موضوع

RanSomWare

استاد: دکتر پورابراهیمی

دانشجو: علی ثاقب موفق – 98571100104

خرداد 1399

تعریف:

RanSomWare ، نوعی بد افزار (Malware) است که در آن مجرم سایبری، با گرفتن کنترل کل شبکه یا بخشی از شبکه یک شرکت، نسبت به اخاذی از قربانی(مسئول شبکه، رئیس شرکت، Admin و ...) در قبال آزاد سازی مجدد شبکه و منابع آن اقدام می کند.

گروه های RanSomWare از ماشین های از قبل آلوده شده از سایر بدافزارها و یا از پروتکل های ارتباط از راه دور دسکتاپ (Remote Deskto Protocol – RDP) برای شروع و نقطه اولیه لنگرگاه خود بر روی شبکه شرکت هدف، استفاده می کنند. باز بودن پورت های شبکه و امکان telnet کردن و یا Ftp به شبکه یا امکان ارتباط Remote به هر نحو، از آسیب پذیری های جدی شبکه محسوب شده که می توان تبدیل به تهدید RanSomWare و نهایتا حملات RanSomWare شود. این نوع حملات (Attack) مستلزم همکاری بین چند گروه است و این شراکت کارآمد و عموما اقتصادی است. حملات هدفمندی که منجر به سودآوری شده و خرابی اقتصادی به بار می آورند.

اهمیت حملات RanSomWare

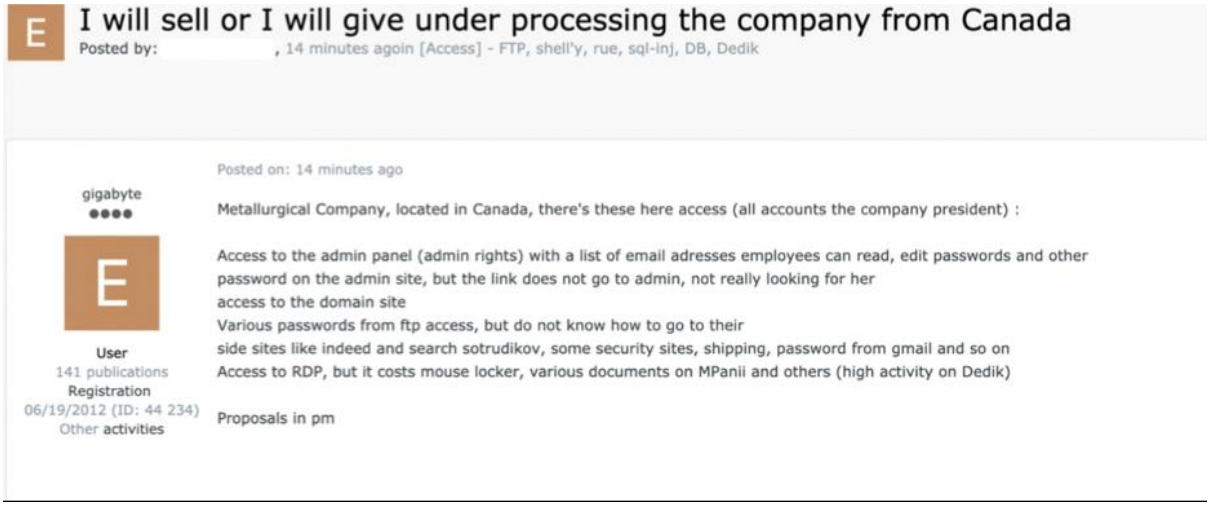
در واقع یوروپل Europol's Internet Organised Crime Threat Assessment (IOCTA) این نوع حملات را در بالاترین سطح تهدیداتی قرارداده است که شرکت ها، مشتریان و بخش های عمومی در سال 2019 با آن مواجه هستند.

بر اساس آنچه که پژوهش های تهدیدات پیشرفته مک کافی McAfee Advanced Threat Research (ATR) در خصوص فعالیت های زیرزمینی انجام داده است، انتظار می رود که جنایتکاران از قربانیان اخاذی خود در ادامه و به طور مستمر نیز بهره برداری نمایند.

افزایش باج افزارهای مورد هدف، منجر به افزایش تقاضا برای شرکت های بزرگ در معرض خطر شده است. این تقاضاها توسط مجرمان سایبری دریافت می شوند، کسانی که متخصص در نقوذ به شبکه های بزرگ هستند و دسترسی کامل به شبکه را در یک مرحله می فروشند.

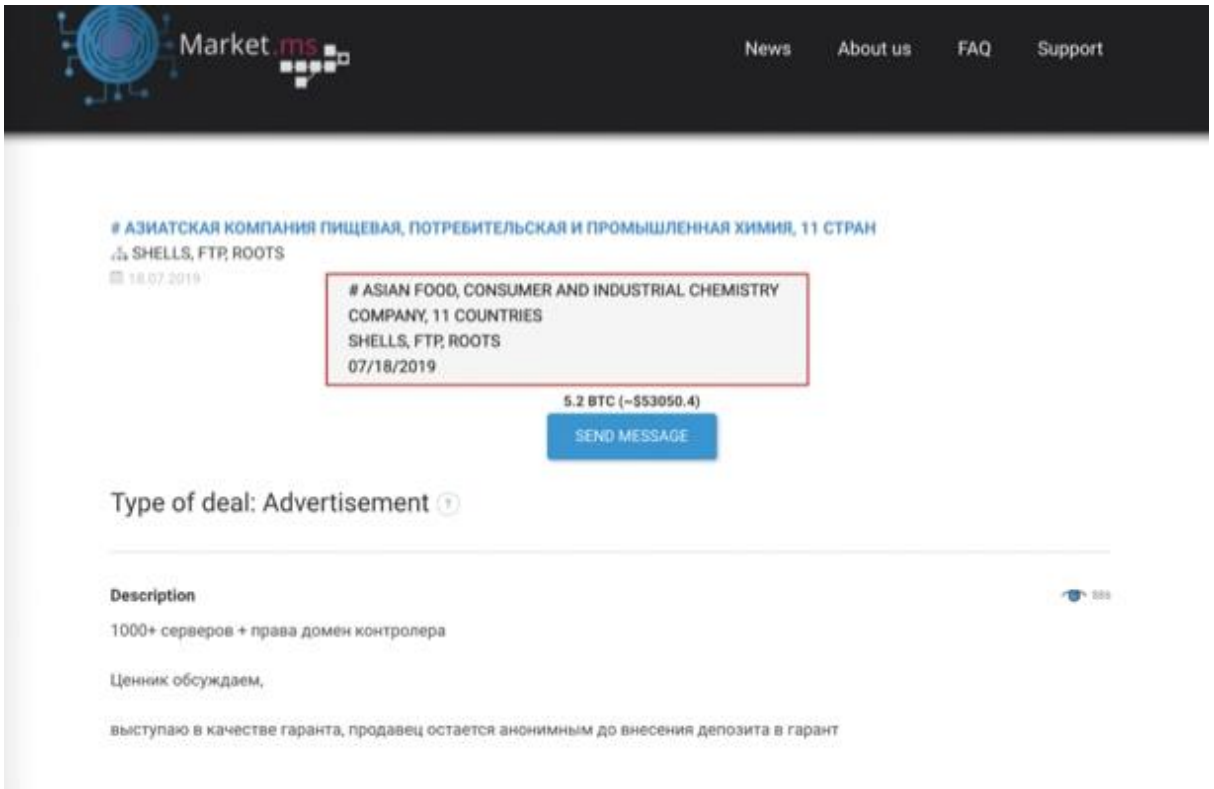
چند نمونه واقعی از حملات RanSomWare

نمونه ای از تبلیغات زیرزمینی برای پیشنهاد دسترسی به شبکه کسب و کار در اینجا آورده شده است:



در این مثال، هکر، دسترسی به پنل Admin یک شرکت کانادایی، با لیستی از ایمیل آدرس های کارکنان و قابلیت ویرایش و... آنها را در معرض فروش گذاشته است و از متقاضیان می خواهد که پیشنهاد خود را در PM او قرار دهند.

نمونه حمله دیگر مربوط به یک شرکت مواد غذایی آسیایی است که در 11 کشور فعالیت دارد و لیست مشتریان و شرکت صنعتی آن توسط هکر پیشنهاد شده است.



مک کافی پیش بینی کرده است که نفوذ به شبکه های بزرگ ادامه داشته و در نهایت به صورت حملات دو مرحله ای رشد خواهند داشت.

در مرحله اول، جنایتکاران سایبری، یک حمله فلج کننده به شبکه را ارائه خواهند داد تا بتوانند برای برگردان فایل ها از قربانی اخاذی نمایند. در مرحله دوم جنایتکاران، برگردان شبکه و بهبود سیستم قربانی RanSomWare را با یک حمله اخاذی ، هدف قرار می دهند. اما اینبار قبل از حمله، قربانی را به افشاء داده های حساس تهدید می کنند.[1]

به عبارت دیگر، اخاذی از قربانی شبکه از جوانب مختلف مطرح می شود که شامل، اخاذی در قبال ارائه پسورد ادمین، اخاذی در قبال ریکاوری شبکه، اتهام زنی به قربانی برای فعالیتهای غیر قانونی احتمالی کشف شده توسط مجرم سایبری و اخاذی، تهدید و اخاذی برای افشاء اطلاعات حساس مشتریان موجود و .. می باشد.

در تحقیقات انجام شده، بر روی حملات دو مرحله ای، مشاهده گردید که ابزارهای رمزنگاری قبل از یک حمله RanSomWare نصب شده است.

پیش بینی حملات RanSomWare **برای سالهای آتی**

برای سال 2020 پیش بینی شده است که مجرمان سایبری به طور فزاینده ای اطلاعات حساس شر کتها را قبل از حمله RanSomWare تصفیه و برای فروش داده های دزدیده شده آنلاین به دیگران یا اخاذی از خود قربانی و افزایش درآمد از آنها استفاده می کنند. به عبارت دیگر حداکثر سوء استفاده مالی از منابع اطلاعاتی و شبکه به عمل می آورند/

روش های نفوذ RanSomWare

زمانی که سیستمی به RanSomWare آلوده شود قربانی راهی جز فرمت سیستم یا اطاعت از باج گیرنده ندارد. نمونه هایی از RanSomWare عبارتند از Revoton ، CryptoLocker ، ScareMeNot و ScarePackage و روش های نفوذ و آلوده سازی سیستم های همان روش های نفوذ معمول از قبیل ایمیل های اسپم و فایل های پیوست آن، لینک های مخرب، بازدید از سایت های مشکوک و مخرب ، رسانه ذخیره سازی خارجی آلوده، فایل دانلود شده از سایت های نامعتبر و .... است.

راه کارهایی برای پیشگیری از RanSomWare

بهترین راه پیشگیری از RanSomWare رعایت ملاحظات امنیتی است. به عبارت دیگر علاج واقعه قبل از وقوع باید کرد. زیرا حداقل در این مورد، بعد از وقوع حمله RanSomWare ، مدیریت آن بسیار مشکل ،

هزینه بر و گاها غیرممکن خواهد بود. برخی از راه های جلوگیری از RanSomWare ، همان روشهای معمول اعمال امنیت از قبیل آگاهی از روش های نفوذ این بدافزار و اهمیت دادن به ملاحظات امنیتی شبکه و هزینه نمودن برای تست نفوذ شبکه (Peneteration Test) و استفاده از ابزارهای امنیتی مثل آنتی ویروس، فایروال امن و موثر در سرور، استفاده از سایت ها و هاست امن ، نرم افزارهای ضد اسپم، بروزرسانی سیستم عامل و آنتی ویروس و پشتیبان گیری مرتب از اطلاعات حساس می باشد. از آنجائیکه اطمینانی به هکرهای باج افزار در اینگونه موارد وجود ندارد و حتی در صورت پرداخت وجه، ممکن است این اخاذی ها همچنان از فرد قربانی ادامه داشته باشد، لذا مراجعه به پلیس فتا می تواند یکی از راه حل ها در صورت وقوع این نوع حمله باشد.

Reference:

[1]. McAfee Labs 2020 Threats Predictions Report