McAfee
Together is power.

گزارش و آمار فصلی از فعالیت

# بدافزارها و تهدیدات سایبری

دسامبر ۲۰۱۸

شبکه گستر
امنیت شما | وظیفه ما

# فهرست مطالب

# چکیده مدیریتی

در این گزارش نتایج بررسی‌های صورت پذیرفته توسط آزمایشگاه‌ها[۱] و بخش تحقیقات پیشرفته تهدیدات[۲] شرکت مک‌آفی در خصوص رخدادها و آمار بدافزارها در سه‌ماهه سوم ۲۰۱۸ ارائه شده است.

در حالی که بیش از یک سال از تعطیلی بازارهای هنسا و آلفابی در وب تاریک می‌گذرد اما اثرات آن همچنان در حال ایجاد تحولاتی چشمگیر در روند کسب‌وکار بازارها در این شبکه مخفی است. وب تاریک همواره جولانگاهی مناسب برای عرضه ابزارهای هک، به خدمت گرفتن نفوذگران و خرید و فروش داده‌های سرقت شده بوده است. در این گزارش ضمن مرور این تأثیرات، تحلیلگران مک‌آفی اصلی‌ترین موضوعات مورد بحث در تالارهای گفتگوی زیرزمینی نفوذگران را نیز به اشتراک گذاشته‌اند.

فروشگاه‌های موسوم به RDP از دیگر موضوعاتی است که در این گزارش به آن پرداخته شده است. بسترهای آنلاینی که در آنها دسترسی RDP به ماشین‌های هک شده در اقصا نقاط جهان به فروش رسانده می‌شود. عمده کاربرد دسترسی RDP به این ماشین‌ها برای تبهکاران سایبری، رمز ربایی، حملات باج‌افزاری و کلاهبرداری‌های بانکی است.

تعداد نمونه باج‌افزارهای جدید که برای دو دوره متوالی روندی نزولی داشته مجددا سیر صعودی به خود گرفته است. GandCrab یکی از فعال‌ترین باج‌افزارها در سه‌ماهه سوم ۲۰۱۸ گزارش شده است. ارائه این باج‌افزار در قالب خدمات "باج‌افزار به‌عنوان سرویس" موجب گردیده که توسط مهاجمان متعدد مورد استفاده قرار بگیرد.

همچون سه دوره قبل، در سه‌ماهه سوم ۲۰۱۸ نیز گسترش روزافزون بدافزارهای ویژه حملات موسوم به رمز ربایی را شاهد بوده‌ایم. تعداد این نوع بدافزارها در پایان سه‌ماهه سوم ۲۰۱۸ در مقایسه با یک سال قبل از آن ۴۰۰۰ درصد افزایش داشته است.

در بخش آمار، روند تغییر تعداد انواع تهدیدات سایبری طی دو سال گذشته ارائه شده است. شرکت مک‌آفی در هر روز ۴۹ میلیارد درخواست را پردازش و تحلیل می‌کند. در سه‌ماهه سوم سال ۲۰۱۸، در هر ثانیه، بیش از هشت بدافزار منحصربه‌فرد جدید به دست آزمایشگاه‌های این شرکت رسیده که ۵۰ درصد افزایش را نسبت به دوره قبل نشان می‌دهد. تعداد کل بدافزارها در این دوره نیز به حدود ۸۳۰ میلیون عدد رسیده است.

در این گزارش مکانیزم‌های به‌کار گرفته شده توسط مهاجمان در حوزه‌های مختلف بر مبنای مدل MITRE ATT&CK ارائه شده است. مک‌آفی در توسعه این مدل و پایگاه دانش آن با شرکت مایتر همکاری نزدیکی دارد.

[۱] McAfee Labs
[۲] McAfee Advanced Threat Research Team

# Cyber

## EVENTS

## چند رویداد سایبری

# تالارهای زیرزمینی تبهکاران سایبری

## بازارهای وب تاریک

وب تاریک[۱] همواره از اصلی‌ترین بسترهای خرید و فروش مواد مخدر، اسلحه و اجناس غیرقانونی بوده است. ضمن اینکه جولانگاهی مناسب برای عرضه ابزارهای هک، به خدمت گرفتن نفوذگران و خرید و فروش داده‌های سرقت شده است. این شبکه اگر چه مبتنی بر اینترنت است اما دسترسی به آن نیازمند بکارگیری ابزارهای خاصی همچون TOR است که هدف آنها مخفی و ناشناس نگاه داشتن هویت خدمات‌دهندگان و کاربران این شبکه گسترده است. بازارهای وب تاریک[۲] نیز به نوعی سایت‌های فروش آنلاینی هستند که فروشندگان، اقلام غیرقانونی خود را در آن عرضه و افرادی نیز اقدام به خرید از آنها می‌کنند. تغییرات ناشی از حذف بازارهای هنسا[۳] و آلفابی[۴] در وب تاریک، در سه‌ماهه سوم ۲۰۱۸ نیز همچنان قابل مشاهده بود. دستگیری گردانندگان این دو بازار در پی عملیاتی مشترک توسط نهادهای قانونی چندین کشور که منجر به تعطیلی آنها در سال ۲۰۱۷ شد موجب رونق بازارهای دیگر گردید. به‌نحوی که دو بازار وال استریت[۵] و دریم[۶] موفق به کسب جایگاه بزرگترین بازارهای وب تاریک شدند. بازار الیمپوس[۷] هم که به‌نظر می‌رسید روزبه‌روز استقبال از آن بیشتر می‌شود ناگهان در سه ماهه سوم ۲۰۱۸ ناپدید شد. برخی این احتمال را مطرح کرده‌اند که گردانندگان الیمپوس از این طریق دارایی‌های فروشندگان و مشتریان این بازار را سرقت کرده‌اند. بر طبق بررسی‌های صورت‌پذیرفته توسط مک‌آفی، چندین فروشنده مستقل بجای حضور در بازارهای بزرگ وب تاریک، خود اقدام به باز کردن بازار کرده‌اند. احتمالا با این امید که هم از گزند تحقیقات نهادهای قانونی – به دلیل محدود بودن دامنه فعالیت آنها – دور بمانند و هم با برقراری ارتباطی از سر اعتماد با مشتریان خود از نگرانی‌های ناشی از تعطیلی بازار بکاهند. موضوعی که سبب رونق کسب‌وکار طراحی و ساخت بازارهای مخفی شده است. برخی فروشندگان نیز با خروج از شبکه TOR به عرضه محصولات و خدمات غیرقانونی خود در بستر تلگرام روی آورده‌اند.

## تالارهای گفتگوی زیرزمینی

برخلاف بازارهای وب تاریک، تالارهای گفتگوی زیرزمینی نفوذگران[۸] تنها در حوزه‌ای خاص فعال بوده و تمرکز اصلی آنها بر روی موضوعات مرتبط با جرایم سایبری است. بر طبق بررسی‌های انجام شده توسط محققان مک‌آفی در سه‌ماهه سوم ۲۰۱۸ موارد اشاره شده در این بخش از اصلی‌ترین موضوعات مورد علاقه مهاجمان بوده است.

### اطلاعات اصالت‌سنجی سرقت / نشت شده

تبادل اطلاعات اصالت‌سنجی[۹] یکی از مباحث پرطرفدار در تالارهای گفتگوی نفوذگران است. تکرر رخدادهای نشت و سرقت داده‌ها نیز بر این محبوبیت می‌افزاید. حساب‌های کاربری معتبر ابزاری برای در اختیار گرفتن زندگی اشخاص و در کنترل داشتن نبض کسب‌وکار سازمانهاست. تبهکاران سایبری معمولا در پی اطلاعات اصالت‌سنجی ایمیل‌ها هستند؛ ایمیل‌ها علاوه بر آنکه گنجینه‌ای مملو از اطلاعات حساس و محرمانه تلقی می‌شوند در بسیاری از موارد خود حاوی ایمیل‌های موسوم به بازگردانی رمز عبور[۱۰] هستند که شناسایی آنها امکان دسترسی مهاجمان به سایر حساب‌های کاربری قربانی را نیز فراهم می‌سازد. استفاده چندباره از یک رمز عبور، بکارگیری یک رمز عبور در در سایت‌ها / سرویس‌های مختلف، عدم بهره‌گیری از مکانیزم تصدیق هویت دوعاملی[۱۱] و تغییر ندادن دوره‌ای رمز عبور اصلی‌ترین عوامل در پررونق نگاه داشتن این موضوع تلقی می‌شوند.

### آسیب‌پذیری‌های امنیتی

گفتگو در مورد ضعف‌ها و آسیب‌پذیری‌های امنیتی[۱۲] و بهره‌جوها[۱۳] از دیگر موضوعات پرطرفدار در تالارهای زیرزمینی تبهکاران سایبری است. در سه‌ماهه سوم ۲۰۱۸، بیشترین تمرکز در تالارهای گفتگو، بر روی بسته‌های بهره‌جوی RIG، Grandsoft و Fallout بوده است. در برخی تالارهای انگلیسی‌زبان و به مراتب کمتر فنی بحث‌هایی در خصوص آسیب‌پذیری‌های قدیمی و ابزارهای در ارتباط با آنها نظیر Trillium MultiSploit در جریان بوده است. موضوعی که از بهره‌گیری مهاجمان از ترکیب آسیب‌پذیری‌های قدیمی و جدید حکایت دارد. معروفیت این موضوعات هشداری برای سازمان‌هاست تا مدیریت آسیب‌پذیری را به‌جد مورد توجه قرار دهند.

۱ Dark Web
۲ Dark Web Markets
۳ Hansa
۴ AlphaBay
۵ Wall Street
۶ Dream
۷ Olympus
۸ Underground Hacker Forums
۹ Credential
۱۰ Reset Password Email
۱۱ Two-factor Authentication
۱۲ Vulnerability
۱۳ Exploit

### باج‌افزار به‌عنوان یک خدمت

یکی دیگر از موضوعات مورد علاقه مهاجمان در تالارهای گفتگوی زیرزمینی مهاجمان عرضه و استفاده از سرویس‌های موسوم به "باج‌افزار به‌عنوان سرویس"[۱] است. در این خدمات، صاحب باج‌افزار، فایل مخرب را به‌عنوان یک خدمت به متقاضی اجاره می‌دهد. متقاضی که ممکن است در برنامه‌نویسی تخصصی نداشته باشد تنها وظیفه انتشار باج‌افزار را برعهده دارد. در نهایت بخشی از مبلغ اخاذی‌شده از قربانی به نویسنده و بخشی دیگر به متقاضی می‌رسد.

### بدافزارهای اندرویدی

در سه‌ماهه سوم ۲۰۱۸، بدافزارهای دستگاه‌های همراه به ویژه بدافزارهای مبتنی بر سیستم عامل اندروید با محوریت مسائلی همچون شبکه‌های مخرب[۲]، کلاهبرداری‌های بانکی، باج‌افزارها و عبور از سد مکانیزم تصدیق هویت دو عاملی از موضوعات اصلی در تالارهای گفتگوی زیرزمینی بوده است.

### سایر بدافزارها و شبکه‌های مخرب

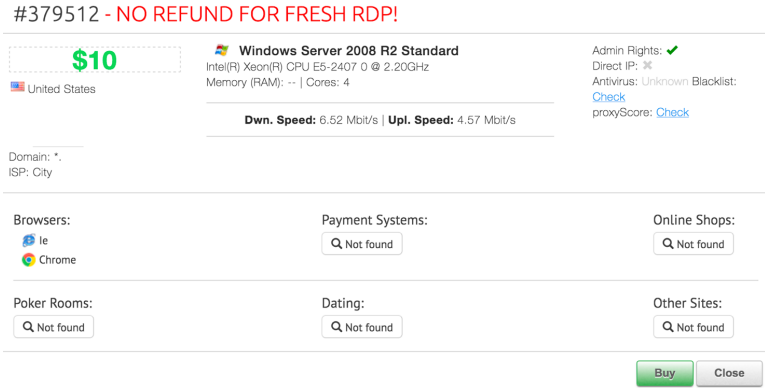
بدافزارها و شبکه‌های مخرب پای ثابت موضوعات پرطرفدار در تالارهای گفتگوی تبهکاران سایبری است. علاوه بر صحبت در خصوص بدافزارهای شناخته شده و شبکه‌های مخرب معروف، مک‌آفی گفتگوهای متعددی را در مورد شبکه‌های مخرب کوچک و ناشناخته، بدافزارهای استخراج ارز رمز و اسب‌های تروای دسترسی از راه دور[۳] رصد کرده است.

### حملات از کاراندازی سرویس

سرویس‌های موسوم به Booter/Stresser که با رابط‌های کاربری ساده اجرای حملات مخرب و پیشرفته "توزیع شده برای از کاراندازی سرویس"[۴] را فراهم می‌کنند در میان تبهکاران سایبری جوان و کم‌تجربه علاقمندان خاص خود را دارند. در سه‌ماهه سوم ۲۰۱۸، گفتگوها در مورد این تهدیدات عمدتا در تالارهای انگلیسی‌زبان و کمتر فنی در جریان بوده است.

## فروشگاه‌های RDP

در اوایل سه‌ماهه سوم، مک‌آفی گزارش مبسوطی در خصوص بسترهای آنلاینی منتشر کرد که در آنها دسترسی Remote Desktop Protocol - به اختصار RDP - به ماشین‌های هک شده در اقصا نقاط جهان به فروش رسانده می‌شود. عملکرد این ماشین‌ها از کامپیوترهای شخصی گرفته تا سیستم‌های درمانی و حتی سازمانی، متفاوت و متنوع گزارش شده است. عمده کاربرد دسترسی RDP به این ماشین‌ها برای تبهکاران سایبری، رمز ربایی، حملات باج‌افزاری و کلاهبرداری‌های بانکی است. تالارهای موسوم به فروشگاه‌های RDP نظیر بلک‌پس[۵] دسترسی کاملی را به ابزارهای مورد نیاز برای انجام هر نوع کلاهبرداری فراهم می‌کنند. علاوه بر دسترسی RDP، آنها اطلاعاتی همچون جزییات بانکی و حساب‌های آنلاین را نیز عرضه می‌کنند. اطلاعات دسترسی به سیستم‌های RDP با چندین حساب آنلاین همچنان خواهان دارد. تبهکاران می‌توانند با دسترسی به این سرورها و از طریق حساب‌های هک شده اقدام به خرید و فروش اقلام غیرقانونی کنند. در سال‌های اخیر هک‌های مبتنی بر RDP به یکی از دغدغه‌های اصلی سازمان‌ها تبدیل شده است. به‌خصوص آن که تعداد قابل توجهی از گردانندگان باج‌افزارهای پیشرفته همچون SamSam، BitPayment و GandCrab به‌طور هدفمند از طریق RDP اقدام به رخنه به سرورها – که در اکثر مواقع حاوی اطلاعات حساس و حیاتی سازمان هستند – می‌کنند.




فروش دسترسی به پودمان RDP یک سرور هک شده در یکی از تالارهای زیرزمینی گفتگوی مهاجمان

۱ Ransomware-as-a-Service
۲ Botnet
۳ Remote Access Trojan - RAT
۴ Distributed Denial-of-Service - DDoS
۵ Blackpass

# کاهش باج‌افزارها

در ماه‌های اخیر تعداد انتشار نمونه‌های منحصربه‌فرد از باج‌افزارها روند افزایشی خود را از دست داده است. دلیل این اتفاق را می‌توان در گرایش گردانندگان باج‌افزار به تهدید نوظهور دیگر یعنی بدافزارهای استخراج ارز رمز جستجو کرد. با این حال باج‌افزارها همچنان از تهدیدات فعال در حوزه بدافزارها تلقی می‌شوند.

GandCrab یکی از فعال‌ترین باج‌افزارها در سه‌ماهه سوم ۲۰۱۸ گزارش شده است. ارائه آن در قالب خدمات "باج‌افزار به‌عنوان سرویس" موجب گردیده که توسط مهاجمان متعدد مورد استفاده قرار بگیرد. از جمله تغییرات اعمال شده در این دوره بر روی GandCrab می‌توان به موارد زیر اشاره کرد:

- بکارگیری بسته بهره‌جوی Fallout
- سوءاستفاده از آسیب‌پذیری CVE-2018-8440
- الصاق پسوندی پنج‌نویسه‌ای به فایل‌های رمزگذاری‌شده
- مجهز شدن به توانایی متوقف کردن پروسه‌های Word، Excel، SQL Server، Oracle، PowerPoint، Outlook و ...
- افزوده شدن سوریه به فهرست کشورهایی که باج‌افزار سیستم‌های شهروندان آنها را مورد دست‌درازی قرار نمی‌دهد.

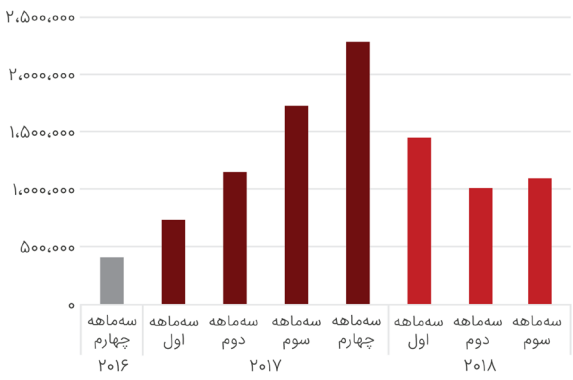
یکی دیگر از تغییرات قابل توجه این باج‌افزار در دوره مذکور، افزایش مبلغ اخاذی‌شده توسط آن است که در نسخه ۵ به میانگین ۲/۴ هزار دلار رسیده است.

شباهت‌های نسخه ۵ با نسخه‌های قبلی را هم می‌توان در موارد زیر خلاصه کرد:

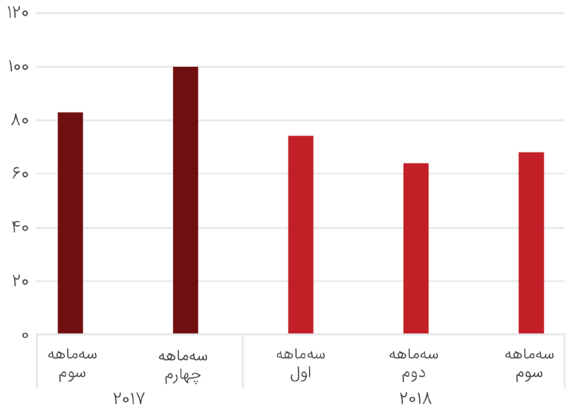
- ارسال اطلاعاتی در خصوص سیستم قربانی به نشانی‌های درج شده در کد باج‌افزار
- عدم تغییر سایت پرداخت که باج همچنان در وب تاریک در مسیر hxxp://gandcrabmfe6mnef[.]onion قابل دسترس است.
- استفاده از کلید jopochlen که در کد باج‌افزار تزریق شده و برای رمزگذاری اطلاعات قربانی به همراه الگوریتم RC4 به‌کار گرفته می‌شود.

لازم به ذکر است که در اوایل آبان ماه شرکت ضدویروس بیت‌دیفندر ابزار رایگانی را عرضه کرد که امکان بازگرداندن فایل‌های رمزگذاری شده توسط اکثر نسخه‌های باج‌افزار GandCrab را فراهم می‌کند.

**باج‌افزارهای جدید**




**خانواده باج‌افزارهای جدید**



دیگر باج‌افزار فعال در این دوره، Scarab است که شش نسخه از آن به همراه چندین به‌روزرسانی با پسوندها و اطلاعیه‌های باج‌گیری جدید منتشر شد. به‌نظر نمی‌رسد که این باج‌افزار تنها صنف یا منطقه‌ای خاص را مورد هدف قرار داده باشد. نسخه‌های جدید از Scarab که در سه‌ماهه سوم دستگاه کاربران را مورد حمله قرار دادند به‌شرح زیر است:

- Scarab-Omerta
- Scarab-Bin
- Scarab-Recovery
- Scarab-Turkish
- Scarab-Barracuda
- Scarab-CyberGod

نسخه‌های به‌روز شده این باج‌افزار در سه‌ماهه سوم نیز شامل موارد زیر می‌باشد:

- Scarab-Please
- Scarab-Bitcoin
- Scarab-Crypt000
- Scarab-DiskDoctor
- Scarab-Bomber

| اجرا | ماندگاری | ترفیع سطح دسترسی | گریز از سد سیستم دفاعی | دسترسی به اطلاعات اصالت‌سنجی | جمع‌آوری اطلاعات |
|---|---|---|---|---|---|
| از طریق WMI[1] | به‌عنوان Startup Item در سیستم عامل macOS[2] | اجرا در حافظه تخصیص داده شده به پروسه‌ای دیگر[6] | اجرا در حافظه تخصیص داده شده به پروسه‌ای دیگر | شنود فراخوانی‌های ارسالی به توابع API و دست‌درازی به آنها | جستجوی فایل‌ها و پوشه‌ها[12] |
| | شنود فراخوانی‌های ارسالی به توابع API و دست‌درازی به آنها[3] | فرمان زمانبندی‌شده | عبور از سد UAC | ضبط داده‌های وارد شده توسط کاربر[11] | |
| | افزودن کلید Run در محضرخانه و یا بهره‌جویی از پوشه Startup[4] | عبور از سد UAC[7] | غیرفعال کردن ابزارهای امنیتی[9] | | |
| | فرمان زمانبندی‌شده[5] | ارسال پروسه جعلی در زمان فراخوانی فایل یک پروسه مجاز[8] | حذف سوابق[10] | | |

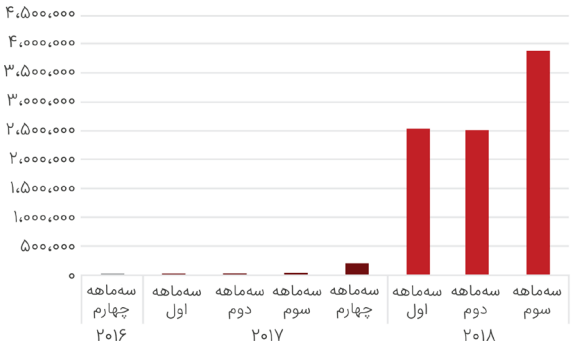
▲
مکانیزم‌های به‌کار گرفته شده توسط مهاجمان در حوزه باج‌افزارها در سه‌ماهه سوم ۲۰۱۸ بر مبنای مدل MITRE ATT&CK؛
پس‌زمینه تیره‌تر نشانه استفاده بیشتر از مکانیزم.

[1] Windows Management Instrumentation | https://attack.mitre.org/techniques/T1047
[2] Startup Items | https://attack.mitre.org/techniques/T1165
[3] Hooking | https://attack.mitre.org/techniques/T1179
[4] Registry Run Keys / Startup Folder | https://attack.mitre.org/techniques/T1060
[5] Scheduled Task | https://attack.mitre.org/techniques/T1053
[6] Process Injection | https://attack.mitre.org/techniques/T1055
[7] Bypass User Account Control | https://attack.mitre.org/techniques/T1088
[8] DLL Search Order Hijacking | https://attack.mitre.org/techniques/T1038
[9] Disabling Security Tools | https://attack.mitre.org/techniques/T1089
[10] File Deletion | https://attack.mitre.org/techniques/T1107
[11] Input Capture | https://attack.mitre.org/techniques/T1056
[12] File and Directory Discovery | https://attack.mitre.org/techniques/T1083

# ادامه روند روبه‌رشد استخراج ارز رمز

در یک سال اخیر استخراج ارز رمز از طریق بدافزار یکی از مباحث اصلی در حوزه امنیت فناوری اطلاعات بوده است. تعداد این نوع بدافزارها در پایان سه‌ماهه سوم ۲۰۱۸ در مقایسه با یک سال قبل از آن ۴۰۰۰ درصد افزایش داشته است. یکی از نمونه‌های قابل توجه در دوره مذکور، بدافزاری با نام OSX.Dummy است که در کانال‌های اسلک، تلگرام و دیس‌کورد با موضوعات مرتبط با استخراج ارز رمز توزیع می‌شده است. در پیام ارسالی توسط نویسنده بدافزار OSX.Dummy در این کانال‌ها تظاهر می‌شده که با دریافت و اجرای نرم‌افزار، مشکلات مربوط به استخراج ارز رمز حل می‌شود. نرم‌افزار مورد اشاره مهاجم، برنامه‌ای جعلی است که با تک‌خط کد در Bash اجرا می‌شود. در حقیقت مهاجم بجای بکارگیری تکنیک‌های پیشرفته‌ای همچون بهره‌جویی از آسیب‌پذیری‌های امنیتی قربانیان را وادار می‌ساخته تا با دست خود دستگاهشان را آلوده کنند. پس از اجرا، OSX.Dummy مهاجم را قادر به اجرای امور مخرب از جمله استخراج ارز رمز به نفع خود با استفاده از منابع دستگاه آلوده شده می‌کرده است. استخراج‌کنندگان ارز رمز از هر موقعیتی برای سود جستن از منابع دستگاه کاربران بهره می‌گیرند. در یک نمونه، انباره‌های غیررسمی فایل Kodi که یک رسانه‌ای[۱] کد باز[۲] است به‌نحوی مورد دست‌درازی قرار گرفت که با نصب آن دستگاه آلوده به یک بدافزار استخراج ارز رمز می‌شود. یا در کارزاری دیگر، مهاجمان با سوءاستفاده از ضعف امنیتی CVE-2018-14847 به روترهای آسیب‌پذیر میکروتیک رخنه کرده و آنها را تبدیل به ابزاری برای استخراج ارز رمز تبدیل کردند. اهمیت ایمن و مقاوم ساختن تجهیزات موسوم به اینترنت اشیا[۳] بیش از هر زمانی دیگر پررنگ شده است. اگر چه در نگاه اول این تجهیزات فاقد منابع قدرتمند برای اموری همچون استخراج ارز رمز هستند اما در مقیاس بالا و با توجه به پیکربندی امنیتی ناصحیح بسیاری از آنها عملا با لشکری از دستگاه‌های آسیب‌پذیر مواجه هستیم که می‌توانند در مجموع عملکردی بالاتر و مناسب‌تر در مقایسه با حتی سرورهای قدرتمند برای مهاجمان فراهم کنند.

**بدافزارهای جدید استخراج‌کننده ارز رمز**




منبع: McAfee Labs Threats Report

| اجرا | ماندگاری | ترفیع سطح دسترسی | گریز از سد سیستم دفاعی | جمع‌آوری اطلاعات | ارتباطات با سرور فرماندهی |
|---|---|---|---|---|---|
| اجرا از طریق NTDLL.dll[۴] | افزودن کلید Run در محضرخانه و یا بهره‌جویی از پوشه Startup | عبور از سد UAC | عبور از سد UAC | کندوکاو در محضرخانه[۷] | عبور از سد UAC |
| اجرا از طریق فرامین cron، at و launchd[۵] | شنود فراخوانی‌های ارسالی به توابع API و دست‌درازی به آنها | شنود فراخوانی‌های ارسالی به توابع API و دست‌درازی به آنها | | | استفاده از درگاه‌های غیرمتداول[۸] |
| فرمان زمانبندی‌شده | | اجرا در حافظه تخصیص داده شده به پروسه‌ای دیگر | | | |
| بهره‌گیری از نرم‌افزار ثالث[۶] | | فرمان زمانبندی‌شده | | | |
| | | به‌عنوان Startup Item در سیستم عامل macOS | | | |

▲ مکانیزم‌های به‌کار گرفته شده توسط مهاجمان در حوزه استخراج ارز رمز در سه‌ماهه سوم ۲۰۱۸ بر مبنای مدل MITRE ATT&CK؛ پس‌زمینه تیره‌تر نشانه استفاده بیشتر از مکانیزم.

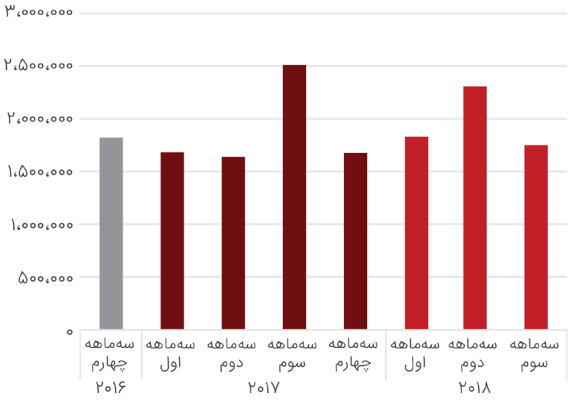
۱ Multimedia Player
۲ Open Source
۳ Internet of Things - IoT
۴ Execution through Module Load | https://attack.mitre.org/techniques/T1129
۵ Local Job Scheduling | https://attack.mitre.org/techniques/T1168
۶ Third-party Software | https://attack.mitre.org/techniques/T1072
۷ Query Registry | https://attack.mitre.org/techniques/T1012
۸ Uncommonly Used Port | https://attack.mitre.org/techniques/T1065

# افزایش تهدیدات موبایلی با برنامک‌های جعلی

بطور کلی، تعداد بدافزارهای جدید موبایلی در سه‌ماهه سوم ۲۰۱۸ حدود ۲۴ درصد کاهش داشته است؛ در همین دوره، مشتریان موبایلی مک‌آفی نیز ۳۶ درصد آلودگی کمتری را به این شرکت گزارش کرده‌اند. علیرغم این روند نزولی، در دوره مذکور تعدادی بدافزار موبایلی غیرمعمول و کاملا هدفمند شناسایی شد. از جمله می‌توان به نمونه‌ای اشاره کرد که مهاجمان آن نیروهای نظامی رژیم صهیونیستی را از طریق برنامک موسوم به زوج‌یابی مورد هدف قرار داده بودند. با نصب برنامک مذکور بدون اطلاع کاربر تماس‌ها ضبط و دوربین دستگاه اقدام به عکسبرداری می‌کند. در ادامه در بازه‌های زمانی از قبل تعیین شده، اطلاعات ضبط شده به همراه داده‌هایی همچون موقعیت دستگاه و فهرست تماس‌ها به مهاجمان ارسال می‌شود. همچنین در سه‌ماهه سوم ۲۰۱۸، مک‌آفی تهدیدی با نام Android/TimpDoor را شناسایی کرد که حداقل ۵ هزار دستگاه را به خود آلوده کرده است. مهاجمان Android/TimpDoor از طریق پیامک کاربر را تشویق به دریافت و نصب یک برنامک جعلی پیام‌رسان صوتی می‌کنند. در صورت نصب، برنامک جعلی مذکور با راه‌اندازی یک پراکسی Socks کلیه ترافیک شبکه‌ای را از یک سرور ثالث از طریق یک ارتباط رمزگذاری شده و یک تونل امن، انتقال داده و عملا امکان اتصال مهاجمان به شبکه داخلی و عبور از سد مکانیزم‌های امنیتی نظیر دیواره‌های آتش را فراهم می‌کند.

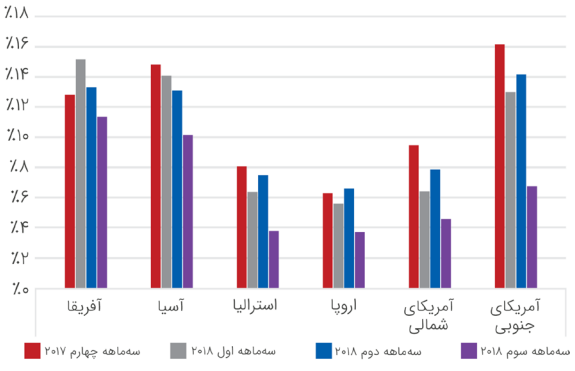
ضمن اینکه بهره‌جویی از موبایل آلوده برای ارسال ایمیل‌های هرزنامه[1] و فیشینگ[2] و اجرای حملات "توزیع شده برای از کاراندازی سرویس" ممکن می‌گردد. برنامک مجهز به مکانیزمی است که ارتباط را برقرار نگاه داشته و بطور پیوسته اطلاعات در خصوص دستگاه را به مهاجمان ارسال می‌کند. اما آنچه کاربر با آن مواجه می‌شود یک برنامک مدیریت پیام‌های صوتی به ظاهر معتبر است؛ اگر چه دگمه‌ها و توابع آن تماما جعلی هستند.

**بدافزارهای جدید دستگاه‌های همراه**



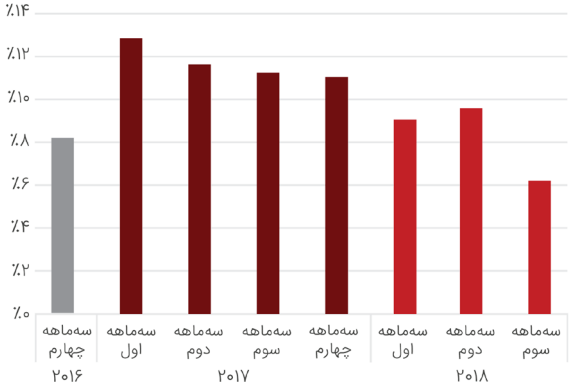

منبع: McAfee Labs Threats Report

**نرخ آلودگی به بدافزارهای دستگاه‌های همراه به تفکیک منطقه**




منبع: McAfee Labs Threats Report

**نرخ آلودگی جهانی به بدافزارهای دستگاه‌های همراه**




منبع: McAfee Labs Threats Report

[1] Spam
[2] Phishing

| رخنه | ماندگاری | گریز از سد سیستم دفاعی | شناسایی | جمع‌آوری اطلاعات | انتقال اطلاعات | ارتباطات با سرور فرماندهی |
|---|---|---|---|---|---|---|
| ارسال ایمیل فیشینگ هدفمند با پیوست مخرب[1] | بهره‌گیری از Dylib در سیستم عامل macOS / OS X[4] | دست‌درازی به توکن دسترسی[5] | شناسایی نام‌های کاربری محلی و تحت دامنه[7] | شنود گفتگوهای کاربر از طریق روش‌هایی همچون فعالسازی میکروفون[13] | ارسال خودکار[19] | استفاده از درگاه‌های غیرمتداول |
| ارسال ایمیل فیشینگ هدفمند حاوی لینک مخرب[2] | | امضای کد[6] | شناسایی برنامه‌های اجراشده[8] | جمع‌آوری خودکار اطلاعات با استفاده از ابزارهایی نظیر اسکریپت‌های حساس به کلمات خاص[14] | فشرده‌سازی[20] | کپی دستی فایل به‌صورت از راه دور[28] |
| ارسال ایمیل فیشینگ هدفمند از طریق فرد / سازمان / سرویس ثالث[3] | | | شناسایی میان‌برهای اینترنتی در مرورگر کاربر[9] | استخراج داده‌های ذخیره شده در بُریده‌دان[16] | رمزگذاری داده‌ها[21] | استفاده از پودمان‌های رایج نظیر HTTP، HTTPS، SMTP یا DNS[29] |
| | | | جستجوی فایل‌ها و پوشه‌ها | استخراج از انباره‌های اطلاعات[15] | انتقال داده‌ها در حجم‌هایی مشخص[22] | |
| | | | شناسایی کاربر اصلی / فعال در سیستم[10] | استخراج داده‌ها از سیستم به‌صورت محلی[16] | ارسال از طریق پودمان‌های جایگزین[23] | |
| | | | شناسایی سرویس‌ها[11] | جمع‌آوری اطلاعات مرتبط با ایمیل از طریق پویش فایل‌هایی همچون PST و OST[17] | ارسال از طریق سرور فرماندهی[24] | |
| | | | | ضبط داده‌های واردشده توسط کاربر | انتقال در بستر رسانه‌های شبکه‌ای[25] | |
| | | | | | انتقال در بستر رسانه‌های فیزیکی[26] | |
| | | | | تصویربرداری از صفحه کار کاربر[18] | انتقال زمانبندی‌شده[27] | |

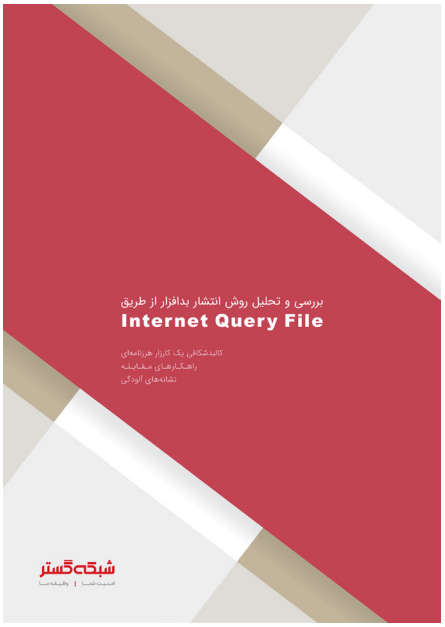
▲

مکانیزم‌های به‌کار گرفته شده توسط مهاجمان در حوزه برنامک‌های مخرب در سه‌ماهه سوم ۲۰۱۸ بر مبنای مدل MITRE ATT&CK؛
پس‌زمینه تیره‌تر نشانه استفاده بیشتر از مکانیزم.

۱ Spearphishing Attachment | https://attack.mitre.org/techniques/T1193
۲ Spearphishing Link | https://attack.mitre.org/techniques/T1192
۳ Spearphishing via Service | https://attack.mitre.org/techniques/T1194
٤ Dylib Hijacking | https://attack.mitre.org/techniques/T1157
٥ Access Token Manipulation | https://attack.mitre.org/techniques/T1134
٦ Code Signing | https://attack.mitre.org/techniques/T1116
۷ Account Discovery | https://attack.mitre.org/techniques/T1087
۸ Application Window Discovery | https://attack.mitre.org/techniques/T1010
۹ Browser Bookmark Discovery | https://attack.mitre.org/techniques/T1217
۱۰ System Owner/User Discovery | https://attack.mitre.org/techniques/T1033
۱۱ System Service Discovery | https://attack.mitre.org/techniques/T1007
۱۲ Audio Capture | https://attack.mitre.org/techniques/T1123
۱۳ Automated Collection | https://attack.mitre.org/techniques/T1119
۱٤ Clipboard Data | https://attack.mitre.org/techniques/T1115
۱٥ Data from Information Repositories | https://attack.mitre.org/techniques/T1213
۱٦ Data from Local System | https://attack.mitre.org/techniques/T1005
۱۷ Email Collection | https://attack.mitre.org/techniques/T1114
۱۸ Screen Capture | https://attack.mitre.org/techniques/T1113
۱۹ Automated Exfiltration | https://attack.mitre.org/techniques/T1020
۲۰ Data Compressed | https://attack.mitre.org/techniques/T1002
۲۱ Data Encrypted | https://attack.mitre.org/techniques/T1022
۲۲ Data Transfer Size Limits | https://attack.mitre.org/techniques/T1030
۲۳ Exfiltration Over Alternative Protocol | https://attack.mitre.org/techniques/T1048
۲٤ Exfiltration Over Command and Control Channel | https://attack.mitre.org/techniques/T1041
۲٥ Exfiltration Over Other Network Medium | https://attack.mitre.org/techniques/T1011
۲٦ Exfiltration Over Physical Medium | https://attack.mitre.org/techniques/T1052
۲۷ Scheduled Transfer | https://attack.mitre.org/techniques/T1029
۲۸ Remote File Copy | https://attack.mitre.org/techniques/T1105
۲۹ Standard Application Layer Protocol | https://attack.mitre.org/techniques/T1071

# گرایش مهاجمان به فایل‌های غیرمتداول

در سه‌ماهه سوم ۲۰۱۸ شاهد افزایش استفاده مهاجمان از فایل‌های غیرمتداول در کارزارهای هرزنامه‌ای بودیم. هدف از بکارگیری این فایل‌ها، عبور از سد سیستم‌های حفاظتی ایمیلی است که وظیفه آنها تجزیه و تحلیل فایل‌های پیوست پراستفاده‌ای همچون فایل‌های فشرده شده، اسکریپت‌ها و نمونه‌هایی از این دست است که مهاجمان به کرات از آنها برای انتقال بدافزار استفاده می‌کنند. در دوره مذکور، هرزنامه‌هایی با پیوست فایل IQY[1] شناسایی شد که اجرای پیوست آنها منجر به آلوده‌سازی دستگاه می‌شد. در این کارزارها با بهره‌گیری از تکنیک‌های مهندسی اجتماعی[2] و با موضوعات جذابی همچون "Photo sent"، "Payment" و "Please confirm" کاربران متقاعد به باز کردن پیوست هرزنامه می‌شدند. عناوین مذکور در نیم‌میلیون هرزنامه ارسالی در این دوره نقش داشته‌اند.




در اتاق خبر
شبکه گستر بخوانید...

# اسب‌های تروای بانکی با قابلیت‌های مخرب‌تر

در سال‌های اخیر موسسات مالی تلاش فراوانی برای حفاظت هر چه بیشتر از حساب‌های آنلاین کاربران خود به‌عمل آورده‌اند. یکی از این اقدامات بکارگیری مکانیزم تصدیق هویت دو عاملی در زمان ورود آنلاین به حساب بانکی و در حین اجرای اموری نظیر انتقال وجه به حساب است. در سه‌ماهه سوم ۲۰۱۸، مک‌آفی بدافزارهای بانکی معروفی همچون Zeus Panda را شناسایی کرد که در نسخه‌های جدید خود با استفاده از روش "تزریق وبی"[3] موفق به دور زدن این مکانیزم تصدیق هویت شده بودند. همچنین در سال ۲۰۱۸ برخی بدافزارهای شناخته‌شده با تغییراتی جزیی به‌روز شدند. برای مثال، گونه جدیدی از اسب تروای بانکی Kronos که نخستین نسخه از آن بیش از چهار سال قبل شناسایی شده بود تحت نام Osiris به فروش رسانده شد. برخی مهاجمان نیز در کارزاری هرزنامه‌ای کاربران آلمانی را هدف این بدافزار مخرب قرار دادند. پیوست این هرزنامه‌ها، فایلی Word بود که ماکروی مخرب درون آن در صورت اجرا اقدام به دریافت و اجرای کد مخرب می‌کرد. همچنین در برخی حملات Kronos در سه‌ماهه سوم ۲۰۱۸، بسته بهره‌جوی RIG که تا پیش از آن در انتشار Zeus Panda نقش داشت مورد استفاده قرار گرفت.

[1] Internet Query File
[2] Social Engineering
[3] Web Inject

| اجـرا | ماندگاری | گریز از سد سیستم دفاعی | دسترسی به اطلاعات اصالت‌سنجی | شناسایی | گسترده کردن دامنه حمله | جمع‌آوری اطلاعات | انتقال اطلاعات | ارتباطات با سرور فرماندهی |
|---|---|---|---|---|---|---|---|---|
| بهره‌جویی از ضعف‌های امنیتی[۱] | دست‌درازی به بخش MBR / VBR[۳] | امضای کد | ارسال پروسه جعلی در زمان فراخوانی فایل یک پروسه مجاز | شناسایی برنامه‌های اجرا شده | بهره‌گیری از فناوری DCOM در سیستم عامل Windows[۱۶] | استخراج داده‌های ذخیره‌شده در بُریده‌دان | فشرده‌سازی | کدگذاری داده[۱۹] |
| اجرا از طریق پروسه معتبر PowerShell[۲] | افزونه / ماژول در سطح هسته سیستم عامل[۴] | دست‌درازی به داده‌های Active Directory[۷] | ضبط داده‌های واردشده توسط کاربر | جستجوی فایل‌ها و پوشه‌ها | اصالت‌سنجی با استفاده از درهم‌ساز رمز عبور[۱۷] | جمع‌آوری اطلاعات مرتبط با ایمیل از طریق پویش فایل‌هایی همچون PST و OST | استفاده از پودمان‌های غیرمتداول | انتقال از طریق پودمان‌های غیررایج |
| اجرا از طریق WMI | بکارگیری فرامین cron، at و launchd | حذف سوابق | | پویش از راه دور سرویس‌های اجرا شده بر روی دستگاه هدف[۱۰] | به‌کارگیری پودمان RDP[۱۸] | | | |
| | اجرا در زمان باز شدن برنامه‌های مجموعه نرم‌افزاری Office[۵] | دست‌درازی به محضرخانه[۸] | | شناسایی تجهیزات جانبی متصل به دستگاه[۱۱] | | | | |
| | افزودن کلید Run در محضرخانه و یا بهره‌جویی از پوشه Startup | اجرا در حافظه تخصیص داده شده به پروسه‌ای دیگر | | شناسایی پروسه‌های اجرا شده[۱۲] | | | | |
| | دست‌درازی به محضرخانه با هدف جایگزینی سرویسی معتبر با پروسه‌ای مخرب[۶] | | | کندوکاو در محضرخانه | | | | |
| | | فشرده‌سازی یا رمزگذاری فایل مخرب[۹] | | شناسایی محصولات امنیتی[۱۳] | | | | |
| | | | | جمع‌آوری اطلاعات در خصوص سیستم[۱۴] | | | | |
| | | | | استخراج ساعت، تاریخ و منطقه زمانی[۱۵] | | | | |

▲
مکانیزم‌های به‌کار گرفته شده توسط مهاجمان در حوزه بدافزارهای بانکی در سه‌ماهه سوم ۲۰۱۸ بر مبنای مدل MITRE ATT&CK؛
پس‌زمینه تیره‌تر نشانه استفاده بیشتر از مکانیزم.

۱ Exploitation for Client Execution | https://attack.mitre.org/techniques/T1203
۲ PowerShell | https://attack.mitre.org/techniques/T1086
۳ Bootkit | https://attack.mitre.org/techniques/T1067
۴ Kernel Modules and Extensions | https://attack.mitre.org/techniques/T1215
۵ Office Application Startup | https://attack.mitre.org/techniques/T1137
۶ Service Registry Permissions Weakness | https://attack.mitre.org/techniques/T1058
۷ DCShadow | https://attack.mitre.org/techniques/T1207
۸ Modify Registry | https://attack.mitre.org/techniques/T1112
۹ Software Packing | https://attack.mitre.org/techniques/T1045
۱۰ Network Service Scanning | https://attack.mitre.org/techniques/T1046
۱۱ Peripheral Device Discovery | https://attack.mitre.org/techniques/T1120
۱۲ Process Discovery | https://attack.mitre.org/techniques/T1057
۱۳ Security Software Discovery | https://attack.mitre.org/techniques/T1063
۱۴ System Information Discovery | https://attack.mitre.org/techniques/T1082
۱۵ System Time Discovery | https://attack.mitre.org/techniques/T1124
۱۶ Distributed Component Object Model | https://attack.mitre.org/techniques/T1175
۱۷ Pass the Hash | https://attack.mitre.org/techniques/T1075
۱۸ Remote Desktop Protocol | https://attack.mitre.org/techniques/T1076
۱۹ Data Encoding | https://attack.mitre.org/techniques/T1132

# تغییر و تحول در بسته‌های بهره‌جو

بسته‌های بهره‌جو ابزاری برای انتقال بدافزار در بسیاری از حملات سایبری هستند. بسیاری تا زمانی که بساط گردانندگان آنها توسط نهادهای قانونی جمع نشود برای سال‌ها فعال می‌مانند. در سه‌ماهه سوم ۲۰۱۸ دو بسته بهره‌جوی جدید Fallout و Underminer ظهور کردند. هر دو بسته بهره‌جوی مذکور از آسیب‌پذیری‌های زیر سوءاستفاده می‌کنند.

- CVE-2018-4878، ضعفی امنیتی در نرم‌افزار Flash Player که امکان اجرای کد به‌صورت از راه دور را برای مهاجم فراهم می‌کند. نسخه ۲۸٫۰٫۰٫۱۳۷ و نسخه‌های پیش از آن در Flash Player از این آسیب‌پذیری تأثیر می‌پذیرند.
- CVE-2018-8174، ضعفی امنیتی در بخش مدیریت‌کننده کدهای VBScript است که امکان اجرای کد به‌صورت از راه دور را برای مهاجم فراهم می‌کند. این آسیب پذیری در ۱۸ اردیبهشت ماه در مجموعه اصلاحیه‌های ماه میلادی می مایکروسافت ترمیم شد.

از بسته بهره جوی Fallout در چندین حمله سایبری از جمله در باج‌افزار GandCrab استفاده شد. همچنین به‌نظر می‌رسد که دامنه فعالیت بسته بهره‌جو Underminer در سه‌ماهه سوم ۲۰۱۸ تنها محدود به منطقه آسیا-اقیانوسیه بوده.

| رخنه | اجرا | ترفیع سطح دسترسی | گریز از سد سیستم دفاعی |
|---|---|---|---|
| آلوده‌سازی دستگاه در زمان مراجعه کاربر به صفحه اینترنتی تحت کنترل مهاجم[1] | بهره‌جویی از ضعف‌های امنیتی | بهره‌جویی از آسیب‌پذیری‌های موسوم به ترفیع امتیازی[3] | عبور از سد UAC |
| بهره‌جویی از آسیب‌پذیری سیستم‌های قابل دسترس در اینترنت[2] | اسکریپت‌نویسی | | بهره‌جویی از آسیب‌پذیری‌های محصول امنیتی به‌کار گرفته شده توسط قربانی[4] |

▲
مکانیزم‌های به‌کار گرفته شده توسط مهاجمان در حوزه بسته‌های بهره‌جو در سه‌ماهه سوم ۲۰۱۸ بر مبنای مدل MITRE ATT&CK؛
پس‌زمینه تیره‌تر نشانه استفاده بیشتر از مکانیزم.

در سه‌ماهه سوم ۲۰۱۸ از چند آسیب‌پذیری به‌طور جداگانه در کارزارهای بدافزاری استفاده شد.

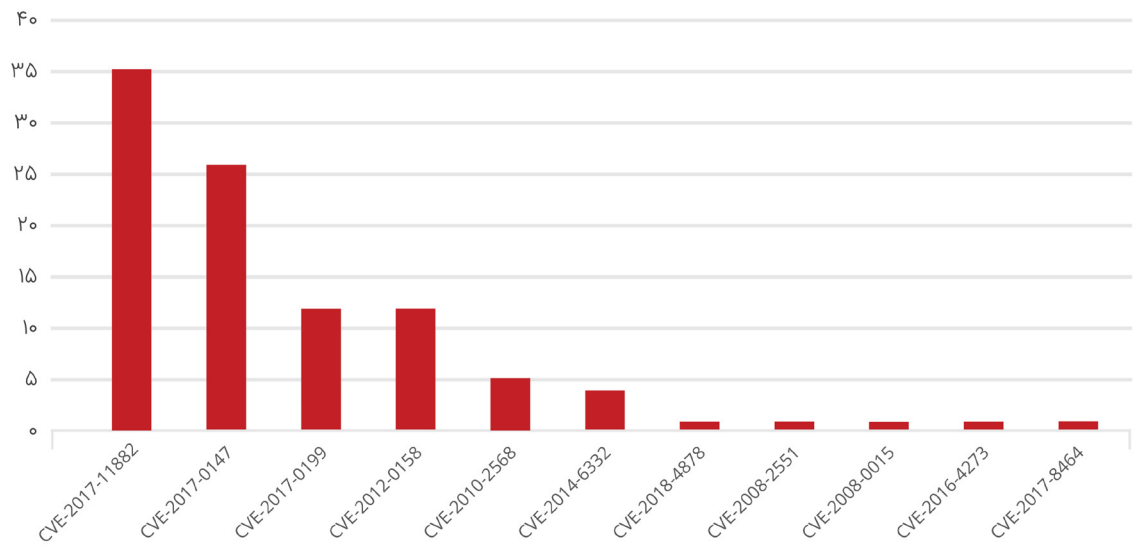
- CVE-2018-8174 – این آسیب‌پذیری در سه‌ماهه سوم توسط Operation Personality Disorder مورد بهره‌جویی قرار گرفت. مهاجمان با بکارگیری فایل‌های RTF آلوده که حاوی کد VBScript مخرب بودند از این ضعف در مرورگر Internet Explorer بهره‌جویی کرده و یک Shellcode را اجرا می‌کردند. کد مذکور با کپی یک درب‌پشتی[5] دسترسی کامل از راه دور به سیستم آلوده شده را برای مهاجمان برقرار می‌کرد. این کارزار توسط گروه Cobalt Gang که گرداننده اصلی آن در سال ۲۰۱۸ در اسپانیا دستگیر شد اجرا شده بود. همچنین در کارزاری دیگر مهاجمان با دست‌درازی به سایت‌های تبلیغاتی معتبر کاربران را به صفحه حاوی بسته بهره‌جوی مذکور هدایت می‌کردند. در صفحه فرود[6] اسکریپت VBScript کد شده در قالب Base64 تزریق شده بود که توسط یک تابع JavaScript قابل رمزگشایی می‌بود. کد باز شده با بهره‌جویی از موتور چیدمان VBScript موجب اجرای Shellcode می‌شد. Shellcode در ادامه کد را دریافت کرده و باج‌افزار GandCrab را در حافظه سیستم آلوده اجرا می‌کرد. همانطور که اشاره شد Fallout و Underminer، هر دو مجهز به بهره‌جوی این دو آسیب‌پذیری هستند.
- CVE-2018-8440 – اولین بار در شهریور ماه SandboxEscaper جزییات ضعفی امنیتی از نوع "ترفیع امتیازی"[7] را در قابلیت Task Scheduler سیستم عامل Windows منتشر کرد. ضعف مذکور که از مدیریت ناصحیح بخش Advanced Local Procedure Call ناشی می‌شود مهاجم را قادر به ترفیع سطح دسترسی خود بر روی دستگاه قربانی می‌کند. این آسیب‌پذیری با شناسه CVE-2018-8440 در مجموعه اصلاحیه‌های ماه سپتامبر توسط مایکروسافت پوشش داده شد.

۱ Drive-by Compromise | https://attack.mitre.org/techniques/T1189
۲ Exploit Public-Facing Application | https://attack.mitre.org/techniques/T1190
۳ Exploitation for Privilege Escalation | https://attack.mitre.org/techniques/T1068
۴ Exploitation for Defense Evasion | https://attack.mitre.org/techniques/T1211
۵ Backdoor
۶ Landing Page
۷ Privilege Escalation

- CVE-2018-8373 – جزییات آسیب‌پذیری CVE-2018-8373 که توسط مجموعه اصلاحیه‌های ماه میلادی آگوست ترمیم شد پیش‌تر به‌طور عمومی منتشر شده بود. بهره‌جویی از آسیب‌پذیری روز-صفر CVE-2018-8373 در نسخه‌های ۹، ۱۰ و ۱۱ نرم‌افزار Internet Explorer مهاجم را قادر به اجرای کد مخرب به‌صورت از راه دور بر روی دستگاه حاوی این مرورگر می‌کند. برای این منظور مهاجم می‌تواند از روش‌هایی نظیر هدایت کاربر به یک سایت حاوی کد بهره‌جو یا ارسال ایمیل با پیوست مخرب استفاده کند. Quasar RAT از جمله بدافزارهایی بود که مهاجمان برای انتشار آن، آسیب‌پذیری CVE-2018-8373 را مورد بهره‌جویی قرار دادند. در بدافزار مذکور، بهره‌جو در تمامی بسترها به‌طور صحیح اجرا نمی‌شد و همیشه در انتقال QuasarRAT بر روی دستگاه قربانی موفق نمی‌بود. چندین گروه از محققان امنیتی از جمله کارشناسان مک‌آفی اطلاعاتی در مورد کارزار و نحوه کار بدافزار منتشر کردند. به گفته یکی از این گروه‌ها VBScript!AccessArray نشانی آرایه‌ای از المنت‌ها را در پشته[1] نگهداری می‌کند. در ادامه VBScript!AccessArray تابع Default Property Get را در اسکریپت فراخوانی می‌کند تا طول آرایه را تغییر دهد. موضوعی که سبب خالی شدن حافظه جزیی که نشانی آن توسط VBScript!AccessArray در پشته ذخیره شده می‌شود. با ترمیم این آسیب‌پذیری در مجموعه اصلاحیه‌های ماه آگوست مایکروسافت، تابع SafeArrayLock آرایه فعلی را پیش از VBScript!AssignVar قفل می‌کند و بنابراین طول آرایه توسط تابع Default Property Get قابل تغییر نخواهد بود.

نمودار زیر میانگین تعداد بهره‌جویی‌های انجام شده از هر آسیب‌پذیری را طی یک هفته در سه‌ماهه سوم نمایش می‌دهد. مهاجمان با بکارگیری اکثر این آسیب‌پذیری‌ها فایل‌های ناقل را از راه دور بر روی دستگاه قربانی به اجرا در می‌آورند.

**میانگین تعداد بهره‌جویی‌های انجام شده از هر آسیب‌پذیری طی یک هفته**




منبع: McAfee Labs Threats Report

[1] Stack

# تهدیدات پیشرفته و مستمر

در سه‌ماهه سوم مک‌آفی بیش از ۳۵ حمله هدفمند را شناسایی کرد. جاسوسی سایبری اصلی‌ترین انگیزه در این حملات گزارش شده است. در دوره مذکور گروه‌های APT28، Dragonfly و Sandworm را که دولت‌ها، آزمایشگاه‌ها، بخش‌های انرژی و نظامی را مورد هدف قرار می‌دهند فعال‌تر از سایر گروه‌ها ارزیابی شده‌اند.

در این دوره محققان شرکت ضدویروس ای‌ست، در گزارشی جزییات بدافزار بسیار پیشرفته‌ای از نوع روت‌کیت، با نام LoJax را منتشر کردند که بر اساس آن می‌توان آن را نخستین روت‌کیت مبتنی بر Unified Extensible Firmware Interface – به اختصار UEFI – دانست. این بدافزار با رخنه در ماژول حافظه Serial Peripheral Interface – به اختصار SPI – نه تنها در صورت تغییر سیستم عامل ماندگار می‌ماند که حتی جایگزینی دیسک سخت نیز تأثیری در حضور این بدافزار نخواهد داشت. بر روی دستگاه‌های هدف قرار گرفته شده توسط LoJax سه ابزار شناسایی شده است. از این سه، دو ابزار، مسئول جمع‌آوری جزییات ثابت‌افزار[1] سیستم و ایجاد رونوشتی از آن از طریق خواندن ماژول حافظه SPI – که UEFI بر روی آن قرار گرفته – هستند. ابزار سوم نیز ماژول مخرب را تزریق کرده و نسخه دستکاری شده را بر روی حافظه SPI ذخیره می‌کند. هدف روت‌کیت LoJax ماندگار کردن بدافزار مورد نظر مهاجمان بر روی دستگاه‌های با سیستم عامل Windows و اجرای خودکار آن در هر بار راه‌اندازی دستگاه است. این محققان، گروه APT28 را که با نام‌های Fancy Bear، Sednit، Strontium و Sofacy شناخته می‌شود سازنده LoJax معرفی کرده‌اند. قربانیان این حمله نهادهای دولتی در شبه‌جزیره بالکان و بخش‌های مرکزی و شرقی اروپا اعلام شدند.

برخی از این گروه‌ها نیز بیش از قبل از ابزارهای کد باز به همراه ماکروها و اسکریپت‌ها بهره گرفتند و در عمل کد آنها بجز بهبودهایی جزیی و پایه‌ای حاوی تغییرات خاص و قابل‌توجهی نبوده است.

دو نمونه از کارزارهای هدفمند که در سه‌ماهه سوم موسسات مالی را مورد حمله قرار دادند به‌شرح زیر است:

- Operation Double Infection - مهاجمان در این کارزار با ارسال ایمیل‌های فیشینگ هدفمند حاوی لینک‌های مخرب تلاش داشتند تا دستگاه اهداف خود را به دو درب‌پشتی آلوده کنند. تمرکز اصلی مهاجمان پشت‌پرده این کارزار بر روی شرکت‌هایی در روسیه و اروپای شرقی بوده است.
- Operation Personality Disorder - در این کارزار فیشینگ، مهاجمان یا قربانی را تشویق به اجری پیوست هرزنامه که ناقل آلودگی بود می‌کردند یا او را متقاعد به کلیک بر روی لینکی که در متن ایمیل درج شده بود می‌نمودند. کلیک بر روی لینک مذکور موجب هدایت کاربر به صفحه‌ای اینترنتی شده و در صورت بی‌توجهی کاربر به ترفندهای به‌کار گرفته شده توسط مهاجمان، درب‌پشتی More_eggs بر روی دستگاه اجرا می‌شد. هدف نهایی این حملات به کنترل درآوردن سیستم قربانی توسط مهاجمان اعلام شده است. در ایمیل‌های فیشینگ مذکور این‌طور تظاهر می‌شد که فرستنده یکی از سازمان‌های مالی معتبر در اروپاست. برخی از فایل‌های RTF مخرب که به این ایمیل‌های فیشینگ پیوست شده بودند حاوی بهره‌جوی مجموعه‌ای از آسیب‌پذیری‌ها نظیر CVE-2018-8174 بودند.

[1] Firmware

هر دو کارزار در موارد زیر اشتراک داشته‌اند:

- مؤسسات مالی در روسیه و اروپای شرقی را هدف قرار می‌داده‌اند.
- در ایمیل‌های فیشینگ اینطور تظاهر می‌شد که فرستنده از موسسات و سازمان‌های معتبر در حوزه مالی است.
- از فایل‌های Word حاوی ماکروی مخرب برای آلوده‌سازی دستگاه استفاده می‌شد.
- از درب‌پشتی‌های سفارشی مبتنی بر JavaScript که خود را فایل‌های متنی بی‌خطر جا می‌زدند برای دسترسی کامل یافتن به سیستم آلوده بهره گرفته می‌شد.
- از ابزار cmstp.exe[۱] به فایلی حاوی اطلاعات نصب برای عبور از سد Windows AppLocker و دریافت و اجرای کد به‌صورت از راه دور استفاده شده است.
- از Useregsvr32.exe نیز برای عبور از سد Windows AppLocker بهره گرفته شده است.
- گروه شناخته شده Cobalt Group گرداننده هر دو کارزار معرفی شده است. این گروه حداقل از سال ۲۰۱۳ فعال بوده و در بیش از یکصد حمله بر ضد مؤسسات مالی در سرتاسرجهان نقش داشته است.
- علیرغم دستگیری فرد مشکوک به رهبری گروه در ماه مارس حملات همچنان در جریان است.

| رخنه | اجرا | ماندگاری | ارتقای سطح دسترسی | عبور از سد سیستم دفاعی | دسترسی به اطلاعات اصالت‌سنجی | شناسایی | گسترده کردن دامنه حمله | جمع‌آوری اطلاعات | انتقال اطلاعات | ارتباطات با سرور فرماندهی |
|---|---|---|---|---|---|---|---|---|---|---|
| آلوده‌سازی دستگاه در زمان مراجعه کاربر به سایت تحت کنترل مهاجم | اجرای فایل‌های INF مخرب از طریق پروسه معتبر CMSTP[۳] | بهره‌گیری از سیستم COM در Windows[۵] | عبور از سد UAC | عبور از سد UAC | اجرای حملات سعی‌وخطا[۷] | شناسایی نام‌های کاربری محلی و تحت دامنه | بهره‌جویی از سرویس‌های به اشتراک گذاشته شده[۱۰] | شنود گفتگوهای کاربر از طریق روش‌هایی همچون فعالسازی میکروفون | ارسال خودکار | درگاه‌های متداول |
| بهره‌جویی از آسیب‌پذیری سیستم‌های قابل دسترس در اینترنت | استفاده از واسط خط فرمان[۴] | ساخت حساب کاربری محلی / تحت دامنه[۶] | جایگزین کردن DLL معتبر فراخوانی شده با فایل DLL مخرب | اجرای فایل‌های INF مخرب از طریق پروسه معتبر CMSTP | کشف اطلاعات اصالت‌سنجی از طریق استخراج فایل‌های مربوطه در سیستم عامل[۸] | جستجوی فایل‌ها و پوشه‌ها | اجرای کدهای موسوم به Logon Script[۱۱] | جمع‌آوری خودکار اطلاعات با استفاده از ابزارهایی نظیر اسکریپت حساس به کلمات خاص | فشرده‌سازی داده‌ها | پراکسی ارتباطی[۱۲] |
| تکثیر از طریق رسانه‌های جداشدنی و سوءاستفاده از قابلیت Autorun[۲] | شنود فراخوانی‌های ارسالی به توابع API و دست‌درازی به آنها | جایگزین کردن DLL معتبر فراخوانی شده با فایل DLL مخرب | بهره‌جویی از ضعف‌های موسوم به ترفیع امتیازی | امضای کد | شناسایی فایل‌های حاوی رمزعبور[۹] | پویش از راه دور سرویس‌های اجرا شده بر روی دستگاه هدف | بکارگیری پودمان RDP | استخراج از انباره‌های اطلاعات | رمزگذاری داده | پودمان سفارشی برای برقراری ارتباط با سرور فرماندهی[۱۳] |

▲

مکانیزم‌های به‌کار گرفته شده توسط مهاجمان در حوزه حملات هدفمند در سه‌ماهه سوم ۲۰۱۸ بر مبنای مدل MITRE ATT&CK؛
پس‌زمینه تیره‌تر نشانه استفاده بیشتر از مکانیزم. (ادامه در صفحه بعد)

۱ Microsoft Connection Manager Profile Installer
۲ Replication Through Removable Media | https://attack.mitre.org/techniques/T1091
۳ CMSTP | https://attack.mitre.org/techniques/T1191
۴ Command-Line Interface | https://attack.mitre.org/techniques/T1059
۵ Component Object Model Hijacking | https://attack.mitre.org/techniques/T1122
۶ Create Account | https://attack.mitre.org/techniques/T1136
۷ Brute Force | https://attack.mitre.org/techniques/T1110
۸ Credential Dumping | https://attack.mitre.org/techniques/T1003
۹ Credentials in Files | https://attack.mitre.org/techniques/T1081
۱۰ Exploitation of Remote Services | https://attack.mitre.org/techniques/T1210
۱۱ Logon Scripts | https://attack.mitre.org/techniques/T1037
۱۲ Connection Proxy | https://attack.mitre.org/techniques/T1090
۱۳ Custom Command and Control Protocol | https://attack.mitre.org/techniques/T1094

| رخنه | اجرا | ماندگاری | ارتقای سطح دسترسی | عبور از سد سیستم دفاعی | دسترسی به اطلاعات اصالت‌سنجی | شناسایی | گسترده کردن دامنه حمله | جمع‌آوری اطلاعات | انتقال اطلاعات | ارتباطات با سرور فرماندهی |
|---|---|---|---|---|---|---|---|---|---|---|
| ارسال ایمیل فیشینگ هدفمند با پیوست مخرب | بهره‌جویی از ضعف‌های امنیتی برای اجرای کد به‌صورت از راه دور | مخفی‌سازی فایل / پوشه[۲] | هوکینگ | بهره‌گیری از سیستم COM در Windows | ارسال پروسه جعلی در زمان فراخوانی فایل یک پروسه مجاز | شناسایی پوشه/درایو به اشتراک گذاشته شده[۱۲] | بهره‌گیری از نرم‌افزار ثالث | استخراج داده‌ها از سیستم به صورت محلی | ارسال از طریق پودمان‌های جایگزین | کد کردن داده‌ها |
| ارسال ایمیل فیشینگ هدفمند حاوی لینک مخرب | استفاده از رابط گرافیکی کاربر[۳] | ارسال پروسه جعلی در زمان فراخوانی فایل یک پروسه مجاز | ساخت سرویس جدید | مبهم‌سازی یا کد کردن فایل یا اطلاعات[۱۰] | ضبط داده‌های وارد شده توسط کاربر | شناسایی تجهیزات جانبی متصل به دستگاه | سوءاستفاده از پوشه‌های اشتراکی مخفی نظیر C$، ADMIN$ و IPC$[۱۴] | جمع‌آوری مرحله‌ای داده‌ها[۱۵] | ارسال از طریق سرور فرماندهی | مبهم‌سازی داده‌ها |
| آلوده‌سازی محصولی که در زنجیره تامین به دست کاربر / سازمان می‌رسد[۱] | بهره‌جویی از راه‌انداز LSASS[۴] | بهره‌جویی از راه‌انداز LSASS | ارسال پروسه جعلی در زمان فراخوانی فایل یک پروسه مجاز | جایگزین کردن DLL معتبر فراخوانی شده با فایل DLL مخرب | نمایش پیام جعلی برای فریب کاربر به وارد کردن اطلاعات اصالت‌سنجی | شناسایی پروسه‌های اجرا شده | | جمع‌آوری اطلاعات مرتبط با ایمیل از طریق پویش فایل‌هایی همچون PST و OST | ارسال از طریق رسانه‌های شبکه‌ای | چند کاناله کردن سرور فرماندهی و چند مرحله نمودن ارتباطات[۱۸] |
| رخنه به سازمان‌های مورداعتماد سازمان هدف قرار گرفته شده[۲] | اجرا از طریق پروسه معتبر PowerShell | دست‌درازی به سرویس‌های موجود[۸] | فرمان زمانبندی‌شده | بهره‌جویی از ضعف‌های محصول امنیتی بکار گرفته شده توسط قربانی | | کندوکاو در محضرخانه | | ضبط داده‌های وارد شده توسط کاربر | | بکارگیری چند پودمان در ارتباطات سرور فرماندهی[۱۹] |
| | بهره‌گیری از پروسه معتبر Regsvr32[۵] | ساخت سرویس جدید[۹] | | حذف سوابق | | شناسایی محصولات امنیتی | | بهره‌جویی از تنظیمات مرورگر برای دست‌درازی به محتوای سایت[۱۶] | | رمزگذاری چندلایه‌ای ارتباطات با سرور فرماندهی[۲۰] |
| | اجرا از طریق پروسه معتبر Rundll32[۶] | افزودن کلید Run در محضرخانه و یا بهره‌جویی از پوشه Startup | | مخفی‌سازی فایل / پوشه | | جمع‌آوری اطلاعات در خصوص سیستم | | تصویربرداری از صفحه کار کاربر | | استفاده ابزارهای دسترسی از راه دور[۲۱] |
| | فرمان زمانبندی‌شده | | | ارزیابی توان محصول امنیتی از لحاظ شناسایی بدافزار[۱۱] | | شناسایی تنظیمات شبکه‌ای دستگاه هدف قرار گرفته شده[۱۳] | | تصویربرداری از طریق روش‌هایی همچون فعالسازی دوربین[۱۷] | | کپی دستی فایل به‌صورت از راه دور[۲۲] |

مکانیزم‌های به‌کار گرفته شده توسط مهاجمان در حوزه حملات هدفمند در سه‌ماهه سوم ۲۰۱۸ بر مبنای مدل MITRE ATT&CK؛
پس‌زمینه تیره‌تر نشانه استفاده بیشتر از مکانیزم. (ادامه از صفحه قبل)

۱ Supply Chain Compromise | https://attack.mitre.org/techniques/T1195
۲ Trusted Relationship | https://attack.mitre.org/techniques/T1199
۳ Graphical User Interface | https://attack.mitre.org/techniques/T1061
۴ LSASS Driver | https://attack.mitre.org/techniques/T1177
۵ Regsvr32 | https://attack.mitre.org/techniques/T1117
۶ Rundll32 | https://attack.mitre.org/techniques/T1085
۷ Hidden Files and Directories | https://attack.mitre.org/techniques/T1158
۸ Modify Existing Service | https://attack.mitre.org/techniques/T1031
۹ New Service | https://attack.mitre.org/techniques/T1050
۱۰ Deobfuscate/Decode Files or Information | https://attack.mitre.org/techniques/T1140
۱۱ Indicator Removal from Tools | https://attack.mitre.org/techniques/T1066
۱۲ Network Share Discovery | https://attack.mitre.org/techniques/T1135
۱۳ System Network Configuration Discovery | https://attack.mitre.org/techniques/T1016
۱۴ Windows Admin Shares | https://attack.mitre.org/techniques/T1077
۱۵ Data Staged | https://attack.mitre.org/techniques/T1074
۱۶ Man in the Browser | https://attack.mitre.org/techniques/T1185
۱۷ Video Capture | https://attack.mitre.org/techniques/T1125
۱۸ Multi-Stage Channels | https://attack.mitre.org/techniques/T1104
۱۹ Multiband Communication | https://attack.mitre.org/techniques/T1026
۲۰ Multilayer Encryption | https://attack.mitre.org/techniques/T1079
۲۱ Remote Access Tools | https://attack.mitre.org/techniques/T1219
۲۲ Remote File Copy | https://attack.mitre.org/techniques/T1105

| اجرا | ماندگاری | عبور از سد سیستم دفاعی | شناسایی | ارتباطات با سرور فرماندهی |
|---|---|---|---|---|
| اسکریپت‌نویسی | فرمان زمانبندی‌شده | تغییر نام / محل ذخیره‌سازی برای فریب محصول امنیتی[۳] | شناسایی کاربر اصلی / فعال در سیستم | استفاده از پودمان‌های رایج نظیر HTTP، HTTPS، SMTP یا DNS |
| اجرا با ثبت یک سرویس جدید یا دست‌درازی به سرویس موجود[۱] | بهره‌جویی از بخش BIOS / UEFI / EFI | دست‌درازی به محضرخانه | شناسایی سرویس‌ها | استفاده از پودمان‌های رمزگذاری برای مخفی ساختن محتوای ارتباطات بجای تکیه به سیستم حفاظتی کانال ارتباطی[۸] |
| بهره‌گیری از نرم‌افزار ثالث | | مبهم‌سازی فایل / اطلاعات[۴] | استخراج ساعت، تاریخ و منطقه زمانی | |
| دخالت دادن کاربر به اجرای فایل مخرب[۲] | | بهره‌جویی از TxF[۴] | | |
| اجرا از طریق WMI | | ارسال پروسه جعلی در زمان فراخوانی فایل یک پروسه مجاز | | |
| | | بهره‌گیری از پروسه معتبر Regsvr32.exe | | |
| | | استفاده از Rootkit[۵] | | |
| | | اجرا از طریق پروسه معتبر Rundll32 | | |
| | | اسکریپت‌نویسی | | |
| | | فشرده‌سازی یا رمزگذاری فایل مخرب | | |
| | | استفاده از ابزارهای توسعه معتبر[۶] | | |
| | | استفاده از حساب کاربری معتبر اما هک شده[۷] | | |

▲

مکانیزم‌های به‌کار گرفته شده توسط مهاجمان در حوزه حملات هدفمند در سه‌ماهه سوم ۲۰۱۸ بر مبنای مدل MITRE ATT&CK؛
پس‌زمینه تیره‌تر نشانه استفاده بیشتر از مکانیزم. (ادامه از صفحه قبل)

۱ Service Execution | https://attack.mitre.org/techniques/T1035
۲ User Execution | https://attack.mitre.org/techniques/T1204
۳ Masquerading | https://attack.mitre.org/techniques/T1036
۴ Obfuscated Files or Information | https://attack.mitre.org/techniques/T1027
۵ Process Doppelg□nging | https://attack.mitre.org/techniques/T1186
۶ Rootkit | https://attack.mitre.org/techniques/T1014
۷ Trusted Developer Utilities | https://attack.mitre.org/techniques/T1127
۸ Valid Accounts | https://attack.mitre.org/techniques/T1078
Standard Cryptographic Protocol | https://attack.mitre.org/techniques/T1032

# Statistics

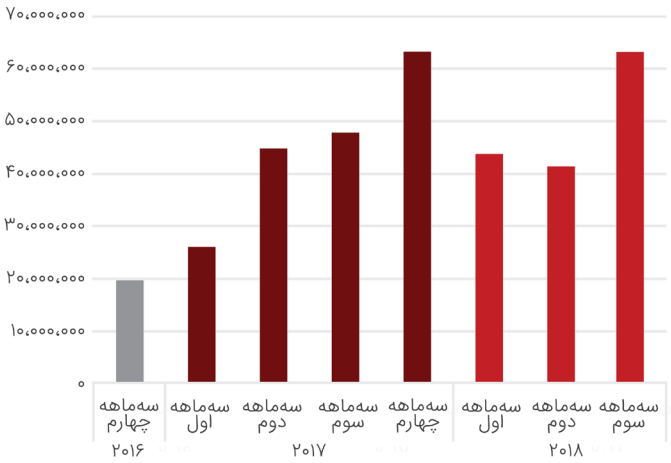
# آمـــار

فناوری McAfee Global Threat Intelligence – به اختصار McAfee GTI –، به‌طور میانگین، در هر روز ۴۹ میلیارد درخواست و ۱۳ میلیارد خط دوری‌سنجی (Telemetry) را در سرتاسر جهان دریافت و پردازش کرده و ۵،۶۰۰،۰۰ نشانی اینترنتی و ۷۰۰،۰۰۰ فایل را به همراه ۲۰۰،۰۰۰ فایل در قرنطینه امن (Sandbox) مورد تحلیل قرار می‌دهد. بررسی آمار این فناوری در سه‌ماهه سوم سال ۲۰۱۸ نتایج زیر را در بر داشته است:

- از بین ۷۷ میلیارد فایل بررسی شده توسط McAfee GTI، ۷۳ میلیون مورد (۰/۰۱ درصد) با ریسک بالا گزارش شده است.
- از میان ۱۶ میلیارد، نشانی URL تحلیل شده توسط McAfee GTI، ۶۳ میلیون مورد (۰/۴ درصد) با ریسک بالا تشخیص داده شده است.
- از بین ۱۵ میلیارد نشانی IP ارزیابی شده، ۶۶ میلیون مورد (۰/۴ درصد) با ریسک بالا گزارش شده است.

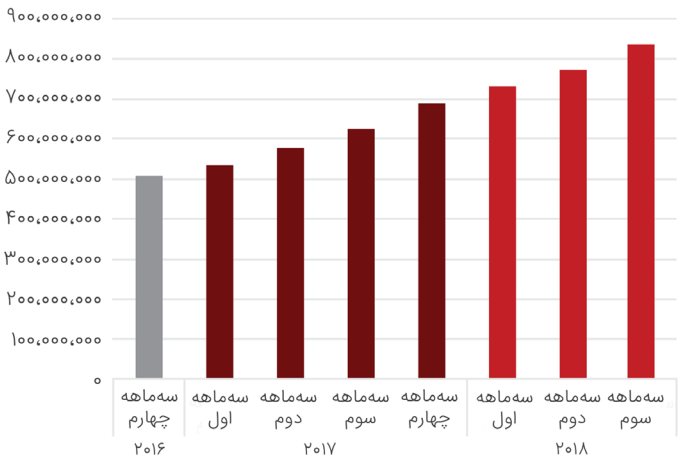
# بـدافـزارهـا

### بدافزارهای جدید




منبع: McAfee Labs Threats Report

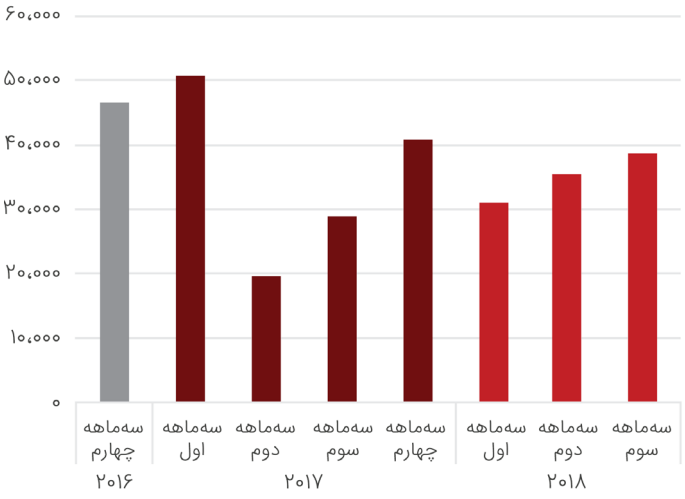
### مجموع کل بدافزارها




منبع: McAfee Labs Threats Report

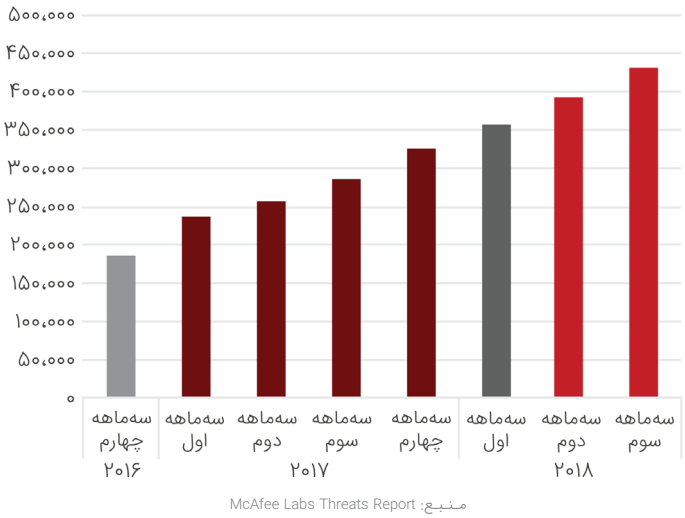
در سه‌ماهه سوم ۲۰۱۸، به‌طور میانگین، در هر ثانیه، بیشـتر از هشـت بدافزار منحصربه‌فرد جـدیـد به دست آزمایشگاه‌های مک‌آفی رسیده است. تعداد کـل بـدافـزارهـا در این دوره نیز به حدود ۸۳۰ میلیون عدد رسیده است.

## بدافزارهای جدید Mac




منبع: McAfee Labs Threats Report

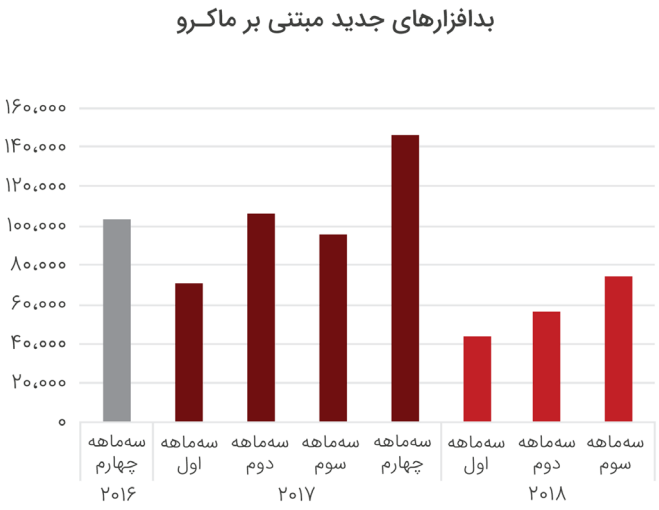
## مجموع کل بدافزارهای Mac




منبع: McAfee Labs Threats Report

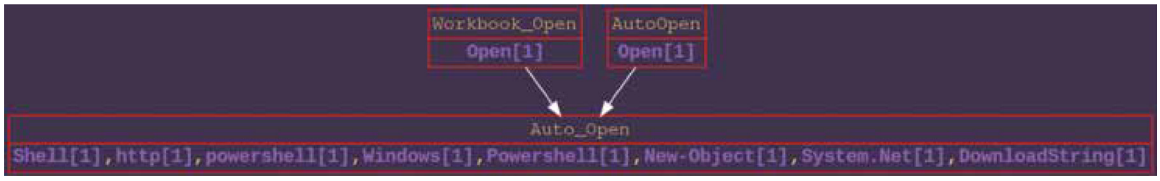
در سه‌ماهه سوم سال ۲۰۱۸، حدود ۴۰ هزار نمونه منحصربه‌فرد جدید از بدافزارهای ویژه سیستم عامل MacOS کشف و شناسایی شده است. تعداد کل بدافزارهای سازگار با MacOS نیز از مرز ۴۳۰ هزار عدد عبور کرده است.

مدتهاست که اکثر قریب به اتفاق کاربران دریافته‌اند که باید از باز کردن پیوست‌های اجرایی ایمیل‌ها خودداری کنند. تقریبا همگان می‌دانند شرکت‌های تولیدکننده نرم‌افزار، فایل‌های اجرایی خود را به ایمیل پیوست نمی‌کنند. اما پیوست بودن فایل‌های مربوط به مجموعه نرم‌افزاری Office موضوعی کاملا عادی محسوب می‌شود. ردوبدل این‌گونه فایل‌ها بخشی از وظایف روزانه بسیاری از کارمندان است. برنامه‌های مجموعه نرم‌افزاری Office مجهز به قابلیتی با عنوان ماکرو[1] هستند که سبب سرعت بخشیدن به اموری می‌شوند که روالی تکرار شونده دارند. اما سرعت بخشیدن به کار بسیاری از کارکنان تنها خاصیت ماکرو نیست. متاسفانه، نفوذگران نیز از ماکرو برای آلوده کردن سیستم‌های سازمان بهره می‌گیرند.

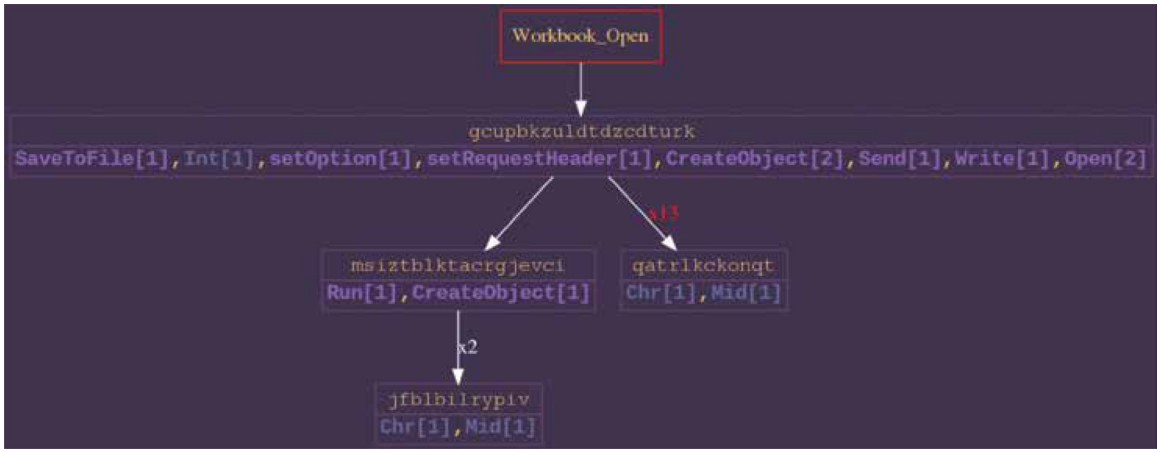



منبع: McAfee Labs Threats Report

یکی از نکات قابل توجه در خصوص کدهای مخرب تحت ماکرو، مبهم‌سازی[2] شدن بسیاری از آنها توسط مهاجمان است. هدف از مبهم‌سازی، دشوار نمودن فرایند تحلیل و شناسایی است. برای مثال تصاویر زیر دو نمونه کد ماکرو با عملکرد تقریبا یکسان را نشان می‌دهند. اما تحلیلگر برای بررسی کدهای درج شده در تصویر دوم که به‌نحو ساده‌ای مبهم‌سازی شده است می‌بایست زمان بیشتری صرف کند.

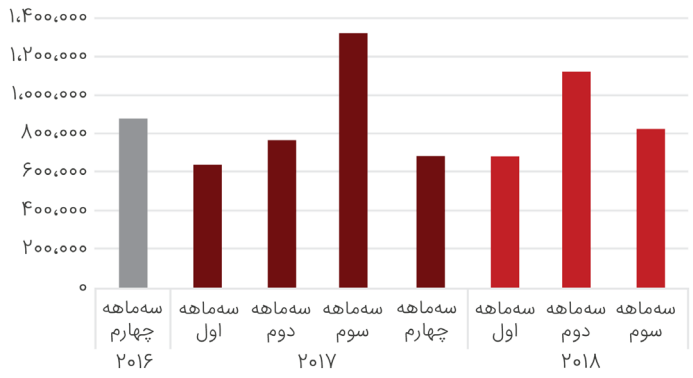



▲▼ کدهای ماکرو قبل و بعد از مبهم‌سازی شدن




[1] Macro
[2] Obfuscation

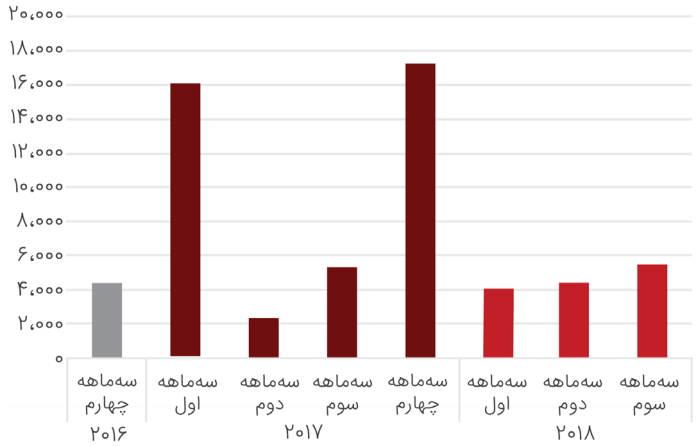
## کدهای مخرب دودویی امضا شده جدید




منبع: McAfee Labs Threats Report

مراجع صدور گواهی[۱] از طریق گواهینامه‌های دیجیتال[۲] امکان ارائه اطلاعات در خصوص کدهای دودویی[۳] (برنامه[۴]) امضا شده[۵] را فراهم می‌کنند. بسیاری از محصولات ضدویروس برنامه‌های امضا شده را معتبر تلقی کرده و آنها را از مورد پویش قرار گرفتن استثنا می‌کنند. مهاجمان نیز با دست یافتن به گواهینامه‌های دیجیتال و تخصیص آنها به کدهای مخرب خود، عبور از سد این محصولات ضدویروس را تسهیل می‌کنند.

## بدافزارهای جدید مبتنی بر PowerShell

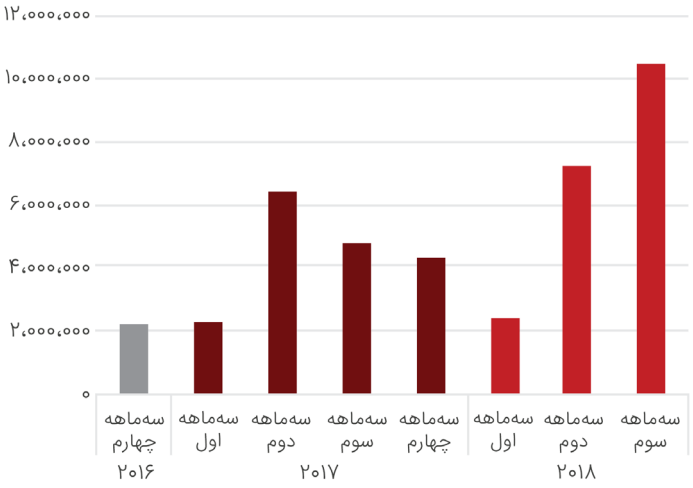



منبع: McAfee Labs Threats Report

یکی از روش‌های پیشرفته ویروس‌نویسان حرفه‌ای در طی دو سال گذشته استفاده از روشی موسوم به "بدون فایل"[۶] بوده که در آن با بهره‌گیری از فایل معتبر Windows PowerShell بدافزار از اینترنت دریافت و بر روی دستگاه قربانی اجرا می‌شود. شناسایی و کشف بدافزارهای از نوع "بدون فایل" بسیار دشوارتر از گونه‌های معمول بدافزارهاست.

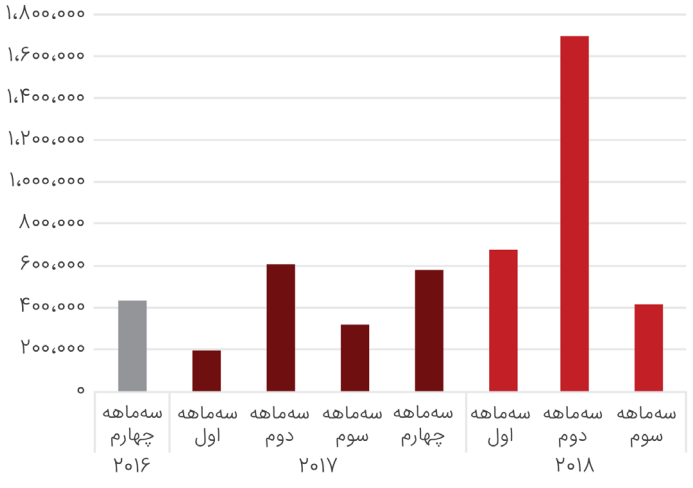
۱ Certificate Authority
۲ Digital Certificate
۳ Binary
۴ Application
۵ Signed
۶ Fileless

### بدافزارهای جدید مبتنی بر JavaScript




منبع: McAfee Labs Threats Report

### بدافزارهای جدید بهره‌جو



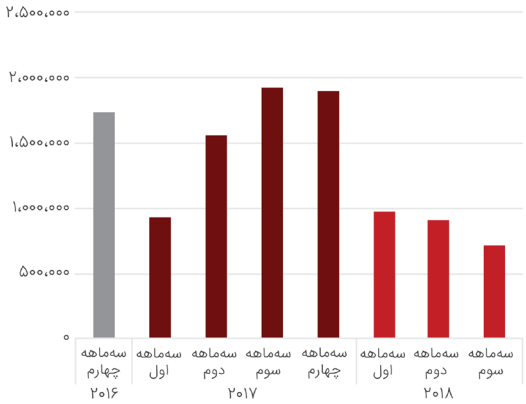

منبع: McAfee Labs Threats Report

سوءاستفاده از آسیب‌پذیری‌های امنیتی در سیستم عامل و نرم‌افزارهای کاربردی یکی از روش‌های نفوذ به اهداف و انتشار بدافزار توسط مهاجمان حرفه‌ای است. وجود یک آسیب‌پذیری حیاتی می‌تواند سبب دور زدن قوی‌ترین محصولات ضدویروس یا دیواره‌های آتش توسط بدافزارها و ابزارهای موسوم به بهره‌جو شود.

# تهدیدات تحت وب و شبکه

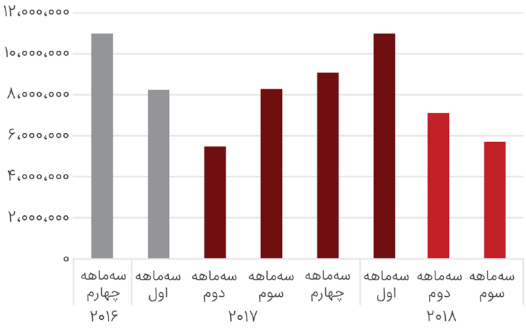
نشانی‌های URL مشکوک شامل تعداد کل سایت‌هایی است که بر اساس درجه‌بندی شرکت مک‌آفی، امتیاز ریسک بالا یا متوسط را دریافت کرده‌اند. نشانی‌های URL مخرب نیز آن دسته از سایت‌هایی هستند که کاربر را به صفحات اینترنتی حاوی برنامه‌های مخربی همچون بدافزارها هدایت می‌کنند. همچنین دریافت‌های مخرب از سایت‌هایی سرچشمه می‌گیرند که بعضا بدون دخالت کاربر کد مخرب یا ناخواسته را بر روی دستگاه او دریافت می‌کنند. نشانی‌های فیشینگ نیز صفحات وبی هستند که معمولا از طریق ایمیل‌های کلاهبرداری کاربر به سمت آنها هدایت شده و در آنها تلاش می‌شود تا با بهره‌گیری از مهندسی اجتماعی اطلاعات حساس کاربر نظیر نام کاربری و رمز عبور او سرقت شود.

نشانی‌های URL جدید، مربوط به دریافت‌های مخرب



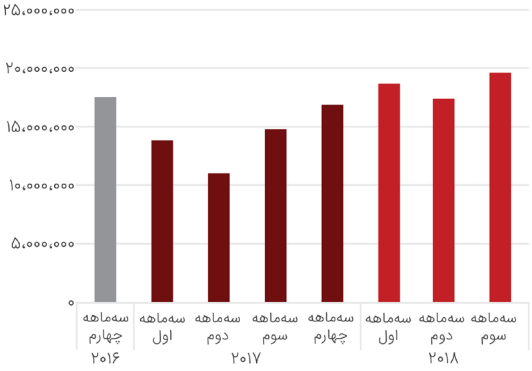

منبع: McAfee Labs Threats Report

نشانی‌های URL مخرب جدید



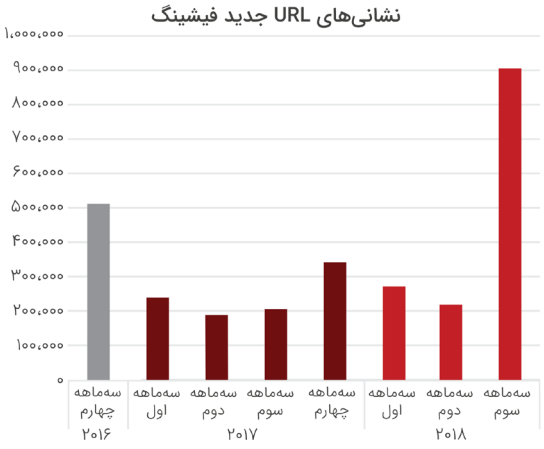

منبع: McAfee Labs Threats Report

نشانی‌های URL مشکوک جدید



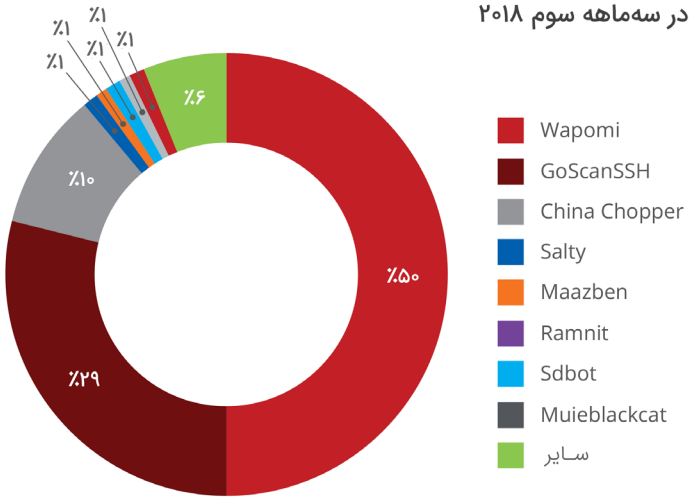

منبع: McAfee Labs Threats Report

نشانی‌های URL جدید فیشینگ



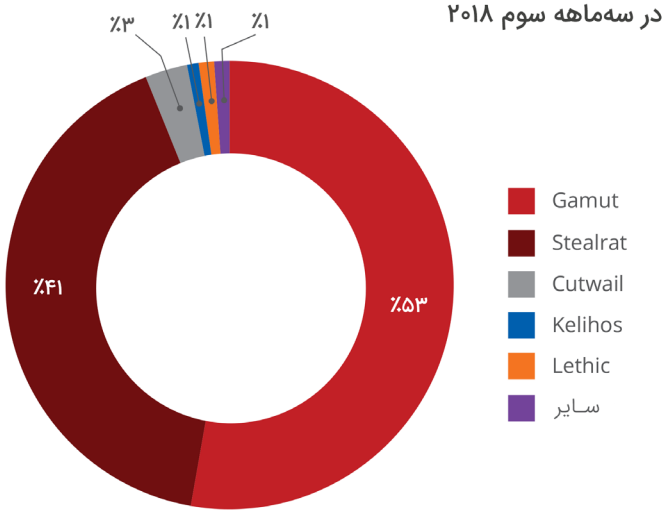

منبع: McAfee Labs Threats Report

### بیشترین بدافزارهای متصل به سرورهای فرماندهی در سه‌ماهه سوم ۲۰۱۸




منبع: McAfee Labs Threats Report

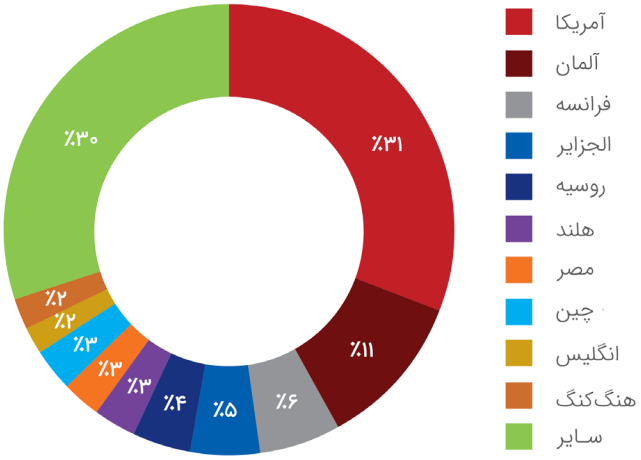
### بزرگترین شبکه‌های مخرب ارسال‌کننده هرزنامه در سه‌ماهه سوم ۲۰۱۸




منبع: McAfee Labs Threats Report

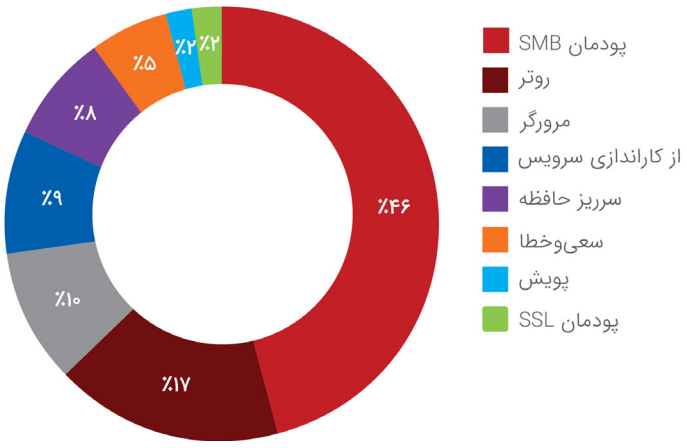
شبکه‌های مخرب Gamut و Stealrat به‌ترتیب در ارسال ۵۳ و ۴۱ درصد هرزنامه‌های سه‌ماهه سوم ۲۰۱۸ نقش داشته‌اند.

## کشورهای با بیشترین تعداد سرور فرماندهی شبکه‌های مخرب در سه‌ماهه سوم ۲۰۱۸




منبع: McAfee Labs Threats Report

## روش‌های اصلی حمله در سه‌ماهه سوم ۲۰۱۸




منبع: McAfee Labs Threats Report


در آذر ماه ۱۳۹۷، شرکت صاحب‌نام مک‌آفی موفق به دریافت نشان Peer Insights Customers' Choice از مؤسسه گارتنر در بخش Enterprise Data Loss Prevention برای سال ۲۰۱۸ میلادی شد.

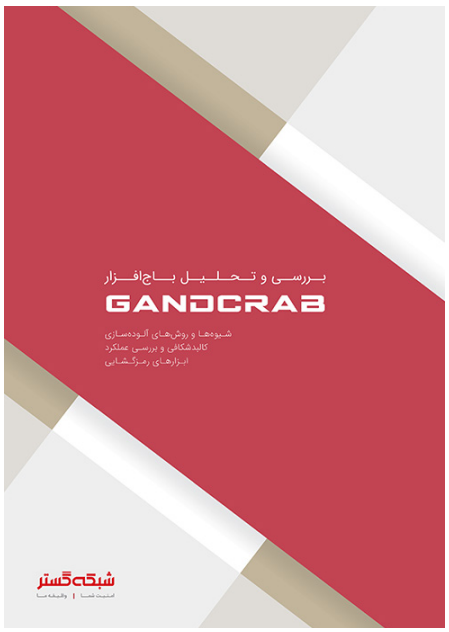
کسب این جایگاه بیانگر این واقعیت است که محصول Data Loss Prevention این شرکت در عین سادگی، انعطاف‌پذیری قابل توجه، قابلیت‌های جامع رقابتی و سرعت بالا، پاسخگوی نیاز مشتریان سازمانی در مقابله مؤثر با تهدیدات روبه‌رشد سرقت اطلاعات و کاهش ریسک ازدست‌رفت داده‌هاست.

مؤسسه گارتنر، یکی از معتبرترین مؤسسات بین‌المللی ارزیابی محصولات فناوری اطلاعات است که نشان Peer Insights Customers' Choice را بر اساس نظرات کاربران متخصص به سازندگان برتر محصولات حوزه مورد بررسی اعطا می‌کند.

برای کسب چنین جایگاهی می‌بایست حداقل ۵۰ نظر تخصصی با میانگین امتیاز ۴٫۲ – از ۵ – و یا بالاتر در بازه زمانی تعیین شده به این مؤسسه اعلام شده باشد. لازم به ذکر است که در ارزیابی سال ۲۰۱۸ مؤسسه گارتنر، ۹۸ متخصص در بررسی محصول McAfee Data Loss Prevention شرکت داشته‌اند.

# در اتاق خبر
# شبکه گستر بخوانید...

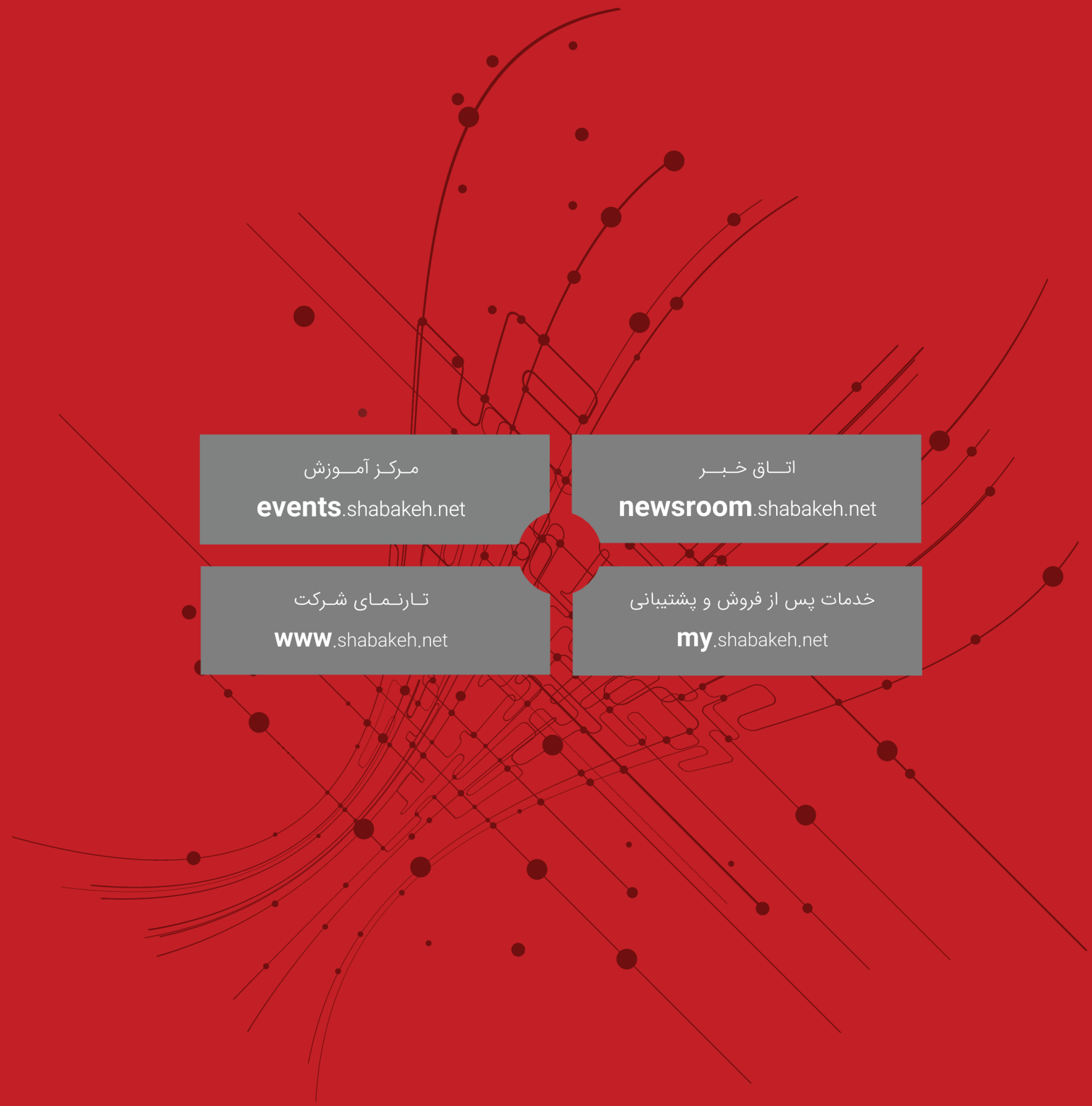





## شبکه گستر

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید. در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید. از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضدویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد. شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه‌اندازی و طولانی مدت ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است. این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

CSQ
ISO 9001




شبکه گستر
شرکت مهندسی شبکه گستر

تهران خیابان شهید دستگردی (ظفر) شماره ۲۷۳
تلفن / دورنگار ۰۲۱-۴۲۰۵۲
info@shabakeh.net
www.shabakeh.net