آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

خبرنامه تحلیلی رویدادهای امنیتی (روزانه)

سه‌شنبه سیزدهم خرداد ماه ۱۳۹۹

کشف باج‌افزار[1] رِگنالاکِر[2] در رایانه‌های ویندوزی

نسخه ۱,۰,۰

نویسنده : مونا رضا زاده **سردبیر :** محمد پیشدار

[1]-Ransomware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

[2]-RagnarLocker

باج‌افزار رِگنالاکِر به کمک برنامه ویرچوال‌باکس[1] از دید ابزارهای امنیتی مخفی می‌شود

تاریخ: ۲۲/ مِی/ ۲۰۲۰

بررسی اجمالی :

اخیرا محققان امنیت سایبری موفق به کشف یک باج‌افزار جدید تحت عنوان رِگنالاکِر بر روی رایانه‌های ویندوز شده‌اند. این باج‌افزار پس از نصب برنامه ویرچوال‌باکس و اجرای ماشین مجازی می‌تواند در یک محیط امن و بدون دسترسی به ضد بدافزار[2] اجرا شود. طبق گفته محققان این اولین باج‌افزار در محیط ماشین مجازی محسوب می‌گردد [۱].

نگاه کلی :

سیستم‌های آسیب‌پذیر	رایانه‌های ویندوزی
راه‌های نفوذ	تاکنون جزئیات مناسبی در دسترس نیست
هدف مهاجمان	دریافت باج و رمزگذاری فایل‌ها

توضیحات بیشتر :

محققان شرکت سوفوس[3] از کشف یک باج‌افزار جدید به نام رِگنالاکِر در سیستم‌عامل ویندوز خبر می‌دهند. باج‌افزاری که با نصب برنامه ویرچوال‌باکس و اجرای ماشین مجازی می‌تواند در یک محیط امن و بدون شناسایی توسط

[1]-Oracle VM VirtualBox (formerly Sun VirtualBox, Sun xVM VirtualBox and Innotek VirtualBox) is a free and open-source hosted hypervisor for x86 virtualization, developed by Oracle Corporation.
[2]-Malware (a portmanteau for malicious software) is any software intentionally designed to cause damage to a computer, server, client, or computer network
[3]-Sophos Group plc is an English security software and hardware company. Sophos develops products for communication endpoint, encryption, network security, email security, mobile security and unified threat management.

برنامه‌های ضد بدافزار به رمزگذاری فایل‌های قربانی بپردازد [۱]. به گفته محققان این اولین موردی از باج‌افزار است که با استفاده از ماشین مجازی به باج‌گیری از کاربران می‌پردازد [۱]. البته بر اساس گزارشات رِگنالاکِر یک باج‌افزار معمولی نبوده و هدف اصلی آن شبکه‌های شرکت‌ها و سازمان دولتی است [۱].

در گذشته این باج‌افزار از طریق خدمات‌رسان‌های کنترل راه دور دِسکتاپ (آر.دی.پی[۱]) قربانیان خود را هدف گرفته و به کمک ابزارهای مدیریت از راه دور (اِم.اِس.پی[۲]) به شبکه‌های داخلی آن‌ها نفوذ می‌کرده است. رِگنالاکِر با قرارگیری در شبکه‌های محلی سازمان‌ها پس از رمزنگاری فایل‌ها هزینه نجومی از قربانیان خود درخواست خواهد کرد [۱].

این گروه از باج‌افزار به جای اجرای مستقیم، ابتدا برنامه ویرچوال‌باکس را بر روی سیستم قربانی نصب و راه‌اندازی می‌کند. با این روش امکان اجرای ماشین مجازی بر روی سیستم کاربر فراهم می‌گردد. در ادامه باج‌افزار با پیکربندی ماشین مجازی، به همه درایوهای محلی و مشترک دسترسی کامل خواهد داشت [۱]. در مرحله بعد با بوت شدن ماشین مجازی یک نسخه از سرویس پَک ۳ ویندوز اِیکس.پی[۳] به نام میکرواِکسپی ۷۰،۸۲[۴] اجرا می‌گردد [۱].

در آخرین مرحله باج‌افزار در ماشین مجازی و بدون شناسایی ضد ویروسی اجرا خواهد شد. در واقع از دید نرم‌افزار ضد ویروس، فایل‌های موجود در سیستم محلی و درایوهای اشتراکی به طور ناگهانی با نسخه‌های رمزگذاری آن جایگزین شده و تمام تغییرات فایل‌ها از یک فرایند قانونی (برنامه ویرچوال باکس) نشات می‌گیرند [۱].

پیشنهادات :

- امن‌سازی نرم‌افزارهای دسترسی از راه دور به سیستم (استفاده از کلمه عبور قوی، فعال‌سازی احراز هویتس دو مرحله‌ای، محدودسازی دسترسی کاربران و حساب‌های دارای قابلیت کنترل از راه دور، استفاده از پروتکل‌های امن ارتباطی نظیر اِس.اِس.اِچ[۵]، فعال‌سازی لاگ‌های مربوط به ابزارهای مدیریت راه دور)
- بروزرسانی ابزارهای امنیتی و دسترسی راه دور
- دقت نسبت به نصب غیرمجاز ابزار ویرچوال‌باکس
- محدودسازی دسترسی به کمک فایروال[۶]ها

[1]-Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection.
[2]- A managed service provider (MSP) is a company that remotely manages a customer's IT infrastructure and/or end-user systems, typically on a proactive basis and under a subscription model.
[3]-Windows XP Service Pack 3
[4]-MicroXP v0،282
[5]-Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network.
[6]-in computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

منابع :

1. Zdnet Website
https://www.zdnet.com/article/ransomware-deploys-virtual-machines-to-hide-itself-from-antivirus-software/