شماره یازدهم - آذر ۱۳۹۶

خبرنامه "آپا" دانشگاه خوارزمی

KHARAZMI CERT
COORDINATOR CENTER
مرکز تخصصی آپا خوارزمی

در این شماره خواهید خواند:

حملات سایبری به کسب و کارها!

تمامی کسب و کارهای اقتصادی در یک سال گذشته، حداقل یکبار مورد حمله‌ی سایبری قرار گرفته اند. براین اساس اخیرا تحقیقی منتشر شد که پژوهشگران، تهدید در حوزه موبایل را مورد بررسی قرار دادند- صفحه ۲ و ۳

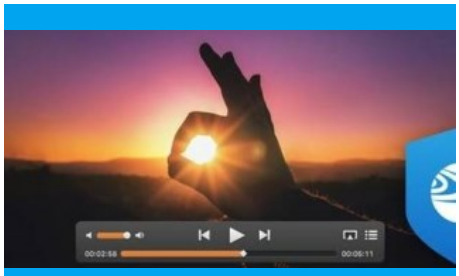
سوءاستفاده بدافزار اندرویدی از آسیب پذیری "Toast"

محققان در میکروترند نشان دادند که اولین قسمت شناخته شده‌ی بدافزار برای سو استفاده از آسیب پذیری‌های تازه پچ شده روی ویژگی توست در اندروید اثر می‌گذارد. - صفحه ۴

مرکز تخصصی آپا خوارزمی در هفته پژوهش

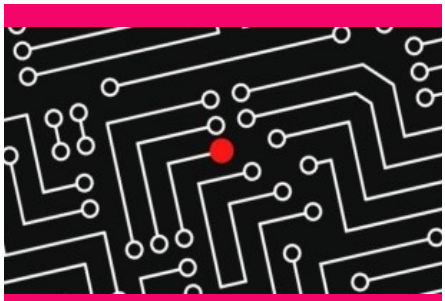
غرفه مرکز تخصصی آپا خوارزمی در هفته پژوهش پذیرای دانشجویان، اساتید و علاقمندان حوزه‌ی فناوری اطلاعات و ارتباطات بود. در این نمایشگاه مرکز آپا نیز به معرفی خود و دستاوردهای خود پرداخت که در ادامه خبر به شرح آن پرداخته شده است.

در ادامه‌ی فعالیت نمایشگاه افراد برجسته‌ی علمی، معاونین دانشگاه و مشاور شهردار بخشی از بازدیدگان غرفه مرکز آپا بودند. دکتر سبحان اللهی رییس دانشگاه خوارزمی، دکتر مشهدی زاده سرپرست معاونت پژوهشی، دکتر قبادیان معاون آموزش و پژوهش وزارت صنعت، معدن و تجارت، دکتر رسول رسولی‌پور مشاور شهردار تهران، دکتر عبداللهی ریاست پردیس بین الملل دانشگاه خوارزمی نیز بازدیدکننده‌ی غرفه مرکز آپا بودند که وجود آپا را یک فرصت بسیار ارزشمند برای دانشگاه دانستند و بر گسترش هرچه بیشتر همکاری و روابط بین مرکز تخصصی آپا و دانشگاه تاکید داشتند. - صفحه ۷



تروجان OSX.Proton در نرم‌افزار Elmedia

اگر شما هم محصولی از کمپانی Eltima نصب کرده‌اید باید گفت که کاملا اوضاع را پیچیده کرده‌اید. شرکت نرم افزاری Eltima که بخاطر دو نرم افزار Elmedia و Flox بسیار مشهور و سرشناخته است، اعتراف کرده که این دو برنامه به طور ناخواسته حاوی تروجان OSX.Proton هستند. - صفحه ۵



Hacker Door

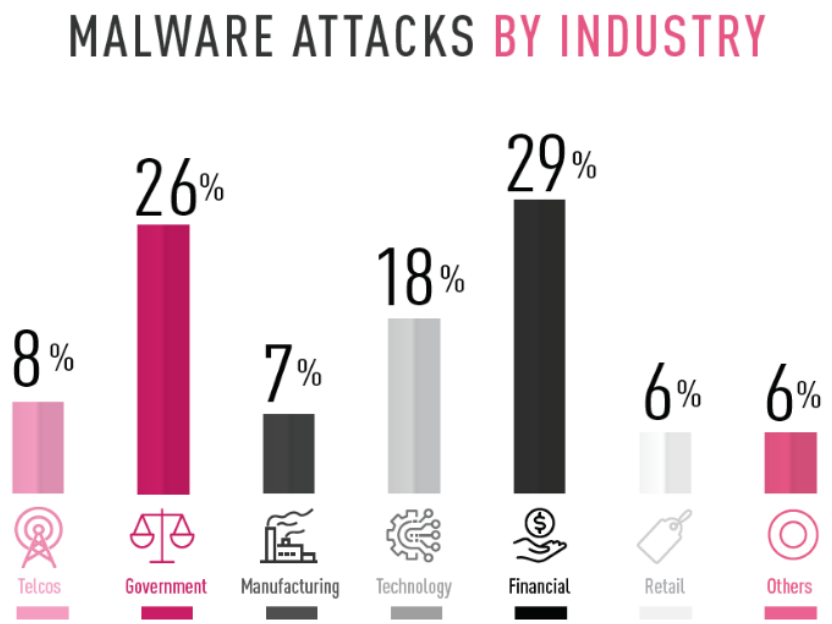
محققان امنیتی یک تروجان دسترسی از راه دور را که مجددا حرکتش را بعد از گذشت ۱۰ سال شروع نموده است کشف کرده‌اند. محققان امنیتی Cylance این بدافزار را Hacker Doorنامیدند. این بدافزار توسط گروهی از هکرهای چینی به نام Winnti هدایت می‌شود. - صفحه ۶

حملات سایبری به کسب و کارها!

تمامی کسب و کارهای اقتصادی در یک سال گذشته، حداقل یکبار مورد حمله‌ی سایبری قرار گرفته اند. براین اساس اخیرا تحقیقی منتشر شد که پژوهشگران، تهدید در حوزه موبایل را مورد بررسی قرار دادند. این گزارش با عنوان "تاثیر حمله سایبری موبایل بر کسب و کار" اولین مطالعه است که بررسی حجم و تاثیر حملات سایبری موبایل در محیط کسب و کار و بازرگانی پرداخته است. آنالیز مطالعات بر روی تهدیدات اندازه گیری شده انجام شده است. اطلاعات به دست آمده از تحقیقات نشان می‌دهد که شرکت‌های موبایل تحت حملات مداوم هستند و در سیستم عامل‌های iOS و اندروید بر تمام مناطق و صنایع اثر می‌گذارند. این تهدیدات به کاربران تلفن همراه اغلب پیچیده است و در نهایت قادر به بخطر انداختن دستگاه است که دسترسی غیرمجاز به اطلاعات حساس شخصی و شرکت‌ها را ممکن می‌سازد.

یافته‌های کلیدی از گزارش امنیتی تلفن همراه عبارتند از:

- هر شرکتی مورد نوعی از حمله موبایل قرارگرفت.
- صنایع آسیب دیده، ارائه دهنده‌ی خدمات مالی و دولتی هستند.
- حملات سایبری موبایل در فعالیت‌های اقتصادی در آمریکا رخ می‌دهد.
- دستگاه‌های iOS دارای نقص هستند و بی نقص نیستند اما اکثر حملات به سیستم عامل اندروید رخ می‌دهد.



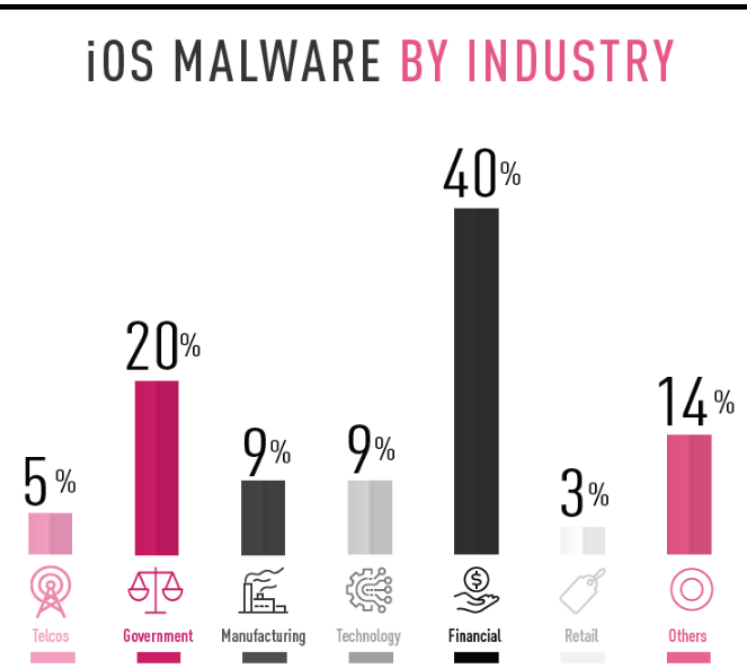
اطلاعات در گزارش چاپ شده، از استقرار تیم بررسی موبایل، در ۸۵۰ سازمان از جولای ۲۰۱۶ تا جولای ۲۰۱۷ جمع آوری شده است. در این نمونه مطالعات، نمایندگان کمپانی‌های دارای تکنولوژی باباالاترین درصد (۳۲٪) از دستگاه‌های امن، پس از خدمات مالی (۲۱٪)، مثل بانک‌ها کارگزاری‌ها و شرکت‌های بیمه قرار داشتند. تولیدکنندگان که ۱۵٪ از جامعه آماری را تشکیل می‌دادند؛ به همراه شرکت‌های مخابراتی (۱۲٪)، خرده فروشان(۷٪)، و سازمان‌های دولتی(۵٪)، باعث گردکردن نتایج آنالیز شدند.

خدمات مالی (۲۹٪) و دولت (۲۶٪)، با مخرب‌ترین حملات موبایل، فراتر از نسبت حضورشان در جامعه‌ی آماری مورد تهاجم واقع شدند. هردو حوزه، دارای پتانسیل ارزمندی برای حمله بودند؛ مانند مخازن بزرگ اطلاعات مالی و شخصی. شرکت‌های دارای تکنولوژی هم به شدت به وسیله‌ی نرم افزارهای مخرب تحت تاثیر قرار داشتند. در این پژوهش نیز نتایجی در مورد حمله به دستگاه‌های دارای سیستم عامل iOS به دست آمد. iOS به طور کلی پلتفرم امن تری را درمقایسه با اندروید، نظر گرفته است. در نتیجه، کارمندان سازمان‌ها بهتر است از دستگاه‌های دارای سیستم iOS به دلیل امنیت بالاتر استفاده کنند. بابررسی‌های موردی مشخص شد که iPhone و iPad در برابر حملات مخرب در هرشرایطی ایمن نیستند.

ادامه خبر در صفحه بعد.

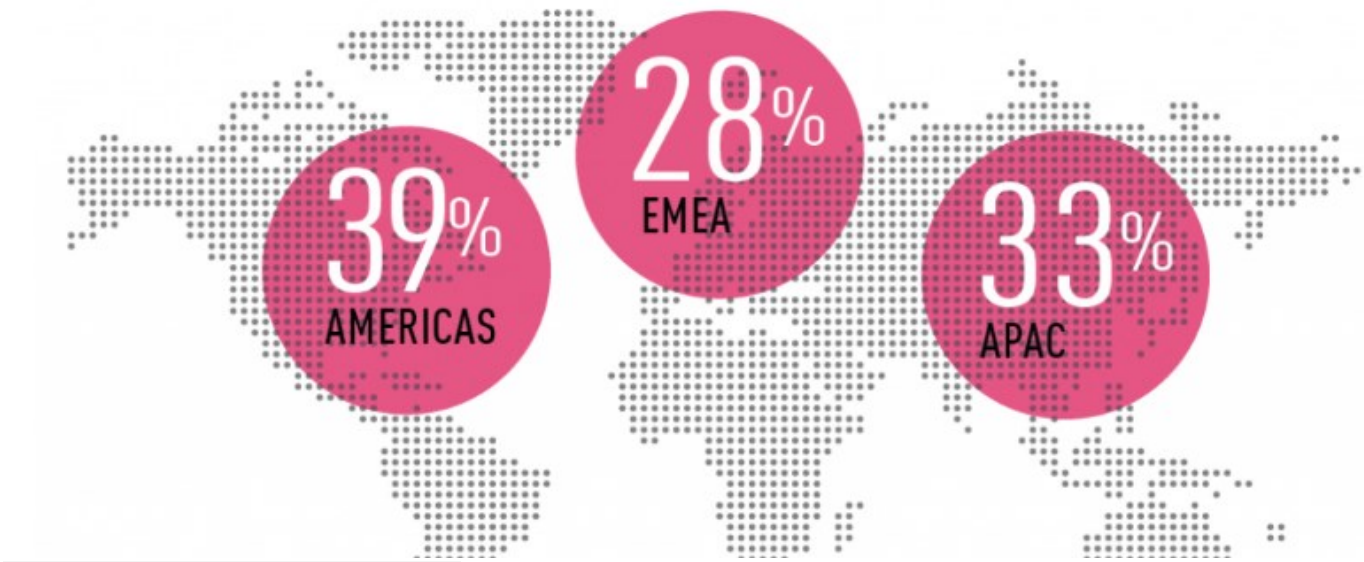
گردآورنده: حسین علیمرادی

حملات سایبری به کسب و کارها! (ادامه...)



تمام بدافزارهایی که نمونه مورد بررسی این تحقیق بوده اند؛ خدمات مالی با درنظر گرفتن داشتن ۴۰٪ از کل حملات، پیشرو بود. دستگاه‌های دولتی نیز با ۲۰٪ کل به شدت مورد هدف قرار گرفتند و پس از آن، شرکت-های فناوری و تولیدکنندگان هرکدام با ۹٪ از کل حملات.

آمریکا در این مورد بررسی نهفته‌ترین حملات را ثبت کرد. کشورهای آسیا و اقیانوسیه، با یک سوم کل، با وجود حجم کمتر در جامعه آماری، محمل حملات موبایل قرار داشتند. این مورد را می‌توان به وسیله‌ی وجود چند مجموعه کمپین بدافزار که در جنوبی‌ترین نقاط آسیا در طول یکسال گذشته قرار داشتند؛ که شامل Hummingbad و CopyCat می‌شوند؛ توضیح داد. مطالعه‌ای نیز روی حملات بدافزارها روی وسایل صنایع کلیدی انجام گرفته است. یعنی شمارنده‌های بیمه، اطلاعات سارقان، شبکه‌های آگهی ناهنجار و تروجان‌های دسترسی از راه دور تلفن همراه (mRATS) که در فرصت‌های آتی به اطلاع علاقه‌مندان خواهد رسید.



گردآورنده: حسین علیمرادی

سوءاستفاده بدافزار اندرویدی از آسیب پذیری "Toast"

محققان در میکروترند نشان دادند که اولین قسمت شناخته شده‌ی بدافزار برای سو استفاده از آسیب پذیری‌های تازه پچ شده روی ویژگی توست در اندروید اثر می‌گذارد.

طبق گفته‌ی محققان در شبکه های پالو آلتو، بدافزارهای مخرب را قادر می‌سازد تا حملاتی را با سوء استفاده از ویژگی Toast اندروید راه اندازی کند، که این اتفاق به اپلیکیشن‌ها اجازه می‌دهد تا پیام‌ها و نوتیفیکیشن‌ها را بالای اپ‌ها نمایش دهند. این ویژگی Toast نامیده می‌شود چون نوتیفیکیشن‌ها درست مثل Toast روی صفحه‌ی نمایش ظاهر می‌شوند. حملات Overlay عموعما توسط بدافزار اندروید برای حملات فیشینگ استفاده می‌شود استفاده از Toast شامل مزایایی ازجمله این که نیاز به نوع اجازه‌ی مشابه مثل ویندوزها را ندارد و به یک اپ اجازه می‌دهد تا یک ویندوز که صفحه‌ی نمایش داخلی دستگاه را می‌پوشاند را اجرا کند. آسیب پذیری ردیابی شده با عنوان CVE-2017-0752 و دسته بندی شده در گروه ریسک بالا، توسط گوگل در سپتامبر با آپدیت‌های امنیتی اندروید ماهانه پچ شده است. حملات Toast برروی دستگاه‌هایی که از اندروید ۸.۰ Oreo استفاده می‌کنند، اثر نمی‌کند.

محققان ترند میکرو دریافتند که اولین قطعه‌ی نفوذ بدافزار با سوءاستفاده از در برنامه‌هایی به عنوان Smart AppLocker وجود دارد که در Google Play در دسترس بود، جایی که صدها هزار بار دانلود شده بود. برنامه‌ها تاکنون از گوگل پلی حذف شده اند.

اپ‌های مخرب ادعای امنیت و محافظت از دستگاه را با یک پین کد دارند. به محض نصب آن‌ها از کاربر درخواست اجازه‌ی دسترسی دارند و کاربر را آگاه می‌کنند که آن‌ها (اپ ها) احتیاج به اسکن گوشی برای اپ‌های حفاظت نشده را دارند. سوءاستفاده از Toast در حالت نمایش یک صفحه‌ی پیشرفت برای "اسکن" انجام می‌شود، اما در پس زمینه بدافزار دستوراتی را از مهاجمان اجرا می‌کند و قسمت دوم بدافزار را که از طرف ترند میکرو AMIGOCLICKER نامیده شده است، نصب می‌کند. علاوه بر دانلو سایر بدافزارها، TOASTAMIGO می‌تواند منجر به این شود که اپ‌های امنیتی موبایل محدود شوند و کارهایی دیگری انجام دهد که خود را از حذف شدن محافظت کند. AMIGOCLICKER قابلیت خود مراقبتی دارد، اما میتواند اکانت های گوگل را جمع آوری کند، بر روی دکمه‌ها در پنجره‌های سیستم کلیک کند، روی تبلیغات فیس بوک کلیک کند و در گوگل پلی به خود امتیاز پنج ستاره بدهد.

محققان ترند میکرو در یک پست وبلاگی گفته اند: "مجموعه‌ای از عملکردهای مخرب بدافزار، در ترکیب با یک بردار حمله ی نسبتا منحصر به فرد، آن‌ها را به تهدیدهای معتبری تبدیل می‌کند. در واقع عملکردهایی که در فوق ذکر شده است برای حملات سایبری بیشتری قابل اصلاح است." چون TOASTAMIGO و AMIGOCLICKER می‌توانند از ویژگی دسترسی اندروید طوری سوءاستفاده کنند که عملا قادر به انجام هرکاری باشد، این بدافزار هنگام دریافت دستور از راه دور سرور، می‌تواند خودش را آپدیت کند.

گردآورنده: حسین علیمرادی

تروجان OSX.Proton در نرم‌افزار Elmedia

اگر شما هم محصولی از کمپانی Eltima نصب کرده‌اید باید گفت که کاملا اوضاع را پیچیده کرده‌اید. شرکت نرم افزاری Eltima که بخاطر دو نرم افزار Elmedia و Flox بسیار مشهور و سرشناخته است، اعتراف کرده که این دو برنامه به طور ناخواسته حاوی تروجان OSX.Proton هستند.

این تعطیلات، یک تعطیلات ناخوشایند برای برخی از کاربران Mac می‌باشد. آنان با سیستم عاملی مواجه می‌شوند که نیاز است مجددا پاک و دوباره نصب گردد. زیرا هکرها بدافزارهای خود را درون برنامه‌ها قانونی قرار داده‌اند.

این تعطیلات، یک تعطیلات ناخوشایند برای برخی از کاربران Mac می‌باشد. آنان با سیستم عاملی مواجه می‌شوند که نیاز است مجددا پاک و دوباره نصب گردد. زیرا هکرها بدافزارهای خود را درون برنامه‌ها قانونی قرار داده‌اند.

شرکت نرم افزاری Eltima که بخاطر دو نرم افزار Elmedia و Flox بسیار مشهور و سرشناخته است، اعتراف کرده که این دو برنامه به طور ناخواسته حاوی تروجان OSX.Proton هستند. این تروجان که به نرم افزار فوق تزریق گردیده است توسط فروشگاه امنیتی ESET شناسایی گردیده است و مراتب به Elmedia اطلاع داده شده است. تحقیقات نشان می‌دهد که از روی اشتباه این بدافزار به سرور توسعه دهندگان راه یافته است و بدافزار توانسته خود را درون فایل‌های دانلود جای دهد. از این رو شرکت نام برده نیز اقدام به پخش آنان کرده است.

بدافزار Proton یک تروجان کنترل از راه دور می‌باشد که برای سیستم عامل Mac طراحی گردیده است. این بدافزار یک درب پشتی برای در اختیار گرفتن کنترل خط فرمان قربانی باز می‌کند و می‌تواند پسوردها، رمزنگاری‌ها، کلیدهای VPN و پول‌های مجازی را به سرقت ببرد. این بدافزار همچنین قابلیت دسترسی به اکانت iCloud و سیستم احراز هویت دو مرحله-ای قربانیان را نیز دارد. این بدافزار با قیمت ۵۰۰۰۰ دلار در ماه مارچ به فروش گذاشته شد.

بدافزار نام برده توسط ESET در دانلود برنامه‌های جدید از این کمپانی تشخیص داده شد و Eltima در ساعت ۳:۱۰ آن را از روی سرورهای خود پاک نمود. اگر شما قبلا این دو برنامه را دانلود و آپدیت کرده باشید این اطمینان خاطر وجود دارد که در نسخه‌ی جدید تروجانی وجود ندارد. اما برای اطمینان، انجام یک اسکن در خصوص فایل‌های زیر مفید است:

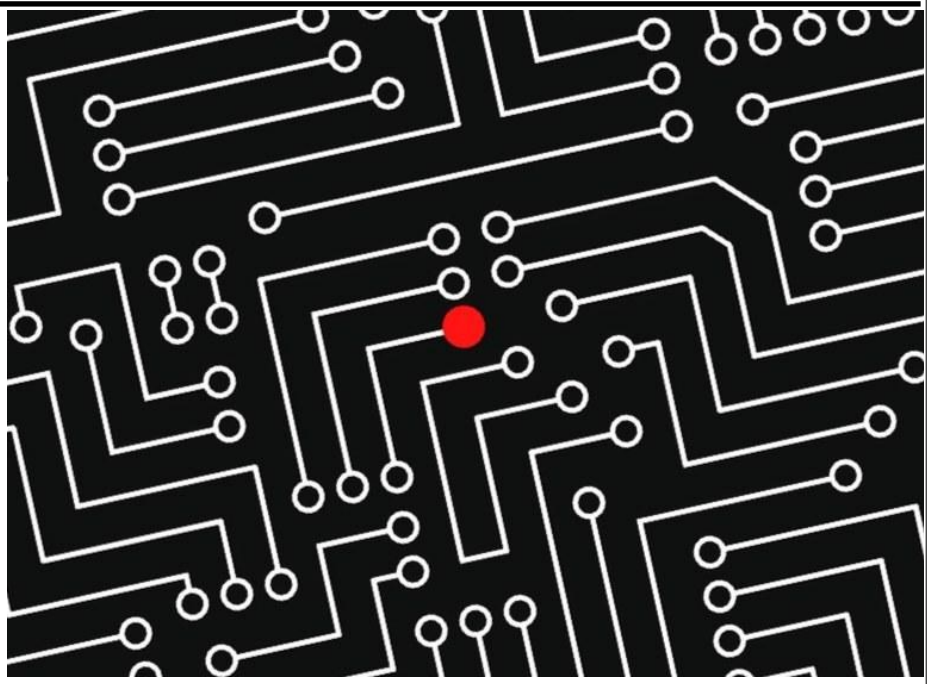
/tmp/Updater.app/
/Library/LaunchAgents/
com.Eltima.UpdaterAgent.plist
/Library/.rand/
/Library/.rand/updateragent.app/

اگر هر یک از فایل‌های بالا موجود باشد یعنی اینکه شما به Proton آلوده شده‌اید. اگرچه این بدافزار توسط آنتی ویروس شما نیز ممکن است تشخیص داده شود اما پاک کردن آن بسیار دشوار بوده و نیاز است تا کل سیستم را از اتصال خارج کنید.

طبق گفته‌ی Eltima "تنها راه مطمئن برای از بین بردن این بدافزار، پاک و نصب مجدد سیستم عامل می‌باشد". این کار یک روش استاندارد برای سیستم‌هایی با دسترسی Admin می‌باشد.

گردآورنده: محمد مرتضوی

Hacker Door



محققان امنیتی یک تروجان دسترسی از راه دور را که مجددا حرکتش را بعد از گذشت ۱۰ سال شروع نموده است کشف کرده‌اند. محققان امنیتی Cylance این بدافزار را Hacker Door نامیدند. این بدافزار توسط گروهی از هکرهای چینی به نام Winnti هدایت می‌شود.

باج افزار جدیدی که به Hacker's Door مشهور است بسیار شبیه به تروجان‌های دسترسی از راه دور (RAT) بوده که در سال ۲۰۰۴ به همین نام نامیده شد ولی در سال ۲۰۰۵ با ویژگی‌های جدیدی به روز رسانی شد. هم اکنون این بدافزار با ویژگی‌های جدید خود توانایی ادامه فعالیت برروی سیستم‌های ۶۴ بیتی را دارد. این ورژن جدید حاوی Back Door ها و Rootkit های بسیاری است که امکان دسترسی به هسته‌ی سیستم عامل را به آن می‌دهد، از این رو مهاجم می‌تواند به اطلاعات سیستم، لیست پردازش‌ها و اجرای فرامین دسترسی داشته باشد. محققین همچنین متوجه شدند که این بدافزار قابلیت سرقت فایل‌ها و تصاویری از صفحه، دانلود فایل‌ها و ابزارهای اضافه و باز کردن پورت Telnet را دارد.

این ابزار همچنین قابلیت استخراج اعتبارنامه‌های کاربر در Sessionهای فعال و سایر اطلاعات سیستم را دارا می‌باشد. ورژن جدید این بدافزار قابلیت پشتیبانی از ویندوز ۷ و ۸.۱ را دارد اما تا لحظه‌ی نگارش این خبر شواهدی از قابلیت تحت تاثیر قرار دادن ویندوز ۱۰ در این بدافزار یافت نشده است.

همچنان مشخص نیست که هدف از اجرا و به کار گیری این بدافزار چه می‌باشد اما در گذشته هکرها برای ایجاد درسترسی از راه دور برای انجام تقلب‌های مالی از آن استفاده می‌کردند. این گروه برروی شرکت‌های دارویی بزرگ و شرکت بازی سازی تمرکز دارد، اما Tom Bonner محقق ارشد Cylance بیان نموده است که "ورژن کنونی بد افزار Hacker's Door در صنعت هوافضا یافت شده است."

همانند موارد گذشته، این بدافزار توسط نویسنده‌اش به فروش گذاشته شده و با یک گواهی سرقت شده، امضا شده است. این امر، آلوده کردن کامپیوترها را با دور زدن شرایط حفاظتی طراحی شده در آنان برای شناسایی کدهای بدون امضا را بسیار ساده می‌کند.

محققان امنیتی می‌گویند که این احتمال وجود دارد که این ابزار همچنان بعنوان بخشی از حملات هدفمند برای طولانی مدت باشد، زیرا سهولت استفاده و عملکرد پیشرفته RAT باعث می شود که Hacker's Door برای مرکز تسلیحاتی دشمنان باشد.

گردآورنده: محمد مرتضوی

مرکز تخصصی آپا خوارزمی در هفته پژوهش

غرفه مرکز تخصصی آپا خوارزمی در هفته پژوهش در تاریخ ۱۱ ام تا ۱۳ ام آذر در پردیس کرج و در تاریخ ۲۶ ام تا ۲۸ ام در پردیس تهران دانشگاه خوارزمی پذیرای دانشجویان، اساتید و علاقمندان حوزه‌ی فناوری اطلاعات و ارتباطات بود. در راستای برگزاری این نمایشگاه، غرفه تخصصی آپا خوارزمی توسط مسئولین مورد بازدید قرار گرفت. در این نمایشگاه مرکز آپا نیز به معرفی خود و دستاوردهای خود پرداخت که در ادامه خبر به شرح آن پرداخته شده است.

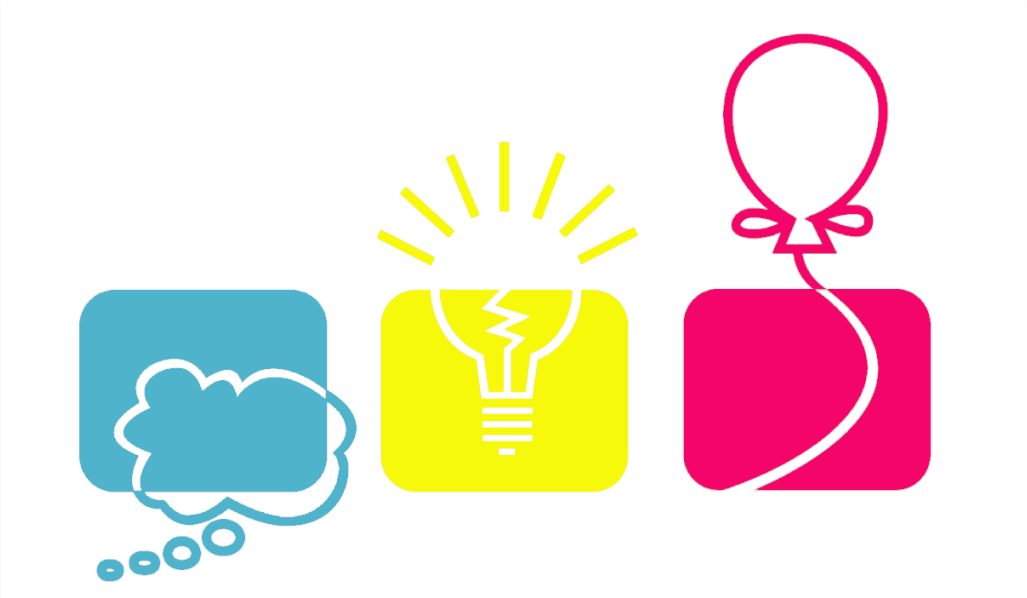
در غرفه‌های مرکز تخصصی آپا و مرکز فناوری اطلاعات و ارتباطات دانشگاه برای اولین بار در دانشگاه‌های ایران آنتی ویروس سیمانتک اورجینال به رایگان در دسترس دانشجویان و اعضای محترم هیئت علمی قرار گرفت. همچنین در این نمایشگاه به کلیه‌ی علاقمندان و بازدید کنندگان، خدماتی از قبیل دسترسی به آرشیو کامل ماهنامه، وب اپلیکیشن واکاوی پورت‌ها، شبکه اجتماعی شاب و خبرخوان خوارزمی ارائه گردید. خدمات نامبرده با استقبال پرشور دانشجویان و سایر علاقمندان همراه بود.

همچنین غرفه مرکز تخصصی آپا با استفاده از شرایط موجود به ارائه‌ی فعالیت‌های خود در زمینه آموزش، امنیت و تولید ابزار پرداخت و با توضیح و معرفی دستاوردهای خود به علاقمندان در این نمایشگاه، زمینه-های همکاری جدیدی را برای دانشجویان فراهم نمود.

در ادامه‌ی فعالیت نمایشگاه افراد برجسته‌ی علمی، معاونین دانشگاه و مشاور شهردار بخشی از بازدیدگان غرفه مرکز آپا بودند. دکتر سبحان اللهی رییس دانشگاه خوارزمی، دکتر مشهدی زاده سرپرست معاونت پژوهشی، دکتر قبادیان معاون آموزش و پژوهش وزارت صنعت، معدن و تجارت، دکتر رسول رسولی‌پور مشاور شهردار تهران، دکتر عبداللهی ریاست پردیس بین الملل دانشگاه خوارزمی نیز بازدیدکننده‌ی غرفه مرکز آپا بودند که وجود آپا را یک فرصت بسیار ارزشمند برای دانشگاه دانستند و بر گسترش هرچه بیشتر همکاری و روابط بین مرکز تخصصی آپا و دانشگاه تاکید داشتند.

گردآورنده: محمد مرتضوی

Kharazmi CERT Coordinator Center



مرکز آپا دانشگاه خوارزمی

رییس مرکز:

دکتر امید مهدی عبادتی

اعضای هیات علمی:

دکتر احسان ملکیان

دکتر امید مهدی عبادتی

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

شیوا بهادری

محسن نادری

محسن یزدی‌نژاد

نشانی:

کرج - دانشگاه خوارزمی - کتابخانه‌ی مرکزی - طبقه‌ی همکف - مرکز آپا

تلفن:

۰۲۶۳۴۵۷۵۰۱۲

۰۲۶۳۴۵۷۵۰۱۸

۰۲۶۳۴۵۷۹۶۰۰ (داخلی ۲۶۲۲)

پست الکترونیک:

cert@khu.ac.ir

وب سایت:

http://cert.khu.ac.ir/

دانلود رایگان:

دانلود رایگان مجموعه کامل خبرنامه‌ها از طریق اسکن کد زیر در دسترس است.