روند تهدیدات سایبری در حوزه مالی و راهکارهای پیشنهادی

بر اساس گزارش آزمایشگاه Kaspersky

مقدمه

چشم‌انداز تهدیدات سایبری در حوزه مالی به طور مداوم در حال تغییر است. در چند سال گذشته، مجرمان سایبری حوزه مالی، تمرکز خود را از حملات علیه کاربران خصوصی بانکداری آنلاین، فروشگاه‌های الکترونیکی و سیستم‌های پرداخت به حملات در زیرساخت سازمان‌های بزرگ همچون بانک‌ها و سیستم‌های پردازش پرداخت همانند خرده‌فروشان، هتل‌ها و کسب‌وکارهای دیگر که پایانه‌های POS را به طور گسترده استفاده می‌کنند، تغییر داده‌اند.

این افزایش تعداد حملات علیه سازمان‌های بزرگ می‌تواند به این شکل توضیح داده شود که اگرچه هزینه-های آماده‌سازی و اجرای چنین حملاتی بسیار زیاد است، اما نتیجه ممکن است صد برابر بیشتر از نتیجه موفقیت‌آمیز اقدامات سازمان‌یافته بدخواهانه علیه کاربران خصوصی باشد. این نظریه توسط گروه جرایم سایبری مالی Carbanak و پیروان آن، از جمله هکرهای جامعه جهانی ارتباطات مالی بین بانکی (SWIFT)[1] که عامل اکثر حوادث جرایم سایبری مالی بزرگ در سال 2016 بوده‌اند، به اثبات رسید. با استفاده از روش‌های حمله غیرجزئی و به حداقل رساندن استفاده از نرم‌افزارهای مخرب منحصر به فرد به کمک ابزارهای منبع باز، این گروه‌ها توانسته‌اند میلیون‌ها دلار را سرقت کنند ولی متأسفانه هنوز دستگیر نشده‌اند.

با این حال، هرچند مجرمان حرفه‌ای هدف‌گیری خود را به سمت اهداف بزرگ تغییر داده‌اند، اما این بدین معنی نیست که کاربران عادی و کسب‌وکارهای کوچک و متوسط، دیگر در معرض خطر جرایم سایبری مالی نیستند. برعکس، پس از اینکه مشخص شد تعداد کاربران مورد حمله در سال‌های 2014 و 2015 کاهش یافته است، تعداد قربانیان در سال 2016 دوباره شروع به رشد کرد. این گزارش به ارائه روند

[1] Society for Worldwide Interbank Financial Telecommunication

تهدیدات سایبری در حوزه مالی اختصاص یافته است و تهدیدات فیشینگ کاربران کامپیوترهای مبتنی بر ویندوز و Mac و بدافزار مالی مبتنی بر ویندوز و مبتنی بر اندروید را شامل می‌شود.

یافته‌های کلیدی

یافته‌های کلیدی این گزارش به صورت زیر است:

حملات فیشینگ

- در سال 2016 سهم فیشینگ مالی با 13/14 واحد درصد[2] رشد به 47/48٪ از کل تشخیص‌های فیشینگ افزایش یافته است. این رقم بالا با توجه به آمار آزمایشگاه کسپرسکی برای فیشینگ مالی بر روی دستگاه‌های مبتنی بر ویندوز به دست آمده است.
- یک چهارم تلاش‌ها برای بارگزاری یک صفحه فیشینگ مسدود شده توسط محصولات آزمایشگاه کسپرسکی مربوط به فیشینگ بانکی است.
- سهم فیشینگ مربوط به سیستم‌های پرداخت و فروشگاه‌های الکترونیکی به ترتیب 11/55٪ و 10/14٪ در سال 2016 تخمین زده شده است. این نسبت، کمی (یک واحد درصد) بیشتر از سال 2015 است.
- سهم فیشینگ مالی برای کاربران Mac، 31/38٪ تخمین زده شده است.

بدافزارهای بانکی

- در سال 2016 تعداد کاربرانی که با استفاده از تروجان‌های بانکی مورد حمله قرار گرفتند با 30/55٪ افزایش به 1.088.900 کاربر رسیدند.
- 17/17٪ از کاربرانی که با بدافزار بانکی مورد حمله قرار گرفتند، کاربران شرکت‌ها بودند.
- کاربران روسیه، آلمان، ژاپن، هند، ویتنام و آمریکا بیشتر توسط بدافزار بانکی مورد حمله قرار گرفته بودند.

[2] Percentage Point

- Zbot هنوز هم شایع‌ترین دسته از بدافزارهای بانکی است (44/08٪ از کاربران را مورد حمله قرار داده است) اما در سال 2016، Gozi (17/22٪) آن را به طور جدی به چالش کشاند.

بدافزارهای بانکی اندروید

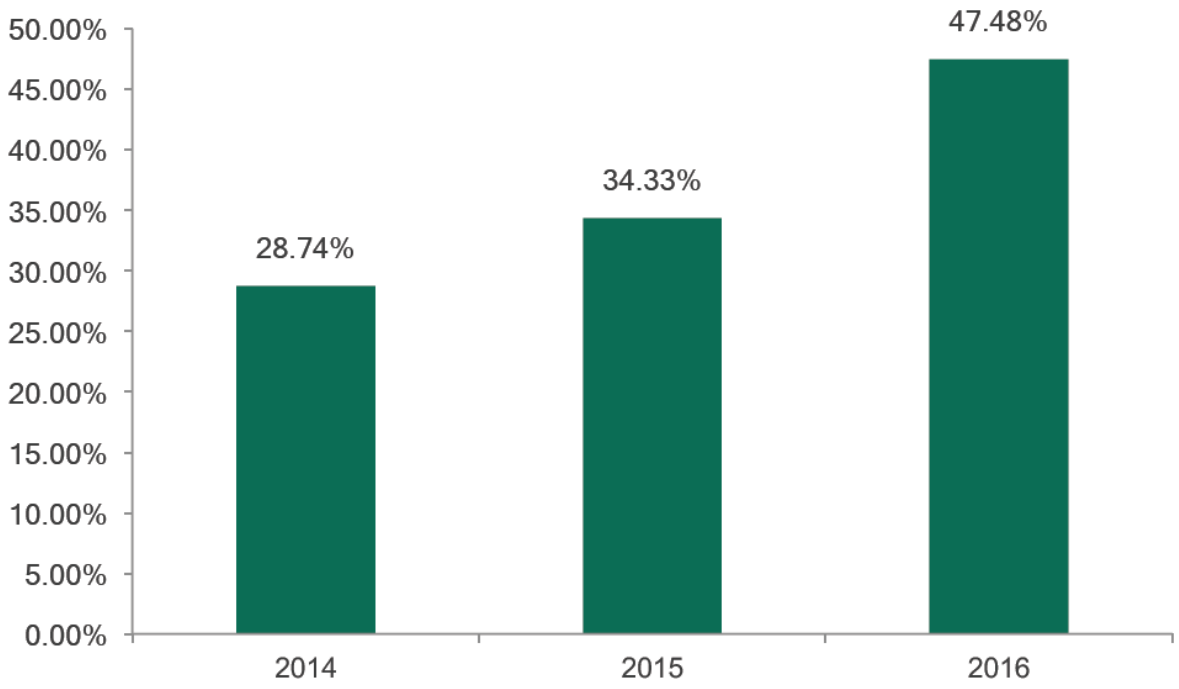
- در سال 2016 تعداد کاربرانی که با بدافزار اندروید مواجه شده بودند با 430٪ افزایش به 305.000 در سراسر جهان رسید. این مقادیر عمدتاً به دلیل تروجانی است که ماه‌ها از یک نقض امنیتی در یک مرورگر محبوب موبایل استفاده می‌کرد.
- فقط سه دسته بدافزار بانکی برای حمله به اکثر قریب به اتفاق کاربران (81٪) مورد استفاده قرار گرفته‌اند.
- روسیه، استرالیا و اوکراین کشورهایی هستند که بالاترین درصد از کاربران مورد حمله توسط بدافزارهای بانکی اندروید را دارند.

فیشینگ مالی

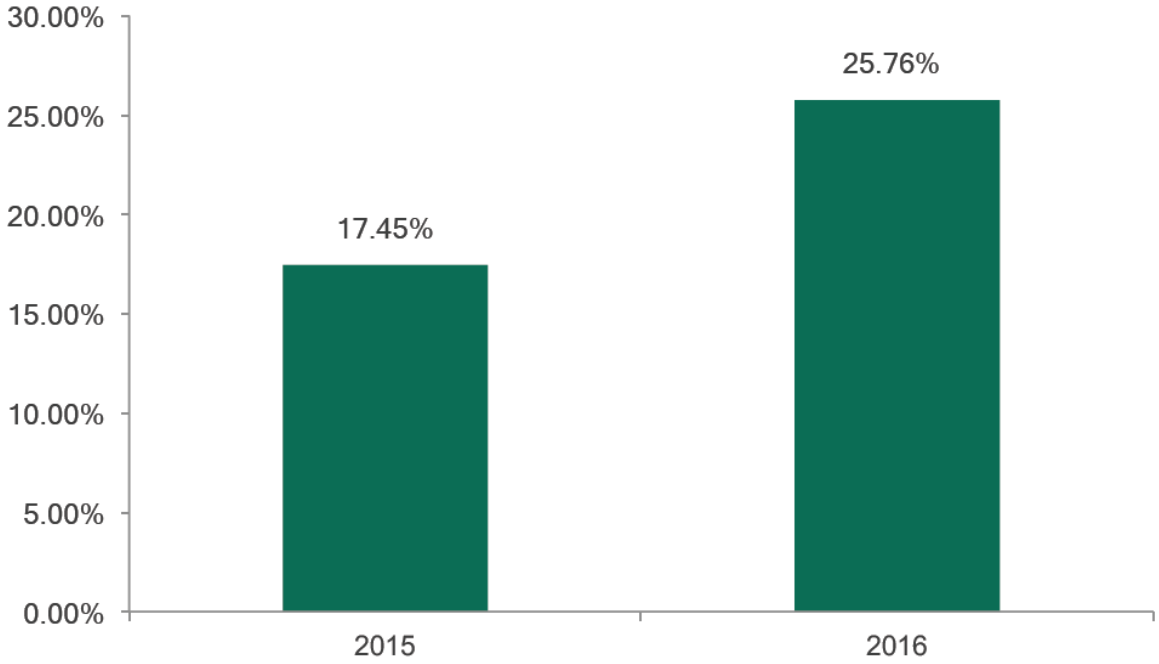
فیشینگ مالی یکی از شایع‌ترین انواع فعالیت‌های جرایم سایبری است. فیشینگ در میان انواع جرایم سایبری موجود، از لحاظ سرمایه‌گذاری و سطح تخصص فنی مورد نیاز، مقرون به صرفه‌ترین مورد است. در عین حال، در اغلب موارد به طور بالقوه سودآور است، در بیشتر موارد نتیجه‌ی یک سری اقدامات سازمان-یافته فیشینگ که موفقیت‌آمیز باشد موجب می‌گردد مجرم به اطلاعات تعداد کافی از کارت‌های اعتباری دست یابد تا بلافاصله پس از آن با خرید یا انتقال از این کارت‌ها به پول برسد یا اطلاعات این کارت‌ها را با قیمت مناسب به سایر مجرمان بفروشد. شاید تلفیق سادگی فنی و کارآیی، این نوع فعالیت مخرب را برای مجرمان مبتدی جذاب کرده است.

در سال 2016، فناوری‌های ضد فیشینگ کسپرسکی 154.957.897 تلاش را جهت بازدید انواع مختلفی از صفحات فیشینگ شناسایی کرد که 47/48٪ از این تشخیص‌های اکتشافی، تلاش برای بازدید از صفحات فیشینگ مالی بودند. این میزان، 13/14 واحد درصد بیشتر از سهم شناسایی فیشینگ‌های ثبت شده در سال

2015 است که 34/33٪ از آنها مربوط به تقلب‌های مالی است. در حال حاضر این میزان، بالاترین درصد فیشینگ مالی است که توسط آزمایشگاه کسپرسکی ثبت شده است.



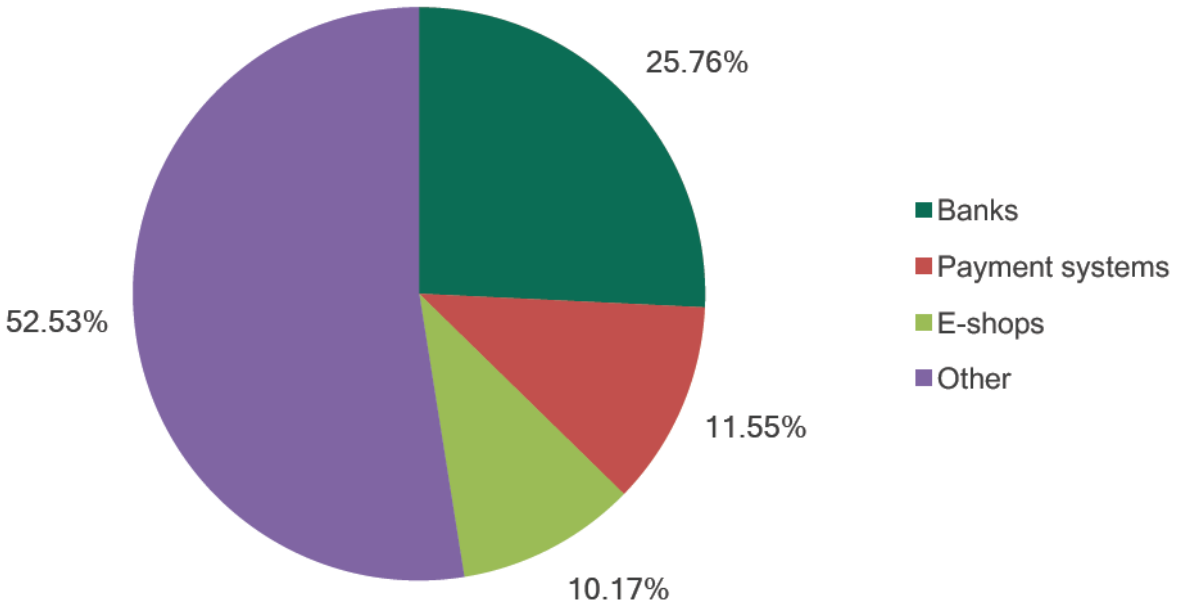
شکل 1- درصد فیشینگ مالی که توسط آزمایشگاه کسپرسکی در طی سال‌های 2014 تا 2016 شناسایی شده است.



شکل 2- درصد فیشینگ بانکی که توسط آزمایشگاه کسپرسکی در طی سال‌های 2015 تا 2016 شناسایی شده است.

علاوه بر این، برای اولین بار در سال 2016، شناسایی صفحات فیشینگ که خدمات بانکی قانونی را تقلید می‌کردند، در نمودار کلی در جایگاه اول قرار گرفت و پیشگامان قدیمی این نمودار یعنی پورتال‌های وب جهانی و شبکه‌های اجتماعی را پشت سر گذاشتند. در سال 2014 یک چهارم از صفحات فیشینگ شناسایی شده، یک صفحه بانکی آنلاین جعلی یا سایر محتوای مربوط به بانک‌ها بودند. با این حال در سال 2016، همانطور که در شکل 2 مشخص است، این درصد تشخیص 8/31 واحد درصد بیشتر از سال 2015 بوده است.

در آزمایشگاه کسپرسکی انواع مختلفی از صفحات فیشینگ به صورت "مالی" دسته‌بندی می‌شوند. علاوه بر بانک‌ها، دسته "سیستم‌های پرداخت" نیز وجود دارد که شامل صفحاتی جعلی است که از برندهای پرداخت شناخته شده مانند PayPal، Visa، MasterCard، American Express و غیره تقلید می‌کنند. همچنین دسته "فروشگاه الکترونیکی" وجود دارد که شامل فروشگاه‌های اینترنتی و مزایده‌ای مانند آمازون، فروشگاه اپل، Steam، E-Bay و غیره است.



شکل 3- توزیع انواع مختلف فیشینگ مالی که توسط آزمایشگاه کسپرسکی در سال 2016 شناسایی شده است.

در سال 2016، هر دو دسته "فروشگاه الکترونیکی" و "سیستم‌های پرداخت" رشد قابل ملاحظه‌ای را نشان دادند. در مقایسه با نتایج سال 2015، سهم حملات فیشینگ به سیستم‌های پرداخت 3/75 واحد درصد افزایش و حملات به فروشگاه‌های الکترونیکی 1/09 واحد درصد افزایش را نشان داد.

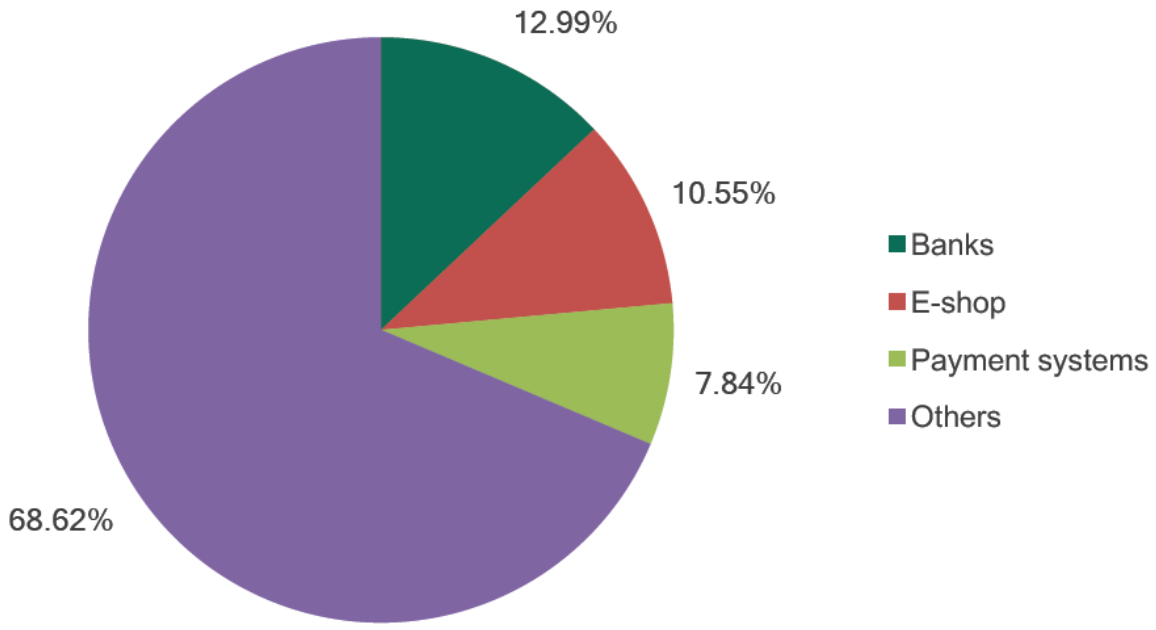
لیست اهداف فیشرها تعجب‌آور نیست. در میان اهداف مورد علاقه فیشرهای مالی، بانک‌های فراملیتی بزرگ، سیستم‌های پرداخت مرسوم و فروشگاه‌های اینترنتی و مزایده‌ای آمریکا، چین و برزیل وجود دارند. لیست این اهداف از سالی به سال دیگر پابرجا می‌ماند؛ چون محبوبیت این برندها یک هدف بزرگ و در عین حال سودآور برای مجرمان سایبری است.

فیشینگ مالی بر روی Mac

به طور کلی، کامپیوترهای مبتنی بر سیستم‌عامل Mac نسبت به ویندوز، پلت‌فرم بسیار امن‌تری را در اختیار دارند. به دلیل اینکه تعداد دسته‌های بدافزاری موجود برای این سیستم‌عامل کمتر از بدافزارهای ویندوز هستند. با این حال، متخصصان اغلب فراموش می‌کنند که تهدیدات فیشینگ اهمیتی نمی‌دهند چه سیستم-عاملی بر روی دستگاه قربانی در حال اجرا است. آمار آزمایشگاه کسپرسکی نشان می‌دهد که کاربران سیستم‌عامل Mac نه به میزان کاربران ویندوز ولی اغلب با تهدیدات فیشینگ مواجه هستند.

در سال 2016، 31/38٪ درصد از حملات فیشینگ علیه کاربران Mac به سرقت داده‌های مالی منجر شده است. این میزان بسیار کمتر از سال 2015 است که 51/46٪ از حملات مالی مسدود شده توسط آزمایشگاه کسپرسکی در حوزه مالی بودند. با این حال، وضعیت سال 2015 به دلیل حجم زیادی از شناسایی‌ها علیه یک بانک بین‌المللی تا حدودی غیرعادی بود. این مقدار آنقدر بزرگ بود که این بانک در بین برندهایی که اغلب مورد کلاهبرداری‌های فیشینگ علیه کاربران Mac قرار می‌گیرند، در رتبه اول قرار گرفت و "پیشگامان" معمول در رتبه‌بندی کلی (موتورهای جستجوی مرسوم و شبکه‌های اجتماعی) را پشت سر گذاشت.

در سال 2016 موج حملات علیه این بانک کاهش یافت و سهم کل فیشینگ مالی را به سطح واقع‌گرایانه-تری رساند. با این حال، 31/38٪ بدین معنی است که یک سوم از حملات فیشینگ مسدود شده در Macها سعی داشتند تا قربانیان را برای به اشتراک گذاشتن اطلاعات مالی‌شان وسوسه کنند. این بانک که در سال 2015 در لیست اهداف مجرمان قرار داشت، هنوز هم هدف اصلی فیشینگ بانکی است، اما تعداد حملات به آن بسیار کمتر شده است.



شکل 4- توزیع حملات فیشینگ علیه کاربران Mac در سال 2016

Mac در برابر ویندوز

بر اساس آمار شناسایی صفحات فیشینگ از کامپیوترهای مبتنی بر ویندوز، در لیست برندهایی که بیشترین استفاده از آنها شده در دسته فروشگاه الکترونیکی، آمازون پیشگام قدیمی این دسته در صدر قرار گرفته است. با این حال، هنگامی که فیشینگ بر روی مک به وقوع می‌پیوندد، پیشگام اپل است. توضیح دومی آسان است: اکوسیستم اپل شامل تعدادی خدمات وب شناخته شده و به طور کلی قابل اعتماد مانند iCloud، iTunes، AppStore و فروشگاه اپل است. مجرمان از این اعتماد مطلع هستند و سعی می‌کنند از آن سوءاستفاده کنند.

هنگامی که به دسته‌های تجارت الکترونیکی و سیستم‌های پرداخت توجه می‌کنیم مشخص می‌شود که تمرکز خاص بر روی اپل، تنها تفاوت بین چشم‌اندازهای تهدید فیشینگ مالی مک و ویندوز نیست.

Mac	Windows
Apple	Amazon.com
Amazon.com	Apple
Global Sources	Steam
Alibaba Group	eBay
eBay	Taobao
Steam	Alibaba Group
Netsuite	Bell Canada
Bell Canada	NOVA PONTOCOM
Bharti Airtel Limited	Wal-Mart

شکل 5- بیشترین برندهای استفاده شده در حقه‌های فیشینگ مالی فروشگاه الکترونیکی

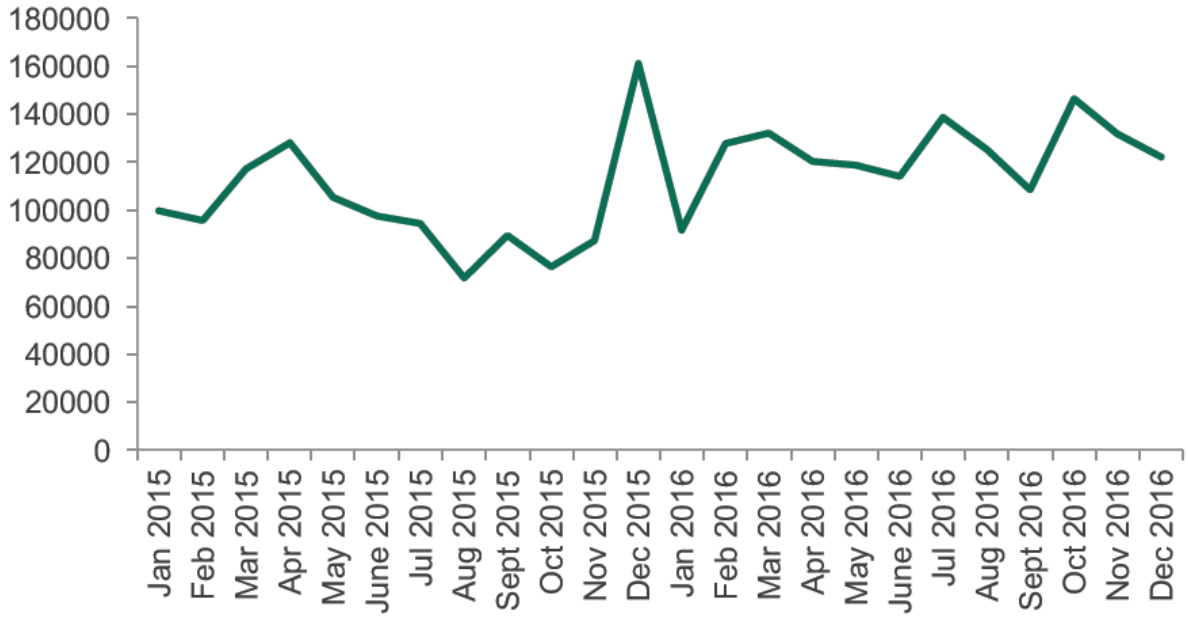
Mac	Windows
PayPal	PayPal
American Express	Visa Inc.
MasterCard	American Express
Visa Inc.	MasterCard
qiwi.ru	Western Union
Xoom	qiwi.ru
NACHA	Cielo S.A.
Skrill Ltd.	Skrill Ltd.
Western Union	eWallet

شکل 6- بیشترین برندهای استفاده شده در حقه‌های فیشینگ مالی سیستم‌های پرداخت

توضیح اینکه چرا اهدف در Macها متفاوت از ویندوز می‌باشد، واقعاً سخت است. ممکن است به دلیل تفاوت در عادت‌های کاربران ویندوز و Mac باشد یا می‌تواند فقط نتیجه توزیع کاربران محصولات کسپرسکی باشد. با این وجود، جداول فوق می‌توانند به‌عنوان یک لیست راهنما برای کاربران به کار روند که نشان می‌دهند مجرمان از این نام‌های شناخته شده برای به دست آوردن غیرقانونی کارت پرداخت کاربر، اعتبارنامه‌های بانکداری آنلاین و سیستم پرداخت استفاده خواهند کرد.

بدافزار بانکی

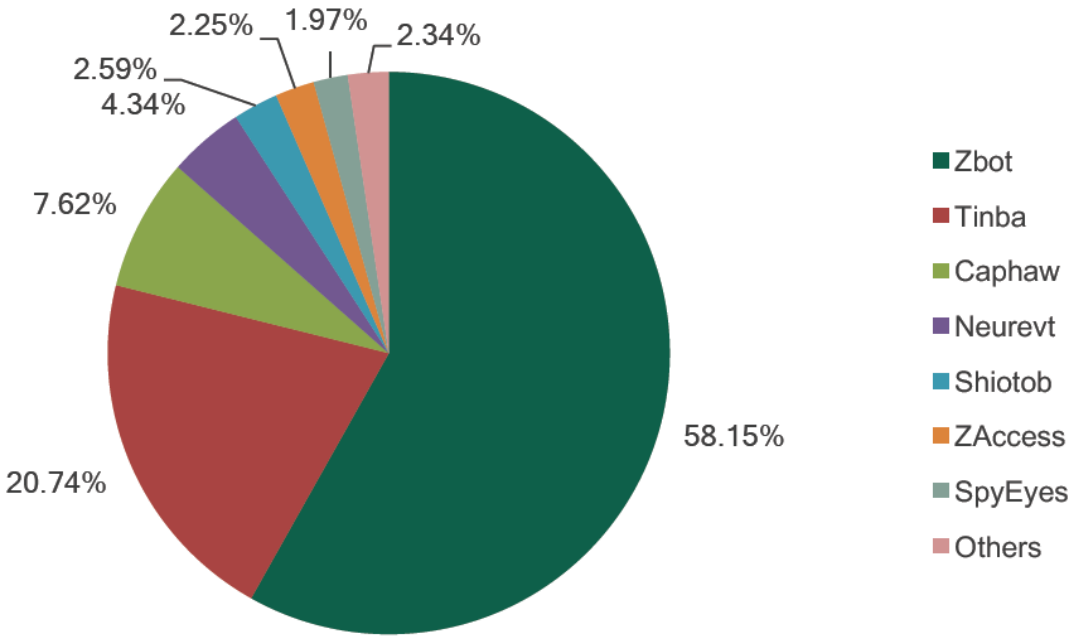
بدافزار بانکی یک نوع برنامه مخرب است که به طور خاص برای پیدا کردن و سرقت اعتبارنامه‌هایی که جهت دسترسی به حساب‌های بانکی آنلاین یا سیستم‌های پرداخت و رهگیری کدهای 2FA (رمزهای عبور یک بار مصرف) استفاده شده‌اند، به وجود آمده است. موارد دیگر در این دسته عبارتند از: نسخه‌های از keylogger که در حملات علیه بانکداری آنلاین و سیستم‌های پرداخت استفاده می‌شوند و به اصطلاح بدافزار "Hosts" یا میزبان نامیده می‌شوند. که یک نوع تروجان است که تنظیمات میزبان کامپیوتر مورد حمله را تغییر می‌دهد تا قربانی را بدون سر و صدا از یک وب‌سایت واقعی به یک وب‌سایت جعلی هدایت کند و همچنین برخی از تروجان‌های عمومی که برای اهداف مختلف از جمله سرقت اعتبارنامه‌های بانکی استفاده می‌شوند.



شکل 7- تغییر تعداد کاربرانی که با بدافزار بانکی در طی سال‌های 2015 تا 2016 مورد حمله قرار گرفته‌اند.

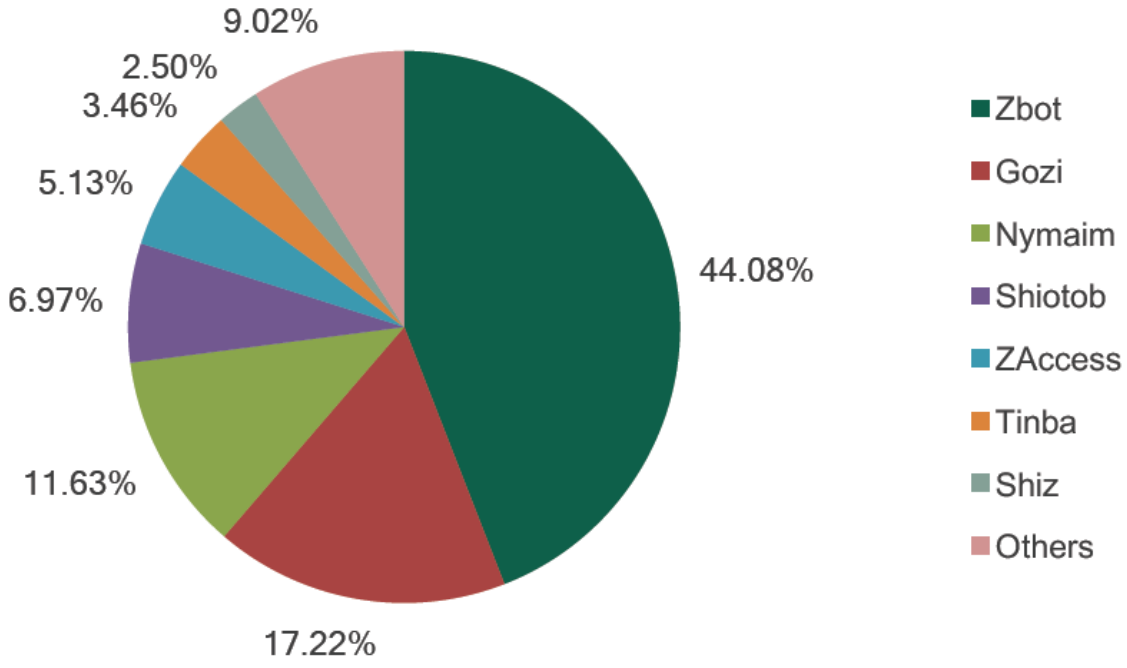
در سال 2014، تعداد کاربرانی که با هر نوع بدافزار مالی مورد حمله قرار گرفتند، کاهش قابل توجهی داشت. در سال 2015 این کاهش ادامه پیدا کرد، اما در سال 2016 تعداد کاربران مورد حمله توسط بدافزاری که داده‌های مالی را هدف قرار داد، دوباره افزایش یافت. این تغییر، تعداد کاربران مورد حمله با تروجان‌های بانکی را نیز تحت‌تأثیر قرار داد. در سال 2015 حداقل 834.099 کاربر در سراسر جهان حداقل یک بار با حمله تروجان بانکی مواجه شده‌اند. در سال 2016، تعداد این کاربران در سراسر جهان 1.088.933 نفر بود که 30/55٪ افزایش داشت. این تغییر بدین معنی است که اگرچه گروه‌های مجرمان سایبری حرفه‌ای توجه خود را به سمت حملات هدفمند علیه شرکت‌های بزرگ از جمله بانک‌ها و سازمان-های مالی دیگر تغییر می‌دهند، اما گروه‌های کوچکتری از مجرمان با کمک بدافزارهای نسبتاً گسترده‌ای که در وب باز در دسترس هستند، قربانیان را هدف قرار می‌دهند.

در آزمایشگاه کسپرسکی حدود 30 دسته از بدافزارهای بانکی ردیابی شده است، اما تنها تعداد کمی از این بدافزارها چشم‌انداز فعلی تهدیدات بانکی را شکل می‌دهند. در ادامه، لیست هفت دسته از فعال‌ترین بدافزارهای بانکی آمده است که در سال 2015 شامل Zbot، Tinba، Caphaw، Neurevt، Shiotob، ZAccess و SpyEye بودند.



شکل 8- توزیع شایع‌ترین دسته‌های بدافزار بانکی در سال 2015

در سال 2016 وضعیت، کمی متفاوت بود. در حالیکه Zbot پیشگامی خود را حفظ کرده بود، Gozi دسته‌ای از تروجان‌های بانکی که در سال 2016 بسیار فعال بود، به طور جدی آن را به چالش کشاند. در همان زمان، Tinba چندین جایگاه را از دست داد و از رتبه دوم خود در سال 2015 به ششم در سال 2016 رسید.

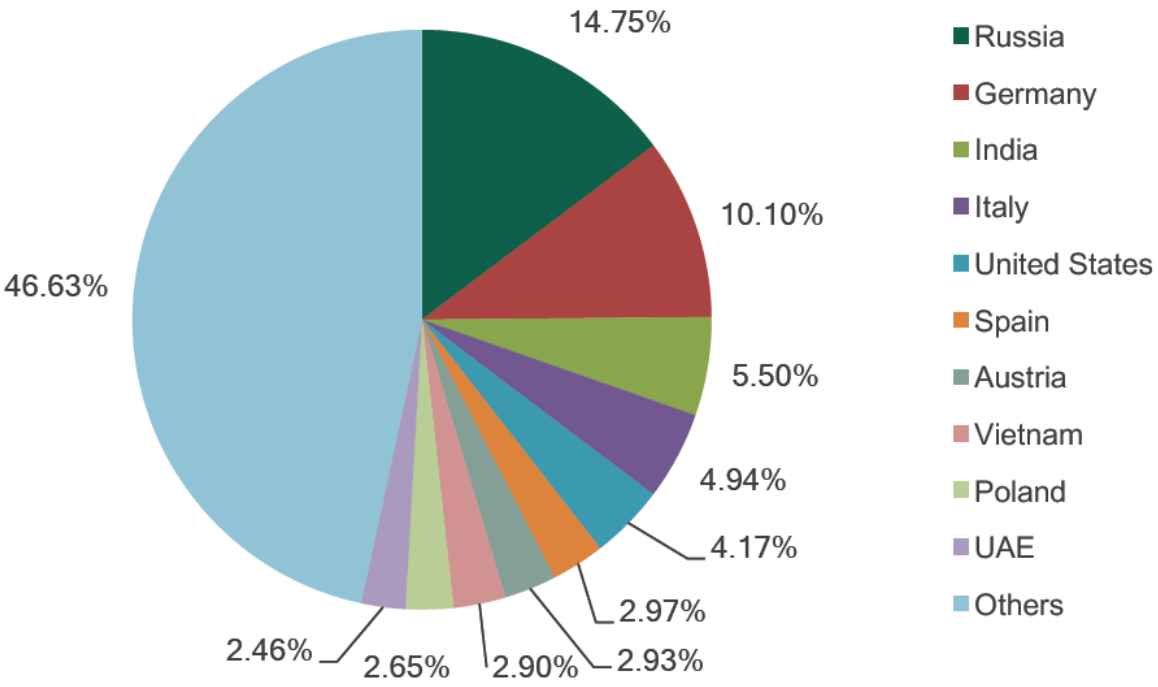


شکل 9- توزیع شایع‌ترین دسته‌های بدافزار بانکی در سال 2016

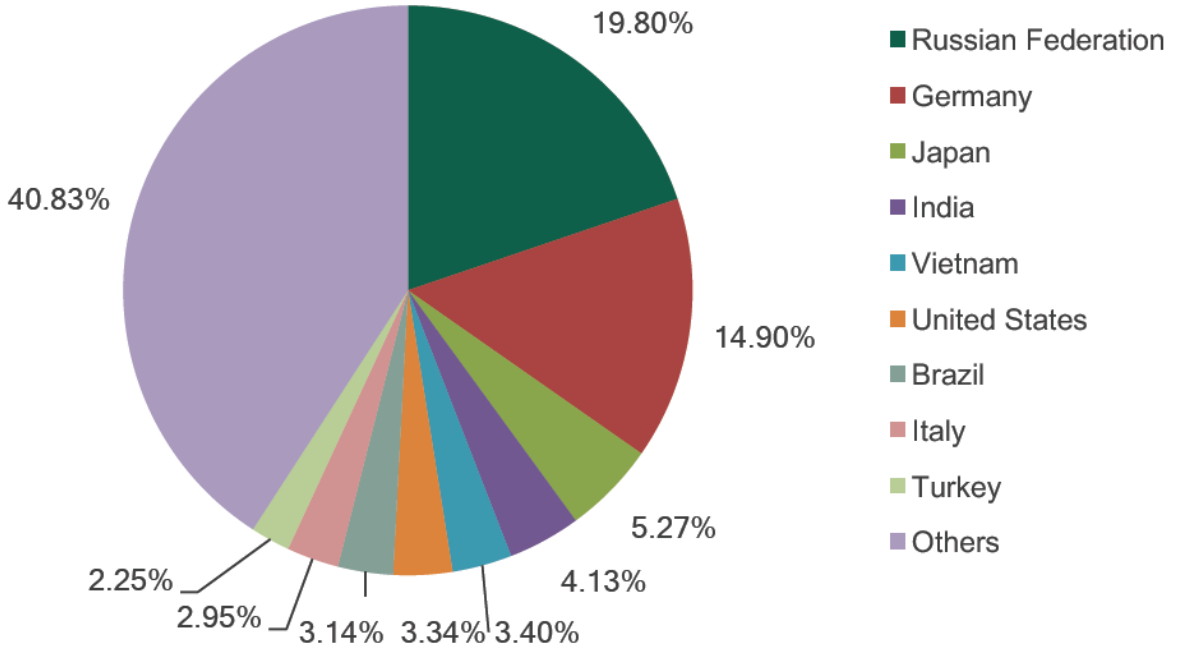
جغرافیای کاربران مورد حمله

همانطور که در شکل‌های 10 و 11 دیده می‌شود، بیش از نیمی از کاربران مورد حمله با بدافزار بانکی در طی سال‌های 2015 و 2016 تنها در 10 کشور قرار داشتند و در سال 2016 سهم 10 کشور برتر 5/6 واحد درصد افزایش یافت.

10 کشور بالای لیست کشورهای مورد حمله تغییر کرده‌اند. در سال 2016 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 5/5 و 4/8 واحد درصد افزایش یافت، در حالیکه درصد کاربران آمریکا، ایتالیا و هند کاهش یافته است.



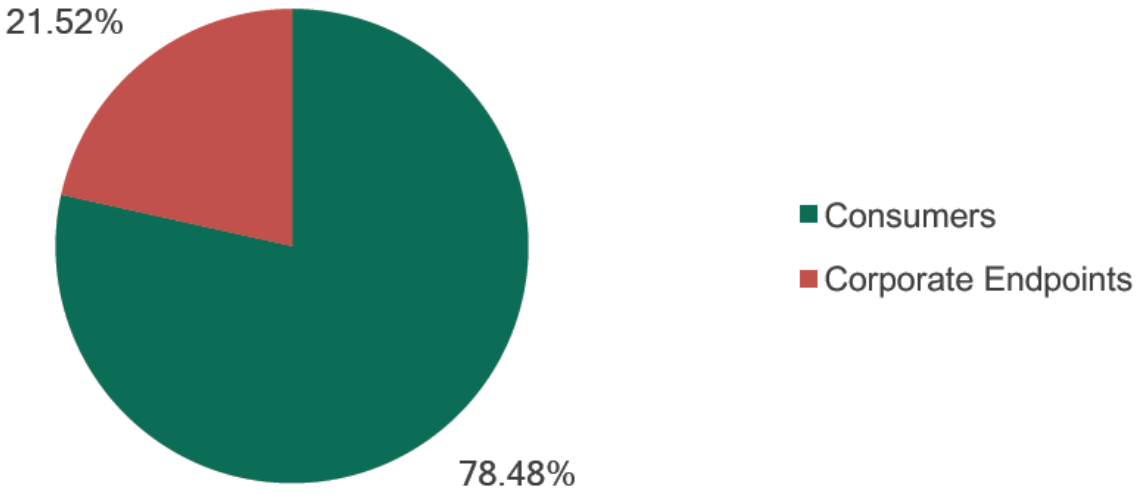
شکل 10- توزیع جغرافیایی کاربران مورد حمله با بدافزار بانکی در سال 2015



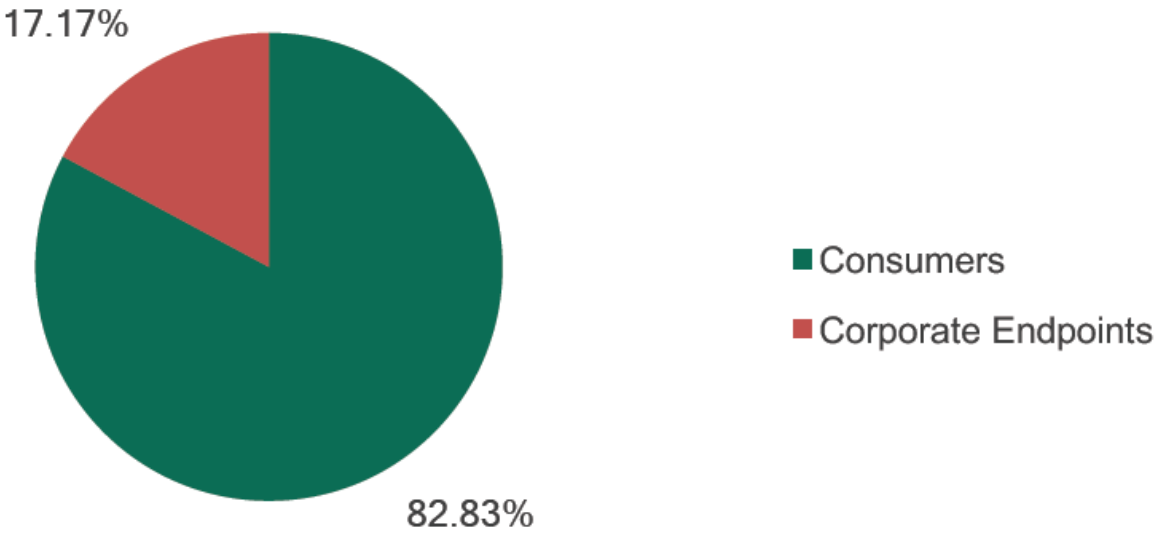
شکل 11- توزیع جغرافیایی کاربران مورد حمله با بدافزار بانکی در سال 2016

نوع کاربران مورد حمله

اگرچه اکثر بدافزارهای بانکی (به استثنای تروجان‌های POS و ATM) معمولاً کاربران خصوصی را هدف قرار می‌دهند، اما براساس آمار، همواره این طور نیست.



شکل 12- توزیع کاربران مورد حمله بر اساس نوع در سال 2015



شکل 13- توزیع کاربران مورد حمله بر اساس نوع در سال 2016

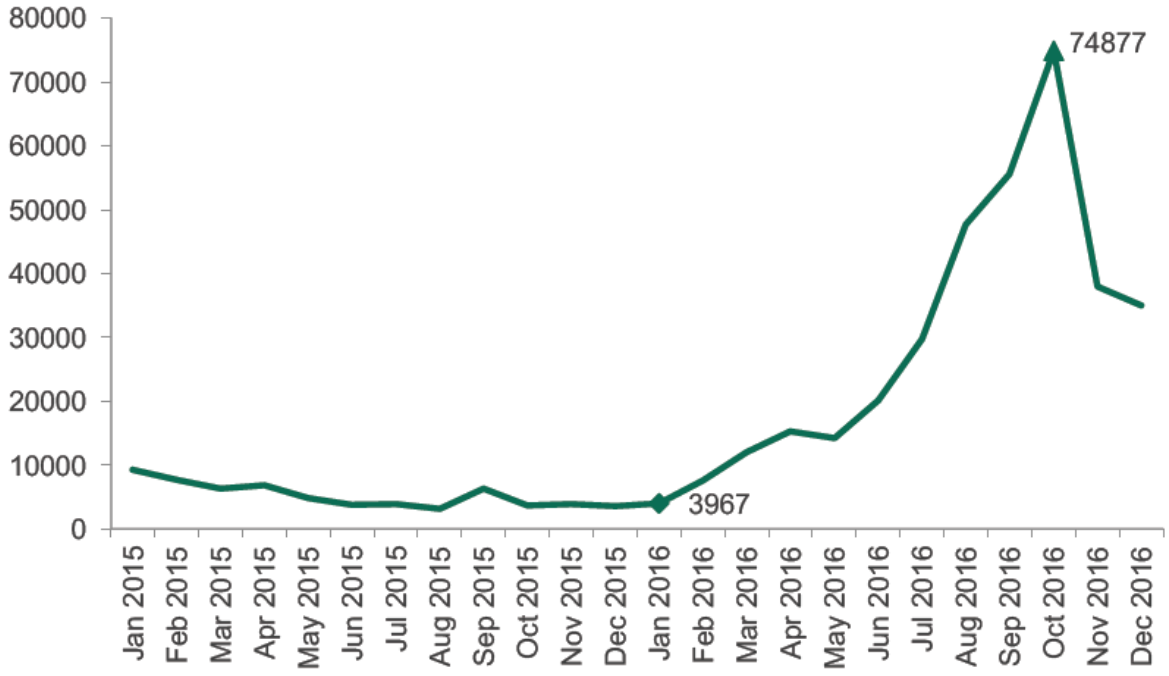
در سال 2015، 21/52٪ از کاربران مورد حمله با بدافزار بانکی، کاربران شرکت‌ها بودند. در سال 2016 سهم این کاربران به 17/17٪ کاهش یافت، اما تعداد واقعی اهداف با 4/16٪ افزایش از 179.494 در سال 2015 به 186.965 در سال 2016 رسید.

شاید سخت باشد که بگوییم اگر سهم کاربران مورد حمله با بدافزار بانکی روندی رو به کاهش داشته است، این روند ادامه خواهد داشت، اما حداقل یک نتیجه‌گیری قابل اطمینان وجود دارد: به مدت دو سال به طور مداوم، تقریباً یک پنجم کاربران مورد حمله با بدافزارهای بانکی، کاربر شرکت‌ها بودند. دست کم گرفتن خطر چنین حملاتی دشوار است: در یک حمله موفقیت‌آمیز به یک کاربر خصوصی، مجرم به سیستم بانکداری خصوصی یا سیستم پرداخت او دسترسی پیدا خواهد کرد. اگر چنین حمله‌ای به کارمند یک شرکت موفقیت‌آمیز باشد، نه تنها حساب شخصی کارمند، بلکه دارایی‌های مالی شرکتی که برای آن کار می‌کند نیز در معرض خطر است.

بدافزارهای بانکی اندروید

بدافزارهای بانکی اندروید چند سال پیش چشمگیر بود اما در چند سال گذشته تعداد کاربران مورد حمله با تروجان‌های بانکی نسبتاً کم شده است. به‌عنوان مثال، در یکی از بررسی‌های صورت گرفته توسط آزمایشگاه کسپرسکی در سال 2014 حملاتی با استفاده از بدافزارهای مالی به حدود 800.000 کاربر در سراسر جهان ثبت شد. اما بیشتر این کاربران توسط تروجان‌های پیامکی[۳] مورد حمله قرار گرفتند و فقط حدود 60.000 کاربر با استفاده از تروجان‌های بانکی مورد حمله قرار گرفته بودند. در آن زمان، در سال 2014، استفاده از تروجان‌های پیامکی از متداول‌ترین انواع تقلب‌های مالی موبایل و تهدید مالی اصلی برای کاربران اندروید بود.

در طول سال 2015، تعداد کاربران مورد حمله توسط تروجان‌های بانکی اندروید حتی کمتر از سال 2014 بود؛ 57.607 کاربر در 12 ماه. اما پس از آن اتفاقی غیرعادی رخ داد.



[3] SMS Trojans

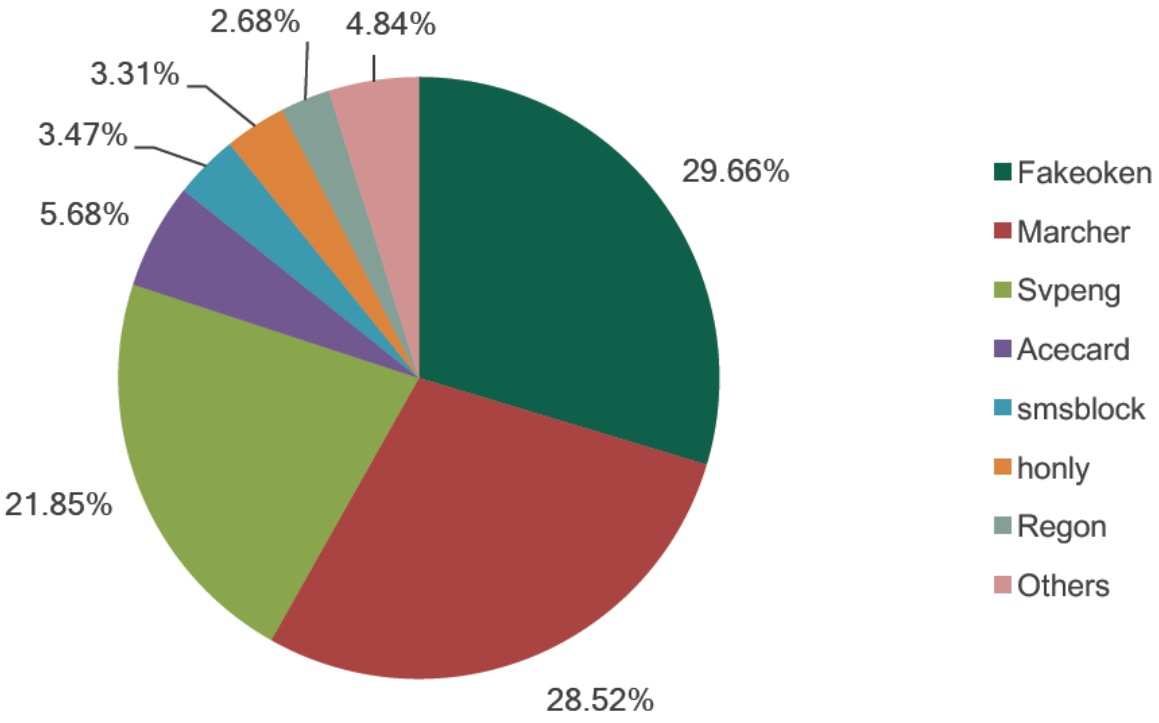
شکل 14- تغییر تعداد کاربرانی که با بدافزارهای بانکی اندروید در طی سال‌های 2015 تا 2016 مورد حمله قرار گرفته‌اند.

این چیزی است که اتفاق افتاده است: به سرعت، تعداد کاربران مورد حمله ماه به ماه از 3.967 کاربر در ژانویه 2016 تا نزدیک به 75.000 کاربر در اکتبر 2016 شروع به رشد کرد.

در مجموع، در سال 2016 بیش از 305.000 کاربر با بدافزارهای مالی مورد حمله قرار گرفتند که 5/3 برابر یا 430٪ بیشتر از سال 2015 است.

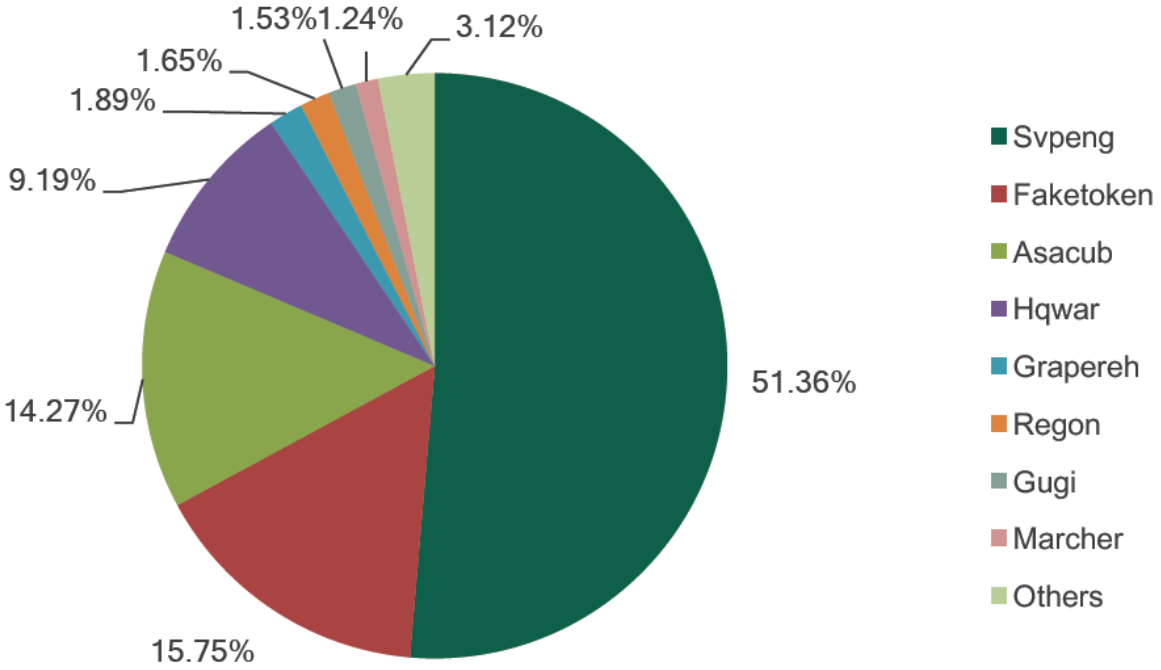
البته محققان آزمایشگاه کسپرسکی به محض اینکه تعداد کاربران مورد حمله شروع به رشد کردند، در مورد علت این افزایش ناگهانی به تحقیق پرداختند که مشخص شد تنها دو دسته از بدافزارها عامل این تغییر عمده هستند. اولین مورد Asacub بود که به طور جدی از ابتدای سال از طریق SMS توزیع شد. مورد دوم Svpeng یک تروجان شناخته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

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 14 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.

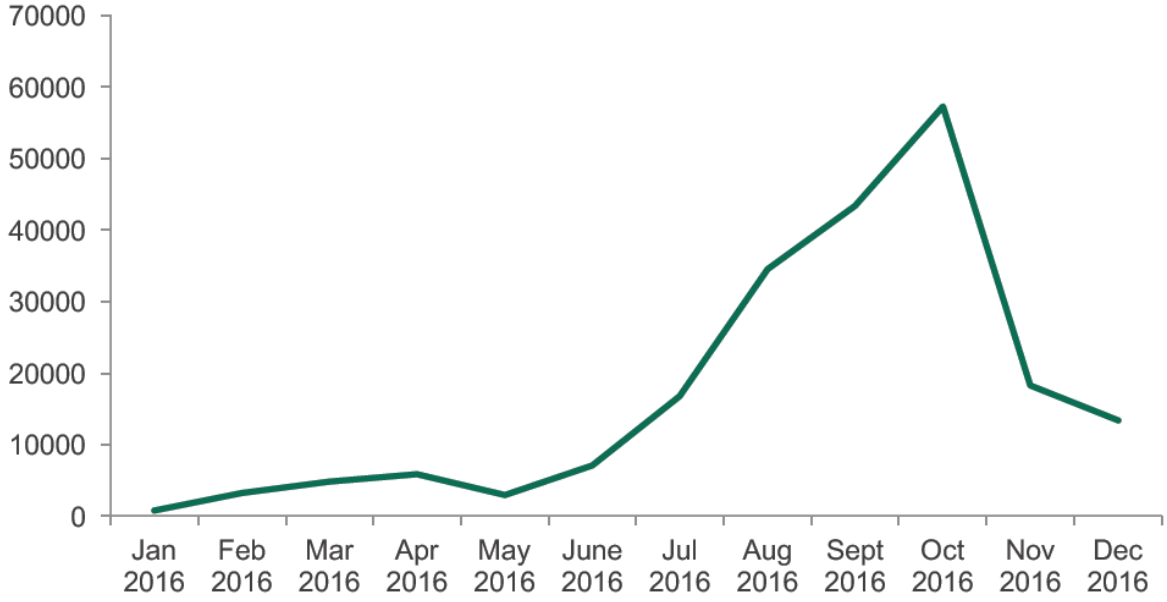


شکل 15- شایع‌ترین بدافزارهای بانکی اندروید در سال 2015

در سال 2016 نمودار کاملاً تفاوت داشت. در این سال، بیش از نیمی از کاربرانی که با تروجان بانکی اندروید برخورد پیدا کردند با Svpeng مواجه شدند. توجه داشته باشید که این دسته بدافزار تنها دسته‌ای نیست که روش توزیع خود را بهبود داده، در نتیجه نسبت به قبل به کاربران بسیار بیشتری آسیب وارد کرده است.

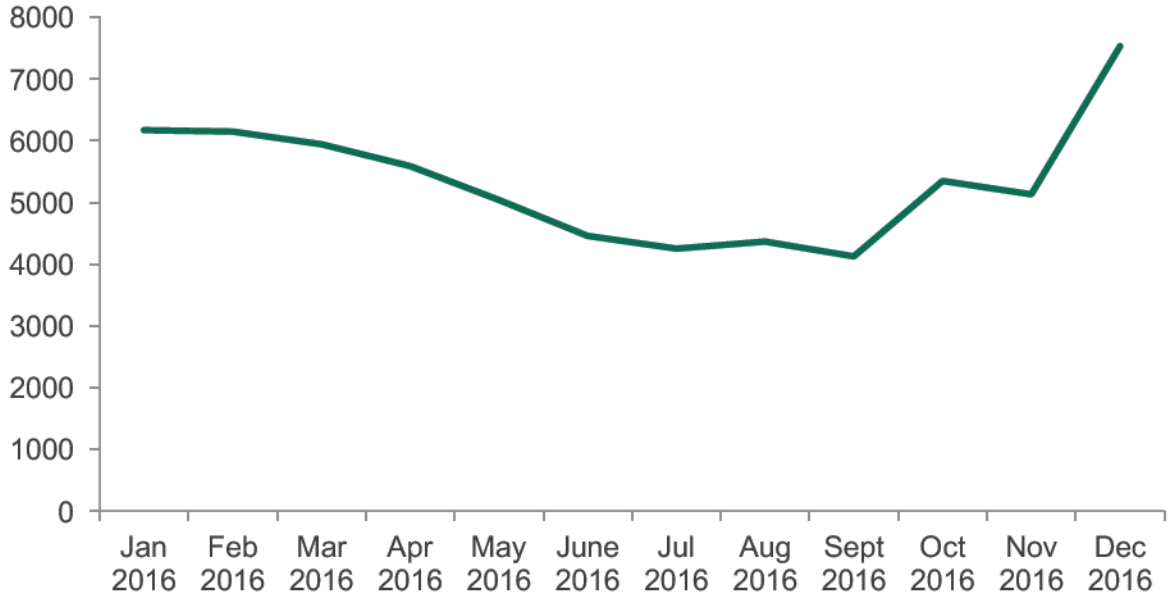


شکل 16- شایع‌ترین بدافزارهای بانکی اندروید در سال 2016

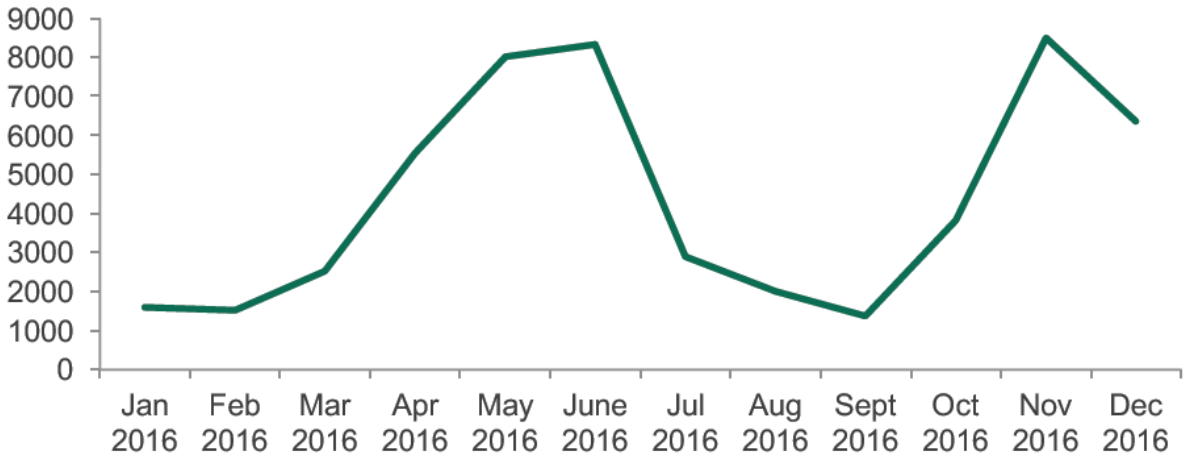


شکل 17- تغییر تعداد کاربران مورد حمله توسط تروجان بانکی اندروید Svpeng

مجرمان برای دسته Faketoken (پیشگام سال 2015) برخی از کارهای تبلیغاتی را نیز انجام دادند که نتیجه آن افزایش تقریباً سه برابری (2/9 برابری) تعداد کاربران مورد حمله از 18.700 در سال 2015 به 54.400 کاربر در سال 2016 بود. تروجان‌هایی از این دسته به صورت اپلیکیشن‌های رایگان مفید جاسازی شده و از طریق چند وب‌سایت مخرب توزیع شده‌اند.



شکل 18- تغییر تعداد کاربران مورد حمله توسط بدافزار بانکی اندروید Faketoken

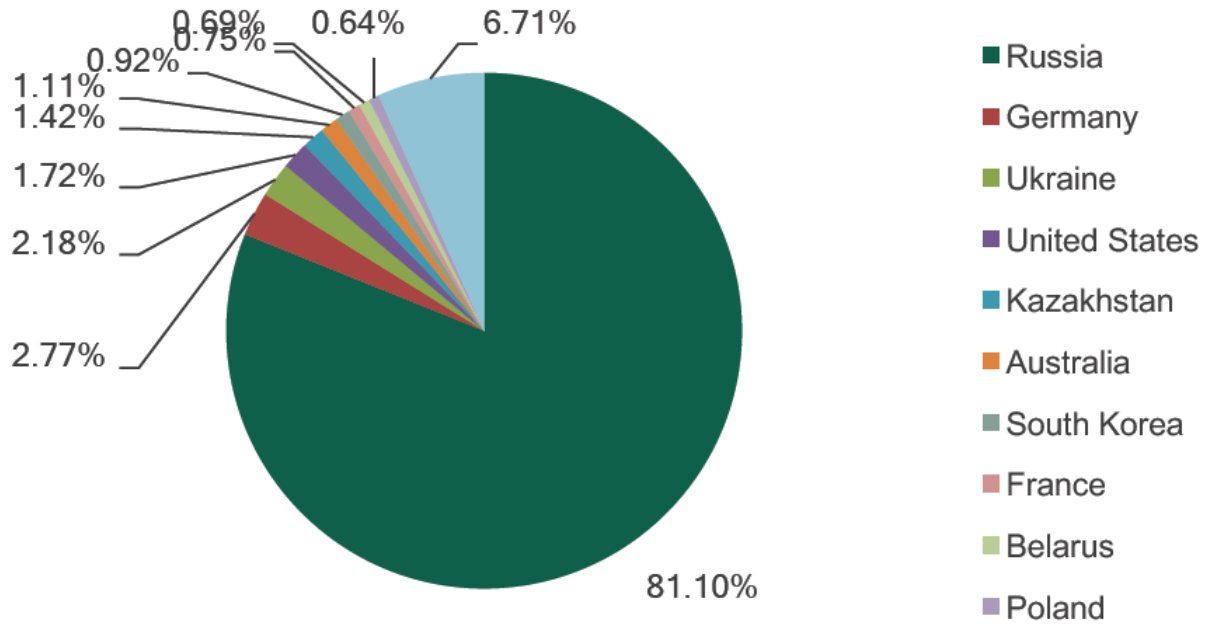


شکل 19- تغییر تعداد کاربران مورد حمله توسط بدافزار بانکی Asacub

هکرهای پشتیبان Asacub، یکی دیگر از اعضای تروجان‌های بانکی اندروید برتر در سال 2016، 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 19 قابل مشاهده است.

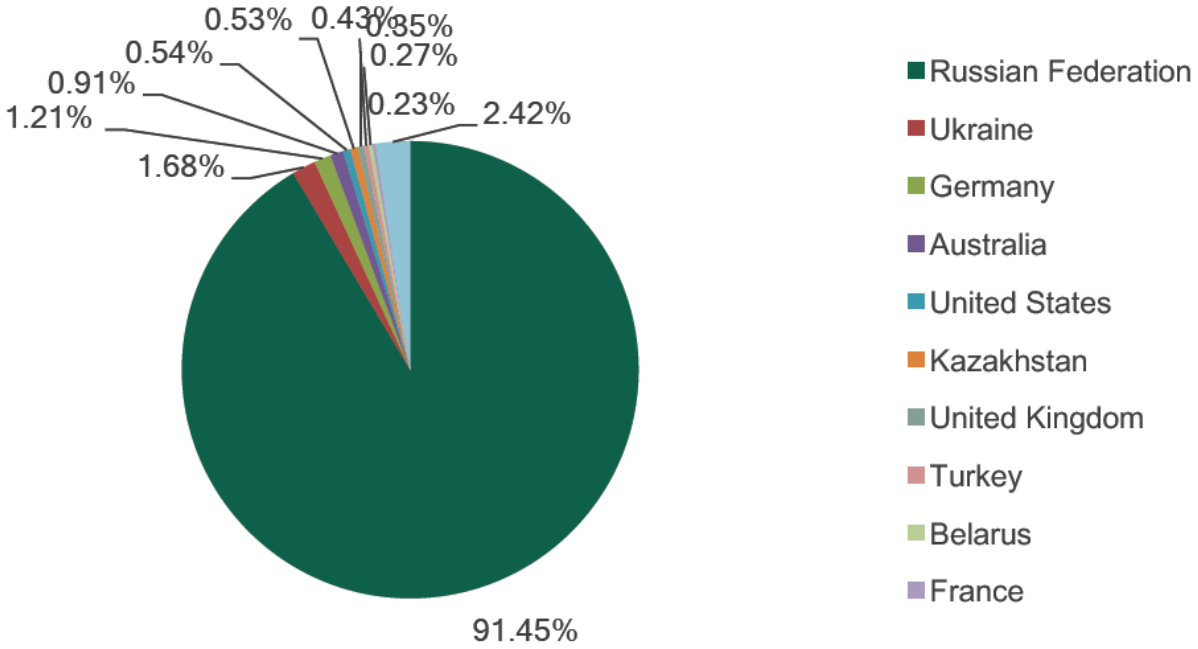
جغرافیای کاربران مورد حمله

جغرافیای حملات نیز در سال 2016 نسبت به سال 2015 تغییر نمود.

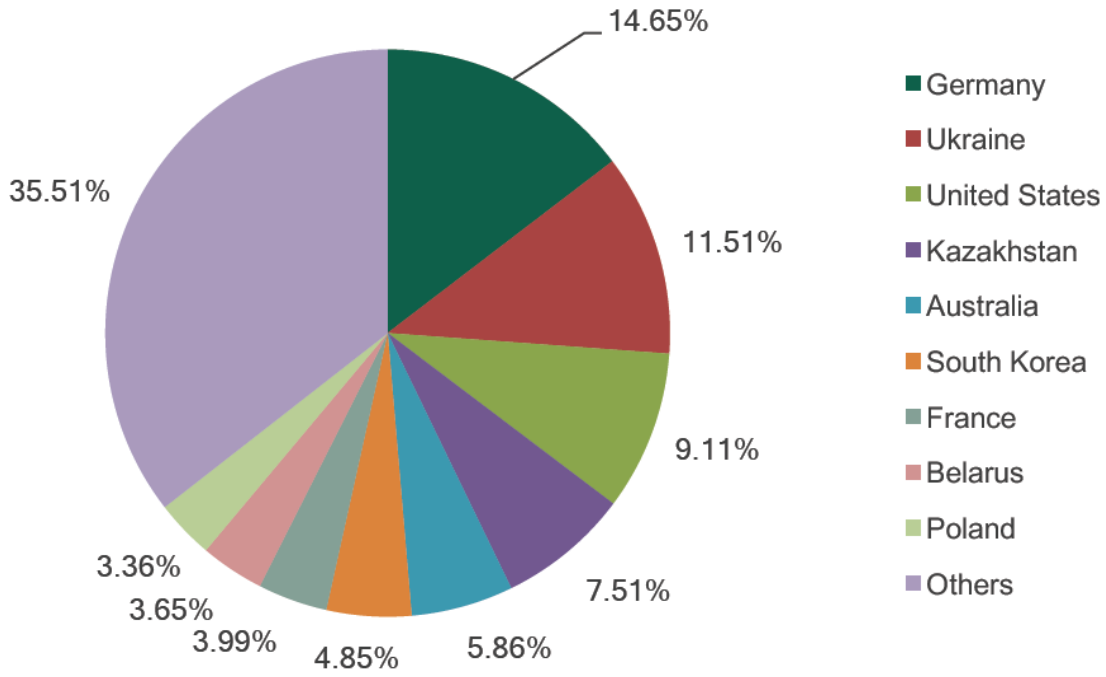


شکل 20- توزیع کاربران مورد حمله توسط تروجان‌های بانکی اندروید در سال 2015

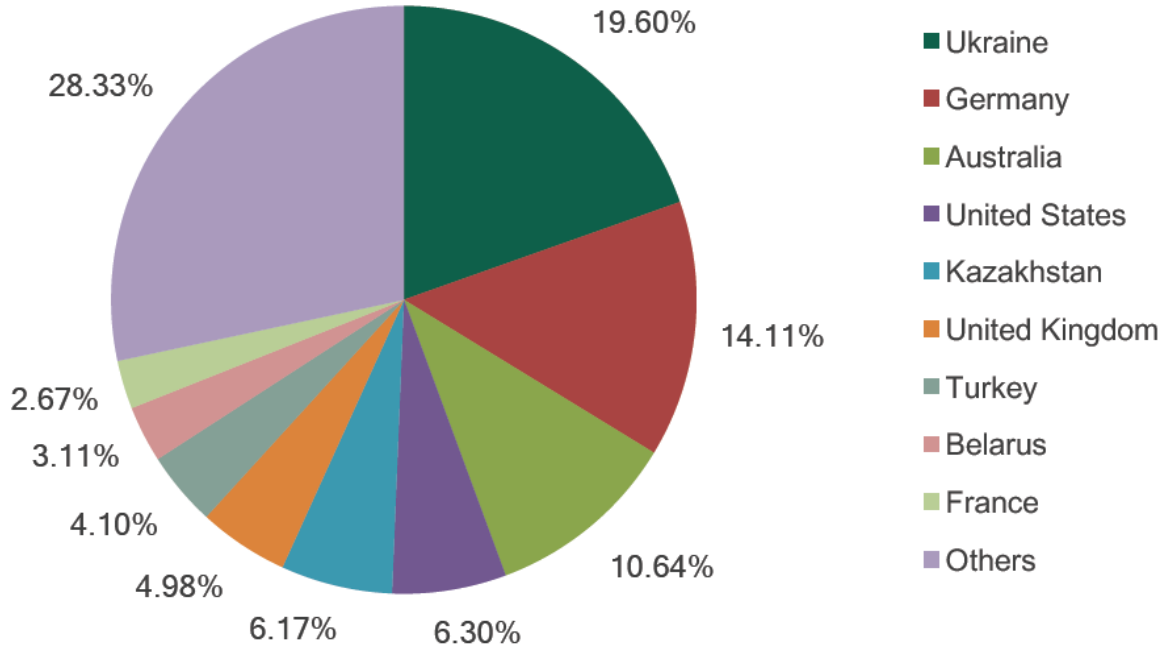
همانطور که در شکل‌های 20 و 21 دیده می‌شود، بدافزار بانکی اندروید عمدتاً در روسیه یک معضل است. لازم به ذکر است که این یافته‌ها تحت‌تأثیر توزیع عمومی کاربران محصولات آزمایشگاه کسپرسکی قرار دارد چون بسیاری از آنها در روسیه حضور دارند همچنین بدافزار Svpeng که از یک آسیب‌پذیری در یک مرورگر استفاده کرده که 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 شکل22 و 23 به تصویر کشیده شده است.



شکل 21- توزیع کاربران مورد حمله با تروجان‌های بانکی اندروید در سال 2016



شکل 22- توزیع کاربران مورد حمله با بدافزارهای بانکی اندروید در سال 2015 (در مجموع 10.887 کاربر، با حذف روسیه)



شکل 23- توزیع کاربران مورد حمله با بدافزارهای بانکی اندروید در سال 2016 (در مجموع 26.110 کاربر، با حذف روسیه)

جایگاه آلمان و اوکراین در رتبه‌بندی سال 2016 در مقایسه با سال 2015 عوض شده است. در حالی که سهم کاربران مورد حمله با بدافزارهای بانکی اندروید در اوکراین، تقریبا دو برابر شده، سهم کاربران آلمانی تقریباً یکسان باقی مانده است. در سال 2016 استرالیا نیز در بین سه کشوری که بیشترین حمله را داشتند (به استثنای روسیه) قرار گرفت و آمریکا نیز دیگر جزو سه کشور بالای لیست نیست.

در صورتی که به تعداد کاربران مورد حمله نگاه کنیم، مشاهده می‌شود که در هر جایی از دنیا به جز روسیه، معضل بدافزارهای بانکی اندروید بزرگترین مشکل نیست. در اغلب کشورها، این‌ها به ندرت از دو هزار کاربر تجاوز می‌کنند.

اگر به درصد کاربران مورد حمله در تصاویر مشابه نگاه کنیم، معیارها نشان می‌دهند که چند درصد از کل کاربران در یک کشور خاص با بدافزارهای بانکی مواجه شده‌اند. در سال 2016، 1/57٪ از کاربران محصولات آزمایشگاه کسپرسکی حداقل یک بار با یک تروجان بانکی روبه‌رو شده‌اند.

Russia	4.01%
Australia	2.26%
Ukraine	1.05%
Uzbekistan	0.70%
Tajikistan	0.65%

South Korea	0.59%
Kazakhstan	0.57%
China	0.54%
Belarus	0.47%
Moldova	0.39%

شکل 24- 10 کشور صدرنشین با بیشترین درصد از کاربرانی که با بدافزارهای بانکی اندروید در سال 2016 مواجه شده‌اند.

همانطور که در جدول بالا دیده می‌شود، حتی با وجود آنکه تعداد واقعی کاربران مورد حمله در اوکراین و استرالیا با روسیه غیرقابل مقایسه هستند، اما همین درصد نشان می‌دهد علاوه بر کاربران روسی، صاحبان گوشی‌های هوشمند اندرویدی در استرالیا و اوکراین نیز باید مطلع باشند که احتمال مواجهه آنها با بدافزارهای بانکی بیشتر از سایر کشورها است.

نتیجه‌گیری و توصیه

در سال‌های اخیر، صنعت مالی (بانک‌ها، سیستم‌های پرداخت و شرکت‌های تجارت الکترونیک) به سختی فعالیت می‌کنند تا تراکنش‌های مالی آنلاین را امن‌تر کنند. احراز هویت چندعاملی به طور گسترده مورد قبول قرار گرفته است و امنیت وب‌سایت‌ها برای کار با داده‌های مالی بسیار توسعه یافته است. سازمان‌ها نیز در اطلاع‌رسانی به مشتریان خود درباره خطرات سایبری مالی بسیار کار کرده‌اند و در حال حاضر محصولات امنیتی را به‌عنوان بخشی از خدمات بانکداری آنلاین خود ارائه می‌دهند. اما هنوز هم موارد زیادی برای تقلب‌های مالی شامل فیشینگ و بدافزارهای بانکی خاص در این حوزه وجود دارد. به منظور پیشگیری از خطر از دست دادن پول در نتیجه‌ی حمله سایبری موارد زیر توصیه می‌شود:

برای کاربران خانگی

- هرگز بر روی لینک‌هایی که توسط افراد ناشناس به شما ارسال می‌شوند، کلیک نکنید و یا لینک‌های 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 صورتی که 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[4] که از آن برای تکمیل 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.

[4] Endpoints

- 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 صورتی که 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.