خبرنامه الکترونیکی ۶۲

مرکز تخصصی آپا دانشگاه سمنان

شماره شصت و دوم، سال ششم، مرداد ۱۴۰۲ | کاری از تیم تولید محتوای مرکز تخصصی آپا دانشگاه سمنان

در این شماره می‌خوانید:

8 ابزار تست نفوذ منبع باز که ممکن است درباره آنها ندانید!

https://cert.semnan.ac.ir info.cert@semnan.ac.ir 023-31535019 @semcert


مرکز آپا دانشگاه سمنان
سیستم دفاعی بدن هر کسب و کاری
امنیت اطلاعات آن کسب و کار است...

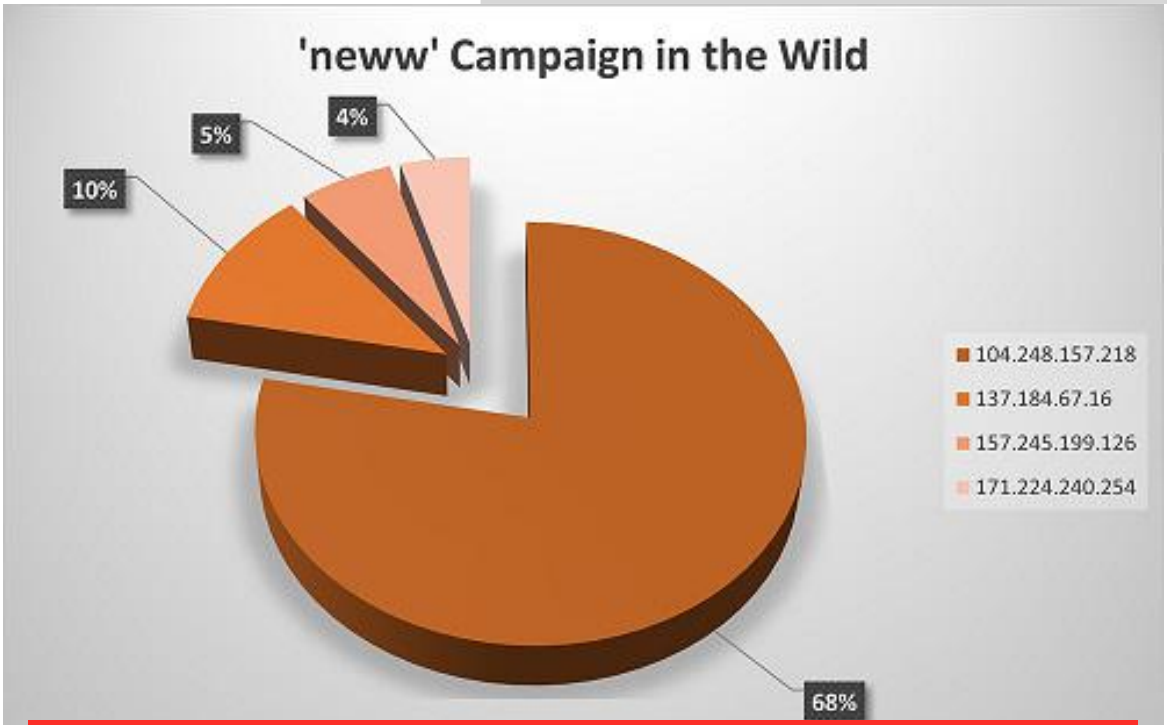
فهرست

خبر

آموزش

مرکز آپا دانشگاه سمنان

خبر

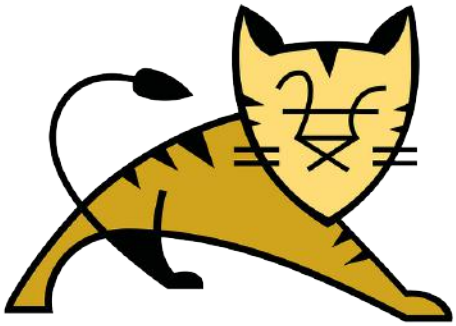


انتشار بدافزار در سرورهای Apache Tamcat

انتشار بدافزار در سرورهای Apache Tamcat

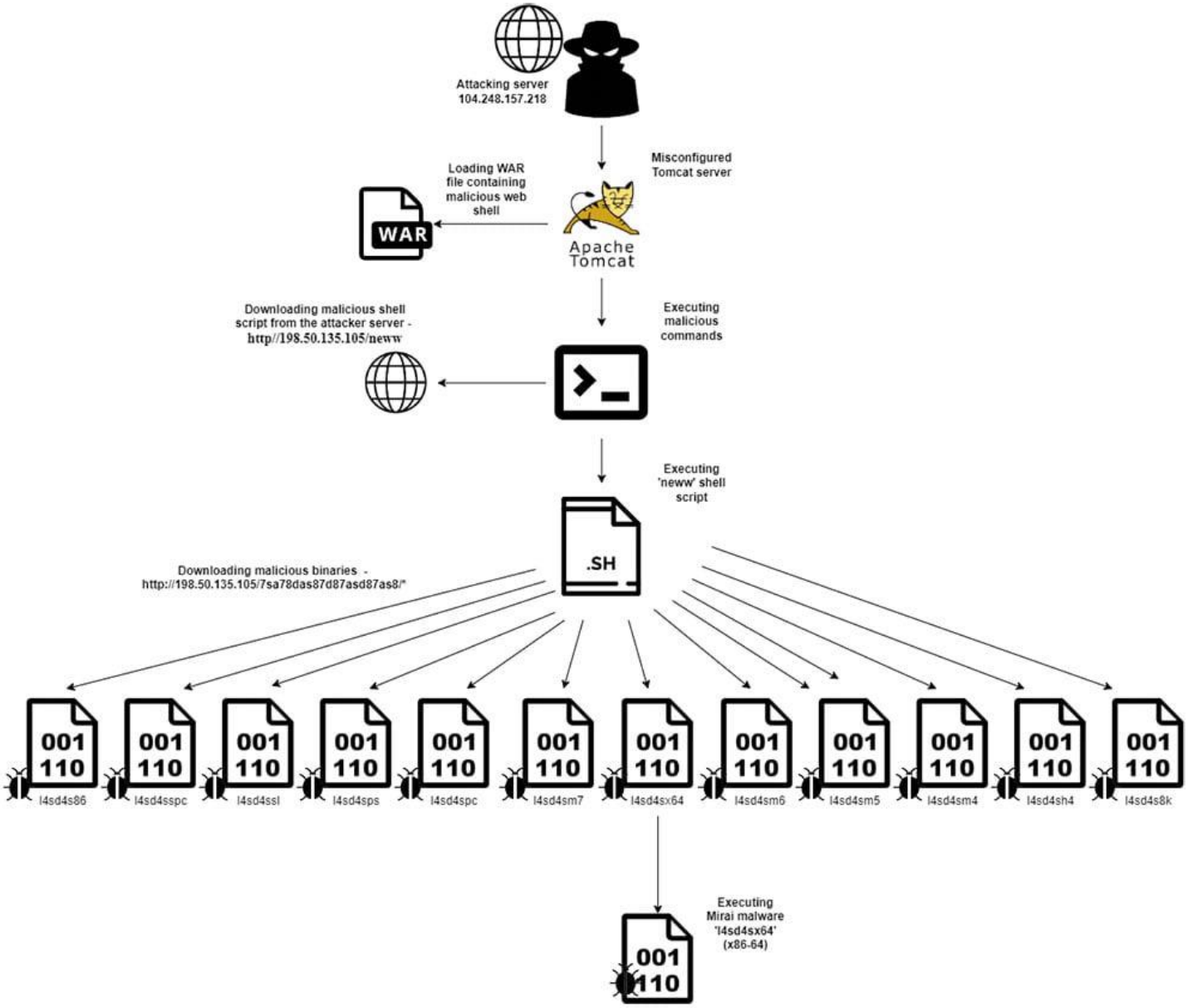
محققان امنیت سایبری Aqua یک کمپین جدید کشف کردند که با پیکربندی نادرست سرورهای Apache Tomcat، بدافزارهای باتنت Mirai را انتشار داده و یا از این طریق به استخراج ارز دیجیتال می‌پردازند. Apache Tomcat، یک سرور رایگان و منبع باز می‌باشد که از فناوری‌های Expression Language، Jakarta Servlet و WebSocket پشتیبانی کرده و یک محیط وب سرور "pure Java" HTTP را ارائه می‌کند و به طور گسترده در Big data، Cloud وWebsite استفاده می‌شود. Aqua طی دو سال، بیش از 800 حمله به هانی‌پات‌های سرور Tomcat خود شناسایی کرد که 96 درصد این حملات از طریق باتنت Mirai صورت گرفته است؛ از بین این حملات،20 درصد (152مورد) آن‌ها از شل اسکریپت "neww" و 24 آی‌پی استفاده کرده‌اند و 68 درصد نیز از آی‌پی 104.248.157.218[.]. حملات خود را انجام داده‌اند. بدافزار مذکور از هاست‌های آلوده، جهت سازماندهی حملات منع سرویس توزیع شده[1] استفاده می‌کند.

مهاجم پس از ورود موفقیت‌آمیز، یک فایل WAR را با وب‌شل cmd.jsp مستقر کرده و از این طریق اجرای فرمان از راه دور را در سرور Tamcat که در معرض خطر است، امکان‌پذیر می‌کند. کل زنجیره حمله شامل دانلود و اجرای شل اسکریپتneww می‌باشد که سپس با استفاده از دستور rm -rf حذف خواهد شد. در تصویر زیر، جریان حمله را مشاهده می‌کنید:



Apache Tomcat

1- DDoS



فایل WAR حاوی فایل‌های ضروری برنامه‌های کاربردی تحت‌وب از جمله Servlets، CSS، HTML و Classes می‌باشد.

در این حملات مهاجم با مجوز معتبر، به مدیریت برنامه وب نفوذ می‌کند، وب‌شل پنهان شده را در فایل WAR آپلود کرده و دستورات را از راه دور اجرا و حمله را آغاز می‌کند. شایان ذکر است که یافته‌ها حاکی از استخراج ارزهای دیجیتال با افزایش ۳۹۹ درصدی و ۳۳۲ میلیون حمله cryptojacking در سراسر جهان در نیمه اول سال ۲۰۲۳ می‌باشد.

این بدافزار سرورهای Apache Tomcat و به تبع آن Cloud، Big data و Website را تحت تأثیر خود قرار می‌دهد.

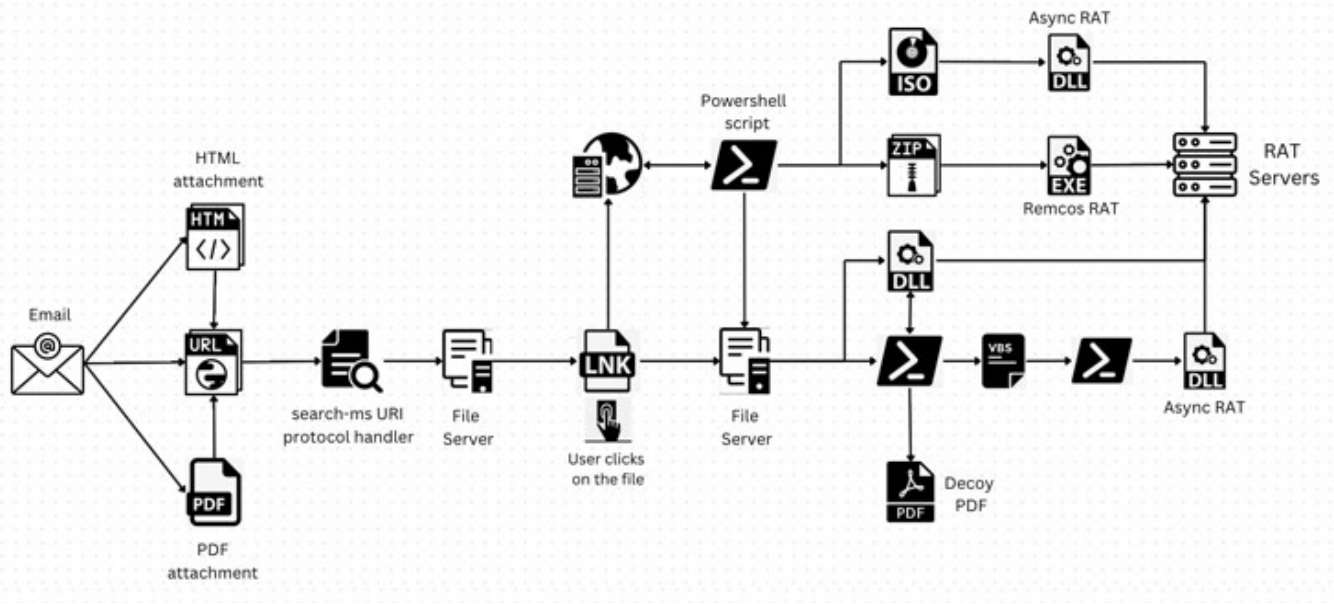
تحلیلگران امنیت سایبری رعایت نکات زیر را جهت کاهش چنین حملاتی توصیه می‌کنند:

- اطمینان از پیکربندی صحیح تمام محیط‌ها و ابزارها
- اطمینان از اسکن مکرر محیط‌های خود در برابر تهدیدات ناشناخته
- توانمندسازی توسعه‌دهندگان، DevOps و تیم‌های امنیتی با ابزارهای ابری جهت اسکن آسیب‌پذیری‌ها و بررسی پیکربندی‌های نادرست
- استفاده از راه‌حل‌ها و تشخیص مناسب در زمان اجرا و پاسخ به موقع به آن‌ها

1-cloud-native

سوء استفاده هکرها از ویژگی جستجوی ویندوز برای نصب تروجان های دسترسی از راه دور

عوامل مخرب ناشناس از یک ویژگی جستجوی قانونی ویندوز برای دانلود پیلودهای دلخواه از سرورهای راه دور سوء استفاده می‌کنند و سیستم‌های هدف را با تروجان های دسترسی از راه دور مانند AsyncRAT و Remcos RAT آلوده می‌کنند.



به گفته شرکت Trellix، تکنیک حمله جدید، از کنترل‌کننده پروتکل «search-ms:» URI بهره می‌برد که به برنامه‌ها و پیوندهای HTML امکان اجرای جستجوهای محلی دلخواه را می‌دهد. همچنین با استفاده از این ویژگی می‌توان پروتکل اپلیکیشن «search:» را فراخوانی کرد. محققین امنیتی Mathanraj Thangaraju و Sijo Jacob در روز پنجشنبه گفتند: مهاجمان، کاربران را به وب‌سایت‌هایی هدایت می‌کنند که از قابلیت search-ms با استفاده از جاوا اسکریپت میزبانی شده در صفحه استفاده می‌کنند. این تکنیک حتی به پیوست‌های HTML نیز گسترش یافته است و سطح حمله را گسترش می‌دهد.

در چنین حملاتی، عوامل تهدید مشاهده شده‌اند که ایمیل‌های فریبنده‌ای را ایجاد می‌کنند که لینک‌ها یا پیوست‌های HTML حاوی URL که کاربران را به وب‌سایت‌های در معرض خطر هدایت می‌کند، جاسازی می‌کنند. این باعث اجرای جاوا اسکریپت می‌شود که از کنترل‌کننده‌های پروتکل URI برای انجام جستجو در سرور تحت کنترل مهاجم استفاده می‌کند.

شایان ذکر است که با کلیک بر روی پیوند، هشداری نمایش داده می‌شود که "Windows Explorer را باز کنم؟"، با زدن دکمه تأیید، نتایج جستجوی فایل‌های میانبر مخرب میزبانی شده از راه دور در Windows Explorer به صورت فایل‌های PDF یا سایر نمادهای قابل اعتماد نمایش داده می‌شوند، درست مانند نتایج جستجوی محلی.

با استفاده از این تکنیک زیرکانه، کاربر متوجه نمی‌شود که فایل‌های ارائه شده به او، فایل‌های راه دور هستند. در نتیجه، کاربر احتمال بیشتری دارد که فایل را با فرض اینکه از سیستم خودش است باز کند و ناآگاهانه آن را اجرا کند.

اگر قربانی روی یکی از فایل‌های میانبر کلیک کند، منجر به اجرای یک کتابخانه پیوند پویا[1] با استفاده از ابزار regsvr32.exe می‌شود.

1-DLL

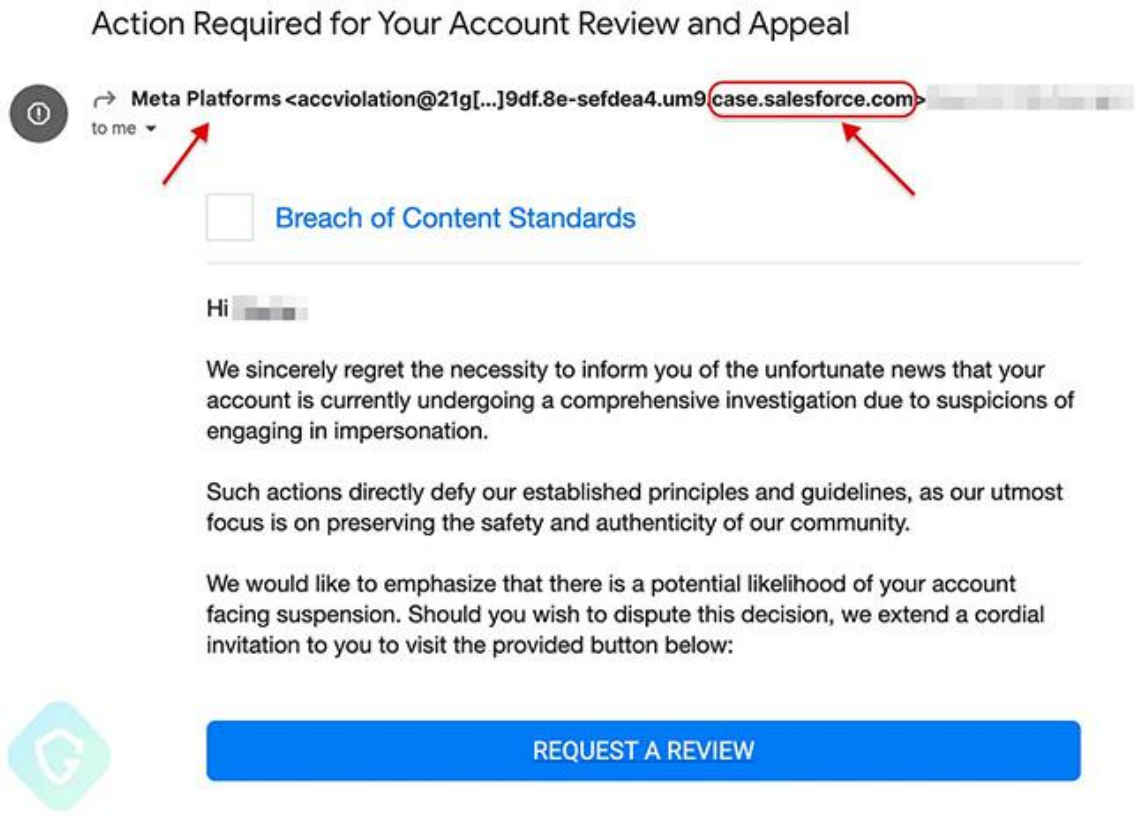
در گونه دیگری از این کمپین، از فایل‌های میانبر برای اجرای اسکریپت‌های PowerShell استفاده می‌شود که به نوبه خود، پیلودهای اضافی را در پس‌زمینه دانلود می‌کنند در حالی که یک سند PDF فریبنده را به قربانیان نمایش می‌دهند.

صرف نظر از روش مورد استفاده، آلودگی‌ها منجر به نصب AsyncRAT و Remcos RAT می‌شود که مسیری را برای عوامل تهدید ارائه می‌دهد تا از راه دور میزبان‌ها را کنترل کنند، اطلاعات حساس را سرقت کنند و حتی دسترسی را به مهاجمان دیگر بفروشند.

برای جلوگیری از این حملات، ضروری است که از کلیک کردن روی URLهای مشکوک یا دانلود فایل از منابع ناشناخته خودداری شود.

Salesforce و Meta از کمپین فیشینگ رنج می‌برند که از روش‌های تشخیص معمولی فرار می‌کند

تیم تحقیقاتی Guardio یک کمپین فیشینگ ایمیل را کشف کرد که از یک آسیب‌پذیری روز صفر در سرویس‌های ایمیل قانونی Salesforce و سرورهای SMTP سوءاستفاده می‌کرد.



نمونه ایمیل فیشینگی که از آدرس ایمیل "salesforce.com@" ارسال شد

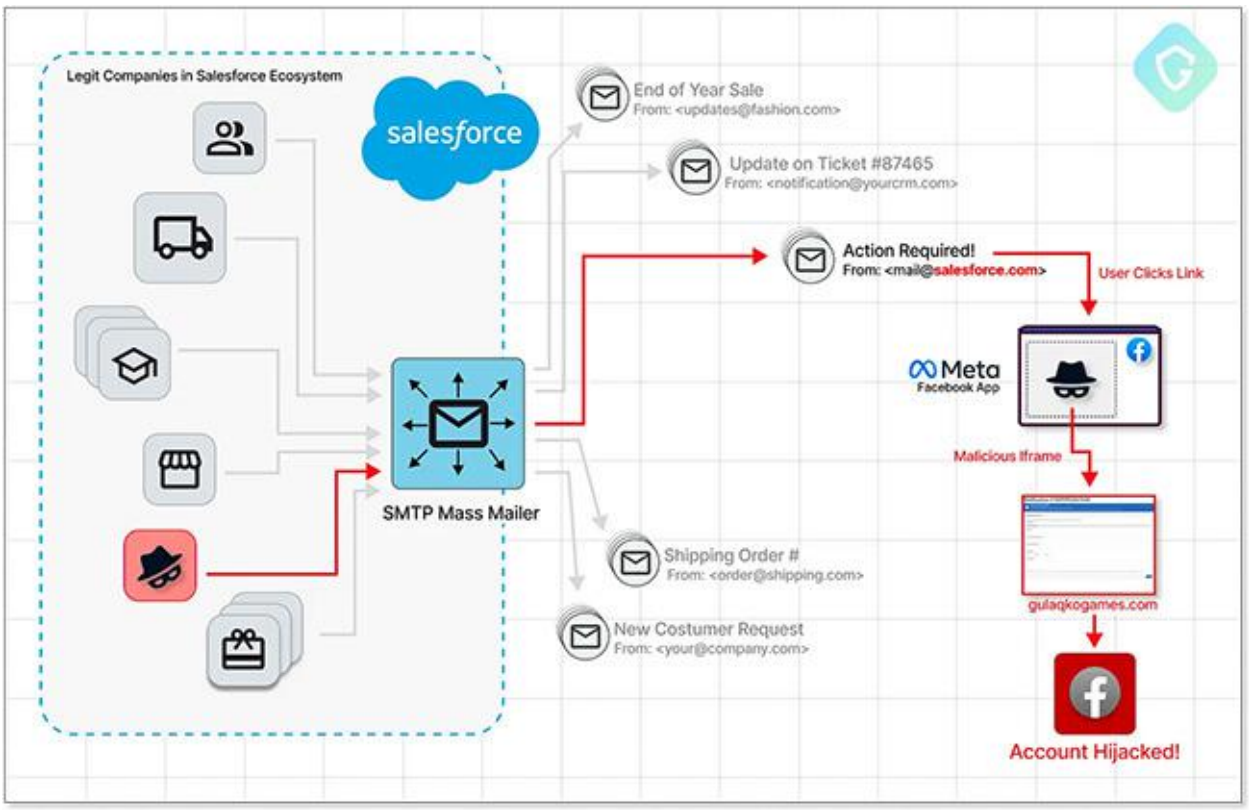
این آسیب‌پذیری به بازیگران تهدید اجازه می‌دهد تا ایمیل‌های فیشینگ هدفمند ایجاد کنند و با استفاده از دامنه و شهرت Salesforce و ویژگی‌های پلتفرم بازی‌های وب فیس‌بوک، از روش‌های تشخیص مرسوم اجتناب کنند.

83 درصد از سازمان‌ها هر ساله با حملات فیشینگ مواجه می‌شوند و ایمیل‌های بازار انبوه رایج‌ترین شکل فیشینگ هستند که به عنوان ایمیل‌های شرکت‌های معتبر پنهان شده‌اند که به واسطه آن دریافت‌کنندگان، فریب داده می‌شوند تا اقدامات مضری مانند دانلود بدافزار یا کلیک کردن روی پیوندهای مخرب انجام دهند که اعتبارنامه حساب‌های اجتماعی و مالی را افشا می‌کند.

با استفاده از تکنیک‌های فیشینگ، عوامل تهدید با موفقیت ترافیک ایمیل مخرب را در سرویس‌های دروازه ایمیل قانونی و قابل اعتماد پنهان کردند و به آن‌ها اجازه می‌داد از بزرگی و شهرت شرکت‌ها استفاده کنند.

- ایمیل‌های فیشینگ معتبر به نظر می‌رسیدند، نام واقعی هدف را ذکر می‌کردند و با موفقیت مکانیسم‌های سنتی ضد هرزنامه و ضد فیشینگ را دور می‌زدند، زیرا حاوی پیوندهای قانونی به فیس‌بوک بودند و از آدرس ایمیل salesforce.com@ سرچشمه می‌گرفتند.
- عوامل تهدید از ویژگی "Salesforce Email-to-Case" سوءاستفاده کردند که برای تبدیل ایمیل‌های ورودی

مشتری به تیکت پشتیبانی طراحی‌شده است و به آن‌ها امکان می‌دهد ایمیل‌های تأیید را دریافت کنند و کنترل یک آدرس ایمیل واقعی @salesforce.com را برای تلاش‌های مخرب فیشینگ خود به دست آورند.



جریان کمپین فیشینگ: از Salesforce تا کیت فیشینگ پنهان در پلتفرم بازی‌های وب Facebook

پس از شناسایی موفقیت‌آمیز این روش، Guardio یافته‌های خود را با Salesforce و Meta در میان گذاشت و هر دو شرکت به این موضوع پرداختند.

Nati Tal، رئیس آزمایشگاه‌های Guardio گفت: «این حادثه مرتبط با Salesforce اهمیت احتیاط بیشتر و اجرای اقدامات سختگیرانه توسط ارائه‌دهندگان خدمات برای جلوگیری از سوءاستفاده از خدمات قانونی به منظور فعالیت‌های مخرب برجسته می‌کند. ما Salesforce و Meta را به خاطر اقدامات سریع و تلاش‌های مداومشان برای تقویت امنیت و انعطاف‌پذیری پلتفرم‌هایشان تحسین می‌کنیم. ما به سایر ارائه‌دهندگان خدمات توصیه می‌کنیم که از این روند پیروی کنند، دروازه‌های داده را ایمن کنند و فرآیندهای راستی‌آزمایی را تقویت کنند».

حمله آکوستیک جدید
با دقت ۹۵ درصد داده‌ها را از ضربه کلید می‌رباید

تیمی از محققان دانشگاه‌های بریتانیا یک مدل یادگیری عمیق را آموزش داده‌اند که می‌تواند داده‌ها را از ضربه‌های صفحه‌کلید ضبط شده با میکروفون با دقت ۹۵ درصد بدزدد.

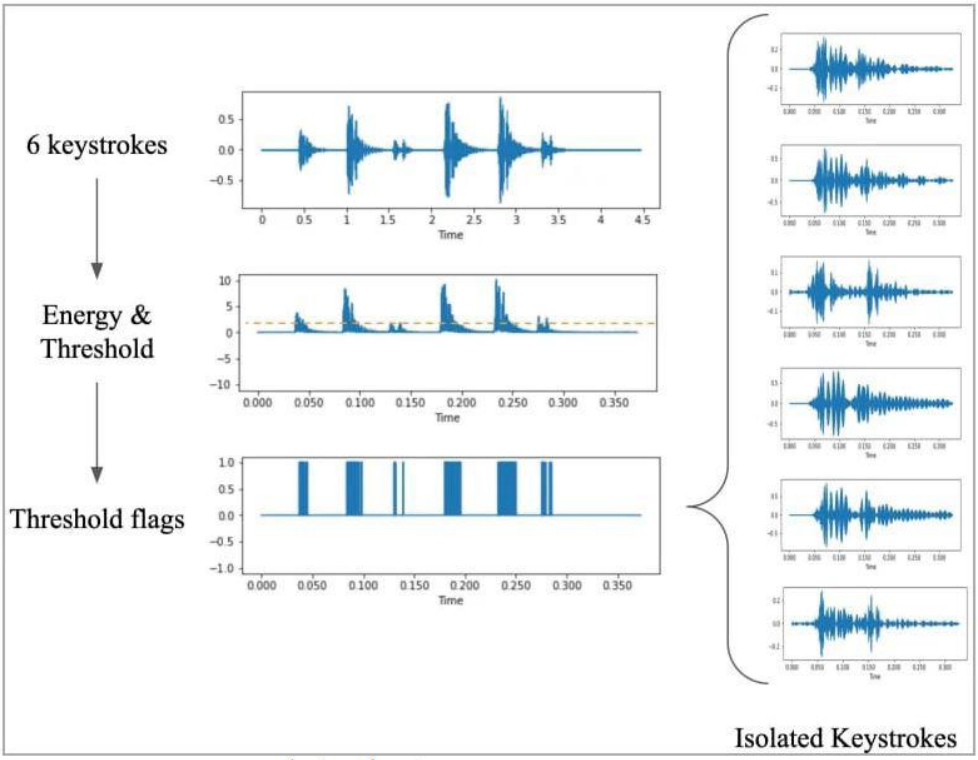
وقتی از نرم‌افزار تماس ویدئویی Zoom برای آموزش الگوریتم طبقه‌بندی صدا استفاده شد، دقت پیش‌بینی به ۹۳ درصد کاهش یافت که هنوز به طور خطرناکی بالاست و برای این رسانه یک رکورد به حساب می‌آید. چنین حمله‌ای به شدت بر امنیت داده‌های هدف تأثیر می‌گذارد، زیرا می‌تواند رمز عبور، گفتگوها، پیام‌ها یا سایر اطلاعات حساس افراد را در اختیار اشخاص ثالث مخرب قرار دهد.

علاوه بر این، برخلاف سایر حملات کانال جانبی که نیاز به شرایط خاصی دارند و در معرض محدودیت‌های سرعت داده و فاصله هستند، حملات صوتی به دلیل فراوانی دستگاه‌های دارای میکروفون که می‌توانند به ضبط صوت با کیفیت بالا دست یابند، بسیار ساده‌تر شده‌اند. این، همراه با پیشرفت‌های سریع در یادگیری ماشین، حملات کانال جانبی مبتنی بر صدا را امکان‌پذیر و بسیار خطرناک‌تر از آنچه قبلاً پیش بینی می‌شد، می‌کند.

گوش دادن به ضربات کلید

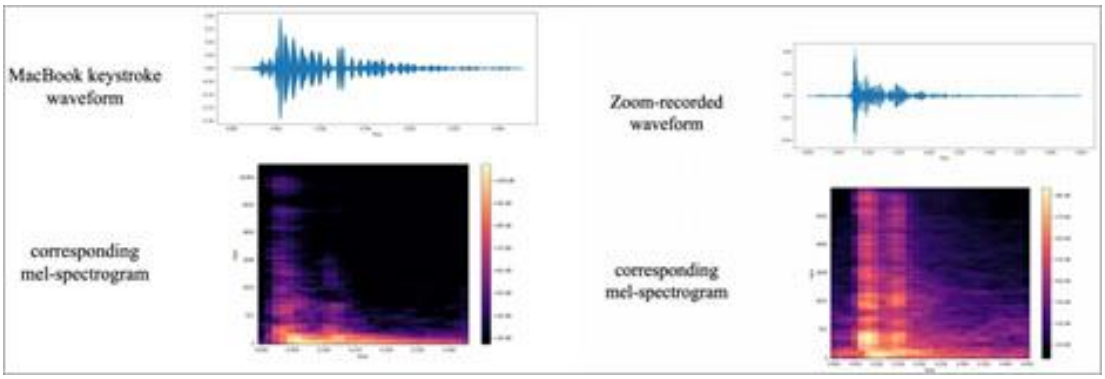
اولین گام حمله، ضبط ضربه‌های کلید روی صفحه‌کلید هدف است، زیرا این داده‌ها برای آموزش الگوریتم پیش‌بینی مورد نیاز است. این را می‌توان از طریق یک میکروفون نزدیک یا تلفن هدف که ممکن است توسط بدافزاری که به میکروفون آن دسترسی دارد آلوده شده باشد، به دست آورد.

از طرف دیگر، ضربه‌های کلید را می‌توان از طریق تماس Zoom ضبط کرد، جایی که یک شرکت‌کننده دغل در جلسه، ارتباط بین پیام‌های تایپ شده توسط هدف و صدای او را ثبت می‌کند. محققان با فشردن ۳۶ کلید روی یک MacBook Pro مدرن ۲۵ بار و ضبط صدای تولیدشده توسط هر فشار، داده‌های آموزشی را جمع‌آوری کردند.



نمونه برداری از صدای ضربه زدن به کلید (arxiv.org)

سپس، آن‌ها شکل موج‌ها و طیف‌نگاری‌هایی را از ضبط‌ها تولید کردند که تفاوت‌های قابل شناسایی را برای هر کلید تجسم می‌کرد و مراحل پردازش داده خاصی را برای تقویت سیگنال‌هایی که می‌توان برای شناسایی ضربه‌های کلید استفاده کرد، انجام دادند.



طیف نگارهای تولید شده (arxiv.org)

تصاویر طیف‌نگاری برای آموزش «CoAtNet» که یک طبقه‌بندی‌کننده تصویر است، استفاده شد، در حالی که این فرآیند به آزمایش‌هایی با پارامترهای تعداد دوره آموزش، نرخ یادگیری و نحوه تقسیم داده‌ها نیاز داشت تا اینکه بهترین نتایج دقت پیش‌بینی به دست آمد.

Parameter	Value
Epochs	1100
Batch Size	16
Loss Type	Cross Entropy
Optimiser	Adam
Max Learning Rate	5e-4
Annealing Schedule	Linear
Timeshift Percentage	0.4
Max Mask Percentage	0.1
Number of Masks Per Axis	2
Mel Bands	64
FFT Window Size	1024
Hop Length	225
Data Split	Random
Normalised Data	Yes

پارامترهای انتخاب شده برای آموزش CoAtNet (arxiv.org)

محققـــان در آزمایش‌هـــای خـــود از لپ‌تـــاپ مشـــابهی کـــه صفحه‌کلیـــد آن در دو ســـال گذشـــته در تمـــام لـــپ تاپ‌هـــای اپـــل اســـتفاده شـــده اســـت، یـــک iPhone 13 mini در فاصلـــه 17 ســـانتی‌متری هـــدف و Zoom اســـتفاده کردنـــد.

راه‌های ممکن کاهش خطر

بـــرای کاربرانـــی کـــه بیش‌ازحـــد نگـــران حمـــلات آکوســـتیک کانـــال جانبـــی هســـتند، ایـــن مقالـــه پیشـــنهاد می‌کنـــد کـــه ســـبک‌های تایـــپ را تغییـــر دهنـــد یـــا از رمزهـــای عبـــور تصادفـــی اســـتفاده کننـــد. ســـایر اقدامـــات دفاعـــی بالقوه شـــامل اســـتفاده از نرم‌افـــزار بـــرای بازتولیـــد صداهـــای ضربـــه زدن بـــه کلیـــد، نویـــز ســـفید یـــا فیلترهـــای صوتـــی مبتنـــی بـــر ضربـــه زدن بـــه کلیـــد اســـت.

مرکز آپا دانشگاه سمنان

آموزش

۸ ابزار تست نفوذ منبع باز که ممکن است درباره آنها ندانید!

Red Siege بسیاری از ابزارهای منبع باز را برای کمک به کار تست نفوذ شما توسعه داده و در دسترس قرار داده است. این شرکت قصد دارد به پشتیبانی از ابزارهای ذکرشده در زیر، چه در قالب رفع اشکال یا ویژگی‌های جدید ادامه دهد. آنها را امتحان کنید، همه آنها به صورت رایگان در GitHub در دسترس هستند.

کریس ترانسر، مشاور ارشد امنیتی و مدیر آموزش Red Siege، به Help Net Security گفت، با انگیزه امکان پر کردن شکاف نرم‌افزاری، خلاقیت‌هایم را متن باز می‌کنم، به این امید که برای دیگران نیز مفید باشند.

AutoFunkt

یک اسکریپت پایتون برای خودکارسازی ایجاد تغییر مسیرهای ابری بدون سرور از پروفایل‌های قابل‌انعطاف C2 Cobalt Strike است.

C2concealer

یک ابزار خط فرمان است که پروفایل‌های قابل‌انعطاف تصادفی C2 را برای استفاده در Cobalt Strike تولید می‌کند.

Dig Dug

با افزودن کلمات از یک فرهنگ لغت به یک فایل اجرایی کار می‌کند. این فرهنگ لغت بارها و بارها اضافه می‌شود تا به اندازه نهایی موردنظر فایل اجرایی برسد. برخی از موتورهای AV و EDR ممکن است آنتروپی را اندازه‌گیری کنند تا مشخص شود که آیا یک فایل اجرایی برای اجرا قابل اعتماد است یا خیر. سایر فروشندگان فایل های اجرایی را برای نشانه‌هایی از pad-ding بایت تهی بررسی می‌کنند.

dumpCake

تلاش‌های احراز هویت رمز عبور را به دیمن SSH می‌ریزد. هر فرآیند فرزند SSHD به اسکریپت متصل می‌شود و پس از تکمیل فرآیند، رمزهای عبور ناموفق و گزارش‌های اتصال به اسکریپت ریخته می‌شوند.

GPPDeception

این اسکریپت یک فایل group.xml تولید می‌کند که یک GPP واقعی را برای ایجاد کاربر جدید در رایانه‌های متصل به دامنه تقلید می‌کند. تیم‌های آبی می‌توانند

از این فایل به‌عنوان honeyfile استفاده کنند. با نظارت بر دسترسی به فایل، Blue Teams می‌تواند pen testers یا عوامل مخربی را که فایل‌های GPP حاوی نام‌های کاربری و گذرواژه‌های cps را برای حرکت جانبی اسکن می‌کنند، شناسایی کند.

WMIOps

یک اسکریپت powershell است که از WMI برای انجام انواع اعمال بر روی هاست ها، محلی یا راه دور، در محیط ویندوز استفاده می‌کند. این در درجه اول برای استفاده در تست های نفوذ یا درگیری‌های تیم قرمز طراحی‌شده است.

Wappybird

یک ابزار Wappalyzer CLI چند رشته‌ای برای یافتن فناوری‌های وب، با خروجی CSV انتخابی است. شما همچنین می‌توانید یک دایرکتوری تهیه کنید و همه داده‌های دورریز شده با یک زیر پوشه در هر هاست ذخیره می‌شوند.

EyeWitness

از وب‌سایت‌ها اسکرین شات می‌گیرد، اطلاعات هدر سرور را جمع‌آوری می‌کند و در صورت امکان اعتبار پیش فرض را شناسایی می‌کند. باعث صرفه جویی در زمان تریاژ وب سایت ها در آزمایش های بزرگ می‌شود. این ابزار معمولاً توسط تسترهای نفوذ استفاده می‌شود که به دنبال بررسی، لیست طولانی وب‌سایت‌ها هستند.

منبع:

https://www.helpnetsecurity.com/2023/07/18/open-source-penetration-testing-tools/

تلاش ما
حفظ امنیت
شماست...