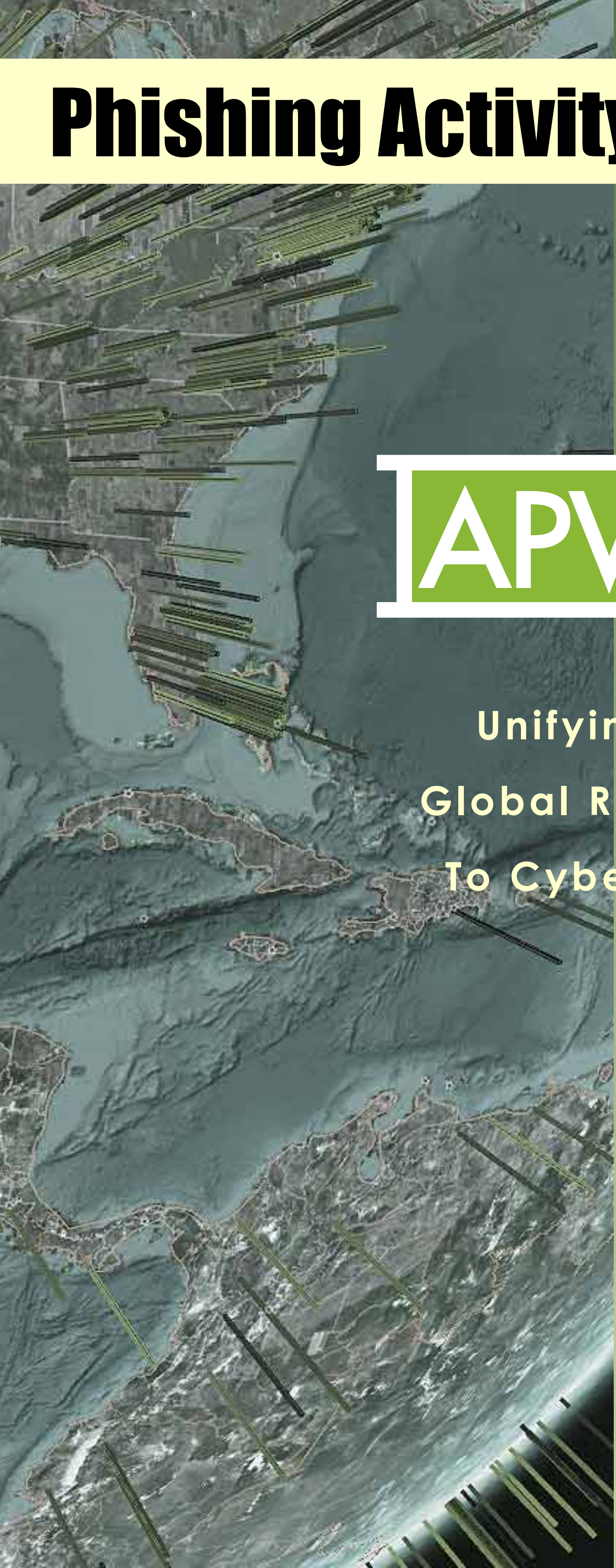
Phishing Activity Trends Report

4th Quarter 2018



APWG

Unifying the Global Response To Cybercrime

Activity October-December 2018

Published March 4, 2019

Phishing Report Scope

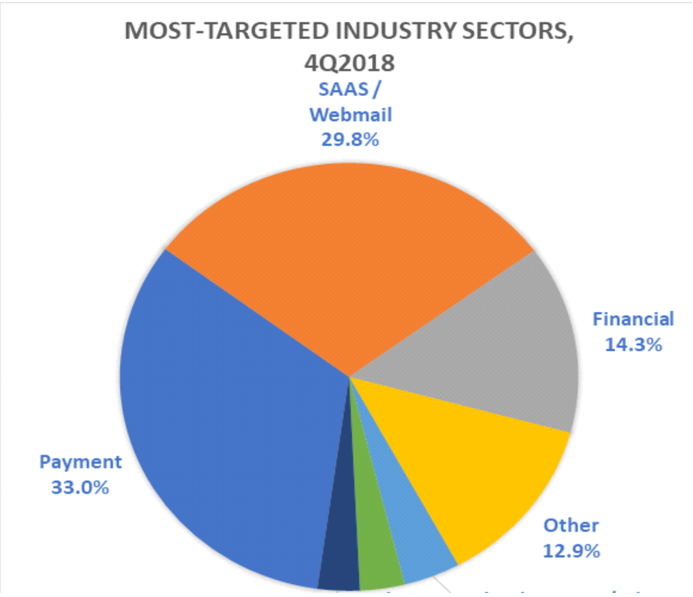
The *APWG Phishing Activity Trends Report* analyzes phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization's website at http://www.apwg.org, and by e-mail submissions to reportphishing@antiphishing.org. APWG also measures the evolution, proliferation, and propagation of crimeware by drawing from the research of our member companies.

Phishing Defined

Phishing is a criminal mechanism employing both *social engineering* and *technical subterfuge* to steal consumers' personal identity data and financial account credentials. Social engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies, designed to lead consumers to counterfeit Web sites that trick recipients into divulging financial data such as usernames and passwords. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using systems to intercept consumers online account user names and passwords -- and to corrupt local navigational infrastructures to misdirect consumers to counterfeit Web sites (or authentic Web sites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes).

Table of Contents

Phishers Shift Efforts to Attack SaaS and Webmail Services



4th Quarter 2018 Phishing Activity Trends Summary

- The number of confirmed phishing sites declined as 2018 proceeded. Detection of phishing sites has become harder because phishers are obfuscating phishing URLs with multiple redirections. [p. 4]
- Phishing that targeted SaaS and webmail services doubled in Q4. [p.5]
- The number of phishing attacks hosted on Web sites that have HTTPS and SSL certificates declined for the first time in history. [p. 9]
- In Brazil, phishers offered Black Friday sales "specials" to their criminal brethren. [p.10]
- Phishing remains most prevalent in the old, large gTLD .COM. But phishing is higher than normal in some new gTLDs and repurposed ccTLDs. [p. 6]

Statistical Highlights for 4th Quarter 2018

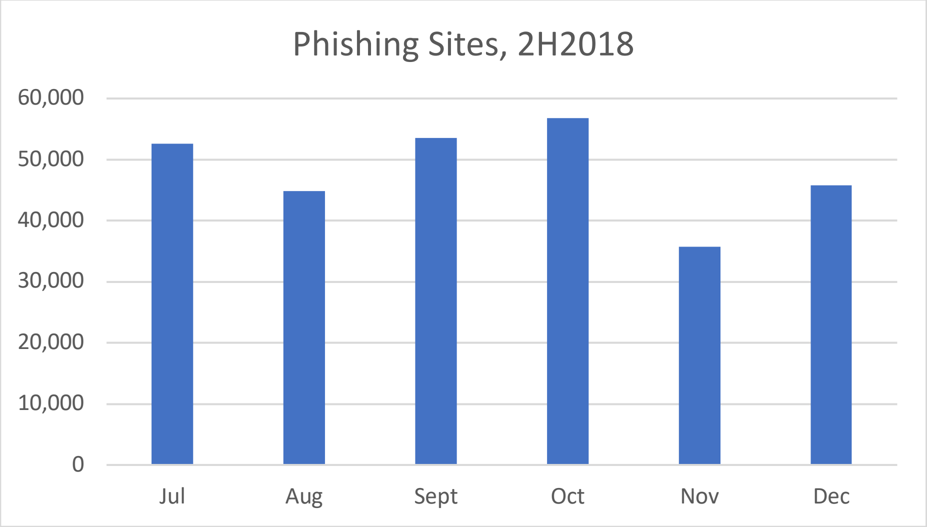
	October	November	December
Number of unique phishing Web sites detected	56,815	35,719	45,794
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	87,619	64,905	87,386
Number of brands targeted by phishing campaigns	293	233	310

The APWG continues to refine its tracking and reporting methodology and to incorporate new data sources into our reports. APWG tracks and reports the number of unique phishing reports (email campaigns) it receives. An e-mail campaign is a unique e-mail sent out to multiple users, directing them to a specific phishing web site (multiple campaigns may point to the same web site). APWG counts unique phishing report e-mails as those found in a given month that have the same email subject line.

The APWG also tracks the number of unique phishing Web sites. This is now determined by the unique base URLs of the phishing sites. (A single phishing site may be advertised as thousands of customized URLs, all leading to basically the same attack destination.) APWG's contributing members also track a variety of additional metrics and data sets in order to track the fast-paced nature of cybercrime.

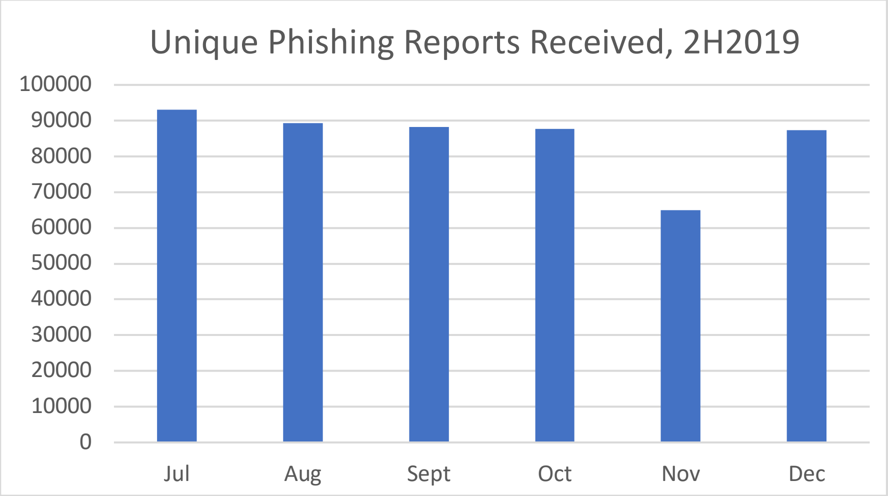
Phishing Site and Phishing E-mail Trends – 4th Quarter 2018

The total number of phishing sites detected by APWG in 4Q was 138,328. That was down from 151,014 in Q3, 233,040 in Q2, and 263,538 in Q1. The number of phishing sites dropped notably in November before returning to previous levels.



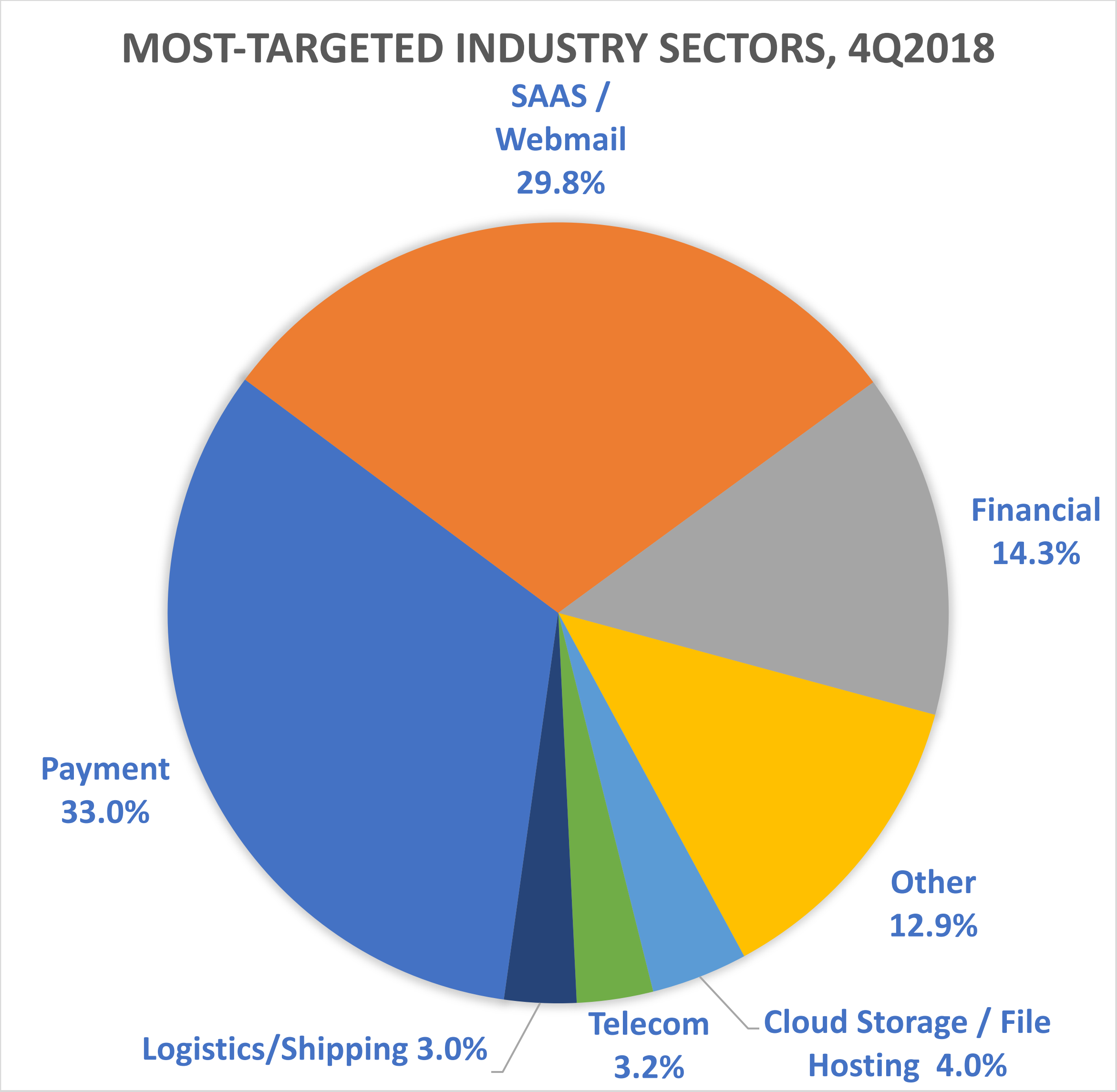
As reported in Q3, MarkMonitor is still detecting an increased number of redirectors prior to the phishing landing page - and as well after the victim submits his or her data - in an effort to obfuscate phishing URLs from detection.

The number of unique phishing reports submitted to APWG during Q4 of 2018 was 239,910, decreasing slightly from the 264,483 in 3Q and the 262,704 seen in Q2:



Most-Targeted Industry Sectors – 4th Quarter 2018

APWG member MarkMonitor saw phishing that targeted software as a service (SaaS) and Webmail services' brands jump from 20.1 percent of all attacks in Q3 to almost 30 percent in Q4. Attacks against cloud storage and file hosting sites continued to drop, decreasing from 11.3 percent of all attacks in Q1 2018 to 4 percent in Q4. Founding APWG member MarkMonitor secures intellectual property and reputations through anti-fraud, brand protection, domain management, and anti-piracy solutions.

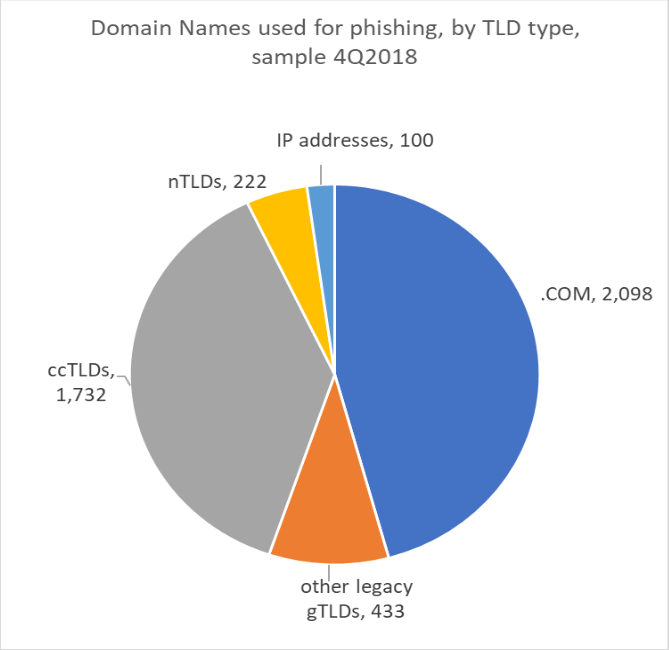


Use of Domain Names for Phishing

RiskIQ analyzed 6,718 confirmed phishing URLs reported to APWG in Q4 2018, and found that they were hosted on 4,485 unique second-level domains (and 100 were hosted on unique IP addresses, without domains). There are three types of top-level domains (TLDs) for purposes of this report:

- "Legacy" generic TLDs, which existed before 2011. These include .COM, .ORG, and TLDs such as .ASIA and .BIZ. They represented 49.57 percent of the domain names in the world as of the beginning of Q4, and represented 56.43 percent of the phishing domains in the sample set. Most of these were in .COM, which had 2,098 domains in the set. There were 2,531 legacy gTLDs in the sample set.
- The new generic top-level domains (nTLDs), such as .ONLINE and .XYZ, were all released after 2011. As of the beginning of Q4, the nTLDs represented 6.83 percent of the domains in the world, and 4.95 percent of the domains in the sample set. There were 222 nTLD domains in the set.
- The country code domains (ccTLDs), such as .UK for the United Kingdom and .MX for Mexico. ccTLDs were 43.6 percent of the domains in the world as of the beginning of Q4, and were 38.62 percent of the domains in the sample set. There were 1,732 ccTLD domains in the sample set. ccTLD Internationalized domain names are included as part of this category, but there was only one such domain (.рф) in the set.

APWG member RiskIQ provides ongoing analysis of where phishing is happening the domain name system. RiskIQ provides digital risk protection by illuminating risk associated with an organization's digital presence in open, deep and dark web, mobile, and social digital channels to proactively protect organizations, brands, people, and data.



The top 20 TLDs used were:

RANK	TLD	TYPE OF TLD	Number of unique domains used for phishing
1	.COM	Legacy gTLD	2,098
2	.PW	ccTLD (Palau)	374
3	.NET	Legacy gTLD	175
4	.ORG	Legacy gTLD	154
5	.UK	ccTLD (UK)	121
6	.CF	ccTLD (Central African	84
7	.INFO	Legacy gTLD	83
8	.BR	ccTLD (Brazil)	82
9	.ML	ccTLD (Mali)	78
10	.GA	ccTLD (Gabon)	68
11	.IN	ccTLD (India)	58
12	.US	ccTLD (USA)	45
13	.RU	ccTLD (Russian Fed.)	44
14	.TK	ccTLD (Tokelau)	40
15	.GQ	ccTLD (Equatorial Guinea)	37
16	.IT	ccTLD (Italy)	37
17	.XYZ	New gTLD	37
18	.ONLINE	ccTLD	33
19	.PL	ccTLD (Poland)	28
20	.CA	ccTLD (Canada)	26

This phishing in some of the TLDs is at an expected level – for example .COM, .NET,.ORG, and .UK are large, long-established TLDs with large numbers of web sites in them and therefore are expected to have some that are on vulnerable hosting that is compromised by phishers. But some of the ccTLDs that had notable amounts of phishing in them were places that phishers went to register domain names directly to perpetrate their crimes. These include the "repurposed" ccTLDs on the list – TLDs where management rights have been granted to third parties who have then commercialized them. .TK, .ML, .GA, .CF, and .GQ are all operated by a Dutch company that offers domain names in those TLDs for free, while .PW is operated by a company based in India.

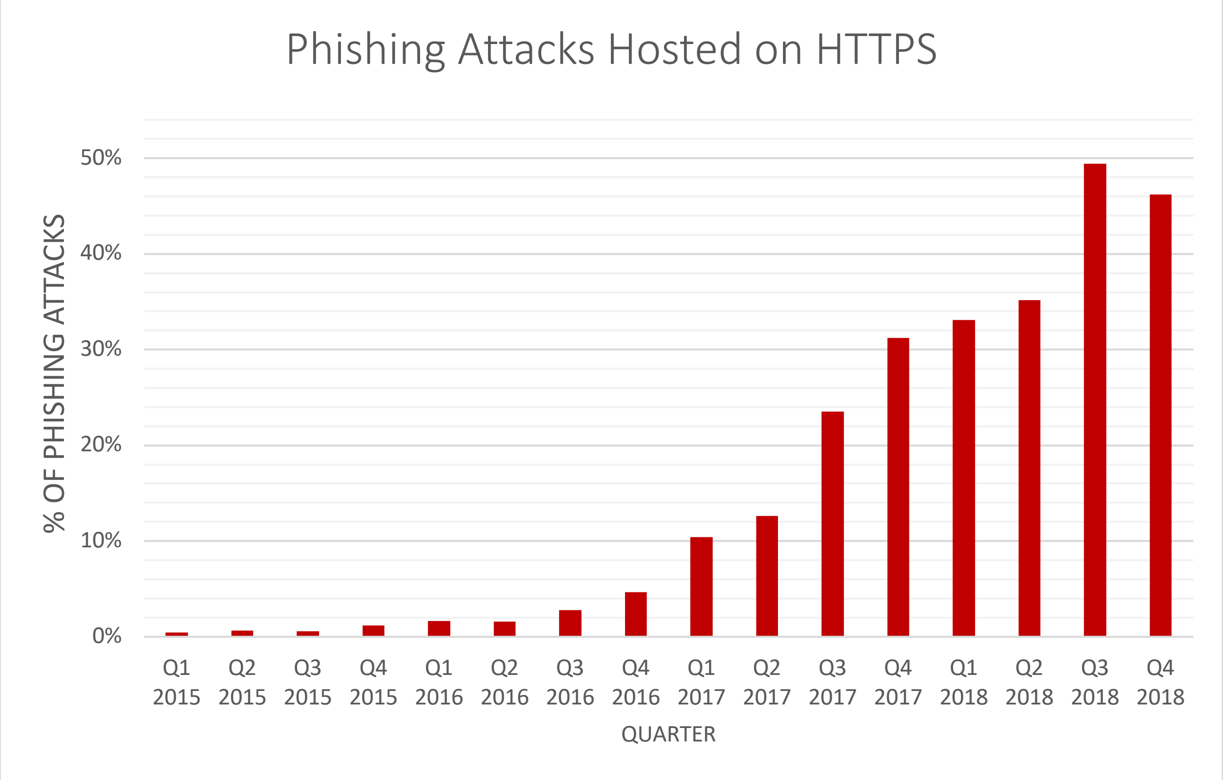
“.XYZ represented 8 percent of the registered nTLD domain names in the world as of the beginning of the quarter, but 16.67 percent of the reported phishing nTLDs in the quarter,” said Jonathan Matkowsky of RiskIQ. “.LOAN was a larger piece of the total nTLD market than .XYZ as of the beginning of the quarter, but there was only one reported .LOAN domain used for phishing in our sample set. .TOP represented 14.4 percent of the total new gTLD market at the beginning of the quarter, but only 4.5 percent of the reporting phishing domains this quarter—half as many as in Q3.”.

RiskIQ also analyzed unique third-level domains that targeted numerous brands on the same unique second-level domain. The domain 000WEBHOSTAPP.COM hosted phishing sites targeting at least 14 unique brands on more than 90 unique third-level domains. 000WEBHOSTAPP.COM is operated by Hostinger International Ltd, a Cyprus private limited company. A user can sign up for a free hosting account with Hostinger by becoming a user of 000webhost. Members can set up a free web hosting account from the provided control panel with instant activation, an ease-of-use that is employed by both honest and criminal users alike. 5GBFREE.COM (associated with NETHOSTING.COM and FIBER.NET) hosted phishing sites targeting at least five unique brands on at least 15 unique third level domains. 5GBfree is an online free website hosting site.

How Phishers Use Encryption to Fool Victims

APWG contributor PhishLabs has been tracking how many phishing sites are protected by the HTTPS encryption protocol. HTTPS is used to secure communications by encrypting the data exchanged between a person's browser and the web site he or she is visiting. HTTPS is especially important on sites that offer online sales or password-protected accounts. Studying HTTP on phishing sites provides insight into how phishers are fooling Internet users by turning an Internet security feature against them. PhishLabs provides managed security services that help organizations protect against phishing attacks targeting their employees and their customers.

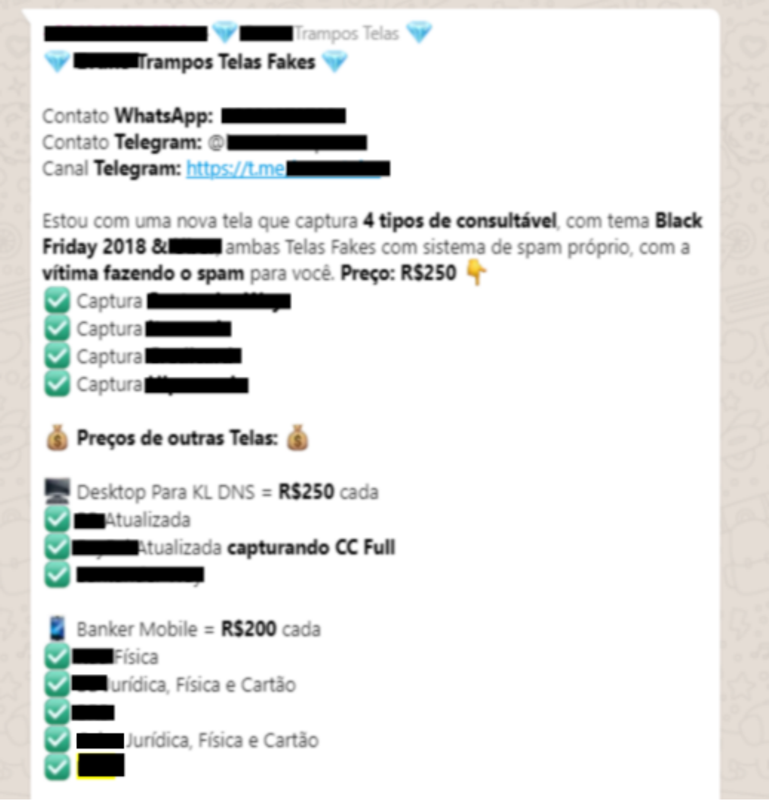
In 4Q 2018, for the first time since PhishLabs began measuring use of the HTTPS encryption protocol, the number of phishing sites protected by HTTPS fell. "Phishing sites using SSL decreased slightly in Q4 2018 compared with Q3 – down 3 percent to about 47 percent," said John LaCour, Chief Technology Officer of PhishLabs. "However, it remains true that nearly half of phishing sites use digital certificates to makes attacks look more legitimate and avoid browser warnings."



Default protocol HTTPs was used by 48.4% of all the websites in December 2018. Many phishing attacks are on hacked web sites, so it is not surprising that about the same percentage of phishing sites use the HTTPS encryption protocol.

Phishing and Identity Theft Techniques in Brazil

In November Brazil-based Axur observed phishing kits being sold with a Black Friday theme. Phishing kits are software packages that allow a phisher to set up phishing sites, send out spam messages to lure in victims, collect the data from the victims, and other useful capabilities. This kind of phishing is very popular in Brazil during the week preceding Black Friday and it affects the country's main e-commerce companies. The ad below offers phishing templates that collect four types of personal information from victims:



[redacted] 💎 [redacted] Trampos Telas 💎
💎 [redacted] **Trampos Telas Fakes** 💎

Contato **WhatsApp:** [redacted]
Contato **Telegram:** @[redacted]
Canal **Telegram:** https://t.me[redacted]

Estou com uma nova tela que captura **4 tipos de consultável**, com tema **Black Friday 2018 &**[redacted] ambas Telas Fakes com sistema de spam próprio, com a **vítima fazendo o spam** para você. **Preço: R$250** 👇
✅ Captura [redacted]
✅ Captura [redacted]
✅ Captura [redacted]
✅ Captura [redacted]

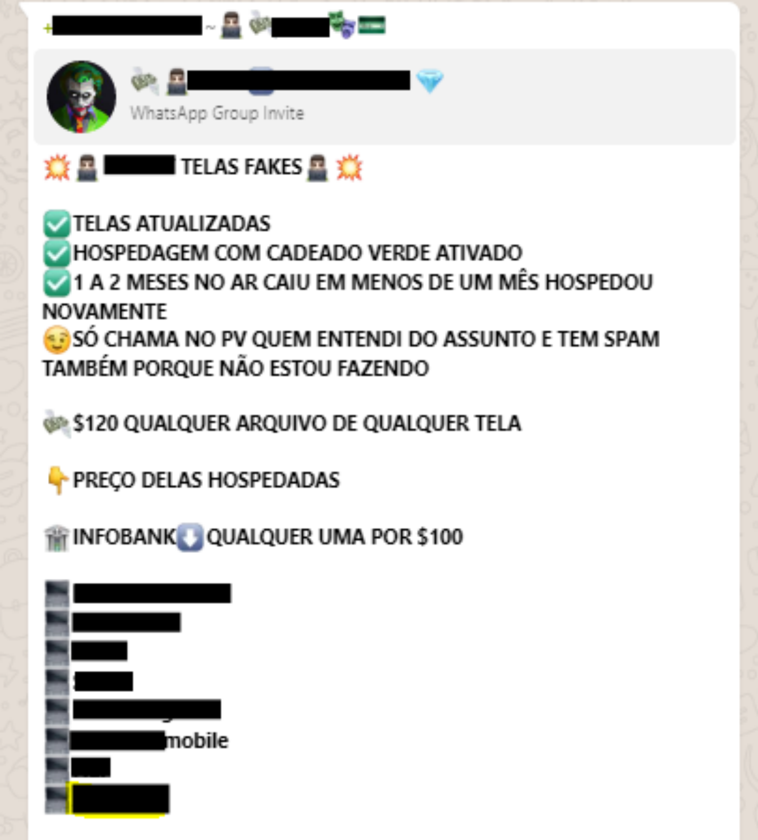
💰 **Preços de outras Telas:** 💰

🖥 Desktop Para KL DNS = **R$250** cada
✅ [redacted] Atualizada
✅ [redacted] Atualizada **capturando CC Full**
✅ [redacted]

📱 Banker Mobile = **R$200** cada
✅ [redacted] Física
✅ [redacted] urídica, Física e Cartão
✅ [redacted]
✅ [redacted] Jurídica, Física e Cartão
✅ [redacted]

This template also comes with a mailer that uses the victim's machine itself to send the phishing campaign to the victim’s contacts. The price asked by the criminal is 250 Brazilian Reais**,** equivalent to about 70 American dollars. In the middle of the message, starting at "Preco de outras telas,” the phisher is selling other templates and says that these are updated to match the target brand websites. Also, the code tries to change the victim's router DNS, probably using the same techniques as the GhostDNS attack that happened back in 2018. At the end of the message, starting at "Banker Mobile,” the phisher is selling phishing with a (mobile/responsive) layout at the price of 200 Brazilian Reais, equivalent to about 55 American dollars. This phishing kit works with both a personal checking account and a business checking account.

This ad sells a different phishing kit:



+[redacted] ~ 👩‍💻 💸 [redacted] 🎭 💵

💸 👩‍💻 [redacted] 💎
WhatsApp Group Invite

💥👩‍💻 [redacted] TELAS FAKES 👩‍💻💥

✅TELAS ATUALIZADAS
✅HOSPEDAGEM COM CADEADO VERDE ATIVADO
✅1 A 2 MESES NO AR CAIU EM MENOS DE UM MÊS HOSPEDOU NOVAMENTE
😉SÓ CHAMA NO PV QUEM ENTENDI DO ASSUNTO E TEM SPAM TAMBÉM PORQUE NÃO ESTOU FAZENDO

💸$120 QUALQUER ARQUIVO DE QUALQUER TELA

👇PREÇO DELAS HOSPEDADAS

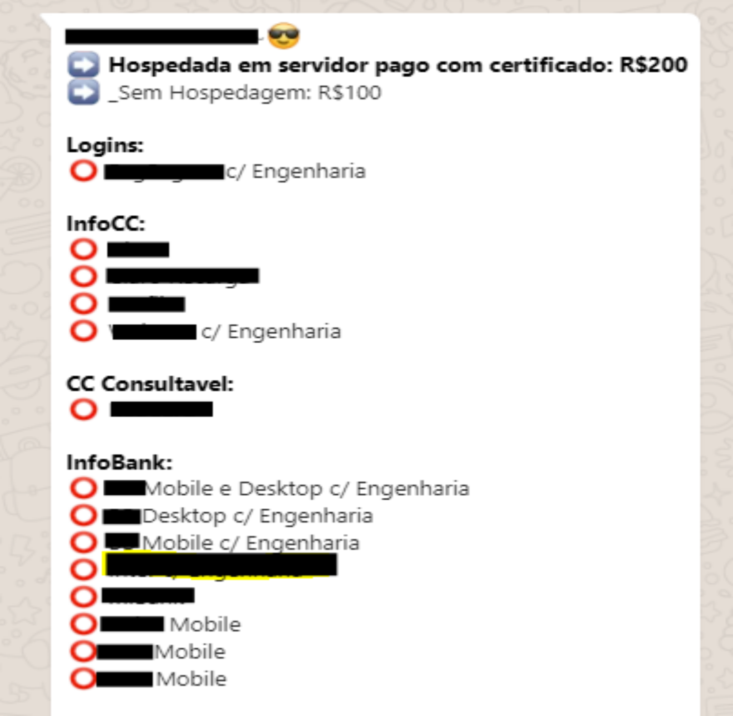
🏦INFOBANK⬇️QUALQUER UMA POR $100

[redacted]
[redacted]mobile
[redacted]

This kit is already hosted on a specific ISP. The criminal guarantees that the phishing web sites will remain active on the ISP for one to two months, and if removed before the first month, he will host them again for free. This is what's called "bulletproof hosting" – criminal hosting that will ignore requests from banks and victims to take the phishing sites offline. The kit seller asks interested customers to call him in private for more information, but only if you know what you are doing and possess a spamming email list, because he will not provide one. The price for this phishing kit is 120 Brazilian Reais, equivalent to about 32 American dollars. The criminal also offers information regarding bank accounts at the price of 100 Brazilian Reais, equivalent to about 27 American dollars.

Also, Axur has detected phishing templates that display a "Loading" or standby message to victims. This "loading page" disappears and is replaced by a phishing page only when the criminal contacts the victim. This kind of fraud is very hard for ISPs to spot and remove due to the fact that the actual phishing content is hidden until something specific happens.

This last ad sells phishing kits that are already set up with hosting and with an SSL certificate for 200 Brazilian Reais, equivalent to about 55 American Dollars. The price of the kit is half of that when purchased without hosting.



[redacted] 😎

➡ **Hospedada em servidor pago com certificado: R$200**
➡ _Sem Hospedagem: R$100

Logins:
○ [redacted] c/ Engenharia

InfoCC:
○ [redacted]
○ [redacted]
○ [redacted]
○ [redacted] c/ Engenharia

CC Consultavel:
○ [redacted]

InfoBank:
○ [redacted] Mobile e Desktop c/ Engenharia
○ [redacted] Desktop c/ Engenharia
○ [redacted] Mobile c/ Engenharia
○ [redacted]
○ [redacted]
○ [redacted] Mobile
○ [redacted] Mobile
○ [redacted] Mobile

The word "Engenharia" refers to "Social Engineering" and is used to communicate that the kit includes this stand-by page.

APWG member company Axur is located in Brazil and concentrates on protecting companies and their users in Brazil from Internet-based threats. Axur especially monitors attacks against banks, technology firms, airlines, and online marketplaces located in the country. Axur's data shows how criminals are perpetrating identity theft in South America's largest economy, and shows how these incidents are both a local and international problems.

.

APWG Phishing Activity Trends Report Contributors

AXUR

Axur works to identify and fight the threats in the cyberspace that interfere with the interests of companies, governments, and individuals

iThreat Cyber Group

iThreat provides risk data, intelligence tools, and analysis to help its clients protect their intellectual & Internet properties.

MarkMonitor
Protecting brands in the digital world

MarkMonitor, a global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks.

PHISHLABS

PhishLabs provides 24/7 managed security services that help organizations protect against phishing attacks targeting their employees and customers.

RISKIQ

RiskIQ is a digital threat management company enabling organizations to discover, understand and mitigate known, unknown, and malicious exposure across all digital channels

About the APWG

Founded in 2003, the Anti-Phishing Working Group (APWG) is a not-for-profit industry association focused on eliminating the identity theft and frauds that result from the growing problem of phishing, crimeware, and e-mail spoofing. Membership is open to qualified financial institutions, online retailers, ISPs, solutions providers, the law enforcement community, government agencies, multi-lateral treaty organizations, and NGOs. There are more than 2,000 enterprises worldwide participating in the APWG.

APWG maintains it public website, <http://www.antiphishing.org>; the website of the STOP. THINK. CONNECT. Messaging Convention <http://www.stopthinkconnect.org> and the APWG's research website <http://www.ecrimeresearch.org>. These are resources about the problem of phishing and Internet frauds– and resources for countering these threats. The APWG, a 501(c)6 tax-exempted corporation, had its first meeting in November 2003 in San Francisco and was incorporated in 2004 as an independent corporation controlled by its board of directors, its executives and its steering committee.

The *APWG Phishing Activity Trends Report* is published by the APWG. For further information about the APWG, please contact APWG Deputy Secretary General Foy Shiver at +1.404.434.7282 or foy@apwg.org. For media inquiries related to the company-content of this report, please contact APWG Secretary General Peter Cassidy at +1.617.669.1123; Stefanie Ellis at Stefanie.ellis@markmonitor.com; Eduardo Schultze of Axur at +55 51 3012-2987, eduardo.schultze@axur.com; Stacy Shelley of PhishLabs at 1.843.329.7824, stacy@phishlabs.com, Kari Walker of RiskIQ at +1.703.928.9996, Kari@KariWalkerPR.com, +1.703.928.9996. **Analysis and editing by Greg Aaron, iThreat Cyber Group.**