آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

ماهنامه تحلیلی رویداد های امنیتی

اردیبهشت ماه ۱۴۰۰

حوزه های مورد بررسی

فصل اول :
بدافزارها
فصل دوم :
شبکه و ارتباطات
فصل سوم :
نرم‌افزار

cert@eng.ikiu.ir

۰۲۸۳۳۹۰۱۱۱۹

قزوین، دانشگاه بین‌المللی امام خمینی،
دانشکده فنی و مهندسی

فهرست مطالب

بنام خداوند بخشنده و مهربان

یادداشت سردبیر

امروزه تهدیدات سایبری به یکی از مهم‌ترین و اصلی‌ترین نگرانی‌های کاربران فضای مجازی اعم از سازمان‌های دولتی، خصوصی و حتی افراد عادی جامعه تبدیل شده است. در واقع بخش بزرگی از اقشار مختلف جامعه تعریف و درک مناسبی از این خطرات نداشته و بعضا قربانی ساده ترین حملات موجود در این حوزه می‌شوند. حملاتی گر چه ساده اما بسیار پر هزینه برای قربانیان که گاهی حتی امکان جبران آنها نیز به طور کامل وجود ندارد. در این ماهنامه به بررسی امنیت فضای مجازی بر اساس مهم‌ترین اخبار موجود در طول اردیبهشت ماه ۱۴۰۰ پرداخته شده است. مطالبی که می‌تواند نقش بسیار مهمی را در آگاهی‌رسانی کاربران مختلف فضای مجازی نسبت به آخرین تهدیدات و حملات سایبری داشته باشند. . این مطالب در قالب ۳ فصل زیر ارائه شده‌اند.

- بدافزار[1]ها
- تهدیدات شبکه و ارتباطات
- تهدیدات نرم‌افزارها

عدم وجود یک تهدید سایبری در مطالب این ماهنامه به معنی کم‌خطر بودن آن نبوده و تنها توسط تیم خبری مرکز آپا قزوین مورد بررسی قرار نگرفته است. در صورت مشاهده هر گونه مشکل در مطالب این سند اعم از موارد فنی و نگارشی خواهشمندیم موضوع را از طریق پست الکترونیکی Cert@eng.ikiu.ac.ir به کارشناسان ما اطلاع دهید.

محمد پیشدار

[1] هر نوع نرم‌افزاری است که از روی عمد برای آسیب‌زدن به رایانه، خدمت‌رسان=یا شبکه رایانه‌ای طراحی شده‌است.

فصل اول : بدافزار

این فصل اخبار امنیتی مربوط به بدافزار در اردیبهشت ۱۴۰۰ را پوشش می‌دهد. مهم‌ترین موضوع این فصل سوءاستفاده مهاجمان از برخی ابزارهای متداول برای انتقال بدافزارها یا برقراری ارتباط بدون مشکل با آن‌ها است. در پراهمیت‌ترین خبر، مهاجمان سایبری از پیام‌رسان تلگرام برای برقراری ارتباط با بدافزارها و عبور از تجهیزات امنیتی موجود به ویژه موارد مستقر در سازمان‌ها استفاده کرده‌اند.

فهرست مطالب

گسترش استفاده از تلگرام برای کنترل بدافزار[۱]ها

تاریخ: ۲۲/ آوریل / ۲۰۲۱

بررسی اجمالی :

بر اساس اعلام یک شرکت امنیت اطلاعات تحت عنوان چک.پوینت[۲] بسیاری از بدافزارها در یک روند صعودی برای ارتباط با خدمت‌رسان‌های فرمان و کنترل از پیام‌رسان تلگرام استفاده می‌کنند. در پژوهش اخیر این موسسه، طی ۳ ماه گذشته بیش از ۱۳۰ آلوده‌سازی توسط یک تروجان[۳] با قابلیت کنترل راه دور به نام "چشم سمی[4]" کشف شده است. این بدافزار برای ارتباط با خدمت‌رسان فرمان و کنترل[۵] خود از پیام‌رسان تلگرام استفاده می‌کند [۲,۱].

توضیحات بیشتر:

طبق اعلام محققان شرکت چک.پوینت پس از آلوده‌سازی حتی در صورت حذف یا عدم استفاده از پیام‌رسان تلگرام همچنان ارتباط بدافزار با خدمت‌رسان فرمان و کنترل ممکن بوده و به ارسال و دریافت دستورات می‌پردازد. البته استفاده از تلگرام برای تسهیل فعالیت‌های مخرب چیز جدیدی نیست و در سال ۲۰۱۹ یک دزد اطلاعاتی با کمک این پیام‌رسان به سرقت اطلاعات کیف پول‌های ارز دیجیتال می‌پرداخت [۲,۱].

یکی از اصلی ترین دلایل استفاده از پیام‌رسان تلگرام برای این نوع ارتباطات ناشناس بودن آن توسط موتورهای ضدویروس در سازمان‌هاست. علاوه بر این هویت کاربران نیز می‌تواند تا حد زیادی به علت سیاست‌های موجود مخفی بماند. به عبارت دیگر ثبت‌نام در این برنامه تنها نیاز به یک شماره تماس داشته و از سرتاسر جهان امکان ورود به آن وجود دارد [۲,۱].

در آخرین بررسی شرکت چک.پوینت بدافزاری به نام "چشم سمی" از طریق پست‌های الکترونیک فیشینگ[۶] به صورت یک فایل ویندوزی مخرب توزیع می‌شود. این بدافزار پس از استقرار و اجرا در سیستم قربانی برای ارتباط با خدمت‌رسان فرمان و کنترل از پیام‌رسان تلگرام استفاده می‌کند. بدافزاری که سرقت، انتقال و حذف داده در سیستم قربانی از جمله توانایی‌های آن است [۲,۱].

زنجیره حمله این بدافزار به این ترتیب است که ابتدا یک ربات تلگرامی توسط مهاجم ایجاد شده و پس از آن توکن[۷]مربوط به این بات در یک کد مخرب جاسازی می‌شود. این کد سپس به صورت یک فایل قابل اجرا درآمده و از طریق پست‌الکترونیکی

---

[۱] هر نوع نرم‌افزاری است که از روی عمد برای آسیب‌زدن به رایانه، خدمت‌رسان=یا شبکه رایانه‌ای طراحی شده‌است.

[۲] CheckPoint

[۳] یک برنامه نفوذی است که از نوع بدافزار است و به سیستم عامل دسترسی سطح بالا پیدا می‌کند در حالی که به نظر می‌آید یک کار مناسب در حال انجام است.

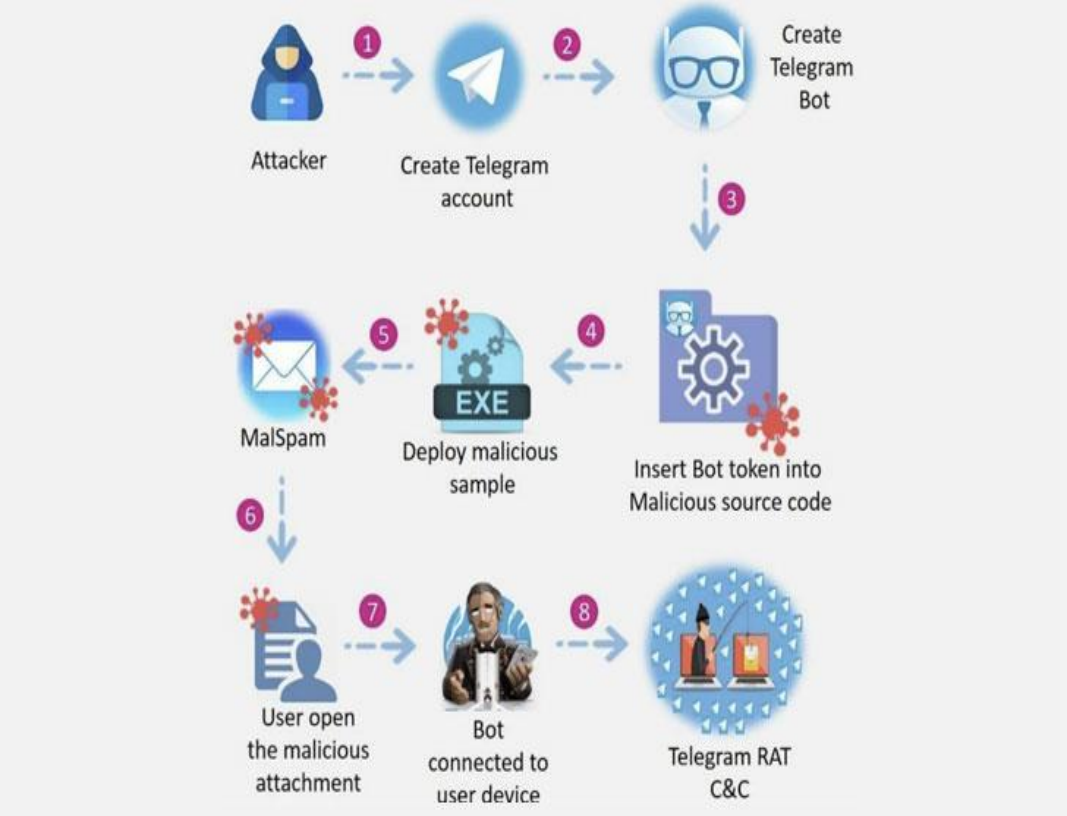
[۴] ToxicEye

[۵] یک خدمت‌رسان مرکزی برای ارسال و دریافت دستورات به یک بدافزار پس از استقرار در سیستم قربانی

[۶] به تلاش برای به دست آوردن اطلاعاتی مانند نام کاربری، گذرواژه، اطلاعات حساب بانکی و مانند آن‌ها از طریق جعل یک وبگاه، آدرس پست الکترونیک و مانند آن‌ها گفته می‌شود.

[۷] Token

و فیشینگ به سیستم قربانی ارسال می‌شود. با اجرای این فایل در سیستم قربانی ارتباط با بات تلگرامی برقرار خواهد شد. این موارد را می‌توان در تصویر شماره ۱ مشاهده نمود [۲,۱].



شکل ۱ : زنجیره حمله استفاده از تلگرام جهت ارتباط با خدمت رسان فرمان و کنترل در بدافزار چشم سمی [۲,۱]

راه حل‌های پیشنهادی :

- کنترل استفاده از پیام‌رسان تلگرام در سازمان
- آشنایی و مقابله با حملات فیشینگ در سازمان
- استفاده از فرآیند جعبه‌شنی[۱] برای اجرای فایل‌های جدید
- استفاده از تجهیزات امنیتی بروز برای کنترل ترافیک ورودی

منابع :

1. The Hacker News Website
https://thehackernews.com/2021/04/cybercriminals-using-telegram-messenger.html
2. Jioforme Website
https://www.jioforme.com/cyber-%E2%80%8B%E2%80%8Bcriminals-using-telegram-messenger-to-control-toxic-eye-malware/363767/

[۱] جعبه شنی (به انگلیسی: Sandbox) یک سازوکار حفاظتی برای جدا نگاه‌داشتن بعضی نرم‌افزارهای در حال اجرا در آن واحد با دیگر نرم‌افزارهاست.

انتقال بدافزار[۱] به کمک موتور بیلد[۲] مایکروسافت

تاریخ: ۱۴/ مِی / ۲۰۲۱

بررسی اجمالی :

مهاجمان سایبری از موتور بیلد مایکروسافت برای انتقال تروجان[۳]های کنترل راه دور یا سارق اطلاعات به سیستم‌های ویندوزی سوءاستفاده کرده‌اند. بر اساس گزارش محققان شرکت امنیت سایبری آنومالی[۴] این فعالیت در حال حاضر فعال بوده و حتی حدود یک ماه از فعالیت آن نیز می‌گذرد [۲,۱].

توضیحات بیشتر:

مایکروسافت بیلد ابزاری متن باز برای پروژه‌های دات‌نت[۵] و ویژوال استودیو[۶] بوده که به کمک آن امکان تدوین کد منبع، بسته‌بندی، آزمایش و استقرار برنامه‌های ویندوزی یا وب ممکن است. بر اساس پژوهش محققان یک شرکت امنیت اطلاعات تحت عنوان آنومالی، یک فایل بیلد مخرب می تواند در فایل‌های اجرایی و کدهای پوسته مخفی شده (به صورت کدشده) و سپس نقش در پشتی[۷] را در سیستم آلوده ایفا کند. به این ترتیب امکان سرقت اطلاعات و حتی کنترل سیستم قربانی فراهم می‌گردد [۲,۱].

هدف مهاجمان از این کار جلوگیری از تشخیص بدافزار و قانونی نشان دادن برنامه آلوده است. به عبارت دیگر بدافزار می‌تواند بدون تشخیص در حافظه اصلی اجرا شده و به سرقت اطلاعات حساس بپردازد. محققان شرکت آنومالی انتقال بدافزارهای زیر را به کمک این روش تا کنون گزارش کرده‌اند [۲,۱].

- Remcos[۸] یک تروجان کنترل و نظارت بر سیستم قربانی بوده که پس از نصب دسترسی کامل به سیستم قربانی را برای مهاجم فراهم می‌سازد. از جمله ویژگی‌های این بدفزار سرقت اطلاعات کاربر، اجرای دستورات، ضبط میکروفون و وبکم می‌باشد.
- Quasar یک تروجان راه دور متن باز بر اساس پروژه دات.نت بوده که قابلیت‌های زیادی از جمله سرقت کلمات عبور و کلیک‌ها را دارد.

---

[۱] نرم‌افزاری که از روی عمد برای آسیب‌زدن به رایانه، سرور، کارخواه، یا شبکه رایانه‌ای طراحی شده است.

[2] Microsoft Build Engine

[۳] یک برنامه نفوذی از نوع بدافزار بوده که به سیستم عامل در قالب یک برنامه عادی دسترسی سطح بالا پیدا می‌کند.

[۴] Anomali

[۵] یک فناوری نرم‌افزاری است که بر روی تمامی ویرایش‌های سیستم‌عامل ویندوز مایکروسافت قابل اجرا است. این چارچوب مجموعه‌ای از زبانهای برنامه‌نویسی و همچنین کتابخانه‌های بسیار غنی جهت کمک به سهولت توسعه نرم‌افزار را در برمیگیرد.

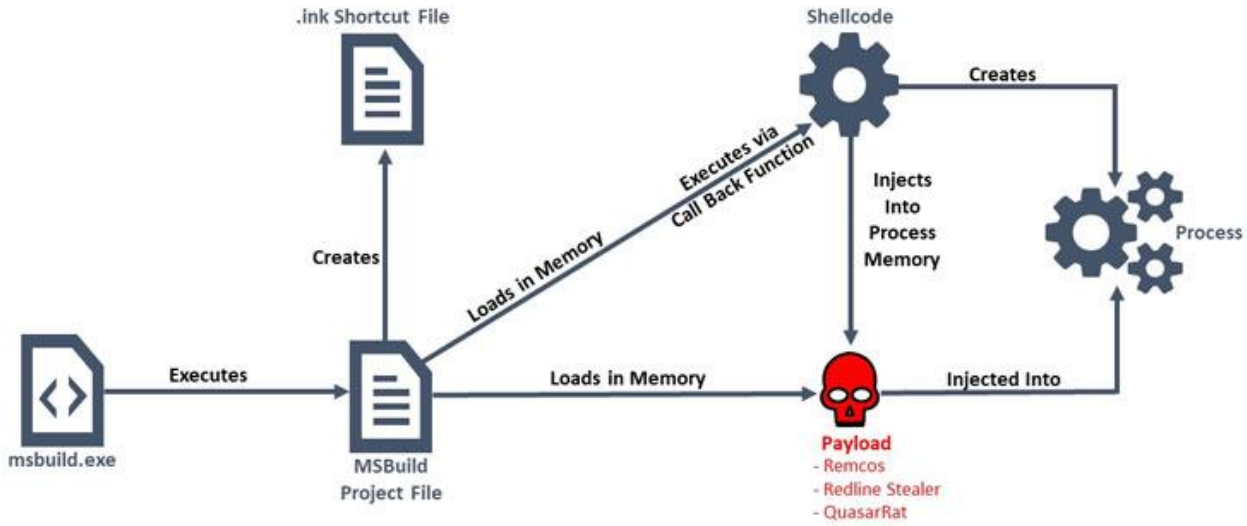
[۶] ویژوال استودیو نام محیط یکپارچه توسعه نرم‌افزار (IDE) شرکت مایکروسافت بوده که جهت تولید برنامه رایانه‌ای برای مایکروسافت ویندوز یا برنامه‌های کاربردی وب استفاده می‌شود.

[۷] به راهی گفته می‌شود که به کمک آن بتوان بدونِ اجازه به قسمت یا قسمت‌های مشخصی از یک سامانه مانند رایانه، دیوار آتش، یا افزاره‌های دیگر دست پیدا کرد.

[8] Remote Control and Surveillance software

- Redline Stealer نیز یکی دیگر از بدافزارهایی است که اطلاعات مهمی مانند کلمات عبور را از مرورگرها، وی.پی.ان[۱]، پیام‌رسان‌ها و کیف پول‌های ارز دیجیتال به سرقت می‌برد.

تارا گولد[۲] و گاجمل[۳] از محققان شرکت آنومالی، در این رابطه گفته‌اند: "مهاجمان سایبری این کمپین، از تحویل بدون پرونده (بدافزاری که سیستم قربانی را آلوده کرده اما هیچ گونه فایل اجرایی بر روی هارد دیسک به جا نمی‌گذارد) به عنوان راهی برای عبور از اقدامات امنیتی استفاده کرده‌اند. بر اساس تحقیقات موجود، اتکا به نرم‌افزار ضد ویروس به تنهایی برای دفاع در برابر این نوع تهدید کافی نبوده و مهاجمان برای پنهان‌سازی بدافزار، آن را به صورت کدهای مجاز جلوه می‌دهند. بر همین اساس این کمپین به سرعت و تصاعدی در حال رشد است" [۲,۱]. در شکل شماره ۱ می‌توانیم مراحل انتقال بدافزار به کمک این روش را مشاهده کنیم.



شکل ۱ : مراحل انتقال بدافزار به کمک موتور بیلد مایکروسافت [۱]

منابع :

1. The Hacker News Website
   https://thehackernews.com/2021/05/hackers-using-microsoft-build-engine-to.html
2. Securityaffairs Website
   https://securityaffairs.co/wordpress/117969/malware/msbuild-delivers-rat.html

[۱] وی‌پی‌ان (به انگلیسی: VPN، مخفف Virtual Private Network)، شبکه‌ای است که اطلاعات در آن از طریق یک شبکه عمومی مانند اینترنت جابه‌جا شده اما با استفاده از الگوریتم‌های رمزنگاری و با احراز هویت ارتباط هم‌چنان اختصاصی باقی می‌ماند.

[2] Tara Gould
[3] Gage Mele

هشدار مایکروسافت نسبت به انتشار یک بدافزار [۱]سارق اطلاعات

تاریخ: ۲۱/ مِی / ۲۰۲۱

بررسی اجمالی :

شرکت مایکروسافت، روز پنجشنبه نسبت به یک فعالیت گسترده یک کمپین انتشار بدافزار از طریق پست‌الکترونیکی هشدار داده است. این بدافزار در اصل به صورت یک تروجان[۲] سارق داده بر مبنای جاوا[۳] بوده که خود را برای پیچیده‌سازی فرآیند تشخیص توسط ابزارهای امنیتی به صورت باج‌افزار[۴] نشان می‌دهد [۲,۱].

توضیحات بیشتر:

تیم تحقیقات امنیت اطلاعات شرکت مایکروسافت در قالب چند رشته توئیت اعلام کرده است که این بدافزار جدید به علت افزودن پسوند crimson به فایل‌ها خود را به صورت باج‌افزار نشان می‌دهد. این در حالیست که هیچگونه رمزنگاری در فایل‌های مذکور صورت نگرفته و تنها با حذف پسوند مربوطه فایل‌ها قابل اجرا خواهند بود [۲,۱].

این تیم همچنان اعلام کرده که کمپین پست الکترونیکی برای نشر این بدافزار به صورت گسترده فعال است. در این فعالیت‌ها پیام‌های زیادی شامل یک فایل پی.دی.اف با عناوین و جزئیات جذاب و محرک‌های مالی منتقل می‌شود. در صورت اجرای فایل مذکور توسط قربانی ارتباط با یک دامنه مخرب برقرار شده که شروع فرآیند بارگیری بدافزار را به دنبال دارد [۱]. در تصویر شماره ۱ می‌توان یک نمونه از این پست‌الکترونیکی را مشاهده نمود.

این بدافزار در ژوئن سال ۲۰۲۰ برای اولین بار توسط یک شرکت امنیتی آلمانی مشاهده و گزارش شده است. یک تحلیل‌گر بدافزار به نام کارستن هان[۵] در این رابطه می‌گوید : "تروجان مذکور بر سرقت اطلاعات مرورگر و سرویس گیرنده‌های پست‌الکترونیک و رمزهای عبور از طریق ورود به سیستم متمرکز است" [۲,۱].

این بدافزار پس از اجرا در سیستم قربانی علاوه بر ارتباط با یک خدمت‌رسان درخواست و کنترل[۶] ویژگی‌های زیادی را نیز از جمله جمع‌آوری کلمات عبور ذخیره شده در مرورگر، فایل‌های ثبت رویداد[۷] و اجرای اسکریپت‌های پاورشل[۸] را به مهاجم سایبری می‌دهد [۲,۱].

---

[۱] هر نوع نرم‌افزاری که از روی عمد برای آسیب‌زدن به رایانه، سرور یا شبکه رایانه‌ای طراحی شده است.

[۲] یک برنامه نفوذی از نوع بدافزار است که به سیستم‌عامل قربانی در قالب یک برنامه عادی دسترسی سطح بالا پیدا می‌کند.

[۳] نکارش استاندارد، مجموعه‌ای از واسطهای برنامه‌نویسی است.

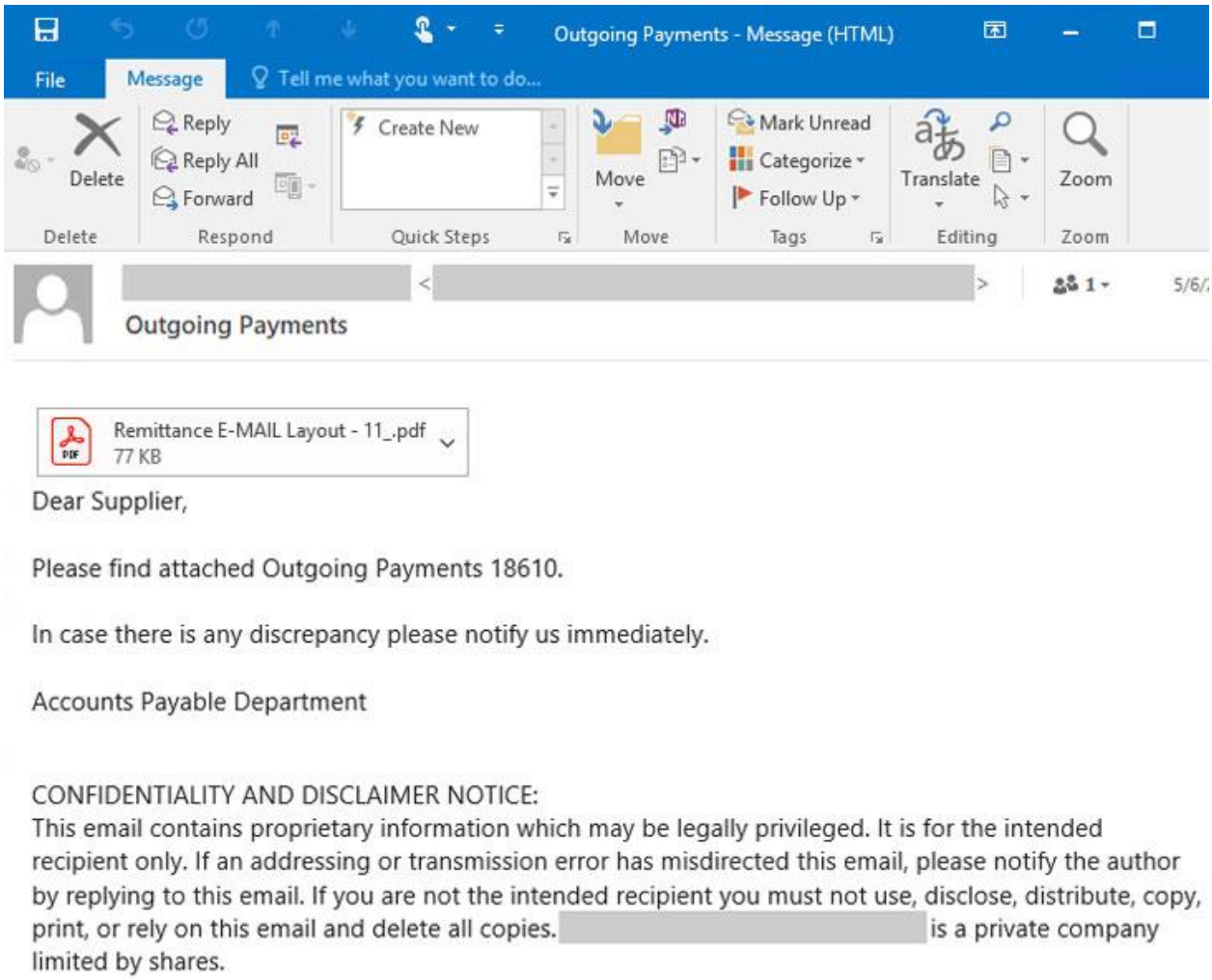
[۴] گونه‌ای از بدافزارها که دسترسی به یک سامانه را محدود کرده و برای برداشتن محدودیت مذکور درخواست باج می‌کنند.

[۵] Karsten Hahn

[۶] یک سیستم رایانه‌ای تحت کنترل مهاجم برای ارسال دستورات و دریافت اطلاعات از سیستم‌های آلوده به بدافزار

[۷] Log File

[۸] یک موتور خودکار قابل ارتقا از طرف مایکروسافت است که شامل یک پوسته خط فرمان و همراه با یک زبان اسکریپت‌نویسی است.



شکل ۱ : نمونه‌ای از پست‌الکترونیکی برای انتشار بدافزار مربوطه [۱]

منابع :

1. The Hacker News Website
   https://thehackernews.com/2021/05/microsoft-warns-of-data-stealing.html
2. Cybersafe Website
   https://www.cybersafe.news/microsoft-warns-of-data-stealing-malware-that-pretends-to-be-ransomware/

فصل دوم : شبکه و ارتباطات

دومین فصل از این ماهنامه مربوط به اخبار شبکه و ارتباطات بوده و در آن سعی شده تا مهم‌ترین موضوعات این حوزه در ماه گذشته بررسی شود. مهم‌ترین خبر فصل جاری را می‌توان کشف آسیب‌پذیری در تمام دستگاه‌های وای.فای دانست. نقصی در پیاده‌سازی استاندارد مورد استفاده در فناوری وای.فای[۱] که تقریبا تمام دستگاه‌های اجراکننده آن را در معرض خطر قرار می‌دهد.

فهرست مطالب

[۱] نامی تجاری است که توسط «اتحادیه وای-فای (Wi-Fi Alliance)» ثبت شده و علامتی است که این اتحادیه به محصولاتی که مورد تأیید این اتحادیه جهت کار در شبکه محلی بی‌سیم تحت استاندارد IEEE۸۰۲/۱۱ می‌باشد، اعطا می‌کند.

نقص امنیتی در بسیاری از دستگاه‌های اینترنت اشیاء[۱]

تاریخ: ۳۰/ آوریل / ۲۰۲۱

بررسی اجمالی :

محققان شرکت مایکروسافت[۲] به تازگی از وجود چندین آسیب‌پذیری امنیتی در تعداد زیادی از دستگاه‌های اینترنت اشیاء و فناوری عملیاتی[۳] خبر داده‌اند. این دستگاه‌ها به طور گسترده در بخش پزشکی، صنعتی و حتی شبکه‌های سازمانی مورد استفاده قرار می‌گیرند. به گفته مایکروسافت، مهاجمان سایبری می‌توانند از این نقص امنیتی برای اجرای کدهای غیرمجاز و یا محروم‌سازی از سرویس[۴] در دستگاه‌های آسیب‌پذیر استفاده کنند [۲,۱].

توضیحات بیشتر:

بر اساس اعلام بخش تحقیقاتی Azure Defender در شرکت مایکروسافت تعدادی آسیب‌پذیری‌های اجرای کد (RCE[۵]) در قالب بیش از ۲۵ سی.وی.ای[۶]، طیف وسیعی از دستگاه‌های اینترنت اشیاء را در صنعت، پزشکی و شبکه‌های سازمانی مورد تهدید قرار می‌دهد [۲,۱]. مجموعه این آسیب‌پذیری‌ها تحت عنوان BadAlloc نام‌گذاری شده چرا که در همه موارد نوع نقص در پیاده‌سازی‌های مربوط به توابع تخصیص حافظه وجود دراد. این پیاده‌سازی‌ها شامل سیستم‌های عامل بی‌درنگ[۷]، کیت‌های توسعه نرم افزار[۸] تعبیه شدهو پیاده‌سازی مربوطه به کتابخانه‌های استاندارد در زبان برنامه‌نویسی سی[۹] هستند [۲,۱].این موارد از استفاده توابع آسیب‌پذیر حافظه مانند malloc ، calloc، realloc، memalign، valloc، pvalloc و غیره ناشی می‌شوند [۲]. به عبارت دیگر فقدان اعتبارسنجی ورودی در این توابع می‌تواند یک مهاجم سایبری را قادر به انجام حملات سرریز بافر[۱۰] کرده که از طریق آن اجرای کد مخرب در یک دستگاه آسیب پذیر ممکن خواهد شد [۲,۱]. شکل شماره ۱ یک نمونه از این نوع آسیب‌پذیری‌ها است.

---

[۱] به‌طور کلی اشیا و تجهیزاتی که به شبکه اینترنت متصل شده و توسط اپلیکیشن‌های موجود در تلفن‌های هوشمند قابل کنترل و مدیریت هستند.

[۲] Microsoft

[۳] بطوری کلی فناوری‌های علمیاتی یا Operational Technology (OT) شامل سیستم‌های سخت‌افزاری و نرم‌افزاری می‌شوند که فرآیندها و تجهیزات فیزیکی که عمدتاً در تأسیسات، نفت، آب، گاز و برق و یا حتی خطوط تولید صنعتی، فرآیندهای داروسازی و شبکه‌های دفاعی دیده می‌شود را کنترل و نظارت می‌کنند.

[۴] تلاش برای خارج کردن ماشین و منابع شبکه از دسترس کاربران مجازش

[۵] Remote Code execution

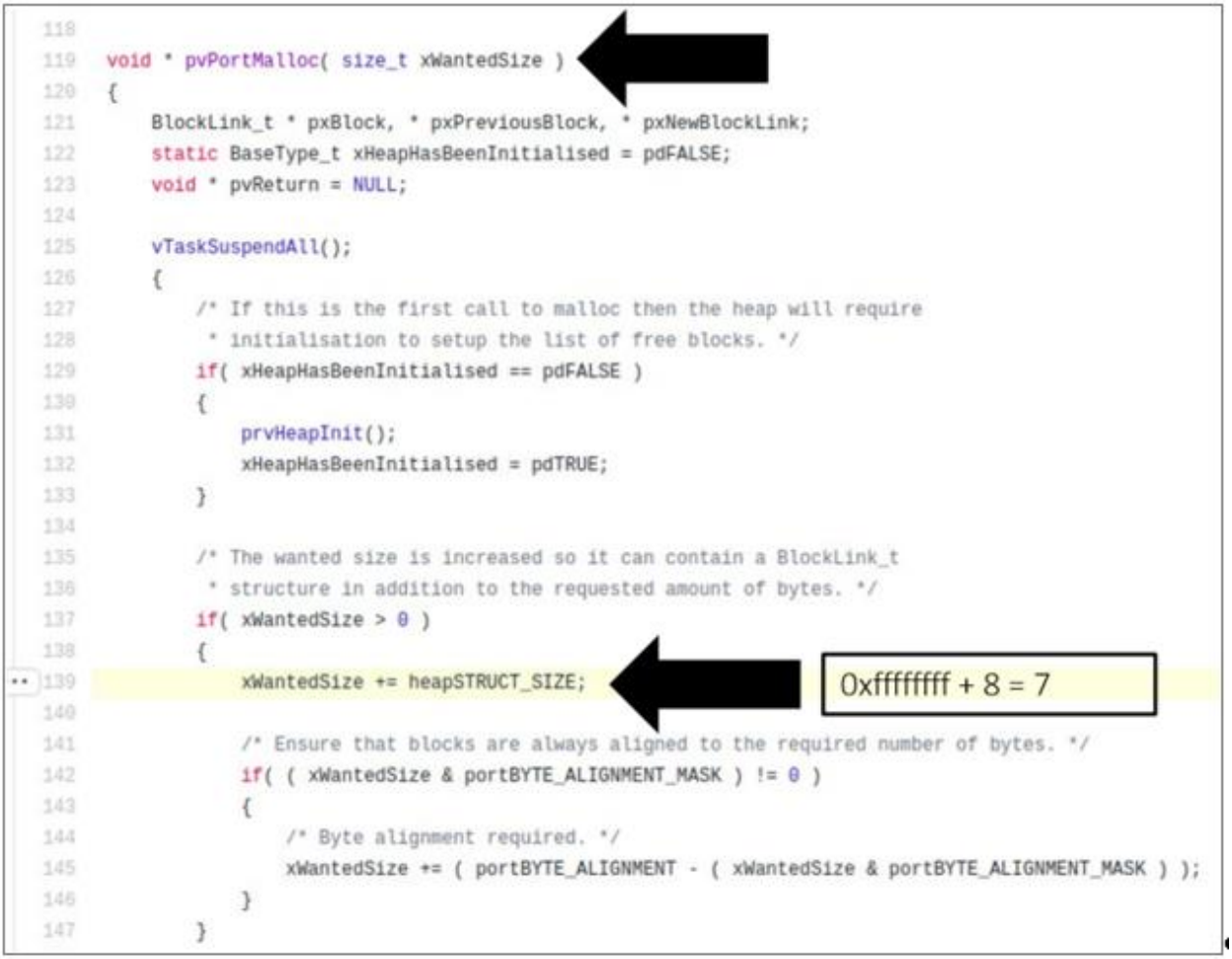
[۶] نوعی شناسه برای تشخیص آسیب‌پذیری‌های رایانه‌ای

[۷] نوعی سیستم‌عامل که دارای ویژگی چند نخی است و برای کاربردهای بی‌درنگ پیچیده ای که نیاز به پاسخگویی‌های سریع و قطعی دارند، طراحی شده‌است.

[۸] مجموعه توابع و کتابخانه‌های کامپایل شده‌ای که تولیدکنندگان نرم‌افزار برای آسان کردن برنامه‌نویسی برای محیط یا سکوی خاصی فراهم می‌کنند.

[۹] نوعی زبان برنامه‌نویسی از نوع همه‌منظوره، کامپایل‌شونده، سطح میانی، ساخت‌یافته، دستوری و روندگرا

[۱۰] یک استثنا است که در آن برنامه، هنگامی که در حال نوشتن داده‌ها به بافر است، از مرز بافر تخطی کرده و باعث رونویسی حافظه مجاور می‌شود.



شکل ۱ : یک نمونه کد دارای آسیب‌پذیری Badalloc [۲].

دستگاه‌های موجود در لیست زیر در برابر مجموعه BadAlloc آسیب‌پذیر هستند [۱].

- Amazon FreeRTOS, Version 10.4.1
- Apache Nuttx OS, Version 9.1.0
- ARM CMSIS-RTOS2, versions prior to 2.1.3
- ARM Mbed OS, Version 6.3.0
- ARM mbed-uallaoc, Version 1.3.0
- Cesanta Software Mongoose OS, v2.17.0
- eCosCentric eCosPro RTOS, Versions 2.0.1 through 4.5.3
- Google Cloud IoT Device SDK, Version 1.0.2
- Linux Zephyr RTOS, versions prior to 2.4.0
- MediaTek LinkIt SDK, versions prior to 4.6.1
- Micrium OS, Versions 5.10.1 and prior
- Micrium uCOS II/uCOS III Versions 1.39.0 and prior
- NXP MCUXpresso SDK, versions prior to 2.8.2
- NXP MQX, Versions 5.1 and prior
- Redhat newlib, versions prior to 4.0.0
- RIOT OS, Version 2020.01.1
- Samsung Tizen RT RTOS, versions prior 3.0.GBB
- TencentOS-tiny, Version 3.1.0
- Texas Instruments CC32XX, versions prior to 4.40.00.07

- Texas Instruments SimpleLink MSP432E4XX
- Texas Instruments SimpleLink-CC13XX, versions prior to 4.40.00
- Texas Instruments SimpleLink-CC26XX, versions prior to 4.40.00
- Texas Instruments SimpleLink-CC32XX, versions prior to 4.10.03
- Uclibc-NG, versions prior to 1.0.36
- Windriver VxWorks, prior to 7.0

مایکروسافت اعلام کرده که تاکنون هیچگونه گزارشی در رابطه با بهره‌برداری از این آسیب‌پذیری‌ها پیدا نکرده است. اگر چه دسترسی به وصله[۱]های منتشر شده امکان استفاده از تکنیکی به نام "patch varying" را جهت مهندسی معکوس[۲]و کشف آسیب‌پذیری در اختیار مهاجمان قرار می‌دهد [۱] .

پیشنهادات :

- اعمال بروزرسانی منتشر شده از طرف شرکت فروشنده دستگاه
- جلوگیری یا مقابله با کشف دستگاه‌های آسیب‌پذیر سازمان در شبکه‌های ناامن
- جداسازی دستگاه‌های اینترنت اشیاء (به خصوص موارد آسیب‌پذیر) از فضای اینترنت
- کنترل و بررسی مداوم ارتباطات ورودی و خروجی به دستگاه‌های آسیب‌پذیر برای کشف و مقابله با موارد مشکوک

منابع :

1. The Hacker News Website
   https://thehackernews.com/2021/04/microsoft-finds-badalloc-flaws.html
2. Microsoft Blog
   https://msrc-blog.microsoft.com/2021/04/29/badalloc-memory-allocation-vulnerabilities-could-affect-wide-range-of-iot-and-ot-devices-in-industrial-medical-and-enterprise-networks/

[۱] مجموعه‌ای از تغییرات در یک برنامه کامپیوتری یا داده‌های پشتیبان آن است که برای به‌وزرسانی، رفع یا بهبود آن طراحی شده‌است.

[۲] فرایند کشف اصول تکنولوژیکی یک دستگاه، شیء یا یک سیستم می‌باشد که از طریق تجزیه و تحلیل ساختار و عملکرد آن حاصل می‌شود.

نقص امنیتی در پردازنده‌های اینتل[۱] و اِی.اِم.دی[۲]

تاریخ: ۰۶/ مِی / ۲۰۲۱

بررسی اجمالی :

Spectre یک گروه از آسیب‌پذیری‌های خاص بوده که پردازنده‌های مدرن را تحت تاثیر قرار می‌دهد. این گروه آسیب‌پذیری در سال ۲۰۱۸ کشف شده و هنوز هم بسیاری از رایانه‌ها را تهدید می‌کند. به عبارت دیگر محققان هنوز موفق به کشف راه‌حلی مناسب برای رفع کامل این خطر نشده‌اند [۲,۱].

توضیحات بیشتر:

تیمی از محققان دانشگاه‌های ویرجینیا[۳]، کالیفرنیا[۴] و سَن‌دیگو[۵]، از حمله جدیدی با قابلیت عبور از تمام محافظت‌های موجود برای آسیب‌پذیری‌های Spectre در تراشه‌های مختلف خبر داده‌اند. حمله‌ای که به طور بالقوه تقریبا تمام سیستم‌های رایانه‌ای از جمله کامپیوترهای رومیزی ، قابل‌حمل ، خدمت‌رسان‌های ابری[۶] و تلفن‌های هوشمند را در معرض خطر قرار می‌دهد [۲,۱].

حدود ۳ سال پیش حملات ملتدان[۷] و Spectre دید مناسبی را در رابطه با تهدیدات سطح پردازنده ایجاد کردند. از آن زمان تا کنون سازندگان تراشه‌های رایانه‌ای نظیر اینتل و اِی.اِم.دی به طور مداوم برای ایجاد راه‌حل‌های دفاعی جهت کاهش آسیب‌پذیری‌های این حوزه در تلاشند. به طوریکه قابلیت خواندن اطلاعات مهمی از جمله رمزهای عبور، کلیدهای رمزگذاری مستقیماً از حافظه هسته رایانه ممکن نباشد [۱].

Spectre جداسازی بین برنامه‌های مختلف را با استفاده از حملات کانال جانبی[۸] از بین برده و سپس به کمک یک روش بهینه‌سازی موجود در پیاده سازی سخت افزار CPU برنامه‌ها را برای دسترسی به مکان های دلخواه در حافظه فریب می‌دهد. در واقع پردازنده با این فریب دستورالعمل‌هایی را در مسیر اشتباه اجرا می‌کند. به این ترتیب امکان شنود اطلاعات حساس فراهم خواهد گردید [۱].

در نوع جدید این حمله، حافظه نهان عملیات میکرو[۹] (واحدی برای افزایش سرعت اجرای دستورات) مورد حمله کانال جانبی قرار می‌گیرد [۲,۱]. این فناوری از سال ۲۰۱۱ در پردازنده‌های اینتل وجود داشته و حتی یک تکنیک نیز تحت عنوان LFENCE برای مقابله با حملات سایبری در آن تعبیه شده است. در این تکنیک کدهای حساس در مکانی مشخص قرار گرفته

---

[۱] اینتل (به انگلیسی: Intel) یک شرکت چندملیتی آمریکایی است که در زمینه تولید و طراحی انواع مختلف سخت‌افزار رایانه فعالیت می‌نماید.

[۲] اِی.اِم.دی (AMD) یک شرکت آمریکایی سازنده انواع پردازنده است که در سال ۱۹۶۹ توسط جری ساندرز تأسیس شد.

[۳] ویرجینیا (به انگلیسی: Virginia) ایالتی است که در منطقه آتلانتیک جنوبیِ ایالات متحده واقع شده‌است.

[۴] کالیفرنیا (به انگلیسی: California)، ایالتی در غرب آمریکا است.

[۵] سَن دیِگو (به انگلیسی: San Diego) یک شهر ساحلی در جنوب کالیفرنیا واقع در گوشه جنوب غربی ایالات متحده آمریکا است.

[۶] رایانش اَبری (به انگلیسی: Cloud computing) مدل رایانشی بر پایه شبکه‌های رایانه‌ای مانند اینترنت است که الگویی تازه برای عرضه، مصرف و تحویل خدمات رایانشی با به‌کارگیری شبکه ارائه می‌کند.

[۷] ملتدان (به انگلیسی: Meltdown) به‌طور مستقیم ریشه در پردازنده‌های کامپیوتری دارد و مرز بین فضای کاربر و هسته سیستم عامل (کرنل) را می‌شکند که باعث نشت اطلاعات از هسته مرکزی به برنامه‌های کاربر می‌شود

[۸] به حمله‌ای گفته می‌شود که بر اساس اطلاعات بدست آمده از پیاده‌سازی یک سیستم رایانه ای باشد نه ضعف‌هایی که در الگوریتم پیاده‌سازی آن وجود دارد.

[۹] Micro-operation cache

تا یک سری عملیات امنیتی بر روی آن‌ها صورت گیرد. در نوع جدید حملات Spectre امکان شنود اطلاعات مهم از این فناوری نیز به کمک حملات کانال جانبی وجود دارد. علاوه بر پردازنده‌های اینتل، محصولات ای.ام.دی نیز در برابر این نوع تهدیدات جدید با نرخ خطای ۵,۵۹ درصد آسیب‌پذیر هستند [۱].

شرکت اینتل برای مقابله با این نوع تهدیدات رعایت اصول برنامه‌نویسی در زمان ثابت را توصیه می‌کند .عملی که گفتن آن از انجامش آسان‌تر بوده و مستلزم کارآیی بالا به علت وجود چالش‌های زباد در وصله[۱]کاری نرم افزارها است. علاوه بر این تغییرات نرم‌افزار به تنهایی نمی تواند تهدیدات ناشی از Spectre را کاهش دهد [۱].

محققان برای محافظت در برابر حمله جدید پیشنهادات زیر را ارائه کرده‌اند [۱].

- حافظه پنهان عملیات میکرو را پاک کنید ،
- شمارنده های کارایی را اهرم کرده و رفتارهای غیرعادی در حافظه نهان عملیات میکرو را تشخیص دهید. سپس حافظه مذکور را بر اساس سطح امتیازات تخصیص یافته به کد تقسیم بندی کرده و از افزایش دسترسی کدها به صورت غیرمجاز جلوگیری کنید.

منابع :

1. The Hacker News Website
   https://thehackernews.com/2021/05/new-spectre-flaws-in-intel-and-amd-cpus.html
2. Engadget Website
   https://www.engadget.com/three-new-intel-amd-spectre-vulnerabilities-092432930.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJWzaaduq01PlHGM5tIzfcYZ2mnC4GjgZMu6kBOCqJE0UNJ3Rqy2k2uYWIJW2ab1SfCyoUKu3SmpeJkVolHE1CWon_shoa9GSzwh-F7LcKf1Ro4iSruHX2-HLtu379hWXGMbnbRn1_Ubv9E8qjXnkOXSexeE7iJI86In_oMSXsYm

[۱] یک پچ (به انگلیسی: Patch) مجموعه‌ای از تغییرات در یک برنامه کامپیوتری یا داده‌های پشتیبان آن است که برای به روز رسانی، رفع یا بهبود آن طراحی شده‌است.

کشف آسیب‌پذیری در تمام دستگاه‌های وای.فای[۱]

تاریخ: ۱۲/ مِی / ۲۰۲۱

بررسی اجمالی :

چند نقص امنیتی در طراحی و پیاده سازی استاندارد IEEE 802.11 شبکه‌های بیسیم کشف شده است. این استاندارد اساس دستگاه‌های وای.فای در سراسر جهان بوده و به کمک آن دستگاه‌های مختلفی نظیر تلفن‌های هوشمند، رایانه‌های همراه و تبلت‌ها با اینترنت از طریق مودم بیسیم ارتباط برقرار می‌کنند. بر اساس اعلام محققان با سوءاستفاده از نقص‌های امنیتی جدید امکان سرقت اطلاعات محرمانه یا کنترل سیستم قربانی وجود دارد [۲,۱].

سیستم‌های آسیب‌پذیر	دستگاه‌های وای.فای
راه‌های نفوذ	ارسال ترافیک مخرب
هدف مهاجمان	جعل و شنود ترافیک، تزریق بسته، حملات محروم‌سازی از سرویس و هدایت قربانی برای استفاده از یک خدمت‌رسان DNS[۲] مخرب
شناسه آسیب‌پذیری	• **CVE-2020-24588** • **CVE-2020-24587** • **CVE-2020-24586** • **CVE-2020-26145** • **CVE-2020-26144** • **CVE-2020-26140** • **CVE-2020-26143** • **CVE-2020-26139** • **CVE-2020-26146** • **CVE-2020-26147** • **CVE-2020-26142** • **CVE-2020-26141**
شدت خطر	نامشخص بر اساس استاندارد سی.وی.اِس.اِس[۳]

توضیحات بیشتر:

[۱] نامی تجاری است که توسط «اتحادیه وای-فای (Wi-Fi Alliance)» ثبت شده و علامتی است که این اتحادیه به محصولاتی که مورد تأیید این اتحادیه جهت کار در شبکه محلی بی‌سیم تحت استاندارد IEEE ۸۰۲/۱۱ می‌باشد، اعطا می‌کند.

[۲] یک سیستم سلسله‌مراتبی نام‌گذاری برای کامپیوترها، سرویس‌ها، یا منابع دیگر است که به شبکه اینترنت یا یک شبکه خصوصی (LAN) متصل هستند.

[۳] نوعی استاندارد برای کمی‌سازی شدت خطر در یک آسیب‌پذیری

نقص‌های امنیتی کشف شده در دستگاه‌های وای.فای توسط حملاتی تحت عنوان Frag[۱] قابل بهره‌گیری هستند. این حملات بر اساس گزارشات موجود تمام پروتکل‌های امنیتی فناوری وای.فای از جمله WEP[۲] و WPA3[۳]را تحت تاثیر قرار می‌دهد. WPA3 یک پروتکل امنیتی بوده که پس از معرفی در ژانویه ۲۰۱۸ در قلب بسیاری دستگاه‌های وای.فای تعبیه شد. به کمک این پروتکل احراز هویت و رمزنگاری پیشرفت مناسبی کرده و امنیت بیشتری را برای ارتباطات بیسیم ممکن می‌سازد. WEP نیز یک پروتکل امنیتی قدیمی برای دستگاه‌های وای.فای بوده که WPA جایگزین آن است. بنابراین تمام دستگاه‌های وای.فای را می‌توان به نوعی آسیب‌پذیر در برابر این حملات جدید عنوان نمود. یک محقق امنیتی تحت عنوان Mathy Vanhoef در دانشگاه نیویورک در رابطه با حملات Frag می‌گوید: "یک مهاجم سایبری با حضور در محدوده رادیویی دستگاه وای.فای قربانی می‌تواند از این نقص‌های امنیتی جدید سوءاستفاده کند. البته تعداد کمی از دستگاه‌های وای.فای تنها نسبت به یک مورد از این مجموعه نقص‌های جدید آسیب‌پذیر هستند" [۲,۱].

بنابر اعلام محققان نقص‌های امنیتی جدید ناشی از اشتباهات برنامه‌نویسی زیاد در پیاده‌سازی استاندارد ۸۰۲,۱۱ به خصوص بخش مدیریت قطعه‌بندی[۴] و تجمیع قاب[۵]ها هستند. اشتباهاتی که با سوءاستفاده از آن‌ها علاوه بر جعل و شنود ترافیک، امکان تزریق بسته، اجرای حملات محروم‌سازی از سرویس[۶] و حتی هدایت قربانی برای استفاده از یک خدمت‌رسان DNS[۷] مخرب نیز ممکن است (در صورت تزریق بسته در نقطه دسترسی شبکه وای.فای امکان عبور از دیواره آتش[۸] نیز وجود دارد). در ویدیو موجود در پیوند زیر می‌توان یک سناریو از بهره‌گیری این آسیب‌پذیری را مشاهده کرد [۲,۱].

https://youtu.be/88YZ4061tYw

بر اساس اطلاعات اتحادیه وای.فای[۹]، یک بروزرسانی استاندارد در طی بازه زمانی ۹ ماهه در دسترس کاربران قرار خواهد گرفت. البته شرکت مایکروسافت برای برخی از این آسیب‌پذیری‌ها در وصله[۱۰] پنجشنبه ۲۱ می ۲۰۲۱ خود بروزرسانی منتشر کرده است. علاوه بر این، خبرهایی نیز از انتشار یک بروزرسانی برای هسته سیستم‌عامل لینوکس در هم وجود دارد. این اتحادیه همچنین اعلام کرده که تا کنون هیچ شواهدی مبنی بر سوءاستفاده مهاجمان سایبری از این آسیب‌پذیری‌ها گزارش نشده است [۲,۱].

منابع :

1. The Hacker News Website
   https://thehackernews.com/2021/05/nearly-all-wifi-devices-are-vulnerable.html
2. Therecord Website
   https://therecord.media/wifi-devices-going-back-to-1997-vulnerable-to-new-frag-attacks/

۱ FRgmentation and AGgregation

۲ Wired Equivalent Privacy

۳ Wifi protected Access

۴ مدیریت ترافیک در لایه دوم شبکه بر اساس مدل TCP/IP

۵ واحد بسته‌بندی ترافیک در لایه دوم شبکه بر اساس مدل TCP/IP

۶ تلاش برای خارج کردن ماشین و منابع شبکه از دسترس کاربران مجاز

۷ یک سیستم سلسله‌مراتبی نام‌گذاری برای کامپیوترها، سرویس‌ها، یا منابع دیگر است.

۸ فایروال نام عمومی برنامه‌هایی است که از دستیابی غیرمجاز به یک سیستم رایانه جلوگیری می‌کنند.

۹ انجمنی غیرانتفاعی , جهانی و صنعتی با بیش از ۵۵۰ شرکت عضو می باشد که در جهت ترویج رشد تکنولوژی WLAN تلاش می کنند

۱۰ مجموعه‌ای از تغییرات در یک برنامه کامپیوتری یا داده‌های پشتیبان آن که برای به روز رسانی، رفع یا بهبود طراحی شده است.

فصل سوم : نرم‌افزار

در این فصل دو خبر در رابطه با امنیت نرم‌افزارها مورد بررسی قرار گرفته است. موضوعاتی که در هر دو آن‌ها، گستردگی دستگاه‌های آسیب پذیر بسیار بالا بوده و کاربران زیادی را تحت تاثیر قرار می‌دهد. به عنوان مثال تنها در خبر دوم این فصل بیش از ۱۰۰ میلیون کاربر سیستم‌عامل اندروید در معرض خطر قرار گرفته‌اند.

فهرست مطالب

آسیب‌پذیری در ابزار مدیریت وابستگی کامپوزر[۱]

تاریخ: ۲۹/ آوریل / ۲۰۲۱

بررسی اجمالی :

تیم توسعه و نگهداری ابزار مدیریت وابستگی کامپوزر در زبان برنامه‌نویسی پی.اِچ.پی[۲] یک بروزرسانی امنیتی منتشر کرده‌اند. در این بروزرسانی یک نقص امنیتی رفع شده که به مهاجمان سایبری امکان ایجاد درب پشتی[۳] و اجرای دستورات دلخواه در یک برنامه پی.اِچ.پی را می‌داد [۲,۱]. لذا پیشنهاد می‌شود کاربران مربوطه هر چه سریعتر نسبت به اعمال بروزرسانی اقدام نمایند.

سیستم‌های آسیب‌پذیر	برنامه‌های کاربردی پی.اِچ.پی دارای ابزار مدیریت وابستگی کامپوزر
راه‌های نفوذ	سوءاستفاده از نقص تجزیه نادرست ورودی و ایجاد یک آدرس مخزن جعلی
هدف مهاجمان	اجرای کدهای غیرمجاز
شناسه آسیب‌پذیری	سی.وی.ای[۴] ۲۰۲۱-۲۹۴۷۲
شدت خطر	بالا با درجه شدت خطر ۸,۸ از ۱۰ در استاندارد سی.وی.اِس.اِس[۵]

توضیحات بیشتر:

کامپوزر یک ابزار مدیریت وابستگی در زبان برنامه‌نویسی پی.اِچ.پی بوده که امکان نصب آسان برخی پکیج‌های لازم در یک پروژه پی.اِچ.پی را فراهم می‌سازد. این ابزار همچنین امکان نصب اپلیکیشن‌های موجود در مخزن پکاگیست[۶] (مخزنی برای پکیج‌های پی.اِچ.پی عمومی قابل نصب توسط کامپوزر) را فراهم می‌سازد. در ۲۲ آوریل این مسئله امنیتی تحت شناسه سی.وی.ای ۲۰۲۱-۲۹۴۷۲ توسط محققان شرکت سونار.سورس[۷] کشف و گزارش گردید. ۱۲ ساعت پس از این موضوع فرآیند رفع و انتشار بروزرسانی توسط تیم توسعه و نگهداری کامپوزر صورت گرفت [۲,۱]. در این بروزرسانی نوعی سخت‌سازی[۸] برای جلوگیری از اجرای دستورات غیرمجاز در ماژول‌های HgDriver/HgDownloader و سایر درایوهای VCS صورت گرفته است [۲,۱].

---

[۱] کامپوزر(به انگلیسی: Composer) یک سامانه مدیریت بسته برای زبان برنامه‌نویسی پی.اِچ.پی است. که قالب استاندارد برای مدیریت وابستگی‌ها و کتابخانه‌ها را در این زبان فراهم می‌کند.

[۲] پی.اچ.پی (به انگلیسی: PHP) نوعی زبان اسکریپت‌نویسی همه منظوره و خاص برای توسعه برنامه‌های تحت وب

[۳] راهی که بتوان از طریق آن بدونِ اجازه به قسمت مشخصی از یک سامانه مانند رایانه، دیوار آتش، یا افزاره‌های دیگر دست پیدا کرد.

[۴] نوعی شناسه برای تشخیص و تقسیم‌بندی آسیب‌پذیری‌های رایانه‌ای

[۵] نوعی استاندارد برای کمی‌سازی شدت خطر در یک آسیب‌پذیری

[6] Packagist

[7] SonarSource

[۸] فرآیندی که طی آن عملیات نفوذ برای یک مهاجم سایبری سخت‌سازی می‌شود.

بر اساس اعلام محققان منشاء این آسیب‌پذیری مربوط به نحوه مدیریت بارگیری منابع از آدرس‌های یو.آر.اِل است. محققان به عنوان اثبات، با سوءاستفاده از یک نقص تجزیه نادرست ورودی[1] یک آدرس مخزن جعلی (دارای آدرس یو.آر.اِل) ایجاد کرده و به کمک گزینه alias در آن به اجرای دستورات مخرب (به انتخاب مهاجم سایبری) در سیستم قربانی پرداخته‌اند [۲,۱].

تیم توسعه و نگهداری کامپوزر اطمینان داده که بر اساس اطلاعات خود تا کنون هیچگونه بهره‌گیری از این آسیب‌پذیری صورت نگرفته است. این شرکت همچنین از کاربران خود خواست برای بارگیری منابع از افزونه‌های قابل اعتماد استفاده کنند [۲,۱].

منابع :

1. The Hacker News Website
   https://thehackernews.com/2021/04/a-new-php-composer-bug-could-enable.html
2. Thecybersecurity Website
   https://thecybersecurity.news/general-cyber-security-news/a-new-php-composer-bug-could-enable-widespread-supply-chain-attacks-8615/

[1] CWE-141: Improper Neutralization of Parameter/Argument Delimiters

افشای اطلاعات خصوصی بیش از صد میلیون کاربر اندروید

تاریخ: ۲۰/ مِی / ۲۰۲۱

بررسی اجمالی :

اخیرا اطلاعات مهم و خصوصی بیش از ۱۰۰ میلیون کاربر اندروید توسط ۲۳ برنامه کاربردی افشاء شده است. اطلاعاتی که منبع بسیار جذابی برای مهاجمان سایبری محسوب شده و می‌تواند زمینه‌ساز بسیاری از حملات این حوزه از جمله فیشینگ[۱] و جعل هویت[۲] باشد [۲,۱].

توضیحات بیشتر:

بنابر اطلاعات منتشر شده توسط محققان شرکت امنیت سایبری چک‌پوینت[۳] در ۲۳ برنامه کاربردی (موجود در گوگل‌پلی[۴]) به علت عدم رعایت مهم‌ترین تکنیک‌های رایج رایانش امن هنگام ارتباط با سرویس‌های ابری[۵] اطلاعات خصوصی بیش از ۱۰۰ میلیون کاربر اندروید افشاء شده است. در بعضی موارد حتی امکان دسترسی به منابع داخلی توسعه‌دهندگان مثل سیستم بروزرسانی هم وجود دارد. نام بعضی از این برنامه‌ها عبارتند از ifax، Screen recorder، logo maker [۲,۱].

محققان ریشه اصلی این نقص را تنظیمات اشتباه در پایگاه‌های داده بلادرنگ[۶]، فراخوانی اعلان‌ها[۷] و کلیدهای مورد استفاده در حافظه‌های ابری می‌دانند. امری که نتیجه آن افشای اطلاعاتی نظیر پست الکترونیکی، متن گفتگوها، نسخه های پشتیبان، کلمات عبور، تصاویر، موقعیت ها و حتی تاریخچه مرورگر است [۱].

دسترسی به کلیدهای توسعه‌دهندگان برای ارسال اعلان‌ها (تعبیه‌شده در منابع مربوطه) نیز در این برنامه‌ها ممکن است. امری که می‌تواند فرآیند ارسال اعلان برای تمام کاربران را در اختیار مهاجمان قرار داده و حتی امکان هدایت قربانی به وبگاه‌های فیشینگ را نیز ممکن سازد. به عبارت دیگر افشای اطلاعات مذکور را می‌توان نقطه‌ای برای اجرای حملات پیشرفته‌تر تلقی نمود [۲,۱].

تا کنون تعداد کمی از ۲۳ برنامه‌های مربوطه نسبت به تغییر تنظیمات برای مقابله با افشای اطلاعات اقدام کرده‌اند. در واقع بخش عمده آن‌ها همچنان در برابر تهدیدات مذکور در خطر بوده و هیچگونه اطلاع رسانی مناسبی نیز صورت نگرفته است. در شکل شماره ۱ می‌توان یک نمونه از این اطلاعات افشاء شده را مشاهده نمود [۲,۱].

---

[۱] به تلاش برای به دست آوردن اطلاعاتی مانند نام کاربری، گذرواژه، اطلاعات بانکی و مانند آن از طریق جعل یک وبگاه، آدرس ایمیل و شبیه این موارد گفته می‌شود.

[۲] موقعیتی است که در آن یک شخص یا برنامه با جعل داده، به صورت موفق به جای دیگری با هدف سودجویی معرفی می‌شود.

[۳] CheckPoint

[۴] یک سرویس پخش دیجیتال محتوای چندرسانه‌ای از شرکت گوگل بوده که شامل یک فروشگاه آنلاین نیز در همین رابطه می‌باشد.

[۵] مدل رایانشی بر پایه شبکه‌های رایانه‌ای مانند اینترنت است که الگویی تازه برای عرضه، مصرف و تحویل خدمات رایانشی با به‌کارگیری شبکه ارائه می‌کند.

[۶] Real-Time

[۷] Notification

Email, Password, Username and ID of a user on Logo Maker

Credentials to Push Notification services embedded into an application

شکل ۱ : دسترسی به اطلاعات کاربران در کد منبع یکی از برنامه‌های کاربردی مذکور [۱]

آویران هازوم[۱] مدیر تحقیقات موبایل شرکت چک‌پوینت نیز در رابطه با این خبر می‌گوید : "کاربران برنامه‌های مذکور در معرض حملات بسیاری از جمله جعل هویت، سرقت شناسه، فیشینگ و دزدی سرویس قرار دارند" [۱] .

منابع :

1. The Hacker News Website
https://thehackernews.com/2021/05/these-23-android-apps-expose-over.html
2. Techspot Website
https://www.techspot.com/news/89762-researchers-found-23-android-apps-exposed-over-100.html

[۱] Aviran Hazum

آزمایشگاه تخصصی آپا، قزوین
دانشگاه بین المللی امام خمینی (ره)

ماهنامه تحلیلی رویداد های امنیتی

اردیبهشت ماه ۱۴۰۰

cert@eng.ikiu.ir

۰۲۸۳۳۹۰۱۱۱۹

قزوین، دانشگاه بین‌المللی امام خمینی،
دانشکده فنی و مهندسی

حوزه های مورد بررسی

فصل اول :
بدافزارها
فصل دوم :
شبکه و ارتباطات
فصل سوم :
نرم‌افزار