همه چیز درباره بدافزار اکتبر سرخ؛ از شناخت تا پاک‌سازی

در طول چند سال گذشته، سطح بالایی از جاسوسی سایبری با هدف قرار دادن شبکه‌های رایانه‌ای سازمان‌های پژوهشی، دیپلماتیک، دولتی و علمی به منظور نفوذ، جمع آوری داده‌ها و اطلاعات از دستگاه‌های تلفن همراه، سیستم‌های رایانه‌ای و تجهیزات شبکه، به طور گسترده‌ای در سطح جهان، در جریان بوده است. بدافزار "اکتبر سرخ" نیز یکی از این شبکه‌های جاسوسی سایبری پیشرفته است که سازمان‌های دیپلماتیک و دولتی بزرگ را مورد هدف قرار داده است. محققان آزمایشگاه تحقیقات امنیتی کسپرسکی، چندین ماه را صرف تجزیه و تحلیل این بدافزار کرده‌اند که با عنوان "Rocra"(کوتاه شده عبارت اکتبر سرخ) شناخته می‌شود و دریافته‌اند که این بدافزار سازمان‌های خاصی را به طور عمده در شرق اروپا، کشورهای عضو اتحاد جماهیر شوروی سابق و کشورهای آسیای میانه، همچنین در غرب اروپا و شمال آمریکا هدف قرار داده است.

نویسنده: محمدمهدی واعظی‌نژاد
Mahdivaezi61@yahoo.com

بدافزار Rocra تاکنون صدها قربانی در هشت گروه اصلی در سراسر جهان داشته، هر چند که ممکن است بخش‌های دیگری را نیز مورد هدف قرار داده باشد که هنوز کشف نشده‌اند و یا در گذشته مورد حمله قرار گرفته‌اند. این هشت گروه عمده عبارتند از: ارگان‌های دولتی، مراکز دیپلماتیک و سفارت‌خانه‌ها، موسسه‌های تحقیقاتی، مراکز تجاری و بازرگانی، نیروگاه‌ها و تاسیسات هسته‌ای، شرکت‌های نفت و گاز، مراکز هوا و فضا و نیروهای نظامی قربانیان Rocra، در ۳۹ کشور شناسایی شده‌اند و تلاش‌ها برای شناسایی سایر قربانیان نیز در حال انجام است. (نمودار ۱)

محققان کسپرسکی که موفق به شناسایی این بدافزار شده‌اند، اعتقاد دارند که مهاجمان حداقل به مدت پنج سال با تمرکز روی سازمان‌های دیپلماتیک و دولتی، مشغول جمع‌آوری اطلاعات از شبکه‌های آلوده بوده‌اند که از این اطلاعات در حملات بعدی خویش استفاده کرده‌اند. به عنوان مثال، اعتبارهای سرقت شده که در یک لیست، وارد می‌شدند و هنگامی که مهاجمان نیاز به حدس زدن کلمات عبور و اعتبار شبکه در مکان‌های دیگر داشته‌اند از آنها استفاده می‌کرده‌اند. طراحان Rocra برای کنترل شبکه‌ای از ماشین‌های آلوده و همچنین کنترل و بازیابی داده‌های قربانیان، بیش از ۶۰ دامنه اینترنتی و چندین سرور میزبان محلی را در کشورهای مختلف ایجاد کرده‌اند که بررسی IPها نشان می‌دهد که سرورهای کنترل و دستور آن به طور عمده در کشورهای روسیه و آلمان واقع شده است. این بدافزار هنوز هم با ارسال داده‌هایی به سرورهای کنترل و دستور متعدد خود از طریق پیکربندی که قبلا در پیچیدگی‌های زیرساختی بدافزار شعله مشاهده شده است، در حال فعالیت است و تخمین زده می‌شود که تاکنون صدها ترابایت اطلاعات را جابه‌جا کرده باشد. موفقیت حمله Rocra که حتی سازمان‌های تحقیقاتی و موسسه‌های نظامی را نیز شامل می‌شود نشان‌گر ضعف جدی در حفاظت سایبری از زیرساخت‌های رایانه‌ای در سراسر دنیاست که در کشور ما نیز تاکنون هفت مرکز مهم آلوده به آن شناسایی شده است.

سایر نام‌ها

این بدافزار در شرکت‌های امنیتی، به نام‌های مختلفی به این شرح شناخته می‌شود:

Red October [Kaspersky], Backdoor.Rocra [Symantec], Backdoor.Rocra!gen1 [Symantec], [Backdoor.Rocra!gen2 [Symantec

سیستم‌های آسیب‌پذیر

Windows 2000, Windows 7, Windows NT, Windows Vista, Windows XP, Windows 95, Windows 98

جدول یک پراکنش جغرافیایی

نام کشور	میزان آلودگی
روسیه	35
قزاقستان	21
آذربایجان	15
بلژیک	15
هند	14
افغانستان	10
ارمنستان	10
ایران	7
ترکمنستان	7
اوکراین	6
آمریکا	6
ویتنام	6
بلاروس	5
یونان	5
ایتالیا	5
مراکش	5
پاکستان	5
سوئیس	5
اوگاندا	5
امارات متحده عربی	5

گزارش‌هایی از توزیع Rocra در شرق اروپا، کشورهای عضو اتحاد جماهیر شوروی سابق، کشورهای آسیای میانه، شمال آمریکا و کشورهای اروپای غربی مانند سوییس و لوکزامبورگ وجود دارد.

گزارش شبکه امنیتی کسپرسکی (KSN) فهرستی از کشورهای با بیشترین میزان آلودگی (فقط برای کشورهای با بیش از پنج قربانی) را در جدول یک نشان می‌دهد. آمارهای ارایه شده، فقط توسط نرم‌افزار کسپرسکی که روی سیستم‌های آلوده نصب است، گزارش شده و مسلما تعداد واقعی سیستم‌های آلوده، بسیار بالاتر از این خواهد بود.

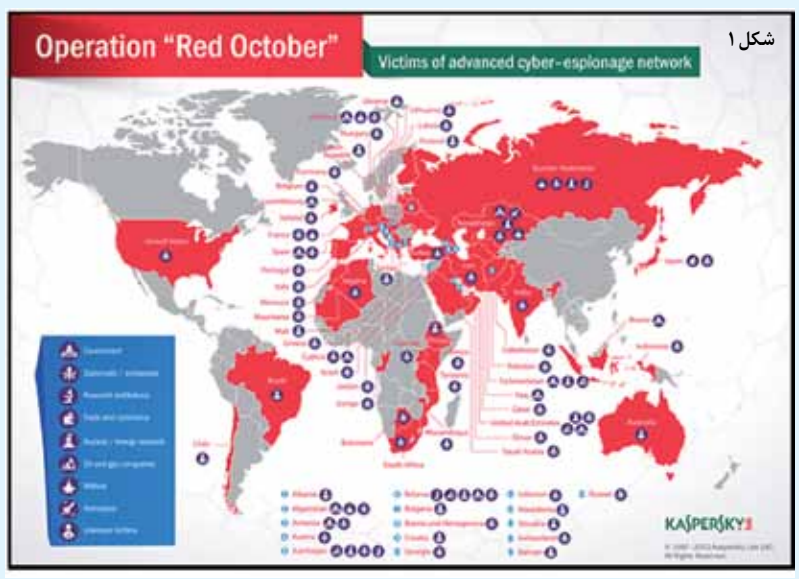
در شکل ۱، توزیع این بدافزار، روی نقشه جهان همراه با مراکز آلوده شناسایی شده توسط کسپرسکی نشان داده شده است:

تاریخچه کشف

اطلاعات ثبت شده برای خرید نام‌های دامنه اینترنتی سرورهای کنترل و دستور بدافزار Rocra و مقایسه PE اجرایی جمع‌آوری شده از آن، نشان می‌دهد که این بدافزار از مه سال ۲۰۰۷ حداقل برای مدت پنج سال بدون شناسایی شدن، در حال فعالیت بوده است.

نخستین بار، محققان کسپرسکی این بدافزار را در ماه اکتبر سال ۲۰۱۲ توسط درخواست یکی از همکاران خود کشف کردند که ترجیح می‌دهند این همکار، همچنان ناشناس باقی بماند. آنگاه با تجزیه و تحلیل حمله، فیشینگ و ماژول‌های بدافزار Rocra، مقیاس آن را درک کرده و تشریح بدافزار شناسایی شده را به طور عمیق آغاز کردند. بدافزار Rocra در روز ۱۴ ژانویه ۲۰۱۳ نیز توسط شرکت امنیتی سیمانتک کشف شده و مورد تجزیه و تحلیل فنی قرار می‌گیرد.

نامگذاری



شکل ۱

بدافزار Rocra، کوتاه شده عبارت اکتبر سرخ (Red October) است که احتمالا نامش از زیردریایی به همین نام، در رمان "شکار اکتبر سرخ" که توسط نویسنده‌ای روسی نوشته شده، گرفته شده است.

طراحی و سازماندهی

محققان کسپرسکی، بر اساس داده‌های ثبت شده از سرورهای کنترل و دستور این بدافزار و همچنین آثار متعدد اجرایی آن، بر این باور هستند که مهاجمان، ملیت روس داشته‌اند. آنها معتقدند که اگرچه با اطلاعات به دست آمده، نمی‌توان به مکان خاصی اشاره کرد. با این حال می‌توان روی دو عامل مهم پافشاری کرد:

- به نظر می‌رسد که کدهای مخرب توسط هکرهای چینی نوشته شده است.
- ماژول‌های بدافزاری Rocra توسط افرادی روس زبان ایجاد شده است.

چندین ماژول Rocra دارای غلط‌ها و اشتباه‌های املایی جالبی است که بر قوت این نظریه، می‌افزاید. برای نمونه در بخشی از کد بدافزار از واژه "PROGA" استفاده شده که ممکن است ترجمه‌ای از واژه روسی عامیانه "ПРОГА" باشد که برنامه‌ای در میان مهندسان نرم‌افزار روسی است. عبارت دیگر استفاده شده در این کد به طور خاص، "Zakladka" است که در روسیه می‌تواند به معنای "bookmark" یا (به احتمال زیاد) در اصطلاح عامیانه به معنی "قابلیت‌های اعلام نشده"، مثلا در نرم‌افزار یا سخت‌افزار باشد. با این حال، همچنین امکان دارد که یک میکروفون جاسازی شده در یک آجر از ساختمان سفارت باشد.

همچنین کلاس c++ این بدافزار که دارای پارامترهای قابل پیکربندی سرورهای کنترل و دستور آن است، "MPTraitor" نامیده شده و بخش پیکربندی مربوط به منابع هم به نام "conn_a" است. برخی از این نمونه‌ها عبارتند از:

- conn_a.D_CONN
- conn_a.J_CONN
- conn_a.D_CONN
- conn_a.J_CONN

با این حال، اگرچه مهاجمان و بدافزار قابل اجرای توسعه یافته توسط آنها در حال حاضر ناشناخته‌اند، اما آنها هرگز ارتباطی با دیگر حملات سایبری هدفمند که در گذشته انجام شده، ندارند و مدرکی که نشان دهنده ارتباط این موضوع با حمله‌ای حمایت شده توسط یک دولت خاص باشد نیز وجود ندارد.

عملکرد

مهاجمان برای تحقق اهداف خویش، یک چارچوب (Framework) چند منظوره ایجاد کرده‌اند که قادر به استفاده از گستره‌های وسیع از ویژگی‌هایی است که اطلاعات را جمع‌آوری می‌کند. این چارچوب که بسیار پیچیده است، از ابتدا توسط همین مهاجمان، طراحی شده و در هیچ یک از عملیات‌های سایبری دیگر استفاده نشده است. علاوه بر اهداف سنتی حمله که شامل ایستگاه‌های کاری رایانه‌ای می‌شود، این بدافزار قادر به سرقت اطلاعات از دستگاه‌های تلفن همراه، از جمله گوشی‌های هوشمند (آیفون، نوکیا و ویندوز موبایل)، روگرفت از پیکربندی تجهیزات شبکه (سیسکو)، ربودن فایل‌ها از دیسک درایوهای قابل جابه‌جایی (حتی شامل فایل‌هایی که در حال حاضر از روی سیستم پاک شده‌اند توسط یک فرآیند بازیابی سفارشی فایل)، سرقت نامه‌های الکترونیکی ذخیره شده در نرم‌افزار Outlook سیستم‌های آلوده یا سرورهای POP3/IMAP از راه دور به همراه فایل‌های ضمیمه آنها، ثبت تمامی کلیدهای فشرده شده روی صفحه کلید، گرفتن تصویرهای فوری و ارسال آنها، تهیه تاریخچه وب گردی از مرورگرهای وب همچون کروم، فایرفاکس، اینترنت اکسپلورر و اپرا، همچنین انحراف مسیر فایل‌ها از سرورهای FTP شبکه محلی است. Rocra علاوه بر سرقت اطلاعات از نرم‌افزارهای متنی، ورد و اکسل، می‌تواند اطلاعات رمزنگاری شده از قبیل pgp و فایل‌های رمزگذاری شده gpg را نیز سرقت کند. همچنین پسوندهای "acid*" که توسط این بدافزار سرقت می‌شود به نرم‌افزار طبقه‌بندی اسناد محرمانه "Acid Cryptofiler" که توسط نهادهای مختلفی از جمله اتحادیه اروپا و ناتو استفاده می‌شود، تعلق دارد. اطلاعات به سرقت رفته از سیستم‌های آلوده، شامل اسنادی با پسوندهای زیر است:

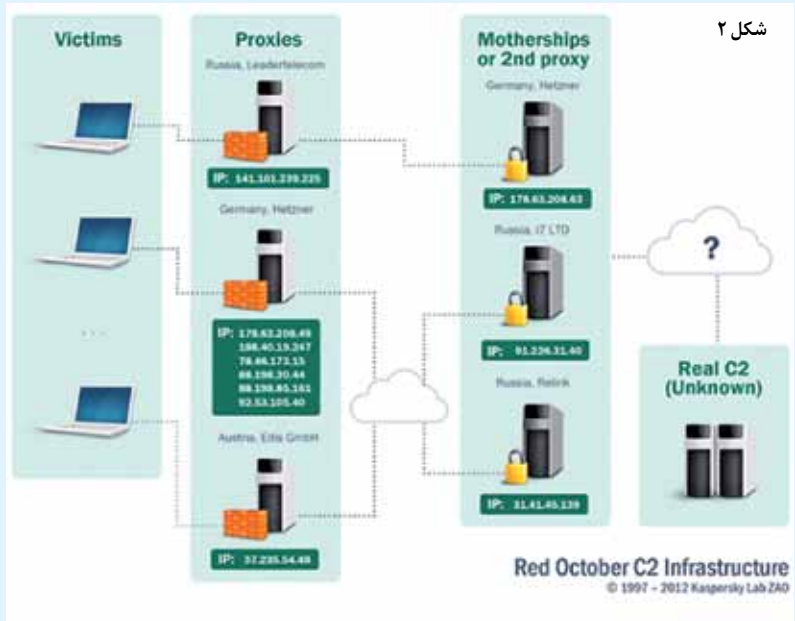
txt, csv, eml, doc, vsd, sxw, odt, docx, rtf, pdf, mdb, xls, wab, rst, xps, iau, cif, key, crt, cer, hse, pgp, gpg, xia, xiu, xis, xio, xig, acidcsa, acidsca, aciddsk, acidpvr, acidppr, acidssa.

اطلاعات به سرقت رفته از قربانیان، اطلاعات سطح بالا و طبقه‌بندی شده ای بوده و شامل داده‌های جغرافیایی سیاسی است که می‌تواند توسط دولت‌های ملی مورد استفاده قرار گیرد. اگر چه هنوز چگونگی استفاده از این اطلاعات همچون یک معما، ناشناخته مانده و فرآیند جمع‌آوری اطلاعات در طول پنج سال گذشته، دامنه کاملا گسترده‌ای را در برداشته است، اما این امکان وجود دارد که اطلاعات گردآوری شده، به صورت مخفیانه و زیرزمینی، در بازار سیاه به بالاترین پیشنهاد فروخته می‌شده یا بعضی از آنها، به صورت مستقیم، مورد استفاده قرار می‌گرفته است. زیرساخت سرورهای کنترل و دستور بدافزار Rocra، درواقع زنجیره‌ای از سرورهایی است که به عنوان پروکسی برای پنهان نمودن محل واقعی سرورها عمل می‌کنند. این سیستم بسیار پیچیده، در برابر تصاحب سرورهای کنترل و دستور، مقاوم بوده و به مهاجمان برای بهبود دسترسی به دستگاه‌های آلوده با استفاده از کانال‌های ارتباطی جایگزین، اجازه می‌دهد. در شکل ۲، یک نمای کلی از زیرساخت سرورهای کنترل و دستور Rocra که در تحقیقات کسپرسکی به دست آمده، نشان داده می‌شود.

تغییرات در سیستم

فایل (های) زیر ممکن است در سیستم آلوده دیده شود:

- %ProgramFiles%\WINDOWS NT\msc.bat



شکل ۲

- %ProgramFiles%\WINDOWS NT\[RANDOM CHARACTERS FILE NAME].lt
- %ProgramFiles%\WINDOWS NT\Svchost.exe

انتشار

این بدافزار می‌تواند خود را در سراسر یک شبکه محلی با استفاده از اعتبارهای مدیر شبکه که قبلا آنها را به دست آورده است، تکثیر کند. آسیب‌پذیری‌های ذکر شده نیز نقش مهمی در انتشار بدافزار Rocra بر عهده دارند.

نصب

بدافزار Rocra با سوءاستفاده از آسیب‌پذیری‌های از پیش شناخته شده زیر عمل می‌کند:

- Microsoft Excel 'FEATHEADER' Record Remote Code Execution Vulnerability (CVE-2009-3129) – MS Excel
- Microsoft Office RTF File Stack Buffer Overflow Vulnerability (CVE-2010-3333) – MS Word
- Microsoft Windows Common Controls ActiveX Control Remote Code Execution Vulnerability (CVE-2012-0158) – MS Word
- Oracle Java SE Rhino Script Engine Remote Code Execution Vulnerability (CVE-2011-3544) – Oracledb

این آسیب‌پذیری‌ها به نام‌های زیر نیز شناخته می‌شود:

- Bloodhound.Exploit.306
- Bloodhound.Exploit.366
- Bloodhound.Exploit.457
- Trojan.Maljava
- Trojan.Maljava!gen27

حملات اولیه‌ای که در سال‌های ۲۰۱۰ و ۲۰۱۱ انجام گرفته، از کد مخرب MS Excel استفاده کرده است و حملات صورت پذیرفته در تابستان سال ۲۰۱۲ از آسیب‌پذیری‌های موجود در MS Word بهره‌مند شده است.

این کدهای مخرب اسناد، در حملات فیشینگی که در طول حملات سایبری مختلف علیه فعالان تبتی، اهداف نظامی و بخش‌های انرژی در آسیا مورد استفاده قرار گرفته‌اند توسط سایر مهاجمان ایجاد شده‌اند. تنها چیزی که در این میان تغییر کرده است کدهای اجرایی جاسازی شده در سندهاست که مهاجمان آن را با کد خود جایگزین کرده‌اند.

شرکت امنیتی F-Secure نیز در وبلاگ امنیتی‌اش اعلام کرده است که مهاجمان از کدهای مخرب قدیمی شناخته شده نرم‌افزارهای Word، Excel و Java استفاده کرده‌اند و نشانه‌ای از آسیب‌پذیری‌های بسیار محرمانه (0-day) بهره‌برداری شده توسط آنها وجود ندارد.

بدافزار Rocra با حمله مهندسی اجتماعی و ترغیب به کلیک روی لینک‌های جعلی که معمولا تبلیغ ثبت نام در خرید یک ماشین لوکس است، فعالیت خود را آغاز می‌کند. شکل ۳، نمونه یک تصویر جعلی است که در حملات فیشینگ، توسط این بدافزار استفاده می‌شود:

همچنین این بدافزار همان طور که در شکل هفت نشان داده شده است، با ارسال یک نامه الکترونیکی که دربردارنده فایل ضمیمه مخرب است و تشویق به دانلود و بازکردن این فایل ضمیمه، اقدام به آلوده کردن سیستم‌ها می‌کند:

سپس مهاجمان یک ماژول را برای اسکن شبکه محلی و جست‌وجوی سیستم‌های آسیب‌پذیر در آن شبکه مستقر کرده، میزبان آسیب‌پذیر برای MS08-067 را یافته (کد مخرب آسیب‌پذیری توسط کرم کانفیکر) یا با اعتبارهای مدیر از پایگاه داده رمز عبور خود، توانایی دسترسی روی سیستم‌های آسیب‌پذیر را پیدا می‌کنند. هنگامی که یکی از این اسناد باز می‌شود، فعالیت رسمی بدافزار آغاز می‌شود و می‌تواند بدافزارهای بیشتری را تحت یک روش که به "قطره چکان تروجان" معروف است، از سرورهای کنترل و دستور خود دریافت کند. این بدافزارهای ثانویه، شامل برنامه‌های جمع‌آوری داده‌ها و ارسال اطلاعات به مهاجمان است. یکی از دستوراتی که در قطره چکان تروجان وجود دارد، می‌تواند کد صفحه سیستم آلوده را به ۱۲۵۱ قبل از زمان نصب و راه‌اندازی، تغییر دهد که این امر، نیازمند آدرس فایل‌ها و دایرکتوری‌هایی است که کاراکترهای سیریلیک (Cyrillic) را در نام‌های خودشان دارند. پس از این آلودگی اولیه، بدافزار توسط خودش در سراسر شبکه، انتشار یافته و مهاجمان در چند روز، فقط اطلاعاتی را در مورد آن شبکه جمع‌آوری می‌کنند. در طول این مدت، اقدام به شناسایی سیستم‌های کلیدی کرده و سپس ماژول‌هایی را در شبکه مستقر می‌کند که می‌تواند سایر رایانه‌ها را با خود همگام و همسو کند. یکی از این ماژول‌ها نیز برای جمع‌آوری اطلاعات به میزبان‌های راه دور آلوده در همان شبکه مورد استفاده قرار می‌گیرد. در تحقیقات انجام گرفته توسط کسپرسکی، بیش از یکهزار ماژول متعلق به ۳۰ دسته‌بندی از ماژول‌های مختلف، کشف شده که بین سال‌های ۲۰۰۷ تا جدیدترین آنها که در هشت ژانویه ۲۰۱۳ ایجاد شده‌اند. در جدول ۲، لیستی از این ماژول‌های شناخته شده و دسته‌بندی آنها آورده شده است:

شکل ۳

Rocra دارای ماژول‌های سفارشی خاصی است که برای هر قربانی، با یک ID منحصربه‌فرد ایجاد شده و برخلاف سایر بدافزارهای سایبری، می‌توان آن را دارای ظرافت خاصی دانست که برای قربانیان مخصوص، شخصی‌سازی شده است. چندین ماژول تلفن همراه نیز برای این بدافزار طراحی شده که اقدام به سرقت اطلاعات از انواع مختلف دستگاه‌های تلفن همراه همچون آیفون، نوکیا و ویندوز موبایل می‌کند. این ماژول‌ها در سیستم، نصب می‌شود و برای اتصال دستگاه‌های تلفن همراه به سیستم قربانی، منتظر می‌ماند و هنگامی که یک اتصال تلفن همراه، شناسایی شد، ماژول شروع به جمع‌آوری داده‌ها از آن تلفن همراه می‌کند. به طور کلی، چارچوب اصلی Rocra برای اجرای "وظایف" توسط سرورهای کنترل و دستور آن طراحی شده است. بسیاری از این وظایف که به عنوان کتابخانه‌های PE DLL از سرور دریافت می‌شود، در حافظه سیستم قربانی اجرا شده و سپس بلافاصله دور انداخته می‌شود. با این وجود، چند کار باید به صورت مداوم در سیستم انجام شود؛ مثلا انتظار برای اتصال دستگاه‌های تلفن همراه. این وظایف به عنوان فایل‌های PE EXE ایجاد شده‌اند که در سیستم آلوده نصب می‌شود. نمونه‌هایی از وظایف "مداوم" شامل مواردی به این شرح است:

- هنگامی که یک درایو USB به سیستم آلوده متصل می‌شود، عمل جست‌وجو توسط بدافزار آغاز می‌شود و فایل‌ها توسط ماسک/فرمت، از آن درایو USB استخراج می‌شود که می‌تواند شامل فایل‌های پاک شده نیز باشد. فایل‌های پاک شده با استفاده از یک تجزیه کننده فایل سیستم ساخته شده، بازیابی می‌شود.
- منتظر می‌ماند تا یک دستگاه تلفن آیفون یا یک گوشی نوکیا به سیستم آلوده وصل شود. پس از اتصال، اطلاعاتی در مورد تلفن، دفترچه تلفن آن، لیست تماس، تاریخچه تماس‌ها، تقویم، پیام‌های SMS و تاریخچه وب‌گردی بازیابی می‌کند.
- منتظر می‌ماند تا یک دستگاه تلفن همراه دارای ویندوز موبایل به سیستم آلوده وصل شود. پس از اتصال، تلفن را با یک نسخه تلفن همراه که از اجزای اصلی Rocra است، آلوده می‌کند.
- منتظر می‌ماند تا یک فایل خاص مایکروسافت آفیس یا سند PDF باز شود تا یک بسته محدود شده را در آن سند اجرا کند. همچنین یک راه مخفیانه ارتباطی را اجرا می‌کند که می‌تواند برای بازگردادن کنترل سیستم آلوده، مورد استفاده قرار گیرد.
- تمامی کلیدهای فشرده شده روی صفحه کلید را ثبت و تصاویر فوری از آنها ایجاد می‌کند.
- ماژول‌های اضافی رمزگذاری شده را با توجه به برنامه از پیش تعیین شده، اجرا می‌کند.
- پیام‌ها و ضمیمه‌های نامه‌های الکترونیکی را از نرم‌افزار مایکروسافت Outlook و از سرویس دهنده پست الکترونیکی مورد دسترس، با استفاده از اعتباری که قبلا به دست آورده است، بازیابی می‌کند.

نمونه‌هایی از وظایفی که "یک بار" اجرا می‌شوند نیز عبارتند از:

- جمع‌آوری اطلاعات کلی محیط‌های نرم‌افزاری و سخت‌افزاری.
- جمع‌آوری فایل سیستم و اطلاعات به اشتراک گذاشته شده در شبکه، ایجاد لیست‌های دایرکتوری، جست‌وجو و بازیابی فایل‌ها توسط ماسک ارایه شده توسط سرور کنترل و دستور بدافزار.
- جمع‌آوری اطلاعات در مورد نرم‌افزارهای نصب شده که مهم‌ترین آنها شامل پایگاه داده اوراکل، برنامه RAdmin، نرم‌افزار سرویس گیرنده پست الکترونیکی از جمله نسخه کلاینتی Mail.Ru، درایوها و نرم‌افزارهای ویندوز موبایل، نوکیا، سونی اریکسون، اچ‌تی‌سی، تلفن‌های آندروییدی و درایوهای USB است.
- استخراج تاریخچه وب‌گردی از مرورگرهای کروم، فایر فاکس، اینترنت اکسپلورر و اپرا.
- استخراج کلمات عبور ذخیره شده وب‌سایت‌ها، سرورهای FTP، پست الکترونیکی و حساب‌های کاربری سرویس دهنده‌های پست الکترونیکی.
- استخراج هش‌های حساب‌های کاربری ویندوز، به احتمال زیاد برای کرک نمودن آفلاین آنها.
- استخراج اطلاعات حساب کاربری نرم‌افزار Outlook؛
- تعیین آدرس IP خروجی سیستم آلوده (به منظور ارتباط با اینترنت).
- دریافت فایل از سرورهای FTP که از طریق سیستم آلوده، در دسترس هستند (شامل آنهایی که به شبکه محلی خود متصل هستند) با استفاده از اعتباری که قبلا به دست آورده است.
- نوشتن و/یا اجرای کدهای دلخواه در داخل وظیفه (task).
- اسکن شبکه، روگرفت از اطلاعات پیکربندی دستگاه‌های سیسکو، در صورت موجود بودن.
- اسکن شبکه در یک محدوده از پیش تعریف شده و تکثیر خود به ماشین‌های آسیب‌پذیر، توسط آسیب‌پذیری MS08-067.
- تکثیر از طریق شبکه با استفاده از اعتبارهای مدیر شبکه که آنها را قبلا به دست آورده است.

جلوگیری

اگرچه هم‌اکنون تمامی آنتی‌ویروس‌ها قادر به شناسایی و پاک کردن Rocra هستند، اما انجام فعالیت‌هایی توسط مدیران و کاربران سیستم می‌تواند باعث جلوگیری و یا کاهش خطر این بدافزار شود. از جمله:

- غیرفعال کردن ویژگی AutoRun یا AutoPlay سیستم برای جلوگیری از اجرای خودکار فایل‌های قابل اجرا در درایوهای قابل جابه‌جایی.
- غیرفعال کردن درایوهای قابل جابه‌جایی از طریق Setup سیستم. در صورت نیاز، فقط حالت read-only را فعال کرده و حتما یک رمز عبور هم برای setup در نظر گرفت.
- اصلاح نقاط آسیب‌پذیر سیستم عامل و نرم‌افزارهای نصب شده، به خصوص برنامه‌هایی که این بدافزار از آسیب‌پذیری‌های موجود در آنها بهره می‌برد.
- به‌روزرسانی نرم‌افزار ضدویروس در فاصله‌های زمانی کوتاه‌مدت و فعال کردن گزینه به‌روزرسانی خودکار برای دریافت خودکار آخرین به‌روزرسانی‌ها؛
- دسترسی به آدرس‌هایی که سرورهای کنترل و دستور این بدافزار هستند باید با استفاده از فایروال و مسیریاب، مسدود شده و با اضافه کردن به فایل local hosts به آدرس ۱۲۷.۰.۰.۱ تغییر مسیر داده شوند.
- استفاده از رمز عبور پیچیده که ترکیبی از عدد، حروف بزرگ و کوچک و نمادها است برای کلمه عبور کاربران، به نحوی که این رمزها توسط حملات دیکشنری به راحتی قابل شناسایی و کشف نبوده و در عین حال، برای کاربران هم به یاد ماندنی باشد.
- همه ارتباطات ورودی از اینترنت به سرویس‌های سازمان که نباید در دسترس عموم باشد را با استفاده از فایروال، غیر فعال کرده و تنها به سرویس‌هایی اجازه دهید که به مردم خدمات ارایه می‌دهند.
- هرگز نباید با یوزر administrator یا root به سیستم login کرد. کاربران و برنامه‌ها هم باید پایین‌ترین سطح دسترسی لازم را داشته باشند.
- غیرفعال کردن اشتراک‌گذاری منابع و فایل‌ها در شبکه اگر به اشتراک‌گذاری آنها نیازی نیست. در صورت نیاز، از لیست‌های کنترل دسترسی استفاده کرده و مشخص نمایید که چه افراد یا کامپیوترهایی اجازه دسترسی به آنها را دارند.
- غیرفعال کردن و حذف سرویس‌های غیرضروری فعال در سیستم. اگر هم کد مخربی علیه یکی از سرویس‌ها پیدا شد، تا زمانی که وصله امنیتی آن سرویس در سیستم نصب نشده است، آن سرویس را غیرفعال کرده و یا دسترسی به آن را محدود کنید.

№	Name	Group			Size (Kb)	Summary
1	RegConn	Recon			~160	Query system software environment
2	WinHttp	Recon		A	~142	Get external IP and send to the C&C
3	SysInfo	Recon		A	~503	Get browser history, usb drives, processes, disks,...
4	GetWebFtp	Recon			~157	Get browser history, http/ftp credentials
5	AuthInfo	Recon		A	~660	Get file manager, browser, ftp, mail client credentials
6	Logic	Recon			~160	Get general information about current Windows machine and available remote network shares
7	ILogic	Recon			~150	Grab Internet Explorer URL history from the local system
8	Repeat2	Recon			~150	Get listing from remote shares available in Windows network neighborhood
9	Reference	Recon			~150	Grab directory/file listings of all drives attached to the local system
10	PswSuperMailru	Password			230-260	Steal Mail.ru account info and Outlook attachments
11	PswOutlook	Password			~31	Steal Outlook account info
12	MSHash	Password			400-550	Steal Windows account hashes
13	MAPIClient	Email			418-440	Steal e-mail data using local MAPI
14	POP3Client	Email			1100-1200	Steal e-mail data from POP3 server
15	USBContainer	USB drive			649-690	Loads and runs embedded USBStealer
16	USBRestore	USB drive			372-376	Recover and steal deleted files on USB drives
17	USBStealer	USB drive			448-504	Steal interesting files from USB drives
18	Keylogger	Keyboard			300-312	Makes screenshots, records keystrokes
19	Scheduler	Persistence			~620	Run various tasks from spec folders
20	DocBackdoor	Persistence			75-88	Runs an embedded module from MSOffice/PDF doc
21	OfficeBDInstaller	Persistence		A	~286	Installs DocBackdoor plugin in MS Office
22	AdobeBDInstaller	Persistence		A	~218	Installs DocBackdoor plugin in Adobe Reader
23	FilePutExec	Spreading		A	~305	Extract and run an embedded file locally or remotely
24	Netscan	Spreading		A	~315	Port scanner, vuln. scanner, Cisco cfg dumper
25	MSExploit	Spreading		A	~1200	Infect target host using MS08-067 exploit
26	DASvcInstall	Spreading		A	~276	Infect target host using admin credentials
27	Frog	Spreading		A	~102	Initial backdoor, used in MSExploit/DASvcInstall
28	iPhone	Mobile			329-331	Steals data from locally attached iPhone
29	Nokia	Mobile			~337	Steals data from locally attached Nokia phone
30	Winmobile	Mobile			~400-700	Infect locally attached Windows Mobile phones with a native backdoor/updater modules
31	Winmobile	Mobile			~7-100	Native mobile backdoor/utilites
32	WinFtpScan	Exfiltration		A	~209	Steals files from local FTP server
33	GetFileReg	Exfiltration		A	~340	Steals files from local/network disks
34	FileInfo	Exfiltration		A	339-340	Uploads various collected files to the C&C

- "online" module: all data is sent to the C&C; no local files created;
- "offline" module; no network communication; all data is stored locally;
- module with embedded script/config in resource named "AAA";
- module with all values hardcoded.

جدول ۲

- سرویس‌هایی همچون HTTP، FTP، Mail و DNS مهم‌ترین سرویس‌های یک شبکه متصل به اینترنت هستند. بنابراین، همیشه وصله‌های امنیتی این سرویس‌ها را مهم در نظر گرفته و به روز نگهدارید. همچنین توسط فایروال، دسترسی به آنها را کنترل کنید.
- پیکربندی سرویس دهنده پست الکترونیک در راستای حذف نامه‌های الکترونیکی که حاوی فایل ضمیمه است. از این فایل‌ها برای گسترش تهدیدهایی همچون .pif، .exe، .bat، .vbs و .scr استفاده می‌شود.
- کامپیوترهای آلوده را به سرعت برای جلوگیری از گسترش بیشتر آلودگی در شبکه ایزوله کنید و تا زمانی که از برطرف شدن آلودگی مطمئن نشده‌اید، آنها را وارد شبکه نکنید.
- استفاده نکردن از بلوتوث در شبکه. در صورت نیاز، دید دستگاه را در حالت پنهان تنظیم کنید تا توسط دستگاه‌های دیگر پیدا نشده و حتما از رمز عبور نیز برای برقراری ارتباط بین دستگاه‌ها استفاده کنید.

پیشگیری

پیشگیری از حوادث و کنترل امنیت سیستم نیاز به یک رویکرد چند لایه دارد که از آن با عنوان "دفاع در عمق" یاد می‌شود. این لایه، شامل سیاست‌ها و رویه‌ها، آگاهی و آموزش، تقسیم‌بندی شبکه، کنترل دسترسی‌ها، اقدام‌های امنیتی فیزیکی، سیستم‌های نظارتی همچون فایروال و ضد ویروس، سیستم‌های تشخیص و جلوگیری از نفوذ، رمز کاربری و غیره است.

بهترین روش برای پیشگیری هم معمولا تجزیه و تحلیل خطر، شناسایی نقاط آسیب‌پذیر سیستم‌ها و شبکه، کنترل سیستم ارزیابی امنیتی و همچنین توسعه برنامه‌های اولویت‌بندی برای از بین بردن یا به حداقل رساندن ریسک خطر است.

منابع:

- www.symantec.com/security_response
- www.securelist.com
- کتاب امنیت اطلاعات، محمدمهدی واعظی‌نژاد، ۱۳۹۱