آذر
۹۳

مجله

امنیت اطلاعات

شماره هفتم

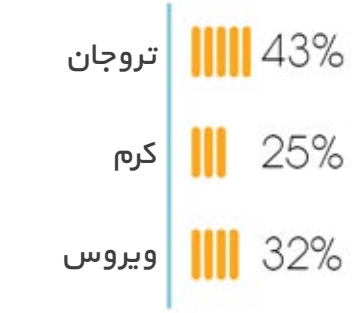
یک کاغذ سفید را هر چقدر هم که سفید و تمیز باشد
کسی قاب نمی‌گیرد
برای ماندگاری باید
حرفی برای گفتن داشت

در این شماره خواهید خواند:
پادویش و بررسی انواع آسیب ها در ۶ماه ابتدای سال ۹۳
اهداف BlackEnergy در سال ۲۰۱۴
آزمون نفوذپذیری، حفظ دسترسی ایجاد شده به سیستم هدف
توسعه نرم افزار به روش اسکرام - قسمت اول
انتشار کد بدافزار BadUsb
هک دستگاههای ATM با بدافزار Tyupkin
استرالیایی ها در چنگ Cryptomalware ها
آسیب پذیری "Shellshock"
بدافزار رجین را بشناسید!

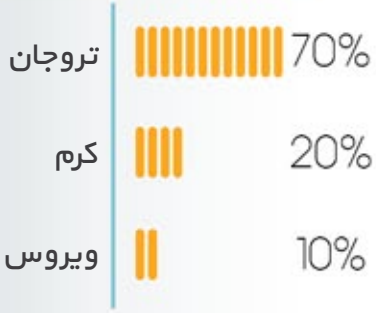
پادویش و بررسی انواع آسیب ها
در ۶ماه ابتدای سال ۹۳

پادویش
ضدویروس
امنیت پیشرفته

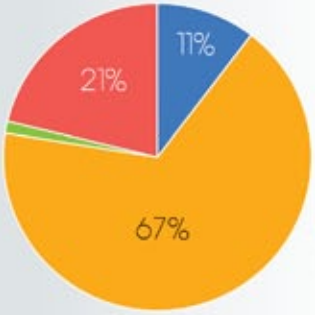
میزان شیوع بدافزارها در سیستم کاربران



تعداد بدافزارهای منحصر به فرد شناسایی شده



توزیع سیستم عامل های کاربران
به همراه جدول پرتعداد ترین بدافزارها



فراوانی نصب پادویش در سیستم عامل های مختلف

Windows 8
Windows XP
Windows 7
Other

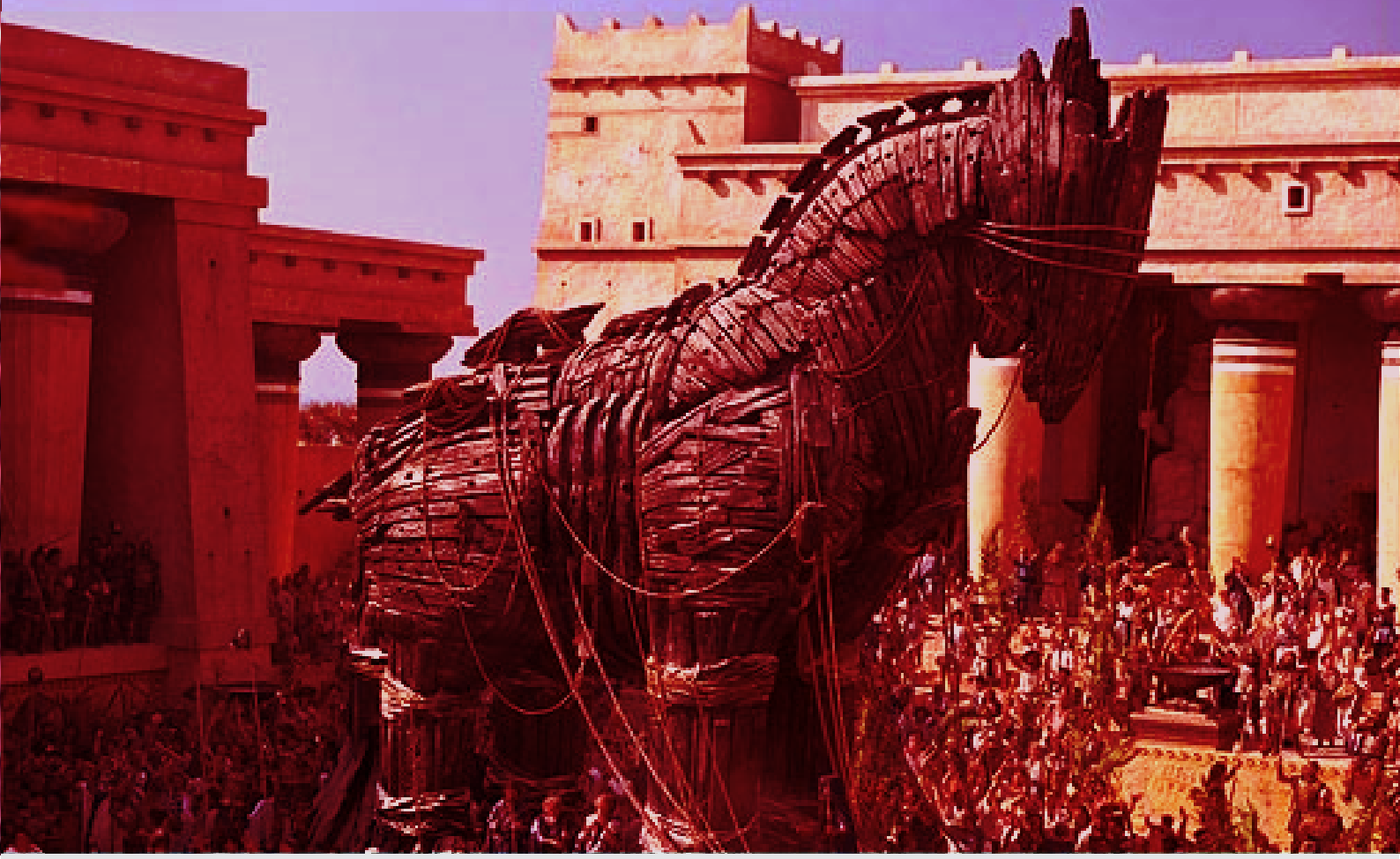
Top Malware

Worm.Win32.Gamarue
Downloader.Win32.Gamarue
USBWorm.Win32.Gamarue
Worm.Win32.AutoRun
Worm.Win32.Debris
Virus.Win32.Virut
Virus.Win32.Sality

توزیع شایع ترین آسیب پذیری ها
به همراه جدول پرتعداد ترین رخنه گرها

Top Exploits

Malware.Exploit.PDF-2012.231821
Exploit.CVE-2010-2568.f.1405092
Exploit.SWF.CVE-2011-0611.z.7465807
Virus.DOS.Explosion.a.3846139
Exploit.Nuker.pksxl.31265
Exploit.CAN.rpelf.30443



اهداف BlackEnergy در سال ۲۰۱۴

بسیاری از سازمان‌ها، شرکت‌های خصوصی و بخش‌های مختلف صنعتی، مورد هدف نرم افزارهای مخرب کشف شبکه و اجرای کد از راه دور و جمع‌آوری اطلاعات از دیسک‌های سخت می‌باشند. نکته قابل توجه در برخی از این نوع حمله‌ها این است که باگذشت زمان وضعیت ژئوپولیتیک آن‌ها در منطقه تغییر می‌کند. از معروف ترین این نوع بدافزارها می‌توان BlackEnergy را نام برد که دارای مکانیسم انتشار متفاوتی بر روی سیستم‌های قربانیان می‌باشد.

طبق نتایج به‌دست آمده، BlackEnergy یک تروجان است که دستخوش تغییرات عملکردی مهمی است. در ابتدا به عنوان یک تروجان DDoS نسبتاً ساده بود اما با گذشت زمان آن را به شکل نرم افزارهای مخرب تکامل یافته که دارای ساختار ماژولار هستند، یافتند. درواقع به عنوان یک ابزار مفید جهت فرستادن و نیز برای تقلب‌های آنلاین در بانک به کار می‌آید. نسخه‌ی دوم BlackEnergy دارای تکنیک‌های روتکیتی بود؛ در این سطح که درایورهای سطح کرنل برای تزریق در پروسس‌های کاربر استفاده می‌شد.

گونه‌های جدید به نام (BlackEnergy Lite) از ابتدای سال ۲۰۱۴ پیدا شده‌اند؛ این نمونه‌ها، بدون اجزاء درایور سطح کرنل هستند، از پلاگین‌ها پشتیبانی کمتری می‌کنند و درکل پیچیدگی و عملکرد خرابکارانه سبک تری دارند. نمونه‌های شناخته شده از BlackEnergy اصلی که در سال جاری تکامل یافته‌اند شامل عملکرد روتکیتی برای پنهان سازی objectهای سیستم نیستند و فقط از درایور خود در سطح کرنل برای تزریق در پردازه‌های سطح کاربر استفاده می‌کنند. گونه‌های سبکتر(Lite) حتی استفاده از این درایور را نیز ندارند. در عوض dll اصلی از تکنیک‌های استانداردتر و معروفتری مانند اجرای ساده‌تر توسط rundll32.exe استفاده می‌کند. دلایل مختلف دیگری برای جداکردن BlackEnergy Lite از BlackEnergy اصلی وجود دارد مانند چارچوب پلاگین، ذخیره سازی پلاگین، فرمت پیکر بندی و غیره.

از زمانی که اولین نسخه BlackEnergy شناسایی شد تا کنون این گونه بدافزار با اهداف مختلفی مانند حملات DDoS، توزیع هرزنامه، کلاه‌برداری بانکی و غیره شیوع پیدا کرده است. این اهداف توسط پلاگین‌های استفاده شده و حملات انتشار پیگیری شده‌اند. هدف این پلاگین‌ها عمدتا کشف شبکه‌ها و اجرای کد از راه دور برای جمع آوری اطلاعات از هارد دیسک قربانیان است. درحملات انتشار بدافزار از تکنیک‌های مختلفی مانند متد آلوده‌سازی از طریق بهره‌برداری از آسیب‌پذیری نرم‌افزارها، مهندسی اجتماعی، فیشینگ ایمیل‌ها و استفاده از اسناد به عنوان طعمه و یا هر دوی آن‌ها استفاده می‌شود.

در ماه آپریل ۲۰۱۴ نسخه ای از این بدافزار به صورت Exploit در Microsoft Word دیده شد (استفاده از آسیب‌پذیری CVE-2014-1761). در نتیجه Exploit شدن کد مخرب، دو فایل در شاخه temp ایجاد می‌شود: یک فایل مخرب با نام "WinWord.exe" و یک سند طعمه با نام "Russian ambassador to Conquer World.doc". این دو فایل توسط تابع Kernel32.WinExec اجرا می‌شوند. فایل "WinWord.exe" برای اجرای دراپر بدافزار BlackEnergy lite به کار می‌رود و محتوای سند طعمه شامل یک متن بحث برانگیز ساختگی است.

یک ماه بعد، فایل دستکاری شده دیگری با نام روسی با ترجمه "Password List" مشاهده شد که برای نصب BlackEnergy Lite ساخته شده بود. این بار هیچ exploitی همراه با فایل، استفاده نشده بود و تنها یک فایل اجرایی ساده با آیکن Microsoft Word بود.

در یک مورد اسناد پاور پوینت دستکاری شده مورد استفاده قرار گرفت در حالی که به نظر می‌رسد تلاش‌های دیگری برای انتشار بدافزار از طریق آسیب پذیرهای ناشناخته جاوا و یا نرم‌افزار کنترل از راه دور Team Viewer در حال انجام باشد.

آزمون نفوذپذیری

حفظ دسترسی ایجاد شده به سیستم هدف

بخش هفتم

در شماره پیشین به بررسی فاز دسترسی سیستم و چگونگی انجام آن اشاره گردید. در این شماره حفظ دسترسی ایجاد شده مورد بررسی قرار می‌گیرد.

آزمون کننده، زمانی که به سیستم هدف دسترسی پیدا می‌کند، نیازمند حفظ این دسترسی می‌باشد؛ زیرا در صورتی که آسیب‌پذیری پیدا شده رفع گردد، دسترسی به سیستم هدف از بین خواهد رفت. همچنین در صورتی که سیستم هدف، دوباره راه‌اندازی گردد و یا ارتباط با شبکه قطع گردد، این اتفاق خواهد افتاد. به همین دلیل، باید از روشی استفاده نمود که بتوان از طریق آن از تمامی دیواره‌های آتش و یا لیست‌های کنترل دسترسی عبور نمود و دسترسی ثابت به سیستم هدف داشت؛ یکی از این روش‌ها، استفاده از Backdoor (در پشتی) می‌باشد که از طریق آن می‌توان از تمامی دیواره‌های آتش عبور نمود و دسترسی نامحدود از سیستم هدف به‌دست آورد.

یکی دیگر از مزیت‌های دسترسی سریع به سیستم هدف این است که زمانی که آزمون کننده به داخل شبکه هدف دسترسی پیدا می‌نماید، آزادی بیشتری به منظور پویش و حمله نمودن به سیستم‌ها وجود دارد زیرا معمولا سیستم‌های دفاعی تنها از حمله‌های خارجی جلوگیری می‌نمایند.

یکی از ابزارهایی که می‌توان در این فاز از آن استفاده نمود، Netcat می‌باشد. این ابزار یک ارتباط بین دو سیستم برقرار می‌نماید. این ابزار به‌گونه‌ای است که به دو صورت سمت سرور و سمت کلاینت قابل استفاده می‌باشد. بدین صورت که هم می‌توان یک ارتباط که دسترسی خط فرمان به سیستم فراهم می‌نماید، ایجاد نمود و هم می‌توان به‌گونه‌ای استفاده گردد که بتوان ارتباطات سیستم در دسترس قرار گرفته را استراق سمع نماید.

اما تمامی فعالیت‌هایی که با Netcat انجام می‌گیرد قابل شناسایی توسط IDSها می‌باشد، بنابراین به منظور جلوگیری از شناسایی شدن، راه‌اندازی یک تونل رمزنگاری شده مانند SSH لازم می‌باشد. از این طریق می‌توان، بدافزار و یا اکسپلویت های دیگری را در سیستم قربانی بدون اینکه شناسایی گردند، نصب و اجرا نمود؛ زیرا ترافیک بین سیستم حمله کننده و سیستم قربانی رمزنگاری شده است.

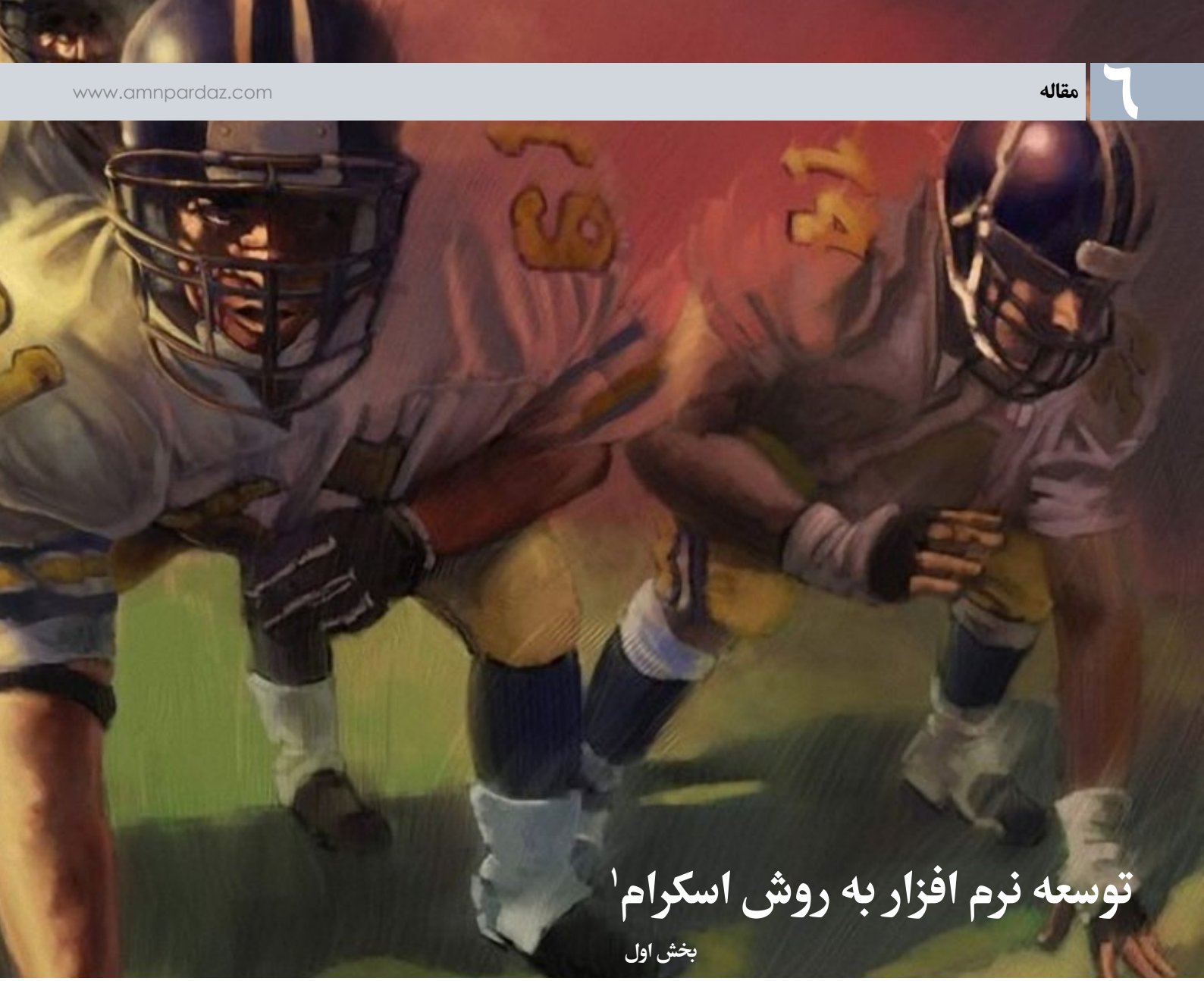
به غیر از SSH چندین روش و ابزار به منظور ایجاد یک کانال رمزنگاری شده وجود دارد که به شرح زیر است:

۱- CRYPTCAST: از الگوریتم رمزنگاری TWOFISH که یک رشته کلید متقارن است، استفاده می‌نماید.

۲- Matahari: با استفاده از این ابزار می‌توان یک ارتباط از سیستم حمله کننده برروی پورت ۸۰ ایجاد نمود.

۳- Proxytunnel: با استفاده از این ابزار می‌توان تمامی داده‌ها را از طریق پراکسی‌های HTTPS منتقل نمود.

بعد از حفظ دسترسی ایجاد شده، آزمون‌کننده نیازمند آن است که تمامی فعالیت‌های خود را بپوشاند، که در شماره بعد به بررسی این فاز پرداخته خواهد شد.



توسعه نرم افزار به روش اسکرام[1]

بخش اول

مقدمه

توسعه یك نرم‌افزار تنها نوشتن کدهای برنامه نیست بلکه چرخه‌ای از تمامی فرآیندها جهت ساخت نرم‌افزارها می‌باشد که این مراحل شامل جمع آوری نیازهای کاربران، طراحی، نوشتن کد و در آخر تست و کنترل کیفیت نرم‌افزار می‌باشد. با انتخاب یک متدولوژی مناسب، می‌توان روالی مناسب به منظور تولید نرم‌افزارهای کوچك و بزرگ به‌وجود آورد.

در سری مقالات "توسعه نرم افزار به روش چابک" به بررسی یکی از این متدلوژی ها به نام اسکرام پرداخته شده است. از آن جایی که هر پروژه نرم‌افزاری با دیگر پروژه‌ها متفاوت است، می‌توان گفت که فرآیند تولید آن پروژه نیز با دیگر پروژه‌ها تفاوت دارد. در نتیجه انتخاب این روش‌ها رابطه مستقیمی با اندازه‌ی گروه در پروژه دارد و توسعه‌ی نرم‌افزارهای مختلف نیاز به رویه‌های تولید متفاوت دارند. اسکرام یکی از متدولوژی های توسعه‌ی چابک است که در این متدولوژی خواسته‌های مشتری از محصول، اولویت بندی شده و تاکید آن بر روی انجام درخواست‌های مشتری با اولویت بالاتر است. در شماره اول این مقاله، ابتدا تاریخچه پیدایش متدولوژی اسکرام به طور کامل معرفی می‌شود. سپس در شماره‌های بعد نقش افراد و تیم توسعه در این متدولوژی تشریح، جلسه های مختلف آن بررسی وابزارهایی که در آن به کار می‌روند معرفی می‌گردند.

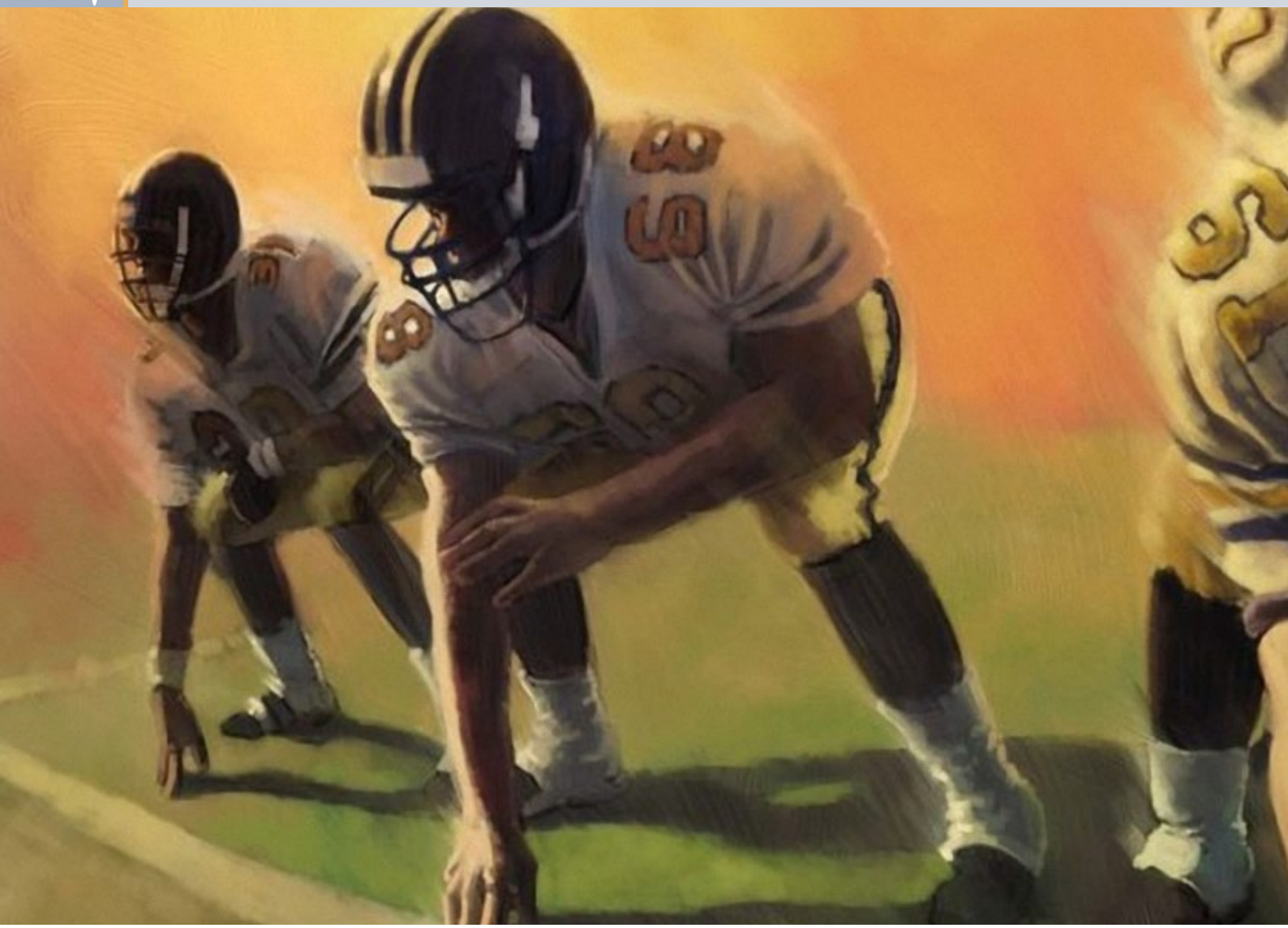
تاریخچه اسکرام

سال‌ها قبل از اینکه اسکرام به عنوان یکی از محبوب‌ترین اعضای خانواده توسعه نرم‌افزارهای چابک مطرح باشد، توسط پروفسور هیروتاکا تاکئوچی[2] تدوین شده بود. آقای تاکئوچی، که علاوه بر تدریس در مدرسه کسب و کار هاروارد (HBS) یکی از ۱۰ پروفسور برتر در حوزه‌ی کسب و کار به انتخاب BusinessWeek است، از اسکرام به عنوان "یک استراتژی منعطف و جامع برای توسعه محصول که در آن تمامی تیم‌های توسعه به عنوان یک واحد برای رسیدن به هدف مشترک عمل می‌کنند" نام برده بود. این اولین تعریف از مفهوم اسکرام در سال ۱۹۸۶ در حوزه‌ی توسعه محصول است.

در اوایل دهه ۹۰، آقای کن شوئیبر اقدام به پیاده سازی و توسعه آنچه بعدها به نام فرآیند اسکرام شناخته شد، در شرکت خود کرد. کن شوابر[3] چند سال بعد، به همراه آقای جف سادرلند[4] برای اولین بار فرآیند توسعه نرم‌افزار اسکرام را در کنفرانس OOPSLA سال ۱۹۹۵ معرفی کردند. کن شوابر در سال ۲۰۰۱ یکی از اعضای موثر ایجاد بیانیه چابکی (The Agile Manifesto) بود. جف سادرلند بخش‌های مهمی از این بیانیه را نوشت.

عرصه‌ی جدید توسعه محصولات جدید - ۱۹۸۶

در مقاله‌ای که در ژانویه سال ۱۹۸۶ در مجله Harvard Business Review تحت عنوان The New Product Development Game منتشر شد، هیروتاکا تاکئوچی و ایکوجیرو نوناکا[5] اولین قدم‌های معرفه بنیان اسکرام نهاده شد. در این مقاله، شش ویژگی روش توسعه محصول جدید که در آمریکا و ژاپن در حال استفاده بود، ارایه شده است که عبارتند از:



- بی ثباتی درونی - built-in instability
- تیم‌های پروژه خود سازمانده - self-organizing project teams
- فازهای توسعه هم پوشان - overlapping development phases
- یادگیری متداوم - multilearning
- کنترل نامحسوس - subtle control
- انتقال دانش سازمانی

این شش ویژگی، مانند اجزای یک پازل در کنار یکدیگر می‌توانند موجب ایجاد فرآیندهای توسعه‌ی محصول جدید منعطف و سریعی شوند که عامل تغییر در آن نه تنها بازدارنده نیست، بلکه در صورت استفاده‌ی درست می‌تواند تبدیل به ماشین خلاقیت و ایجاد ایده‌هایی مبتنی بر نیاز بازار شود.

تدوین چارچوب فرآیند اسکرام

پس از معرفی رسمی اسکرام از سوی سادرلند و شوابر در کارگاه Business Object Design and Implementation که بخشی از رویداد OOPSLA 95' در شهر آستین بود، این دو نفر تلاش کردند تا این فرآیند را به عنوان روشی که امروزه به نام اسکرام می‌شناسیم به صنعت نرم‌افزار معرفی کنند. در سال ۲۰۰۱، شوابر به همراه مایک بیدل[۶]، در کتاب Agile Software Development with Scrum اسکرام را به صورت مکتوب به عنوان یکی از روش‌های توسعه چابک معرفی کردند. هر چند اسکرام مخفف کلمه‌ی خاصی نیست، و بیشتر به خاطر اشاره شوابر به بازی راگبی است که افراد برای به دست آوردن توپ نهایت تلاش خود را کرده و پس از رسیدن به آن تا مقصد با تکنیک ها و مهارت هایی که تا کنون کسب کرده اند. توپ (هدف) را به شکل درست تا رسیدن به مقصد هدایت می‌کنند. برخی شرکت‌ها هنگام نوشتن این کلمه از حروف بزرگ (SCRUM) استفاده می‌کنند.

در سال‌های بعد، Scrum Alliance متولی توسعه‌ی اسکرام و همچنین برنامه‌های آموزشی و اعتبار سنجی مانند Certified Scrum Master بود. در سال ۲۰۰۹، Ken به عنوان یکی از اعضای اصلی Scrum Alliance این گروه را ترک کرد و با راه‌اندازی scrum.org تلاش کرد تا اصالت روش اسکرام را حفظ کند و آن‌را توسعه دهد.

در شماره بعد به توضیح درباره نقش‌ها و وظایف افراد تیم در اسکرام پرداخته می‌شود.

---

۲. Hirotaka Takeuchi
۳. Ken Schwaber
۴. Jeff Sutherland
۵. Ikujiro Nonaka
۶. Mike Beedle

انتشار کد بدافزار BadUsb
بدافزاری که درایو USB را به یک سلاح سایبری غیرقابل کشف تبدیل می‌کند

یک بار دیگر USB به عنوان یک تهدید برای تعداد زیادی از کاربران که از درایوهای USB استفاده می‌کنند، معرفی شد. محققان امنیتی مجموعه ای از ابزار هک را که می‌تواند به منظور تبدیل درایو USB به یک بدافزار استفاده شود، منتشر نموده اند. کد مربوط به این آسیب‌پذیری توسط محققان در وب سایت Github منتشر شده است. لازم به ذکر است که این آسیب پذیری برای مهاجمان، هکرها و تمامی‌افراد قابل دسترسی می‌باشد.
خبر خوب این است که این آسیب‌پذیری فقط در USBهای شرکت phison وجود دارد. اما خبر بد این است که اگر این USB به هر وسیله‌ای متصل گردد آن‌را تحت تاثیر قرار می‌دهد. این USB می‌تواند هر کامپیوتری را آلوده کند، اما هنوز مشخص نیست که آیا کامپیوتر آلوده می‌تواند هر USBای که به آن‌ها متصل شده است، را آلوده کند یا خیر.

آسیب‌پذیری "Shellshock"

"Shellshock" یا "Bash bug" آسیب‌پذیری جدید می‌باشد (CVE-2014-6271) که پتانسیل آسیب رساندن به تمامی‌ورژن‌های سیستم عامل‌های Unix ، Linux و Mac OS X را دارا می‌باشد. با استفاده از این آسیب‌پذیری و در صورت رخ دادن موفقیت آمیزexploit، مهاجم می‌تواند علاوه بر دزدی اطلاعات، کنترل کامل کامپیوتر قربانی را نیز به دست گیرد، همچنین پتانسیل دسترسی به دیگر کامپیوترهای موجود در شبکه قربانی توسط مهاجم، وجود دارد.
Bash در واقع به عنوان یک مفسر زبان دستورات می‌باشد، که به کاربر این امکان را می‌دهد تا دستورات خود را به صورت ساده و بر اساس متن در پنجره مربوطه وارد کند و سیستم عامل آن دستورات را اجرا نماید. علاوه بر آن Bash این امکان را فراهم می‌کند که برنامه‌های کاربردی برای اجرای دستورات خود از آن استفاده نمایند که این ویژگی Bash باعث آسیب‌پذیری بیشتر می‌شود و مهاجم می‌تواند از راه دور دستورات خود را اجرا کند.
لازم به ذکر است که شرایط خاص دیگری برای موفقیت exploit که استفاده از (Common Gateway Interface) CGI که یک سیستم برای ایجاد محتوای وب می‌باشد و به صورت بسیار گسترده ای استفاده می‌شود، نیاز است. مهاجم از CGI برای ارسال یک متغیر محیطی ناهنجار به یک وب سرور آسیب پذیر استفاده می‌کند. از آنجایی که سرور از Bash برای تغییر این متغیر استفاده می‌کند، منجر به اجرای دستورات مخرب می‌شود. علاوه بر کامپیوترها ، ابزارهای آسیب پذیر دیگری مثل Linux-based routerها که از CGI برای رابط وب خود استفاده می‌کنند نیز در معرض این خطر می‌باشند.

هک دستگاه‌های ATM با بدافزار Tyupkin

پول همواره یکی از انگیزه‌های مهم برای مجرمان رایانه ای بوده است که به این منظور مجرمان رایانه ای از روش‌های متفاوتی برای ربودن شماره‌ی کارت‌های اعتباری استفاده می‌نمودند. اما اکنون این مجرمان با استفاده از بدافزار Tyupkin توانستند مبالغی را بدون نیاز به کارت از دستگاه‌های خودپرداز دریافت نمایند.
به منظور نصب این بدافزار، مهاجمان نیاز به دسترسی فیزیکی به سیستم‌های خودپرداز که دارای نسخه ویندوز ۳۲ بیتی می‌باشند، دارند. براساس تحقیقات صورت گرفته این تهدید در چند ماه اخیر در کشورهای آسیایی، اروپا و آمریکای لاتین مشاهده شده است. هنوز هیچ جزییاتی در رابطه با باندی که در این حمله دست داشته است وجود ندارد، اما تاکنون میلیون‌ها دلار از دستگاه‌های خودپرداز دنیا به سرقت رفته است.
به منظور نصب این بدافزار مخرب، باید به صورت فیزیکی سی دی که شامل این بدافزار است در دستگاه قرار گیرد. زمانی که دستگاه دوباره راه اندازی شد، دستگاه خودپرداز تحت کنترل قرار خواهد گرفت. پس از نصب، این بدافزار در پشت صحنه در حال اجرا است و مهاجم می‌تواند با وارد نمودن دستورات از آن استفاده نماید. هم‌چنین، یک کلید تصادفی تولید می‌گردد که مهاجمان با دانستن الگوریتم تولید این کلید یک کلید جلسه تولید می‌کنند. زمانی‌که این کلید جلسه به درستی وارد شود، دستگاه خودپرداز تمامی جزییات مربوط به این‌که چه میزان وجه در هر دستگاه موجود است، نمایش می‌دهد.

استرالیایی ها در چنگ Cryptomalware ها

Cryptomalware یک نوع خاص از بدافزار می‌باشد که به رمزنگاری تمام فایل های اطلاعاتی سیستم قربانی پرداخته و سپس تلاش می‌کند تا با دریافت پول از قربانی، فایل های او را به حالت اولیه برگرداند. از انواع این بدافزارها می‌توان: Cryptowall و Cryptodefense را نام برد. از آنجایی که فایل های اطلاعاتی (سند، عکس و..) برای افراد ارزش بالایی دارد و فرد تمایل به بازیابی آن‌ها را دارد، بنابراین بسیار روش کارآمدی برای باج گیری بوده و در حال گسترش است.

این در حالی است که گسترش و تعداد حملات در استرالیا بسیار بارز بوده و حملات جدید توسط بدافزار cryptolocker صورت می‌گیرد. این نمونه توسط شبکه های اجتماعی بر اساس ایمیل گسترش داده می‌شود.

البته جزئیات حملات بر اساس منطقه جغرافیایی که در حال گسترش است، متفاوت می‌باشد. برای مثال در استرالیا مهاجم تلاش می‌کند تا خود را جای یک شرکت محلی، مثل: شرکت عرضه انرژی جهت پرداخت قبض ها و یا اداره پست جا بزند. همان‌طور که بیان شد یک سری ویژگی‌های خاص تمامی این ایمیل ها دارا می‌باشند که عبارت است از:

- یک کاربر به صورت غیر منتظره ایمیلی را دریافت می‌کند که شامل اطلاعاتی در مورد قبض، پیشنهادها، تحویل کالا و ... می‌باشد.
- از کاربر خواسته می‌شود تا لینکی را کلیک کند تا محتوای دقیق پیغام را مشاهده نماید.
- از کاربر خواسته می‌شود تا CAPTCHA کدی را وارد نماید. با این کار مهاجم میخواهد مطمئن شود که شرکت های امنیتی در حال دانلود فایل مخرب او نیستند.
- با وارد کردن کد، یک فایل zip شروع به دانلود می‌کند. این فایل باید در واقع شامل یک فایل متنی باشد در حالی که شامل یک فایل اجرایی می‌باشد.
- اگر فایل دانلود و اجرا شد، در واقع بدافزار اجرا شده و شروع به جستجو برای فایل های اطلاعاتی کرده و آنها را رمزنگاری می‌نماید.
- در نهایت وقتی تمام فایل ها رمز شدند، کاربر پیغامی را مشاهده می‌کند که متوجه می‌شود آلوده گشته است و برای بازگرداندن فایل هایش چه مراحلی را باید طی کند.

کاربرها چه کارهایی می‌توانند بکنند:

- نسبت به ایمیل های دریافتی خود بسیار مشکوک باشید.
- اگر ایمیلی شما را به صفحه ای راهنمایی کرد تا فرمی را پر کنید، حتما دقت کنید که آدرس سایت قانونی باشد.
- فایل های آرشیو(.7z، .jar، .msi، .tar، .rar، .zip) و اجرایی / اسکریپت ها(.cmd، .wsf، .vbe، .jse، .js، .bat، .scr، .com، .exe) را دانلود نکنید. شرکت ها نیاز به ارسال فایل‌هایی از نوع متن برای مستندات خود دارند.
- روی سیستم خود آنتی ویروس نصب کرده و آن را همواره به روز نگه دارید.
- عادت به گرفتن نسخه پشتیبان دوره ای و منظم از اطلاعات خود داشته باشید.
- در صورتی که آلوده شدید، به خلاف‌کاران هزینه ای نپردازید زیرا هیچ ضمانتی وجود ندارد که با وجود پرداخت پول ، فایل‌های شما را باز گردانند. علاوه بر آن پرداخت باج به آنها موجب گسترش این نوع حملات شده و خلاف‌کاران را به این سمت جذب می‌کند.

آسیب‌پذیری Shellshock از آسیب‌پذیری Heartbleed خطرناکتر است!

با استفاده از آسیب‌پذیری Shellshock میلیون‌ها سرور و تجهیزات دیگر به خطر می‌افتند. این‌که این آسیب پذیری به چه میزان گسترش یافته و چه مشکلات مالی را ایجاد نموده است، هنوز مشخص نشده است. اما موضوعی که مشخص است این است که Shellshock از آسیب پذیری Heartbleed خطرناک تر است.

آسیب پذیری Heartbleed تنها برنامه‌ای که توسط سرور به منظور رمزنگاری و ایمن نمودن ارتباطات استفاده می‌شود را تحت تاثیر قرار داده است. این آسیب پذیری به مهاجمان اجازه می‌دهد که به اطلاعات حساسی همچون کلیدهای رمزنگاری و یا کلمات عبور را از سرورهای آسیب پذیر، دست یابد. اما Shellshock به مهاجمان قدرت بیشتری می‌دهد. آنها می‌توانند از این آسیب‌پذیری به منظور ایجاد دسترسی کامل و کنترل سیستم بدون داشتن نام کاربری و رمزعبور استفاده نمایند. به منظور سوء استفاده از این آسیب پذیر نیازی به مهارت خاصی وجود ندارد. به دلیل این‌که مهاجم می‌تواند از Shellshock برای اجرای کد از راه دور بر روی یک سیستم استفاده کند، می‌تواند از آن به منظور ایجاد یک "کرم" استفاده نماید که با استفاده از آن به سیستم های دیگر حمله می‌کند و آن‌ها را به مخاطره می‌اندازد.

آسیب پذیری Shellshock در بسته‌ی نرم افزاری Bash، مفسر خط فرمان یا شل، که روشی قدرتمند در اجرای فرمان ها بر روی یک کامپیوتر است، می‌باشد. این بسته نرم افزاری به صورت پیش فرض برروی تمامی سیستم عامل‌های لینوکس و اپل وجود دارد. همچنین Bash به منظور ایجاد ارتباط با تجهیزات دیگر استفاده می‌شود. در نتیجه نه تنها سرورها بلکه روترهای خانگی، دوربین ها و سایر تجهیزات می‌تواند به خطر بیفتد.

زمانی‌که آسیب پذیری Shellshock گزارش شد، شواهدی مبنی بر استفاده از این آسیب پذیری در یک محدوده وسیع گزارش داده شد. لازم به ذکر است که شرکت ها و سازمان ها باید اقدامات پیشگیرانه‌ای به منظور جلوگیری از اجرای این حمله در خود، انجام دهند.

بدافزار رجین را بشناسید!

رجین[1] نوعی بدافزار درب پشتی[2] است که در رده‌ی بدافزارهای با پیچیدگی بالا قرار می‌گیرد. تکنیک‌های استفاده شده در این بدافزار از جمله نادرترین تکنیک‌های به کار رفته در بدافزارهای فضای مجازی است. رجین برای نگه داری برخی از ماژول‌های خود به جای استفاده از روش‌های معمول ذخیره سازی فایل، از روشهای پیشرفته‌ای همچون NTFS EA و ذخیره سازی در رجیستری بهره برده است. به این ترتیب حجم زیاد مربوط به یک فایل به بخش‌های کوچک تر شکسته شده و هر بخش به صورت رمز شده ذخیره می‌شود. بالعکس در زمان بارگذاری فایل کلیه‌ی بخش‌های شکسته شده جمع آوری شده و رمزگشایی می‌شوند. علاوه بر این برای نگه داری بخشی از اطلاعات از تکنولوژی EVFS نیز استفاده شده است.

رجین میتواند از راه‌های پیچیده و متفاوتی برای برقراری ارتباط با حمله گران خود استفاده کند که از جمله ی آنها می‌توان به ICMP، دستورات تعبیه شده در کوکی[3]های HTTP و پروتکل‌های خاص TCP و UDP اشاره کرد.

رجین با رنج گسترده ای از توانایی‌ها و کاربردها پیاده سازی شده است که هریک بنا به هدف مورد حمله به کار گرفته می‌شوند؛ این موضوع به طراحانش امکان میدهد تا به راحتی به نظارت، جاسوسی و سرقت اطلاعات از سازمان‌های دولتی، سازمان‌های مادر، بنگاه‌های تجاری و تحقیقاتی و افراد خاص بپردازند.

پیچیدگی و سازمان دهی مناسبی که در طراحی این بدافزار به کار رفته است نیازمند صرف زمان و برخورداری از منابع قابل توجهی است که نشانگر این مطلب است که طراحی آن هدفمند بوده است و از حمایت مالی منابع قدرتمند برخوردار بوده است.

در سال‌های اخیر نمونه‌های جمع آوری شده از این بدافزار از نقاط مختلف جهان مورد بررسی قرار گرفته اند که حاصل این بررسی نشان میدهد که نمونه‌ها ارتباط خاصی با یکدیگر نداشته، همگی آنها رمزنگاری شده هستند و اطلاعات کمی را در اختیار می‌گذارند.

با بررسی دقیق قربانیان این بدافزار در میابیم که هدف اصلی طراحان آن حمله به مراکز علمی و موسسات جمع آوری اطلاعات بوده است. از جمله مراکزی که مورد حمله قرار گرفته اند می‌توان موارد زیر را نام برد:

- اپراتورهای مخابراتی
- مراکز دولتی
- افراد سیاسی
- مراکز مالی
- مراکز تحقیقاتی
- افراد فعال در تحقیقات علوم ریاضی و رمزنگاری

اگر چه در بیشتر موارد حمله‌های صورت گرفته برای مراکز علمی و تحقیقاتی هدف گذاری شده اند، در میان حملات گزارش شده تعدادی مربوط به اپراتورهای مخابراتی است. هدف از حملات دسته ی دوم گرفتن کامل کنترل شبکه برای شروع حملات گسترده‌ی بعدی است. یکی از حملات به طور مستقیم یکی از اپراتورهای بزرگ GSM را هدف قرار داده است. فایل‌های جمع آوری شده بعد از این حمله حجم بالایی از اطلاعات جاسوسی شده و اقدامات صورت گرفته در روال کار اپراتور را نشان می‌دهد. از جمله اقدامات بدافزار در این حمله

استفاده از دستورات استاندارد برای گزارش برداری از اطلاعات موجود در سیستم‌های اپراتور است.

هنوز مشخص نشده است که این بدافزار اولین بار چگونه راه اندازی شده است، اما بسیاری از حدسیات مبتنی بر استفاده از اکسپلویت‌ها در برنامه‌های اینترنتی است.

رجین را می‌توان یک حمله‌ی تمام عیار در فضای مجازی خواند که به طراحان خود اجازه می‌دهد در تمامی سطوح به لایه‌های شبکه‌ی قربانی دسترسی از راه دور داشته باشند. در بسیاری از نمونه‌های دیده شده بدافزار توانایی دسترسی از راه دور را دارد که به وسیله‌ی این ویژگی می‌تواند اقدام به تهیه‌ی تصاویر از رایانه، گرفتن کنترل کاربری ماوس، سرقت اطلاعات رمز کاربری، جاسوسی و نظارت بر ترافیک شبکه و بازیابی فایل‌های پاک شده کند.

یکی از ویژگی‌های مهم این بدافزار حضور کم رنگ آن در سیستم است. داشتن این ویژگی به معنی آن است که بسیاری از سیستم‌ها می‌توانند سال‌ها به رجین آلوده باشند بدون آنکه فایل‌های آنها کشف شود. حتی بعد از تشخیص فایل‌های بدافزار در سیستم قربانیان تحلیل آنها با دشواری همراه است چرا که کلیه‌ی فایل‌ها دارای لایه‌های رمزنگاری است. علاوه بر این در زمان تحلیل فایل‌ها با مجموعه دستوراتی مواجه می‌شویم که ارتباطی با کاربری بدافزار نداشته و مربوط به کدهایی با کاربری دیگر هستند. به نظر می‌رسد افزوده شدن این دستورات به منظور بالا بردن پیچیدگی تحلیل بخش‌های اصلی بدافزار بوده است.

طراحی رجین نیز هم چون بدافزارهای پیچیده‌ی قبلی اش، از جمله فلیم[۴] و استاکس‌نت[۵]، ماژولار و چند سطحی ست. طراحی ماژولار به طراحان رجین اجازه می‌دهد تا به راحتی بتوانند بنا به هدف و قربانی خود حمله‌ای خاص را صورت داده و اطلاعاتی خاص را جمع آوری و سرقت کنند.

این بدافزار در پنج مرحله اجرا می‌شود که هر مرحله به نوعی پنهان شده و رمزنگاری شده است. روش غیر متداولی که در روال اجرایی این بدافزار دیده می‌شود آغاز اجرای آن در سطح کرنل است. البته این مورد در نسخه‌های ۶۴ بیتی رجین دیده نمی‌شود و علت آن را می‌توان دشوار بودن اجرای کدهای سطح کرنل در سیستم‌های ۶۴ بیتی دانست.

از لحاظ جغرافیایی دامنه‌ی حملات صورت گرفته به طور اکثریت شامل کشورهای روسیه، عربستان، مکزیک، ایرلند، هند، افغانستان، ایران، بلژیک، اتریش و پاکستان است.

---

۱. Regin
۲. Backdoor
۳. Cookie
۴. Flame
۵. Stuxnet

الگوریتم‌های مورد استفاده در شناسایی بدافزارها

بخش اول

بعد از انتخاب یک آنتی‌ویروس و نصب آن بر روی سیستم کاربر سه انتظار اصلی از آنتی‌ویروس نصب شده دارد. ۱. کشف ویروس‌ها ۲. شناسایی و تعیین هویت ویروس ۳. پاک‌سازی آلودگی‌هایی که ویروس روی فایل‌ها ایجاد کرده است.

این سه مورد از اساسی ترین پارامترهای مرتبط با یک آنتی‌ویروس می‌باشد. در سری مقالات «مقابله با بدافزار، از کشف تا پاکسازی» سعی بر این است که در مورد روش‌های کشف ویروس‌ها صحبت شود و مزایا و معایب هر روش و لزوم وجود این روش‌ها مورد بررسی قرار گیرد.

کشف ویروس‌ها :

به راحتی می‌توان گفت که کشف ویروس‌ها یکی از پرهزینه‌ترین و سخت‌ترین کارها در زمینه مبارزه با ویروس‌های کامپیوتری است، که همواره نیازمند متخصصانی در این حوزه می‌باشد که بتوانند فایل‌های حاوی بدافزارها را به خوبی تحلیل کرده و راه‌کارهایی جهت شناسایی بدافزارها استخراج کنند. از این رو سوالات متعددی به وجود می‌آید. مثلاً، آیا روش‌های شناسایی بدافزار به صورت عمومی و کلی هستند یا این‌که برای هر خانواده از بدافزارها نیازمند یک روش جداگانه هستیم؟ آیا پاسخ حاصل از این روش‌های کشف ویروس‌ها کامل و دقیق می‌باشند؟ آیا این روش‌های کشف خطری برای سیستم کاربر ندارند؟ و سوال‌هایی از این قبیل که سعی داریم در اینجا به صورت مختصر پاسخ‌های را برای این پرسش‌ها داشته باشیم.

خروجی حاصل از مراحل کشف ویروس را می‌توان به ۴ حالت کلی بیان کرد :

۱. اگر ویروس واقعاً وجود داشته باشد و نتیجه حاصل از کشف هم مثبت باشد پاسخ مثبت درست خواهیم داشت.

۲. اگر ویروس واقعاً وجود داشته باشد و نتیجه حاصل از کشف منفی باشد، پاسخ منفی نادرست اعلام خواهد شد.

۳. اگر ویروس واقعاً وجود نداشته باشد و نتیجه حاصل از کشف هم منفی باشد پاسخ منفی درست اعلام خواهد شد.

۴. اگر ویروس واقعاً وجود نداشته باشد و نتیجه حاصل از کشف مثبت باشد آنگاه پاسخ مثبت نادرست اعلام خواهد شد.

میزان درصدهای این حالات در پویش فایل‌های یک سیستم معیار اصلی جهت تعیین قدرت شناسایی آنتی‌ویروس‌ها می‌باشد.

روش‌های کشف بر اساس اینکه آیا در زمان بررسی، می‌بایست فایل مربوطه اجرا شود یا خیر به دو گروه تقسیم می‌شود :

۱. شناسایی ایستا

۲. شناسایی پویا .

در شماره بعدی شرح روش‌های شناسایی ایستا و پویا داده خواهد شد.

پادویش

خلاق و هوشمند، در خدمت امنیت

موتور هوشمند، مقابله
با ویروس های ناشناخته

رهایی از کابوس
فلش های ویروسی

سرعت در پویش
قدرت در پاکسازی

www.padvish.com

شرکت نرم افزاری

امن پرداز

آدرس: تهران، خیابان ملاصدرا، خیابان شیخ بهایی جنوبی، گرمسار غربی، پلاک ۷۶
تلفن: ۰۲۱-۴۳۹۱۲۰۰۰ فکس: ۰۲۱-۴۳۹۱۲۸۰۰
www.amnpardaz.com
info@amnpardaz.com