باسمه تعالی

مروری بر تهدیدات مالی سایبری

بر اساس گزارش شرکت امنیتی Symantec

فهرست مطالب

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

۱- چکیده اجرایی

تهدیدات مالی هنوز برای مجرمین سایبری سودآور بوده و بنابراین این تهدیدات بخش ثابتی از گستره تهدیدات سایبری محسوب می‌شوند. مجرمین از مسیرهای حمله مختلفی، از تروجان‌های مالی که برای حمله به بانکداری آنلاین استفاده می‌شود گرفته تا حملات به ATMها و تراکنش‌های جعلی بین بانکی استفاده می‌کنند.

همانطور که در سال ۲۰۱۵ پیش‌بینی شده بود، در سال ۲۰۱۶ حملات بر علیه شرکت‌ها و مؤسسات مالی افزایش داشت. این مسئله در مجموعه‌ای از دزدی‌ها با ارزش قیمتی بالا که مشتریان جامعه جهانی ارتباطات مالی بین بانکی (SWIFT) را هدف گرفته بود مشخص شد. به طور متوسط ۳۸ درصد از تهدیدات مالی که در سال ۲۰۱۶ توسط Symantec کشف شد در مکان‌های تجاری بزرگ بودند. بیشتر این تلاش‌ها، حملات هدفمند نبودند بلکه با کمپین‌های ایمیلی گسترده انجام می‌شدند.

اگرچه تشخیص تعداد بدافزارهای مالی در سال ۲۰۱۶، ۳۶ درصد کاهش داشت، اما این کاهش بیشتر به دلیل تشخیص زودتر در زنجیره حمله و حملات متمرکزتر بوده است. فضای تهدیدات مالی با بیش از ۱/۲ میلیون تشخیص سالیانه، هنوز ۲/۵ برابر بزرگتر از باج‌افزار است. برای مثال، تعداد تشخیص‌های Ramnit تقریباً با همه تشخیص‌های باج‌افزار برابری می‌کند. صحنه تهدیدات تروجان‌های مالی در سلطه سه خانواده از بدافزارهاست: Ramnit، Bebloh و Zeus. این سه خانواده مسئول ۸۶ درصد کل حملات تروجان مالی در سال ۲۰۱۶ بوده‌اند. اما به دلیل دستگیری‌ها، فروپاشی‌ها و گروه‌بندی مجدد، شاهد نوسانات زیادی در سال گذشته بوده‌ایم. برای مثال، بعد از فروپاشی شبکه Avalanche در سال ۲۰۱۷، Bebloh تقریباً از بین رفت. گونه‌های جدید زیادی از این خانواده‌ها ظاهر شدند که روی بخش‌های خاصی تمرکز می‌کردند. این مهاجمین بیشتر از کلاهبرداری کمپین‌های ایمیلی با تنوع کم و پیوست‌های ساده استفاده می‌کنند. برای مثال ۵۵۰۰۰ تشخیص در سال ۲۰۱۶ فقط مربوط به یک نمونه از Bebloh بودند.

ژاپن تمرکز اصلی تروجان‌های مالی Bebloh و Snifula در سال ۲۰۱۶ بوده است و بیش از ۹۰ درصد فعالیت آنها در این کشور متمرکز بوده است. روشن نیست که چرا این دو تهدید توجه خود را به این سمت تغییر داده‌اند اما نشانه‌هایی وجود دارد که آنها از یک منبع مشترک برای حمله به اهداف مشابه استفاده

می‌کنند. در مقیاس جهانی، با توجه به نمونه‌های تحلیل شده توسط Symantec، مؤسسات مالی در ایالات متحده، لهستان و ژاپن بیشتر از بقیه مورد هدف قرار گرفته‌اند.

روندهایی در بدافزارهای مالی مشاهده شد که به دنبال پنهان کردن فایل‌های پیکربندی از محققین بوده‌اند و همچنین روندهایی که به حملات تغییر مسیر روی آورده‌اند یا حتی به‌صورت دستی به سیستم وارد شده تا در صورت تشخیص نرم‌افزار مالی مورد علاقه‌شان، تراکنش‌های بزرگ را منتشر کنند.

با وجود اینکه Symantec و سایر تحقیق‌کنندگان، با تمرکز روی خانواده‌های تهدیدات خاص، تحقیقات متعددی منتشر کرده‌اند، این گزارش به صورت مفصل‌تر در مورد تغییرات کلی تهدیدات مالی سایبری بحث خواهد کرد.

۲- یافته‌های کلیدی

- جرایم سایبری در سال ۲۰۱۶ قربانی‌های سطح بالا و دستاوردهای مالی بی‌سابقه‌ای داشته‌اند. حملات Lazarus که در سال ۲۰۱۶ رخ دادند اولین نشانه‌های محکم از دست داشتن دولت در جرایم سایبری مالی بودند.
- Ramnit فعال‌ترین تروجان مالی در سال ۲۰۱۶ بود که ۳۸ درصد فعالیت در این عرصه را به خود اختصاص داده بود، Bebloh (۲۵ درصد) و Zeus (۲۳ درصد) در جایگاه‌های بعدی قرار داشتند.
- ۸۶ درصد کل حملات تهدید مالی توسط سه خانواده از تهدیدات انجام شده‌اند.
- ژاپن، چین و هند به ترتیب بیشترین آلودگی را داشتند.
- بر اساس نمونه‌های تحلیل شده توسط Symantec، مؤسسات مالی در ایالات متحده، لهستان و ژاپن به ترتیب بیشتر از بقیه مورد هدف حملات بوده‌اند.
- در سال ۲۰۱۶ تعداد تشخیص‌های تروجان‌های مالی ۳۶ درصد کاهش داشت (۷۳ درصد در سال ۲۰۱۵).
- تولیدکنندگان بدافزار با مبهم‌سازی[۱] لیست URLهای بانک‌های مورد حمله، استخراج آمار دقیق همه خانواده‌های تهدید را غیرممکن کرده‌اند.

[۱] obfuscating

- حملات تغییر مسیر به سایت‌های جعلی دوباره افزایش یافته است.
- نرخ فیشینگ در مارس ۲۰۱۷ به ۱ در هر ۹۱۳۸ ایمیل کاهش یافت.
- استفاده از گواهی‌های SSL معتبر سلف‌سرویس رایگان روی سایت‌های خرابکار افزایش یافت.
- بدافزارهای بانکی موبایل به حداقل ۱۷۰ اپلیکیشن برای سرقت اطلاعات ورود، حمله کردند.
- گروه‌های APT از بدافزارهای مالی استفاده می‌کنند تا آنها را با حملات رایج‌تر ترکیب کنند.
- ۵۵۰۰۰ تشخیص در سال ۲۰۱۶ در سراسر جهان فقط مربوط به یک نمونه Bebloh بوده است.
- به طور متوسط، ۶۲ درصد از تشخیص‌های تهدیدات مالی روی کامپیوترهای مصرف‌کننده بوده است.

۳- مقدمه

تهدیدات مالی که هدف آنها تصرف تراکنش‌های مشتریان و جلسات بانکی آنلاین است هنوز قدرتمند هستند. با وجود اینکه باج‌افزارهای رمزنگاری شده در میان مجرمان سایبری برای رسیدن به سود در حال رایج شدن هستند، هنوز حجم قابل توجهی از بدافزارها هستند که سازمان‌های مالی و مشتریان آنها را هدف می‌گیرند.

مؤسسات مالی اقدامات امنیتی خود را برای تراکنش‌هایی که با مشتریان دارند و همچنین برای زیرساخت و سیستم‌های backend خود افزایش داده‌اند. اما مجرمان سایبری، حملات خود را با این اقدامات تطبیق داده‌اند و تا حد ممکن رفتار مشتریان را تقلید می‌کنند و به خود مؤسسات حمله می‌کنند.

در بسیاری از این حملات هنوز مهندسی اجتماعی نقش اصلی را ایفا می‌کند. با افزایش محبوبیت احراز هویت تراکنش از طریق برنامه‌های کاربردی موبایل یا پیام‌های متنی، شاهد افزایش بدافزارهای موبایل هستیم که به دنبال سرقت اطلاعات ورود کاربران هستند. روش کار ساده شده یک بدافزار مالی رایج را می‌توان در مراحل ذیل خلاصه کرد:

- بدافزار از طریق یکی از روش‌های آلوده کردن رایج روی کامپیوتر هدف نصب می‌شود.

- بدافزار منتظر می‌ماند تا کاربر از وب‌سایت مورد علاقه او بازدید کند، سپس یا اطلاعات ورود را سرقت می‌کند، یا داده مرورگر را به شکلی که می‌خواهد تغییر می‌دهد یا ترافیک را به یک سرور راه‌دور که در کنترل مهاجمین است هدایت می‌کند تا حملات مرد میانی (MitM) را انجام دهد.
- وقتی مهاجمین به سرویس بانکداری آنلاین دست یافتند سعی می‌کنند تراکنش‌های جعلی خود را انجام دهند.
- اغلب اوقات این پول به قاچاقچیان پول[۲] ارسال می‌شود که کارشان فقط برداشت پول و ارسال آن پول از روش‌های دیگر به مجرمان است.

شکل ۱- مروری بر تهدیدات شایع علیه مؤسسات مالی

[۲] money mule

این حملات فقط مشتریان بانک‌ها را هدف نمی‌گیرند. حملات متعددی هم بر علیه خود مؤسسات مشاهده شده است که مهاجمین سعی می‌کنند حجم‌های بالایی را در تراکنش‌های جعلی بین‌بانکی جابه‌جا کنند.

حملات بر علیه کسب‌وکارهای خرده‌فروشی و هتل‌ها که پایانه‌های فروش (POS) را هدفگیری می‌کنند نیز در سال ۲۰۱۶ ادامه یافت. حتی تهدیدات ATM هنوز وجود دارند و در حال تکامل هستند اگرچه در این موارد اغلب اوقات باید دسترسی فیزیکی به ماشین ATM وجود داشته باشد.

مؤسسات مالی در زمینه‌های مختلف با این حملات رودررو می‌شوند. دو نوع اصلی این حملات شامل حملات بر علیه مشتریان و حملات بر علیه خود زیرساخت هستند.

۴- آلودگی، شیوع و توزیع

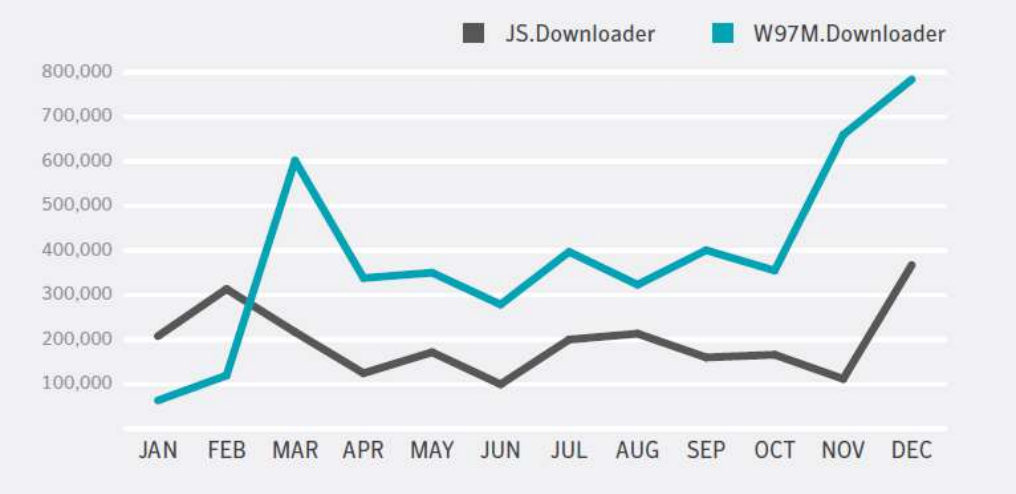
۴-۱- روش‌های آلوده کردن

روش‌های آلوده کردن برای تروجان‌های مالی در سال گذشته تغییر چندانی نکرده‌اند و هنوز همانند سایر تروجان‌های رایج هستند. توزیع، بیشتر به ایمیل‌های اسپم با پیوست‌های مخرب و ابزارهای کدهای مخرب[۳] وب وابسته است. استفاده از ایمیل‌های کلاهبرداری رایج‌ترین روش برای توزیع تروجان‌های مالی در سال ۲۰۱۶ بود. پیوست اسناد آفیس با ماکروهای مخرب هنوز به صورت گسترده استفاده می‌شود. با این حال از اسکریپت‌های ویژوال بیسیک (VBS) و جاوااسکریپت (JS) به شکل‌های مختلف پیوست، از طریق هرزنامه-های انبوه برای توزیع بدافزار استفاده می‌شود. همچنین اسناد آفیس بدون ماکرو نیز مشاهده شده است که از اشیاء OLE تعبیه‌شده استفاده می‌کنند و با استفاده از دستورالعمل‌هایی، کاربر را به دو بار کلیک بر روی payload ترغیب می‌کنند. بات‌نت Necure که فقط در یک روز در نوامبر ۲۰۱۶، بیش از ۱/۸ میلیون دانلودکننده JS ارسال کرد، اندازه بعضی 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[۴] در مایکروسافت ورد 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.

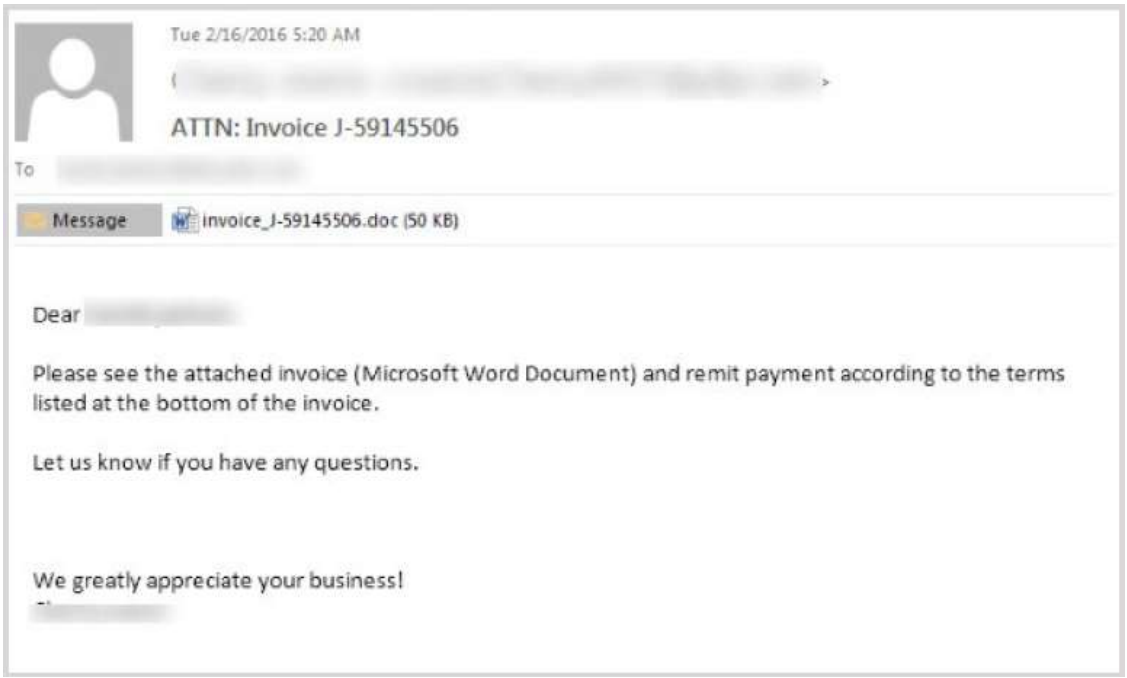
[۳] exploit toolkits

[۴] zero-day



شکل ۲- تشخیص‌های دانلودکننده JS و ماکروی سند در هر ماه سال ۲۰۱۶

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 کرده‌اند. بعضی از ایمیل‌های کلاهبرداری حتی توسط ارائه‌دهنده خدمات ایمیل (ESP) شناخته‌شده و معتبر ارسال شده‌اند که خدمات بازاریابی ایمیلی و ایمیل تراکنشی ارائه می‌داده‌اند. طبقه گفته GovCERT سوئیس، این مسئله می‌تواند شانس این ایمیل‌ها برای دستیابی به صندوق ورودی کاربران را افزایش دهد. در مورد Dridex، ایمیل مورد نظر بسیار قابل باور طراحی شده بود و کاربر را به یک دانلودکننده JS خرابکار هدایت می‌کرد.



شکل ۳- یک نمونه ایمیل فریبکارانه با پیوست سند مخرب

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. فیشینگ ساده برای بیشتر بانک‌ها و مؤسسات مالی قابل استفاده نیست زیرا آنها به ندرت فقط از رمزهای عبور ثابت استفاده می‌کنند. اما حملات فیشینگ هنوز می‌توانند با موفقیت اطلاعات اکانت و کارت اعتباری خرده‌فروشان آنلاین را سرقت کنند.

ابزارهای کدهای مخرب وب در طول این سال تنوع زیادی داشتند. فعال‌ترین تولکیت اکسپلویت در ژانویه ۲۰۱۶، Angler بود. در مارس Spartan بیشترین فعالیت را داشت و در می همان سال دوباره Angler فعال‌ترین تولکیت بود. ماه جولای Neutrino و بقیه سال متعلق به RIG بود. در مارس ۲۰۱۷، RIG مسئول ۱۳/۶ درصد کل فعالیت‌های ابزارهای کدهای مخرب بود که نسبت به ۲۵ درصد فعالیتش در ماه فوریه یک کاهش جزئی داشته است اما هنوز جلوتر از SunDown و Magnitude بود. در مارس ۲۰۱۷، روزانه ۵۸۴۰۰۰ حمله وب توسط Symantec، مسدود شد که بیشتر آنها مربوط به تروجان‌های مالی و باج‌افزارها بودند. تعداد کمپین‌های تبلیغاتی مخرب که در آنها از تبلیغات وب آلوده برای هدایت کاربر به صفحه فرود[۵] تولکیت اکسپلویت وب استفاده شده است در سال ۲۰۱۶ کمی افزایش داشته‌اند.

۲-۴- شیوع

گستره تروجان‌های مالی پیوسته در حال توسعه است و شاهد حرکت به سمت نسخه‌های جدیدتر هستیم. فعال‌ترین خانواده‌های تهدید در سال ۲۰۱۶ شامل Ramnit، Bebloh، Snifula و گونه‌های Zeus بودند. کاهش تعداد تلاش‌ها برای آلوده کردن با تروجان‌های مالی در سال گذشته ادامه داشت. در سال ۲۰۱۶ نسبت به سال ۲۰۱۵، شاهد ۳۶ درصد تشخیص کمتر در نقاط پایانی[۶] بودیم. در سال ۲۰۱۵ هم شاهد ۷۳ درصد کاهش نسبت به سال قبل از آن بودیم. یکی از دلایل این کاهش این است که شرکت‌های امنیتی در مسدود کردن زودتر این تهدیدات در زنجیره کشتار[۷] سایبری موفق‌تر بوده و به‌صورت کاراتر اسپم‌ها را

[۵] landing page

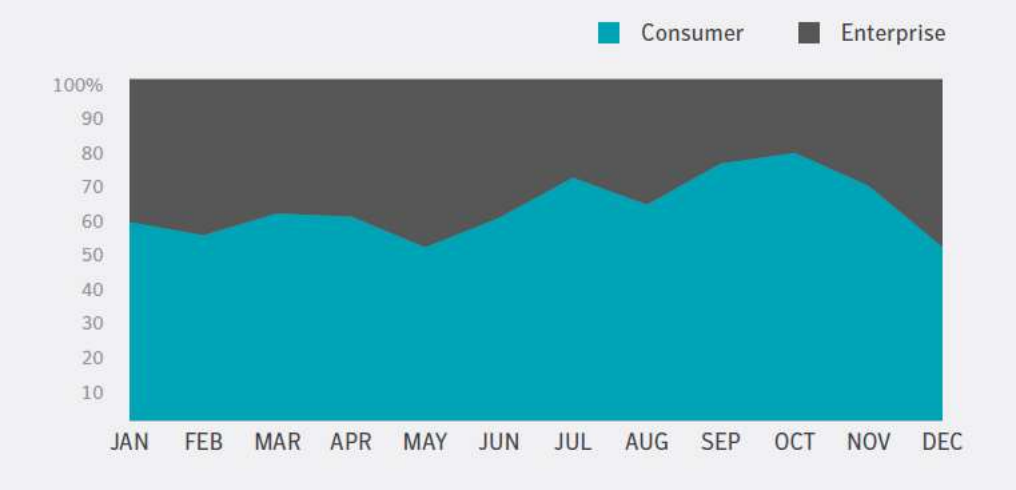
[۶] endpoints

[۷] kill chain

مسدود کرده‌اند. تشخیص موفق بدافزار dropper، تعداد آلودگی‌ها به تروجان مالی مرتبط را کاهش داده است. بنابراین تعداد واقعی بدافزارهایی که به کاربران نهایی به صورت هرزنامه ارسال می‌شوند بیشتر از تعدادی هستند که به نقطه پایانی می‌رسند. افزایش تشخیص‌ها در سپتامبر و اکتبر ۲۰۱۶ بیشتر به دلیل افزایش فعالیت تروجان Bebloh در ژاپن بوده است.

شکل ۴- تشخیص‌های تروجان بانکی بر روی کامپیوتر در سال‌های ۲۰۱۵ و ۲۰۱۶

به طور متوسط ۳۸ درصد کل تشخیص‌های بدافزارهای مالی از کامپیوترهای شرکتی هستند. در پایان سال ۲۰۱۶ این عدد به ۴۹ درصد افزایش یافت. البته بیشتر این تلاش‌ها برای آلوده کردن، به دلیل ارسال گسترده در شبکه توسط تعداد زیادی کمپین اسپم، دچار آسیب موازی کاری هستند. اما همانطور که قبلاً گفته شد، شاهد افزایش تلاش‌های هدفمند برای آلوده کردن مشتریان سازمانی با تهدیدات مالی به‌منظور کلاهبرداری کردن حجم زیادی پول از آنها بوده‌ایم.



شکل ۵- توزیع تشخیص‌های بدافزار مالی

۳-۴- توزیع خانواده تهدید

Ramnit، Zeus و گونه‌های مختلف آن‌ها در سال ۲۰۱۶ سهم بازار خود را دوباره از دست دادند در حالیکه تهدیداتی مانند Bebloh در اواخر سال، توجه زیادی را به خود جلب کردند. دسترسی عمومی کد منبع Zeus باعث شد پروژه‌های متعددی شکل بگیرند و در نتیجه گروه‌های زیادی با انجام برخی تغییرات، تهدیدات تازه‌ای را به وجود آورند.

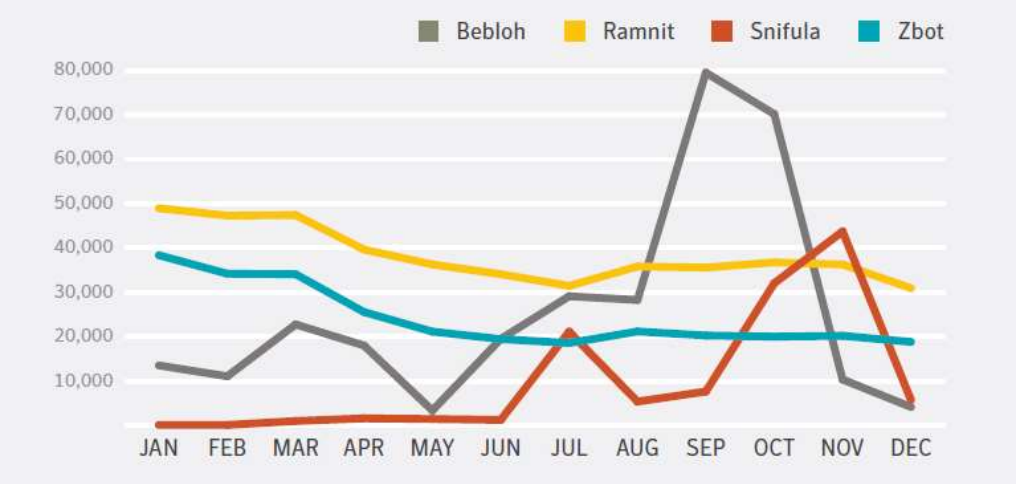
بعد از عملیات فروپاشی بر علیه Ramnit در فوریه ۲۰۱۵، این تهدید غیرفعال شد اما در سال ۲۰۱۶ دوباره ظاهر شده و بر گستره تروجان‌های مالی سلطه پیدا کرد. یک سال تمام، تعداد تشخیص‌های Ramnit بسیار بالا بود. جالب است با توجه به اینکه Ramnit اغلب در گذشته با استفاده از کیت اکسپلویت Angler توزیع می‌شد، با ناپدید شدن Angler در میانه سال از فعالیت آن کم نشد. این نشان می‌دهد بازیگران پشت این تهدید، تکنیک‌های آلوده‌کردن خود را تطبیق داده‌اند، به عنوان مثال، در طی این زمان گزارش‌هایی از انتشار Ramnit از طریق ایمیل در انگلیس وجود دارد.

باید به این نکته نیز اشاره کرد که بعضی از گونه‌های خودتکثیر Ramnit فایل‌های اجرایی و HTML را آلوده می‌کنند که به شیوع آن کمک می‌کند. شاید بعضی از این فایل‌های آلوده قدیمی‌تر غیرفعال شده باشند اما هنوز می‌توانند دوباره منتشر شوند. برای مثال، در جولای ۲۰۱۶، شمار زیادی از آلودگی‌های Ramnit در چین گزارش شد. تصور بر این بود که این مسئله به فایل‌های آلوده قدیمی‌تر مربوط است که یک بار دیگر در حال انتشار هستند. موارد مشابهی نیز در ژاپن دیده شده است.

همانطور که در شکل ۶، Bebloh را در جایگاه دوم لیست تروجان‌های مالی مشاهده می‌کنید، به سرعت در حال افزایش بود به طوری که 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.

Threat	Compromised computers in 2016	Compromised computers in 2015
Ramnit/Gootkit	~460,000	~779,000
Bebloh	~310,000	~13,000
Zeus/Citadel & variants	~292,000	~960,000
Snifula/Vawtrak	~122,000	~4,500
Dridex/Cridex	~23,000	~62,000
Dyre	~4,500	~55,000
Shylock	~4,500	~14,000
Pandemiya	~3,500	~600
Shifu	~2,000	~200
SpyEye	~1,500	~3,500

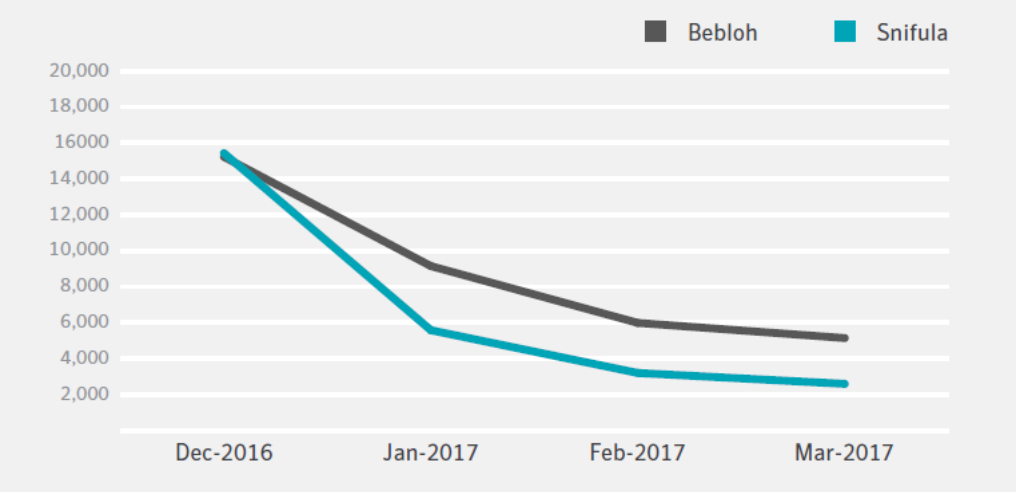
شکل ۶- تعداد تشخیص‌های تهدید مالی در سال‌های ۲۰۱۵ و ۲۰۱۶



شکل ۷- تعداد تشخیص ماهانه برای چهار تهدید اول در سال ۲۰۱۶

همانطور که قبلاً اشاره شد، فروپاشی‌ها می‌توانند تغییرات زیادی در صحنه تهدیدات ایجاد کنند که می‌توان این مسئله را در مورد محوشدن تروجان‌های Dyre و Shylock در سال ۲۰۱۶ شاهد بود. از هم پاشیدن

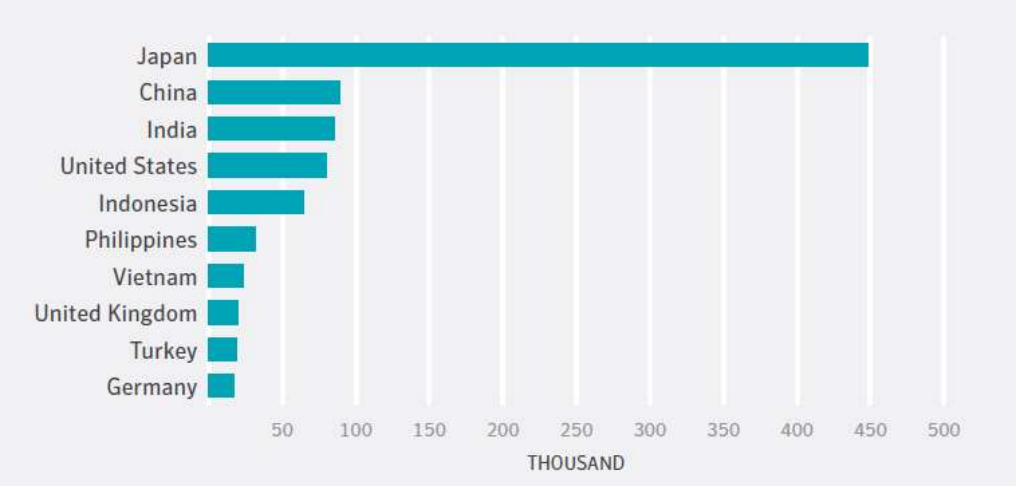
شبکه میزبان بدافزار Avalanche در پایان سال ۲۰۱۶، که Bebloh نیز از آن استفاده می‌کرد باعث کاهش چشمگیر فعالیت Bebloh در ابتدای نوامبر شد. پس از دستگیری متهم ایجادکننده تروجان Snifula در ژانویه ۲۰۱۷، کاهش تشخیص‌های Snifula گزارش شد. این رویدادها باعث کاهش تعداد تشخیص‌ها شدند، Bebloh از دسامبر ۲۰۱۶ تا مارس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



شکل ۸- تعداد تشخیص Snifula و Bebloh در فصل اول سال ۲۰۱۷

۴-۴- توزیع جغرافیایی

همانطور که بحث شد، نرخ‌های تشخیص کمّی برای هر کشور تا حد زیادی به گروه تهدید و دوره زمانی فعالیت گروه بستگی دارد. بعضی از تهدیدات در یک منطقه کوچک جغرافیایی متمرکز هستند و در سراسر جهان توزیع نشده‌اند در حالیکه سایر گروه‌ها به صورت موجی از یک کشور به کشور دیگر جابه‌جا می‌شوند. در تحلیل توزیع تهدیدات مالی در کشورهای مختلف دو روند قابل توجه وجود دارد. یکی اینکه تشخیص‌ها در ژاپن افزایش قابل توجهی داشتند. تعداد تشخیص‌ها در ژاپن در سال ۲۰۱۶ بیشتر از ۱۱ برابر شد که باعث شد ژاپن به بزرگترین هدف حمله در سراسر جهان تبدیل شود. روند جالب توجه دیگر کاهش ۲۶ درصدی حملات در ایالات متحده بود که جایگاه این کشور را به کشور چهارم در کشورهای هدف حملات در جهان پایین آورد.



شکل ۹- کامپیوترهای آلوده به تروجان‌های بانکی در کشورها در سال ۲۰۱۶

البته روشن است که تهدیدات مالی یک مشکل جهانی هستند و هیچ کشوری از آنها در امان نیست. کشورهای کوچکتر شاید در میان ۱۰ کشور با بیشترین تعداد تشخیص نباشند اما نسبت به جمعیت متصل به اینترنت این ریسک هنوز بالاست. برای مثال IBM در سپتامبر ۲۰۱۶ در مورد حملات Dridex گزارش داد، که این حملات بر روی کشور لتونی متمرکز شده است، کشوری که در گذشته اولویت مجرمین مالی نبوده است.

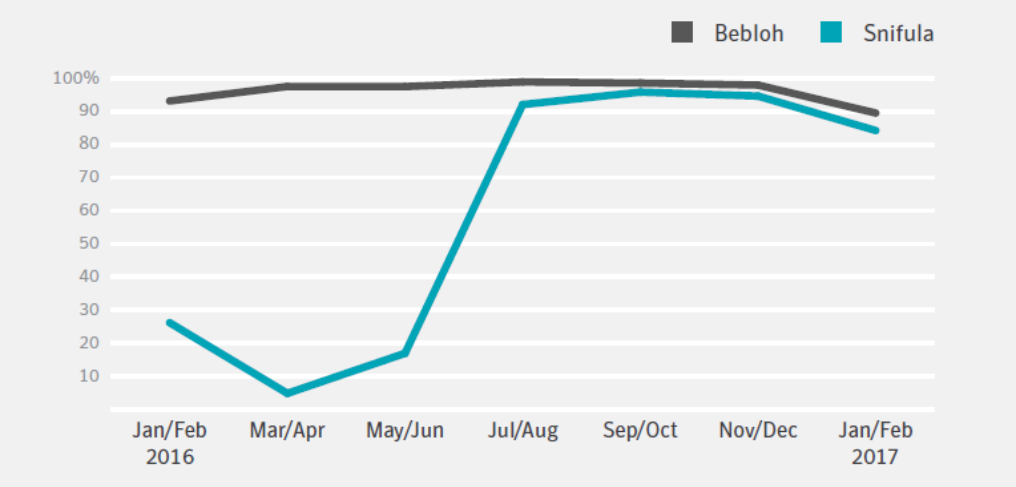
Region	Percentage of global detections 2016	Percentage of global detections 2015
Japan	36.69%	3.21%
China	6.92%	4.69%
India	6.37%	6.31%
United States	6.30%	8.54%
Indonesia	4.78%	6.31%

شکل ۱۰- رده‌بندی کشورها بر اساس درصد تشخیص‌های جهانی مشاهده شده در هر سال

۵-۴- تمرکز روی ژاپن

در مقاله Financial Threats 2015 شاهد رشد چشمگیر حملات بر علیه ژاپن و پیش‌بینی درست حملات بیشتر به این کشور بودیم. افزایش چشمگیری در تشخیص تروجان‌های مالی در آسیا رخ داد، که ژاپن، چین، هند، فیلیپین و ویتنام در میان ۱۰ کشور بالایی این لیست قرار گرفتند. این موضوع نشان می‌دهد مهاجمین سعی می‌کنند به مناطق با تمرکز جمعیتی کمتر حمله کنند که ممکن است کمتر محافظت شوند.

Bebloh و Snifula به صورت اختصاصی روی اهداف مالی در ژاپن تمرکز کرده‌اند که همین مسئله به افزایش تعداد آلودگی در این کشور کمک کرده است. بیش از ۹۰ درصد تشخیص‌های Bebloh در ژاپن بودند. در ژانویه ۲۰۱۶، ۳۰ درصد تشخیص‌های Snifula در کشور ایالات متحده، اما در نیمه دوم سال، بیش از ۹۰ درصد تشخیص‌های این تهدید در ژاپن رخ دادند. مشخص نیست چه چیزی باعث این تغییر شده است.



شکل ۱۱- تشخیص‌ها در ژاپن بر اساس درصد تشخیص‌های جهانی، گروه‌بندی شده به مدت دو ماه در سال ۲۰۱۶

حداقل ۱۹ مؤسسه مالی در ژاپن هدف Snifula و Bebloh قرار گرفتند. همانطور که دیگران نیز اشاره کرده‌اند، جالب است که این خانواده‌های حملات از webinjectهای مشابه استفاده می‌کنند و تقریباً لیست یکسانی از URLها را هدف می‌گیرند.

این موضوع می‌تواند نشان‌دهنده این باشد که هر دو گروه از یک سرویس برای ساختن webinjectها استفاده می‌کنند.

اگر به نمونه‌ها نگاه کنیم، یک نمونه از Bebloh به تنهایی مسئول ۴۷ درصد کل تشخیص‌های سراسر جهان در ژانویه ۲۰۱۶ بوده است. پنج نمونه از فعال‌ترین نمونه‌های Bebloh با هم نماینده ۹۳ درصد کل تشخیص‌های جهانی در ژانویه ۲۰۱۶ هستند. ۹۰ درصد کل تشخیص‌ها در ژاپن در این دوره از این پنج نمونه بوده‌اند. در دسامبر ۲۰۱۶، هنوز همین پنج نمونه مسئول ۰/۶ درصد کل تشخیص‌های جهانی بوده‌اند. همه این نمونه‌ها در ایمیل‌های ساده به شکل اسنادی از یک اسکنر با یکی از این نام فایل‌های دو پسوندی ارسال می‌شوند:

scan(2).doc.2016.01.20.PDF.exe
scan01_doc_2015~jpeg.jpeg.exe
IMAGE(1).15_02_2016_PDF_PNG.PDF.EXE
image_n_(1) 20160217_PNG,PDF.png.exe

برای Snifula که پنج نمونه از آن در دسامبر ۲۰۱۶، ۹۴ درصد کل تشخیص‌ها را تشکیل می‌دادند نیز موقعیت مشابهی را می‌توان یافت. همانند Bebloh، این نمونه‌ها در ایمیل‌هایی با نام فایل‌های دوپسوندی زیر ارسال می‌شدند:

MX_20161031_1530380.JPG.exe
43894370932861.html.exe
IMG_20161020_095456~1.jpg.exe
ID654093871066.PDF.EXE

همانطور که قبلاً گفته شد، Bebloh و Snifula بعد از فروپاشی‌هایی که با اجرای قانون در ابتدای سال ۲۰۱۷ صورت گرفت با کاهش قابل‌توجهی مواجه شدند.

۶-۴- توزیع در رابطه با پیکربندی

کارشناسان هنگام تحلیل سه نمونه از Dridex، که فایل پیکربندی مشابهی داشتند و به احتمال زیاد از یک ارسال اسپم آمده بودند، به نکته جالبی رسیدند که هر کدام از آنها ۱۶ نشانی وب مالی یکسان در آلمان و ۱۰ نشانی وب در اتریش را هدف می‌گیرند. بررسی پنج کشور بالای لیست که در آنها این نمونه‌ها دیده شده‌اند الگوی جالبی را آشکار می‌کند. همانطور که انتظار می‌رفت، همه آنها در آلمان و اتریش دیده شده‌اند اما این دو کشور فقط برای یکی از این سه نمونه، از مکان‌های متداول بوده‌اند. این نمونه‌ها در ایالات متحده نیز مشاهده شده‌اند که یک VPN یا ارائه‌دهنده اینترنت که از آدرس‌های آی‌پی در آن کشور استفاده می‌کند می‌تواند این مسئله را توضیح دهد. اما جای تردید است که از این توصیف برای توضیح آلودگی‌های

اسرائیل یا فیلیپین استفاده شود. تمام چیزی که می‌توان گفت این است که احتمالاً به دلیل الگوی توزیع انتخاب شده برای ایمیل اسپم، حمله‌ها به اندازه‌ای که کارشناسان انتظار داشتند هدفمند نبوده‌اند. البته سه نمونه، نماینده مناسبی برای هزاران اجرای اسپم نیست اما آنها دریافتند که این مسئله برای بسیاری از نمونه‌هایی که بررسی شده است صحت دارد. این موضوع نشان می‌دهد که میزان فاصله انتشار نمونه‌ها، کاملاً به خانواده تهدید و گروه مجرمین پشت آن بستگی دارد. طبق مشاهدات، ممکن است تقریباً همه تشخیص‌های بعضی از گونه‌های Bebloh و اهداف آنها در ژاپن باشند درحالیکه نمونه‌های Dridex توزیع گسترده‌تری دارند.

	Sample 1	Sample 2	Sample 3
United States	42.7%	8.7%	89.4%
Germany	22.9%	26.1%	2.1%
Austria	16.7%	34.8%	3.4%
France	7.3%	17.4%	3.9%
Israel	10.4%	0.0%	0.0%
Philippines	0.0%	13.0%	0.0%
China	0.0%	0.0%	1.3%

شکل ۱۲- بررسی توزیع منطقه‌ای سه نمونه Dridex

۷-۴- تحلیل مؤسسات هدف

در سال ۲۰۱۶، شاهد این بودیم که گروه‌های مهاجم روی مکان‌های جغرافیایی خاص تمرکز می‌کنند. بنابراین بعضی از تهدیدات شاید نقش مهمی در سطح جهانی بازی نکنند اما می‌توانند در بازارهای کوچکتر بسیار فعال باشند.

Symantec، ۶۸۴ نمونه را از چهار خانواده از تهدیدات تحلیل کرد: Dridex، Snifula، Panda Banker و Trickbot. ۳۰۱ الگوی URL منحصر به فرد از ۱۳۲ مؤسسه در ۱۷ کشور که بدافزار آنها را مانیتور می‌کرد آشکار شد. اگر روی کشورهایی که در میان تمام نمونه‌های تحلیل شده مشترک هستند تمرکز کنیم، ۷۹ درصد از حمله‌ها حداقل به یک مؤسسه مالی در ایالات متحده حمله کرده‌اند که نشان می‌دهد مؤسسات

این کشور بیشتر از همه هدف حمله بوده‌اند، لهستان و ژاپن در جایگاه‌های بعدی قرار دارند. به طور متوسط هر نمونه ۳۷ مؤسسه مختلف را هدف گرفته است.

Rank	Country
1	United States
2	Poland
3	Japan
4	Australia
5	New Zealand
6	Germany
7	Austria
8	United Kingdom
9	Canada
10	Italy
11	Iran
12	China
13	Spain
14	Tonga
15	France

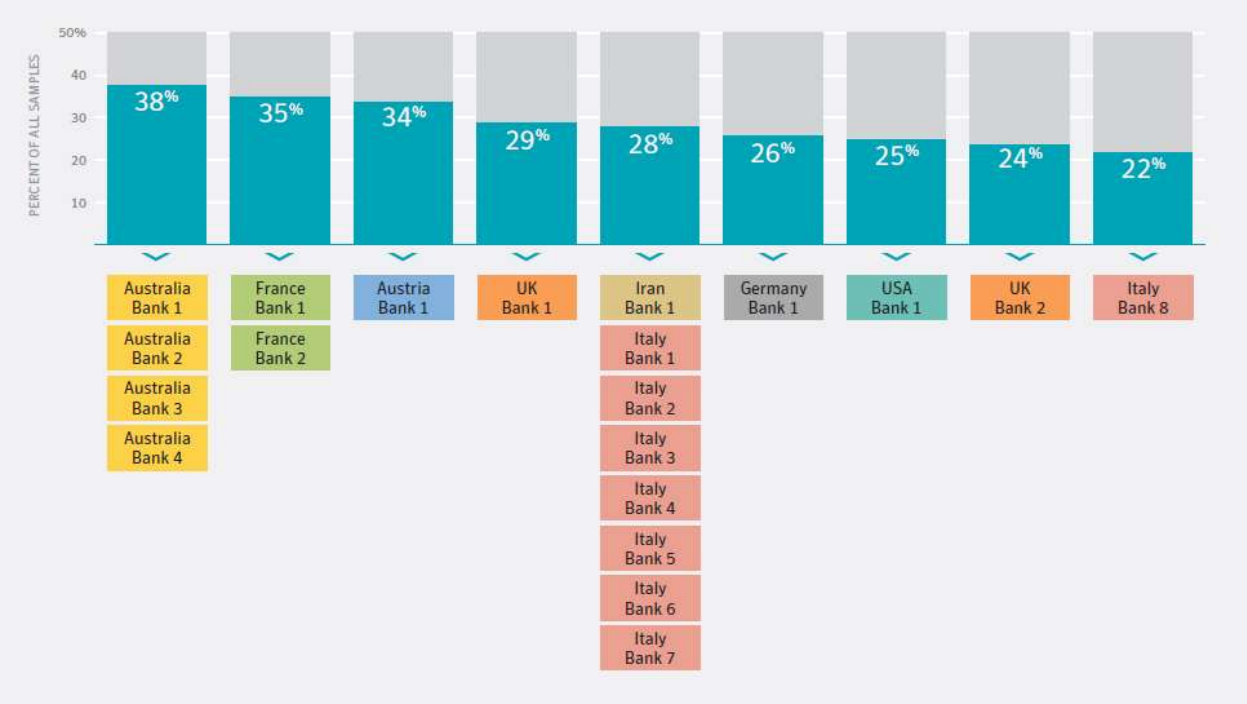
شکل ۱۳- مورد هدف‌ترین کشورها براساس URLها در پیکربندی webinject

متأسفانه لیست بانک‌ها و کشورهای مورد هدف، بسیار به اجراهای اسپم خاص مجرمین سایبری وابسته است. ممکن است یک کشور در یک ماه در بالای لیست قرار گیرد و در ماه بعد در میان ۲۰ کشور بالای لیست نباشد. برای مثال، موج‌های حمله‌ای وجود داشته است که در آن مجرمین یک شبه از حمله به استرالیا و زلاندنو به حمله به آلمان و بریتانیا تغییر رویه دادند.

علاوه بر این، روندی در تهدیدات دیده شده است که ترافیک را به طور کامل تغییر جهت می‌دهند یا از تزریق‌های پویا از یک سرور راه دور استفاده می‌کنند. این نمونه‌ها ترافیک را از هر وب‌سایت بازدید شده‌ای

که شامل کلمه «بانک» در URL خود هستند هدایت می‌کنند. این یعنی بدافزار فایل پیکربندی کامل را برای کلاینت دانلود نمی‌کند و اطلاعات را به محققین نمی‌دهد. علاوه بر این، برخی از نویسندگان بدافزار به طور کامل چیزهایی که تعبیه کرده‌اند را پنهان می‌کنند. فایل‌های تروجان‌های مالی که از قبل پیکربندی شده‌اند شامل لیستی از نشانی‌های وب مورد علاقه مجرمین هستند که در یک فایل رمزنگاری شده ذخیره شده‌اند. اما گونه‌های جدیدی از Blackmoon مشاهده شده است که فقط هش SHA1 آن URL را ذخیره می‌کنند که یک مقدار Salt منحصر به فرد به آن متصل شده است. این باعث می‌شود درست کردن مجدد لیست کامل نشانی‌های وب هدف تقریباً غیرممکن باشد.

با این وجود با در نظر گرفتن تمام نمونه‌های تحلیل شده و وزن‌دهی به آنها بر اساس شیوع آنها مشخص می‌شود چهار بانک که مرکز آنها در استرالیا قرار دارد در ۳۸ درصد همه نمونه‌ها قرار دارند.



شکل ۱۴- برترین مؤسسات مالی مورد هدف در گروه نمونه

Rank	Country	Percentage
1	United States	17.16
2	Turkey	11.24
3	France	10.65
4	Germany	9.47
5	Australia	7.10
6	Thailand	5.92
7	United Kingdom	5.92
8	Poland	5.33
9	Austria	4.73
10	Russia	3.55

شکل ۱۵- ده کشور اول مورد هدف توسط Android.Fakebank.B

توزیع کشوری تهدیدات موبایل کمی متفاوت است. 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.

۵- حملات به ATM، POS و موبایل

۵-۱- ATM و POS

حمله به ATM و پایانه‌های فروش (POS) در سال ۲۰۱۶ نیز افزایش یافت. ده سال است که بدافزار ATM وجود دارد اما هنوز کارآمد است. با افزایش حملات هدفمند به بانک‌ها، شاهد افزایش حملات به ATMها از درون شبکه مالی نیز بودیم. خانواده‌های تهدید ATM و POS زیادی وجود دارند مانند Ploutus، Flokibot، Trojan.Skimer، FastPOS، Infostealer.Poslit، Infostealer.Donpos، Infostealer.Jackpos، Infostealer.Scanpos و Backdoor.Pralice.

در دنیای حملات ATM، درجات مختلفی از پیچیدگی وجود دارند. مجرمین برای بعضی از حملات به دسترسی فیزیکی به کامپیوتر ATM نیاز دارند و این کار را با باز کردن پوشش آن با استفاده از یک کلید

دزدی یا برداشتن قفل انجام می‌دهند. 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 کنند (بدافزار Ploutus از این روش حمله استفاده می‌کند).

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

با دسترسی فیزیکی به ATM، می‌توان از یک روش حمله دیگر نیز استفاده کرد. طبق گزارشی در آوریل ۲۰۱۷، بعضی مهاجمین متوجه شده‌اند می‌توانند با سوراخ کردن بدنه ATM به سیستم گذرگاه داخل آن دسترسی پیدا کنند. به محض دسترسی پیدا کردن، تنها چیزی که نیاز است میکروکامپیوتر است تا با استفاده از آن بتوان دستورات را به گذرگاه ارسال کرد تا ATM همه پول‌ها را بیرون بریزد.

در همه حملات ATM و POS نیازی به دسترسی فیزیکی نیست. در نوامبر ۲۰۱۶، FBI درباره گروه Buhtrap هشدار داد که به شبکه‌های داخلی مؤسسات مالی نفوذ می‌کند و دستورات ATM را صادر می‌کند که باعث می‌شود پول توزیع کند و این کار را بدون دستکاری فیزیکی دستگاه انجام می‌دهد. پلیس چین تایپه تخمین می‌زند حملات سایبری باعث از دست رفتن ۳۰۰ میلیون دلار شوند. در یک مورد دیگر، مهاجمین توانستند بدافزار ATMitch را روی چند ATM نصب کنند و حداقل ۸۰۰۰۰۰ دلار به‌دست آورند.

در مورد حملات POS 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 می‌کنند سپس با استفاده از نرم‌افزار TeamViewer و Ammyy Admin از راه دور کامپیوترهای آلوده را کنترل کرده و حملات خود را پیش می‌برند.

در آگوست ۲۰۱۶، وب‌سایت یک فروشنده نرم‌افزار POS آلوده شد. طبق گزارش‌ها، اطلاعات دزدیده شده، دسترسی راه دور به سیستم‌های POS خرده‌فروش‌های متعددی را در اختیار مهاجمین قرار داده بود. این افشا باعث شده فروشنده تمام رمزهای عبور سیستم‌های آلوده را ریست کند.

۲-۵- تهدیدات مالی اندروید

از زمان معرفی برنامه‌های کاربردی بانکداری موبایل و احراز هویت دو مرحله‌ای (2FA)، مجرمین سایبری به دنبال روش‌هایی برای دور زدن احراز هویت دو مرحله‌ای با استفاده از مهندسی اجتماعی یا حمله به پلت-فرم موبایل بوده‌اند. در سال‌های اخیر تهدیدات مالی روی گوشی‌های اندروید بیش از پیش رواج یافته‌اند اما هنوز تعداد آلودگی‌ها و تنوع خانواده‌های تهدید در مقایسه با تهدیدات ویندوز بسیار کمتر است.

به طور کلی تعداد تشخیص‌های بدافزار موبایل با ۲۹ درصد افزایش به ۷/۲ میلیون در سال ۲۰۱۶ افزایش یافت. بیش از نیمی از تشخیص‌ها به تهدیدهای دانلودکننده مانند Android.MalDownloader مربوط می‌شوند. تهدیدات مالی موبایل بعد از برنامه‌های کاربردی ارسال‌کننده پیام متنی و باج‌افزارها در جایگاه سوم تهدیدات رایج هستند. بیشتر تهدیدات موبایل به مجوزهای root نیازی ندارند اما بعضی از آنها اکسپلویت‌های افزایش سطح دسترسی را دانلود می‌کنند که به تهدید اجازه می‌دهد رمزهای کش شده را از مرورگر و سایر برنامه‌های کاربردی سرقت کند. یک تاکتیک رایج، نمایش پیام «فعال‌سازی ادمین دستگاه» به‌صورت پی در پی است تا اینکه کاربر به برنامه‌کاربردی مجوز ادمین بدهد.

روش آلوده کردن معمولاً شامل مهندسی اجتماعی و یک لینک اسپم به تهدید مورد نظر است که شبیه یک برنامه کاربردی معتبر است. مهاجمین ابزار معتبر را به صورت تروجان درمی‌آورند و آنها را برای دانلود تبلیغ می‌کنند. روش دیگر برای توزیع، استفاده از وب‌سایت‌های آلوده است که بدافزارها روی آنها به شکل یک پخش‌کننده فیلم که باید برای نمایش محتوا نصب شود قرار دارند. معمولاً کاربران فریب داده می‌شوند تا هشدارهای امنیتی را نادیده بگیرند و خودشان داوطلبانه برنامه‌های کاربردی مخرب را نصب کنند. مطالعه دقیق مجوزهای درخواست شده در پیام نصب، یکی از مؤثرترین روش‌های محافظت است و بعضی از برنامه‌های کاربردی این درخواست‌ها را به تأخیر می‌اندازند تا بتوانند مهندسی اجتماعی بیشتری انجام دهند. برنامه‌های کاربردی مخرب فقط در فروشگاه‌های برنامه‌کاربردی شخص ثالث مشکل ایجاد نمی‌کنند. هنوز هم شاهد این هستیم هر از گاهی برنامه‌های کاربردی مخرب روی فروشگاه Google play رسمی قرار می‌گیرند. برای مثال، در فوریه ۲۰۱۷ یک گونه از Android.Fakebank.B خودش را به شکل یک برنامه کاربردی به نام «هوای خوب» جا زد و روی فروشگاه Google play قرار گرفت و تقریباً ۵۰۰۰ کاربر آن را دانلود کردند.

با تکامل مداوم سیستم‌عامل اندروید، شاهد تغییر مداوم روش‌ها و تاکتیک‌های استفاده شده توسط مهاجمین هستیم. روش‌های اصلی به کار گرفته شده توسط تهدیدات مالی موبایل شامل SMS و فوروارد کردن تماس، فرم‌های جعلی، سرقت اطلاعات و برنامه‌های کاربردی بانکداری موبایل جعلی هستند.

تهدیدات موبایل، برنامه‌های کاربردی غیرمالی مانند برنامه‌های کاربردی رسانه اجتماعی یا برنامه‌های کاربردی چت را نیز هدف می‌گیرند. یکی از گونه‌های Android.Fakebank.B با نام Marcher نیز وجود داشت که بیشتر از ۱۲۵ مؤسسه مختلف را هدف گرفته بود. مهاجمین در بعضی از حملات از یک پیام متنی جعلی از طرف بانک استفاده می‌کنند که از کاربر می‌خواهد تراکنش کلاهبرداری را تأیید کند که این درخواست حالت اضطراری ایجاد می‌کند و کاربر را مجبور می‌کند بلافاصله وارد برنامه کاربردی مالی شود.

تاکتیک دیگری که توسط Android.Fakebank.B استفاده می‌شود اضافه کردن خودش به لیست سفید استثناهای بهینه‌سازی باطری است به گونه‌ای که ویژگی جدید اندروید ۶، در زمان صرفه‌جویی باطری، این تروجان را متوقف نمی‌کند. به این ترتیب این تهدید می‌تواند به سرور C&C خودش متصل بماند. همین خانواده بدافزار در ماه مارس از قابلیت محدود کردن تماس استفاده کرده است. بدین معنی که بدافزار می‌تواند هر تماس خروجی به یک لیست از پیش تعیین شده از شماره‌های خدمات مشتری را مسدود کند (در این مورد شماره‌ها با بانک‌های روسیه و کره جنوبی ارتباط داشتند). این ویژگی باعث می‌شود کاربر نتواند با تماس با مؤسسه مالی، تراکنش‌های مشکوک را بررسی یا لغو کند. این کار مشابه تاکتیک استفاده شده توسط بدافزار ویندوز Shylock است که وقتی کاربر از وب‌سایت بانک بازدید می‌کند شماره تلفن‌های پشتیبانی مشتری بانک را با شماره‌های روی کامپیوتر آلوده جایگزین می‌کند.

بعضی اوقات مهاجمین از ترفندهای ساده برای رسیدن به اهداف خود استفاده می‌کنند. در ابتدای سال ۲۰۱۶، Android.Bankosy از یک ترفند ساده برای سرقت توکن‌های صوتی 2FA استفاده کرد (زمانی که بانک با مشتری تماس می‌گیرد و یک صدای کامپیوتری کد 2FA را برای کاربر می‌خواند). این تروجان با استفاده از کد سرویس ویژه #[DESTINATION NUMBER]*21* ، فوروارد تماسی اضافه می‌کند که بسیاری از شبکه‌های تلفن از آن پشتیبانی می‌کنند. وقتی این سرویس فعال شود، تماس از طرف بانک با شماره VOIP تحت کنترل مهاجم صورت می‌گیرد و آنها می‌توانند به کد 2FA مورد نیاز برای انجام تراکنش‌های کلاهبرداری خود دست پیدا کنند.

۶- نتیجه‌گیری

با وجود اینکه تعداد تشخیص‌های بدافزار مالی در سال ۲۰۱۶، ۳۶ درصد کاهش داشته است، اما این دسته از تهدیدات هنوز به رغم فروپاشی‌ها و دستگیری‌های متعدد، بسیار فعال و رایج هستند. سه بازیگر اصلی سال ۲۰۱۶، Ramnit، Bebloh و Zbot بودند که با هم مسئول ۸۶ درصد کل فعالیت‌های مرتبط با تهدیدات مالی بودند. در کمال شگفتی، بیشتر شیوع این بدافزارها به واسطه تعداد نمونه‌های کمی به‌دست آمده بودند. برای مثال، فقط یک نمونه از Bebloh مسئول ۴۷ درصد از همه تشخیص‌ها در ژانویه ۲۰۱۶ بود. این وضعیت، نتیجه انتشار گسترده میلیون‌ها ایمیل مخرب بود. روش‌های آلودگی برای تهدیدات مالی همانند سایر بدافزارهای رایج مانند باج‌افزار هستند و مشاهده شده است که گروه‌های زیادی از بات‌نت‌های اسپم یا ابزارهای اکسپلویت مشابه استفاده کرده‌اند.

ژاپن هدف ۳۷ درصد کل حملات بدافزار مالی در سال ۲۰۱۶ بود که این موضوع نشان می‌دهد وقتی هدف‌های موجود اشباع می‌شوند، یا به خوبی محافظت شده و به راحتی نمی‌شود از آنها سرقت کرد، مهاجمین به سرعت خودشان را با بازارهای جدید تطبیق می‌دهند.

ترفندهای اجتناب از جعبه شنی[۸] و ضد اشکال‌زدایی[۹] در سال ۲۰۱۶ تغییر نکرد. اما استفاده از حملات تغییر جهت افزایش یافت. یکی دیگر از روندهای قابل توجه، افزایش حملات به خود شرکت‌ها و مؤسسات مالی است. به طور متوسط، ۳۸ درصد کل تشخیص‌های تهدیدات مالی در شرکت‌ها بوده است. وقتی مهاجمین آلودگی را شناسایی کردند از راه دور وارد شده و به مرور زمان یاد می‌گیرند چگونه تراکنش‌ها را انجام دهند. آنها بر اساس فرصت‌های موجود سعی می‌کنند تراکنش‌های تقلبی را به دستورات پرداخت ماهیانه تزریق کنند یا در صورتی که هدف بانک باشد، سعی می‌کنند انتقال‌های بین بانکی را ثبت کنند. با وجود اینکه انجام این حملات دشوارتر است و زمان بیشتری می‌برد، اما به سود بیشتری می‌انجامد. برای نمونه گروه Lazarus که با حملات بانکی سطح بالا ارتباط دارد و این اولین باری است که یک بازیگر سطح دولتی این گونه حملات را با انگیزه مالی انجام می‌دهد.

[۸] sandbox evasion

[۹] anti-debugging

تهدیدات موبایل روی اندروید بیشتر روی حملات برنامه‌های کاربردی بانکداری آنلاین تمرکز دارند. بیش از ۱۷۰ برنامه کاربردی موبایل هدف بدافزار موبایل قرار گرفته‌اند. تهدیدات موبایل هنوز رایج هستند و تعداد زیادی از مؤسسات مالی از طریق برنامه‌های کاربردی گوشی موبایل، احراز هویت دو مرحله‌ای را پیاده‌سازی کرده‌اند. به دلیل اینکه انجام این حملات در آخرین نسخه از سیستم‌عامل اندروید دشوارتر شده است، شاهد بازگشت مهاجمین به حملات مهندسی اجتماعی هستیم که در آن قربانی‌ها برای انجام تراکنش‌ها فریب داده می‌شوند. کاربر نهایی هنوز ضعیف‌ترین حلقه این زنجیره در طول انجام یک تراکنش آنلاین است که این موضوع نشان می‌دهد حتی قوی‌ترین فناوری‌ها هم مستعد حملات مهندسی اجتماعی هستند.

انتظار می‌رود که تهدیدات مالی در آینده هم برای کاربران نهایی یک مشکل باشند اما به احتمال زیاد مهاجمین روی بخش‌های مالی شرکت‌ها تمرکز خواهند کرد و از مهندسی اجتماعی بر ضد آنها استفاده خواهند نمود.

۷- محافظت

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

- احتیاط هنگام کار با بانکداری آنلاین به ویژه وقتی رفتار و ظاهر وب‌سایت بانک تغییر کرده است.
- احتیاط در هنگام دریافت ایمیل‌های ناخواسته، غیرمنتظره یا مشکوک
- به‌روز نگه‌داشتن نرم‌افزارهای امنیتی و سیستم‌های عامل
- فعال کردن امکانات امنیتی پیشرفته حساب مانند 2FA و اطلاع‌رسانی ورود در صورت امکان
- استفاده از رمزهای قوی برای همه حساب‌های کاربری
- خروج از جلسه ایجاد شده بعد از اتمام کار
- بررسی منظم صورت‌حساب‌های بانکی
- اطلاع‌رسانی به بانک در مورد هر رفتار مشکوک هنگام استفاده از خدمات
- آگاهی نسبت به پیوست‌های آفیس که از کاربران می‌خواهند ماکروها را فعال کنند.

منابع:

[1] 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