McAfee
Together is power.

گزارش و آمار فصلی از فعالیت

بدافزارها و تهدیدات سایبری

سپتامبر ۲۰۱۸

شبکه گستر
امنیت شما | وظیفه ما

فهرست مطالب

خلاصه مدیریتی

بر کسی پوشیده نیست که انگیزه و هدف اصلی بخش اعظم تبهکاران سایبری رسیدن به منافع مالی است. اما همانطور که در گزارش فصلی شرکت مک‌آفی در خصوص وضعیت تهدیدات سایبری در سه‌ماهه دوم سال ۲۰۱۸ میلادی خواهیم دید راه‌های تحقق این هدف، دائما در حال تغییر و تحول است.

در حالی که باج‌افزارها[۱] تا همین چندی پیش از پرسودترین بدافزارها تلقی می‌شدند مدتی است که محبوبیت گذشته خود را در میان نویسندگان ویروس از دست داده‌اند و برای دومین دوره متوالی، تعداد نمونه‌های جدید آنها، روندی نزولی داشته است. با این حال، در این دوره تعداد آلودگی‌ها به باج‌افزار Scarab که نخستین نسخه از آن در ژوئن سال میلادی گذشته کشف و شناسایی شد به‌طور قابل توجهی افزایش داشته است. به‌نحوی که نسخه‌های اخیر آن روی هم رفته سهمی بیش از ۵۰ درصد از کل نمونه‌های Scarab را تا به امروز به خود اختصاص داده‌اند.

همچون دوره قبل، در سه‌ماهه دوم ۲۰۱۸ نیز گسترش روزافزون بدافزارهای ویژه حملات موسوم به رمز ربایی[۲] را شاهد بوده‌ایم. بر خلاف باج‌افزارها که از عبارت "شلیک کن و امیدوار باش که پرداخت کنند" برای توصیف آنها استفاده می‌شود در رمز ربایی آلودگی هر دستگاه به‌معنای استخراج[۳] قطعی ارز رمز به نفع مهاجم، آن هم برای مدت طولانی است.

شاید کسی تصور نمی‌کرد که روترها و دستگاه‌های موسوم به اینترنت اشیا[۴] روزی به یکی از اهداف اصلی گردانندگان بدافزارهای رمز ربا تبدیل شوند. متاسفانه رمزهای عبور ضعیف یا پیش‌فرض و آسیب‌پذیر بودن ثابت‌افزار اکثر این تجهیزات، تسخیر آنها را توسط مهاجمان بسیار تسهیل کرده است.

تزریق کدهای رمز ربا در مرورگر کاربران از طریق روترهای تسخیر شده نیز یکی دیگر از نگرانی‌های اصلی راهبران شبکه در این روزهاست. نفوذگران با آلوده نمودن روترها سبب می‌گردند تا در صفحات فراخوانی شده در مرورگر کاربرانی که در سطح شبکه از طریق این تجهیزات به اینترنت متصل می‌شوند اسکریپت‌های Coinhive که وظیفه آنها استخراج ارز رمز با استفاده از منابع سخت‌افزاری دستگاه کاربر است تزریق شود.

امنیت بسترهای ابری نیز همچنان موضوعی چالش برانگیز است. بهره‌گیری از فناوری Container، انتشار برنامه‌ها را در بسترهای ابری به‌نحوی موثر سرعت می‌بخشد. اما حملاتی را شاهد هستیم که مهاجمان با جاسازی Container دستکاری شده در بستر ابری سازمان، از آنها برای رمزربایی بهره‌گیری می‌کنند.

در بخش آمار، روند تغییر تعداد انواع تهدیدات سایبری در طی دو سال گذشته ارائه شده است. در سه‌ماهه دوم سال ۲۰۱۸، شرکت مک‌آفی به‌طور میانگین در هر روز ۴۹ میلیارد درخواست را پردازش و تحلیل کرده است. با این حال تعداد بدافزارهای جدید برای دومین بار در یک سال اخیر روندی کاهشی داشته است. اگر چه با توجه به افزایش خارج از معمول بدافزارهای جدید در سه‌ماهه چهارم ۲۰۱۷ نمی‌توان این روند کاهشی را نشانه‌ای از بهبود اوضاع دانست. آمار بدافزارهای موبایلی نیز در سه‌ماهه دوم ۲۰۱۸، ۲۷ درصد افزایش را در مقایسه با دوره قبل نشان می‌دهد. این سومین دوره پیاپی است که این بدافزارها سیری صعودی داشته‌اند.

در این گزارش به برخی از تحقیقات صورت پذیرفته توسط آزمایشگاه‌های مک‌آفی در سه‌ماهه دوم ۲۰۱۸ نیز اشاره شده است.

۱ Ransomware
۲ Cryptojacking
۳ Mine
۴ Internet of Things - IoT

Cyber

EVENTS

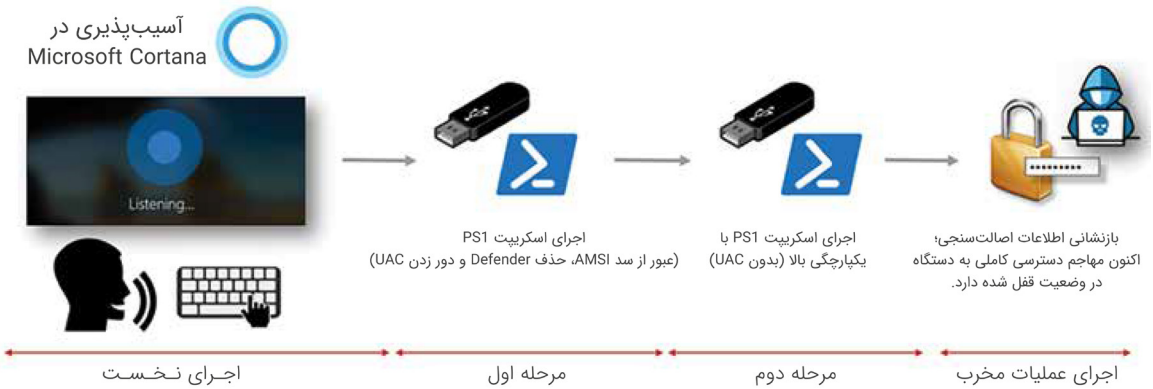
چند رویداد سایبری

داستان کشف یک آسیب‌پذیری

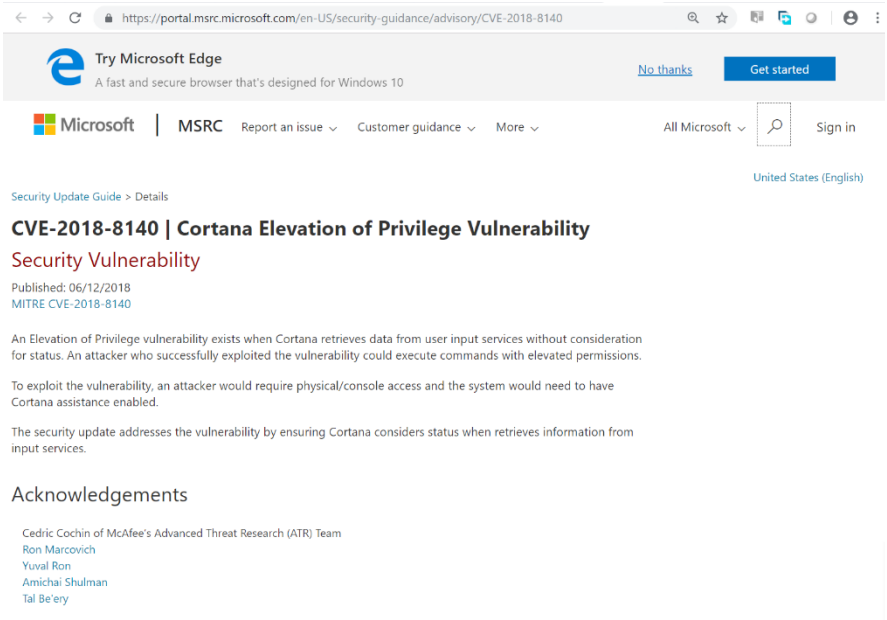
می‌خواهید به دستگاهی که Windows آن در وضعیت قفل شده قرار دارد متصل شوید؟ از Cortana بپرسید!

در ماه آوریل، محققان مک‌آفی، وجود یک ضعف امنیتی را در دستیار صوتی Cortana در Windows 10 به شرکت مایکروسافت گزارش کردند. آسیب‌پذیری مذکور، به مهاجم امکان می‌دهد حتی در صورت قفل بودن سیستم عامل، به دستگاه متصل شده و کد مورد نظر خود را بر روی آن به اجرا در آورد.

شکل زیر مراحل بهره‌جویی از این آسیب‌پذیری را به تصویر کشیده است.



در پی اعلام موضوع توسط مک‌آفی، مایکروسافت در ماه ژوئن با عرضه اصلاحیه امنیتی، ضعف مذکور را ترمیم و اصلاح کرد.


https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8140

Try Microsoft Edge
A fast and secure browser that's designed for Windows 10
No thanks | Get started

Microsoft | MSRC | Report an issue | Customer guidance | More | All Microsoft | Sign in

United States (English)

Security Update Guide > Details

CVE-2018-8140 | Cortana Elevation of Privilege Vulnerability

Security Vulnerability

Published: 06/12/2018
MITRE CVE-2018-8140

An Elevation of Privilege vulnerability exists when Cortana retrieves data from user input services without consideration for status. An attacker who successfully exploited the vulnerability could execute commands with elevated permissions.

To exploit the vulnerability, an attacker would require physical/console access and the system would need to have Cortana assistance enabled.

The security update addresses the vulnerability by ensuring Cortana considers status when retrieves information from input services.

Acknowledgements

Cedric Cochin of McAfee's Advanced Threat Research (ATR) Team
Ron Marcovich
Yuval Ron
Amichai Shulman
Tal Be'ery

مشروح گزارش مک‌آفی در لینک زیر قابل دریافت و مطالعه است:

https://securingtomorrow.mcafee.com/mcafee-labs/want-to-break-into-a-locked-windows-10-device-ask-cortana-/cve-2018-8140

Exploit ◦

چالش‌های زنجیره بلوکی

در اوایل امسال، محققان از شناسایی آسیب‌پذیری‌هایی در زنجیره بلوکی ارز رمز EOS خبر دادند که بهره‌جویی از آنها مهاجم را قادر به در اختیار گرفتن کنترل دستگاه عضو زنجیره می‌کند. در بهمن ماه سال گذشته نیز در جریان حمله‌ای سایبری مهاجمان موفق به سرقت ارزمرز NEM به ارزش ۵۳۲ میلیون دلار از صرافی کوین‌چک شدند. در طی ماه‌های اخیر کم نیستند اخباری مشابه این دو خبر که در آنها به هدف قرار گرفتن ارز رمزها و زنجیره بلوکی توسط مهاجمان اشاره شده است.

زنجیره بلوکی چیست؟

حتی اگر نام زنجیره بلوکی را هم نشنیده باشید به احتمال زیاد ارز رمز بیت‌کوین برای شما نامی آشناست. در اواخر سال ۲۰۱۷، افزایش ارزش بیت‌کوین و رسیدن آن به ۲۰ هزار دلار، توجه بسیاری از افراد از جمله تبهکاران سایبری را به خود جلب کرد. اساس کار ارز رمزها مفهومی با عنوان زنجیره بلوکی است. زنجیره بلوکی یک دفتر کل توزیع شده و مبتنی بر اجماع است که به‌صورت مستمر فهرستی از رکوردها را که هرکدام به گزینه‌های قبلی فهرست ارجاع می‌دهند حفظ می‌کند و بدین‌وسیله در برابر بازنگری غیرمجاز ایمن می‌شود. زنجیره بلوکی را می‌توان نوعی پایگاه داده دانست که بجای تمرکز اطلاعات آن بر روی یک یا چند سرور بر روی تمام دستگاه‌های متصل به شبکه که از آن با عنوان گره یا Node یاد می‌شود، توزیع شده است.

حملات زنجیره بلوکی

در چند ماه گذشته، مهاجمان با بهره‌گیری از روش‌های مختلف کاربران و سازمان‌های بسیاری را با محوریت ارز رمز هدف حملات خود قرار داده‌اند. برای مثال در اوایل سال میلادی جاری، یک مهاجم با راه‌اندازی سایتی فیشینگ موفق شد تا در مدت کمتر از شش ماه ارز رمزهای IOTA با ارزش نزدیک به ٤ میلیون دلار را از کاربران سرقت کند. ضمن اینکه آمار متعدد از تغییر رویکرد بسیاری از ویروس‌نویسانی حکایت دارد که تا اندکی پیش تمام تمرکز خود را بر روی ساخت باج‌افزار گذاشته بودند. ویروس‌نویسانی که با پی بردن به بازده بالای ابزارهای معروف به استخراج‌کننده ارز رمز، ساخت و انتشار بدافزارهایی مبتنی بر این ابزارها را که به رمز ربا معروف شده‌اند در کانون اهداف مخرب خود قرار داده‌اند. بهره‌جویی از آسیب‌پذیری‌های امنیتی از دیگر روش‌های مورد استفاده مهاجمان برای منفعت جستن از ارز رمزهاست. برای نمونه، وجود آسیب‌پذیری‌هایی امنیتی در معماری ارزمرز Verge مهاجمان را قادر به ایجاد ارز رمزهای جدید بدون صرف هر گونه هزینه بر روی فرآیند استخراج کرد. همچنین اجرای حملات موسوم به Majority هر چند در نگاه اول بسیار دشوار به نظر می‌آید اما بررسی‌ها حاکی از اجرای موفق چنین حملاتی توسط مهاجمان بر ضد ارز رمزهای نه چندان متداولی نظیر Krypton است. حملات مبتنی بر لغت‌نامه، دیگر تهدید رایج بر ضد زنجیره بلوکی است. در اکثر این موارد این بی‌احتیاطی کاربران در انتخاب رمزهای عبور پیچیده است که اجرای موفق چنین حملاتی را برای مهاجمان ممکن می‌سازد. ضمن اینکه علیرغم هشدار بسیاری از کارشناسان امنیتی در خصوص آسیب‌پذیر بودن کیف‌های موسوم به Brainwallet به حملات مبتنی به لغت‌نامه، همچنان بسیاری از کاربران ارز رمز از این نوع کیف استفاده می‌کنند. صرافی‌های ارز رمز یکی دیگر از بازیگران اصلی در زنجیره بلوکی و در نتیجه از اصلی‌ترین اهداف مهاجمان سایبری هستند که به یکی از نمونه‌های آن در ابتدای این مطلب اشاره شد. ارز رمزها و زنجیره بلوکی از فناوری های نوین در دنیای امروز هستند. محققان بخش تحقیقات پیشرفته تهدیدات در شرکت مک‌آفی گزارشی با عنوان Blockchain Threat Report منتشر کرده‌اند که در آن به تفصیل به بررسی تهدیدات جاری بر ضد ارز رمزها و زنجیره بلوکی پرداخته شده است. این گزارش در لینک زیر قابل دریافت و مطالعه است.

https://newsroom.shabakeh.net/wp-content/uploads/2018/06/rp-blockchain-security-risks.pdf

٦ Cryptocurrency
٧ Blockchain

روترهای میکروتیک در تسخیر رمز رباها

چندین ماه است که مهاجمان با رخنه به روترهای میکروتیک، اسکریپت‌های استخراج‌کننده ارز رمز را بر روی دستگاه‌های متصل به این روترها به اجرا در می‌آورند. این حملات که به‌نظر می‌رسد در ابتدا محدود به کشور برزیل بوده به سرعت دامنه آنها به کشورهای مختلف جهان از جمله ایران گسترش پیدا کرده است.

نفوذگران با آلوده نمودن دستگاه میکروتیک سبب می‌گردند تا در صفحات فراخوانی شده در مرورگر کاربرانی که در سطح شبکه از طریق این تجهیزات به اینترنت متصل می‌شوند اسکریپت‌های Coinhive که وظیفه آنها استخراج ارز رمز با استفاده از منابع سخت‌افزاری دستگاه کاربر است تزریق شود.

جالب اینکه به‌منظور کاهش حساسیت و شک کاربران به افزایش پردازش‌های صورت گرفته بر روی دستگاه – در نتیجه اسکریپت‌های اجرا شده -، عملیات تزریق صرفا محدود به صفحات حاوی پیام‌های خطا – از هر نوع – شده است.

با این حال با در نظر گرفتن تعداد حداقل ده‌ها هزار روتر آلوده و با فرض اینکه هر یک از آنها ده‌ها و شاید صدها کامپیوتر را به اینترنت متصل می‌کنند می‌توان نتیجه‌گیری کرد که حتی با این روش محدودسازی، همچنان سود سرشاری نصیب گردانندگان این حملات می شود.

در حملات مذکور از یک آسیب‌پذیری حیاتی در بخش Winbox روترهای ساخت میکروتیک بهره‌جویی می‌شود. شرکت میکروتیک اصلاحیه این آسیب‌پذیری را در ماه آوریل عرضه کرد. اما تعداد بسیار بالای روترهای آلوده بیانگر عدم نصب اصلاحیه توسط بسیاری از راهبران تجهیزات میکروتیک است.

لازم به ذکر است، مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای کشور (ماهر) در چندین نوبت نسبت به اجرای حملات گسترده بر ضد روترهای میکروتیک در سطح کشور هشدار داده است.

PooleZoor،
نمونه‌ای از باج‌افزارهای فارسی

در اواسط تابستان، منابع مختلف از شناسایی باج‌افزاری خبر دادند که پس از رمزگذاری فایل‌های کاربر با الگوریتم AES به آنها پسوند poolezoor را الصاق می‌کند.

این باج‌افزار بر پایه پروژه کد باز HiddenTear توسعه داده شده است.

نکته جالب در خصوص باج‌افزار PooleZoor، درج یک جمله انگلیسی و دو جمله فارسی با نویسه‌های انگلیسی در اطلاعیه باج‌گیری آن با نام READ_me_for_encrypted_Files.txt و با متن زیر است.

Files has been encrypted with PooleZoor

Ba pardakht 10,000,000 Riyal File hay khod ra bazgardanid

In Pool sarf omre kheyriye khahad shod

```
public void messageCreator()
{
    string userName = Environment.UserName;
    string str = "C:\\Users\\";
    string str2 = "\\Desktop\\READ_me_for_encrypted_Files.txt";
    string path = str + userName + str2;
    string[] contents = new string[]
    {
        "Files has been encrypted with PooleZoor",
        "Ba pardakht 10,000,000 Riyal File hay khod ra bazgardanid",
        "In Pool sarf omre kheyriye khahad shod"
    };
    File.WriteAllLines(path, contents);
}
```

در بخشی از کد این باج‌افزار نیز به رمز عبور "Amir12345" اشاره شده است.

```
public void startAction()
{
    string userName = Environment.UserName;
    string str = "C:\\Users\\";
    string password = "Amir12345";
    string str2 = "\\Desktop\\";
    string location = str + userName + str2;
    this.encryptDirectory(location, password);
    this.messageCreator();
    Application.Exit();
}
```

برخی منابع، وبلاگ http://ransomware-poolezoor.blogspot.com را که دیگر در سامانه Blogger قابل دسترس نیست به نویسنده یا نویسندگان این باج‌افزار نسبت داده‌اند. شکل زیر تصویری از این وبلاگ را پیش از حذف شدن نمایش می‌دهد.

متن درج شده در وبلاگ به شرح زیر است:

"برای اینکه مارو حمایت بکنید مبلغ یک میلیون تومان به ما پرداخت و برای ما ارسال کنید و در جواب ایمیل شما ما Decryptor را در اختیار شما قرار می دهیم.

نحوه پرداخت:

ورود به لینک: /http[:///]sep.shapaarak.cf

تصویر پرداخت خود را در زیر این پست به همراه ادرس ایمیل خود برای ما ارسال نمائید."

نشانی استفاده شده در متن مذکور، سایتی فیشینگ است که هدف آن کلاهبرداری و سرقت اطلاعات بانکی کاربر است. بنابراین در صورت مراجعه قربانی به سایت مذکور و وارد کردن اطلاعات کارت بانکی در آن نه فقط ابزار رمزگشایی در اختیار او قرار نمی‌گیرد که تمام اطلاعات بانکی وارد شده نیز در خدمت نویسنده یا نویسندگان PooleZoor قرار خواهد گرفت.

PooleZoor تنها یک نمونه از باج‌افزارهایی است که هدف آنها بطور خاص کاربران ایرانی است. این باج‌افزارها معمولا با عنوان "باج‌افزار فارسی" شناخته می‌شوند.

آمـــــار

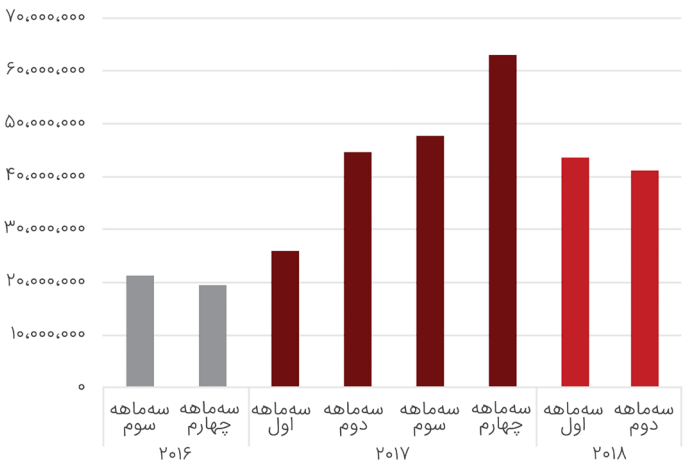
فناوری McAfee Global Threat Intelligence – به اختصار McAfee GTI –، به‌طور میانگین، در هر روز ۴۹ میلیارد درخواست و ۱۳ میلیارد خط دوری‌سنجی (Telemetry) را در سرتاسر جهان دریافت و پردازش کرده و ۱،۸۰۰،۰۰ نشانی اینترنتی و ۸۰۰،۰۰۰ فایل را به همراه ۲۰۰،۰۰۰ فایل در قرنطینه امن (Sandbox) را مورد تحلیل قرار می‌دهد.

بررسی آمار این فناوری در سه‌ماهه دوم سال ۲۰۱۸ نتایج زیر را در بر داشته است:

- از بین ۸۶ میلیون فایل بررسی شده توسط McAfee GTI، ۸۶ هزار مورد (۰/۱ درصد) بالقوه مخرب گزارش شده است.
- از بین ۷۳ میلیون، نشانی URL تحلیل شده توسط McAfee GTI، ۳۶۵ هزار مورد (۰/۵ درصد) با ریسک بالا تشخیص داده شده است.
- از بین ۶۷ میلیون، نشانی IP ارزیابی شده، ۲۶۸ هزار مورد (۰/۴ درصد) بالقوه مخرب گزارش شده است.

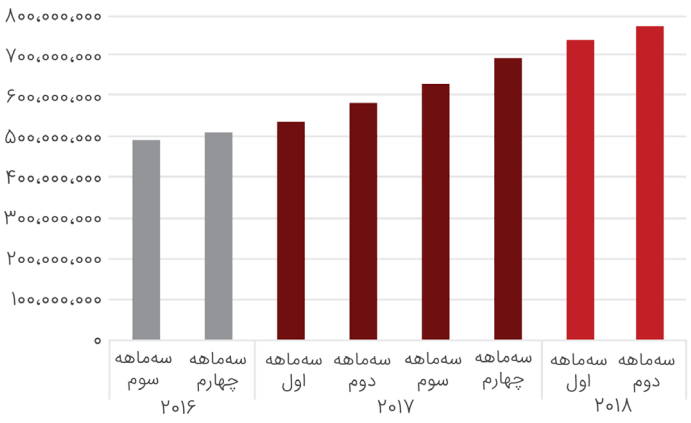
بـدافـزارهـا

بدافزارهای جدید



منبع: McAfee Labs Threats Report

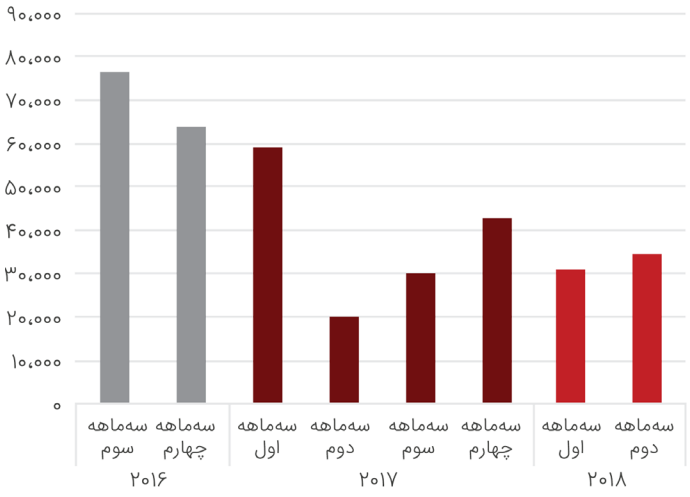
مجموع کل بدافزارها



منبع: McAfee Labs Threats Report

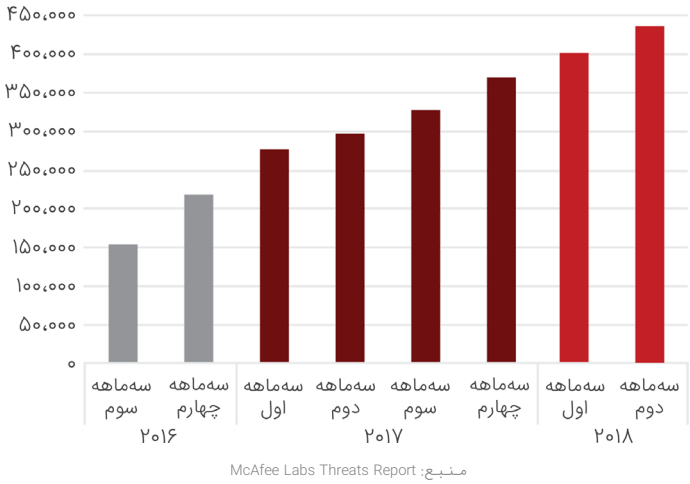
در سه‌ماهه دوم ۲۰۱۸، به‌طور میانگین، در هر ثانیه، پـنـج بدافزار منحصربه‌فرد جـدیـد به دست آزمایشگاه‌های McAfee رسیده است. تعداد کـل بـدافـزارهـا در این دوره به حدود ۷۹۰ میلیون عدد رسیده است.

بدافزارهای جدید Mac



منبع: McAfee Labs Threats Report

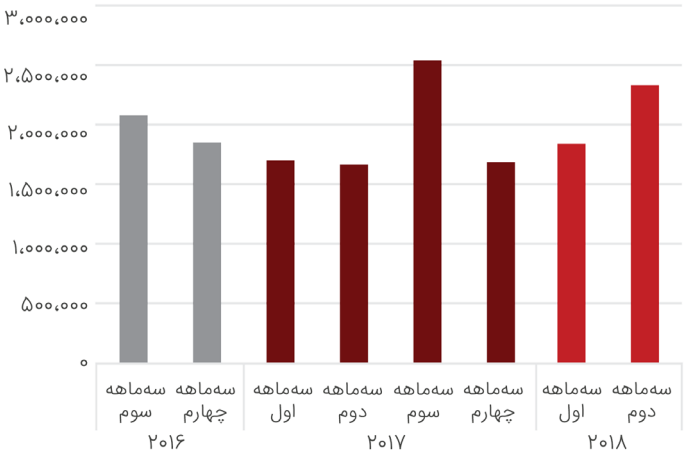
مجموع کل بدافزارهای Mac



منبع: McAfee Labs Threats Report

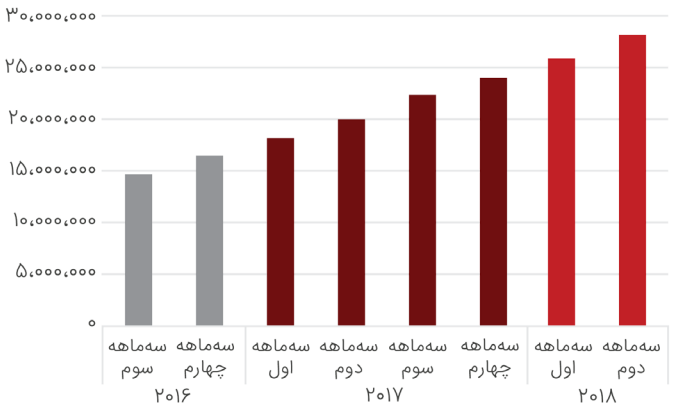
در سه‌ماهه دوم سال ۲۰۱۸، بیش از ۳۰ هزار نمونه منحصربه‌فرد جدید از بدافزارهای ویژه سیستم عامل MacOS کشف و شناسایی شده است. تعداد کل بدافزارهای سازگار با MacOS نیز از مرز ٤٤٠ هزار عدد عبور کرده است.

بدافزارهای جدید دستگاه‌های همراه



منبع: McAfee Labs Threats Report

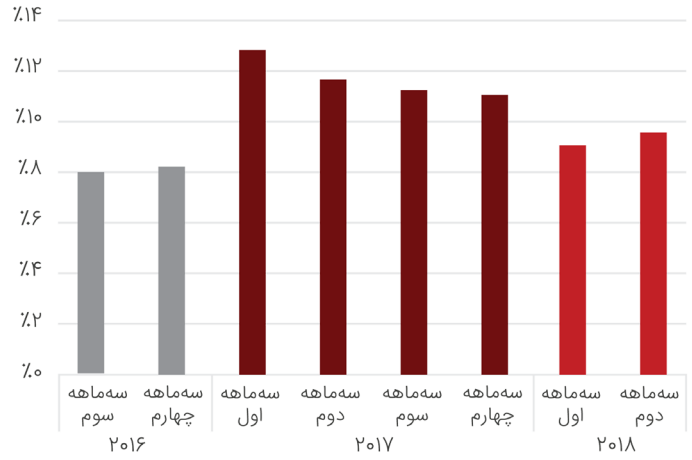
مجموع کل بدافزارهای دستگاه‌های همراه



منبع: McAfee Labs Threats Report

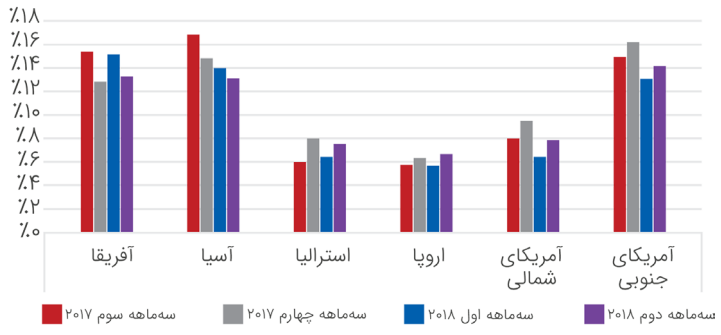
آمار بدافزارهای دستگاه‌های همراه در سه‌ماهه دوم ۲۰۱۸، ۲۷ درصد افزایش را در مقایسه با دوره قبل نشان می‌دهد. این سومین دوره پیاپی است که این بدافزارها سیری صعودی داشته‌اند.

نرخ آلودگی جهانی به بدافزارهای دستگاه‌های همراه

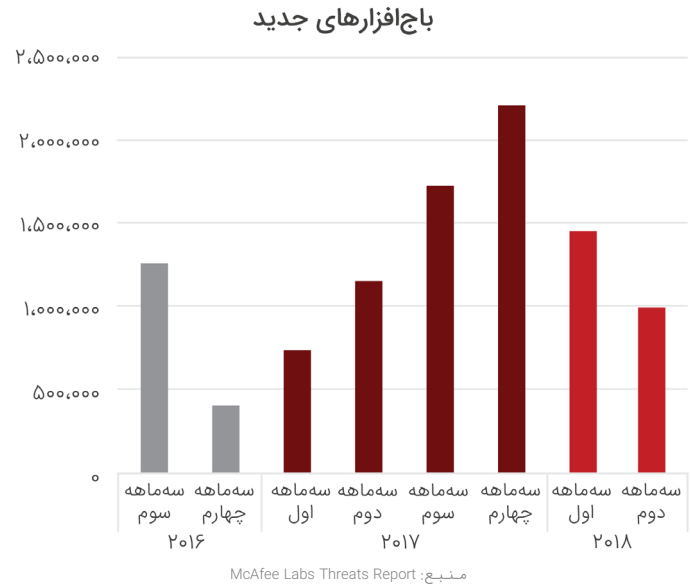


منبع: McAfee Labs Threats Report

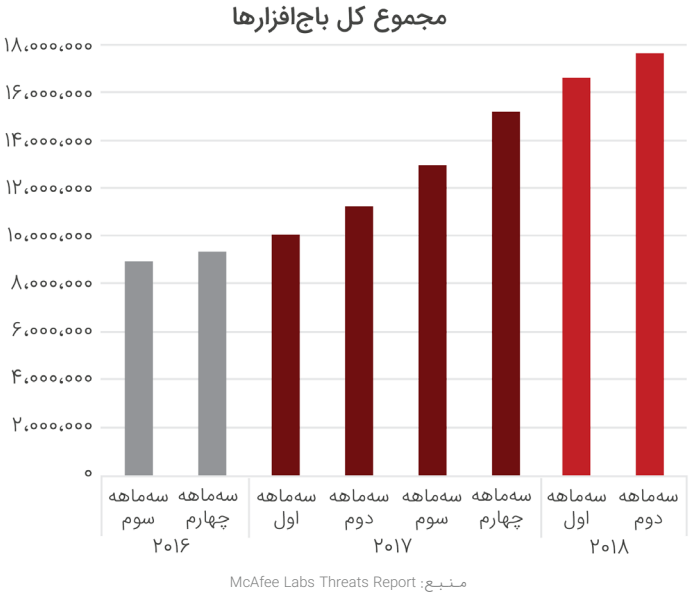
نرخ آلودگی به بدافزارهای دستگاه‌های همراه به تفکیک منطقه



منبع: McAfee Labs Threats Report



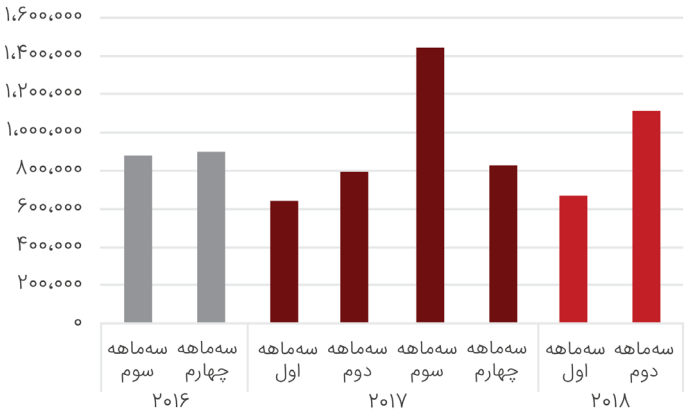
منبع: McAfee Labs Threats Report



منبع: McAfee Labs Threats Report

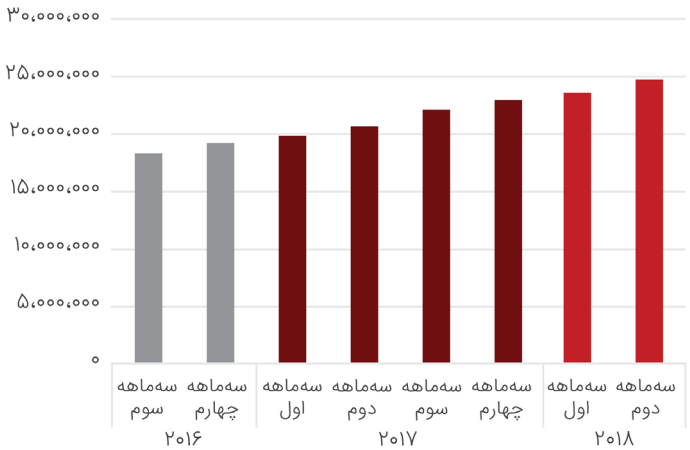
در این دوره تعداد آلودگی‌ها به باج‌افزار Scarab که نخستین نسخه از آن در ژوئن سال میلادی گذشته کشف و شناسایی شد به‌طور قابل توجهی افزایش داشته است. به‌نحوی که نسخه‌های اخیر آن روی هم رفته سهمی بیش از ۵۰ درصد از کل نمونه‌های Scarab را تا به امروز به خود اختصاص داده‌اند.

کدهای مخرب دودویی امضا شده جدید



منبع: McAfee Labs Threats Report

مجموع کل کدهای مخرب دودویی امضا شده

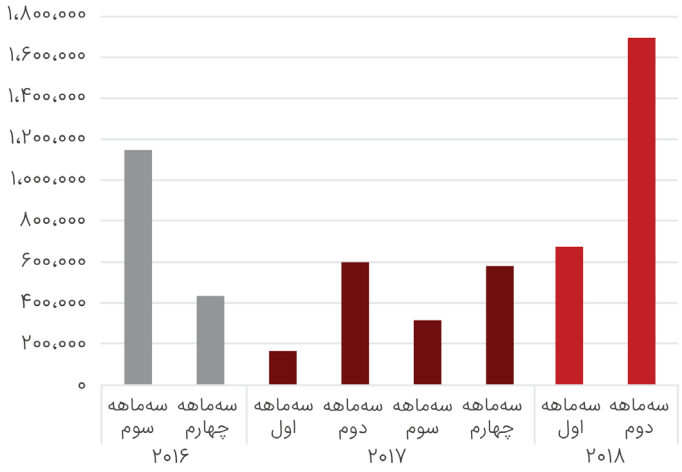


منبع: McAfee Labs Threats Report

مراجع صدور گواهی[۸] از طریق گواهینامه‌های دیجیتال[۹] امکان ارائه اطلاعات در خصوص کدهای دودویی[۱۰] (برنامه[۱۱]) امضا شده را فراهم می‌کنند. بسیاری از محصولات ضدویروس برنامه‌های امضا شده[۱۲] 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.

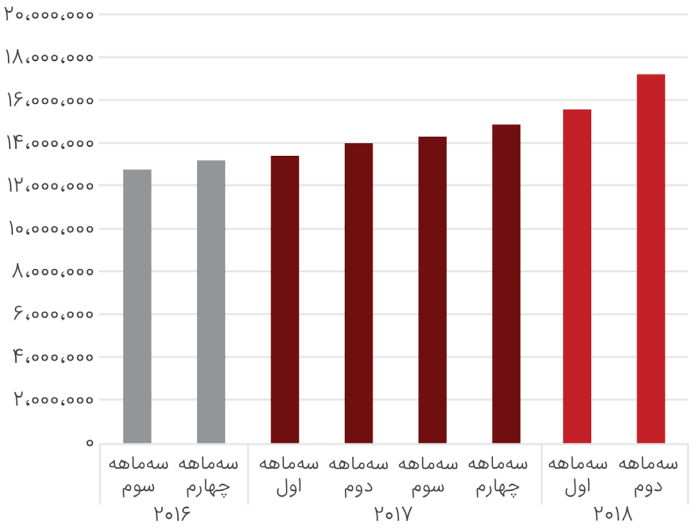
۸ Certificate Authority
۹ Digital Certificate
۱۰ Binary
۱۱ Application
۱۲ Signed

بدافزارهای جدید بهره‌جو



منبع: McAfee Labs Threats Report

مجموع کل بدافزارهای بهره‌جو

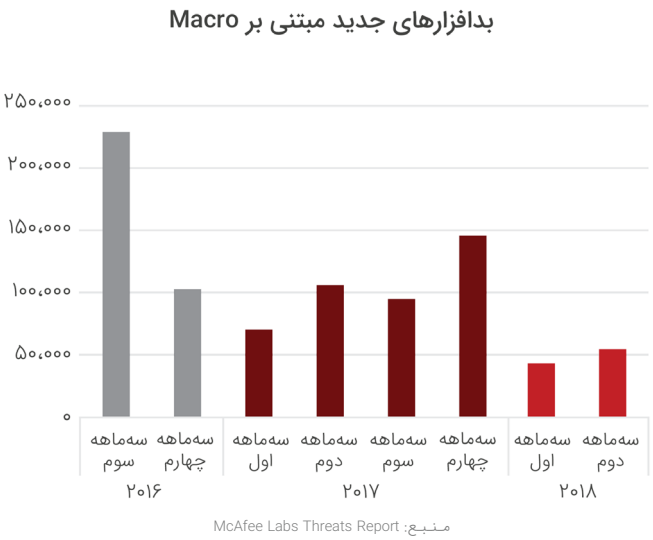


منبع: McAfee Labs Threats Report

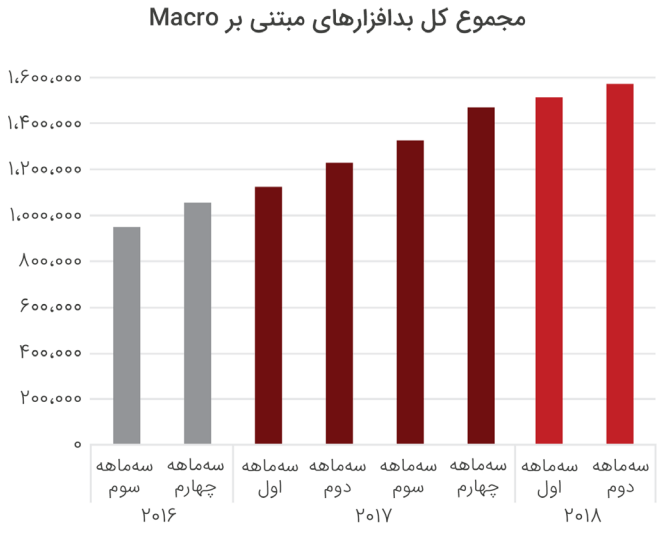
سواستفاده از آسیب‌پذیری‌های امنیتی[۱۳] در سیستم عامل و نرم‌افزارهای کاربردی یکی از روش‌های نفوذ به اهداف و انتشار بدافزار توسط مهاجمان حرفه‌ای است. وجود یک آسیب‌پذیری حیاتی می‌تواند سبب دور زدن قوی‌ترین محصولات ضدویروس یا دیواره‌های آتش توسط بدافزارها و ابزارهای موسوم به بهره‌جو شود. بدافزارهای بهره‌جو در سه‌ماهه دوم سال میلادی جاری افزایشی ۱۵۱ درصدی داشته‌اند.

[۱۳] Security Vulnerability

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

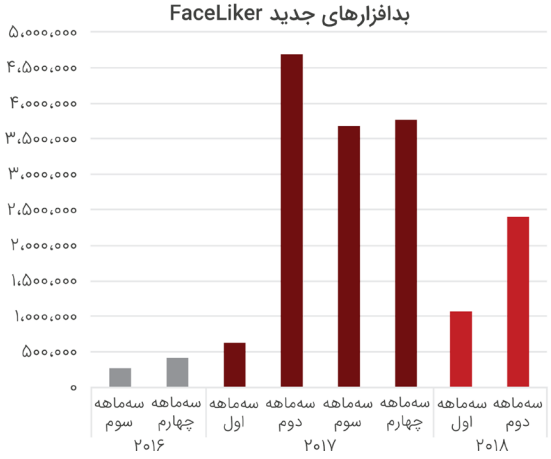


منبع: McAfee Labs Threats Report



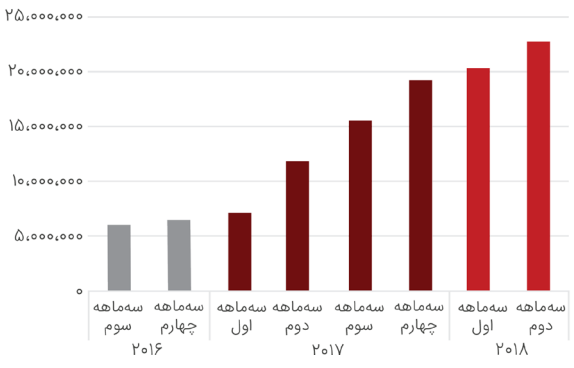
منبع: McAfee Labs Threats Report

بدافزارهای جدید FaceLiker



منبع: McAfee Labs Threats Report

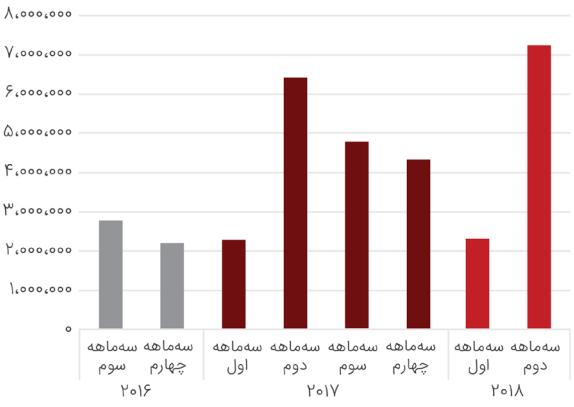
مجموع کل بدافزارهای FaceLiker



منبع: McAfee Labs Threats Report

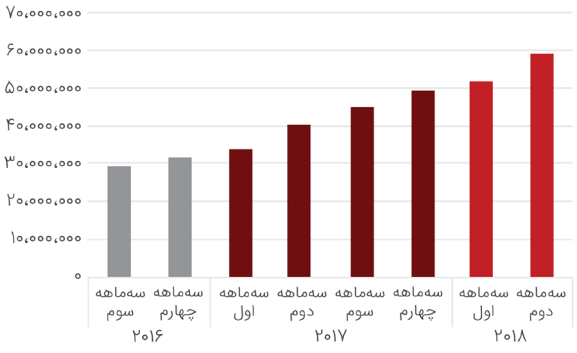
اسب‌های تروای موسوم به FaceLiker با بهره‌گیری از کلیک‌های انجام شده در شبکه اجتماعی Facebook سبب افزایش تعداد "می‌پسندم"[۱۴] برای محتواهای خاص می‌شوند.

بدافزارهای جدید مبتنی بر JavaScript



منبع: McAfee Labs Threats Report

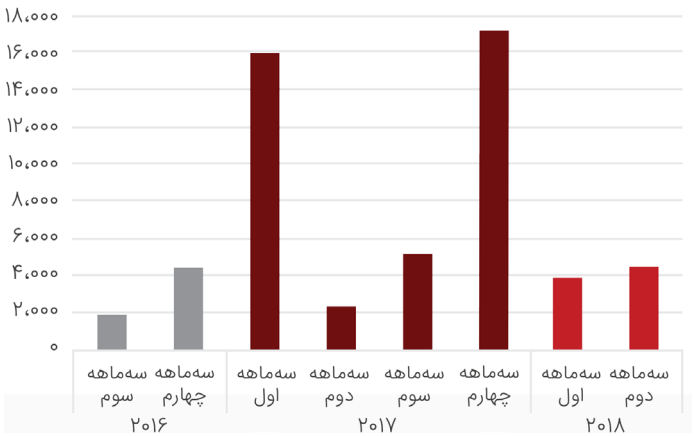
مجموع کل بدافزارهای مبتنی بر JavaScript



منبع: McAfee Labs Threats Report

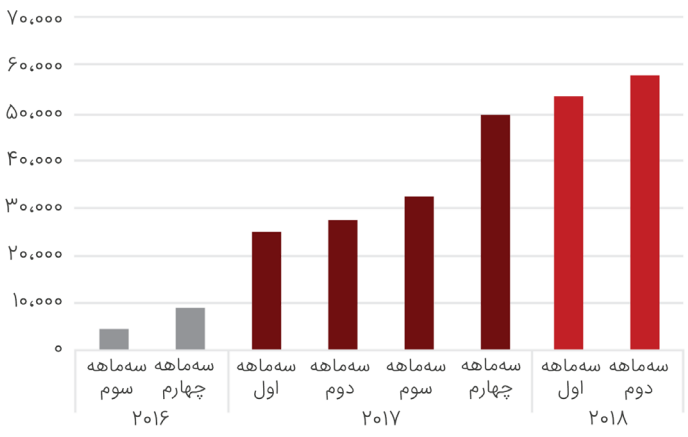
[۱۴] Like

بدافزارهای جدید مبتنی بر PowerShell



منبع: McAfee Labs Threats Report

مجموع کل بدافزارهای مبتنی بر PowerShell

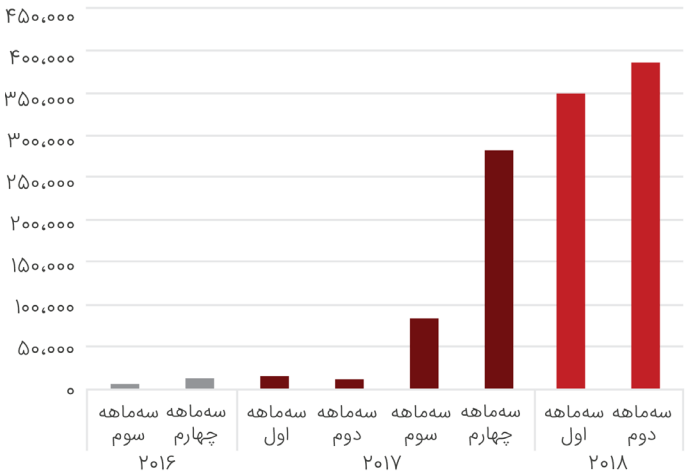


منبع: McAfee Labs Threats Report

یکی از روش‌های پیشرفته ویروس‌نویسان حرفه‌ای در طی دو سال گذشته استفاده از روشی موسوم به "بدون فایل"[۱۵] بوده که در آن با بهره‌گیری از فایل مجاز 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.

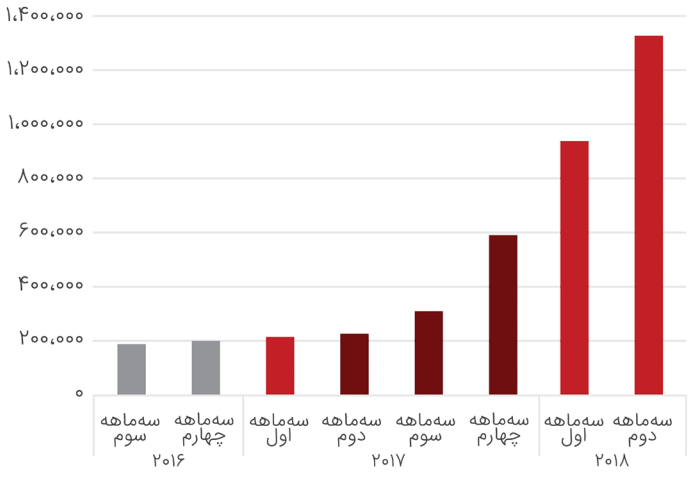
[۱۵] Fileless

بدافزارهای جدید مبتنی بر LNK



منبع: McAfee Labs Threats Report، ژوئن ۲۰۱۸

مجموع کل بدافزارهای مبتنی بر LNK

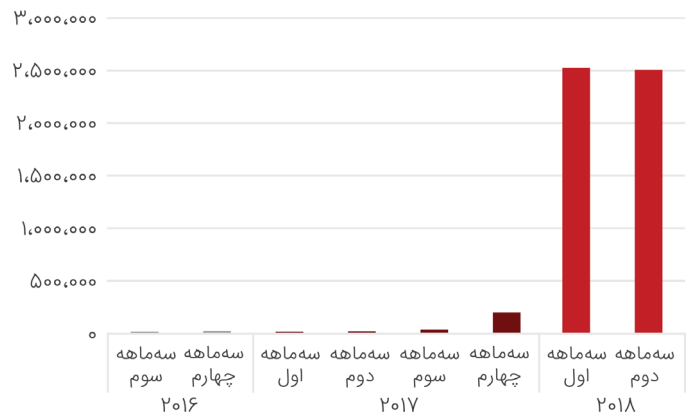


منبع: McAfee Labs Threats Report

نویسندگان بدافزار به‌شدت در حال استفاده از میانبرهای[۱۶] موسوم به LNK برای اجرای مخفیانه کدها و اسکریپت‌های مخرب خود بر روی دستگاه‌های با سیستم عامل Windows هستند.

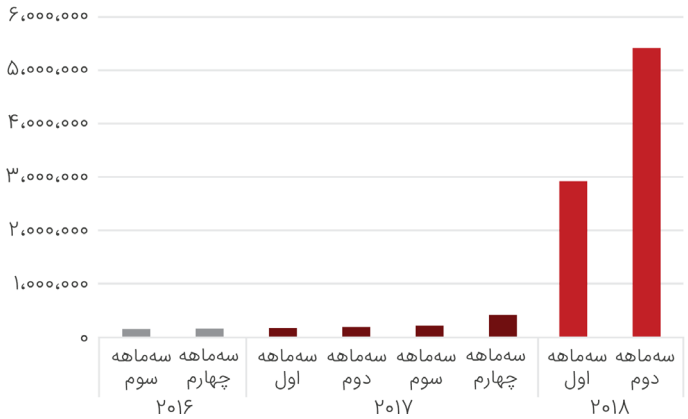
[۱۶] Shortcut

بدافزارهای جدید استخراج‌کننده ارز رمز



منبع: McAfee Labs Threats Report

مجموع کل بدافزارهای استخراج‌کننده ارز رمز

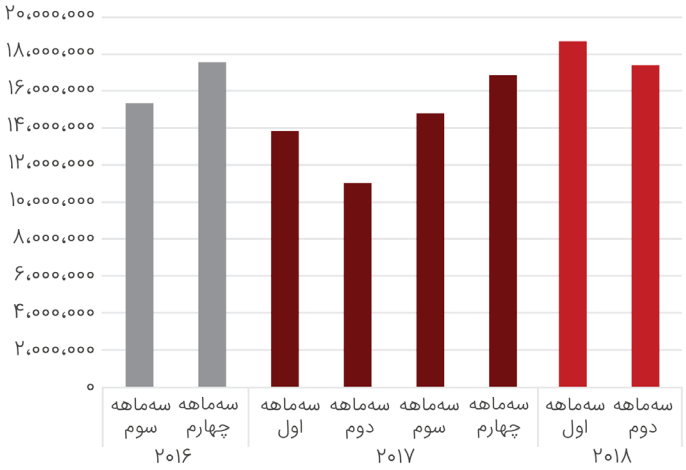


منبع: McAfee Labs Threats Report

در ارز رمزها، فرآیندی با عنوان استخراج وجود دارد که یکی از اصلی‌ترین وظایف آن تایید اطلاعات تبادل شده در شبکه این واحدهای پولی است. فرآیند استخراج مستلزم فراهم بودن توان پردازشی بسیار بالاست. در نتیجه شبکه ارز رمز نیز در قبال تلاشی که برای این پردازش‌ها انجام می‌شود به استخراج‌کنندگان پاداشی اختصاص می‌دهد. از همین رو، برخی افراد نیز با بکارگیری برنامه‌های موسوم به استخراج‌کننده تلاش می‌کنند تا در ازای استخراج ارز رمز، مشمول پاداش شبکه واحد دیجیتال شوند. اما با توجه به نیاز به توان پردازش بالا، انجام استخراج می‌تواند یک سرمایه‌گذاری هزینه‌بر برای استخراج‌کننده باشد. به همین خاطر در حملات موسوم به Cryptojacking، استخراج‌کننده بدخواه با آلوده نمودن دستگاه دیگران به بدافزارهای ویژه استخراج، از توان پردازشی آنها به نفع خود بهره‌گیری می‌کند. بدافزارهای استخراج‌کننده ارز رمز در سه‌ماهه دوم سال میلادی جاری افزایشی ۸۶ درصدی داشته‌اند.

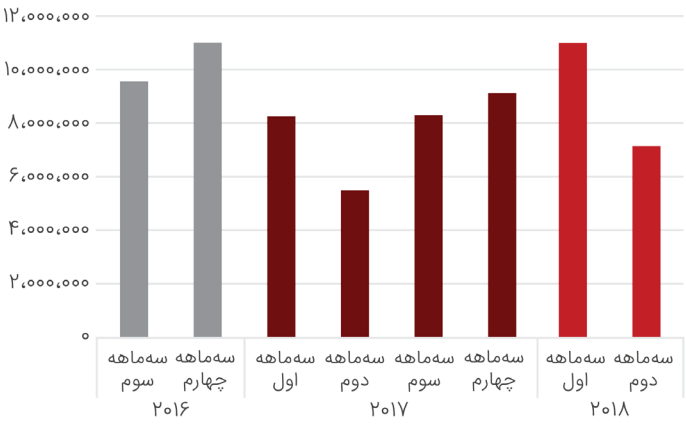
تهدیدات تحت وب و شبکه

نشانی‌های URL مشکوک جدید



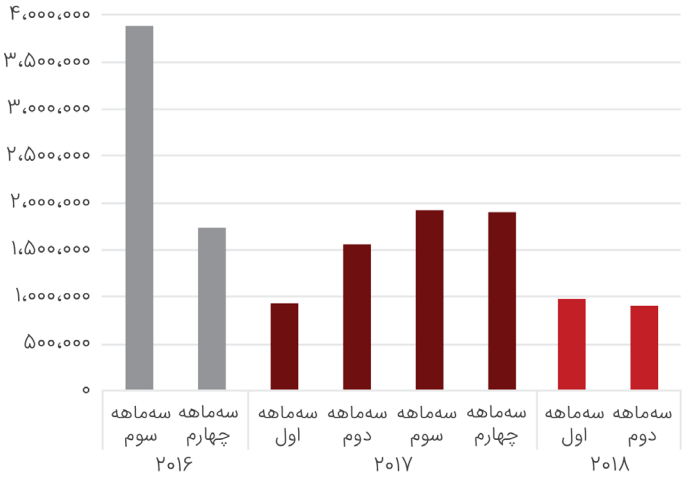
منبع: McAfee Labs Threats Report

نشانی‌های URL مخرب جدید



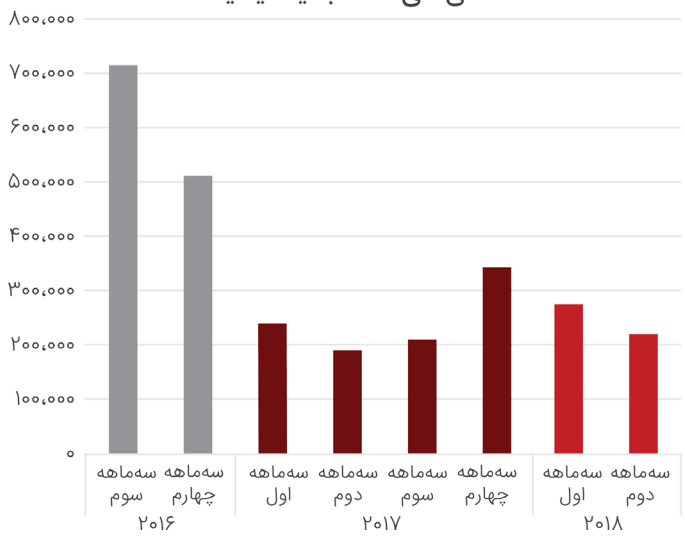
منبع: McAfee Labs Threats Report

نشانی‌های URL جدید، مربوط به دریافت‌های مخرب



منبع: McAfee Labs Threats Report

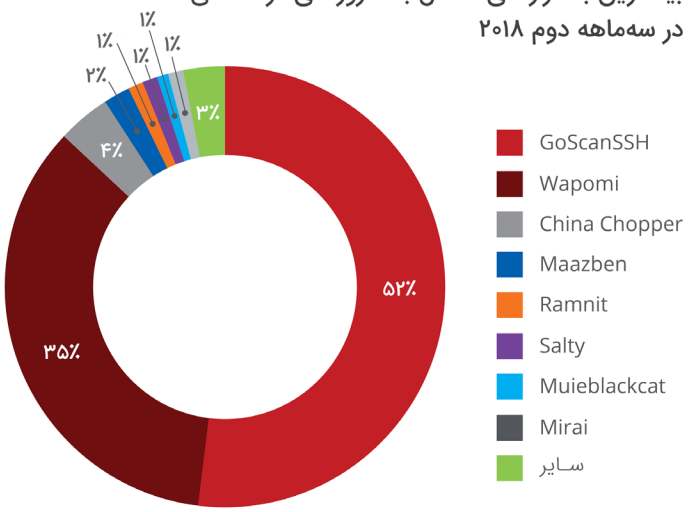
نشانی‌های URL جدید فیشینگ



منبع: McAfee Labs Threats Report

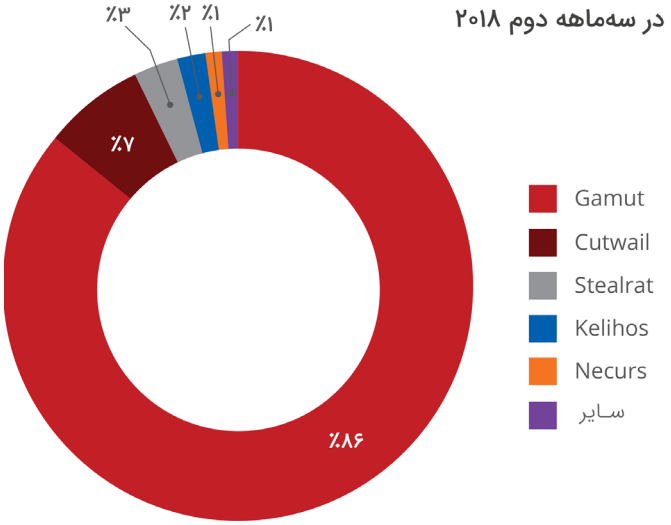
نشانی‌های URL مشکوک شامل تعداد کل سایت‌هایی است که بر اساس درجه‌بندی شرکت McAfee، امتیاز ریسک بالا یا متوسط را دریافت کرده‌اند. نشانی‌های URL مخرب نیز آن دسته از سایت‌هایی هستند که کاربر را به صفحات اینترنتی حاوی برنامه‌های مخربی همچون بدافزارها هدایت می‌کنند. همچنین دریافت‌های مخرب از سایت‌هایی سرچشمه 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.

بیشترین بدافزارهای متصل به سرورهای فرماندهی در سه‌ماهه دوم ۲۰۱۸



منبع: McAfee Labs Threats Report

بزرگترین شبکه‌های مخرب ارسال‌کننده هرزنامه در سه‌ماهه دوم ۲۰۱۸

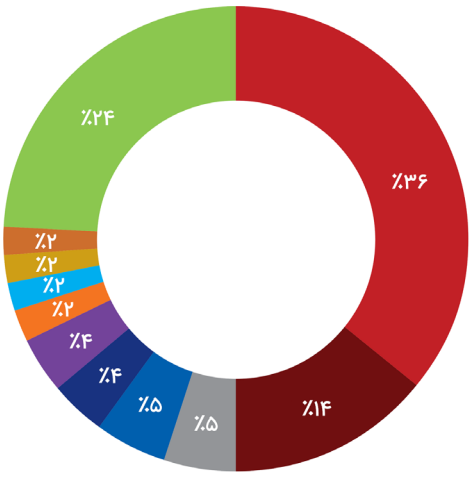


منبع: McAfee Labs Threats Report

شبکه مخرب[۱۷] Gamut در ارسال بیش از ۸۰ درصد هرزنامه‌های[۱۸] سه‌ماهه دوم ۲۰۱۸ نقش داشته است.

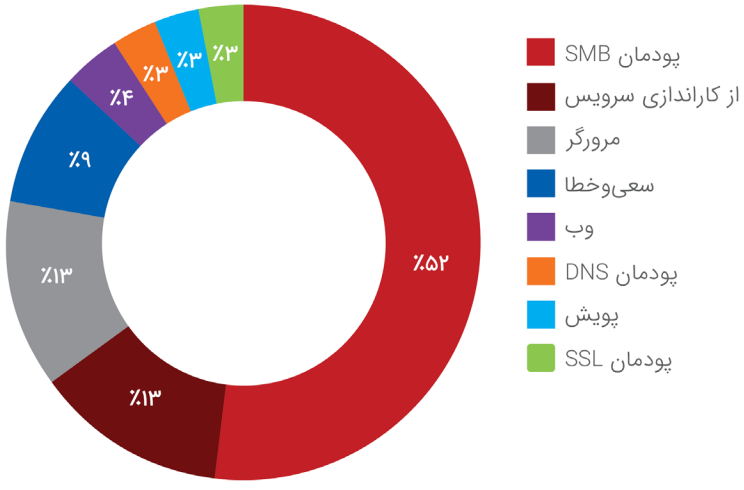
۱۷ Botnet
۱۸ Spam

کشورهای با بیشترین تعداد سرور فرماندهی شبکه‌های مخرب در سه‌ماهه دوم ۲۰۱۸



منبع: McAfee Labs Threats Report

روش‌های اصلی حمله در سه‌ماهه دوم ۲۰۱۸

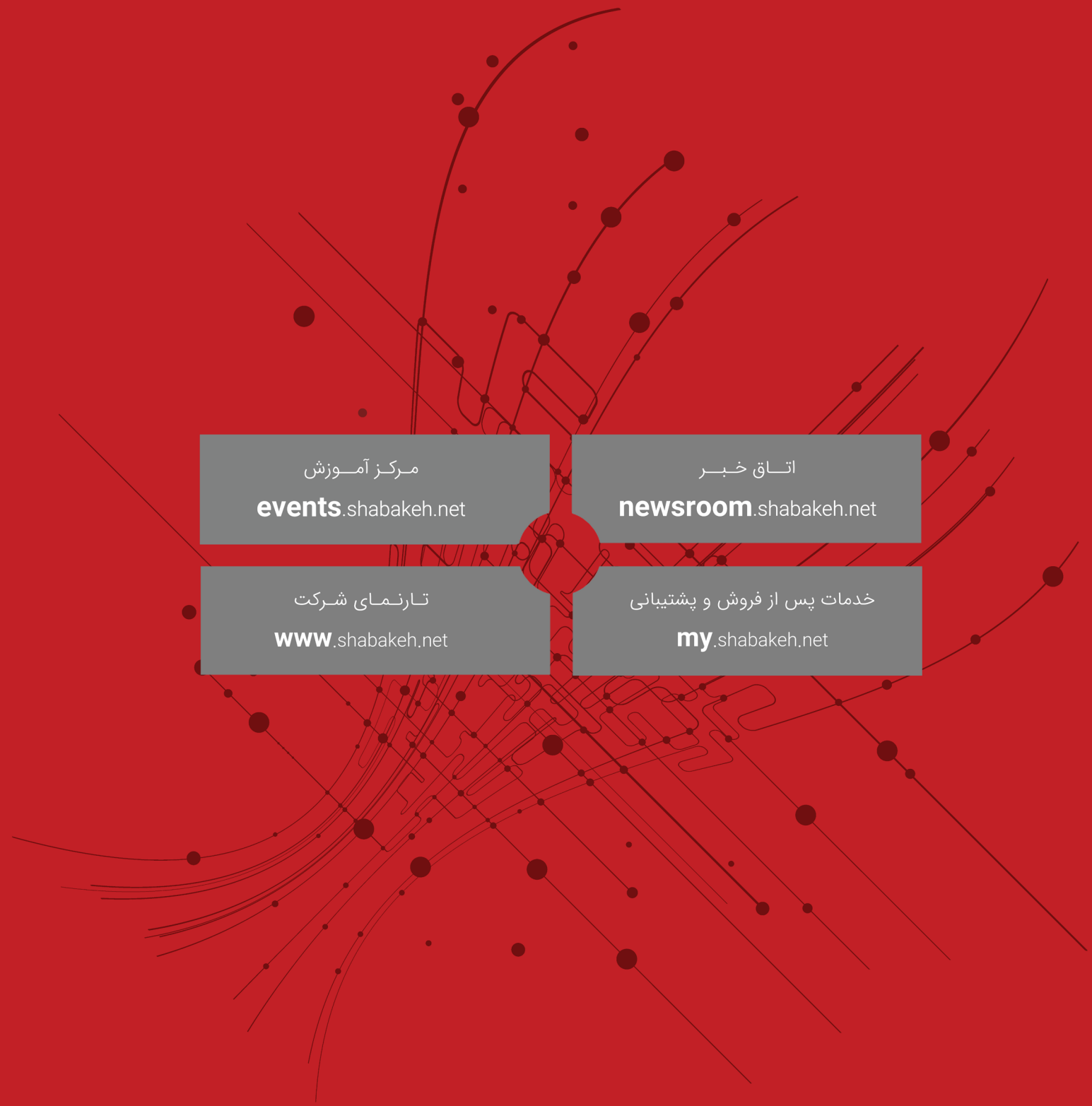


منبع: McAfee Labs Threats Report

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 ۴۲۰۵۲-۰۲۱
info@shabakeh.net
www.shabakeh.net