ویروسهای باج گیر در شبکه های کامپیوتری

ویروس های باج گیر، بدافزارهایی هستند که بطور معمول از طریق پیوست های ایمیل، دانلود فایلهای ناشناس مخرب و از همه مهمتر از طریق ریموت وارد سیستم و شبکه کامپیوتری شده و سپس در طی مراحلی اقدام به رمزگذاری اطلاعات مربوطه کرده و درخواست باج بابت فایلهای رمز شده می نمایند.

در آخرین اخبار که طبق رصدهای مرکز ماهر (مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای) گزارش شده، موج بالایی از حملات باج افزاری از طریق آسیب پذیری سرویس REMOTE DESKTOP **(کنترل از راه دور کامپیوتر) در سطح سرورهای ویندوزی صورت گرفته که در طی آن مهاجمین با سوءاستفاده از سرویس** Remote Desktop **ویندوز و وجود رمز عبور ضعیف، وارد سیستم ها شده و با انتقال فایل، اقدام به رمزگزاری اطلاعات موجود بر روی فایل‌های سرور می کنند.**

لذا توصیه های موکد بر این بوده که تا حد امکان از باز بودن پورت Remote Desktop **اجتناب نمایید.**

مدیران شبکه‌هایی که از ریموت دسکتاپ ویندوز برای اتصال به ایستگاه‌های کاری از خارج مجموعه استفاده می‌کنند، در معرض حملات باج‌افزارها هستند. به تازگی نمونه‌هایی از باج‌افزارها کشف شده‌اند که از طریق ضعف امنیتی ریموت دسکتاپ ویندوز اقدام به ورود به سیستم و کدگذاری فایل‌ها می‌کنند و پس از آن مبالغ هنگفتی را برای بازگرداندن اطلاعات طلب می‌کند.

چگونگی عملکرد این باج افزارها بدین صورت است که ابتدا باج‌گیران از طریق نرم‌افزارهای خودکار اقدام به اسکن درگاه‌های باز روی آدرس‌های IP **اینترنتی کرده و در صورتی که پورت ریموت دسکتاپ روی آنها باز باشد، اقدام به حدس زدن رمزهای عبور مختلف نموده و شانس خود را برای ورود به سیستم محک می‌زنند. در صورتی که فایروالی با قابلیت تشخیص اینگونه حملات در شبکه فعال نباشد و همچنین مقرراتی برای جلوگیری از ورود پسوردهای اشتباه به دفعات متعدد موجود نباشد، ممکن است بعد از گذشت فاصله زمانی کمی، نرم‌افزارهای باجگیر بتوانند رمز عبور صحیح را حدس زده و دسترسی ورود به سیستم را دریافت کنند.**

پس از گرفتن دسترسی به سیستم‌عامل، حتی در صورتی که نرم‌افزارهای مخصوص ضد باج‌افزار نیز روی سیستم نصب باشد، باز هم با توجه به داشتن دسترسی مدیریتی، هکرها قادر به حذف هرگونه محصول امنیتی خواهند بود، و پس از آن به راحتی باج‌افزار خود را اجرا و اقدام به کدگذاری تمامی فایل ها خواهند نمود. متاسفانه به علت داشتن دسترسی مدیریتی هیچ نرم‌افزار امنیتی قادر به مقاومت در برابر آنها نخواهد بود؛ زیرا تمامی فعالیت‌ها بر مبنای دسترسی مدیر سیستم و به‌صورت قانونی انجام می‌پذیرد.

<u>باج افزار جدید بنام BlackRouter که توسط ابزار شناخته شده قانونی راه دور، راه اندازی شده است.</u>

به تازگی باج افزار BlackRouter **که از طریق نرم‌افزار مشهور مدیریت از راه دور بنام** AnyDesk **، انتشار پیدا کرده است.**

AnyDesk به طور گسترده ابزار دسکتاپ راه دور شبیه به Teamviewer است که می تواند کنترل از راه دور دو طرفه بین سیستم عامل های مختلف دسکتاپ، از جمله ویندوز، macOS، لینوکس و FreeBSD، و همچنین دسترسی یک طرفه در اندروید و iOS را برقرار نماید.

مجرمان اینترنتی با استفاده از نرم‌افزار AnyDesk ، باج افزار BlackRouter را در سیستم های کامپیوتری وارد می کنند و اطلاعات انها را رمز می نمایند. این باج افزار ممکن است به همراه نرم افزارهای قانونی نصب شود و تکنیک هایی را استفاده کرده باشد که از تشخیص نرم‌افزارهای امنیتی مثل آنتی ویروس جلوگیری نماید.

فرآیند آلوده کردن باج‌افزار BlackRouter

این باج‌افزار به همراه فایلهای دیگر از طریق کپی، دانلود ریموت و ... وارد کامپیوترها می شود.

این باج‌افزار سپس برای فرایند تخریب از AnyDesk برای انتقال فایل و باج‌افزار BlackRouter برای رمزگذاری فایل های سیستم آلوده استفاده می کند و انواع فرمت هایی مانند gif، mp4، pdf، xls ، فایهای دیتابیس و غیره رمزگذاری می کند.

در طول روند آلوده‌سازی، AnyDesk شروع به کار در پس‌زمینه سیستم می‌کند و باج‌افزار BlackRouter فایل‌ها را فایل‌ها را رمزگذاری می‌کند.

پس از اتمام فرایند رمزگذاری، یادداشت هایی را در مورد آنچه که می تواند در کامپیوتر آلوده اتفاق بیفتد، نمایش می دهد. این پیام حاوی درخواست پرداخت پول برای دسترسی به فایلهای قفل شده است. و می گوید، هنگامی که قربانیان مبلغ هزینه را پرداخت می کنند پس از آن کلید رمزگشایی را از طریق تلگرام دریافت خواهند کرد.

مهندس جلال پورفخیمی/ سرپرست واحد انفورماتیک

منابع:

https://blog.trendmicro.com
https://security.tosinso.com
https://creativestudio.one
http://academy.atinegar.com
http://www.ertebateamn.com