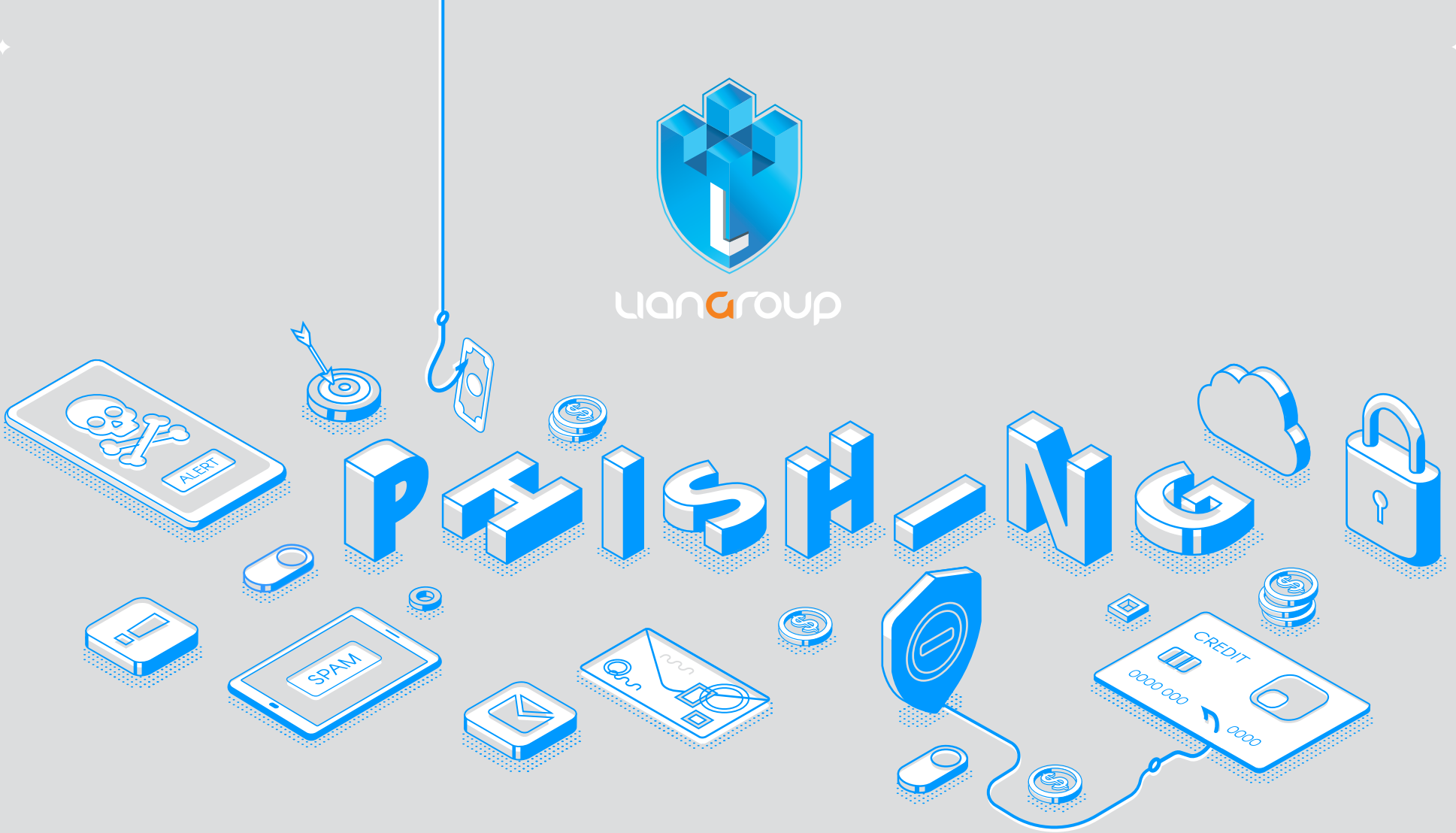
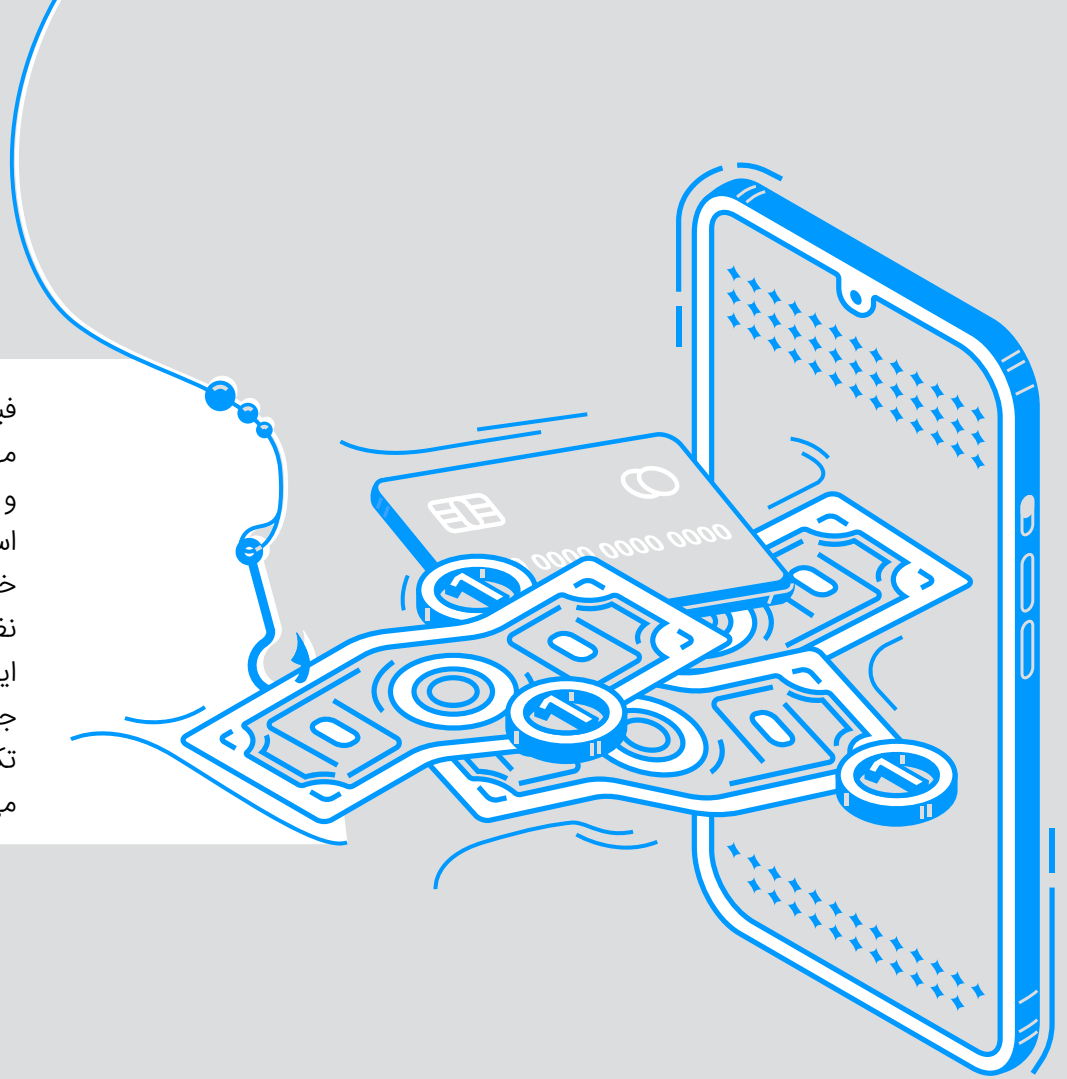

LianGroup
PHISH-ME
ALERT
SPAM
CREDIT
0000 000
0000

فیشینگ به دسته‌ای از جرایم گفته می‌شود که در آن مجرم، هم از مهندسی اجتماعی و هم از تکنیک‌های فنی، برای سرقت اطلاعات هویتی و مالی افراد استفاده می‌کند. مهندسی اجتماعی، از عدم آگاهی افراد استفاده می‌کند تا آن‌ها را فریب داده و وادارشان کند که اطلاعات حساس خود را لو دهند. این فرایند معمولا شامل ایمیل و پیام‌هایی است که به نظر می‌رسد از طرف افراد آشنا و قابل اعتماد ارسال شده‌اند. طراحی این پیام‌ها به گونه‌ای است که در نهایت کاربر را به سمت سایت‌های جعلی هدایت کرده تا بتواند اطلاعات محرمانه آن‌ها را به سرقت ببرد. تکنیک‌های فنی، شامل بدافزارهایی است که به کامپیوتر کاربر تزریق می‌شوند تا مهاجم بتواند اطلاعات مهم را به‌طور مستقیم سرقت کند.

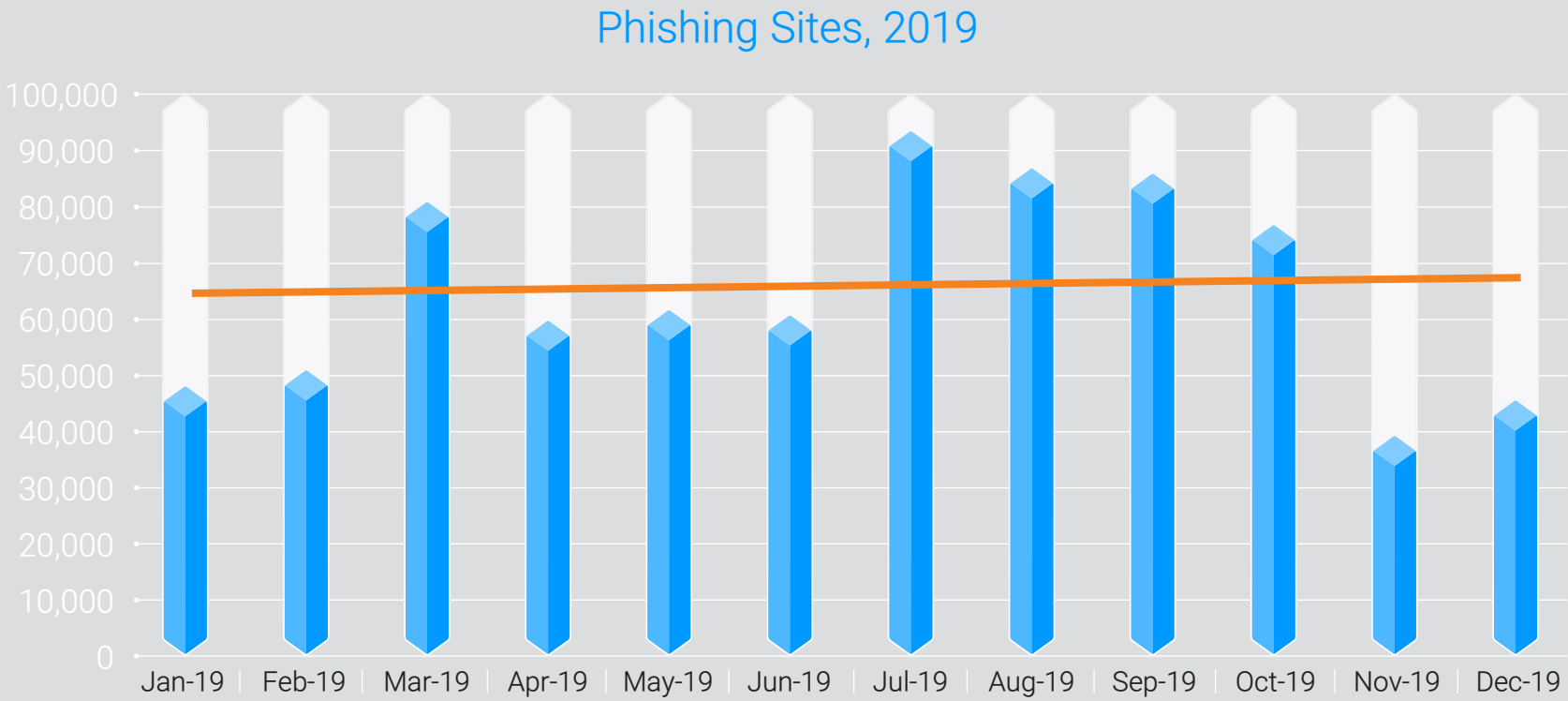


خلاصه ترندهای فعالیت فیشینگ در سه ماهه آخر ۲۰۱۹

- تعداد حملات فیشینگ در سراسر جهان کاهش یافته و به مقدار میانگین نزدیک شده است.
- در سال ۲۰۱۹، تعداد حوادث فیشینگ در برزیل ۲۳۲٪ افزایش یافته است.
- حملات فیشینگی که کاربران webmail و SaaS را مورد هدف قرار می‌دهند، همچنان بیشترین میزان فیشینگ را به خود اختصاص داده‌اند.
- مجرمان حملات BEC، در طول تعطیلات، از کارت هدیه استفاده کردند.
- تقریباً سه چهارم سایت‌های فیشینگ از SSL استفاده می‌کنند. این عدد که بالاترین میزان را نسبت به اوایل سال ۲۰۱۵ نشان می‌دهد، بیانگر این است که کاربران نباید برای اعتماد به یک سایت، تنها به وجود SSL اکتفا کنند.
- از دامنه‌های gTLD بیشتر از دامنه‌های ccTLDs استفاده می‌شود.

	October	November	December
تعداد وبسایت‌های فیشینگ کشف شده	۷۶,۸۰۴	۳۹,۵۸۰	۴۵,۷۷۱
تعداد ایمیل‌های فیشینگ گزارش شده	۴۵,۰۵۷	۴۲,۴۲۴	۴۵,۰۷۲
تعداد برندهایی که مورد هدف کمپین‌های فیشینگ قرار گرفته‌اند.	۳۳۳	۳۲۵	۳۴۱

در یک چهارم پایانی سال، ۱۶۲/۱۵۵ سایت فیشینگ شناسایی شده که این رقم نسبت به سه ماهه دوم و سوم کمتر، اما از سه ماهه چهارم سال ۲۰۱۸ بیشتر است.



طبق گفته یکی از محققان ارشد APWG، فیشینگ در سال ۲۰۱۹، نمودار پر فراز و نشیبی را تجربه کرده است. به این صورت که ماه ژوئیه و اکتبر، بدترین دوره فیشینگ، طی ۳ سال بود اما بعد از آن سطح فیشینگ به سطح نرمال آن بازگشت.

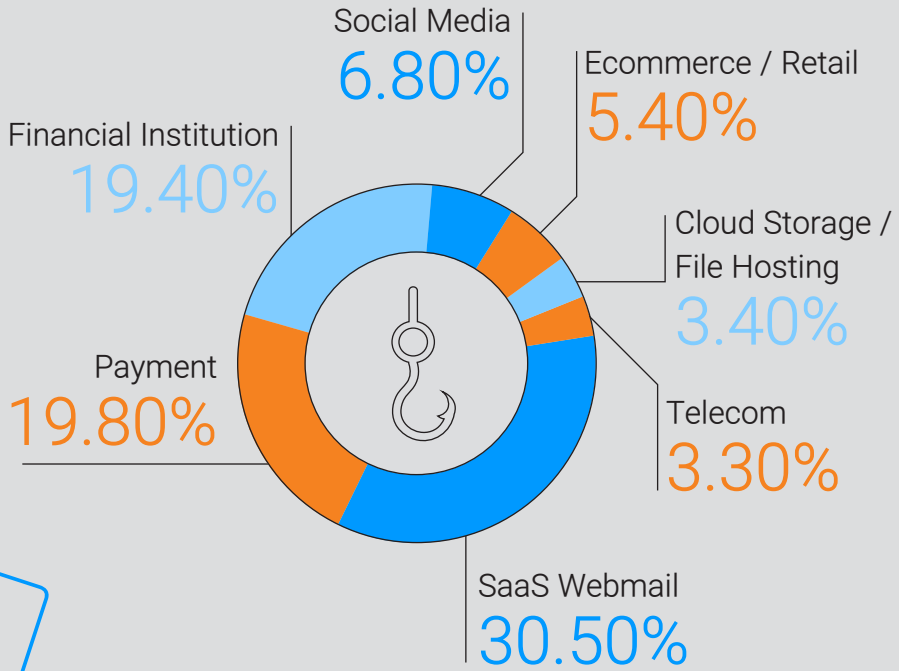
تعداد دامنه‌های یکتای مورد استفاده برای فیشینگ، نرخ پایین‌تری را تجربه کرده است. تعداد این دامنه‌ها در اکتبر ۱۳/۵۹۷، در نوامبر ۱۵/۲۶۱ و در دسامبر به ۱۲/۲۶۰ رسید.

تعداد گزارش‌های دریافت شده از ایمیل‌ها و کمپین‌های فیشینگ، ۱۳۲/۵۵۳ بود که باز هم این عدد از سه ماهه دوم و سوم بیشتر است.

در سه ماهه چهارم سال ۲۰۱۹، OpSec Security متوجه شد که سایت‌های webmail و SaaS همچنان محبوب‌ترین اهداف فیشینگ هستند. فیشرها از این سایت‌ها برای حملات BEC (Business e-mail compromising) و نفوذ به حساب‌های شرکتی SaaS استفاده می‌کنند. فیشینگ در شبکه‌های اجتماعی، در هر سه ماهه سال، رشد کرده و در طول ۲۰۱۹ دو برابر شده است.

حملات علیه حافظه ابری و سایت‌های هاستینگ فایل، همچنان محبوبیت کمتری داشتند. میزان حملات علیه ارز رمزنگاری شده، لجستیک/ حمل و نقل، بازی، بیمه، انرژی، دولت و بخش مراقبت‌های درمانی، در طول یک چهارم پایانی سال ناچیز بود؛ هر کدام از این موارد، کمتر از ۱ درصد از کل حملات فیشینگ را به خود اختصاص می‌دادند.

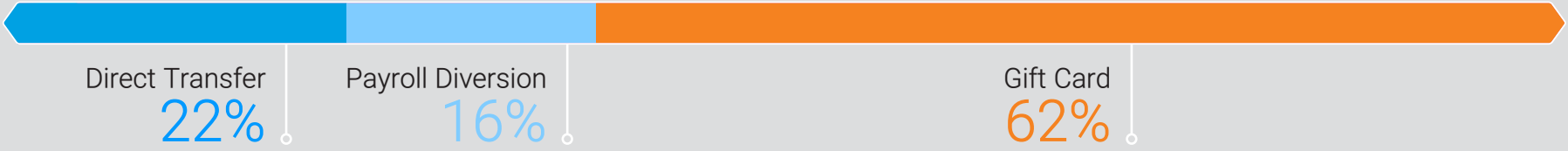
MOST-TARGETED SECTORS, 4Q2019



سوءاستفاده از ایمیل‌های شرکتی

شرکت Agari تکنیک سرقت هویت موسوم به BEC را مورد بررسی قرار داده است. در حمله BEC، کلاهبردار، کارمندان واحد مالی شرکت را مورد هدف قرار می‌دهند. معمولاً این کار را با ارسال ایمیل از طریق حساب‌های جعلی یا هک شده (حمله فیشینگ spear) انجام می‌دهند. شخص کلاهبردار، هویت یک کارمند یا شخص مورد اعتماد دیگری را جعل می‌کند و تلاش می‌کند او را وادار به واریز پول کند. مهاجم ممکن است هفته‌ها زمان صرف شناسایی شبکه و حساب‌های شرکت یا حتی نحوه برخورد مدیرعامل کند. حملات BEC میلیاردها دلار خسارت به شرکت‌های بزرگ و کوچک وارد کرده است. Agari هزاران مورد حمله BEC را در یک چهارم پایانی سال مورد بررسی قرار داده تا مجموعه داده‌های خود را تکمیل کند. طبق گزارش Agari، مهاجمان در ۶۲٪ از حملات BEC، کارت‌های هدیه درخواست کرده‌اند که این عدد از سه ماهه سوم بیشتر و از سه ماهه دوم کمتر است. حدود ۱۶ درصد از حملات، درخواست اعمال تغییرات در حقوق و دستمزد را داشتند که این میزان از سه ماهه قبل کمتر است. حدود ۲۲٪ از حملات BEC نیز شامل درخواست انتقال مستقیم بانکی بود.

BEC CASH-OUT METHOD, 4Q 2019

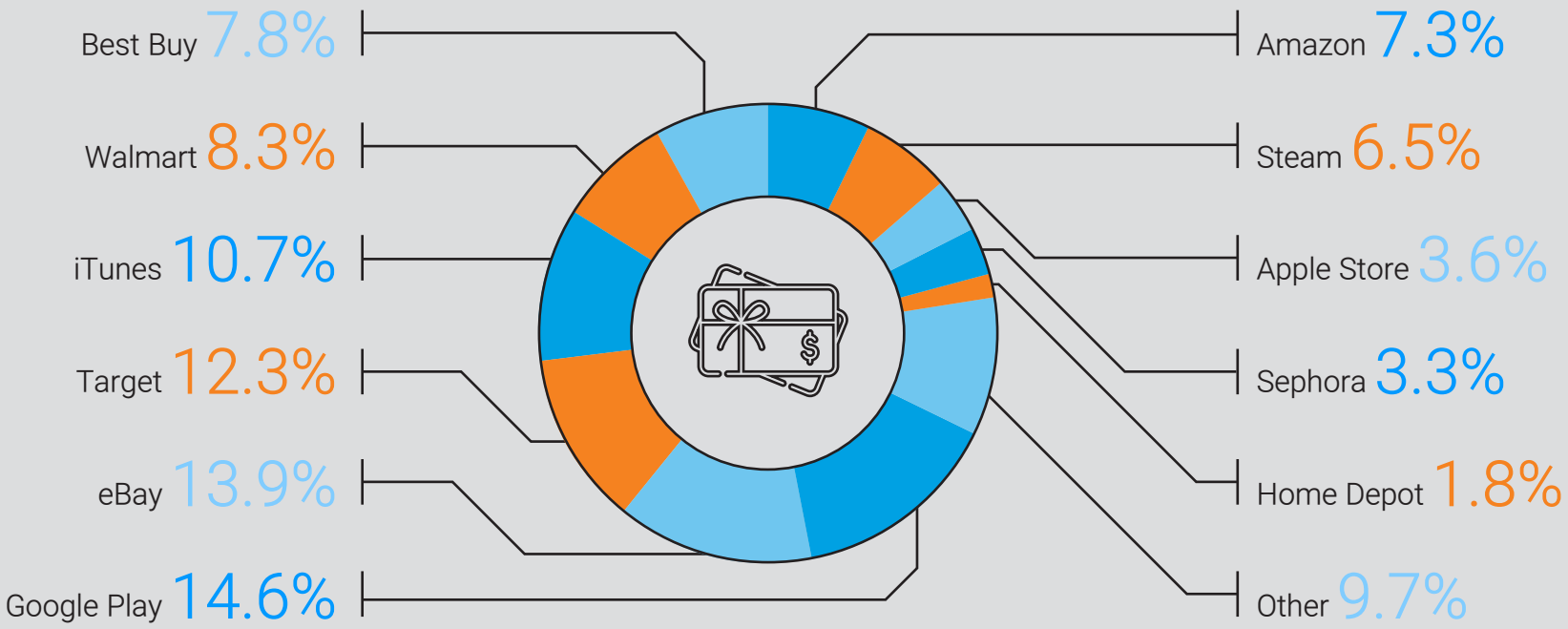


میزان درآمد یک مهاجم از کارت‌های هدیه، به میزان قابل توجهی کمتر از انتقال الکترونیکی است. در طول سه ماهه چهارم، میانگین کارت‌های هدیه‌ای که یک مهاجم BEC درخواست کرده بود، بیش از ۱/۶۰۰ دلار است. اما میانگین مبلغ درخواستی در انتقال الکترونیکی حملات BEC، بیش از ۵۵/۰۰۰ دلار بود:

	میانگین	متوسط	کمترین	بیشترین
انتقال وجه الکترونیکی	$55,395	$28,350	$2,550	$680,456
کارت هدیه	$1,627	$1,200	$150	$10,000

یکی از موارد قابل توجهی که در طول یک چهارم انتهایی سال شاهد آن بودیم، تغییر در انواع گیفت کارت‌های درخواستی بود. Google Play همچنان بیشترین میزان تقاضا را در میان کارت‌های هدیه داشت اما این میزان از ۲۷ درصد به ۱۵ درصد کاهش یافت. در این بازه، شاهد افزایش تقاضا به سمت کارت‌های هدیه Best Buy، Target، eBay و Sephora بودیم. این افزایش تقاضا، می‌تواند به این دلیل باشد که تمام این شرکت‌ها کالاهای فیزیکی می‌فروشند و حملات در طول تعطیلات اتفاق افتاده است. این موضوع می‌تواند نشانگر این باشد که کلاهبرداران به جای پولشویی از طریق ارز دیجیتال، به دنبال پولشویی از طریق خرید کالاهایی هستند که بعدا می‌توانند بفروشند.

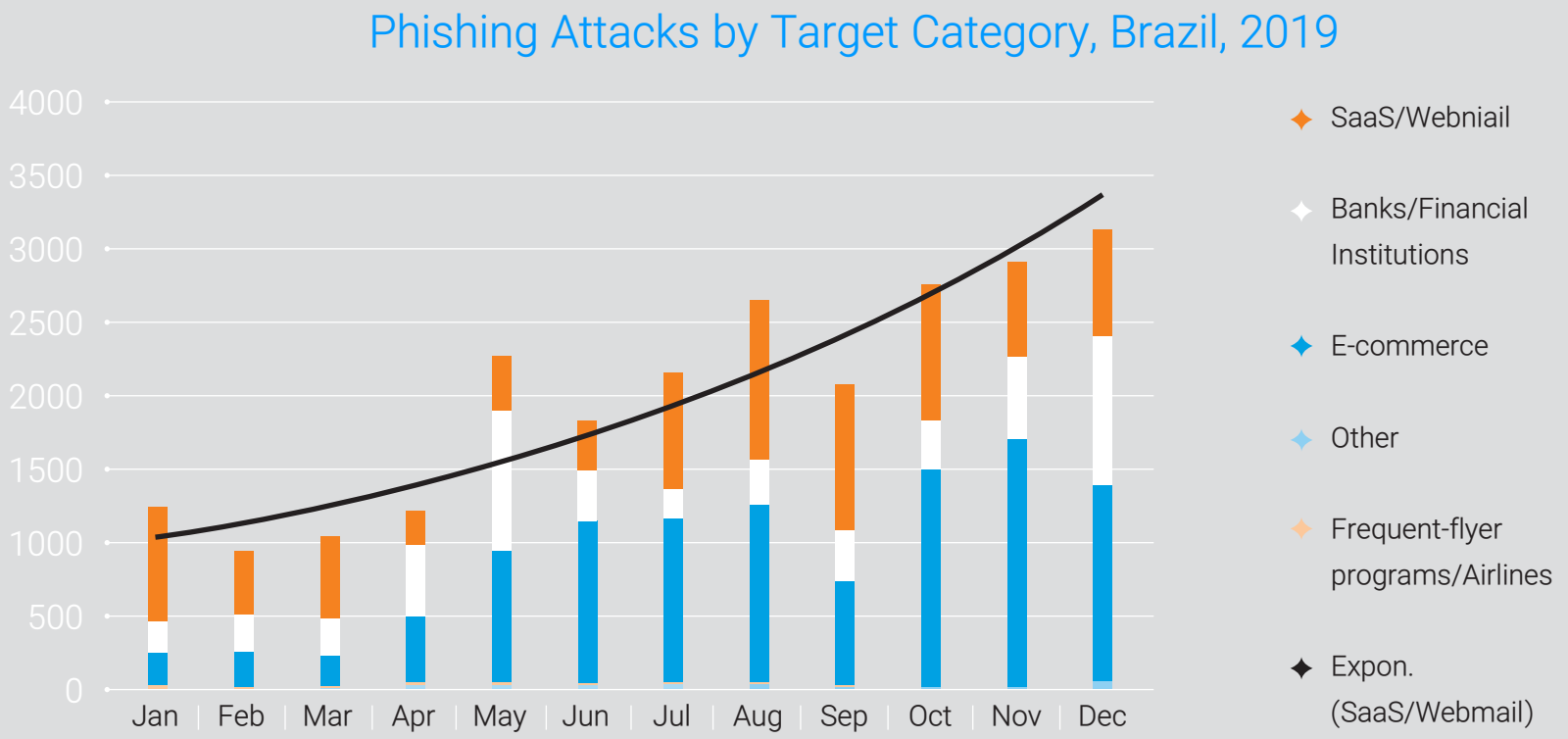
GIFT CARDS REQUESTED IN BEC ATTACKS, 3Q 2019



به طور کلی، مهاجمان BEC در ۲۰ درصد موارد از حساب‌های Gmail استفاده می‌کنند. با توجه به نوع حساب پست الکترونیکی، مهاجمان در ۵۷ درصد موارد، از حساب‌های webmail (Gmail ۳۵ درصد از آن را شامل می‌شود)، در ۳۹ درصد مواقع از حساب‌های استاندارد ایمیل سایر دامنه‌ها و در ٤ درصد مواقع از ایمیل‌های هک شده، استفاده می‌کنند.

فعالیت‌های مجرمانه در برزیل

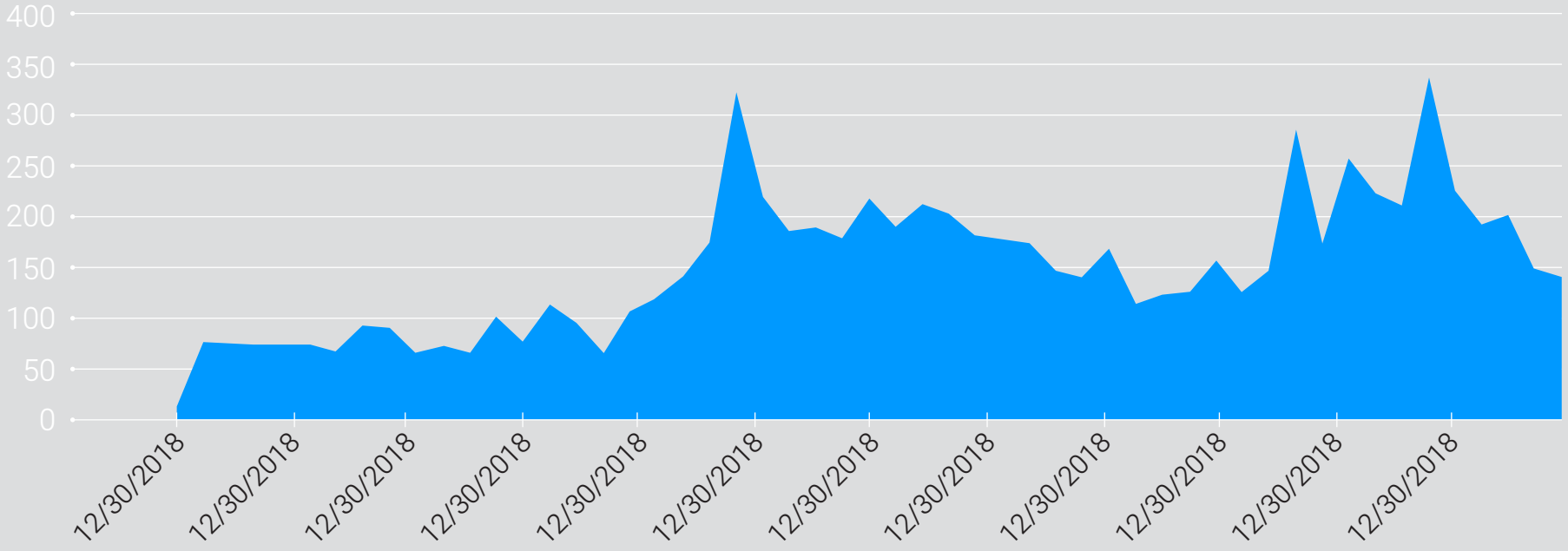
در سه ماهه پایانی سال ۲۰۱۹، شرکت Axur ۸۷۲,۸ مورد حمله فیشینگ شناسایی کرد. این عدد، بسیار بیشتر از اعدادی است که Axur طی ۹ ماه قبل پیدا کرده بود. این حملات، به طور ویژه برندهای برزیلی یا خدمات خارجی را که به زبان پرتقالی در برزیل فعالیت می‌کردند، تحت تأثیر قرار می‌داد.



232%

از فوریه تا دسامبر ۲۰۱۹، تعداد کل حوادث ماهیانه فیشینگ در برزیل، ۲۳۲٪ افزایش یافت:

PHISHING AGAINST E-COMMERCE SITES, BRAZIL, 2019



پیک حملات با ۱,۶۸۵ مورد، در نوامبر اتفاق افتاد. این رقم بالاترین میزان حمله در سال را نشان می‌دهد و بیشتر آن مربوط به کلاهبرداری در خریدهای مربوط به جمعه سیاه است. همیشه میزان حملات در برزیل، نزدیک تعطیلات پایان سال افزایش می‌یابد و بخش مالی را برای سرقت داده‌ها مورد هدف قرار می‌دهد.

Domain Name

استفاده از Domain Name برای فیشینگ

شرکت RiskIQ به طور مداوم روی محل وقوع فیشینگ در DNS تحقیق می‌کند. RiskIQ ۲,۱۴۹ مورد URL فیشینگ را تأیید کرده که توسط ۱,۳۲۸ دامنه درجه دو میزبانی می‌شدند.

سه نوع دامنه سطح بالا (TLDs) وجود دارد

- TLDهای عمومی «Legacy»، قبل از سال ۲۰۱۱ وجود داشتند. این TLDها شامل .org ، .com و TLDهایی نظیر .ASIA و .BIZ می‌شوند. این‌ها ۴۹٪ از نام‌های دامنه در جهان و ۶۵٪ از دامنه‌های فیشینگ در مجموعه نمونه را از ابتدای سه ماهه‌ی چهارم شامل می‌شدند. در مجموعه نمونه، ۸۶۵ legacy gTLD وجود داشت که اکثر آن‌ها .com بودند.

- دامنه‌های عمومی جدید سطح بالا (nTLD) مانند .work و .ICU بعد از سال ۲۰۱۱ انتشار پیدا کردند. در ابتدای سه ماهه چهارم، nTLDها ۷٪ از دامنه‌های جهان را تشکیل می‌دادند و ۷٪ از کل دامنه‌های مجموعه نمونه را شامل می‌شدند. ۸۸ دامنه nTLD در مجموعه نمونه وجود داشت.

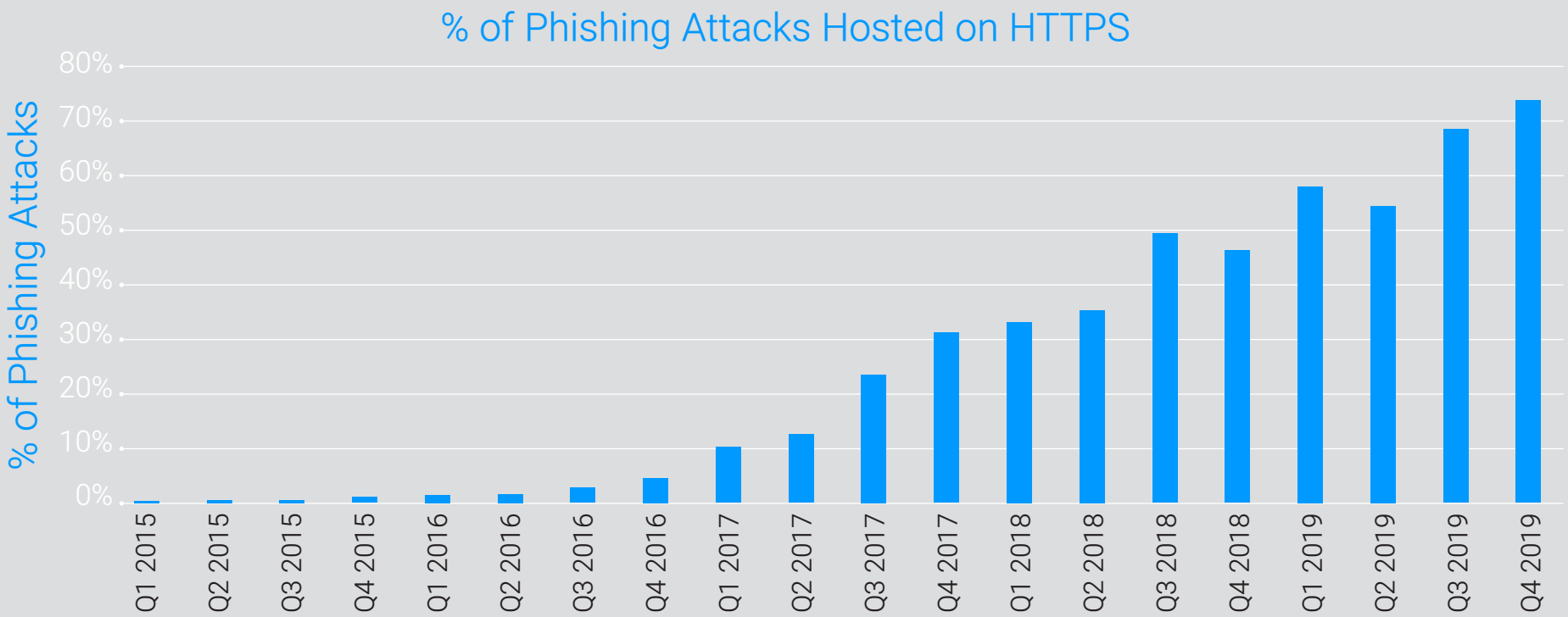
- دامنه‌های کد کشور (ccTLDs)، مانند .uk و .MX ۴۵٪ از دامنه‌های جهان را از ابتدای سه ماهه چهارم شامل می‌شدند. اما این دامنه‌ها، تنها ۲۸٪ از دامنه‌ها را در مجموعه نمونه تشکیل می‌دادند. ۳۷۵ دامنه در مجموعه نمونه وجود داشت.

نمودار زیر TLDهایی را نشان می‌دهد که دارای دامنه‌های سطح دو بی‌نظیری هستند که برای فیشینگ مورد استفاده قرار گرفته‌اند.

Rank	TLD	Category	# of Unique Domains in Sample Set (4Q 2019)
1	.COM	generic	727
2	.ORG	generic	50
3	.BR	ccTLD	46
4	NET	generic	43
5	.INFO	generic	33
6	.UK	ccTLD	29
7	.RU	ccTLD	24
8	IN	ccTLD	23
9	.XYZ	nTLD	18
10	.ML	ccTLD	15
11	.AU	ccTLD	14
12	.TOP	nTLD	13
12	.KR	ccTLD	13
13	.ZA	ccTLD	12
14	.CF	ccTLD	10
14	.TK	ccTLD	10
14	.VN	ccTLD	10
15	.MX	ccTLD	9

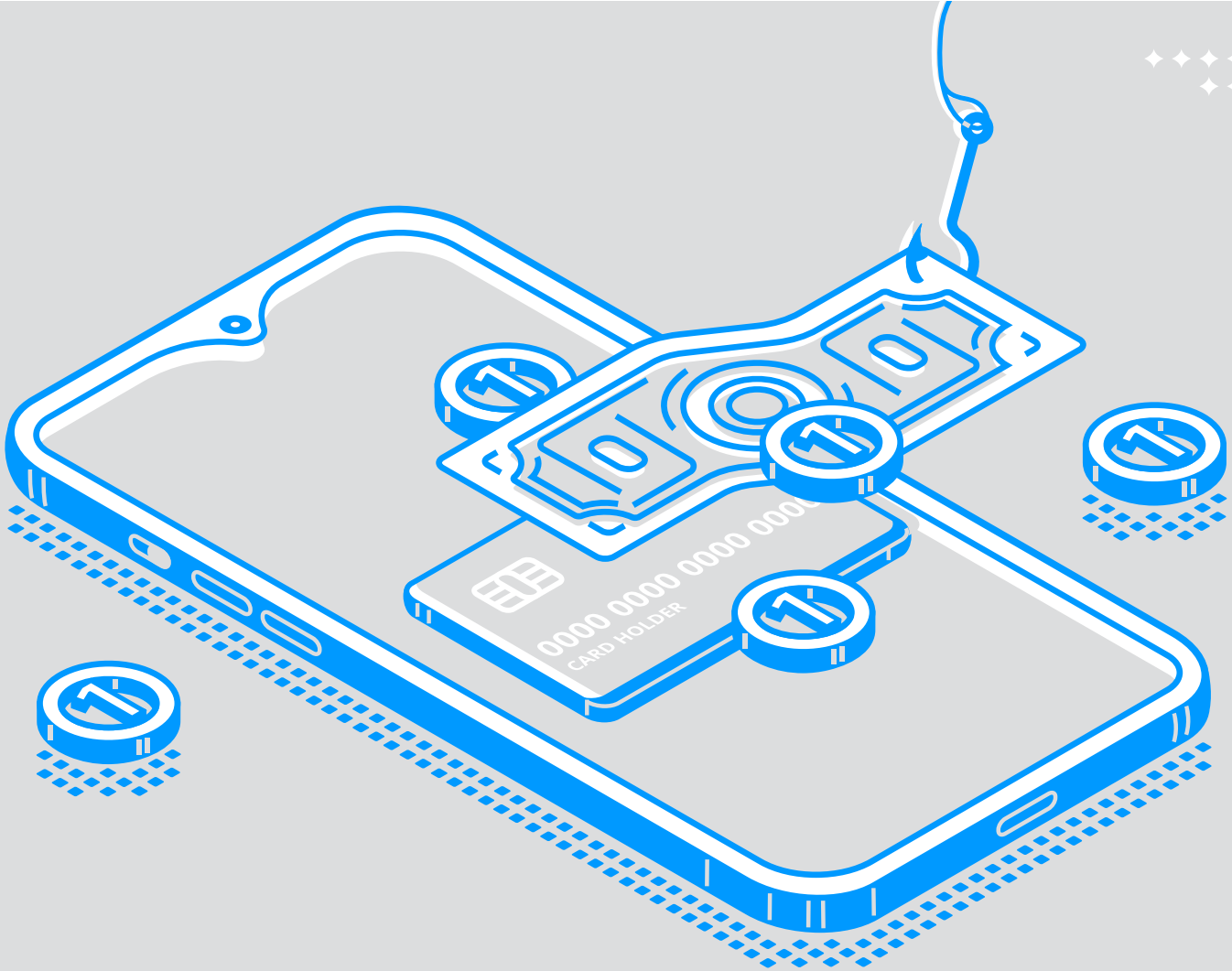
بیش از ۸۰ میلیون دامنه یکتا یا آدرس IP در مجموعه نمونه برای فیشینگ استفاده شدند که شرکت‌ها و برندهای آن‌ها را مورد هدف قرار داده بودند. بخش عمده آن‌ها روی هاست‌های رایگان قرار نداشتند اما روی دامنه‌ها یا سایت‌های هک شده‌ای بودند که منحصراً برای فیشینگ استفاده می‌شدند؛ البته باز هم این موارد درصد بسیار پایینی از مجموعه نمونه را شامل می‌شد.

HTTPS با استفاده از رمزنگاری، مبادله اطلاعات بین مرورگر شخص و وبسایت مورد بازدید او را ایمن می‌کند. وجود HTTPS به ویژه در سایت‌هایی که فروش آنلاین دارند یا حساب‌های کاربری که توسط رمزعبور محافظت شده‌اند، لازم است.



در سه ماهه سوم ۲۰۱۹، ٦٨٪ از سایت‌های فیشینگ، از SSL استفاده کرده بودند اما در پایان سال این عدد به ٧٤٪ رسید. مهاجمان در سایت‌های فیشینگی که می‌سازند، از گواهینامه رایگان استفاده و از رمزنگاری موجود در وبسایت‌های هک شده، سوءاستفاده می‌کنند.

منبع: APWG



تهران، خیابان هویزه، پلاک ۱۲۱، واحد ۲
۰۲۱ ۹۱۰۰٤۱۵۱
www.liangroup.net