شماره چهارم – نیمه دوم آذر ۱۳۹۶

خبرنامه "آپا" دانشگاه محقق اردبیلی

در این شماره می‌خوانیم:

- ✓ مهم ترین نگرانی‌های امنیت سایبری سال ۲۰۱۸
- ✓ هشدار ۹۱٪ متخصصان امنیت سایبری درباره استفاده هکرها از هوش مصنوعی
- ✓ شاخص‌ترین آسیب‌پذیری‌های سامانه‌های وب
- ✓ دانلود میلیونی برنامه ربودن پسورد
- ✓ توصیه‌های قابل اطمینان اما غیرعملی گروه ICS-CERT درباره بروزرسانی آنتی‌ویروس‌ها در سازمان‌ها
- ✓ استفاده بدافزار سیستم‌عامل مک از یک روش مخفی‌شدن خلاقانه
- ✓ رایانه غیرقابل هک؛ یک گام نزدیک‌تر به واقعیت
- ✓ انفجار گوشی به دلیل بدافزار خطرناک اندرویدی
- ✓ بدترین پسوردهای سال ۲۰۱۷
- ✓ ParseDroid تهدیدی برای همه برنامه‌های توسعه داده شده اندروید
- ✓ شیوع باج افزار جدید بانکی با نام Spider
- ✓ کشف حفره بزرگ خطرناک در برنامه‌های بانکی ۱۰ میلیون کاربر

045 31505718
cert@uma.ac.ir
اردبیل - خیابان دانشگاه - دانشگاه محقق اردبیلی

مهم ترین نگرانی‌های امنیت سایبری سال ۲۰۱۸

پیش بینی‌های ارائه شده در این مطلب، تنها چند نمونه از تهدیدات امنیتی خواهد بود که در سال جدید میلادی با آن‌ها روبرو خواهیم شد. راهکارهای ارائه شده نیز علاوه بر اینکه باید چندین لایه حفاظتی ارائه دهد، باید با تغییر ماهیت تهدیدات نیز تغییر یابد.

در سال ۲۰۱۷ برخی از بزرگترین تهدیدات امنیتی چند سال اخیر اتفاق افتاد. در این سال، شاهد تحت تاثیر قرار گرفتن میلیون‌ها فرد تا هزاران شرکت توسط تهدیداتی مانند حمله WannaCry و نشت اطلاعاتی شرکت‌های Equifax و Uber بوده‌ایم. براساس گزارش‌های موسسه گارتنر(Gartner) تا پایان سال ۲۰۱۷ هزینه‌های برقراری امنیت اطلاعات بالغ بر ۸۶,۴ میلیارد دلار خواهد بود و طبق پیش‌بینی‌های موجود در گزارش cybersecurityventures، میزان خسارات جرائم سایبری تا سال ۲۰۲۱ به مبلغ سالیانه ۶ تریلیون دلار خواهد رسید.

اما شرکت‌ها چگونه می‌توانند خود را از خطرات حملات سایبری سال بعد در امان نگه دارند؟ در ادامه با ۵ موردی که احتمال مواجهه با آن‌ها در سال ۲۰۱۸ وجود دارد و نیازمند توجه و مراقبت می‌باشد، آشنا خواهیم شد.

۱. اولویت قرار گرفتن استخراج ارز الکترونیکی با استفاده از توان محاسباتی قربانیان برای مجرمان سایبری

روش جدید استخراج ارز الکترونیکی (مانند بیت‌کوین، اتریم و...) با استفاده از توان محاسباتی سیستم‌های قربانی (Cryptojacking)، از اواخر سال ۲۰۱۷ شروع و به احتمال زیاد در سال ۲۰۱۸ با توجه به رشد فزاینده ارزش این ارزها با شدت بیشتری ادامه پیدا خواهد کرد. با توجه به مبهم بودن تشخیص این گونه فعالیت‌های مجرمان سایبری از کاربران عادی، این فعالیت جذابیت بیشتری برای مجرمان سایبری پیدا می‌کند. این جذابیت به این دلیل می‌باشد که علاوه بر مهاجمان، صاحبان وبسایت‌ها نیز می‌توانند از توان پردازشی سیستم‌های بازدیدکنندگان خود جهت انجام فعالیت‌های استخراج ارز الکترونیکی استفاده کنند. در چنین شرایطی به احتمال زیاد، چنین فعالیت‌های استخراج می‌توانند جایگزین نمایش تبلیغات بر روی وب‌سایت‌ها شده و به روش جدید درآمدزایی تبدیل شوند. با این حال بخش بزرگی از این روش برای وب‌سایت‌های قانونی مورد نفوذ قرار گرفته توسط مهاجمان برای استخراج ارز، مورد استفاده قرار خواهد گرفت.

۲. افزایش حملات مبتنی بر PowerShell

در ابتدای سال جاری بخش‌هایی از دولت عربستان سعودی مورد نفوذ قرار گرفت؛ این نفوذ از طریق یک ماکرو برنامه Microsoft Word جهت آلوده‌سازی کامپیوتر هدف با یک تروجان سرقت اطلاعات انجام شده بود. در این حمله ابتدا تعدادی وبسایت مورد نفوذ قرار گرفته بود که بعدا برای گم کردن ردپای خود، از آن‌ها به عنوان سرور پروکسی برای واحد کنترل بدافزار استفاده شده بود. این بدافزار برای برقراری ارتباط پایدار بر روی دستگاه و ارتباط با واحد کنترل خود از یک اسکریپت مخرب استفاده می‌کرد. حملات مبتنی بر اسکریپ مخرب، به طور خاص از PowerShell در حملات خود استفاده می‌کنند. شناسایی این حملات کار دشواری می‌باشد و به راحتی قابلیت دور زدن آنتی‌ویروس‌ها را داشته و جذابیت دوچندان برای مجرمان سایبری ایجاد می‌کند. پس احتمالا با حملات بیشتری بر اساس PowerShell روبرو خواهیم شد.

۳. افزایش رشد مجرمان زیرزمینی

درحالی که به نظر می‌رسد در وضعیت کنونی از هرسو تحت تاثیر حملات سایبری قرار داریم، تعداد این حملات در سال ۲۰۱۸ کاهش نخواهد یافت. با توجه به اینکه ابزارهای مخرب جدید برای استفاده به دانش کمتری نیاز دارند، تعداد حملات سایبری رو به افزایش نیز خواهد بود. این رشد دلایلی همچون پوشش رسانه‌ای بیشتر و نمایان شدن میزان سود بالای ناشی از حملات سایبری

آدرس: دانشگاه محقق اردبیلی، دانشکده فنی و مهندسی، مرکز آپا دانشگاه محقق اردبیلی ۳۱۵۰۵۷۱۸(۴۵)
cert.uma.ac.ir | cert@uma.ac.ir

دارد. بعنوان مثال باج‌افزارها در سال گذشته درآمد یک میلیارد دلاری برای مجرمان سایبری داشته است. تابویِ بودن یک مجرم سایبری دیگر شکسته شده و حتی در قسمت‌هایی از جهان مجرمان سایبری با صفات منفی شناخته نمی‌شوند و این کار به عنوان یک تجارت پرسود شناخته می‌شود. از سوی دیگر مجرمان سایبری متخصص و حرفه‌ای نیز با تمرکز و قدرت بیشتری برای کسب سود بیشتر به انجام فعالیت می‌پردازند. همچنین ممکن است در آینده شاهد تجارت‌های مجرمانه چندملیتی با استراتژی‌های پیچیده برای به دست آوردن میزان سود بیشتر و همچنین گم کردن ردپای خود باشیم.

۴. مورد هدف قرار گرفتن خود نرم‌افزارهای امنیتی

در سال ۲۰۱۸ مجرمان سایبری نرم‌افزارهای امنیتی بیشتری را مورد حمله و سوء استفاده قرار خواهند داد. با هدف قرار دادن نرم‌افزارهای مورد اطمینان و سخت افزار، حمله‌کنندگان می‌توانند دستگاه‌ها و کاربران را کنترل نمایند. هکرها محصولات امنیتی را مورد نفوذ و بهره-برداری قرار خواهند داد تا بتوانند با دزدیدن و ارسال ترافیک سرویس‌های ابری به هدف خود دست یابند. با نمایان شدن این اتفاقات(آلوده شدن و سوءاستفاده از برنامه‌ها) دیدگاه افراد و شرکت‌ها نسبت به برنامه‌های امنیتی، به خصوص آنتی ویروس‌ها تغییر کرده و روندی منفی را خواهد داشت.

۵. افزایش جرایم سایبری استفاده‌کننده از بدافزارهایی با رفتار مشابه کرم رایانه‌ای

در سال ۲۰۱۷، ما WannaCry و Trickbot را داشتیم که با استفاده از رفتار مشابه کرم به شیوع بدافزار (خود) پرداختند. در سال ۲۰۱۸ نیز با توجه به بیشتر بودن سرعت پخش این روش نسبت به سایر روش‌ها، بدافزارهای بیشتری از آن برای شیوع خود در شبکه استفاده خواهند کرد. اگر هکرها بتوانند روشی را برای استفاده از روش کرم بدون اینکه باعث ایجاد علائم آشکار شوند(مشکل قدیمی این روش)، این روش به سرعت قربانی زیادی را برای آن‌ها به همراه خواهد داشت.

در پایان دوباره یادآور می‌شویم که این پیش‌بینی‌ها تنها چند نمونه از تعداد زیادی از تهدیدات در سال ۲۰۱۸ خواهد بود. همچنین همه ساله شاهد تغییر و بلوغ روش های نفوذ برای وارد کردن خسارت بیشتر هستیم. آیا نفر بعدی این حملات ما هستیم؟ سوالیست که نمی‌توانیم به آن جوابی بدهیم!

در عین حال افزایش هوشیاری، مطالعه و آموزش کارهایی است که باید انجام دهیم. کارمندان بخش IT شرکت‌ها، پیشگامان این میدان نبرد بوده و می‌توانند با هشداردهی به کارمندان شرکت و اینکه تنها با یک کلیک نکردن می‌توانند جلوی ساعت‌ها کار را بگیرند سهم به سزایی را داشته باشند. در سال جدید با افزایش راهکارهای امنیتی و روش‌های مقابله با تهدیدات می‌توان به مقابله و جنگ با بدافزارها پرداخت.

منبع : csoonline مترجم: مهندس وحید فتحی

هشدار ۹۱٪ متخصصان امنیت سایبری درباره استفاده هکرها از هوش مصنوعی

بر طبق گزارشی جدید از Webroot بیش از ۹۰٪ متخصصان امنیت وب، نگرانی‌هایی درباره استفاده مهاجمان از هوش مصنوعی در حمله به شرکت‌ها دارند؛ این حمله‌ها نسبت به روش‌های دیگر بسیار پیچیده‌تر بوده و شناسایی آن‌ها سخت‌تر است.

استفاده از هوش مصنوعی هم دارای مزایا و هم تهدیداتی برای امنیت سایبری است: در حالی که این فناوری می‌تواند به شرکت‌ها کمک کند تا کاستی‌های امنیتی خود را تکمیل کنند و از اطلاعات حفاظت کنند؛ در عین حال به مهاجمان ابزار جدیدی برای حمله داده است. در ماه آگوست، محققان موفق به ساخت نوعی هوش مصنوعی شدند که قادر است با تغیر بدافزار، نرم‌افزار آنتی‌ویروس مجهز به مکانیزم ویروس‌یابی با یادگیری ماشین را دور بزند. طبق گفته ZDNet، حملات سایبری رایج مانند فیشینگ اگر توسط هوش مصنوعی طراحی شده باشند بسیار مخرب‌تر خواهند بود.

Webroot در یک نظرسنجی بیش از ۴۰۰ نفر از کارشناسان امنیت سایبری در شرکت‌هایی با ۱۰۰ نفر یا بیشتر کارمند را در ایالات متحده و ژاپن را مورد بررسی قرار داد. Webroot بر این عقیده است که ایالات متحده از پیشگامان استفاده از هوش مصنوعی برای امنیت سایبری است: ۸۷ درصد از کارشناسان امنیت سایبری ایالات متحده گزارش می‌دهند که شرکت‌هایشان در حال حاضر از هوش مصنوعی به عنوان بخشی از استراتژی امنیت سایبری خود استفاده می‌کنند. علاوه بر این، با توجه به بررسی‌های انجام شده سه چهارم از مختصصان امنیت سایبری معتقدند که در سه سال آینده، سازمان‌های آن‌ها قادر نخواهند بود بدون استفاده از هوش مصنوعی از تجهیزات خود محافظت کنند.

طبق یافته‌های Webroot تقریبا تمام متخصصان امنیت سایبری (۹۹ درصد) بیان کردند که معتقدند هوش مصنوعی می‌تواند امنیت سازمان‌های آن‌ها را بهبود بخشد. از جمله کمک‌های هوش مصنوعی، تشخیص تهدیداتی است که بدون استفاده از هوش مصنوعی قابل شناسایی نبودند که در نتیجه باعث کاهش میزان مثبت کاذب‌ها(false positive - نتایجی که به اشتباه مثبت ارزیابی می‌شوند) می‌شود. ۹۷ درصد از این کارکنان اظهار داشتند که شرکتشان قصد دارد در سه سال آینده بودجه‌های مربوط به هوش مصنوعی و ابزارهای یادگیری ماشین را افزایش دهند. Hal Lonas، مدیر فناوری اطلاعات Webroot، در بیانیه مطبوعاتی خود گفت: "هیچ شک و تردیدی در مورد اینکه هوش مصنوعی آینده امنیت است وجود ندارد، چرا که این حجم از تهدیدات به تنهایی توسط انسان قابل ردیابی نیست."

Webroot چهار راهکار زیر را برای ترکیب هوش مصنوعی و تکنولوژی‌های یادگیری ماشین به سازمان‌ها ارائه می‌دهد:

۱. **استخدام و گسترش متخصصان هوش مصنوعی/یادگیری ماشین.** بر خلاف باور عموم، این تکنولوژی‌ها نمی‌توانند جایگزین انسان شوند و استفاده از آن‌ها نیازمند آموزش و نظارت انسانی است.

۲. **خلاقانه فکر کنید.** همانطور که مجرمان سایبری به استفاده از هوش مصنوعی و یادگیری ماشین برای تولید تهدیدات پیشرفته ادامه می‌دهند، متخصصان سایبری باید با تفکر خلاقانه از خطرات جدید جلوگیری کنند. ماشین‌ها می‌توانند با انجام خودکار بعضی از وظایف دستی، زمان بیشتری برای نیروی انسانی ایجاد کنند تا این زمان صرف فکر کردن در مورد راه‌های جدید برای شناسایی تهدیدات و حل مشکلات شود.

۳. **از اشتباهات خود درس بگیرید.** مورد نفوذ قرار گرفتن سامانه‌ها، بیشتر مسئله "کی اتفاق می‌افتد؟" است تا اینکه "آیا اتفاق می‌افتد؟". شرکت‌ها باید رویکردی را در پیش بگیرند که در آن با درک بیشتر تهدیدات و نحوه پاسخ به آن‌ها از اشتباهات امنیتی پیشین خود درس بگیرند تا حملات بعدی را بهتر مدیریت کنند.

۴. **خودکار سازی.** گسترش هوش مصنوعی و تکنولوژی‌های مبتنی بر یادگیری ماشین به وظایفی مانند اجرای سیاست امنیتی، مسدود کردن فایل‌ها و IP-های مخرب و محافظت در برابر حملات فیشینگ (phishing) کمک می‌کند.

منبع : techrepublic

مترجم: نیلوفر زبردست

شاخص‌ترین آسیب‌پذیری‌های سامانه‌های وب

OWASP مخفف عبارت Open Web Application Security Protocol Project می‌باشد و یک پروژه با دسترسی آزاد است که در آن معیارهایی که باید برای امن‌تر شدن نرم افزارها بکارگرفته شود؛ تشریح شده است.

به دلیل گستردگی تکنولوژی‌های وب و همچنین پیچیدگی ساختارهای برنامه‌نویسی و مبحث امنیت، پروژه‌ی OWASP به ۹ پروژه مختلف تقسیم شده است. یکی از این پروژه‌ها OWASP Top Ten می‌باشد که هدف آن اطلاع رسانی در خصوص امنیت برنامه‌های کاربردی وب است و مهم‌ترین خطرات امنیتی برنامه‌های تحت‌وب بیان می‌شود. در همین راستا این نهاد هر چند سال یکبار لیستی از شاخص‌ترین آسیب‌پذیری‌های متداول در نرم‌افزارها و سرویس‌های تحت وب در سرتاسر جهان را ارائه می‌دهد. در ادامه ده آسیب‌پذیری شاخص سال ۲۰۱۷ بیان می‌شود.

OWASP Top 10 – 2017
A1 – Injection
A2 – Broken Authentication
A3 – Sensitive Data Exposure
A4 – XML External Entities (XXE)
A5 – Broken Access Control
A6 – Security Misconfiguration
A7 – Cross-Site Scripting (XSS)
A8 – Insecure Deserialization
A9 – Using Components with Known Vulnerabilities
A10 –Insufficient Logging & Monitoring

Injection: مشکلات تزریق از قبیل: تزریق SQL، OS و LDAP زمانی رخ می‌دهند که داده‌ی نامعتبر و غیر قابل اعتماد به عنوان یک دستور یا درخواست به یک مفسر مانند مفسر دستورات SQL ارسال می‌شود. نفوذگر می‌تواند مفسر را دچار اشتباه کرده و موجب اجرای دستورات ناخواسته و یا دسترسی به داده‌های حساس شود.

Broken Authentication: بسیاری از اوقات مکانیزم‌های مربوط به احراز هویت و مدیریت نشست، بصورت صحیح پیاده‌سازی نمی‌شوند و به نفوذگران اجازه می‌دهند تا به پسوردها، کلیدها، و توکن‌های نشست‌ها دسترسی داشته باشند و یا از مشکلات پیاده‌سازی دیگر سوء استفاده کنند و هویت کاربران دیگر را جعل کرده و از آن‌ها استفاده کنند.

Sensitive Data Exposure: بسیاری از برنامه‌های تحت‌وب، از اطلاعات حساس از قبیل کارت‌های اعتباری و اطلاعات احراز هویت محافظت نمی‌کنند و ممکن است نفوذگران، این داده‌ها را به سرقت ببرند یا آن‌ها را تغییر دهند تا جعل هویت یا سرقت هویت یا جرائم دیگری را انجام دهند. اطلاعات حساس نیاز به محافظت بیشتری از قبیل رمزگذاری در حین انتقال، یا احتیاط در مبادله داده‌ها با مرورگر دارند.

XML External Entities: بسیاری از پردازشگرهای قدیمی XML یا پردازشگرهایی با پیکربندی ضعیف، موجودیت‌های خارجی را با مستندات XML می‌سنجند. این موجودیت‌های خارجی می‌توانند برای افشای فایل‌های داخلی با کمک file URL handler، اشتراک فایل‌های داخلی، اسکن پورت‌های داخلی، تزریق کد و حمله محروم سازی از سرویس (DOS Attack) استفاده شوند.

Broken Access Control: محدودیت‌هایی که یک کاربر احراز هویت شده را محدود می‌کنند، گاهی اوقات به خوبی اعمال نمی‌شوند. نفوذگر از این جریان برای دسترسی به عملکردها و داده‌های سیستم استفاده می کند. برای مثال به حساب کاربری دیگران دسترسی پیدا کرده، فایل‌های حساس را می‌بینند، داده‌های کاربر را دستکاری می‌کند و حتی دسترسی‌ها را تغییر می‌دهد.

Security Misconfiguration: پیکربندی نادرست امنیتی نتیجه‌ی مجموعه‌ای از فعالیت‌ها مانند: استفاده از پیکربندی پیش‌فرض ناامن، پیکربندی بدون ساختار

مناسب، سرآیندهای HTTP با پیکربندی غلط و پیام‌های خطا که اطلاعات افشا می‌کنند، می‌باشد. همه سیستم-عامل‌ها، کتابخانه‌ها و چهارچوب‌ها نه تنها باید به صورت امن پیکربندی شوند، بلکه باید در اولین فرصت ارتقاع یافته و وصله شوند.

Cross Site Scripting (XSS): مشکلات XSS زمانی رخ می‌دهند که یک برنامه داده‌های مورد اعتماد را می‌گیرد و آن‌ها را بدون بررسی مناسب به مرورگر ارسال می‌کند. این آسیب پذیری به نفوذگر اجازه می‌دهد که در مرورگر قربانی، اسکریپت‌هایی را اجرا کند که می‌تواند منجر به سرقت نشست کاربر (session hijacking)، هک شدن وب‌سایت، یا هدایت کاربر به وب‌سایت‌های مخرب شود.

Insecure Deserialization: این آسیب‌پذیری نتیجه بازگردانی داده‌های سریال‌سازی‌شده به اشیا سریال-سازی‌نشده می‌باشد که منبع آن می‌تواند از طریق درخواست شبکه، فایل و ... باشد. اگر این فرآیند ناامن باشد برخی اوقات منجر به تزریق کد از راه دور می‌شود و حتی اگر تزریق کد از راه دور ممکن نباشد؛ می‌تواند برای حملات تزریق استفاده شود.

Using Components with Known Vulnerabilities: عناصر و مولفه‌های آسیب‌پذیر از قبیل توابع کتابخانه‌ای، چهارچوب‌ها و ماژول‌های نرم‌افزارهای دیگر، تقریبا همیشه با بالاترین سطح دسترسی در سیستم‌عامل اجرا می‌شوند. بنابراین زمانی-که مورد سوء استفاده قرار می‌گیرند، می‌توانند سبب از دست دادن اطلاعات مهم شوند. بنابراین قدرت دفاعی سیستم هنگام استفاده از این عناصر و مولفه‌های آسیب‌پذیر پایین می‌آید.

Insufficient Logging & Monitoring: عدم رویداد-نگاری و مانیتورینگ همراه با عدم کارایی و یا نبود مدیریت حادثه، زمینه لازم برای حملات بیشتر هکرها را فراهم می‌آورد. به این ترتیب هکرها کنترل سیستم را در دست می‌گیرند و داده‌ها را استخراج، دستکاری و یا از بین می‌برند. بررسی‌ها نشان می‌دهد که زمان تشخیص اشکالات بیش از ۲۰۰ روز می‌باشد و در بیشتر موارد نه تنها مانیتورینگ و فرآیندهای داخلی نمی‌توانند اشکالات را تشخیص دهند، بلکه کشف اشکالات توسط عضوهای خارجی صورت می‌گیرد.

منبع:OWASP مترجم: مهندس سمیرا سیفی

دانلود میلیونی برنامه ربودن پسورد

با وجود تلاش‌های فراوان گوگل برای جلوگیری از نفوذ نرم‌افزارهای مخرب، این نرم‌افزارها وارد فروشگاه Google Play می‌شوند. محققان حداقل ۸۵ برنامه در این فروشگاه کشف کرده‌اند که برای ربودن اطلاعات ورود کاربران شبکه اجتماعی VK.com استفاده شده‌اند. یکی از معروف‌ترین نرم‌افزارهای مخرب که میلیون‌ها بار دانلود شد، یک بازی بود که در ماه مارس ۲۰۱۷ بدون هیچ آسیب‌پذیری در گوگل قرار گرفت. این بازی پس از گذشت هفت ماه با کد آلوده‌ای برای ربودن اطلاعات شخصی به روزرسانی شد. خوشبختانه در حال حاضر تمام برنامه‌های مخرب از این فروشگاه حذف شده‌اند اما کاربرانی که این برنامه‌ها را قبلا دانلود کرده بودند، باید مطمئن شوند که قابلیت Google Play Protect را در دستگاه خود فعال کرده‌اند. Google Play Protect بخشی از برنامه فروشگاه Google Play می‌باشد که با استفاده از هوش‌مصنوعی و برنامه‌های تحلیلگر میزان استفاده منابع، برنامه‌های مخرب اندروید را پاک می‌کند. با این وجود نگرانی در مورد برنامه‌های آلوده همواره وجود دارد، به همین دلیل بهترین راه‌حل هوشیار بودن در هنگام دانلود برنامه‌ها و بازرسی و کنترل سطوح دسترسی برنامه می‌باشد. همچنین توصیه می‌شود تا یک آنتی ویروس قدرتمند نصب کنید تا بتواند چنین برنامه-های مخرب را قبل از اینکه تاثیری در دستگاه شما بگذارند، کشف کرده و از بین ببرد.

منبع خبر:thehackernews مترجم: مهندس سمیرا سیفی

توصیه‌های قابل اطمینان اما غیرعملی گروه ICS-CERT درباره بروزرسانی آنتی‌ویروس‌ها در سازمان‌ها

ICS-CERT به عنوان واحدی از NCCIC که تحت نظر وزارت امنیت آمریکا (DHS) کار می‌کند، تلاش دارد با به‌کارگیری سامانه‌های کنترلی و تسهیل در به‌اشتراک‌گذاری اطلاعات، با حوادث امنیتی مقابله کند و خطرهای حملات سایبری را کاهش دهد. آخرین "خبرنامه پایش" این سازمان درباره نحوه به‌روزرسانی آنتی‌ویروس‌ها در سامانه‌های صنعتی سازمان‌ها توصیه‌هایی ارائه کرده است. ICS-CERT بیان کرد: «آنتی‌ویروس‌ها زمانی که به درستی نصب و به‌روزرسانی شوند، بخش مهمی از رویکرد دفاع در عمق برای محافظت از سامانه‌ها در برابر بدافزارها را تشکیل می‌دهند. چنین نرم‌افزارهایی به طور گسترده در فناوری اطلاعات و زیرساخت‌های کنترل صنعتی مورد استفاده قرار می‌گیرند. در مجموعه‌های کوچک و سیستم‌های شخصی، آنتی‌ویروس‌ها را به صورتی تنظیم می‌کنند تا به طور مستقیم از طریق سرور آنتی‌ویروس به‌روزرسانی شوند؛ با این حال از آن‌جا که لازم است سیستم‌های فناوری اطلاعات و سامانه‌های کنترل صنعتی توسط معماری DMZ از همدیگر تفکیک شوند، سامانه‌های کنترل صنعتی نیاز دارند که از روش‌های به‌روزرسانی آنتی‌ویروس متفاوتی استفاده کنند.»

DMZ سامانه‌های کنترل صنعتی لایه‌ای بین منطقه سازمانی و شبکه کنترلی است. این DMZ علاوه بر سرورهای دسترسی از راه دور و ثبت‌کننده‌های رویدادهای سامانه، می‌تواند شامل آنتی‌ویروس و سرویس‌های به‌روزرسانی سرور ویندوز (WSUS) نیز باشد. از آن‌جایی که DMZ سامانه‌های کنترل صنعتی، معمولاً اجازه ندارد که به طور مستقیم به اینترنت متصل شود، به‌روزرسانی این سرویس‌ها نیز به طور خودکار از طریق سرور تولیدکنندگان آنتی‌ویروس نمی‌تواند انجام شود. یک روش برای به‌روزرسانی آنتی‌ویروس‌ها در این سامانه‌ها این است که به صورت دستی دانلود شده و یک کپی از آن‌ها در یک درایو قابل حمل مانند USB/DVD/CD قرار داده شوند و سپس این درایو به دستگاهی که به این به‌روزرسانی‌ها نیاز دارد متصل شود. با این حال این فرآیند آن‌طور که به نظر می‌رسد، ساده نیست. ICS-CERT به سازمان‌ها توصیه می‌کند که ابتدا منبع به‌روزرسانی منتشرشده را بررسی کنند و سپس فایل به‌روزرسانی را در یک هاست اختصاصی دانلود کنند. این فایل باید از نظر مخرب بودن مورد پویش قرار بگیرد و باید درهم‌ساز آن با اطلاعات درهم‌ساز فایل ارائه شده توسط تولیدکننده آن بررسی شود تا از عدم دستکاری فایل اطمینان حاصل شود. وقتی فایل‌های به‌روزرسانی کپی شدند، این درایو قابل حمل باید به منظور کشف بدافزار پویش شده و قفل شود (یعنی از نوشته شدن فایل‌های دیگر در آن جلوگیری شود). قبل از این‌که این به‌روزرسانی‌ها روی یک سیستم نهایی نصب شوند، باید روی یک محیط آزمایشی که تا حد امکان مشابه سیستم نهایی است، مورد آزمایش قرار گرفته و سالم بودن آن صحت‌سنجی شود.

کارشناسان امنیت، توصیه‌های گروه ICS-CERT را کاملاً عملی نمی‌دانند و هشدار می‌دهند که سازمان‌ها برای حفاظت از سامانه‌های حیاتی خود نباید تنها به آنتی‌ویروس‌ها متکی باشند.

یک کارشناس امنیت سامانه‌های کنترل صنعتی در آزمایشگاه کسپرسکی به نام Anton Shipulin اظهار کرد: «هرچند این روش (عمل انتقال فایل‌ها از یک سامانه به دیگری به وسیله یک درایور قابل حمل) برای به‌روزرسانی نرم‌افزارهای محافظتی مانند آنتی‌ویروس‌ها در شبکه‌هایی که با هم ارتباط فیزیکی ندارند، قابل استفاده است، اما در عمل، سازمان‌ها در به‌روز نگه داشتن سامانه‌های خود با مشکلاتی مواجه هستند. محصولات کسپرسکی اغلب در تحلیل شبکه‌های سیستم‌های کنترل صنعتی در خلال ارزیابی‌های خود،

آنتی‌ویروس‌هایی شامل پایگاه‌داده‌های بدافزاری قدیمی پیدا می‌کنند.»

این کارشناس توضیح داد: «برای این‌که این فرآیند کارا باشد، باید به صورت منظم انجام شود و نرم‌افزارهای امنیتی که از نظر فنی پیشرفته هستند به کار گرفته شوند. همچنین این امکان وجود داشته باشد که این نرم‌افزارها از سرورهای به‌روزرسانی متمرکز گرفته شوند؛ این روش که در آن به‌روزرسانی‌ها فقط به یک دستگاه واحد منتقل می‌شوند، سریع و آسان است. همچنین لازم به ذکر است که چنین فرآیندی باید برای تمام سیستم عامل‌ها و سامانه‌های کنترلی و به‌روزرسانی‌های نرم‌افزار دستگاه‌ها الزامی باشد (با توافق تامین‌کنندگان و تولیدکنندگان سامانه‌های کنترل صنعتی).»

Rick Kaun، معاون ارشد شرکت امنیت سایبری صنعتی Verve اظهار کرد: «اعمال دستی به‌روزرسانی‌ها می‌تواند بسیار پیچیده‌تر از فرآیند توصیف شده توسط گروه ICS-CERT باشد.»

وی توضیح داد: «به عنوان مثال، همه‌ی به‌روزرسانی‌های آنتی‌ویروس‌ها یکسان نیستند. اگر شما برای یک آنتی‌ویروس دارای ضمانت و پشتیبانی یک تولیدکننده به‌خصوص هستید، شما نه تنها باید فایل آنتی‌ویروس را دانلود کنید بلکه باید این فایل را از تولیدکننده آن بگیرید و یا حداقل مطمئن شوید که فروشنده مربوطه این فایل را تایید می‌کند. علاوه بر این بسیاری از سازمان‌ها ممکن است محصولات خود را از چند تولیدکننده مختلف خریداری کنند و هر کدام از این تولیدکننده‌ها محصولات آنتی‌ویروس متفاوتی را ارائه کنند، بنابراین شما نیاز دارید که این روش را روی بیش از چندین فایل روی چند سامانه اعمال کنید؛ مدیریت و ارائه گزارش از روند تکمیل این فرآیند یکی از چالش‌های پیش‌رو است.»

Kaun افزود: «اکنون بیایید نرخ انتشار به‌روزرسانی برای آنتی‌ویروس‌ها را مورد بررسی قرار دهیم. اگر فایل‌های مربوط به آنتی‌ویروس‌ها هر ماه یک‌بار به‌روزرسانی شوند، به احتمال زیاد این روند قابل مدیریت است. اگر این فایل‌ها به صورت هفتگی به‌روز شوند، روند به‌روزرسانی دستگاه‌ها بیشتر چالش برانگیز می‌شود. اکنون فرض کنید اگر فایل‌های آنتی‌ویروس به صورت روزانه و یا حتی سریع‌تر به‌روزرسانی شوند چه اتفاقی می‌افتد؟ موضع شرکت شما در رابطه با سرعت انتشار به‌روزرسانی آنتی‌ویروس‌ها چیست؟ این مسأله بسیار مهم است که به شکلی تصمیم‌گیری شود که یک تعادل مناسب بین راحتی و حداکثر حفاظت (جدیدترین و مناسب‌ترین فایل‌های به‌روزرسانی آنتی‌ویروس‌ها) برقرار باشد.»

این کارشناس گفت: «سازمان‌های بسیار کمی وجود دارند که قادرند دقت و نرخ به‌روزرسانی یک برنامه آنتی‌ویروس را چنان‌که در مقاله ICS مشخص شده، حفظ کنند. این مقاله به خوبی نوشته شده و توصیه‌های خوبی در آن ذکر شده است اما در مورد برنامه‌هایی که روز به روز تغییر می‌کنند بدون توجه به نیروی انسانی و ابزارهای خودکار چندان عملی نیست.»

اکثر کارشناسان معتقدند که برای حفاظت از سامانه‌های کنترل صنعتی، استفاده از آنتی‌ویروس‌ها به تنهایی کافی نیست. در حالی‌که سازمان‌های صنعتی اغلب نگرانند که نرم‌افزارهای امنیتی می‌توانند تاثیر منفی روی کارایی عملیات‌های آن‌ها داشته باشند، راه‌حل‌های جدیدِ مخصوص سامانه‌های کنترل صنعتی طراحی شده‌اند که در کنار ارائه راه‌کارهای حفاظتی جامع، کم‌ترین تأثیر را روی این سامانه‌ها داشته باشند. علاوه بر این آنتی‌ویروس‌ها نمی‌توانند به طور مستقیم روی دستگاه‌های کنترلی مانند PLCها و DCSها نصب شوند. با این حال محصولات جدید صرف‌نظر از نوع دستگاه هدف، به‌طور مداوم شبکه‌ها را برای یافتن فعالیت‌های مشکوک به صورت غیر مستقیم پایش می‌کنند.

Patrick McBride، مدیر ارشد بازاریابی در شرکت Claroty اشاره کرد که محصولات امنیتی که برای محیط‌های فناوری اطلاعات (IT) طراحی شده‌اند هرگز

نباید در شبکه‌های فناوری عملیاتی (OT) مورد استفاده قرار بگیرند.

Dana Tamir از شرکت Indegy نیز به یک نکته‌ی جالب دیگر اشاره کرد: «با این‌که آنتی‌ویروس‌ها تا حدی می‌توانند راه‌کارهای حفاظتی ارائه دهند (مخصوصا در برابر تهدیدات شناخته‌شده)، ممکن است حتی استفاده از آنتی‌ویروس‌های قدیمی نیز در برخی سازمان‌ها امکان-پذیر نباشد، زیرا بسیاری از سازمان‌ها در شبکه‌های ICS خود همچنان به سامانه‌های قدیمی مانند ویندوز NT و XP متکی هستند و ممکن است این سامانه‌های قدیمی توسط تولیدکنندگان آنتی‌ویروس‌ها پشتیبانی نشوند.»

این مسأله توسط یک مطالعه‌ی تحقیقاتی شرکت امنیت صنعتی CyberX نیز تایید شده است، این مطالعه نشان داد که سه مورد از چهار محیط صنعتی همچنان از سیستم‌عامل‌های قدیمی در شبکه‌های سامانه‌های کنترل صنعتی خود استفاده می‌کنند.

Phil Neray، معاون ارشد بخش امنیت سایبری صنعتی در CyberX گفت: «توصیه گروه ICS-CERT این واقعیت را نادیده می‌گیرد که بسیاری از محیط‌های ICS هیچ‌یک از وصله‌های امنیتی ویندوز را نصب نمی‌کنند و یا به دلیل استفاده از سیستم‌عامل‌ها پشتبانی‌نشده مانند ویندوز ۲۰۰۰ و XP از هیچ محصول آنتی‌ویروسی استفاده نمی‌کنند.»

Tamir همچنین اظهار کرد: «یک سازمان می‌تواند آنتی-ویروس‌هایی را روی تمام رایانه‌های مدیریت‌شده نصب کند. اما اگر از یک راه‌حل جامع برای دستگاه‌های مدیریت‌نشده استفاده نکند، تهدیدها می‌توانند از طریق دستگاه‌ها به شبکه‌ی ICS سازمان وارد شوند.»

منبع : securityweek مترجم: مهندس معصومه خیری

استفاده بدافزار سیستم‌عامل مک از یک روش مخفی‌شدن خلاقانه

بدافزار HiddenLotus یک نسخه جدید از بدافزار OceanLotus می‌باشد و از طریق یک برنامه به نام Lê Thu Hà یا HAEDC که دارای پسوند (extension) pdf. است و مانند یک فایل Adobe Acrobat به نظر می‌آید، توزیع می‌شود.

این برنامه از یک روش قدیمی برای این رفتار استفاده می‌کند. به این صورت که از ویژگی قرنطینه فایل که در سیستم عامل Leopard (Mac OS X 10.5) معرفی شده است و فایل‌های دانلود شده از اینترنت به صورت قرنطینه در نظر گرفته می‌شوند، استفاده می‌کند.

OceanLotus آخرین بار در تابستان سال جاری به صورت یک سند Word دیده شد و کاربران ویتنامی را هدف قرار داد. بدافزار جدید سطح جدیدی از تغییر ظاهر جهت مخفی‌سازی خود را به نمایش می‌گذارد. در حالی که بدافزار قبلی دارای یک پسوند app. مخفی بود که نشان می‌داد این فایل یک برنامه است، HiddenLotus در واقع دارای یک پسوند pdf. است و هیچ پسوند app. در این بدافزار جدید وجود ندارد.

براساس کشف Arnaud Abbati، این تهدید از یک پسوند مخفی استفاده می‌کند به این صورت که حرف d در پسوند pdf. درواقع عدد رومی D (نشان‌دهنده‌ی عدد ۵۰۰) به صورت حروف کوچک است.

شرکت Malwarebytes بیان می‌کند: «یک برنامه برای این‌که بتواند مانند یک برنامه رفتار کند، نیاز نیست که دارای یک پسوند app. باشد. برنامه در سیستم عامل مک در واقع یک پوشه با یک ساختار داخلی خاص به نام باندل (bundle) است. یک پوشه با یک ساختار مناسب همچنان فقط یک پوشه است. اما اگر یک پسوند app. به آن بدهید، آن پوشه در همان لحظه به یک برنامه تبدیل می‌شود.» به همین دلیل، برنامه مدیریت فایل سیستم-عامل مک (Finder) با آن مانند یک فایل رفتار می‌کند و وقتی روی آن دوبار کلیک شد، به جای باز کردن پوشه، مانند یک برنامه شروع به اجرای آن می‌کند. هنگامی که کاربر روی یک فایل یا پوشه دوبار کلیک می‌کند، سرویس اجرای برنامه‌ها (Launch Services) ابتدا پسوند آن را بررسی می‌کند و در صورتی که پسوند آن را

بشناسد، آن فایل یا پوشه را باز می‌کند. یک فایل با پسوند txt. به صورت پیش‌فرض توسط برنامه TextEdit باز می‌شود، بنابراین یک پوشه با پسوند app. نیز در صورتی که دارای ساختار داخلی درستی باشد، مانند یک برنامه اجرا خواهد شد. اگر پسوند توسط سیستم‌عامل شناخته نشده باشد، وقتی که کاربر می‌خواهد این فایل را باز کند، از او خواسته می‌شود تا یک برنامه برای باز کردن آن فایل انتخاب کند و یا در Mac App Store جست‌وجو کند. وقتی روی یک پوشه با پسوند ناشناس دوبار کلیک می‌شود، Launch Services ساختار داخلی پوشه را مورد بررسی قرار می‌دهد.

بدافزار HiddenLotus با این روش نفوذ می‌کند: انتقال‌دهنده بدافزار (dropper) یک پوشه با ساختار داخلی یک برنامه است. به خاطر استفاده از یک عدد رومی در پسوند pdf. و از آن‌جایی که برنامه‌ای روی دستگاه وجود ندارد که بتواند این پسوند را پشتیبانی کند، سیستم با آن مانند یک برنامه رفتار می‌کند؛ این در حالی است که فایل مورد نظر دارای پسوند app. نیست.

شرکت Malwarebytes می‌گوید: «هیچ نکته خاصی درباره این پسوند pdf. (با استفاده از عدد رومی d) وجود ندارد، به جز این‌که یک پسوند استفاده‌نشده در سیستم‌عامل مک می‌باشد. به همین دلیل هر پسوندی که استفاده نشده باشد با این روش کار می‌کند.»

پژوهش‌گران امنیتی همچنین اشاره کردند: «فهرست بسیار گسترده‌ای از پسوندهای احتمالی وجود دارد که عاملان مخرب می‌توانند از آن‌ها سوءاستفاده کنند، مخصوصا زمانی که از کاراکترهای یونیکد استفاده کنند. به همین دلیل، ممکن است کاربران فریب خورده و فایل‌هایی را باز کنند که به ظاهر مانند اسناد Word (دارای پسوند doc.)، Excel (دارای پسوند xls.) و یا اسناد Pages (دارای پسوند pages.) هستند.»

منبع : securityweek مترجم: مهندس معصومه خیری

رایانه غیرقابل هک؛ یک گام نزدیک‌تر به واقعیت

هک شدن رایانه‌ها مشکلی است که تاکنون راه‌حل قطعی برای آن یافت نشده، ولی در سال ۲۰۱۷ شاهد پیشرفت‌هایی در این زمینه بوده‌ایم.

وزارت دفاع آمریکا در سال ۲۰۱۷ بودجه‌ای ۵۰ میلیون دلاری را به برنامه دارپا اختصاص داده تا در قالب آن امنیت سایبری ارتقا یابد.

محققان دانشگاه میشیگان با استفاده از بخشی از این بودجه موفق به طراحی سیستم امنیتی تازه‌ای شده‌اند که با حفاظت ویژه از سخت‌افزارهای رایانه‌ای آن‌ها را غیرقابل هک می‌کند.

این محققان می‌گویند با طراحی انبوهی از باج‌افزارهای سارق اطلاعات که از آسیب‌پذیری‌های بی پایان ویندوز و دیگر سیستم‌عامل‌ها استفاده می‌کنند، باید از روش‌های نوینی برای از کارانداختن حملات هکری استفاده کرد. به خصوص که این حملات می‌توانند فعالیت‌های عادی بانک‌ها، بیمارستان‌ها، شرکت‌های تجاری و نهادهای دولتی را مختل کنند.

در قالب طرح تحقیقاتی جدید هفت نوع مختلف از مشکلات و ضعف‌های سخت‌افزاری شناسایی شده‌اند که در صورت برطرف شدن آن‌ها می‌توان تقریبا جلوی نیمی از حملات مبتنی بر ضعف‌های نرم‌افزاری را گرفت.

با تکمیل برنامه دارپا امید می‌رود تا ظرف پنج سال راهی برای غلبه بر هر هفت ضعف سخت‌افزاری شناسایی شده یافت شود. بر همین اساس به جای استفاده از برنامه‌های امنیتی نرم‌افزاری از راه‌حل‌های سخت‌افزاری استفاده می‌شود.

محققان دانشگاه میشیگان با بودجه‌ای ۳,۶ میلیون دلاری سخت‌افزاری ساخته‌اند که قادر به کنترل و منحرف کردن داده‌های مشکوک و مخربی است که در بخش‌های مختلف رایانه وجود دارند.

در این روش، هر بار که بدافزارها یا ویروس‌ها بتوانند یک ضعف نرم‌افزاری برای دسترسی به داده‌های حساس شناسایی کنند، راه‌حلی برای دور کردن آن‌ها از این

داده‌ها و هدایت آن‌ها به مسیری انحرافی طراحی خواهد شد. در قالب این روش رایانه‌ها به یک معمای غیرقابل حل تبدیل می‌شوند. مثل اینکه شما برای حل مکعب روبیکی تلاش کنید که ترتیب رنگ‌های آن لحظه به لحظه تغییر کند.

انتظار می‌رود تکمیل این طرح به چهار سال دیگر زمان نیاز داشته باشد.

منبع خبر: نیواطلس

انفجار گوشی به دلیل بدافزار خطرناک اندرویدی

بسیاری از بدافزارهای طراحی شده برای آلوده کردن گوشی‌های اندرویدی تنها برای سرقت داده‌ها طراحی می‌شوند اما فعالیت تخریبی یک بدافزار جدید آنقدر شدید است که باعث آسیب فیزیکی می‌شود.

به گزارش اکستریم تک، این بدافزار که توسط کارشناسان موسسه امنیتی کاسپرسکی شناسایی شده، Loapi نام دارد و برای سرقت تمامی اطلاعات موجود در گوشی اعم از داده‌های مربوط به ارزهای دیجیتال مانند بیت کوین تا دیگر داده‌های ذخیره شده در تلفن همراه طراحی شده است. محققان می‌گویند بدافزار یادشده تا بدان حد فعالیت کرده و باعث اشغال ظرفیت پردازنده و رم گوشی می‌شود که در نهایت موجب داغ شدن بیش از حد باتری و انفجار آن می‌شود. بدافزار Loapi از هیچ آسیب‌پذیری امنیتی برای دسترسی به گوشی کاربران استفاده نمی‌کند و در زمانی که کاربران به سایت‌های آلوده و غیرمطمئن مراجعه کنند، ممکن است از آن‌ها درخواست شود تا برنامه‌ای با محتوای مستهجن را بر روی گوشی خود نصب کنند. اگر کاربران چنین اشتباهی انجام دهند، در حین نصب برنامه از آن‌ها خواسته می‌شود تا تنظیمات امنیتی گوشی خود را نیز تغییر دهند که با این کار بدافزار Loapi دسترسی مورد نظر را به اطلاعات ذخیره شده در گوشی پیدا کرده و سرقت داده‌ها را آغاز می‌کند. بعد از نصب Loapi این بدافزار نسبت به ارسال انبوهی از پیام‌های ناخواسته برای دیگر کاربران اقدام می‌کند، آگهی‌های تبلیغاتی متعددی را بر روی گوشی به نمایش درمی‌آورد و از گوشی فرد برای اجرای حملات بات نت استفاده می‌کند. سرقت بیت کوین و دیگر ارزهای دیجیتال نیز توسط Loapi صورت می‌گیرد. فشاری که این بدافزار برای انجام این حجم از فعالیت به پردازنده گوشی وارد می‌کند، در مواردی به داغ شدن بیش از حد باتری و انفجار آن نیز منجر شده و لذا کاربران باید به طور جدی از نصب برنامه‌های مشکوک و تایید نشده خودداری کنند.

منبع خبر: اکستریم تک

بدترین پسوردهای سال ۲۰۱۷

شرکت آمریکایی EPC Group پس از تحقیقات، بدترین پسوردهای سال ۲۰۱۷ میلادی را اعلام کرد.

برای تهیه این فهرست، از اطلاعات مربوط به ۵ میلیون پسورد افشا شده در سال گذشته استفاده شده است. درهرحال این تحقیق نشان داد همچنان بدترین رمز کلمات ۱۲۳۴۵۶ و password هستند. جالب آن‌که در این فهرست برخی از ساده‌ترین و بی‌تاثیرترین پسوردها همچنان توسط کاربران استفاده می‌شوند. به عنوان مثال کلمه رمز qwerty در فهرست بدترین پسوردها رتبه چهارم را دارد، admin در رتبه یازدهم و login در رتبه چهاردهم می‌باشد. جالب آنکه رتبه شانزدهم این فهرست نام یک فیلم (starwars) است. میان بدترین پسوردها نام چند خودرو مانند فراری و مرسدس نیز دیده می‌شود.

همچنین این تحقیق نشان داد مردان ۲,۸ برابر بیش از زنان از عبارت‌های ساده به عنوان پسورد استفاده می‌کنند. ۲۵ پسورد بد این فهرست به ترتیب از راست به چپ عبارتند از :

12345	qwerty	12345678	password	123456
iloveyou	football	1234567	letmein	123456789
Abc123	login	monkey	welcome	admin
master	Passw0rd	dragon	123123	starwars
trustno1	qazwsx	whatever	freedom	hello

منبع خبر: ایتنا

ParseDroid تهدیدی برای همه برنامه‌های توسعه داده شده اندروید

تحلیل و بررسی‌های جدید نشان می‌دهد که آسیب-پذیری موجود در ابزارهای توسعه اندروید – که به آن‌ها مجموعه ParseDroid گفته می‌شود– سازمان‌هایی را که دارای برنامه‌های جاوا یا اندروید باشند را در معرض خطر قرار می‌دهد.

براساس تحقیقات تیم Check Point، ابزارهای توسعه قابل دانلود و ابزارهای مبتنی بر شبکه‌ی ابری، که در برنامه‌های اندروید استفاده می‌شوند، تحت تاثیر قرار گرفته‌اند. این برنامه‌ها شامل ابزارهایی می‌باشند که برنامه‌نویسان جاوا یا اندروید برای توسعه برنامه‌های شرکت‌ها، برنامه‌های تحلیل‌گر امنیت و ابزارهای مهندسی معکوس استفاده می‌کنند.

محققان تیم Check Point در تحلیل فنی اشاره کرده‌اند: "با توجه به تحقیقاتی که انجام داده‌ایم چندین آسیب-پذیری که ابزارهای توسعه اندروید مانند Android Studio، Intellij IDEA و Eclipse و همچنین ابزارهای مهندسی معکوس مانند APKtools-، The Cuckoo Droid Service را تحت تاثیر قرار داده‌اند، کشف کرده-ایم." در یک نمونه از تحلیل، با نگاه‌کردن به کد منبع APKtools، تیم Check Point آسیب‌پذیری XML External Entity (XXE) را یافته و دلیل آن را عدم غیرفعال سازی ارجاعات موجودیت‌های خارجی هنگام پردازش یک فایل XML توسط پردازشگر XML داخل برنامه اعلام کرده است. این تابع آسیب‌پذیر LoadDocument نام‌گذاری شده و در هسته APKtool استفاده شده است. این آسیب‌پذیری کل سیستم مدیریت فایل سیستم‌عامل استفاده‌کنندگان از APKtool را در معرض تهدید قرار می‌دهد و در نتیجه مهاجمان می‌توانند هر فایلی را در سیستم قربانی باز کرده و این اطلاعات را به سرور خود ارسال نمایند.

تیم Check Point همچنین اشاره کرده است که: "این سناریو، فقط یکی از چندین تکنیک حمله XXE است که می‌تواند عواقب خطرناکی را به بار آورد". هم‌چنین در مورد ویژگی این آسیب‌پذیری که اجازه اجرای کد از راه دور را می‌دهد، اشاره داشته‌اند که: "در عمل، روش پیمایش مسیر، این اجازه را به ما می‌دهد تا هر فایلی را در مکانی از سیستم کپی کنیم که این کار باعث می‌شود حمله در سطح وسیع و متنوعی انجام بگیرد".

شرکت‌های Google و JetBrain این آسیب‌پذیری امنیتی را تایید کرده و نحوه برطرف سازی آن را منتشر کردند. در نتیجه بسیار مهم است که توسعه‌دهندگان، کد برنامه‌های خود را ویرایش و به‌روزرسانی کنند تا امکان جاسوسی و خطرات احتمالی دیگر از بین برود.

منبع : infosecurity-magazine

مترجم: مهندس ابوالفضل علیقلی‌وند

شیوع باج افزار جدید بانکی با نام Spider

باج افزار جدیدی با نام Spider از طریق ایمیل‌های اسپم که ابتدا در منطقه بالکان (کشورهای بوسنی و هرزگوین، صربستان و کرواسی) توزیع شده بود، شیوع پیدا کرده است. این ایمیل اسپم شامل فایل Word مخرب می‌باشد که فایل‌های باج‌افزار Spider را در سیستم قربانی دانلود و نصب می‌کند. در ایمیل‌های ارسالی، یک فایل Word ضمیمه شده است که متن آن به زبان کرواسی نوشته شده است و وقتی کاربر برروی Enable Editing کلیک می‌کند، فایل شروع به ارتباط با آدرس‌های سرور خود کرده و فایل‌های اجرایی بدافزار را دانلود و آن‌ها را اجرا می‌کند.

"Potrazivanje Dugovanja" موضوع ایمیل‌های اسپم می‌باشد که به زبان صربستانی بوده و به معنی "پرداخت

بدهی" در زبان فارسی می‌باشد. بدافزار فایل اجرایی را با نام‌های Dec.exe و Enc.exe دانلود می‌کند که Enc.exe فایل‌های سیستم را رمزگذاری کرده و پسوند spider. را به فایل‌ها اضافه می‌کند.

فایل Dec.exe بعد از اتمام کار Enc.exe کار خود را شروع کرده و اقدام به نمایش پیام برای کاربر می‌کند. این پیام‌ها در قالب کدگذاری Base64 می‌باشد که Dec.exe وظیفه تبدیل این رشته‌های رمزشده به پیام قابل خواندن برای کاربر را برعهده دارد.

برای رمزگشایی اطلاعات، قربانی این باج‌افزار باید 0.00726 بیت کوین پرداخت کند.

تحلیل فنی کامل این باج‌افزار را در وبسایت مرکز آپا دانشگاه محقق اردبیلی می‌توانید دریافت کنید.

گردآوری و تحلیل فنی : مهندس ابوالفضل علیقلی وند

منبع ۱: bleepingcomputer.com

منبع ۲: zdnet.com

کشف حفره بزرگ خطرناک در برنامه‌های بانکی ۱۰ میلیون کاربر

محققان حوزه امنیت، به تازگی حفره‌ای را در برنامه‌های بانکی کشف کرده‌اند که می‌تواند بیش از ده میلیون کاربر را مورد حملات مرد میانی (MITM) قرار دهد. آسیب-پذیری مورد نظر نتیجه این واقعیت می‌باشد که گواهی امضا شده برنامه نتوانسته نام هاست مورد نظر را روی سروری که با آن ارتباط برقرار کرده تایید کند. این آسیب‌پذیری به افراد دیگر اجازه می‌دهد، تا به همان شبکه‌ی قربانی وارد شده و کنترل نشست‌های یک عملیات بانکی را در دست بگیرند و به رمز عبور و نام کاربری که اطلاعاتی مختص به حساب کاربری است، دسترسی پیدا کند.

محققان بعد از اجرای یک ابزار تست به نام "Spinner" که به تازگی توسعه داده‌اند، بیش از ۴۰۰ حفره امنیتی در برنامه‌های آسیب‌پذیر که شامل برنامه‌های بانک‌های HSBC، NatWest و Co-op می‌شود، پیدا کرده‌اند.

محققان همچنین به جزئیات "حملات فیشینگ درون برنامه‌ای" که در برنامه‌های کاربری بانک‌های Santander وAllied Irish وجود دارد، اشاره کردند. این آسیب‌پذیری به مهاجم اجازه می‌دهد تا قسمتی از صفحه مورد استفاده کاربر را ربوده و از آن در حمله فیشینگ برای اهدف خود، یعنی ورود به حساب کاربری استفاده کند. دانشگاه بیرمنگام که کاشف تعدادی از این آسیب-پذیری‌ها بوده است، با مرکز امنیّتی سایبری ملی (NSCS) و بانک‌های مورد هدف قرار گرفته برای برطرف سازی این مشکل همکاری کردند. سپس در کنفرانس سالیانه برنامه‌های امنیتی کامپیوتری در شهر Orlando، این آسیب‌پذیری را اعلام عمومی کردند.

محقق امنیتی Tom Chotia می‌گوید که: "به طورکلی، امنیت برنامه‌هایی که بررسی کرده بودیم در سطح خوبی قرار داشت اما این آسیب‌پذیری که پیدا کردیم به سختی قابل کشف بود و توانستیم ضعف‌های بسیاری را فقط با ابزارهایی که به تازگی توسعه داده بودیم پیدا کنیم".

وی همچنین اشاره کرد که: "غیرممکن است که این آسیب‌پذیری مورد سوء استفاده قرار گرفته باشد؛ مگر اینکه مهاجمان بتوانند به برنامه‌های بانکیِ کاربرانی که به شبکه‌های در معرض خطر وصل شده‌اند، دسترسی پیدا کرده باشند."

Ilia Kolochencko، مدیر اجرایی شرکت امنیت وب High-Tech Bridge بیان نمود که اکثر برنامه‌های موبایل سال‌ها این آسیب‌پذیری‌ها را به همراه خود داشته‌اند. همچنین او اضافه کرد: "این کار می‌تواند نتیجه کمبود توسعه‌دهندگان مجرب، بی‌توجه بودن اکثر سازمان‌ها نسبت به مسئله امنیت برنامه‌های موبایلی و امکان سوء استفاده بدلیل پیچیدگی‌های برطرف کردن نقص‌های موجود در برنامه‌های موبایل باشد."

منبع : infosecurity-magazine

مترجم: مهندس ابوالفضل علیقلی‌وند

آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی

با توجه به افزایش تعداد حوادث امنیتی رایانه‌ای و لزوم وجود مراکز تخصصی دانشگاهی برای پشتیبانی و رفع نیازهای پژوهشی جامعه در این حوزه، و با انگیزه ارتقای دانش و توان مهندسی در حوزه امنیت سیستم‌های کامپیوتری و پردازش اطلاعات و انتقال نتایج به جامعه، آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی، از اواخر سال ۱۳۹۴ فعالیت خود را آغاز نمود و از زمان آغاز فعالیت، اقدامات زیر صورت گرفته است:

۱. ارزیابی امنیتی و انجام آزمون نفوذپذیری سامانه‌ها و شبکه‌های رایانه‌ای

تست نفوذ یا ارزیابی امنیتی روشی است که توسط آن قادر می‌توان آسیب‌پذیری‌های موجود در نرم‌افزارها، شبکه، وب‌سایت و بانک‌های اطلاعاتی خود را شناسایی کرده و پیش از آنکه نفوذگران واقعی به سیستم وارد شوند، امنیت سیستم خود را افزایش داد. این روش با استفاده از ارزیابی جنبه‌های مختلف امنیتی کمک می‌کند تا با کاهش دادن ریسک‌های امنیتی موجود، احتمال نفوذ غیرمجاز به شبکه کاهش یابد.

۲. مشاوره در زمینه امن‌سازی سامانه‌ها و شبکه رایانه‌ای

با توجه فعالیت‌های مختلفی که آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی در زمینه زیرساخت‌های امنیتی مانند پیاده‌سازی سیستم مدیریت امنیت اطلاعات، پیاده‌سازی انواع ابزارهای امنیتی، تدوین الگوهای امنیتی داشته است، کارشناسان این مرکز دارای دیدی جامع نسبت به مسایل امنیتی با توجه به اهداف استراتژیک و راهبردی و با توجه به موجودیت‌های هر سازمان دارند و آماده ارائه راهکار امنیت اطلاعات و شبکه در تمامی سازمان‌ها با ویژگی‌ها و موجودیت‌های مختلف می‌باشند. خدمات و راهکارهای امنیت اطلاعات و سیستم‌های کامپیوتری این مرکز، با بررسی وضعیت فعلی سیستم‌های موجود در سازمان آغاز می‌شود و با بهره‌گیری از تکنولوژی و تخصص روز، با معماری و اجرای راه حل‌های جامع ایمن سازی سیستم های کامپیوتری ، کامل می گردد.

۳. برگزاری دوره‌های آموزشی در زمنیه دانش امنیتی برای سازمان‌ها و نهادهای زیربط

امنیت فضای سایبری فرآیندی است و باید آن را گام به گام و به روز جلو برد بنابراین آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی با هدف ارتقاء دانش امنیت اطلاعات متولیان فاوای سازمان‌ها و نیز به منظور تربیت نیروهای متخصص چندین دوره کارگاه‌های آموزشی برگزار نموده است.

۴. تولید نرم‌افزارهای امنیتی

آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی با هدف ارتقا سطح امنیت فضای سایبری به تولید نرم افزارهای امنیتی اقدام نموده است که عبارت است از: سامانه تحلیل‌گر فایل‌های اجرائی (ستفا)، دیده‌بان، رادار

۵. پاسخگویی به حملات

آزمایشگاه و مرکز تخصصی آپای دانشگاه محقق اردبیلی به محض دریافت درخواستی مبنی بر وقوع حملاتی تحت وب، زیرساخت‌های شبکه، سامانه‌های اداری و حملات بدافزاری در اسرع وقت با سازمان مورد حمله ارتباط برقرار می‌کند و با شناسایی نوع و فرایند حمله، مولفه‌های مربوط به آسیب‌پذیری سیستم، راهکارهای مناسب برای جلوگیری از حمله مجدد و بهره‌برداری از ضعف سیستم را ارائه می‌دهد همچنین با شناسایی نقاط ضعف سیستم و ارائه مشاوره برای رفع این نقاط آسیب‌پذیر سیستم را در مقابل حملات جدید مقاوم می‌سازد.

آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی
cert.uma.ac.ir

آدرس: دانشگاه محقق اردبیلی، دانشکده فنی و مهندسی، مرکز آپا دانشگاه محقق اردبیلی ۳۱۵۰۵۷۱۸(۴۵)
cert.uma.ac.ir | cert@uma.ac.ir