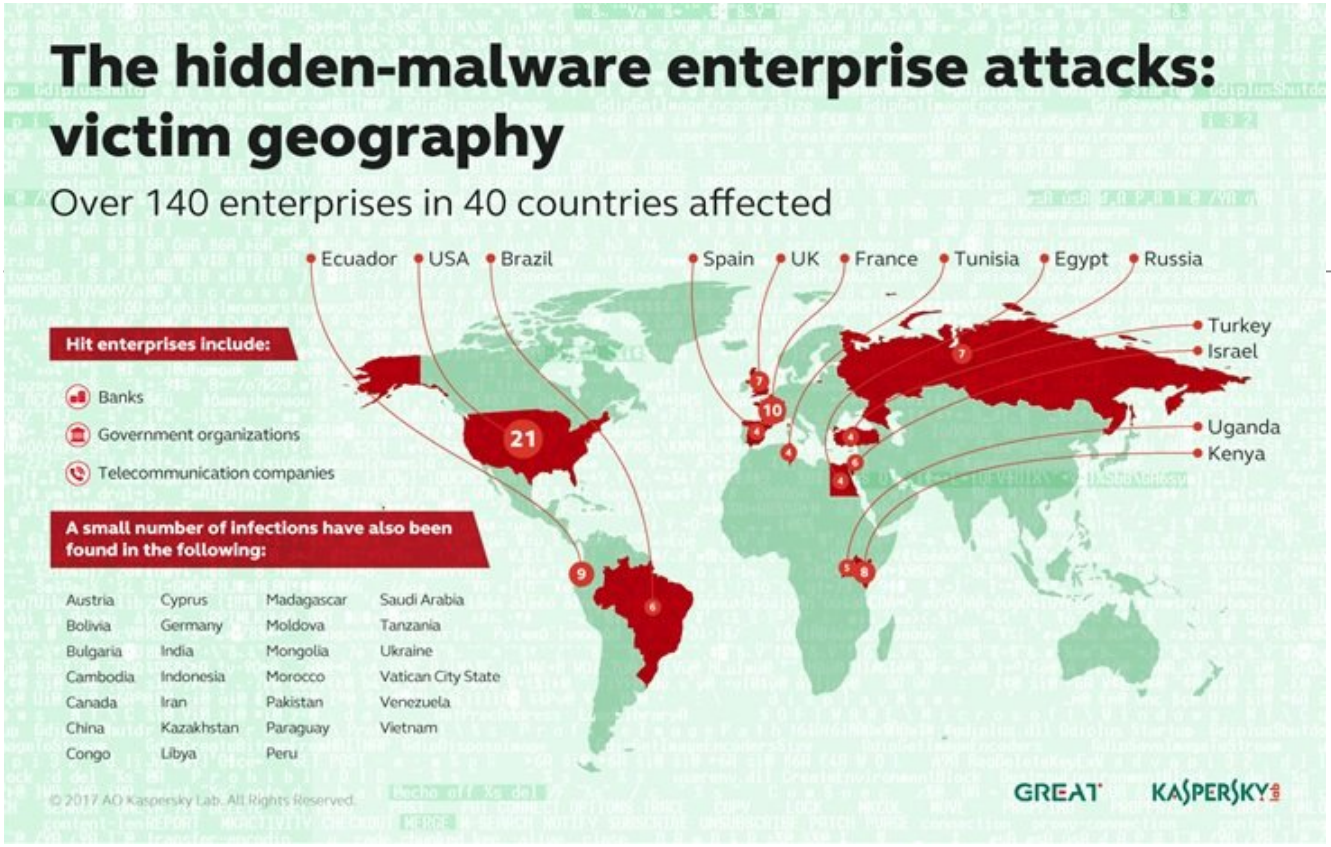
بدافزار غیر قابل رویت

بدافزاری که در سیستم بانکی بیش از 40 کشور پنهان شده بود



بانک‌ها، شرکت‌های فعال در حوزه ارتباطات و حتا آژانس‌های دولتی در ایالات متحده، کشورهای مستقر در امریکای جنوبی، اروپا و حتا آفریقا از جمله قربانیان این بدفزار مخوف بوده‌اند. این بدافزار به راحتی توانسته بود به درون سامانه‌های کامپیوتری این کشورها وارد شود و به دور از دید کارشناسان امنیتی فعالیت‌های مخرب خود را انجام دهد.

گزارشی که به تازگی از سوی آزمایشگاه کسپرسکی منتشر شده نشان می‌دهد حداقل 140 بانک و سازمان قربانی بدافزار فوق بوده‌اند. بدافزاری که تقریبا نامریی بوده است. رقم آلوده‌سازی در 140 کشور رسمی و معتبر بوده، با این وجود به نظر می‌رسد به دلیل موانعی که بر سر راه شناسایی این بدافزار وجود دارد، تعدادی از کشورهای آلوده به این بدافزار هنوز شناسایی نشده‌اند در نتیجه ممکن است میزان آلودگی به مراتب فراتر از آن رقمی باشد که به آن اشاره شده است. این آلودگی دقیقا شبیه به موردی است که شرکت کسپرسکی چند سال قبل آن‌را در شبکه خود شناسایی کرده بود. بدافزار Duqu 2.0 که در آن زمان کسپرسکی موفق شد آن‌را شناسایی کند به لحاظ عملکرد متفاوت از نمونه‌هایی بود که تا به آن روز شناسایی شده بودند. بسیاری از کارشناسان در آن اعلام داشتند که Duqu 2.0 بر مبنای کدهای بدافزار استاکس‌نت نوشته شده است. Duqu 2.0 به مدت شش ماه و بدون آن‌که کسپرسکی از وجود آن اطلاع پیدا کند در شبکه این شرکت امنیتی به فعالیت مشغول بود.

مطلب پیشنهادی

جاسوسی هدفمند

تلویزیون هوشمندی که از کاربرانش جاسوسی می‌کرد

پیاده‌سازی حملات جدید

آلودگی فوق درست همانند یک حادثه آتش‌سوزی بزرگ است که به سرعت شعله‌ور شده و بانک‌ها را یکی پس از دیگری طعمه حریق می‌سازد. آلودگی فوق که به سختی می‌توان آن‌را شناسایی کرده از ابزارهای قانونی مدیریت بر شبکه و ابزارهای امنیتی همچون PowerShell، Metaspolit و Mimikatz استفاده می‌کند تا کدهای مخرب را به درون حافظه اصلی کامپیوتر وارد کند. کسپرسکی گفته است: «ما در ارتباط با بانک‌ها و موسساتی که به آن‌ها حمله

شده است هیچ‌گونه اطلاعاتی منتشر نخواهیم کرد، اما تنها به این نکته اشاره می‌کنیم که آژانس‌های متعلق به 40 کشور در معرض حمله این بدافزار قرار داشته‌اند.» به ترتیب کشورهای ایالات متحده، فرانسه، اکوادر، کنیا و انگلستان در صدر فهرست کشورهایی هستند که این بدافزار بیشترین حمله را به آن‌ها داشته است.

مطلب پیشنهادی

ابزارهای به سرقت رفته از Cellebrite منتشر شدند
وقتی ابزارهای هک هم به سرقت می‌روند

موضوعی که باعث شده است عملکرد این بدافزار مورد توجه رسانه‌ها و شرکت‌های امنیتی قرار بگیرد این است که بدافزار فوق به مدت بسیار طولانی و به شکلی ناشناس فعال بوده است. همین موضوع باعث شده است تا امکان شناسایی طراحان آن به سختی امکان‌پذیر باشد. کارشناسان امنیتی حتا با قاطعیت نمی‌توانند به این موضوع اشاره کنند که آیا یک گروه یا چند گروه هکری در پس زمینه این حملات قرار داشته‌اند. حتا به درستی مشخص نیست این بدافزار ماحصل همکاری نهادهای دولتی بوده است یا مجرمان سایبری سازمان یافته آن‌را طراحی کرده‌اند. اگر هیچ گروه هکری مسئولیت این حمله را عهده‌دار نشود، آن‌گاه باید مدت زمان طولانی را به انتظار بنشینیم تا کارشناسان امنیتی و مقامات دولتی عامل بروز این حملات را معرفی کنند.

بدافزار فوق چگونه کار می‌کند؟

اولین مرتبه نشانه‌هایی از وجود این بدافزار در روزهای پایانی سال 2016 شناسایی شد. یک تیم از پژوهشگران امنیتی بانکی موفق شدند یک کپی از Meterpreter را در حافظه فیزیکی یک کنترل‌کننده دامنه مایکروسافت شناسایی کنند. کارشناسان فوق پس از تحلیل اولیه اعلام کردند کدهای متعلق به Meterpreter با استفاده از دستورات پاورشل به درون حافظه تزریق شده است. ابزار شبکه طراحی شده از سوی مایکروسافت موسوم به NESH از سوی یک ماشین آلوده به منظور ارسال داده‌ها به سمت سرورهایی که تحت کنترل هکرها قرار داشته مورد استفاده قرار گرفته بود.

هکرها همچنین از Mimiktaz به منظور دریافت امتیازهای مدیریتی لازم و پیاده‌سازی عملیات مختلف استفاده کرده بودند.

دستورات پاورشل نیز با هدف پاک‌کردن گزارش‌هایی که در رجیستری ویندوز ثبت می‌شوند مورد استفاده قرار گرفته بودند. همین موضوع باعث شده بود تا ردیابی فعالیت‌ها غیر ممکن شود. تحلیل‌ها نشان می‌دهد هکرها از این سازوکار برای به دست آوردن گذرواژه متعلق به مدیران شبکه و همچنین مدیریت از راه دور بر ماشین‌های آلوده میزبان استفاده کرده‌اند. عاملی که باعث شد تا کارشناسان امنیتی موفق شوند بدافزار فوق را شناسایی کنند این است که هکرها در تمامی حملات خود از چنین سازوکاری استفاده می‌کردند.

تاریخ انتشار:

23 بهمن 1395

نشانی منبع: https://www.shabakeh-mag.com/security/6764