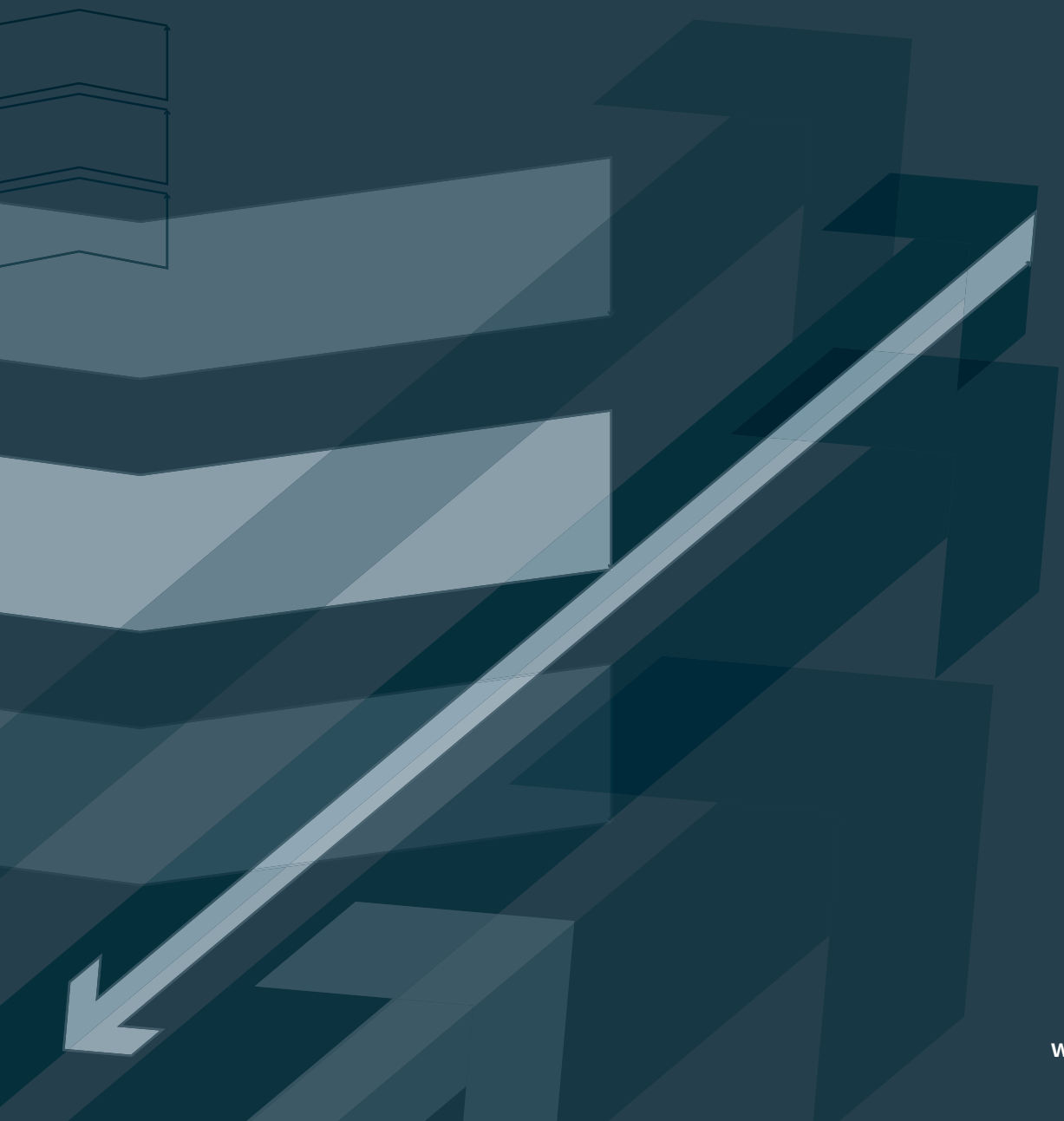
PHISHLABS

PHISHING TRENDS & INTELLIGENCE REPORT

Q2 2017



www.phishlabs.com

Overall phishing volume in the second quarter of this year was 41% higher than in the first quarter.

INTRODUCTION

Welcome to the Q2 2017 Phishing Trends and Intelligence (PTI) Report. This is the second quarterly report of 2017. As with the annual PhishLabs PTI Reports, the quarterly reports provide insight into significant trends, tools, and techniques being used to carry out phishing attacks.

The data and observations presented in this report are sourced from the continuous work PhishLabs does to fight back against phishing attacks and the threat actors behind them. The information highlighted in this report will help organizations better assess and mitigate the risk posed by modern phishing attacks.

Key findings of the Q2 2017 PTI Report include:

- Overall phishing volume in Q2 was 41% higher than in Q1.
- The volume of phishing attacks targeting the financial industry nearly doubled in Q2 and is the largest quarterly volume PhishLabs has ever observed.
- Nearly 88% of attacks in the second quarter targeted five industries: financial institutions, webmail/online services, payment services, cloud storage/file hosting services, and e-commerce companies.
- The volume of attacks targeting SaaS platforms increased 104% quarter-over-quarter, doubling the total volume of SaaS platform attacks observed in all of 2016.
- The volume of attacks targeting social networking sites increased 70% quarter-over-quarter, exceeding the total volume of social networking attacks observed in all of 2016.
- Phishing attacks targeting cloud storage providers continued to decline in Q2, signaling a clear shift in targets by phishers.
- The usage of "Secure" phishing sites hosted using SSL certificates is becoming more and more common, growing from just 1% to 13% of overall phishing volume in the last year.
- Padding URLs with hyphens to obscure phishing domains in mobile browsers is an emerging tactic that is growing quickly in popularity.

Thank you for reading this report, and we hope you find it useful. If you would like to discuss it, contact us at **info@phishlabs.com**. For more information on PhishLabs and how we help organizations fight back, visit **www.phishlabs.com**.

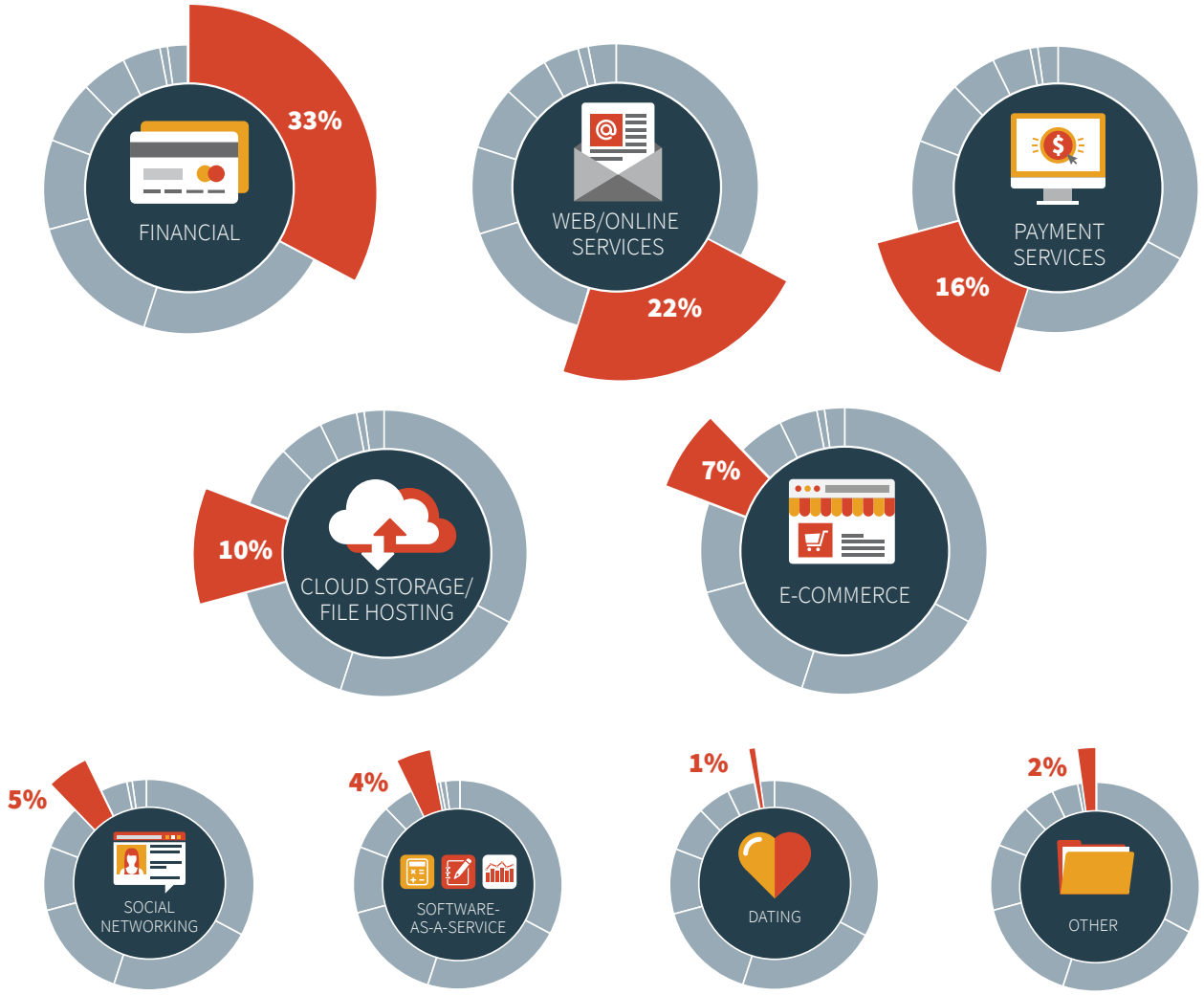
61,000
210,100

In the second quarter of 2017, PhishLabs observed more than 210,100 confirmed malicious phishing sites hosted on more than 61,000 unique domains. These attacks targeted 701 brands from 398 parent institutions, a slight increase from the first quarter of 2017, where phishing attacks targeted 664 brands from 388 institutions. Of those institutions targeted in the second quarter of 2017, 95 had not been targeted at any point in the first quarter.

Attacks Targeting Financial Institutions, Social Networking, Software-as-a-Service Companies Continue to Grow

Globally, total phishing volume increased 41% from the first quarter of 2017; however, the volume of attacks was only four percent higher than the second quarter of 2016. Nearly 88% of all phishing attacks in the second quarter targeted five industries: financial institutions, webmail/online services, payment services, cloud storage/file hosting services, and e-commerce companies.

FIGURE 1: Industries targeted by phishing attacks (Q2 2017).



FINANCIAL SERVICES

For the second quarter in a row, phishing attacks targeting the financial industry grew to the largest quarterly volume observed, nearly doubling in volume between the first and second quarters. Compared to the second quarter of 2016, which had also seen historically high phishing volume, the frequency of phishing attacks targeting financial services in Q2 of 2017 was 46% higher.

The boom in financial phishing attacks this quarter can be primarily attributed to a significant surge in attacks targeting two global financial institutions, which comprised 52% of all volume within the financial industry.

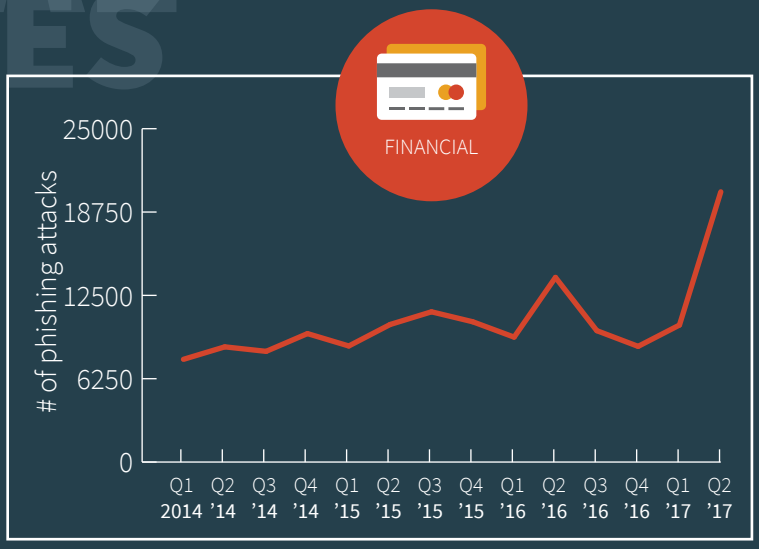


FIGURE 2: Phishing attacks targeting financial services companies by quarter (2014–2017).

The anomalous number of attacks targeting these two financial institutions were the result of multiple shared virtual server attacks, which target vulnerable compromised web servers. By compromising a web server, a phisher has access to all hosts on that server. Using automated tools, phishing content can be added to every domain residing on each host. This allows phishers to increase their attack vector from one domain to potentially hundreds.

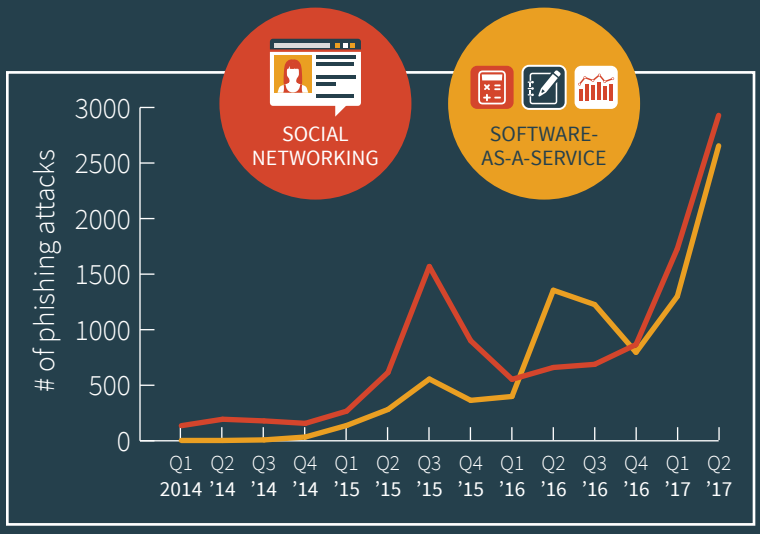
This tactic was observed many times in Q2. Here are several examples:

- A single compromised web server managed by a hosting provider based in the Virgin Islands was used to launch more than 700 attacks targeting one of the financial institutions.
- Nearly 500 attacks targeting the same financial institution were launched from a webserver managed by a Texas-based hosting provider.
- A web server managed by an Illinois-based hosting provider was compromised and used to launch more than 600 attacks against the other financial institution.

This was just the tip of the iceberg. More than 4,600 attacks this quarter were created by just 14 compromised web servers. And there were many more. PhishLabs observed at least 57 compromised web servers targeting the financial services industry Q2.

Following trends observed in Q1 2017, phishing attacks targeting social networking sites and software-as-a-service (SaaS) companies continued to rise. In the second quarter of 2017, the number of phishing attacks targeting users of social media sites exceeded the total number of attacks seen during the entirety of 2016! Compared to the first quarter of 2017, social media

FIGURE 3: Phishing attacks targeting social media sites and SaaS companies by quarter (2014–2017).



phishing attacks grew by nearly 70% and were nearly four-and-a-half times higher than the volume observed during the same quarter last year.

Similar to social networking phishing trends, phishing attacks targeting SaaS companies reached the highest volume ever observed, increasing 104% quarter-over-quarter and nearly doubling the volume observed in the second quarter of 2016. All of the primary companies targeted in this industry saw considerable increases in volume.

Contrary to the previous sectors, attacks against cloud storage services continued to drop in the second quarter, to a level not seen since the end of 2014. There were 17% fewer phishing attacks targeting cloud storage services compared to the first quarter and less than half of the volume observed during the same quarter last year. Based on the consistent downward trend over multiple quarters, it appears cloud storage services may be falling out of favor as a preferred target as phishers shift their attention to other industries.

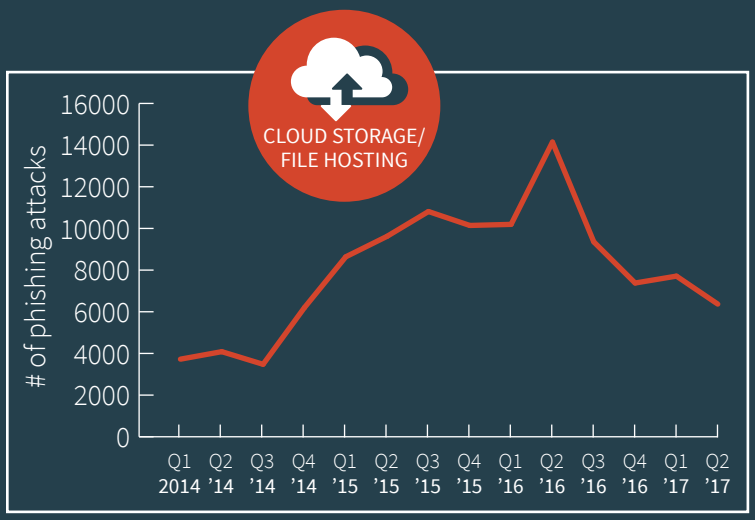
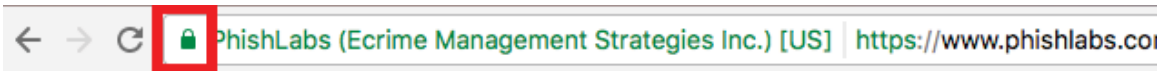


FIGURE 4: Phishing attacks targeting cloud storage services by quarter (2014–2017).

Continued Growth of "Secure" Phish

As mentioned in the Q1 PTI Report, one of the tactics that has seen a significant increase in popularity is the use of SSL certificates to create more authentic-looking phishing sites. Depending on the browser, victims visiting a website with a valid SSL certificate will see a lock icon and/or the word "Secure" in the URL bar, indicating that it is a "trusted" website. By using these certificates, phishers give their fraudulent sites a hint of legitimacy by giving victims a visual cue of security.

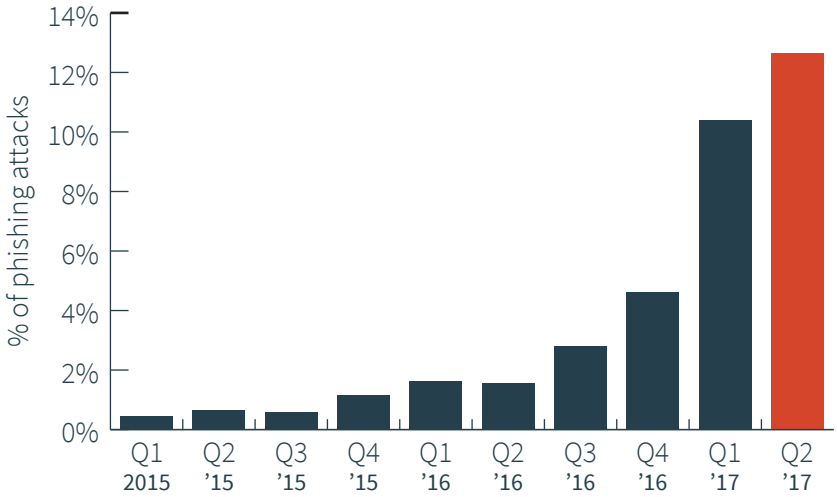
FIGURE 5: Example lock icon on a website with a valid SSL certificate.



The use of "secure" phishing sites to host phishing content continued to grow in the second quarter of 2017, comprising nearly 13% of total phishing volume. During this quarter last year, phishing attacks hosted on domains with valid SSL certificates consisted of only a little over 1% of the quarter's total volume.

More than 55% of all phishing attacks using SSL certificates were associated with attacks targeting two companies: a large payment services provider and a large web/online services company; however, this is down from the 70% share observed during the first quarter. As a percentage of their overall volume, more than 19% of attacks targeting the payment services provider and 38% of attacks targeting the web/online services company used SSL certificates in the second quarter. For all other brands, nearly 8% of phishing attacks used SSL certificates, up from 4% observed in the first three months of the year. This suggests the "secure" phishing sites tactic is being more broadly applied to target more organizations.

FIGURE 6: Percentage of phishing attacks using SSL certificates (2015–2017).



Scarcely Used New gTLDs on the Rise

In the second quarter of 2017, PhishLabs identified phishing sites hosted on 365 different top-level domains (TLDs). A little over half of all phishing sites identified in the second quarter of 2017 were hosted domains registered with the .COM TLD, which is consistent with historical trends. The most common TLDs were .COM, .NET, .ORG, .BR, .IN, .INFO, .UK, .AU, .ZA, and .ID. These ten TLDs comprised nearly 74% of all phishing sites.

The second quarter saw significant increases in volume in some country code TLDs (ccTLDs). The ccTLD that saw the most growth was .VE (Venezuela). The number of phishing sites using the .VE ccTLD increased 467% from the previous quarter and was 198% higher than the average throughout all of 2016. Other ccTLDs that saw significant increases this quarter were .MX (+278%), .ZA (+153%), and .IN (+113%). Overall, ccTLDs were associated with nearly a third of second quarter phishing attacks.

FIGURE 7: Top TLDs associated with phishing sites in Q1 2017.

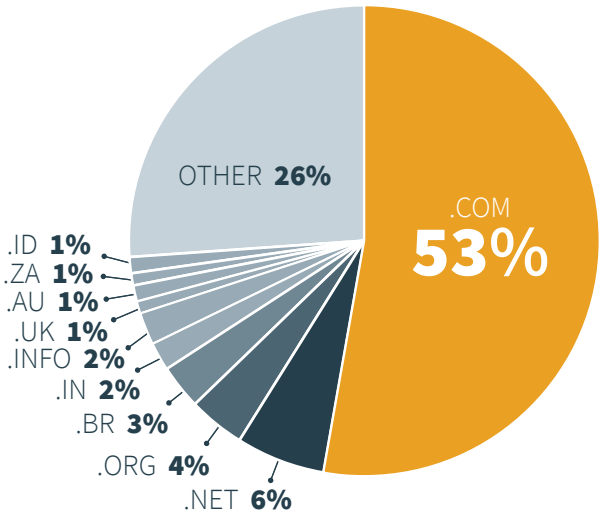


FIGURE 8: Significant changes in phishing TLD volume.

TLD	Change from Previous Qtr	Change from 2016 Avg.
.VE	+467%	+197%
.MX	+278%	+107%
.ZA	+153%	+106%
.IN	+113%	+80%
.RU	-33%	-40%
.DE	-45%	12%

FIGURE 9: Distribution of TLD type associated with phishing sites (Q2 2017).

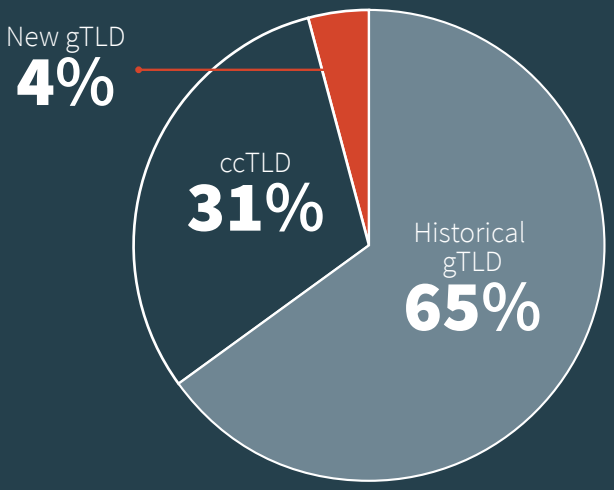
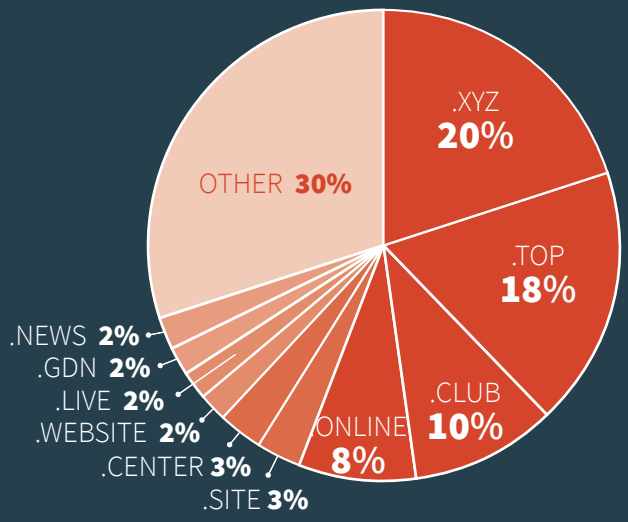


FIGURE 10: Most common new gTLDs associated with phishing attacks (Q2 2017).



A common ccTLD associated with phishing sites, .RU, experienced a 33% decrease in volume in the second quarter of 2017 and is at the lowest level observed since late-2015. Another ccTLD that saw a significant decrease in the second quarter of 2017 was .DE (-45%). Despite the significant decrease in this quarter, phishing sites using .DE are still 12% higher than the 2016 average.

Although a growing number of domains associated with phishing attacks have used recently created generic TLDs (gTLDs), only four percent of attacks were associated with them in the second quarter, which is unchanged from the previous quarter. The most common new gTLDs used by phishers in the second quarter were .XYZ, .TOP, .CLUB, .ONLINE, .SITE, .CENTER, .WEBSITE, .LIVE, .GDN, and .NEWS. Interestingly, a couple of sparingly used new gTLDs, .NEWS and .DATE, saw marked increases between the first and second quarter of 2017. This continues the trend of phishers using new gTLDs in campaigns to add an air of legitimacy and evade detection. Some of the full domains observed in the second quarter of 2017 using these methods to host phishing content include the following:

New Mobile Threats Utilizing URL Padded Phish

In addition to the use of gTLDs to create authentic looking phish, threat actors have identified a new way to create believable URLs, and it's focused exclusively on the mobile market. Instead of trying to create legitimate-looking URLs, threat actors have started including real, legitimate domains within a larger URL, and padding it with hyphens to obscure the real destination. For example: *hxxp://m.facebook.com----------validate----step1.rickytaylk[dot]com/sign_in.html*. Although it starts with m.facebook.com (the genuine path for Facebook's mobile site), the actual domain in this case is rickytaylk.com.

The tactic of padding the URL with hyphens makes it possible to obscure the real domain, and make it appear as though the victim has been directed to a legitimate website. To take things a stage further, in most cases another legitimate-seeming word (e.g., login, secure, account) has been inserted immediately following the string of hyphens, further adding to the illusion of authenticity.

Although we first noticed this phishing tactic in January, the use of this technique has grown in the second quarter. Between April and June of this year, we identified more than 50 phishing attacks utilizing this tactic targeting a range of web/online services companies and social networking sites.

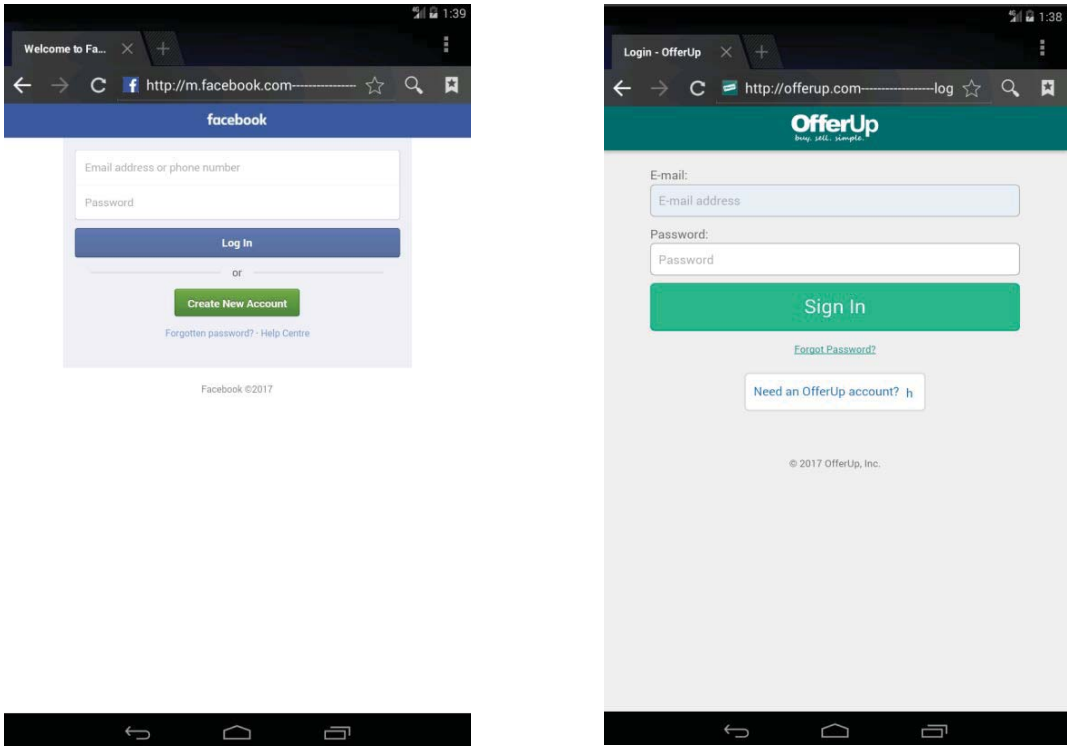


FIGURE 11: Examples of URL padded phishing sites rendered in a mobile browser.

CONCLUSION

The trends and information presented in this report show security leaders, practitioners, and others in the community the current state of the phishing threat landscape. It provides context regarding the environmental conditions that we all operate in and must account for to effectively manage risk.

With a 41% increase in overall phishing volume, Q2 demonstrates a phishing threat landscape that is both thriving and volatile as cybercriminals pivot and exploit different targets.

The volume of attacks targeting the financial industry essentially doubled in Q2, reaching the largest quarterly volume ever observed. Attacks targeting Software-as-a-Service and social networking sites also continue to grow at rates well above average. As the cybercrime focus has shifted towards these industries, attacks targeting cloud storage providers have steadily declined from their peak a year ago.

Phishing threats continue to evolve tactically as cybercriminals adopt new techniques that make their scams more convincing. The percentage of phishing attacks hosted using SSL certificates, which help to create a false sense of legitimacy, continues to rise as the technique is applied to target a broader range of companies. URL padding, a technique used to obscure phishing domains when viewed in mobile browsers, is also on the rise. Additionally, cybercriminals are increasingly registering domains using new country code top-level domains, such as .VE (Venezuela), which increased 467% quarter over quarter. As new ccTLDs have been adopted, the once-popular .RU (Russia) ccTLD has declined. This is likely due to the raised suspicion associated with that ccTLD.

PHISHING
CYBERCRIME
ATTACKS

Thank you for reading the Q2 2017 Phishing Trends and Intelligence Report. We hope you found the information to be useful. If you would like to discuss it, contact us at **info@phishlabs.com**.

For more information on PhishLabs and how we help organizations fight back against phishing, visit **www.phishlabs.com**.

For more research and commentary, sign up for our blog at **blog.phishlabs.com.**

You can also follow us social media:

@PhishLabs

www.linkedin.com/company/phishlabs

www.facebook.com/PhishLabs/

PHISHLABS