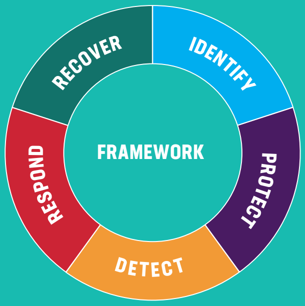
	Traditional Phishing	Real-time Phishing Proxy (RTPP)
Method	Fraudster creates a replica of the target website using a clone or phishing kit.	RTPP acts as person-in-the-middle, dynamically intercepting requests from the client and initiating a new connection from the attacker to the target site.
Timing	Asynchronous; credentials are harvested for use hours or days later	Synchronous; attacks conducted in real time as user interacts with phishing site
Information gathered	Usernames, passwords, answers to security questions	Usernames, passwords, answers to security questions, MFA codes, session cookies
Pros (for fraudsters)	Easy to set up	Difficult to detect and shutdown, able to defeat MFA schemes
Cons (for fraudsters)	Services exist to detect and shutdown phishing sites	Requires advanced knowledge to set up

Two real-time phishing proxies found in active use are Modlishka and Evilginx2.,[xiv] [xv] F5 Labs and Shape Security will be monitoring the growing use of RTPP over the coming months.

Combating Phishing

As with other social engineering tactics, phishing attacks look to exploit the human element of any system. While businesses can and should look to ensure they are taking a proactive stance to combat phishing, end users also need to be vigilant.

FIGURE 32. THE NIST CYBERSECURITY FRAMEWORK FIVE FUNCTIONS



Protecting the Business

Every organization will be a target of phishing attacks, whether those attacks are directed or indiscriminate. Not all organizations implement robust information security management frameworks, however, and while many of them accomplish the same goals, the NIST Five Functions[xvi] provides a useful way to think about any cyber threat.

Identify Your Assets and Highly Targeted Users

- Learn how your brand or business might be targeted.
- Consider use of attack chain frameworks, such as ATT&CK,[xvii] to help identify likely avenues of phishing messages (for example, email, SMS, WhatsApp, Facebook, etc.).
- Consider staff members as well as customers.
- Understand how attackers are likely to clone your site.
- Determine which staff members are high risk (C-level, finance operators, IT administrators).
- Think about which suppliers or services fraudsters may use to trick employees.
- Understand the workflow and authorization procedure for financial transactions.
- Identify all web properties that could be compromised by fraudsters to host phishing pages.

Protect Your Users and Your Networks

- Train staff members in modern phishing tactics such as fraudsters emulating Office 365 login pages.
- Implement strong password practices.
  - Monitor lists of breached accounts and passwords.
  - Proactively ask staff and customers to change passwords should their account be detected in another data breach.
  - Do not allow the use of the most common passwords.
- Implement multifactor authentication wherever possible, particularly for high-risk people and technology. Understand the limitations of MFA and how attackers can circumvent it.
- Consider technologies to mitigate web app compromise, bot attacks, and fraudulent transactions (automated and manual).
- Ensure that web apps and content management system (CMS) plugins are always up to date to reduce chances of the website becoming compromised.
- Block frequently abused domains, such as 000webhostapp.com, appspot.com, etc.
- Block or closely monitor traffic to newly registered domains.

Detect Encrypted Traffic and Active Phishing

- Discover phishing sites impersonating your business.
  - Monitor certificate transparency (CT) logs.
  - Monitor newly registered domains.
  - Make use of a phishing detection service.
- Monitor inbound traffic.
  - Detect automated (bot) transactions to minimize malicious login attempts
- Monitor encrypted outbound traffic.
  - Block non-standard outbound web ports to prevent malware communicating with command and control and drop zone servers.
  - Inspect SSL/TLS connections to ensure that malicious and potential phishing web traffic is being blocked.

Respond to Phishing Campaigns

- Have a plan and know who to work with to take down phishing sites as soon as they are identified.
- Investigating phishing sites can identify the primary target and activity of the fraudster, but evasion techniques may make this difficult.
  - Make use of a good VPN service and user-agent switcher extension for your browser when performing reconnaissance.
  - Consider a dedicated mobile device for investigative purposes since phishing sites may only reveal themselves if the correct target device tries to connect.
- Despite the best efforts of the business, customers and end-users are likely to identify more phishing attacks and malicious sites than any security control. It is essential that users have a clear and simple way to report successful and unsuccessful phishing attempts to your business.

Recover and Improve Your Phishing Plan

- Good information security management policies should be constantly evolving.
- Learn from active phishing attempts and successful attacks to focus on the most targeted job roles within the business.
- Put policies in place in order to deal with and recover from successful phishing attempts. Plan how to deal with stolen credentials, fraudulent money transfers, and unauthorized access to networks, applications, and data.

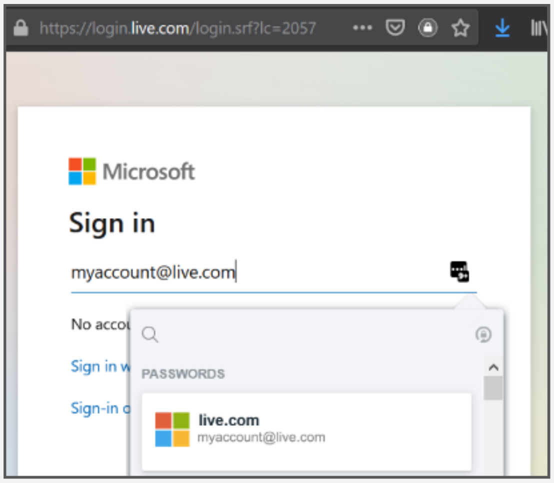
Protecting Users

Regardless of the lengths to which businesses go to protect their brand and their customers, the end user will always be a target of social engineering attacks. Just as security programs must keep up to date with changing tactics, so too must consumers. Here are some useful tips to avoid losing your password and, possibly, your life savings.

Use a Password Manager

A password manager—best used as a browser extension—serves two obvious purposes. Firstly, it helps create random and unique passwords for each site you visit. This is incredibly important password hygiene as it prevents the theft of your password from one website being used against you on another. Secondly, it remembers them all for you. All you need to remember is one long complex password which, yes, is okay to write down (so long as you leave it at home). But the less talked about benefit of the password manager is the ability to automatically enter your passwords into web sites for you (autofill), and the side benefit this has of potentially highlighting malicious sites. Since password managers will only autofill your password for a domain it recognizes, any spoofed site, no matter how genuine looking, will not prompt the extension to autofill (see Figure 33 and Figure 34).

FIGURE 33. PASSWORD MANAGER HAS KNOWN PASSWORDS FOR THIS SITE



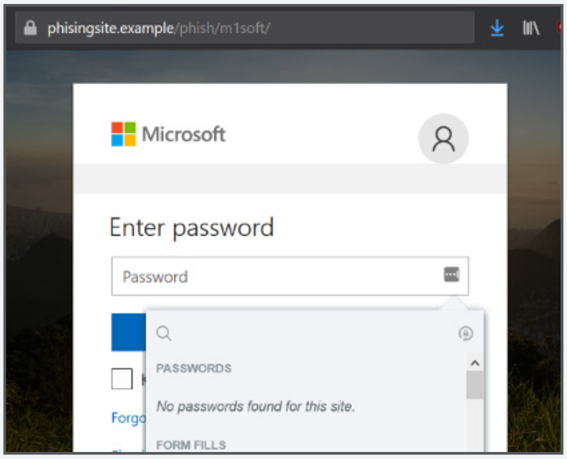
https://login.live.com/login.srf?lc=2057

Microsoft

Sign in

myaccount@live.com

FIGURE 34. PASSWORD MANAGER HAS NO SAVED PASSWORDS FOR THIS DOMAIN



phisingsite.example/phish/m1soft/

Microsoft

Enter password

Password

No passwords found for this site.

Don’t Trust the Padlock!

We’ve been teaching users for years to “look for the padlock.” With almost 80% of all phishing sites now using HTTPS certificates, simply looking for the padlock or an address that starts with https:// is no longer suitable. In fact, it’s actively dangerous to advise this since it implies that sites are inherently trustworthy simply by having a digital certificate. We must train users to look for the valid domain at the end of the URL.

Never Click on Links in Emails

From hiding hyperlinks to disguising text as images, there are too many ways for fraudsters to mask the real destination of a hyperlink within an email. Many businesses now recognize this and do not include links in emails (although many still do). Consumers must become develop the habit of entering the website address themselves and manually searching for the information they seek.

Use Prepaid or Disposable Credit Cards

Similar to how multi-factor tokens constantly change their value, disposable credit cards allow shoppers to use a credit card with a constantly changing card number. These cards allow users to pay for goods and services online without worrying about their payment card details being stolen. After each transaction, the disposable credit card generates a brand-new card number for the subsequent use. Should a cybercriminal manage to capture payment card details, they will soon find that this card number has immediately become invalidated.

Conclusion

Phishing attacks will continue to be successful as long as there is a human who can be psychologically manipulated in some way. Security controls and web browsers alike must become more proficient at highlighting fraudulent sites to users. From deceptive URLs to abuse of HTTPS certificates, both staff and customers must be continuously trained on the latest techniques that fraudsters are using.

Our Methods

This year we have combined multiple data sources in order to provide the most accurate and consistent conclusions as possible. There are, however, always limitations when comparing data collected from different sources, and understanding the context and limitations of the data is important before drawing conclusions.

Datasets Used in This Report

F5 Security Operations Center

This dataset contains details of all security incidents affecting customers in which the SOC was involved to help remediate the situation. This detailed dataset allowed us to analyze incidents over a five year period with accurate incident dates, compare domain names and paths with customer names, track attacks across industry sectors, and compare the use of insecure HTTP and secure HTTPS malicious URLs.

The limitations of this data are related only to the comparatively small sample size when compared with data from BrightCloud Threat Intelligence or the Phishing Database. However, what this data lacks in size it makes up for in context and richness. Our own data have a wealth of metadata associated with it from specific incident dates and times through to customer names and industry sector.

BrightCloud Threat Intelligence Phishing Sites

Webroot, an OpenText company, kindly sent us a sample of phishing sites that were active in September 2020 from their BrightCloud Threat Intelligence. We used this list of sites to probe for HTTPS certificates and build a comprehensive picture of domain and TLD use. With the number of malicious sites that employ evasion techniques, it's important to remember that automated scanning of sites has its limits. The scan may either fail to connect to a URL if the site has been removed completely, or it may capture misleading information if the site is actively redirecting automated traffic.

Open Source Phishing Lists

We used phishing sites URL obtained from:

- Phishing Database: 78,411 phishing URLs of which 37,578 were active as of September 2020
- OpenPhish: 3,208 phishing URLs, all of which were active as of September 2020.

Vigilante:

- We used the Vigilante Darkweb Intelligence service to search for stolen payment card details.

Glossary

APT	Advanced persistent threat. An organized group of expert threat actors who favor the use of specific tactics, techniques, and procedures (TTPs).
APWG	Anti-Phishing Working Group. A consortium of businesses, law enforcement, and cyber security organizations who share intelligence to educate and combat phishing.
BEC	Business email compromise. A spear phishing attack that targets staff with the power of authorizing financial transactions. Attackers impersonate senior staff, often CEOs, requesting funds be transferred to a new account.
Bot, Botnet	A computer, mobile device, or Internet of Things (IoT) device that has been compromised and is under the control of a threat actor. Botnets, collections of bots, can be tens of thousands in size and are used to launch a multitude of attacks such as denial of service, crypto-mining, and phishing and spam campaigns.
Brute force	Also known as “exhaustive search.” Any attack in which the attacker must sequentially attempt every possible combination to gain access to a resource.
C2 / C&C	Command and control. The control point (usually a web server) from which threat actors send attack instructions to compromised devices. The C2 is used to instruct bots to launch DDoS attacks or send phishing emails.
ccTLD	Country-code top-level domain (TLD). Specific TLDs were intended to be used only by certain countries. For example, .uk is reserved for the United Kingdom. Some ccTLDs, such as .tk, are now in widespread use by users all over the world.
Credential stuffing	Unlike brute force attacks that must attempt many thousands or millions of possible passwords for any one user account, credential stuffing works by attempting known good username and password combinations that have been obtained from phishing campaigns or data breaches. This attack benefits from the high number of people reusing passwords from site to site.
Darknet	Websites and services that are only available by accessing them via the Tor web browser. Many darknet sites are forums and markets that offer the sale of illegal goods or services such as drugs, firearms, and personal data. Some darknet markets are invitation-only while others allow anonymous users to sign up.
Digital Certificate	Digital certificates mathematically bind the identity of a website (its domain name) with cryptographic keys. The owner of a certificate should be trusted since only they have access to the private key.
Domain	A hierarchical structure for defining addresses on the web. Colloquially used to describe the primary website address an organization uses as its presence on the web, such as example.com. Phishers may create fraudulent domain names that appear similar to the genuine one, such as examp1e.com.
Drop zone	An attacker-controlled server used to collect and store stolen data.
Europol	The law enforcement agency of the European Union that handles criminal intelligence and combats serious international organized crime and terrorism through cooperation between authorities of EU member states.
Formjacking	Attackers can compromise a vulnerable web page or vulnerable third-party components in that page to inject malicious scripts. These scripts silently steal personal data as users interact with the infected website.
Host	The base domain on which a resource (web page, for example) is hosted.
HTTPS	The secure form of the web’s most fundamental protocol, HTTP. Makes use of TLS and certificates to secure the web and provide trust to users.
IDN	Internationalized Domain Name. Allows non-ASCII characters (for example, foreign language alphabets) to be used in domain names. IDNs are stored in DNS in ASCII using Punycode translation.
IOCTA	Internet Organized Crime Threat Assessment. An annual report on organized crime created by Europol.
Malware	The catch-all term for malicious software, including trojans, ransomware, and remote access trojans.

MFA / 2FA	Multifactor authentication (also referred to as two-factor authentication). Single factor authentication schemes rely on something you know (typically, passwords). A second (or multi) factor scheme relies on something you know and something you have, for example a token or an SMS code sent to your device. MFA schemes aim to minimize the risk of having credentials lost or stolen.
Path	The exact location on a domain that retrieves a specific resource (image or HTML, for example).
Phishing	A method of social engineering designed to trick victims into disclosing personal information. Phishing commonly manifests as fraudulent emails claiming to be from someone the victim knows. Phishing may also be conducted using SMS (text messages), voicemails, messaging services such as WhatsApp, or social media, such as Facebook. Phishing is often untargeted with fraudsters casting their net wide to capture as many victims as possible.
Phishing-as-a-Service	Some organized crime groups have created Phishing-as-a-Service platforms that aspiring fraudsters can use without having to create or host their own phishing site. Instead, they simply craft phishing emails and lure victims to a centralized phishing site.
Phishing kit	A turnkey phishing solution that includes all of the images, web pages, and tools needed to launch a phishing campaign. Phishing kits usually target one specific company or brand.
RAT	Remote Access Trojan (or Remote Administration Tool). Malware used to grant the attacker invisible access to a victim's computer, allowing them to view the screen, capture input, and even control the device.
Smishing	Phishing conducted over SMS (text messages).
Social engineering	Psychological manipulation used by criminals to trick victims into performing certain actions or divulging personal information. A form of confidence trick.
Spear phishing	Targeted phishing. Attackers construct phishing emails with very personalized details aiming to capture credentials or other personal information from a specific individual. Common targets include personal assistants, workers in finance, and board-level employees.
Subdomain	A sub-section of a website. A "child" to the domain's "parent." For example, "login" is a subdomain in login.example.com. Phishers commonly include the target's brand name in subdomains, for example yourbank.example.com.
TLD	Top-level domain. A reserved set of letters used to denote different types of organizations on the web, for example, .com, .org, .gov.
TLS	Transport Layer Security. A cryptographic protocol to secure web pages and prevent eavesdropping and tampering.
Tor	The Onion Router. The ultra-encrypted and privacy-focused network that allows users to surf the web with anonymity. The Tor network has proven useful in allowing residents in oppressive regimes to access information on the web. It also allows nefarious darknet markets to operate outside of the purview of traditional web browsers and search engines.
Trojan	An application that appears to offer a genuine and benign function but also carries with it a hidden piece of malicious code. Trojans are commonly created by tampering with genuine software (for example, teleconferencing software) and then tricking victims into installing the trojanized version of the app.
TTP	Tactics, techniques, and procedures. Specific threat actors follow a set procedure or consistently use a tool to accomplish their goal. Defining a threat group's TTPs enables defenders to profile them and track their activities.
URL	Often referred to as a web address, the Uniform Resource Locator tells web browsers where and how to connect to a resource. It includes the host and path. It may optionally specify the port to connect to as well as queries (for example, search terms) to submit to the page.
Vishing	Phishing conducted by leaving voicemails on victims' cell phones.

Endnotes

[i] https://ico.org.uk/action-weve-taken/data-security-incident-trends/

[ii] https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/

[iii] https://enterprise.verizon.com/resources/reports/dbir/

[iv] https://www.europol.europa.eu/iocta-report

[v] https://www.clearskysec.com/the-kittens-are-back-in-town-3/

[vi] https://apwg.org/trendsreports/

[vii] Use of the term “workers” in the report seems somewhat generic and it is likely that “key workers” was implied.

[viii] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

[ix] https://www.scirp.org/html/36435.html

[x] https://info.shapesecurity.com/credentialspillreportcyberwire.html

[xi] https://en.wikipedia.org/wiki/List_of_data_breaches

[xii] https://domainnamestat.com/statistics/tld/others

[xiii] https://apwg.org/trendsreports/

[xiv] https://github.com/drk1wi/Modlishka

[xv] https://github.com/kgretzky/evilginx2

[xvi] https://www.nist.gov/cyberframework/online-learning/five-functions

[xvii] https://attack.mitre.org/techniques/T1566/

F5 LABS

APPLICATION THREAT
INTELLIGENCE

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com