مرکز تخصصی آپا دانشگاه بیرجند

ویژه نامه امنیتی

مرکز تخصصی آپا دانشگاه بیرجند

تهدیدات سایبری در حوزه مالی

پیش بینی تهدیدات سایبری برای خدمات حوزه ی مالی
پیش بینی تهدیدات سایبری برای پول های رمزنگاری شده

Threat Predictions for Financial Services
Threat Predictions for Cryptocurrencies

2018

مروری بر تهدیدات سایبری در حوزه مالی

روش‌های آلودگی برای تروجان‌های مالی همانند تروجان‌های شایع دیگر می‌باشد. توزیع آن‌ها، بیشتر توسط ایمیل‌های اسپم با پیوست‌های مخرب و ابزارهای کدهای مخرب[1] وب صورت می‌گیرد. پیوست اسناد office با ماکروهای مخرب هنوز به صورت گسترده استفاده می‌شود. با این حال از اسکریپت‌های ویژوال بیسیک (VBS) و جاوااسکریپت (JS) به صورت پیوست‌های مختلف، از طریق هرزنامه‌های انبوه برای توزیع بدافزار استفاده می‌شود. باتنت Necure که فقط در یک روز در نوامبر ۲۰۱۶، بیش از ۱/۸ میلیون بارگیر JS ارسال کرد، اندازه برخی از این حملات را مشخص می‌کند.

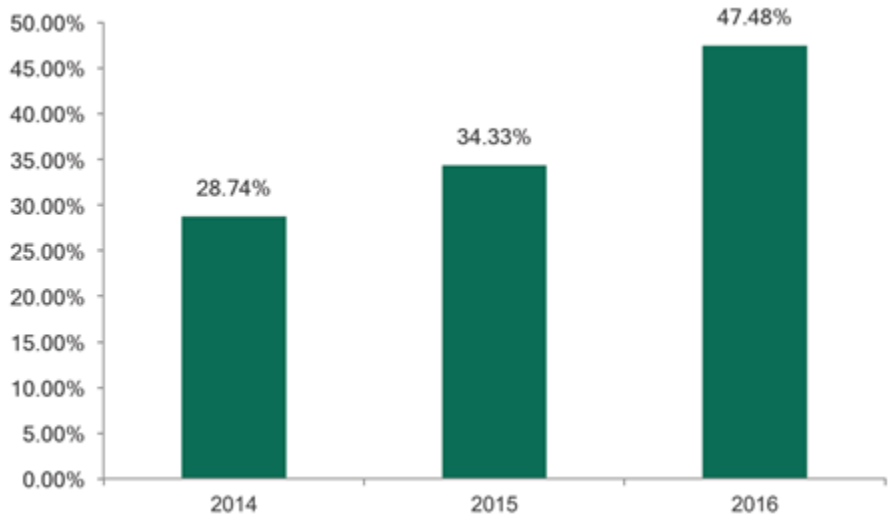
بعضی از گروه‌ها به سرعت از اکسپلویت‌های جدید استفاده می‌کنند، برای مثال در ۱۰ آوریل ۲۰۱۷، Dridex از یک آسیب‌پذیری صفر روزه[2] در Microsoft Word برای آلوده کردن هزاران کاربر استفاده کرد. حجم بالایی از ایمیل‌های آلوده ارسال شد و باز کردن سند، کامپیوتر را به یکی از گونه‌های Dridex آلوده می‌کرد.

سایر گروه‌ها روی مهندسی اجتماعی تمرکز می‌کنند. ایمیل‌های فیشینگ کاملاً شخصی دیده شده است که از نام و سایر اطلاعات به‌دست آمده از رخنه‌های داده‌ای استفاده می‌کنند. بعضی از ایمیل‌های کلاهبرداری حتی توسط ارائه‌دهنده خدمات ایمیل (ESP) شناخته‌شده و معتبر ارسال شده‌اند که خدمات بازاریابی ایمیلی و ایمیل تراکنشی ارائه می‌داده‌اند. در مورد Dridex، ایمیل موردنظر بسیار قابل باور طراحی شده بود و کاربر را به یک بارگیر JS خرابکار هدایت می‌کرد.

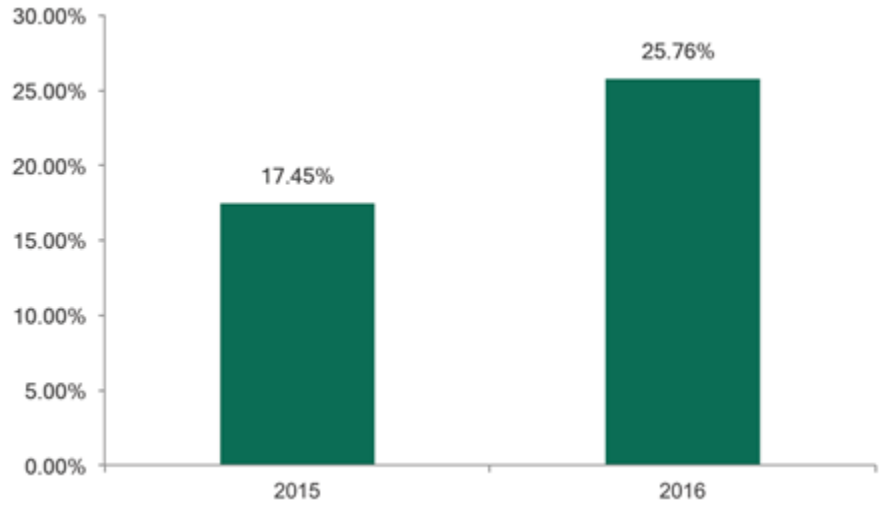
ایمیل‌های فیشینگ که در آن‌ها قربانی به سمت وب‌سایت‌های جعلی هدایت شده و فریب می‌خورد تا اطلاعات حساب خودش را وارد کند به ۱ ایمیل فیشینگ در ۹۱۳۸ ایمیل در مارس ۲۰۱۷ کاهش یافت. در سال ۲۰۱۶، متوسط تعداد ایمیل‌های فیشینگ کمی بیشتر از ۱ در ۳۰۰۰ ایمیل بود.

در سال ۲۰۱۶، فناوری‌های ضد فیشینگ کسپرسکی ۱۵۴,۹۵۷,۸۹۷ تلاش را جهت بازدید انواع مختلفی از صفحات فیشینگ شناسایی کرد که ۴۷/۴۸ درصد از این تشخیص‌ها، تلاش برای بازدید از صفحات فیشینگ مالی بودند. این میزان، ۱۳/۱۴ واحد درصد بیشتر از سهم شناسایی فیشینگ‌های ثبت شده در سال ۲۰۱۵ است که ۳۴/۳۳ درصد از آن‌ها مربوط به تقلب‌های مالی بودند.

[1] exploit toolkits
[2] zero-day

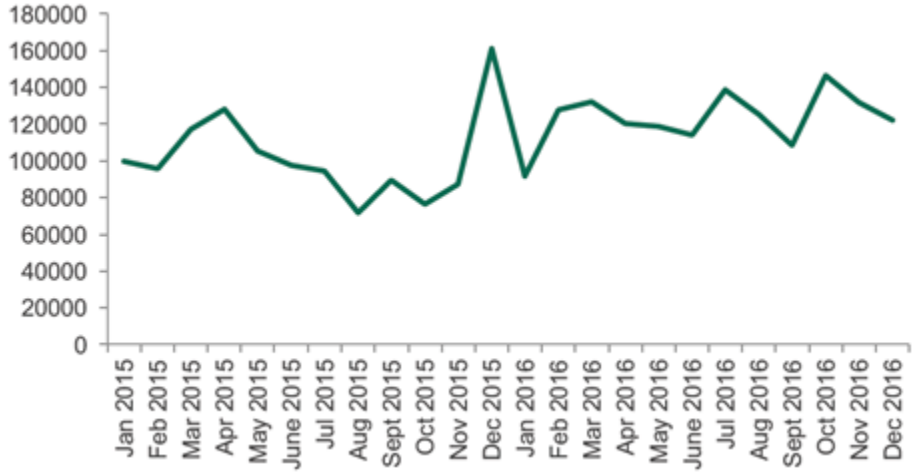


شکل ۱- میزان فیشینگ مالی شناسایی شده توسط آزمایشگاه کسپرسکی در طی سال‌های ۲۰۱۴ تا ۲۰۱۶



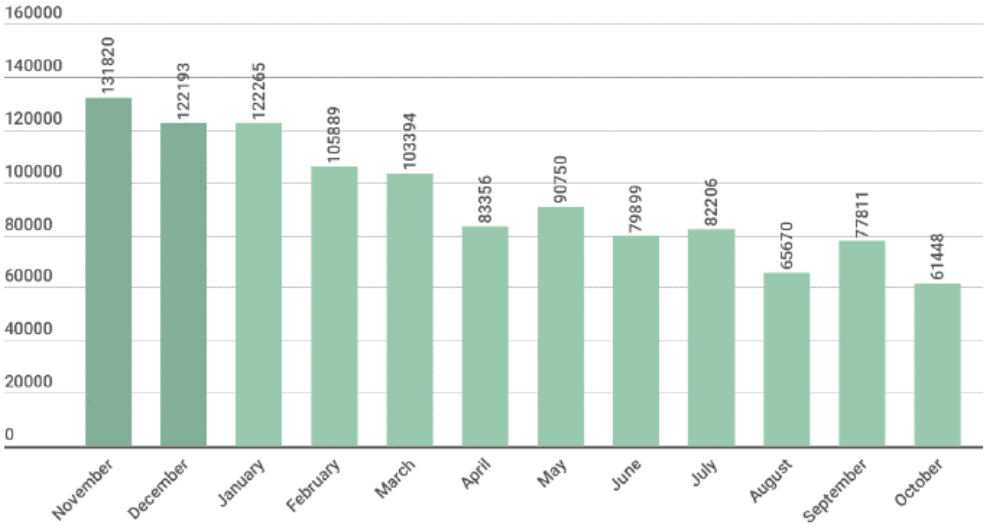
شکل ۲- میزان فیشینگ بانکی شناسایی شده توسط آزمایشگاه کسپرسکی در طی سال‌های ۲۰۱۵ تا ۲۰۱۶

در سال ۲۰۱۵ حداقل ۸۳۴,۰۹۹ کاربر در سراسر جهان دست کم یک بار با حمله تروجان بانکی مواجه شده‌اند. در سال ۲۰۱۶، تعداد این کاربران در سراسر جهان به ۱,۰۸۸,۹۳۳ نفر رسید که ۳۰/۵۵ درصد افزایش داشت.



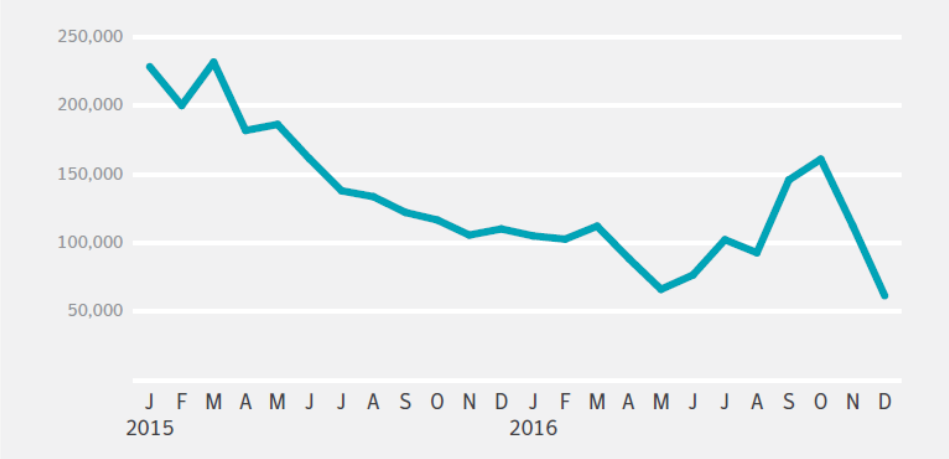
شکل ۳- تغییر تعداد کاربران مورد حمله با بدافزارهای بانکی در طی سال‌های ۲۰۱۵ تا ۲۰۱۶

در سال ۲۰۱۷، راهکارهای امنیتی آزمایشگاه کسپرسکی یک یا چند برنامه مخرب بر روی ۱۱۲۶۷۰۱ کامپیوتر را که تلاش می‌کردند از طریق بانکداری آنلاین به سرقت پول افراد بپردازند، مسدود کردند.



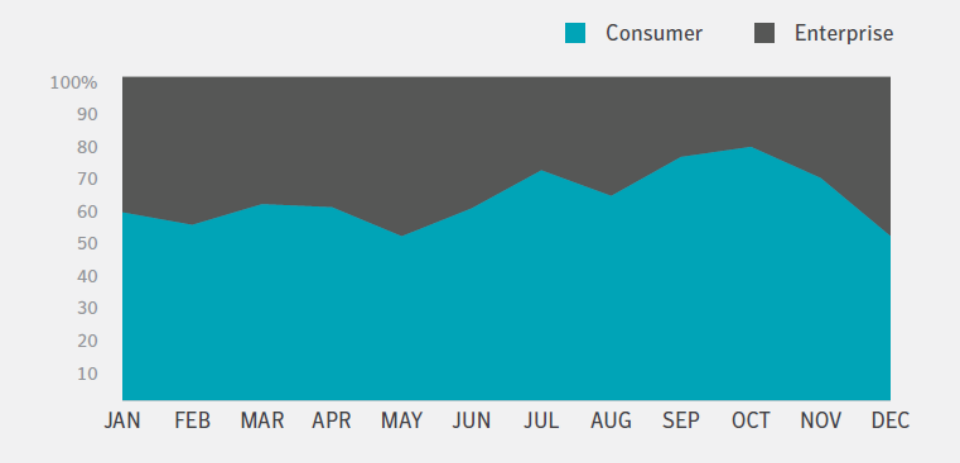
شکل ۴- تعداد کاربران مورد حمله با بدافزارهای مالی از ماه نوامبر ۲۰۱۶ تا اکتبر ۲۰۱۷

آمار سالانه کسپرسکی برای سال ۲۰۱۷ مبتنی بر داده‌های دریافتی بین ماه‌های نوامبر ۲۰۱۶ تا اکتبر ۲۰۱۷ است. این آمار فقط شامل برنامه‌های مخرب برای دستگاه‌های خودپرداز و پایانه‌های فروش می‌شود اما تهدیدات موبایل را در بر نمی‌گیرد.



شکل ۵- تشخیص تروجان بانکی بر روی کامپیوتر در سال‌های ۲۰۱۵ و ۲۰۱۶

در سال ۲۰۱۶ نسبت به سال ۲۰۱۵، شاهد ۳۶ درصد تشخیص کمتر در نقاط پایانی[3] بودیم. در سال ۲۰۱۵ هم شاهد ۷۳ درصد کاهش نسبت به سال قبل از آن بودیم.

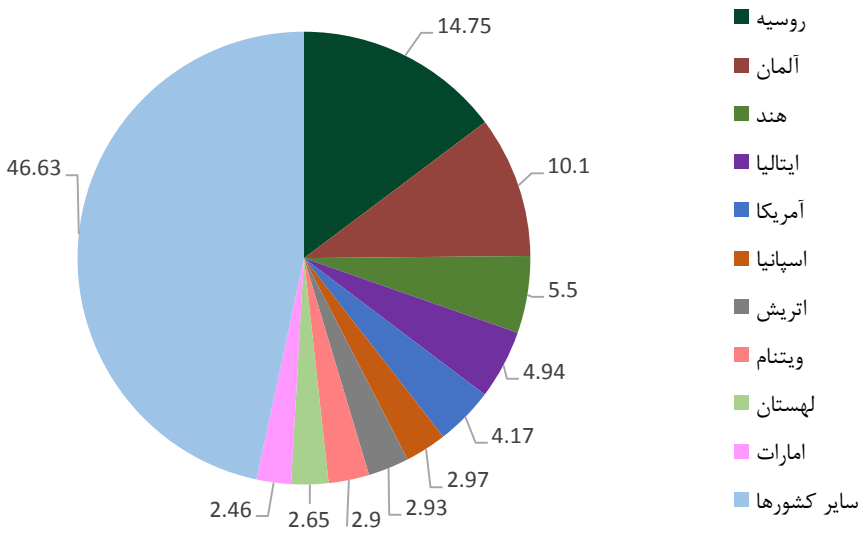


شکل ۶- توزیع تشخیص‌های بدافزار مالی

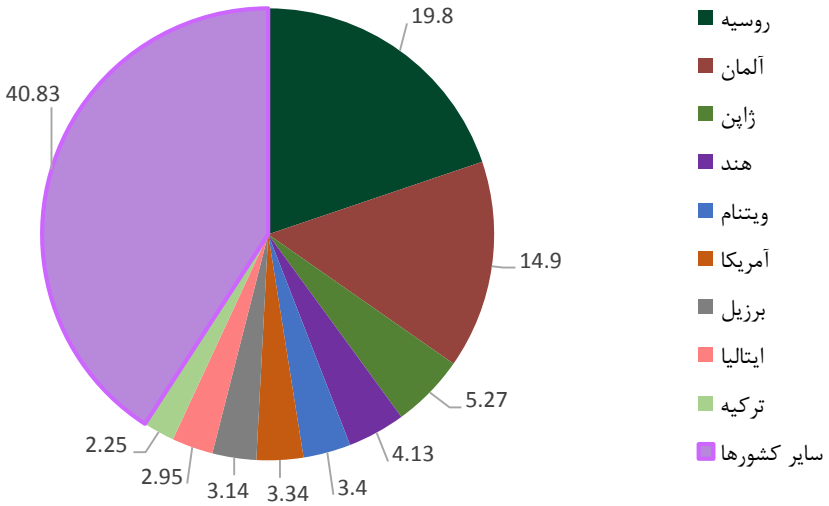
به طور متوسط ۳۸ درصد از کل تشخیص‌های بدافزارهای مالی مربوط به کامپیوترهای شرکتی هستند. در پایان سال ۲۰۱۶ این مقدار به ۴۹ درصد افزایش یافت.

[3] endpoints

توزیع جغرافیایی حملات بدافزار بانکی



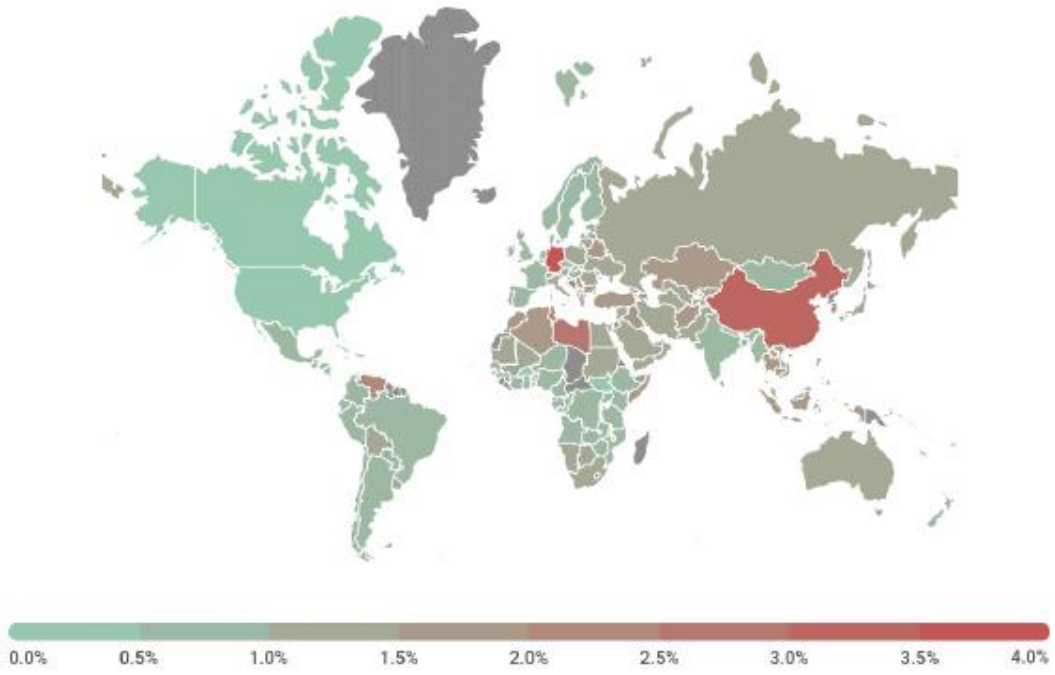
شکل ۷- توزیع جغرافیایی کاربران مورد حمله با بدافزار بانکی در سال ۲۰۱۵



شکل ۸- توزیع جغرافیایی کاربران مورد حمله با بدافزار بانکی در سال ۲۰۱۶

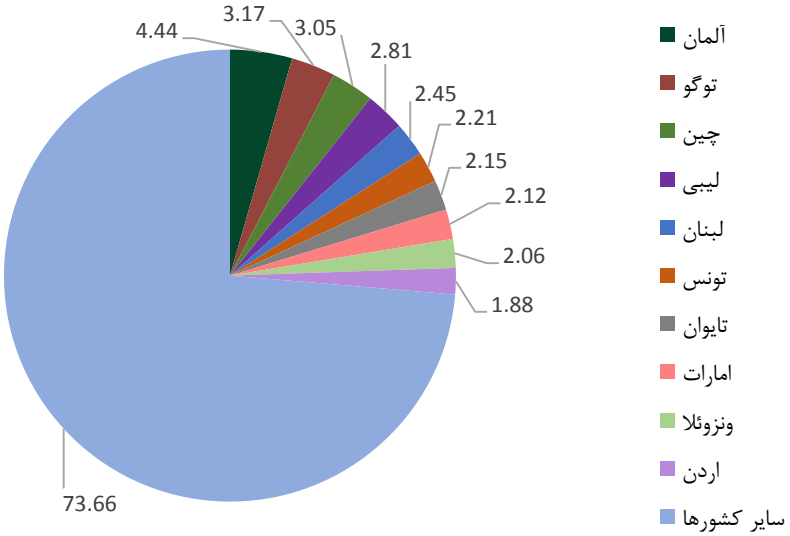
بیش از نیمی از کاربران مورد حمله با بدافزار بانکی در طی سال‌های ۲۰۱۵ و ۲۰۱۶ تنها در ۱۰ کشور قرار داشتند و در سال ۲۰۱۶ سهم ۱۰ کشور برتر ۵/۶ واحد درصد افزایش یافت.

در سال ۲۰۱۶ اسپانیا، اتریش، لهستان و امارات این لیست را ترک کردند و جایگاه خودشان را به ژاپن، برزیل و ترکیه دادند. سهم کاربران روسیه و آلمان به ترتیب ۵/۵ و ۴/۸ واحد درصد افزایش پیدا کرد، در حالیکه درصد کاربران آمریکا، ایتالیا و هند کاهش یافت.



شکل ۹- توزیع جغرافیایی حملات بدافزار بانکی در سال ۲۰۱۷

همانطور که در شکل ۹ مشاهده می‌شود، آزمایشگاه کسپرسکی برای ارزیابی و مقایسه خطر آلودگی به وسیله تروجان‌های بانکی و بدافزارهای دستگاه‌های خودپرداز و پایانه‌های فروش در سراسر جهان، درصد کاربران محصولات کسپرسکی در کشورهایی که در طول مدت گزارش با این تهدیدات مواجه شده‌اند را نسبت به کل کاربران محصولات کسپرسکی در آن کشورها محاسبه کرده است.



شکل ۱۰- توزیع جغرافیایی کاربران مورد حمله با بدافزار بانکی در سال ۲۰۱۷

(نادیده گرفتن کشورهایی که تعداد کاربران محصولات کسپرسکی در آن‌ها نسبتاً کم است (کمتر از ۱۰۰۰۰))

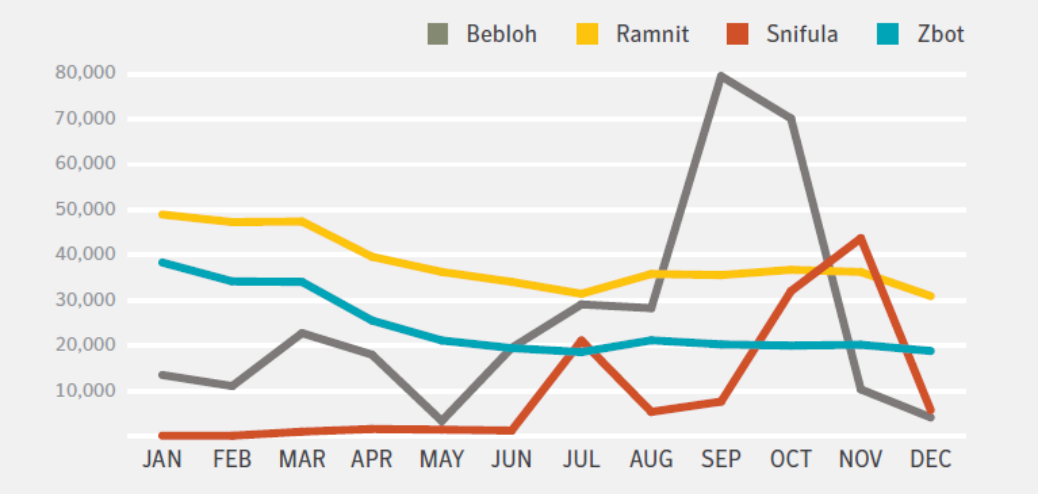
توزیع خانواده تهدید

فعال‌ترین خانواده‌های تهدید در سال ۲۰۱۶ شامل Ramnit، Bebloh، Snifula و گونه‌های Zeus بودند. بعد از عملیات فروپاشی بر علیه Ramnit در فوریه ۲۰۱۵، این تهدید غیرفعال شد؛ اما در سال ۲۰۱۶ دوباره ظاهر شد و بر گستره تروجان‌های مالی سلطه پیدا کرد. یک سال تمام، تعداد تشخیص‌های Ramnit بسیار بالا بود. باید به این نکته اشاره کرد که بعضی از گونه‌های خودتکثیر Ramnit فایل‌های اجرایی و HTML را آلوده می‌کنند که به شیوع آن کمک می‌کند.

Bebloh به سرعت در حال افزایش بود به طوریکه در طول یک سال تعداد تشخیص‌های آن بیش از ۲۳ برابر شد. در سپتامبر و اکتبر رشدهای ناگهانی در آلودگی‌های Bebloh به‌خصوص با کمپین‌های ایمیلی متمرکز روی ژاپن مشاهده شد.

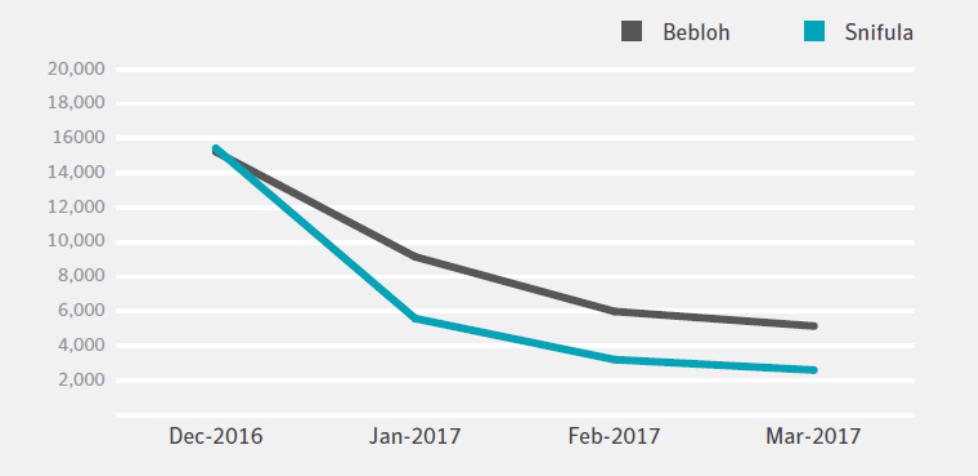
جدول ۱- تعداد تشخیص‌های تهدیدات مالی در سال‌های ۲۰۱۵ و ۲۰۱۶

تهدید	تعداد کامپیوترهای آلوده در سال ۲۰۱۵	تعداد کامپیوترهای آلوده در سال ۲۰۱۶
Ramnit/Gootkit	~۷۷۹,۰۰۰	~۴۶۰,۰۰۰
Bebloh	~۱۳,۰۰۰	~۳۱۰,۰۰۰
Zeus/Citadel & variants	~۹۶۰,۰۰۰	~۲۹۲,۰۰۰
Snifula/Vawtrak	~۴,۵۰۰	~۱۲۲,۰۰۰
Dridex/Cridex	~۶۲,۰۰۰	~۲۳,۰۰۰
Dyre	~۵۵,۰۰۰	~۴,۵۰۰
Shylock	~۱۴,۰۰۰	~۴,۵۰۰
Pandemiya	~۶۰۰	~۳,۵۰۰
Shifu	~۲۰۰	~۲,۰۰۰
SpyEye	~۳,۵۰۰	~۱,۵۰۰

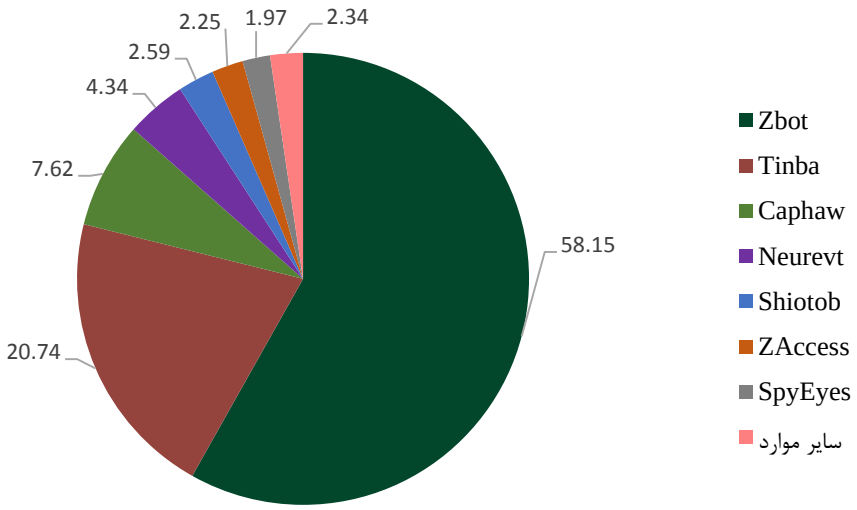


شکل ۱۱- تعداد تشخیص ماهانه برای چهار تهدید اول در سال ۲۰۱۶

از هم پاشیدن شبکه میزبان بدافزار Avalanche در پایان سال ۲۰۱۶، که Bebloh نیز از آن استفاده می‌کرد باعث کاهش چشمگیر فعالیت Bebloh در ابتدای نوامبر شد. پس از دستگیری متهم ایجادکننده تروجان Snifula در ژانویه ۲۰۱۷، کاهش تشخیص‌های Snifula گزارش شد. این رویدادها باعث کاهش تعداد تشخیص‌ها شدند، Bebloh از دسامبر ۲۰۱۶ تا مارس ۲۰۱۷، ۶۶ درصد و Snifula در همین بازه زمانی ۸۳ درصد کاهش داشت. اکنون به نظر می‌رسد که این تهدیدات تقریباً محو شده‌اند.

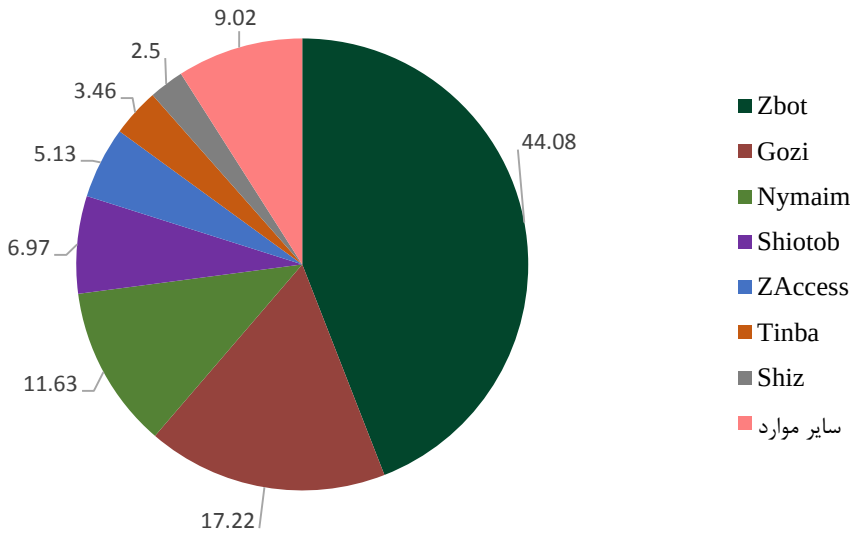


شکل ۱۲- تعداد تشخیص Snifula و Bebloh در فصل اول سال ۲۰۱۷



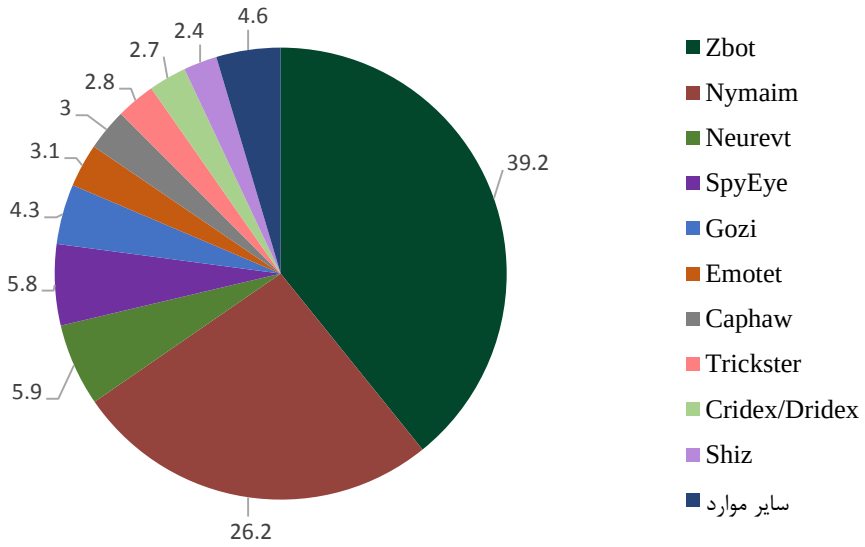
شکل ۱۳- توزیع شایع‌ترین خانواده‌های بدافزار بانکی در سال ۲۰۱۵

در سال ۲۰۱۶ وضعیت، کمی متفاوت بود. در حالیکه Zbot پیشگامی خود را حفظ کرده بود، Gozi خانواده-ای از تروجان‌های بانکی که در سال ۲۰۱۶ بسیار فعال بود، Zbot را به چالش کشاند. در همان زمان، Tinba چندین رتبه تنزل یافت و از رتبه دوم خود در سال ۲۰۱۵ به ششم در سال ۲۰۱۶ رسید.



شکل ۱۴- توزیع شایع‌ترین خانواده‌های بدافزار بانکی در سال ۲۰۱۶

شکل بعد ۱۰ خانواده از شایع‌ترین بدافزارها را نشان می‌دهد که در سال ۲۰۱۷ برای حمله به کاربران بانکی (برحسب درصد کاربران مورد حمله) مورد استفاده قرار گرفته‌اند.

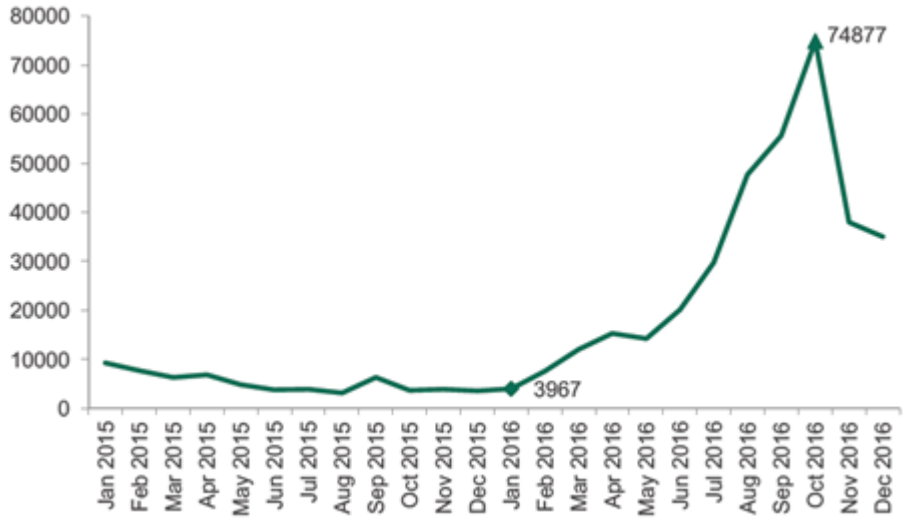


شکل ۱۵- توزیع شایع‌ترین خانواده‌های بدافزار بانکی در سال ۲۰۱۷

بدافزارهای بانکی اندروید

در یکی از بررسی‌های صورت گرفته توسط آزمایشگاه کسپرسکی در سال ۲۰۱۴ حملاتی با استفاده از بدافزارهای مالی به حدود ۸۰۰,۰۰۰ کاربر در سراسر جهان ثبت شد، اما بیشتر این کاربران توسط تروجان-های پیامکی مورد حمله قرار گرفتند و فقط حدود ۶۰,۰۰۰ کاربر با استفاده از تروجان‌های بانکی مورد حمله قرار گرفته بودند. در آن زمان، در سال ۲۰۱۴، استفاده از تروجان‌های پیامکی از متداول‌ترین انواع تقلب‌های مالی موبایل و تهدید مالی اصلی برای کاربران اندروید بود.

در طول سال ۲۰۱۵، تعداد کاربران مورد حمله توسط تروجان‌های بانکی اندروید با ۵۷,۶۰۷ کاربر در ۱۲ ماه حتی کمتر از سال ۲۰۱۴ بود.

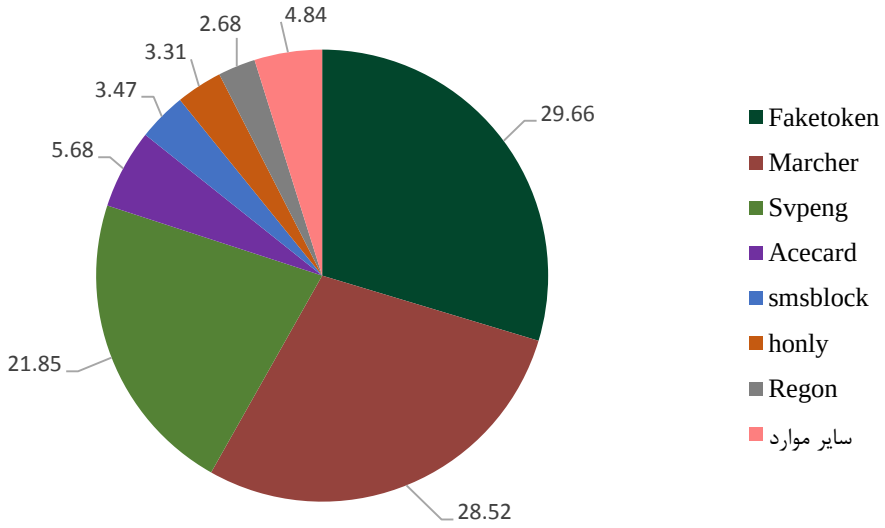


شکل ۱۶- تغییر تعداد کاربران مورد حمله با بدافزارهای بانکی اندروید در طی سال‌های ۲۰۱۵ تا ۲۰۱۶

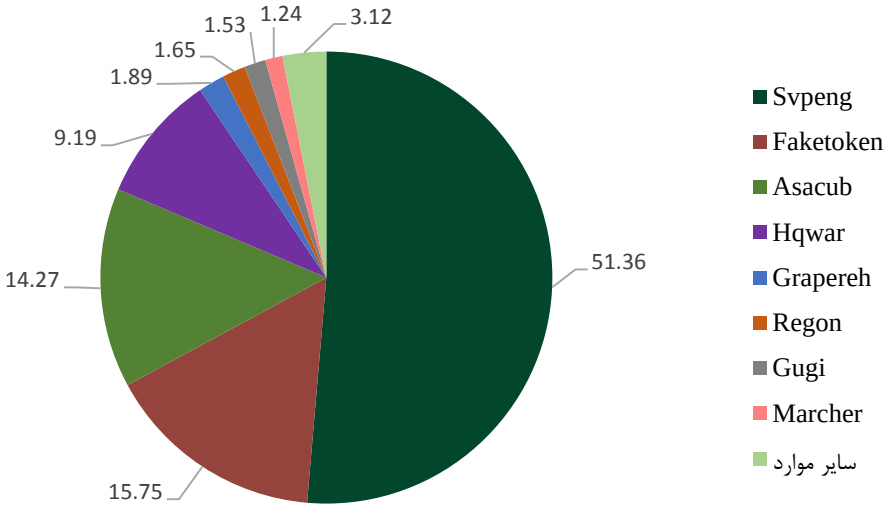
اما تعداد کاربران مورد حمله از ۳,۹۶۷ کاربر در ژانویه ۲۰۱۶ تا نزدیک به ۷۵,۰۰۰ کاربر در اکتبر ۲۰۱۶ رشد پیدا کرد و در مجموع، در سال ۲۰۱۶ بیش از ۳۰۵,۰۰۰ کاربر با بدافزارهای مالی مورد حمله قرار گرفتند که ۴۳۰ درصد بیشتر از سال ۲۰۱۵ است.

البته محققان آزمایشگاه کسپرسکی به محض اینکه تعداد کاربران مورد حمله شروع به رشد کردند، در مورد علت این افزایش ناگهانی به تحقیق پرداختند که مشخص شد تنها دو خانواده از بدافزارها عامل این تغییر عمده هستند. اولین مورد Asacub بود که به طور جدی از ابتدای سال ۲۰۱۶ از طریق SMS توزیع شده بود. مورد دوم Svpeng یک تروجان شناخته شده بانکی بود. این تروجان با روش جدیدی از طریق شبکه تبلیغاتی Google AdSense توزیع شده بود.

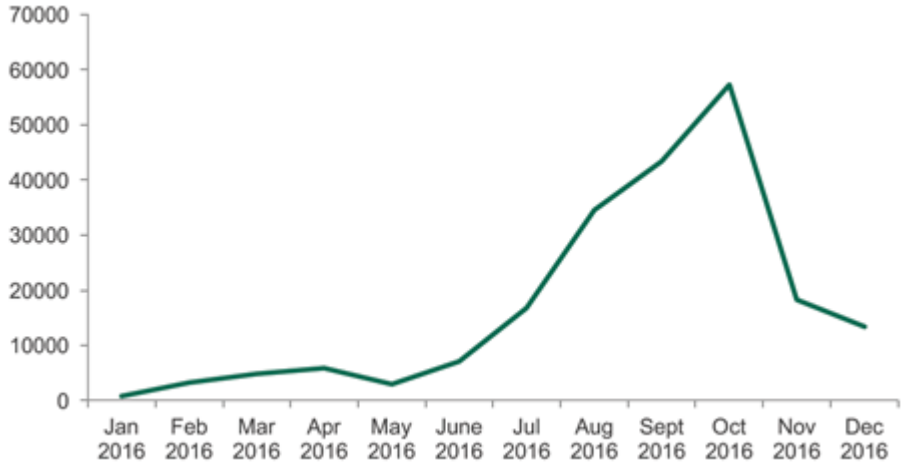
این بدافزار عمدتاً کاربران روسیه و کشورهای مشترک‌المنافع و تنها کسانی که در چندین رسانه خبری محبوب حضور داشتند را هدف قرار داد. امکان توزیع بالای تروجان به دلیل یک مسئله امنیتی شناسایی شده توسط محققان آزمایشگاه کسپرسکی در یک مرورگر محبوب موبایل بود که مجوز دانلود اپلیکیشن‌های مخرب را به صورت خودکار بر روی دستگاه مورد حمله داده بود. همانطور که در شکل ۱۶ دیده می‌شود، به محض اینکه توسعه‌دهنده مرورگر یک patch را منتشر نمود و گوگل متوجه شد که چگونه می‌تواند آگهی-های مخرب را شناسایی و مسدود کند، تعداد کاربران مورد حمله به سرعت کاهش یافت.



شکل ۱۷- شایع‌ترین بدافزارهای بانکی اندروید در سال ۲۰۱۵

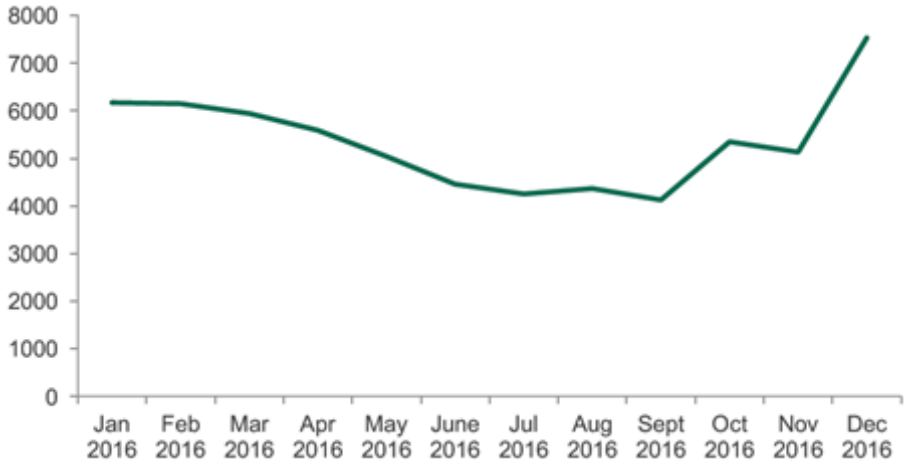


شکل ۱۸- شایع‌ترین بدافزارهای بانکی اندروید در سال ۲۰۱۶

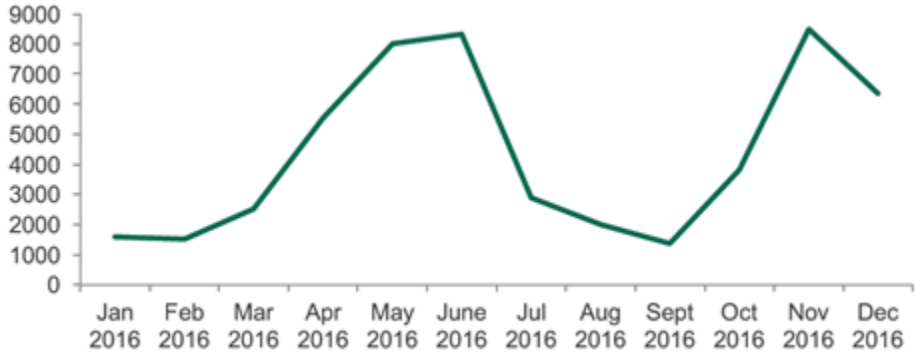


شکل ۱۹- تغییر تعداد کاربران مورد حمله توسط تروجان بانکی اندروید Svpeng

مجرمان برای خانواده Faketoken (پیشگام سال ۲۰۱۵) برخی از کارهای تبلیغاتی را نیز انجام دادند که نتیجه آن افزایش تقریباً سه برابری (۲/۹ برابری) تعداد کاربران مورد حمله از ۱۸,۷۰۰ در سال ۲۰۱۵ به ۵۴,۴۰۰ کاربر در سال ۲۰۱۶ بود.



شکل ۲۰- تغییر تعداد کاربران مورد حمله توسط بدافزار بانکی اندروید Faketoken

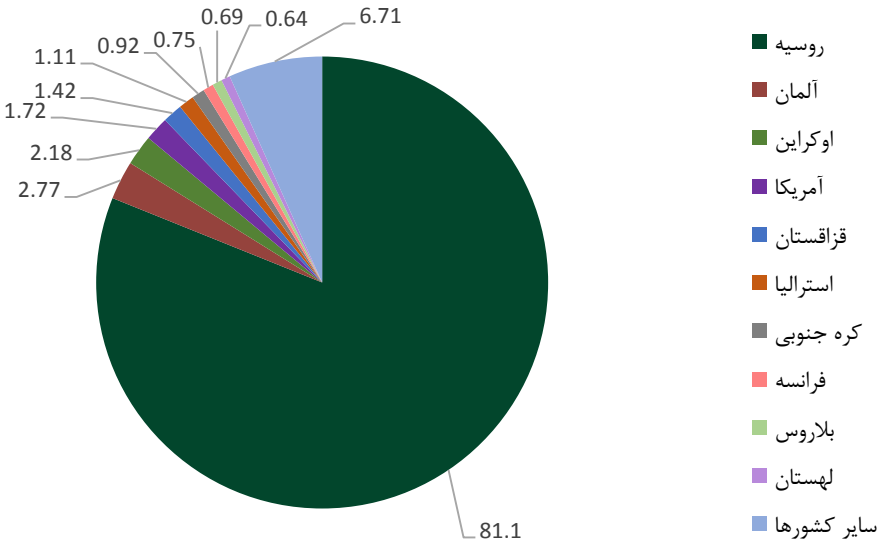


شکل ۲۱- تغییر تعداد کاربران مورد حمله توسط بدافزار بانکی اندروید Asacub

هکرهای پشت پرده Asacub، یکی دیگر از اعضای تروجان‌های بانکی اندروید برتر در سال ۲۰۱۶، برای روش توزیع خود از SMS-spam استفاده کردند. اکثر این اقدامات سازمان‌یافته از فوریه تا ژوئن و سپس از سپتامبر تا نوامبر ثبت شده بودند که به وضوح در شکل ۲۱ قابل مشاهده است.

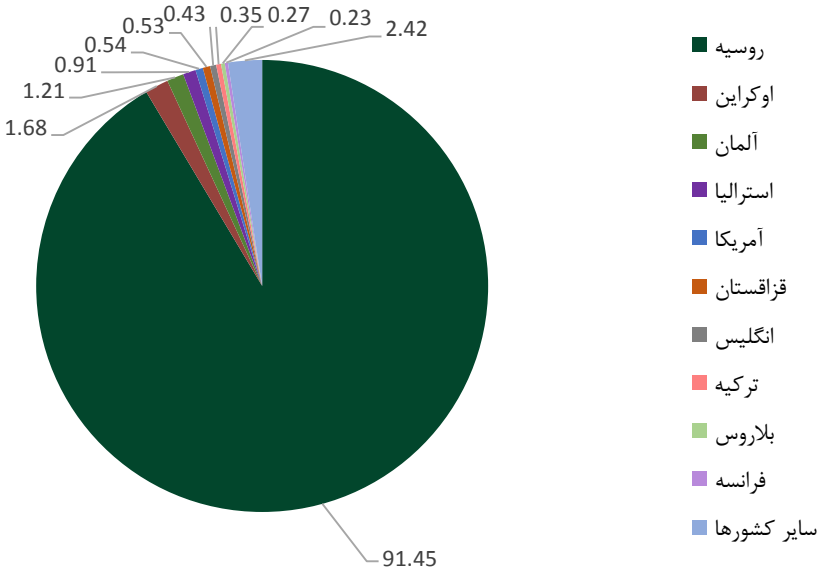
جغرافیای کاربران مورد حمله با بدافزار بانکی اندروید

جغرافیای حملات نیز در سال ۲۰۱۶ نسبت به سال ۲۰۱۵ تغییر نمود.

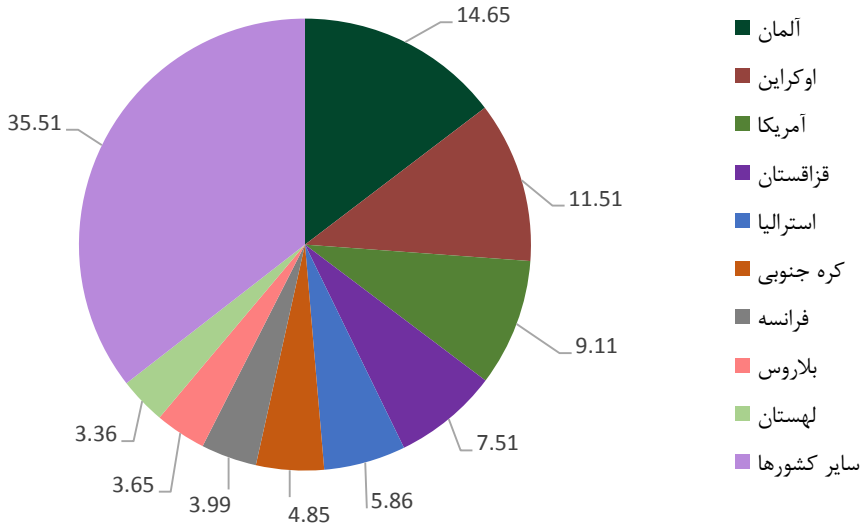


شکل ۲۲- توزیع کاربران مورد حمله با تروجان‌های بانکی اندروید در سال ۲۰۱۵

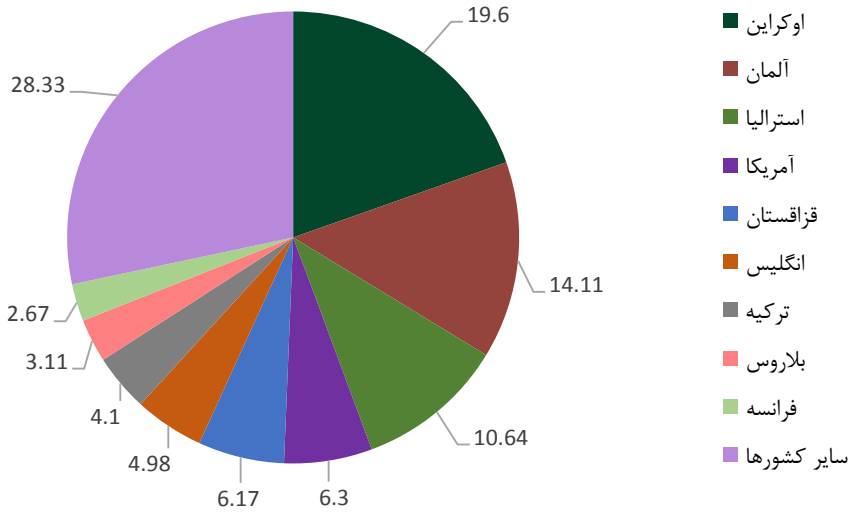
همانطور که در شکل‌های ۲۲ و ۲۳ دیده می‌شود، بدافزار بانکی اندروید عمدتاً در روسیه یک معضل است. لازم به ذکر است که این یافته‌ها تحت‌تأثیر توزیع عمومی کاربران محصولات آزمایشگاه کسپرسکی قرار دارد که بسیاری از آن‌ها در روسیه حضور دارند، همچنین بدافزار Svpeng که از یک آسیب‌پذیری در یک مرورگر استفاده کرده که عمدتاً این مرورگر در روسیه به‌کار رفته است. با توجه به این موضوع، تصویر نرمال‌سازی شده توزیع جغرافیایی حملات بانکی اندروید (با حذف داده‌های روسیه) در شکل ۲۴ و ۲۵ به تصویر کشیده شده است.



شکل ۲۳- توزیع کاربران مورد حمله با تروجان‌های بانکی اندروید در سال ۲۰۱۶



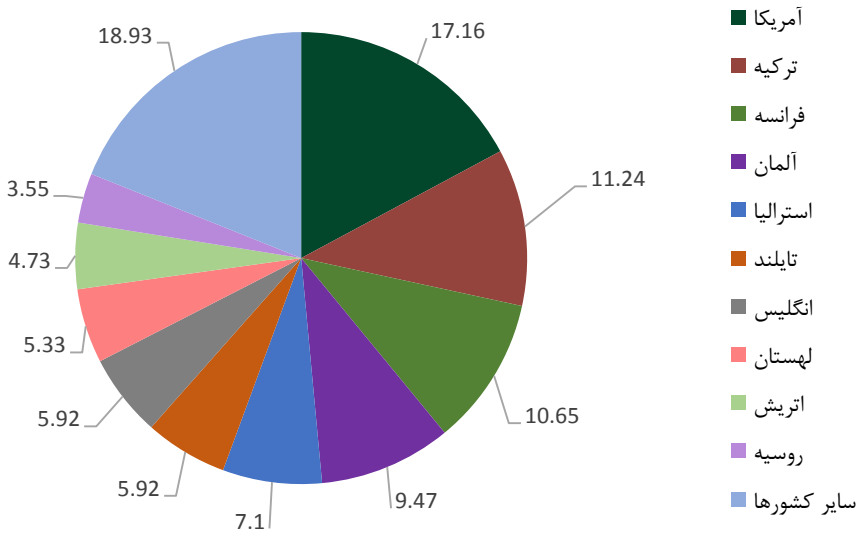
شکل ۲۴- توزیع کاربران مورد حمله با بدافزارهای بانکی اندروید در سال ۲۰۱۵ (۱۰،۸۸۷ کاربر، با حذف روسیه)



شکل ۲۵- توزیع کاربران مورد حمله با بدافزارهای بانکی اندروید در سال ۲۰۱۶ (۲۶،۱۱۰ کاربر، با حذف روسیه)

در سال ۲۰۱۶، ۱/۵۷ درصد از کاربران محصولات آزمایشگاه کسپرسکی حداقل یک بار با یک تروجان بانکی روبه‌رو شده‌اند.

نمونه‌های تحلیل شده بدافزار موبایل Android.Fakebank.B، ۱۶۹ برنامه کاربردی موبایل مختلف را از ۲۴ کشور مختلف هدف می‌گیرند. ایالات متحده با ۲۹ حمله به مؤسساتش در رأس کشورهای مورد حمله قرار گرفته است و ترکیه و فرانسه در جایگاه‌های بعدی هستند.



شکل ۲۶- ده کشور اول مورد هدف توسط Android.Fakebank.B

حمله به دستگاه‌های خودپرداز و پایانه‌های فروش

حمله به دستگاه‌های خودپرداز (ATM) و پایانه‌های فروش (POS) در سال ۲۰۱۶ نیز افزایش یافت. حدود ۱۰ سال است که بدافزارهای مربوط به دستگاه‌های خودپرداز وجود دارند؛ اما هنوز هم کارآمد هستند. با افزایش حملات هدفمند به بانک‌ها، حمله به دستگاه‌های خودپرداز از درون شبکه مالی نیز افزایش یافته است.

مجرمین برای برخی از حملات مربوط به دستگاه‌های خودپرداز به دسترسی فیزیکی به کامپیوتر ATM نیاز دارند و این کار را با باز کردن پوشش دستگاه با استفاده از یک کلید دزدی یا برداشتن قفل انجام می‌دهند. آن‌ها وقتی به درگاه USB یا CD-ROM دست یافتند می‌توانند بدافزار خود را نصب کنند یا صفحه کلیدی را متصل کرده و دستوراتی را صادر نمایند (بدافزار Ploutus از این روش حمله استفاده می‌کند).

حملات مشابهی نیز در هتل‌ها گزارش شده است که در این حملات مهاجمین اغلب از درگاه‌های USB پشت کامپیوترهای پرداخت برای نصب بدافزار استفاده می‌کنند و یا در فروشگاه‌های خرده‌فروشی که مهاجمین به درگاه شبکه داخل فروشگاه یک sniffer اضافه می‌کنند؛ بدین ترتیب می‌توانند هر دستگاه POS متصل را آلوده کرده و حافظه را برای اطلاعات کارت پرداخت کاوش کنند.

با دسترسی فیزیکی به دستگاه خودپرداز، می‌توان از یک روش حمله دیگر نیز استفاده کرد. طبق گزارشی که در آوریل ۲۰۱۷ منتشر شد، برخی از مهاجمین متوجه شدند که می‌توانند با سوراخ کردن بدنه دستگاه خودپرداز به سیستم گذرگاه داخل آن دسترسی پیدا کنند. به محض دسترسی پیدا کردن، تنها چیزی که موردنیاز است میکروکامپیوتر است تا با استفاده از آن بتوان دستورات را به گذرگاه ارسال نمود تا خودپرداز همه پول‌ها را بیرون بریزد.

در همه حملات مربوط به دستگاه‌های خودپرداز و پایانه‌های فروش نیازی به دسترسی فیزیکی به دستگاه نیست. در نوامبر ۲۰۱۶، FBI درباره گروه Buhtrap هشدار داد که به شبکه‌های داخلی مؤسسات مالی نفوذ کرده و دستورات مربوط به دستگاه خودپرداز را صادر می‌کرد که منجر به توزیع پول می‌شد. گروه Buhtrap این کار را بدون دستکاری فیزیکی دستگاه انجام می‌داد. در یک نمونه دیگر، مهاجمین توانستند بدافزار ATMitch را بر روی چندین دستگاه خودپرداز نصب کنند و حداقل ۸۰۰۰۰۰ دلار به‌دست آورند.

در رابطه با حملات پایانه‌های فروش نیز می‌توان به‌صورت راه دور عمل کرد. برای مثال، تروجان Flokibot کامپیوترهای پایانه‌های فروشی را جستجو می‌کند که تراکنش‌های کارت پرداخت را پردازش می‌کنند. مهاجمین با استفاده از ایمیل‌های فیشینگ هدفدار، کامپیوترها را آلوده کردند و سپس با استفاده از نرم‌افزار TeamViewer و Ammyy Admin کامپیوترهای آلوده را از راه دور کنترل کرده و حملات خود را پیش بردند.

در آگوست ۲۰۱۶، وب‌سایت یک فروشنده نرم‌افزار POS آلوده شد. طبق گزارش‌های منتشر شده، اطلاعات به سرقت رفته، دسترسی راه دور به سیستم‌های پایانه فروش خرده‌فروش‌های متعددی را در اختیار مهاجمین قرار داده بود. این افشا باعث شد تا فروشنده تمام رمزهای عبور سیستم‌های آلوده را ریست نماید.

راهکارهای پیشنهادی

کاربران به منظور کاهش خطرات حملات سایبری، باید این توصیه‌ها را به کار گیرند:

برای کاربران خانگی

- هرگز بر روی لینک‌هایی که توسط افراد ناشناس به شما ارسال می‌شوند، کلیک نکنید و یا لینک-های مشکوک را باز نکنید، حتی اگر از طریق شبکه‌های اجتماعی یا ایمیل از طرف دوستان‌تان ارسال می‌شوند. این لینک‌های مخرب برای دانلود بدافزار بر روی دستگاه شما طراحی شده‌اند و یا شما را به صفحات وب فیشینگ هدایت می‌کنند تا اعتبارنامه‌های مالی را به‌دست آورند.
- مراقب فایل‌های ناشناخته باشید. هرگز آن‌ها را بر روی دستگاه خود باز یا ذخیره نکنید، چون ممکن است مخرب باشند.
- اگرچه استفاده از شبکه‌های Wi-Fi عمومی مناسب به نظر می‌رسند، اما می‌توانند ناامن و غیرقابل اعتماد باشند و اکثراً hotspotها هدف اصلی هکرها برای سرقت اطلاعات کاربر می‌شوند. برای حفظ امنیت اطلاعات محرمانه خود، هرگز از hotspotها برای پرداخت‌های آنلاین و یا به اشتراک گذاشتن اطلاعات مالی استفاده نکنید. با این حال، اگر هیچ گزینه دیگری ندارید، از یک سرویس VPN استفاده کنید که تمام داده‌هایی را که انتقال می‌دهید، رمزنگاری می‌کند.
- وب‌سایت‌ها می‌توانند آوردگاهی برای مجرمان سایبری، تنها با هدف جمع‌آوری داده‌های شما باشند. در صورتی‌که یک سایت به نظر مشکوک یا ناشناخته است، برای جلوگیری از افتادن اطلاعات محرمانه‌تان در دست دیگران، اطلاعات کارت اعتباری‌تان را وارد نکنید یا خرید انجام ندهید.
- برای پیشگیری از به دام افتادن، همیشه قبل از وارد کردن اعتبارنامه‌های خود با دوبار چک کردن فرمت URL یا املای نام شرکت بررسی کنید که وب‌سایت، واقعی باشد. وب‌سایت‌های جعلی ممکن است درست مانند وب‌سایت‌های واقعی باشند، اما ناهنجاری‌هایی وجود خواهند داشت که به شما کمک خواهد کرد تا اختلاف را تشخیص دهید.
- برای اطمینان بیشتر در هنگام ارزیابی ایمنی یک وب‌سایت، فقط از وب‌سایت‌هایی استفاده کنید که با HTTPS:// شروع می‌شوند که در واقع یک اتصال رمز شده را ارائه می‌دهند. سایت‌های HTTP:// امنیت مشابه را ارائه نمی‌دهند و می‌توانند اطلاعات شما را در معرض خطر قرار دهند.

- هرگز رمزهای عبور خود را به هیچ‌کس حتی نزدیک‌ترین دوستان خود نشان ندهید. به اشتراک-گذاری آن‌ها سطح خطر برای حساب‌های شخصی شما را افزایش می‌دهد. این موضوع می‌تواند موجب دسترسی به اطلاعات مالی شما توسط مجرمان سایبری و سرقت پول‌تان شود.
- برای ایمن نگه داشتن اعتبارنامه‌های خود باید سطوح امنیتی و حفاظتی را در تمام دستگاه‌های خود مانند دسکتاپ، لپ‌تاپ یا موبایل اعمال کنید. سوءاستفاده مجرمان سایبری هیچ مرزی ندارد.

برای کسب‌وکارها

- به کارکنان خود اطلاع دهید که بر روی لینک‌های ناشناخته کلیک نکنند یا پیوست‌های دریافت شده از منابع غیرقابل اعتماد را باز نکنند.
- به نقاط پایانی که از آن برای انجام عملیات مالی استفاده می‌شود توجه خاصی کنید: ابتدا نرم‌افزار نصب شده در این نقاط پایانی را به‌روزرسانی کنید و راهکارهای امنیتی آن را به‌روز نگه دارید.
- به طور منظم برای آموزش امنیت سایبری کارکنانی که از ابزارهای مالی آنلاین در شرکت شما استفاده می‌کنند، سرمایه‌گذاری کنید. به آن‌ها کمک کنید تا یاد بگیرند چگونه ایمیل‌های فیشینگ را تشخیص دهند و در صورتی‌که یک نقطه پایانی آلوده شده است، چگونه آن را شناسایی کنند.
- استفاده از راهکارهای امنیتی مجهز به فناوری‌های حفاظت مبتنی بر رفتار که باعث می‌شود حتی بدافزارهای بانکی ناشناخته نیز شناسایی شوند.

منابع:

[1] Kaspersky Labs' "*Financial Cyberthreats in 2016"* report, February 2017.

[2] Symantec, "*Financial Threats Review 2017",* An ISTR Special report, May 2017, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf

[3] Kaspersky Lab, "*Overall Statistics for 2017*", Kaspersky Security Bulletin, 14 December 2017.

Kaspersky Lab, "*Threat Predictions for Financial Services and Fraud*", Kaspersky Security Bulletin: Threat Predictions for 2018, 6 December 2017.

Kaspersky Labs, "*Threat Predictions for Cryptocurrencies*", Kaspersky Security Bulletin: Threat Predictions for 2018, 15 November 2017.

پیش‌بینی تهدیدات سایبری برای خدمات حوزه مالی در سال ۲۰۱۸

چشم‌انداز تهدیدات سایبری برای حوزه مالی در سال ۲۰۱۷

در سال ۲۰۱۷ حملات کلاهبرداری[1] بسیاری علیه خدمات حوزه مالی انجام گرفت که این حملات به‌طور فزاینده‌ای بر روی حساب‌های کاربری مشتریان بانکی متمرکز بوده‌اند. اطلاعات مشتری، یک عامل کلیدی برای انجام حملات کلاهبرداری در مقیاس گسترده است و فراوانی نقض داده‌ها در بین انواع مختلفی از حملات موفق دیگر، منابع ارزشمندی از اطلاعات شخصی افراد را در اختیار مجرمان سایبری قرار داده است تا آن‌ها از این اطلاعات برای دسترسی غیرمجاز به حساب کاربری[2] مشتریان یا حملات جعل هویت[3] استفاده کنند. حملاتی که بر روی حساب‌های کاربری مشتریان بانکی متمرکز[4] است، می‌تواند منجر به زیان‌های بیشتری از جمله کاهش اعتماد افراد و افشای بیشتر اطلاعات مشتری شود. بنابراین کاهش این حملات، هم برای کسب‌وکارها و هم برای مشتریانی که از خدمات حوزه مالی استفاده می‌کنند به یک اندازه مهم می‌باشد.

در سال ۲۰۱۸ منتظر چه اتفاقی می‌توان بود؟

سال ۲۰۱۸، سالی همراه با نوآوری و تغییرات در خدمات حوزه مالی خواهد بود، زیرا سرعت تغییر در این فضا بسیار زیاد است. همزمان با ارائه خدمات مالی جدید و کانال‌های ارتباطی بیشتر، تهدیدات و حملات نیز متنوع‌تر خواهند شد. خدمات حوزه مالی به منظور شناسایی موفق کلاهبرداری‌های بیشتر از حساب‌های بانکی آنلاین تا کانال‌های ارتباطی جدیدتر، نیاز به تمرکز بر روی پیشگیری از کلاهبرداری در کانال‌های همه‌کاره[5] دارند. به‌دلیل سودآوری حملات انجام شده برای مجرمان سایبری، تلاش‌های بیشتری برای حمله به روش‌های پرداخت جدید صورت خواهد گرفت.

[1] Fraud attacks
[2] Account takeover
[3] False identity attacks
[4] Account-centric attacks
[5] omni-channel

چالش‌های پرداخت بلادرنگ

افزایش تقاضای مشتریان برای انجام تراکنش‌های مالی بین‌المللی و بلادرنگ، موجب فشار برای تحلیل هرچه سریع‌تر ریسک می‌شود. انتظارات مشتریان برای پرداخت‌های سازگار[۶] نیز این کار را سخت‌تر می‌کند. خدمات حوزه مالی نیازمند بازنگری و ایجاد فرآیندهای مؤثرتری با عنوان «شناخت مشتریان»[۷] می‌باشند. یادگیری ماشین و در نهایت راه‌حل‌های مبتنی بر هوش مصنوعی در برطرف کردن نیاز به تشخیص هرچه سریع‌تر کلاهبرداری و ریسک نقش مهمی دارند.

تقاضای رو به رشد برای انجام تراکنش‌های بسیار سریع و آسان (از جمله پرداخت‌های آنی بین‌المللی) سبب می‌شود تا بانک‌ها، سیستم‌های پرداخت و غیره، تصمیمات سریع‌تری در خصوص صحت یک تراکنش اتخاذ کنند و این امر احتمال اشتباه و لغزش در کلاهبرداری از طریق شبکه اینترنت را افزایش می‌دهد، بنابراین با ریسک بزرگی در این زمینه مواجه هستیم. راه‌حل این کار، انجام بررسی‌های دقیق‌تر و در عین حال سریع است که این موضوع با کمک راهکارهای مبتنی بر هوش مصنوعی و یادگیری ماشین میسر خواهد شد.

حملات مهندسی اجتماعی[۸]

خدمات حوزه مالی باید بر روی تکنیک‌هایی از حملات متمرکز شوند که مورد آزمایش قرار گرفته‌اند. علی‌رغم وجود تهدیدات پیچیده‌تر، مهندسی اجتماعی و فیشینگ که به‌عنوان یکی از ساده‌ترین و سودآورترین حملات هستند، همچنان از عامل انسانی به‌عنوان ضعیف‌ترین حلقه زنجیر استفاده می‌کنند. بنابراین باید آموزش‌هایی مستمر به مشتریان و کارمندان، جهت آگاهی از آخرین حملات و کلاهبرداری‌ها ارائه شود.

تهدیدات موبایل

با توجه به آخرین فهرست امنیت سایبری کسپرسکی، در حال حاضر بیشتر کارهای آنلاین از طریق موبایل انجام می‌شود. به‌عنوان مثال، در حال حاضر ۳۵ درصد از مردم از تلفن هوشمند خود برای بانکداری آنلاین و ۲۹ درصد برای سیستم‌های پرداخت آنلاین استفاده می‌کنند (این میزان در سال ۲۰۱۶، به‌ترتیب بیش از ۲۲ درصد و ۱۹ درصد بود).

[6] Friction-free payments
[7] Know Your Customer
[8] Social engineering attacks

کاربران مبتدی موبایل، بیش از پیش جزء اهداف اصلی کلاهبرداری خواهند بود. مجرمان سایبری از خانواده بدافزارهای موفق قدیمی و جدید استفاده خواهند کرد تا اطلاعات محرمانه بانکی کاربر را به روشی خلاقانه سرقت کنند. در سال ۲۰۱۷ یک نمونه اصلاح شده از خانواده بدافزار Svpeng مشاهده شد. در سال ۲۰۱۸، خانواده‌های دیگری از بدافزارهای موبایل، با ویژگی‌های جدید و با هدف سرقت اطلاعات محرمانه بانکی کاربران به وجود خواهند آمد. شناسایی و حذف بدافزارهای موبایل برای مؤسسات ارائه‌دهنده خدمات حوزه مالی ضروری می‌باشد تا آن‌ها بتوانند این حملات را در مراحل اولیه متوقف کنند.

نقض داده‌ها[9]

نقض داده‌ها در سال ۲۰۱۸ نیز ادامه خواهد داشت و تأثیر ثانویه‌ای بر مؤسسات مالی از طریق ایجاد حساب کاربری جعلی و حملات دسترسی غیرمجاز به حساب کاربری احساس خواهد شد. نقض داده‌ها، هرچند سخت‌تر از انجام حملات کلاهبرداری انفرادی علیه مشتریان است، اما در صورت موفقیت‌آمیز بودن، به‌دلیل حجم بالای داده‌های افشا شده مشتریان، برای مجرمان بسیار سودآور است. خدمات حوزه مالی باید به‌طور منظم راهکارهای دفاعی خود را تست کرده و از راه‌حل‌هایی برای تشخیص هرگونه دسترسی مشکوک در مراحل اولیه استفاده کنند.

اهداف پول رمزنگاری شده[10]

بیشتر مؤسسات مالی، برنامه‌های کاربردی پول‌های رمزنگاری شده را بررسی می‌کنند و حمله به این پول‌ها را یک هدف کلیدی برای مجرمان سایبری می‌دانند. در سال ۲۰۱۷ بدافزارهای استخراج افزایش پیدا کردند و انتظار می‌رود که در سال ۲۰۱۸ به منظور سوءاستفاده از این پول‌ها تلاش‌های بیشتری صورت گیرد. باید راهکارهایی که قادر به شناسایی آخرین خانواده بدافزارها هستند و همچنین ترکیبی از آخرین تهدیدات هوشمندانه، به‌عنوان استراتژی‌های پیشگیرانه به کار روند.

[9] Data breaches
[10] Cryptocurrency

دسترسی غیرمجاز به حساب کاربری

در دهه گذشته، بیشتر پرداخت‌های فیزیکی امن به واسطه فناوری تراشه و پیشرفت‌های پایانه فروش موجب تغییر کلاهبرداری آنلاین شده‌اند. در حال حاضر به‌دلیل اینکه امنیت پرداخت آنلاین از طریق نشانه‌گذاری[11]، فناوری بیومتریک[12] و دیگر موارد بهبود پیدا کرده است، کلاهبرداران به حملات دسترسی غیرمجاز به حساب کاربری روی آورده‌اند. برآوردهای صنعتی نشان می‌دهد که این شیوه کلاهبرداری از لحاظ مالی میلیاردها دلار برای کلاهبرداران سود دارد، به همین دلیل کلاهبرداران این مسیر حمله بسیار سودآور را دنبال می‌کنند. خدمات حوزه مالی، نیازمند بازنگری هویت دیجیتال و استفاده از راه‌حل‌های نوآورانه می‌باشند تا اطمینان حاصل کنند مشتریان همان افرادی هستند که ادعا می‌کنند.

طبق گزارش مؤسسه "اقدام علیه کلاهبرداری مالی انگلیس"[13]، دسترسی غیرمجاز به حساب کاربری، هر ساله افزایش می‌یابد (به‌عنوان مثال، افزایش ۵ درصدی از سال ۲۰۱۵ تا سال ۲۰۱۶)؛ این در حالی است که با توجه به برآوردهای Forrester، دسترسی غیرمجاز به حساب‌های کاربری سبب حداقل ۶/۵ میلیارد دلار زیان سالانه می‌شود، رقمی که در سال‌های آینده افزایش می‌یابد.

ایجاد فشار برای نوآوری

در سال ۲۰۱۸، کسب‌وکارها بیش از پیش به پیشنهادات بانکداری باز[14] و راهکارهای پرداخت عمل خواهند کرد. نوآوری برای شرکت‌های عهده‌دار خدمات حوزه مالی که به دنبال مزیت رقابتی در برابر تعداد بیشتری از رقبا هستند، کلیدی خواهد بود. این پیشنهادات جدید پس از عرضه به مشتریان یکی از اهداف کلاهبرداران خواهند بود و راه‌حل‌های جدیدی که به صورت ایمن طراحی نشده باشند، تبدیل به هدفی آسان، برای مجرمان سایبری می‌شوند.

نمونه‌هایی از نوآوری در ارائه خدمات بانکی شامل: Square، شرکت ارائه‌دهنده خدمات پرداخت آنلاین[15] است که تبادل بیت‌کوین را برای مشتریان معرفی کرد و همچنین فیس‌بوک شبکه رسانه‌های اجتماعی که مجوز بانکی را در سال ۲۰۱۶ کسب کرد.

---

[11] tokenization
[12] Biometric technology
[13] Financial Fraud Action UK
[14] Open banking
[15] Online payments company

پیش‌بینی تهدیدات سایبری برای پول‌های رمزنگاری شده در سال ۲۰۱۸

مقدمه

امروزه، پول رمزنگاری شده تنها مختص افراد متخصص در حوزه کامپیوتر و فناوری اطلاعات نیست. پول رمزنگاری شده بیشتر از آنچه که مردم متوجه شده‌اند، بر زندگی روزمره آن‌ها تأثیر گذاشته است و در عین حال، به سرعت به یک هدف جذاب برای مجرمان سایبری تبدیل شده است.

برخی از تهدیدات سایبری از پرداخت‌های الکترونیکی، نشأت گرفته شده‌اند مانند تغییر آدرس کیف پول مقصد در حین تراکنش‌ها، سرقت کیف پول الکترونیکی و موارد دیگر. با این حال، پول‌های رمزنگاری شده منجر به ایجاد روش‌های جدید و بی‌سابقه‌ای برای کسب درآمد از اقدامات خرابکارانه شده‌اند.

چشم‌انداز پول‌های رمزنگاری شده در سال ۲۰۱۷

در سال ۲۰۱۷، باج‌افزار تهدید اصلی جهانی برای کاربران بود و قربانیان به منظور بازیابی فایل‌ها و داده‌های رمزنگاری شده خود توسط مهاجمان، مجبور بودند که باج تقاضا شده را با استفاده از پول رمزنگاری شده پرداخت کنند. در هشت ماهه نخست سال ۲۰۱۷، محصولات آزمایشگاه کسپرسکی ۱/۶۵ میلیون کاربر را از استخراج‌کننده‌های[1] مخرب پول رمزنگاری شده محافظت نمودند و انتظار می‌رود که این رقم تا پایان این سال به بیش از دو میلیون نفر رسیده باشد. علاوه بر این، پس از گذشت چند سال در سال ۲۰۱۷ بازگشت سارقان بیت-کوین دیده شد.

در سال ۲۰۱۸ چه انتظاری می‌توان داشت؟

با افزایش مداوم تعداد، پذیرش و ارزش بازاری پول رمزنگاری شده، نه تنها این پول‌ها به‌عنوان یک هدف جذاب برای مجرمان سایبری باقی خواهند ماند، بلکه منجر به استفاده از تکنیک‌ها و ابزارهای پیشرفته‌تری برای ایجاد پول‌های رمزنگاری شده بیشتر خواهند شد. مجرمان سایبری به سرعت توجه خود را به سمت سودآورترین طرح‌های پول‌سازی معطوف خواهند نمود. بنابراین، احتمالاً سال ۲۰۱۸ سال استخراج‌کنندگان مخرب در وب خواهد بود.

[1] miner

حملات باج‌افزار، کاربران را مجبور به خرید پول رمزنگاری شده خواهد کرد.

به دلیل بازار نابسامان و تقریباً بی‌نام و نشان پول رمزنگاری شده که نیازی به اشتراک‌گذاری هیچ اطلاعاتی با هیچ‌کس ندارد، کسی آدرس مجرم را مسدود نخواهد کرد و یا او را دستگیر نمی‌کند و همچنین احتمال کمی که برای ردیابی شدن شخص وجود دارد، مجرمان سایبری همچنان با پول رمزنگاری شده تقاضای باج می‌کنند. در عین حال، تسهیل بیشتر روند کسب درآمد، منجر به اشاعه گسترده‌تر رمزگذارها خواهد شد.

حملات هدفمند با استخراج‌کنندگان

انتظار می‌رود که حملات هدفمند به شرکت‌ها به منظور نصب استخراج‌کنندگان افزایش یابد. در حالی‌که باج-افزار درآمدزایی زیاد اما فقط برای یک بار را دارد، استخراج‌کنندگان کسب درآمد پایین‌تر اما درازمدتی را خواهند داشت.

افزایش استخراج‌کنندگان ادامه خواهد یافت و افراد جدیدی را در بر خواهد گرفت.

در سال ۲۰۱۸، استخراج در سراسر جهان گسترش خواهد یافت و افراد بیشتری را به سمت خود جذب خواهد کرد. مشارکت استخراج‌کنندگان جدید بستگی به توانایی آن‌ها در دسترسی به منبع برق رایگان و پایدار خواهد داشت. بنابراین، افزایش "استخراج‌کنندگان داخلی" مشهود خواهد بود، به طوریکه کارمندان بیشتری در سازمان‌های دولتی شروع به استخراج با کامپیوترهای دولتی می‌کنند و همچنین کارکنان شرکت‌های تولیدی بیشتری از امکانات متعلق به شرکت استفاده خواهند نمود.

استخراج در وب

استخراج در وب، یک تکنیک استخراج پول رمزنگاری شده است که به طور مستقیم با نصب یک اسکریپت خاص بر روی یک صفحه وب در مرورگر صورت می‌گیرد. مهاجمان قبلاً ثابت کرده‌اند که بارگذاری یک اسکریپت بر روی یک وب‌سایت آلوده ساده است و با این اقدام، کامپیوترهای بازدیدکنندگان را برای استخراج به کار می‌گیرند؛ در نتیجه، سکه‌های بیشتری به کیف پول مجرمان افزوده می‌شود.

در سال ۲۰۱۸، استخراج در وب به طرز چشمگیری بر ماهیت اینترنت تأثیر خواهد گذاشت و منجر به راهکارهای جدیدی برای کسب درآمد وب‌سایت خواهد شد. یکی از این موارد، جایگزینی تبلیغات خواهد بود: در صورتی که کاربر موافق پرداخت هزینه محتوا باشد، وب‌سایت‌ها اسکریپت استخراج را به صورت دائمی حذف خواهند کرد. از سوی دیگر، انواع مختلف سرگرمی مانند فیلم، به صورت رایگان در ازای استخراج شما ارائه خواهد شد. یکی از روش‌های دیگر، مبتنی بر یک سیستم بررسی امنیت وب‌سایت است. تأیید Captcha برای تشخیص انسان از ربات با روش‌های استخراج در وب جایگزین خواهد شد و مهم نخواهد بود که یک بازدیدکننده ربات است یا انسان؛ چرا که آن‌ها با استخراج منفعت خواهند رساند.

کاهش ICO[۲] (عرضه اولیه سکه)

عرضه اولیه سکه به معنی سرمایه‌گذاری جمعی از طریق پول‌های رمزنگاری شده است. سال ۲۰۱۷ از این لحاظ، رشد فوق‌العاده‌ای را داشت که با جمع‌آوری بیش از ۳ میلیارد دلار توسط پروژه‌های مختلف، به نوعی با زنجیره بلوک[۳] بیشترین ارتباط را داشت. باید انتظار داشت که در سال ۲۰۱۸ با دنباله‌ای از شکست‌ها (عدم توانایی برای تولید محصول سرمایه‌گذاری شده توسط عرضه اولیه سکه) و انتخاب دقیق‌تر پروژه‌های سرمایه‌گذاری، تب و تاب عرضه اولیه سکه کاهش یابد. تعدادی از پروژه‌های ناموفق عرضه اولیه سکه ممکن است بر نرخ پول‌های رمزنگاری شده مبادله‌ای (Bitcoin، Ethereum و ...) که در سال ۲۰۱۷ رشد بی‌سابقه‌ای را تجربه کردند، تأثیر منفی بگذارد. بنابراین، تعداد حملات فیشینگ و هک برای هدف قرار دادن عرضه اولیه سکه، قراردادهای هوشمند و کیف‌های پول کاهش خواهد یافت.

نتیجه‌گیری

فناوری‌های ارتباطی، امکان ایجاد زندگی بهتر و امن‌تری را فراهم می‌آورند، اما آن‌ها آسیب‌پذیری‌های جدیدی را نیز به وجود می‌آورند که مهاجمان سایبری به سرعت از آن بهره می‌برند. این پیش‌بینی‌ها بر اساس تجربیات محققان و متخصصان امنیت در سال گذشته به دست آمده است. این پیش‌بینی‌ها نظرات کارشناسی هستند و ممکن است که همه آن‌ها تحقق نیابند. اما آماده شدن نیمی از نبرد است.

[2] Initial Coin Offering
[3] blockchain