اسفند
۹۳

مجله

امنیت اطلاعات

شماره نهم

رُستوک

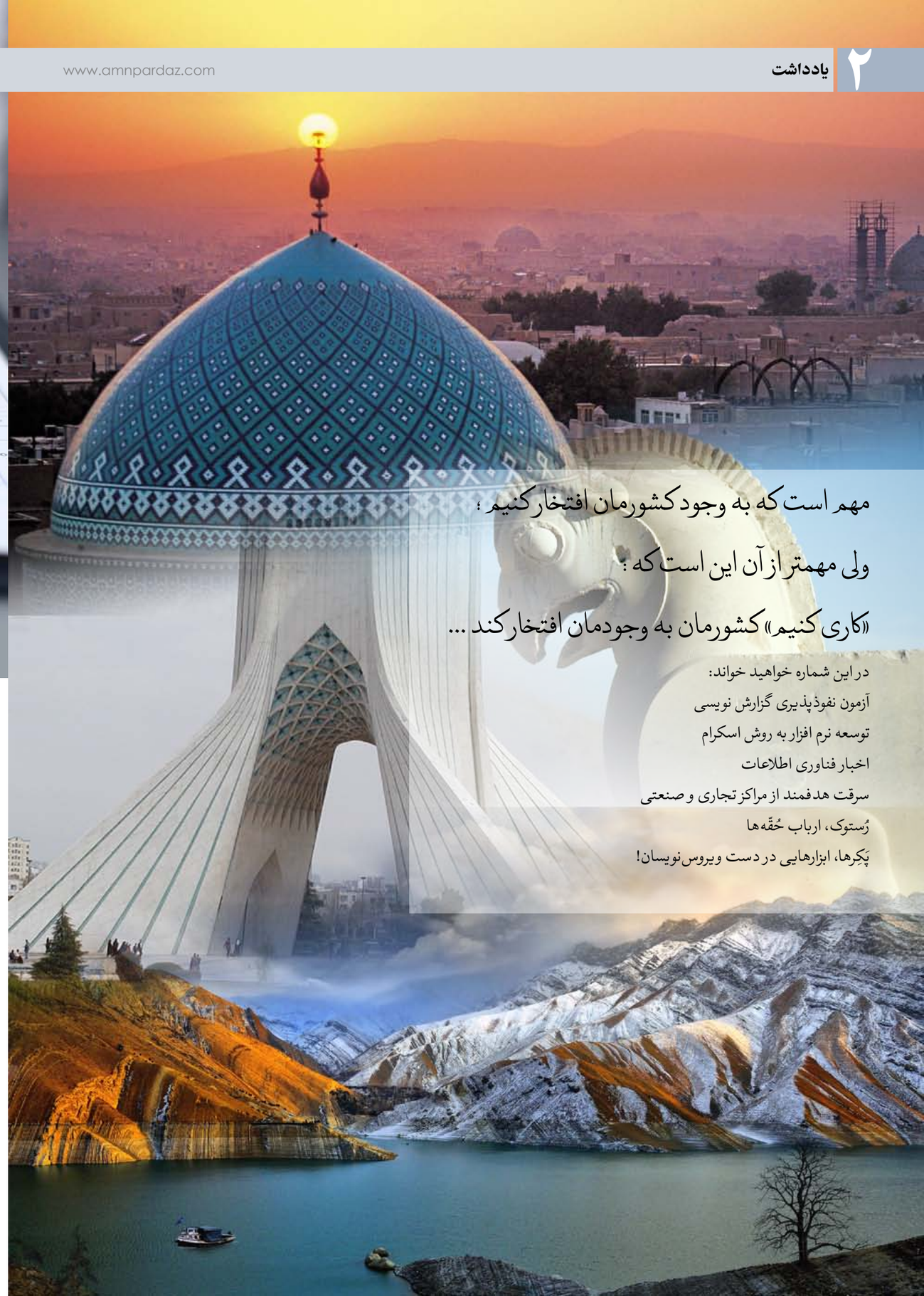
ارباب حُقّه‌ها

سرقت هدفمند

از مراکز تجاری و صنعتی

آزمون نفوذپذیری، پوشاندن مسیر

پَکِرها، ابزارهایی در دست ویروس‌نویسان!



مهم است که به وجود کشورمان افتخار کنیم ؛

ولی مهمتر از آن این است که :

«کاری کنیم» کشورمان به وجودمان افتخار کند ...

در این شماره خواهید خواند:

آزمون نفوذپذیری

گزارش نویسی بخش آخر

در این قسمت به آخرین فاز آزمون نفوذ پرداخته می‌شود که گزارش نویسی است. اهمیت این فاز نباید کم درنظر گرفته شود؛ زیرا بیان کننده اقداماتی است که آزمون کنندگان انجام داده‌اند. در گزارش آزمون نفوذ، تمامی جزییات مرتبط با آزمون بیان می‌گردد.

مخاطبان این گزارش بنابر نوع سازمان متفاوت می‌باشند، اما به صورت پیش‌فرض مخاطبان آن، مدیر ارشد، مدیر فناوری اطلاعات و کارکنان فنی فناوری اطلاعات می‌باشند.

- مدیر ارشد: مدیران ارشد به جزییات اهمیت نمی‌دهند و آن‌ها را متوجه نمی‌شوند و فقط به این مطلب که "آیا سیستم‌های آن‌ها امن است یا خیر؟" توجه می‌کنند.
- مدیر فناوری اطلاعات: توجه این گروه به امنیت کلی سازمان و اینکه هیچ یک از بخش‌های اصلی سازمان مشکلی به وجود نخواهند آورد، معطوف است.
- کارکنان فنی فناوری اطلاعات: این گروه شامل افراد متخصصی می‌باشد که وظیفه آن‌ها رفع آسیب‌پذیری‌های کشف شده است. توجه این گروه به جزییات بیش از دو گروه پیشین است.

گزارش آزمون نفوذ باید شامل چه مواردی باشد؟

۱- اطلاعات کلی از تیم آزمون کننده، نام کارفرما و نوع آزمون می‌باشد.

۲- خلاصه اجرایی: شامل محدوده‌ی آزمون و نتیجه‌ی آزمون نفوذ آن، اهمیت آسیب‌پذیری‌های کشف شده و علت توجه به آن‌ها، و پاسخ به این سوال که "آیا سیستم امن می‌باشد یا خیر؟" است.

۳- خلاصه‌ی آسیب‌پذیری‌ها: این بخش دیدی کلی برای مدیران فناوری اطلاعات مبنی بر اینکه چه فعالیت‌هایی لازم است صورت گیرد، فراهم می‌کند.

۴- لیست ابزارهای مورد استفاده در آزمون نفوذ: شامل نام ابزار و نسخه‌ی آن می‌باشد.

۵- جزییات آسیب‌پذیری‌ها: در این بخش، هر آسیب پذیری دارای یک جدول می‌باشد که در آن نوع آسیب‌پذیری، درجه آسیب‌پذیری، اطلاعات کشف شده توسط آسیب پذیری، راهکار جهت رفع آن و این‌که آسیب‌پذیری چه مخاطراتی ایجاد می‌نماید می‌باشد.

در شماره‌های پیشین به مراحل مختلف آزمون نفوذ اشاره گردید؛ در این شماره نیز آخرین مرحله آزمون نفوذ شرح گردید.

توسعه نرم افزار به روش اسکرام[1] بخش سوم

مقدمه

در شماره‌های پیشین تاریخچه اسکرام ، نقش ها و وظایف هر یک از افراد در تیم مورد بررسی قرار گرفته شد. در این شماره به موضوع اسکرام چه می‌کند و چرخه‌ی دمینگ[2] پرداخته شده است.

اسکرام بر پایه هم‌نوایی و نظم نهاده شده است. نظم و هماهنگی در رگ و ریشه انسان نهادینه شده است و آهنگ تپش قلب در عمیق‌ترین بخش‌های ذهن شنیده می‌شود. فطرت ما انسان‌ها همیشه به دنبال نظم و هم‌آهنگی در تمامی بخش‌های زندگی است. اما، آهنگ‌ها همیشه برای شادی و خوشی نیستند. ریتم و یکنواختی می‌تواند باعث تشدید عادت‌های بی‌دلیل و یا افسردگی و کرختی شود.

کافی است در راهروی بسیاری از اداره‌ها و سازمان‌ها قدمی بزنید تا کرختی و یکنواختی کارهای روزمره را در افراد ببینید. این حس و حال در هر جایی که افراد احساس به دام‌افتادگی در فضای اداری دارند، بیشتر می‌شود. اوضاع هنگامی بدتر می‌شود که آدم‌ها از اینکه به عنوان یک ماشین به آن‌ها نگاه می‌شود، عصبانی هم باشند. اگر صدها سال به عقب برگردید، همیشه این تجربه انسانی، همراه بشر بوده است. همیشه انسان‌ها از اینکه اسیر سیستم‌ها باشند، احساس درماندگی می‌کنند. قرن بیستم، و محیط‌های کسب و کار سیستماتیک این مسخ شدگی را به بخشی از سرنوشت انسان‌ها تبدیل کرده است.

اسکرام چه می‌کند؟

اسکرام تلاش می‌کند تا نوعی دیگر از ضرب‌آهنگ را ایجاد کند. روش اسکرام با پذیرش اینکه ما انسان‌ها موجودات عادت-دوستی هستیم، که همیشه به دنبال یک آهنگ مشخص حرکت می‌کنیم و حتی تا حدودی قابل پیش‌بینی هستیم، قبول کرده است که توانایی‌های خارق‌العاده و جادویی دیگری هم داریم. اسکرام، تلاش می‌کند تا با استفاده از عادت‌طلبی انسان و ایجاد نواخت‌های روزانه و هفتگی، به افراد شانس دیدن نقاط ضعف و قدرت خودشان را در آینه کارها و تصمیم‌هایشان بدهد. عادت‌ها و درگیرشدن بیش از حد در چرخه‌های روزانه و هفتگی می‌تواند مانند یک سرطان زمان و تلاش‌های تیم‌ها را از بین ببرد. اسراف و درگیری بیش از حد در چرخه‌ها حاصلی به جز از بین رفتن تیم‌های کاری و هدر رفتن زمان نخواهد داشت. اسکرام تلاش می‌کند تا در بازه‌های زمانی مناسب، امکان بازبینی کارها و بررسی خروجی‌ها را برای افراد فراهم کند تا در صورتی که کارها به بیراه می‌روند، از اسراف و دورریزی منابع جلوگیری کند.

برای اینکه بیشتر از میزان اسراف در کارها صحبت کرده باشیم، آماری که آقای جف سادرلند[3] در کتاب Scrum : The Art of Doing Twice the Work in Half the Time مطرح کرده است، شاید جالب باشد. طبق اعلام ایشان، در بیشتر سازمان‌هایی که از سوی موسسه اسکرام مورد بررسی قرار گرفته‌اند، در حدود ۸۵٪ کارها بدون نتیجه بوده‌اند و در بهترین حالت معمولا تنها به ۶۰٪ از برنامه‌های از پیش تعیین شده رسیده‌اند.

پرهیز از اسراف

آقای تای‌ایچی اونو[4] به عنوان بنیان‌گذار سیستم تولید تویوتا (Toyota Production System) در خصوص به هدر رفتم منابع و سرمایه‌ها می‌گوید: "اسراف بیشتر از آنکه زیان اقتصادی برای کسب و کارها باشد، جرمی است بر ضد جوامع". آنچه آقای تای‌ایچی اونو از آن به عنوان اسراف یاد می‌کند در فرهنگ ژاپنی شامل سه بخش می‌شود:

- موری – Muri: اسراف و زیان به دلیل عدم توجه به منطق
- مورا – Mura: اسرف و هدر رفتن به خاطر تناقض‌ها
- مودا – Muda: به هدر رفتن خروجی‌ها و دست‌آوردها

مبارزه با این اسراف‌ها و جلوگیری از زیان‌دهی با در نظر داشتن این سه مورد، بسیار شبیه چرخه دمینگ PDCA است. تصور کنید:

- برنامه ریزی (Plan) به معنی جلوگیری از موری
- انجام (Do) به معنی دوری از مورا
- بررسی (Check) به معنی پرهیز از مودا
- اقدام (Act) به معنی هدف گذاری، انگیزه و تشخیص

مهمترین هدف از پیاده سازی و استفاده از اسکرام، ترکیب چرخه‌های پیشرفت سودمند PDCA با عادت‌های معمول انسان و جلوگیری از اسراف و زیان‌دهی در منابع است.

درس اول – در هر زمان، یک کار را انجام دهید

همه ما در تجربه‌های روزمره‌مان، افراد مختلفی را دیده‌ایم (و به احتمال زیاد خودمان هم یکی از این افراد هستیم) که ادعا می‌کنند در یک زمان قادر به انجام چند کار هستند. همزمان رانندگی می‌کنند و با تلفن صحبت می‌کنند. (و البته تصادف هم می‌کنند.) و یا همزمان چت می‌کنند و درس می‌خوانند (و چیزی متوجه نمی‌شوند) و یا همزمان چندین زبان برنامه نویسی را فرا می‌گیرند. (و در هیچ کدام متخصص نمی‌شوند.) از نظر این افراد تمامی این کارها به خصوص در زمان حاضر که جریان‌های اطلاعاتی و پروژه‌ها بی‌اندازه زیاد شده‌اند، بدیهی و لازم است. اما ظاهرا نتیجه واقعی کمی برعکس است. پروفسور David Sanbonmatsu از دانشگاه یوتا یک تحقیق جالب در این خصوص منتشر کرده است. در این تحقیق از افراد خواسته شده بود تا در ابتدا نسبت به توانایی انجام کارهای متعدد (Multi-Tasking) خودشان رتبه دهند و سپس همان موارد را به صورت عملی آزمایش کنند. نتیجه کاملا برعکس فرضیات شرکت‌کنندگان بود. هر چقدر افراد به توانایی چندکارگی خودشان رتبه بالاتری دادند، نتیجه عملی موضوع نتیجه پایین‌تری داشت. ایشان در متنی که در سال ۲۰۱۳ در بلاگ NPR منتشر کردند، بیان می‌کنند شاید این احساس فردی از توانایی‌های منحصر به فرد، ناشی از استرس و عدم توانایی تمرکز بر روی کارهایشان باشد. وقتی افراد مجبور باشند چندین کار را انجام دهند و به صورت غیر ارادی توانایی تمرکز بر روی یک کار را نداشته باشند، احساس می‌کنند تحت درماندگی یک سیستم قرار دارند و در نتیجه ممکن است باعث به هدر رفتن (اسراف) منابع و زمان شوند. اولین درس را با یک تمرین کوچک تمام می‌کنیم. تلاش کنید تا این جدول را در دو حالت بنویسید(جدول۱) در حالت اول، روی یک کاغذ، جدول بالا را به صورت سطر به سطر بنویسید. بدین ترتیب از ۱ تا ۱۰ به اعداد فارسی، از A تا J به حروف انگلیسی و از الف تای در سیستم ابجد شکل خواهد گرفت. در حالت دوم، همین جدول را به صورت ستونی آماده کنید. این کار برای من در حالت اول ۴۲ ثانیه و در حالت دوم ۱۶ ثانیه طول کشید. اگر از این تمرین ذهنی با نتیجه مشابهی بیرون آمدید، شاید جدول زیر از آقای Gerald Weinberg در کتاب Quality Software Management نیز جالب باشد. آقای جرالد وینبرگ یکی از معروفترین استاد روانشناسی و انسان‌شناسی در توسعه نرم‌افزار هستند. کتاب The Psychology of Computer Programming یکی از مراجع رفتار برنامه‌نویسان در طول سال‌های متعدد است.

در شماره بعد به بررسی شرکت‌های داخلی و خارجی که از متدلوژی اسکرام استفاده می‌کنند به همراه مزایا و معایب آن پرداخته می‌شود.

۱	A	۱
ب	B	۲
ج	C	۳
د	D	٤
ه	E	۵
و	F	٦
ز	G	۷
ح	H	۸
ت	I	۹
ی	J	۱۰

تعداد پروژه‌های هم‌زمان	درصد زمان قابل دسترسی برای هر پروژه	زیان زمانی به خاطر تغییر حالت
۱	٪۱۰۰	٪۰
۲	٪٤۰	٪۲۰
۳	٪۲۰	٪٤۰
٤	٪۱۰	٪٦۰
۵	٪۵	٪۷۵

1. Scrum
2. W. Edwards Deming
3. Jeff Sutherland
4. Taiichi Ohno

انتشار نسخه جدید محبوب ترین زبان اسکریپ نویسی

به نقل از خبرگزاری Threat Post نسخه جدید محبوب ترین زبان اسکریپ نویسی، PHP 5.6.5 منتشرشد.
در این نسخه چندین آسیب‌پذیری خطرناک، که یکی از آن‌ها منجر به RCE (اجرای کد از راه دور) می‌شد نیز رفع شده است.
یکی از آسیب‌پذیری‌های رفع شده، شامل اشاره گر اولیه در Exif بود. مورد دیگر، آسیب‌پذیری بود که در ماه دسامبر سال ۲۰۱۴ توسط آقای "استفان ایسر" کشف و گزارش شده بود و برای آن یک Patch نیز ارائه شد، اما نتوانسته بود به درستی تمام ایرادات امنیتی آن را برطرف نماید.
وی در ایمیل ارسالی خود به مسئولین این شرکت گفت: "در بسته‌ای (Patch) که برای رفع این آسیب پذیری ارائه داده، از zend_hash_find استفاده کرده است، در حالی که در بسته منتشر شده از Zend-symtable - find استفاده شده و همین تغییر باعث می‌شود که بسته ارائه شده از سوی کمپانی، کامل نباشد." وی گفت: " علت اینکه نباید در Objectها از مقادیر Integer استفاده کرد، این است که اگر یک هکر با مقدار "AAA" تلاش کند، برنامه وی را تشخیص خواهد داد، ولی اگر این امر با مقدار "۱۲۳" صورت بگیرد، برنامه آن را به عنوان یک مقدار عددی تشخیص نداده و عملا امکان دور زدن، برای مهاجم فراهم می‌شود. "
در نسخه جدید، این ایرادات برطرف شده و اقدامات امنیتی پیشرفته‌ای نیز به کار گرفته شده است.

تیر تروجان رها شده از چله کمان، در قلب کاربران فیسبوک

به نقل از خبرگزاری Threat Post، تروجان جدیدی راه خود را در بزرگ ترین شبکه اجتماعی دنیا، فیسبوک، باز کرده‌است. به واسطه این تروجان صد و ده هزار کاربر تنها طی دو روز آلوده شده‌اند.
این تروجان خود را از طریق ارسال لینک یک ویدئو غیراخلاقی در یک پست، توسط اکانت کاربری که قبلا آلوده شده است، منتشر می‌کند. تروجان بر روی پست آلوده، ۲۰ نفر از دوستان کاربر را برچسب (Tag) می‌زند. وقتی یکی از این افراد، بر روی لینک کلیک می‌نماید، ویدئو شروع به پخش می‌کند، اما پس از لحظه‌ای متوقف شده و از کاربر می‌خواهد که نسخه جدید Flash Player را نصب کند. سپس برای کاربر بسته‌ای که ظاهرا محتوی فایل نصب Flash Player است، نشان داده شده و دانلود می‌شود ، درحالی که بسته در واقع شامل فایل دانلود تروجان همراه با یک بدافزار است.
تحقیقات اولیه در مورد این تروجان، در پستی در وبسایت Seclist.org، توسط پژوهشگر امنیتی آقای "محمد فغانی" منتشر شد. به گفته وی، این تروجان می‌تواند کلیدهای فشرده شده در صفحه‌کلید کاربر و حرکات ماوس او را دستکاری کند. یکی از علائم حضور این تروجان در سیستم کاربران، وجود chrome.exe در لیست برنامه‌های در حال پردازش توسط ویندوز است.
برخلاف تروجان‌های قبلی فیسبوک که اساس کارشان بر مبنای آلوده کردن پیام‌های خصوصی رد و بدل شده میان کاربران بود، تروجان جدید با آلوده کردن یک پست و برچسب زدن چندین کاربر دیگر بر روی آن، خود را نه تنها میان کاربران آلوده، بلکه بین دوستان آن‌ها نیز منتشر می‌کند. همین امر سبب می‌شود تا شیوع این تروجان، بسیار سریع باشد.
آقای فغانی گفته است که همچنان در حال بررسی این تروجان و ابعاد حمله می‌باشد.

هکرها در مقابل سد دفاعی ۱۴ میلیارد دلاری آمریکا

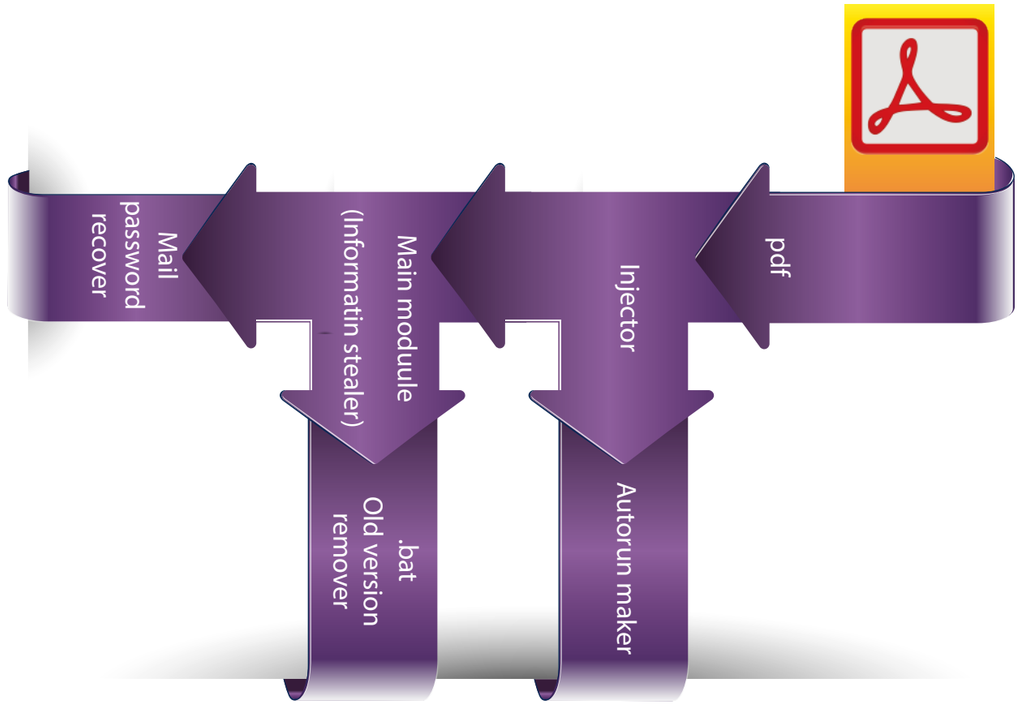
به نقل از خبرگزاری رویترز و به نوشته خبرگزاری CNet، دولت آمریکا با تصویب مجلس سنا در سال ۲۰۱۵ میلادی، بودجه‌ای ۱۴ میلیارد دلاری برای ارتش سایبری خود اختصاص داد. اختصاص این مبلغ که با اکثریت آراء موافق مجلس سنا همراه بود، نشان از دغدغه این کشور در حوزه مرتبط با امنیت فضای سایبری دارد. رییس جمهور آمریکا در توضیح اختصاص این مبلغ و اهداف اجرایی آن گفت که چنین بودجه هنگفتی برای افزایش به اشتراک گذاری اطلاعات مابین شرکت‌های خصوصی و دولت، افزایش امکانات و قابلیت‌های ضدجاسوسی و گسترش آموزش سایبری در دولت فدرال در نظر گرفته شده است.
استفاده از این بودجه برای پروژه‌ها و برنامه‌های خاصی مثل "سیستم تشخیص نفوذ انیشتین"، نظارت بر شبکه‌های کامپیوتری فدرال و شش مرکز Cyberops در جهت انجام امور سایبری این کشور در نظر گرفته شده است. رییس جمهور آمریکا گفت که این بودجه منابع مورد نیاز ما را برای دفاع از ملت مان در برابر حملات سایبری فراهم می‌کند. وی در ادامه افزود که هیچ کشور خارجی و هیچ هکری نباید بتواند اطلاعات تجاری محرمانه ما را بدزدد، شبکه کشور ما را مختل کند و یا حریم خصوصی خانواده‌های آمریکایی را مورد تعرض قراردهد.
اینطور که به نظر می‌رسد، پس از هک شدن شرکت سونی و ضرر هنگفتی که متوجه این شرکت شد، دولت‌ها برآن شده اند تا با تمام توان خود از کشورشان در برابر این گونه حملات دفاع کنند.

سرنوشت نامعلوم پیل تن دنیای IT در میانه بلوای خودساخته

به نقل از خبرگزاری The Hacker News، پژوهشگران امنیتی به کاربران اندروید در مورد وجود یک جفت آسیب‌پذیری در Google Play Store هشدار داده‌اند که باعث می‌شود کلاهبرداران اینترنتی بتوانند از راه دور(Remote) بر روی دستگاه‌های اندرویدی، برنامه‌های مخرب نصب کنند.
آقای "تاد بردسلی" که مدیر تیم فنی Metasploit Framework در شرکت Rapid7 هستند، در توضیح این مورد گفته‌اند که یک آسیب‌پذیری جدید در اندروید نسخه JellyBean در قسمت WebView کشف شده است و زمانی که مورد مذکور با آسیب‌پذیری X-frame option ترکیب شود، به هکرها اجازه می‌دهد تا از طریق Google Play Store بر روی دستگاه اندرویدی قربانی، هرگونه نرم‌افزار مخربی را از راه دور نصب و اجرا کنند.
برای این کار هکرها حتی نیاز به تایید کاربران در هنگام نصب نرم‌افزار نیز ندارند.
WebView مولفه اصلی (Core Component) بارگذاری صفحات اینترنتی بر روی دستگاه‌های اندرویدی است.
خطر این آسیب‌پذیری متوجه کاربرانی است که از سیستم‌عامل JellyBean 4.3 و نسخه‌های ماقبل آن استفاده می‌کنند، چرا که تیم امنیتی اندروید دیگر آپدیتی برای WebView این نسخ از سیستم‌های عامل خود ارائه نمی‌کند. همچنین کاربرانی که از مرورگرهای Third Party استفاده می‌کنند نیز تحت تاثیرات مخرب این آسیب‌پذیری هستند.
با توجه به اینکه در حال حاضر هیچ گونه به‌روزرسانی و یا بسته‌ای جهت رفع این آسیب‌پذیری منتشر نشده است، پژوهشگران جهت حفاظت کاربران در برابر این آسیب‌پذیری راهکارهای زیر را ارائه نموده‌اند:
• استفاده از مرورگرهای Firefox، chrome و یا Dolphin و عدم استفاده از مرورگر پیش‌فرض اندرویدی
• کاربران از اکانت خود در Google Play خارج شوند! این پیشنهاد هرچند که کمی عجیب به نظر می‌رسد، اما حداقل باعث کاهش خطر آسیب‌پذیری کاربران می‌شود.

واتس اپ؛ جولانگاه جدید هرزنامه‌ها

برنامه‌ی واتس اپ در زمره محبوب ترین برنامه‌های پیامکی در تمام دنیاست و به دلیل قابلیت انعطاف پذیری که دارد، می‌تواند برروی پلت فرم‌های مختلف تلفن همراه اجرا شود.
به نقل از خبرگزاری Threat Post، پژوهشگران شرکت "Adaptive Mobile" طی گزارشی اعلام نمودند، بسیاری از کمپین‌های ارسال هرزنامه که پیشنهاد خرید لوازم کم ارزش به کاربران می‌دهند، سرمایه‌گذاری‌های کلاهبردارانه انجام می‌دهند، محتوای غیراخلاقی تولید می‌کنند و فعالیت‌های بی‌ارزش دیگری از این دست انجام می‌دهند؛ جهت نیل به اهداف خود آرام آرام به سمت پلت فرم‌های پیامکی می‌روند.
امروزه برنامه‌های پیامکی (SMS App) به یکی از ابزارهای موردعلاقه این کمپین‌ها تبدیل شده است. اما رواج استفاده از واتس اپ در اروپا و هندوستان توجه ویژه آن‌ها را برانگیخته است. مدیرعامل پروژه واتس اپ آقای " ژان کوم " چندی پیش اعلام نمودند که روزانه ۳۰ میلیارد پیام در این برنامه رد و بدل می‌شود.
واتس اپ برخلاف برنامه‌های مشابه خود، چیزی فراتر از یک SMS App است، چرا که می‌تواند جایگزینی برای سرویس‌های پیامکی ارائه شده توسط مخابرات باشد.
به گفته مدیر بخش تحلیل داده‌های هوشمند شرکت Adaptive Mobile، آقای "چارلز مک دید"، تعیین مقیاس حملات ارسال هرزنامه در واتس اپ مشکل است. اما روشن است که واتس اپ هم در حال پیوستن به جرگه سیستم‌های پیام رسانی است که بستر و ویژگی‌های مناسبی برای ارسال هرزنامه دارند.



سرقت هدفمند از مراکز تجاری و صنعتی

در ماه‌های اخیر برخی از مراکز تجاری و صنعتی در ایران مورد حمله‌ی مجرمان سایبری قرار گرفتند و مبالغ کلانی از آن‌ها دزدیده شده است. در یکی از موارد تیم تخصصی شرکت امن پرداز برای بررسی‌های بیشتر در محل به صورت حضوری اقدام به عملیات Forensics نمودند.

با بررسی‌های انجام شده این نتیجه به دست آمد که قربانی از طریق ایمیل، آلوده به نوعی بات(Bot) شده است. روش کار این حمله بدین شکل بوده است که با توجه به نوع کاری مرکز تجاری یا صنعتی از مهندسی اجتماعی استفاده کرده و ایمیلی با عنوانی مرتبط با کار آن واحد می‌فرستد که در آن محتوایی تبلیغاتی

```
Public Sub Form_Load1() '402590
loc_004025B2: var_8 = &H401130
loc_004025F0: var_1C = "JavaLEMngt"
loc_004025FC: var_58 = "appdata"
loc_00402603: var_60 = 8
loc_0040260A: var_40 = "appdata"
loc_00402618: var_50 = Environ(var_40)
loc_00402622: var_50 = var_40
loc_0040265E: var_2C = var_50 & 00401FE0h
loc_0040266D: var_30 = var_2C & "Microsoft\JavaLEMngt"
loc_0040267C: var_18 = var_30 & ".exe"
loc_0040269F: Proc_004027E0(var_2C, var_30, var_1C)
loc_004026A9: var_20 = Proc_004027E0(var_2C, var_30, var_1C)
loc_004026BC: call InStr(edi, var_18, var_20, 80000001h, &H80000001h, "SOFTWARE\Microsoft\Windows\CurrentVersion\Run", var_1C, var_50, var_50)
              If InStr(edi, var_18, var_20, 00000001h, &H80000001h, "SOFTWARE\Microsoft\Windows\CurrentVersion\Run", var_1C, var_50, var_50) = 0 Then GoTo loc_004026F6
loc_004026CB: var_2C = "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
loc_004026E1: var_64 = &H80000001h
loc_004026E8: Proc_00403010(var_2C, var_1C, var_64)
loc_004026F6:
loc_00402705: Proc_004027E0(Proc_00403010(var_2C, var_1C, var_64), edx, var_2C)
loc_0040270F: var_24 = Proc_004027E0(Proc_00403010(var_2C, var_1C, var_64), edx, var_2C)
loc_0040271C: call InStr(edi, var_18, var_24, 80000001h, &H80000001h, "Software\Microsoft\Windows NT\CurrentVersion\Windows", "Run", var_64, var_2C)
              If InStr(edi, var_18, var_24, 00000001h, &H80000001h, "Software\Microsoft\Windows NT\CurrentVersion\Windows", "Run", var_64, var_2C) = 0 Then GoTo loc_0040276C
loc_00402754: Proc_00403010("Software\Microsoft\Windows NT\CurrentVersion\Windows", "Run", &H80000001h)
loc_0040276C:
loc_00402771: GoTo loc_00402797
loc_00402796: Exit Sub
loc_00402797:
End Sub
```

شکل ۱. اولین کد تزریق شده Decompile شده

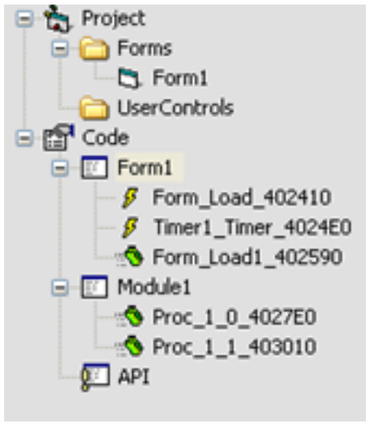
یا اطلاع رسانی قرار دارد. ضمیمه این نامه یک فایل اجرایی با آیکن به شکل PDF است. در واقع فایل اولیه بدافزار به شکل یک PDF جعلی طراحی شده است تا بتواند با فریفتن کاربر او را وادار به اجرای فایل مخرب خود کند. پس از اجرای فایل بدافزار پسوردهای مهم از جمله پسورد ایمیل مرکز دزدیده شده و بعدا مورد سوء استفاده قرار گرفته است.
شکل بالا صفحه قبل کلی اجرای بدافزار را نمایش می‌دهد.

مرحله‌ی اول

در اولین قدم یک فایل اجرایی با نمای یک فایل PDF قلابی برای قربانی فرستاده شده و استفاده از این تکنیک باعث شده است کاربر به اشتباه آن را اجرا نموده و آغازگر روال اجرای بدافزار باشد.
در بررسی ایمیل قربانی دو فایل PDF تقلبی یافت شد.
فایل اجرایی که به آن اشاره شد همان Dropper بدافزار است که به زبان C# نوشته شده و به شکلی بسیار پیشرفته مبهم‌سازی(Obfuscate) شده است. علی‌رغم اینکه نوع مبهم‌سازی استفاده شده شناخته شده نیست اما تکنیک‌های به کار رفته در روال آن پیچیده می‌باشد.
یکی از تکنیک‌های به کار رفته برای سخت کردن روال تحلیل، استفاده از تکنیک تولید کد IL در هنگام اجرا است.
کد IL لود شده ابتدا چهار پـــــردازه به نام vbc.exe را از مسیر C:\Windows\Microsoft.NET\Framework\v2.0.50727 به صورت معلق ایجاد می‌کند. سپس به صورت تصادفی به دو تا از پردازه‌های ایجاد شده کدی را تزریق کرده و به اجرای دو پردازه‌ی دیگر خاتمه می‌دهد. بعد از این کار دراپر یک کپی از فایل خود را در مسیر C:\Users ایجاد می‌کند. مرحله‌ی دوم تحلیل مربوط به بررسی کد تزریق شده در این دو پردازه‌ی انتخابی است.

مرحله‌ی دوم

کدهای تزریق شده به زبان Visual Basic نوشته شده‌اند.
اولین کد تزریق شده مربوط به حفظ بقای بدافزار است. این کد برای انجام هدف خود از تکنیک قرار دادن نام فایل خود در لیست



شکل ۲. دومین کد تزریق شده Decompile شده

```
loc_0041422B: 00000009h = 00000009h + Me.GetTypeInfoCount
loc_0041422D: ecx = VarPtr(var_2A0)
loc_00414240: Proc_00414CB0(var_2AC, 3, ecx)
loc_0041424E: call Erase(00000000h, var_2AC, "kernel32", "CreateProcessW", var_2AC)
loc_00414266: call ReDim(00000880h, 00000010h, var_2AC, 00000000h, 00000001h, 00000001h, 00000000h)
loc_00414272: var_2BC = &H4003
loc_0041427C: var_2B4 = var_2A0
loc_00414294: shl ecx, 04h
loc_0041429C: Me.GetTypeInfoCount = Me.GetTypeInfoCount - Me.%x1 = GetIDsOfNames(%x2) 'Ignore this
loc_004142A4: call MSVBVM60.DLL.__vbaVarZero
loc_004142B2: var_2C4 = var_14C
loc_004142CB: shl ecx, 04h
loc_004142CE: var_3A0 = Me.%x1 = GetIDsOfNames(%x2) 'Ignore this
loc_004142DD: Me.GetTypeInfoCount = Me.GetTypeInfoCount - Me.%x1 = GetIDsOfNames(%x2) 'Ignore this
loc_004142DF: Me.GetTypeInfoCount = Me.GetTypeInfoCount + 00000010h
loc_004142E2: call MSVBVM60.DLL.__vbaVarZero
loc_004142F5: Proc_00414CB0(MSVBVM60.DLL.__vbaVarZero, &H4003, var_2AC)
loc_00414303: call Erase(00000000h, var_2AC, "ntdll", "NtUnmapViewOfSection", var_2AC)
loc_0041431B: call ReDim(00000880h, 00000010h, var_2AC, 00000000h, 00000001h, 00000004h, 00000000h)
```

```
loc_0041442D: ecx = 64
loc_00414440: Proc_00414CB0(var_2AC, var_2AC, ecx)
loc_0041444E: call Erase(00000000h, var_2AC, "kernel32", "VirtualAllocEx", var_2AC)
loc_00414466: call ReDim(00000880h, 00000010h, var_2AC, 00000000h, 00000001h, 00000004h, 00000000h)
loc_00414478: var_2B4 = var_2A0
loc_0041447E: var_2BC = &H4003
loc_0041448E: shl ecx, 04h
loc_00414491: var_3AC = Me.%x1 = GetIDsOfNames(%x2) 'Ignore this
loc_004144A6: Me.GetTypeInfoCount = Me.GetTypeInfoCount - Me.%x1 = GetIDsOfNames(%x2) 'Ignore this
loc_004144A8: call MSVBVM60.DLL.__vbaVarZero
```

```
loc_00414601: Proc_00414CB0(var_2AC, var_2AC, ecx)
loc_0041460F: call Erase(00000000h, var_2AC, "kernel32", "WriteProcessMemory", var_2AC)
loc_0041462C: var_384 = var_17A - 0001h
loc_00414632:
              If  Then GoTo loc_004148EB
loc_00414677: imul edx, 28h
loc_00414692: var_354 = var_4C-Me.%x1 = GetIDsOfNames(%x2) 'Ignore this
              If eax < 0 Then GoTo loc_004146BA
```

```
loc_00414985: Me.GetTypeInfoCount = Me.GetTypeInfoCount + 00000010h
loc_00414988: ecx = VarPtr(&H10007)
loc_0041499B: Proc_00414CB0(Me.%x1 = GetIDsOfNames(%x2) 'Ignore this, 3, var_2AC)
loc_004149A9: call Erase(00000000h, var_2AC, "kernel32", "GetThreadContext", var_2AC)
loc_004149C1: call ReDim(00000880h, 00000010h, var_2AC, 00000000h, 00000001h, 00000004h, 00000000h)
loc_004149D3: var_2B4 = var_2A0
loc_004149D9: var_2BC = &H4003
loc_004149E9: shl ecx, 04h
loc_004149EC: var_3C4 = Me.%x1 = GetIDsOfNames(%x2) 'Ignore this
loc_00414A01: Me.GetTypeInfoCount = Me.GetTypeInfoCount - Me.%x1 = GetIDsOfNames(%x2) 'Ignore this
```

```
loc_00414AF6: Proc_00414CB0(var_2AC, var_2AC, ecx)
loc_00414B04: call Erase(00000000h, var_2AC, "kernel32", "WriteProcessMemory", var_2AC)
loc_00414B30: var_19C = var_158 + var_14C
loc_00414B36: call ReDim(00000880h, 00000010h, var_2AC, 00000000h, 00000001h, 00000001h, 00000000h)
loc_00414B42: var_2BC = &H4003
loc_00414B4C: var_2B4 = var_29C
loc_00414B64: shl ecx, 04h
loc_00414B67: var_3CC = Me.%x1 = GetIDsOfNames(%x2) 'Ignore this
loc_00414B76: Me.GetTypeInfoCount = Me.GetTypeInfoCount - Me.%x1 = GetIDsOfNames(%x2) 'Ignore this
loc_00414B78: call MSVBVM60.DLL.__vbaVarZero
loc_00414B87: var_2C4 = VarPtr(&H10007)
loc_00414BA6: shl ecx, 04h
```

شکل ۳. روش تزریق کد

فایل‌های Autorun در رجیستری استفاده کرده است، به گونه‌ای که به طور مداوم اقدام به نوشتن نام فایل خود در این بخش رجیستری می‌کند. این کار سبب می‌شود در صورت پاک شدن نام فایل در رجیستری به هر دلیلی، بار دیگر نام آن در این قسمت قرار بگیرد. به این ترتیب با هر بار بالا آمدن سیستم بدافزار نیز به طور اتوماتیک اجرا خواهد شد. در ادامه آدرس کلید ساخته شده، نام آن و پارامتر قرار گرفته در آن نشان داده شده است.

SOFTWARE\Microsoft\Windows\CurrentVersion\Run
SOFTWARE\Microsoft\Windows Nt\CurrentVersion\Run

اولین کد تزریق شده Decompile شده است که قسمت‌هایی از آن را در شکل ۱ مشاهده می‌کنید.

شکل ۲ مربوط به Decompile شده‌ی دومین کد تزریق شده است. دومین کد تزریق شده هسته‌ی اصلی بدافزار را شامل می‌شود که توانایی تزریق کد و ارتباط با سرور اصلی خود را دارد. این برنامه در ابتدا اقدام به سرقت اطلاعات کرده و سپس با سرور خود از طریق FTP ارتباط برقرار کرده و اطلاعات جمع‌آوری شده را که در قالب یک فایل HTML ذخیره کرده است، به آن ارسال می‌کند. علاوه بر آن، این ماژول توانایی دارد با دریافت دستورات از سرور خود، فایل بدافزار را با نسخه‌های جدیدتر به روزرسانی کند.

یکی دیگر از قسمت‌های مربوط به این ماژول مربوط به ایجاد یک فایل bat به نام Temptemp.bat است. این فایل توسط ماژول اجرا شده و بعد از اجرا توسط خود ماژول بدافزار پاک می‌شود. محتوای فایل bat به صورت زیر است.

```
@echo off
There:
del "C:\Windows\Microsoft.NET\Framework\v2.0.50727vbc.
exe"
if exist "C:\Windows\Microsoft.NET\Framework\
v2.0.50727vbc.exe" goto there
del %0
```

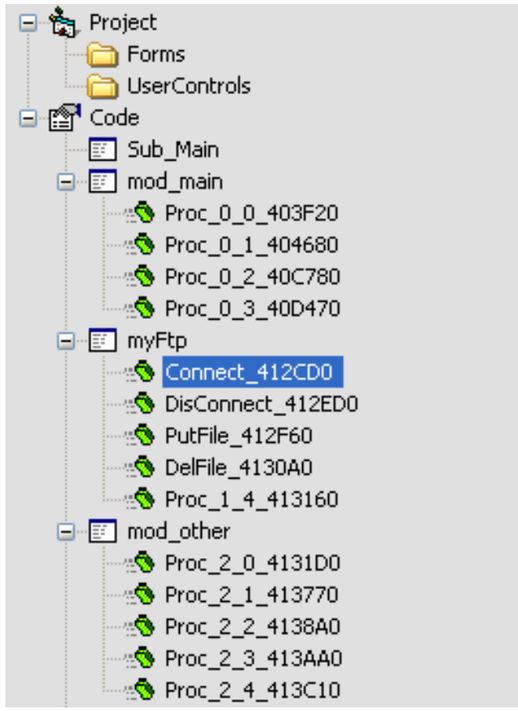
همان طور که مشاهده می‌کنید دستورات نوشته شده در این فایل bat اقدام به پاک کردن فایلی به نام v2.0.50727vbc.exe در مسیر C:\Windows\Microsoft.NET\Framework می‌کند. این فایل شناخته شده نیست و در سیستم قربانی نیز وجود نداشته است.

علاوه بر مراحل ذکر شده، این کد خود اقدام به تزریق کد می‌کند که روش استفاده شده برای این تزریق را در شکل ۳ مشاهده می‌کنید.

کد سوم تزریق شده در حقیقت یک ماژول سالم است که تولید شده توسط شرکت معروف Nirsoft می‌باشد. این ماژول با هدف بازیافت گذرواژه‌های پست‌های الکترونیکی (Email Password Recovery) کاربران طراحی شده است. بدافزار با استفاده از این ماژول اقدام به جمع‌آوری گذرواژه‌های پست‌های الکترونیکی قربانی کرده و آن‌ها را سرقت می‌کند.

راه های پیش گیری از این گونه خطرات

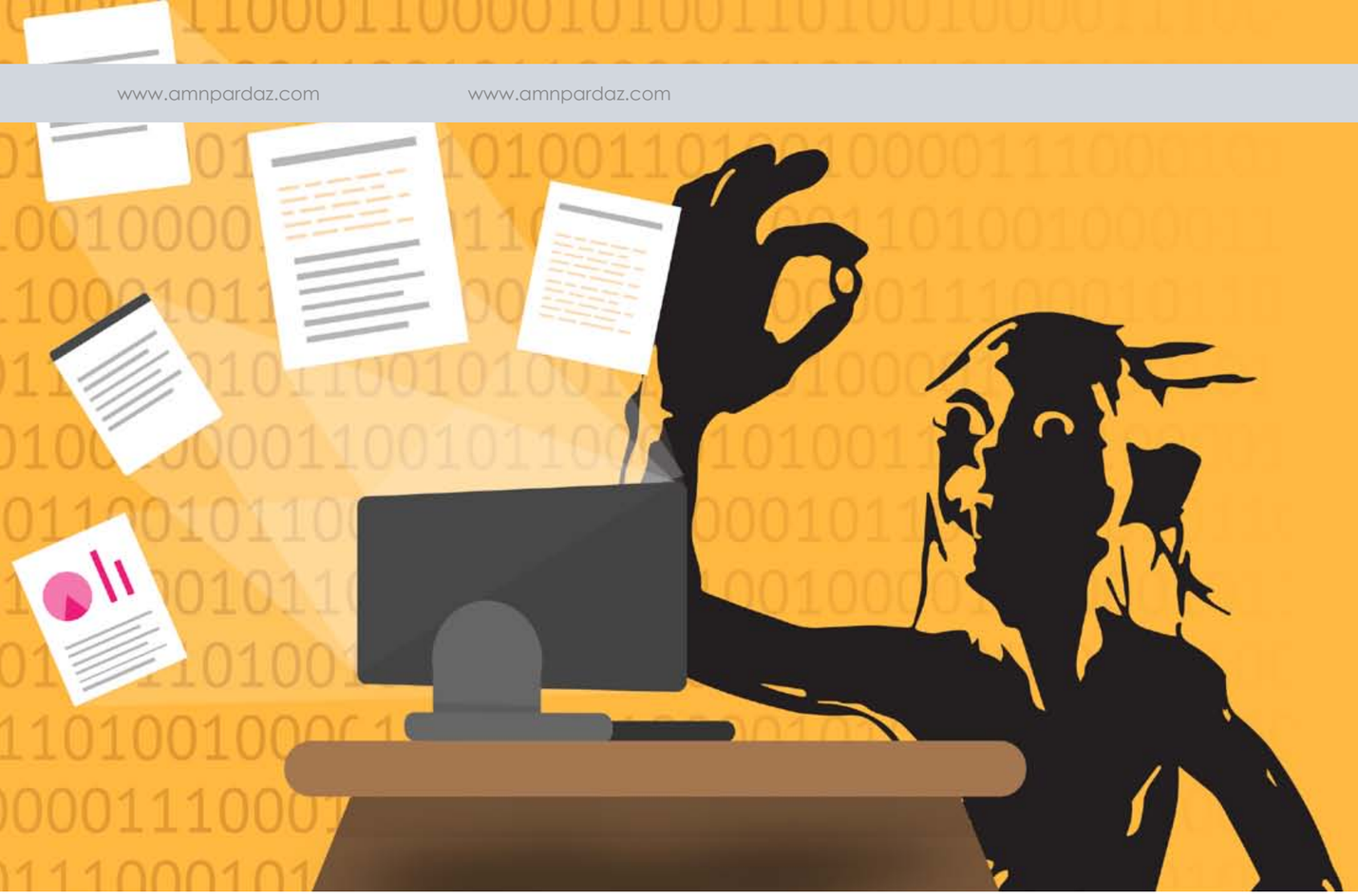
اکثر این نوع حملات با استفاده از فریب کاربران عادی با روش‌های مختلف صورت می‌گیرد که به اصطلاح به آنها Social engineering می‌گویند.



رعایت نکات زیر می‌تواند تا حد زیادی باعث جلوگیری از این گونه کلاهبرداری ها شود:

- ایمیل‌هایی که از طرف اشخاص ناشناس فرستاده می‌شود را باز نکنید.
- فایل‌هایی که از طریق پیوست ارسال می‌شود و از نوع اجرایی می‌باشد و پسوندی مانند exe،src و... دارند را اجرا نکنید.
- بر روی لینک‌هایی که از طرف افراد غیر معتبر برای شما فرستاده می‌شود کلیک نکنید.
- آنتی ویروس خود را همیشه به روز نگه دارید تا در صورت آلوده شدن، سیستم شما پاک‌سازی شود.

www.amnpardaz.com



رُستوک[1]، ارباب حُقّه‌ها

بدافزار روسی رُستوک از جمله روت‌کیت‌های ارسال کننده هرزنامه است که برای اولین بار در نوامبر سال ۲۰۰۵ مشاهده شد. این بدافزار برای پنهان سازی عملیات خود از تکنیک های پیشرفته ای بهره برد که تا آن موقع درمیان روت‌کیت ها بی نظیر بود. می توان براساس رفتار رُستوک روی سیستم قربانی، آن را به سه گونه متفاوت تقسیم کرد که آخرین بررسی های انجام شده نشان می دهد گونه سوم آن (با نام Rustock.C معروف است) رفتار مخفیانه تری از دیگر گونه های بدافزار دارد.

نکات قابل توجه که در نتیجه تحلیل این بدافزار به دست آمده است را در چند بخش به شرح زیر می‌توان بیان کرد:

• رمزگذاری: رُستوک دارای دو بخش اجرایی dropper و درایور می باشد که هر دو بخش با استفاده از الگوریتم های فشرده‌سازی و رمزنگاری Rc4 و Aplib کد شده و طی روند اجرا رمزگشایی خواهند شد. از جمله نقاط قوتی که می‌توان در این بدافزار به آن اشاره نمود وجود رمزگذارهای چندلایه است. بدافزار با استفاده از jumpهای چندریختی که به کدهای spaghetti معروف هستند، سعی می‌کند روال تحلیل را برای تحلیلگران دشوار ساخته و با تکیه بر هوک هایی که بر روی توابع هسته انجام می‌دهد، دسترسی و تغییر علائم حیاتی خود را کنترل کند. در بسیاری از نسخه ها نیز درصورت دیباگ و دسترسی باعث بروز BSOD[2] در سیستم قربانی می‌شود.

• فایل سیستم مورد استفاده: شروع کار بدافزار با اجرای dropper آغاز خواهد شد که مسئولیت تولید فایل درایور را برعهده دارد. براساس نوع گونه بدافزار که بر روی سیستم قربانی اجرا شده است، درایور مورد نظر در یکی از مسیرهای C:\windows یا C:\windows\system32\drivers به صورت فایل یا ADS قرار گرفته و با شروع سرویس روی آن، روت‌کیت به عنوان یک سرویس هسته به اجرا درخواهد آمد. لازم به ذکر است که در گونه های اولیه dropper، درایور بدافزار به جای یکی از درایورهای سیستمی همانند Beep.sys یا null.sys کپی می شده و بعد از بارگذاری در حافظه، محتوای اصلی درایور سیستم بر سرجای خود بازگشت داده می‌شد. یکی از نقاط قوتی که در آن زمان، این بدافزار را به بدافزاری پنهان از دید ضدویروس ها تبدیل کرده بود استفاده از Alternative Data Stream روی پوشه C:\windows\system32 بود. ADS[3]ها در واقع رشته هایی هستند که هرفایل یا پوشه‌ی موجود در فایل سیستم می‌تواند برای ذخیره اطلاعات از آن ها استفاده کند که البته این رشته ها می‌توانند محتوای اجرایی داشته باشند. بسیاری از ضدویروس ها در آن زمان از پویش این اطلاعات اجتناب کرده و متوجه حضور این بدافزار نمی‌شدند.

• از جمله تکنیک های بسیار نادری که درایور بدافزار در ابتدای روال اصلی اجرای کد خود از آن استفاده می‌کند، هوک کردن آدرس SYSENTER_EIP (MSR 0x176) است که به تابع KiFastCallEntry اشاره می‌کند. روت‌کیت با این ترفند سعی می‌کند فراخوانی هایی که روی توابع شروع شونده با حروف Zw انجام می‌گیرد را کنترل نماید و در صورت هرگونه استفاده از این توابع برای خواندن کلید رجیستری خود، باعث BSOD شود.

• پنهان سازی و عدم دسترسی فایل: از دیگر ترفندهای پنهان ساز فایل، که علاوه بر رُستوک توسط بدافزاری همانند TDL نیز استفاده شده است هوک کردن IofCallDriver pI است. اکثر بدافزارهایی که از این تکنیک استفاده می‌کنند، تمامی IRPهای ارسالی به درایورها را پویش کرده تا در نهایت IRPهای مدنظر خود را فیلتر کنند. رُستوک نیز با دو هدف خاص از این هوک استفاده می‌کند. یکی پنهان سازی نام فایل خود از میان فایل های یک دایرکتوری و دیگری پنهان سازی و منع دسترسی به فایل ADS خود است که به ترتیب مربوط به استفاده از IRP_MJ_DIRECTORY_CONTROL و IRP_MJ_QUERY_INFORMATION می‌شود. از دیگر تکنیک های معروفی که توسط این بدافزار مورد استفاده قرار گرفته است، هوک بر روی تابع IRP_MJ_CREATE از درایور Ntfs است. در برخی نسخه های رُستوک که فایل روت‌کیت از دیدها پنهان نیست هر فراخوانی روی فایل باعث منع دسترسی به آن می شود.

• بقای روت‌کیت: یکی از ترفندهای رُستوک برای بقای خود روی سیستم قربانی، بازنویسی مداوم فایل درایور است. حتی اگر فایل بدافزار توسط ابزارهای متفاوت ضدویروس پاکسازی شود، یکی از نخ هایی که سمت هسته توسط درایور روت‌کیت ایجاد شده است آن فایل را مکرراً بازنویسی خواهد کرد. همین نکته باعث شده تا این بدافزار از دسته بدافزارهایی محسوب شود که پاکسازی سیستم قربانیان را دشوار کرده و یک راه چاره را پاکسازی به هنگام شروع مجدد ویندوز قرار دهد.

• ارسال هرزنامه: نسخه هایی از این روت‌کیت در زمان خود از قویترین بدافزارهای ارسال کننده هرزنامه به شمار می‌آمده‌اند. برای ارسال هرزنامه از سمت کاربر، روت‌کیت نیازمند اجرای بخش هایی از کد و توابع خود درون پردازه های سیستم است. بنابراین با استفاده از تزریق APC[4] به پردازه‌ی services.exe و نگاشت بخشی هایی از Image درایور و کدهای ارسال هرزنامه درون پردازه موفق به راه اندازی ارسالگر هرزنامه خود شده و کار خود را به سرانجام می‌رساند.

برای مطالعه گزارش کامل تحلیلی این بدافزار به بخش گزارش‌های تحلیلی در سایت ضدویروس پادویش مراجعه نمایید:

http://www.padvish-antivirus.com/types.php/6

1. Rustock
2. Alternative Data Stream
3. Blue Screen of Death
4. Asynchronous Procedure Call

پَکِرها، ابزارهایی در دست ویروس‌نویسان!

یک فایل اجرایی (exe) دنباله‌ای است از اعداد باینری که شامل بخش‌های کد و داده می‌باشد. فایل‌های اجرایی استاندارد که توسط کامپایلر ایجاد می‌شوند را به راحتی می‌توان تحلیل کرد. یعنی می‌توان با استفاده از ابزارهای موجود همانند دیباگرها، کدهای موجود در فایل را مورد بررسی قرار داده و به رفتار و شیوه عملکرد آنها پی برد.

امروزه برنامه نویسان و شرکت‌های برنامه نویسی علی‌الخصوص ویروس نویسان برای اینکه افراد به راحتی نتوانند به کدهای نوشته شده توسط آنها نفوذ کنند و محافظت از برنامه های خود، فایل اجرایی برنامه را قبل از انتشار با استفاده از ابزارهایی به نام پَکر ، پَک[2] می‌نمایند. پَک کردن اصطلاحی است که به صورت کلی برای تغییر شکل دادن فایل‌های اجرایی به کار برده می‌شود. پکرها نیز ابزارهایی هستند که با دریافت یک فایل اجرایی به عنوان ورودی، تغییراتی را در دنباله باینری اعم از کد و دیتای آن ایجاد می‌کنند تا شکل ظاهری آن با فایل اصلی متفاوت باشد، اما رفتار آن بدون تغییر باقی بماند.

تغییر شکل ظاهری فایل اجرایی، علاوه بر اینکه تحلیل و نفوذ به کد این فایلها را دشوار می‌سازد، دارای مزیت مهم دیگری نیز برای ویروس‌نویسان می‌باشد. آنتی ویروس‌ها در مرحله اول برای تشخیص ویرس‌ها از امضای باینری استفاده می‌کنند، حال با تغییر شکل ظاهری ویروس با استفاده از پکر، به دلیل اینکه امضای موجود در ویروس نیز تغییر می‌یابد، آنتی ویروس‌ها از طریق امضای باینری قادر به شناسایی ویروس نیستند و باید از روش‌های دیگری بهره بگیرند.

پکرهای مختلف دارای مکانیزم و اهداف متفاوتی می‌باشند. بعضی از پکرها همانند upx برای فشرده‌سازی و کاهش حجم فایل مورد استفاده قرار می‌گیرند. در این نوع پکرها هدف اصلی فشرده‌سازی فایل می‌باشد و معمولا مکانیزمی برای جلوگیری از تحلیل وجود ندارد. برنامه نویسان نیز برای اهداف مختلف همانند آسان بودن انتقال فایل، از این نوع پکرها استفاده می‌کنند. برخی دیگر از پکرها، بیشتر برای محافظت و جلوگیری از نفوذ به کد برنامه مورد استفاده قرار می‌گیرند. این نوع پکرها در واقع بخش‌هایی به فایل اجرایی اضافه می‌کنند که معمولا حجم فایل نهایی را افزایش می‌دهند و همچنین افراد به راحتی قادر نخواهند بود این فایلهای را با استفاده از ابزارهای موجود تحلیل کنند و به کد اصلی دست پیدا کنند. اخیرا استفاده از این نوع پکرها در بین ویروس‌نویسان حرفه‌ای متداول شده‌است، بدین دلیل که آنتی‌ویروس‌ها به راحتی قادر به درک رفتار اصلی فایل و همچنین تهیه امضا از این فایل‌ها نیستند.

پکرها از نگاهی دیگر به دو دسته چندریختی[3] و غیر چندریختی تقسیم می‌شوند. در پکرهای چندریختی، در هر دفعه پک کردن فایل با استفاده از این پکرها، فایلهای متفاوتی تولید می‌شود، اما در پکرهای غیر چندریختی، در هر دفعه پک کردن یک فایل با استفاده از این پکرها، فایل خروجی یکسانی تولید خواهد شد.

بر اساس آمار بیان شده در shadow server[4] ، در حال حاضر پکر upx متداول ترین پکر بین ویروس‌نویسان می‌باشد. از دلایل این امر می‌توان به رایگان بودن این پکر اشاره کرد. یکی از دلایل دیگر برای متداول بودن پکر upx این است که این پکر به راحتی میتواند هر نوع فایلی را بدون ایجاد مشکل در رفتار آن پک نماید. برخی دیگر از متداولترین پکرها عبارتند از:

۱. Aspack
۲. Pecompact
۳. Fsg
۴. Themida
۵. Packman

در مقابل پکرها، ابزارهایی به نام آنپکر نیز وجود دارند که کار آنپک کردن را انجام می‌دهند. این ابزارها با دریافت فایل‌های پک شده، فایل اصلی را از داخل آن استخراج می‌کنند. یکی از روش‌هایی که آنتی‌ویروس‌ها از طریق آن ویروس‌های پک شده را شناسایی می‌کنند، استفاده از آنپکر می‌باشد.

1. Packer
2. Pack
3. Polymorph
4. https://www.shadowserver.org/wiki/pmwiki.php/Stats/PackerStatistics

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