رویداد

موافقت اوباما با حمله سایبری گسترده به روسیه

● **خبرآنلاین:** اسناد جدید نشان می‌دهد دولت سابق آمریکا به ریاست اوباما دستور حمله سایبری گسترده به روسیه را صادر کرده بود. واشنگتن‌پست دراین‌باره نوشت: اوایل آگوست ۲۰۱۶ که سیستم انتخابات آمریکا به وسیله روس‌ها هک شد، دولت اوباما با پیاده‌سازی پروتکل امنیتی جدید با مشارکت سیا، NSA و سایر گروه‌های اطلاعاتی-امنیتی-سایبری سعی کرد دست به حمله پیشگیرانه علیه شبکه روسیه بزند. مدارک جدید نشان از چهار جلسه مداوم از روز چهارم آگوست به بعد با حضور اوباما، رئیس سیا و سایر مقامات برای ایجاد مقدمات حمله اینترنتی دارد. اوباما حتی از طریق کانال امن طراحی‌شده برای جلوگیری از مواجهه هسته‌ای به روسیه هشدار فرستاد اما مسکو یک هفته بعد دخالت خود در انتخابات آمریکا را رد کرد. ترامپ هشتم نوامبر آمد و برنامه حمله سایبری به روسیه تا دسامبر به تعویق افتاد. اوباما یک بار در سال ۲۰۰۸ از مقامات مربوطه خواست تا میزان تأثیر هکرهای روس بر سیستم انتخابات آمریکا را بررسی کنند و همان موقع با پاسخ ضعیف روبه‌رو شد که در آن تأکید شده بود که روس‌ها خیلی نمی‌توانند تأثیرگذار باشند. این منبع بیان کرده است قبل از رفتن اوباما، دولتش ۳۵ مأمور اطلاعاتی روسیه را از آمریکا اخراج کرد و روسیه را مورد تحریم قرار داد و بعدا اوباما به واحد US Cyber Command اجازه حمله را صادر کرد.

افشای ۳۲ ترابایت اطلاعات مخفی ویندوز ۱۰ در اینترنت

● **مهر:** حجم زیاد و بی‌سابقه‌ای از کدهای برنامه‌نویسی سیستم‌عامل ویندوز ۱۰ در فضای مجازی منتشر شده است. کدهای مذکور حاوی ۳۲ ترابایت داده است. براساس گزارش بیزینس اینسایدر، این کدها شامل کدهای منبع ویندوز ۱۰ و کدهای دیگری است که فقط در داخل شرکت مایکروسافت به‌طور داخلی مورد استفاده بوده‌اند. مایکروسافت بعد از تأیید این کدها، اصالت آنها را تأیید کرده است. بخشی از این کدها مربوط به سخت‌افزارهای رایانه‌های شخصی مانند درایوهای یواس‌بی، وای‌فای و بلوتوث هستند که برای کارکردن با ویندوز ۱۰ طراحی شده‌اند. کارشناسان امنیتی هشدار می‌دهند که هکرها با سوءاستفاده از کدهای نشت‌کرده به اینترنت می‌توانند آسیب‌پذیری‌های جدیدی را شناسایی کرده و از آنها برای طراحی بدافزارهای تازه به منظور سرقت اطلاعات کاربران استفاده کنند. بررسی‌ها نشان می‌دهد سرقت این کدها از شرکت مایکروسافت در ماه مارس گذشته رخ داده و اولین‌بار در سایت BetaArchive.com منتشر شده است. مدیران این سایت می‌گویند بعد از اطلاع از موضوع تمامی کدهای مذکور را پاک کرده‌اند. مایکروسافت می‌گوید احتمالا منشأ نشت این کدها برنامه‌ای موسوم به Shared Source Initiative است که مایکروسافت از آن برای به اشتراک‌گذاری کدهای منبع خود با شرکت‌های سازنده رایانه‌های شخصی و دیگر همکاران خود بهره می‌گیرد. در این مجموعه کدهای متنوعی از برخی نسخه‌های ویندوز ۱۰ که هرگز در اختیار کاربرانی در خارج از شرکت مایکروسافت قرار نگرفته‌اند، نیز مشاهده می‌شود.

رونمایی از برنامه مقابله با تبلیغات تروریستی

● **فارس:** فیس‌بوک از طرح خاصی موسوم به شهامت آنلاین مدنی در انگلیس رونمایی کرده تا هزینه مقابله با انتشار محتوای نامناسب و تروریستی در این شبکه اجتماعی تأمین شود. براساس گزارش ورج، به دنبال فشارهای گسترده دولت‌های اروپایی بر فیس‌بوک برای حذف سریع محتوای حاوی مطالب نفرت‌پراکن و حامی تروریسم از این شبکه اجتماعی، فیس‌بوک طرحی را در انگلیس اجرا کرده تا سازمان‌های محلی در این کشور بتوانند چنین محتوایی را شناسایی و در حذف آن به فیس‌بوک کمک کنند. در قالب این طرح هم بودجه‌ای به این سازمان‌ها اختصاص می‌یابد و هم راهنمایی‌های لازم به آنها ارائه می‌شود. فیس‌بوک قبلا برنامه‌های مشابهی را با همین هدف در فرانسه و آلمان به اجرا گذاشته بود. فیس‌بوک هفته قبل هم اعلام کرده بود اقدامات جدیدی را برای مقابله با تهدیدات تروریستی و تبلیغات گروه‌های تندرویی مانند داعش اجرا خواهد کرد تا از انتقادات فزاینده علیه خود در این زمینه بکاهد. این شرکت یک میز پشتیبانی هم برای دریافت اطلاعات مردمی در این زمینه تأسیس کرده و تبلیغاتی را نیز در این مورد پخش خواهد کرد. شریل سندبرگ، مدیر امور عملیاتی فیس‌بوک، می‌گوید: جایی برای مطالب نفرت‌پراکن و ترویج خشونت در فیس‌بوک نیست و ما از فناوری‌هایی مانند هوش مصنوعی برای حذف تبلیغات تروریستی استفاده خواهیم کرد و گروه‌هایی را نیز برای حذف این نوع محتوا از فیس‌بوک آموزش داده و به کار خواهیم گرفت. با وجود همه این تلاش‌ها هنوز شبکه‌های اجتماعی آمریکایی به طور گسترده از سوی تروریست‌های داعش برای انتشار مطالب نفرت‌پراکن به کار می‌روند.

پارلمان آلمان تصویب کرد

قانونی‌شدن هک تلفن‌های هوشمند مظنونان

پارلمان آلمان (بوندس‌تاگ) قانونی تصویب کرد که براساس آن پلیس و بازرس‌ها می‌توانند روی تلفن‌های هوشمند، تبلت و رایانه افراد مظنون به صورت مخفیانه نرم‌افزار جاسوسی نصب کنند. با نصب این نرم‌افزار، امکان مشاهده تمامی فعالیت‌های فرد مظنون ازجمله بررسی پیام‌های واتس‌اپ و دیگر پیام‌رسان‌ها ممکن می‌شود. نصب این «تروجان دولتی» مشکل بررسی پیام‌های رمزگذاری‌شده را مرتفع خواهد کرد زیرا اطلاعات دستگاه موردنظر به صورت مستقیم در اختیار بازرسان خواهد بود. علاوه بر نظارت آنلاین بر فعالیت‌های فرد تحت نظر، قانون جدید به مقامات اجازه می‌دهد به همه محتویات دستگاه هک‌شده بدون محدودیت دسترسی داشته باشند. به گزارش دویچه‌وله، اکثر پیام‌رسان‌های اینترنتی معتبر، پیام‌های کاربران را به صورت رمزگذاری‌شده ارسال می‌کنند تا امکان بررسی این پیام‌ها به وسیله شرکت‌های ارائه‌کننده خدمات اینترنتی دشوار شود. اما «تروجان دولتی» درست مانند خود کاربر به همه اطلاعات دسترسی خواهد داشت. سیاست‌مداران وابسته به احزاب حاکم دموکرات مسیحی (CDU)، سوسیال‌مسیحی (CSU) و سوسیال‌دموکرات (SPD) می‌گویند قانون جدید برای مقابله با تروریست‌ها و جنایت‌کارانی لازم است که برای برقراری ارتباط به جای تلفن از ابزارهای آنلاین استفاده می‌کنند. مایکل فریزر، کارشناس سیاست داخلی حزب محافظه‌کار دموکرات مسیحی، روز پنجشنبه در پارلمان آلمان گفت: «این قانون کارآمد و پیشرفته‌ای است که برای همه ما امنیت بیشتری فراهم می‌کند». اما منتقدان می‌گویند قانون جدید، نقض آشکار حریم خصوصی افراد است و با قوانین دادگاه قانون اساسی، بالاترین نهاد قضائی آلمان، همخوانی ندارد. هانس کریستیان اشتروبله، نماینده پارلمان و عضو کمیته قضائی حزب سبزها، معتقد است گرچه دلایلی قابل‌توجه برای نظارت بر ارتباطات آنلاین وجود دارد، اما قانون جدید راهی اشتباه برای انجام این نظارت است. او در گفت‌وگو با دویچه‌وله، اضافه کرد: «دادگاه قانون اساسی برای موارد این‌چنینی، قوانین مشخصی را به تصویب رسانده است». این نماینده حزب سبزها اضافه کرد: «به‌عنوان نمونه قانون باید تضمین کند که تمام گفت‌وگوهای خصوصی و اطلاعات شخصی افراد که نرم‌افزار جاسوسی در اختیار بازرسان قرار می‌دهد، بلافاصله حذف شوند. اما این خواسته برآورده نشده است». پاتریک سنسبورگ، نماینده پارلمان و عضو کمیسیون قضائی حزب محافظه‌کار دموکرات مسیحی، معتقد است اشتروبله قوانین مصوب دادگاه قانون اساسی را نادرست تفسیر می‌کند. او با اشاره به اینکه این قوانین فقط به ارتباطات قبلی مظنونان اشاره دارند، به دویچه‌وله گفت: «البته اگر فرد مظنون از گوشی موبایل خود یک پیتزا سفارش دهد زیر نظارت خواهد بود اما بازرسان اجازه نخواهد داشت به مکالمات پیشین او سرک بکشند». اعضای ائتلاف حاکم بر این باورند که قانون جدید برای حمایت قانونی از پلیس در مبارزه با جرم و جنایت سازمان‌یافته ضروری است. آوا هگل، معاون ریاست گروه پارلمانی حزب سوسیال‌دموکرات، در بیانیه‌ای که برای دویچه‌وله ارسال کرده، نوشته است: «در شرایط حاضر که با تهدید دائمی تروریست‌ها روبه‌رو هستیم، باید همه منفذهای امنیتی را ببندیم».

یکی دیگر از انتقادهای مطرح‌شده، نحوه ارائه و تصویب این قانون در پارلمان آلمان بوده است. اقدامات نظارتی جدید در آخرین لحظات به لایحه پیشنهادی دیگری اضافه شد که شامل تغییرات جزئی در قوانین کیفری آلمان بود. اشتروبله از حزب سبزها معترض است که نمایندگان در زمان بسیار کوتاهی که از تغییرات اضافی مطلع شدند، برای انجام یک بحث همه‌جانبه فرصت کافی نداشتند. او اضافه می‌کند: «این یک روش غیردموکراتیک و غیرپارلمانی بود. قانونی با این درجه از اهمیت باید حتما با تمامی جزئیات به بحث گذاشته می‌شد؛ امری که به هیچ عنوان امکان‌پذیر نبود». با وجود این، سنسبورگ نماینده حزب دموکرات مسیحی در پارلمان مدعی شد مقدمات این قانون در توافق‌نامه میان احزاب دولت ائتلافی پس از انتخابات فدرالی سال ۲۰۱۳ لحاظ شده و از آن زمان درباره جزئیات آن، مذاکراتی در جریان بوده است. اما کانون وکلای آلمان با اپوزیسیون احزاب حاکم هم‌نظر است و تصریح می‌کند یک نوع شتاب‌زدگی در کل روند بررسی و تصویب این قانون دیده می‌شود. اولریش شلنبرگ، رئیس کانون وکلای آلمان، به دویچه‌وله گفت: «تصور می‌کنیم این نقض جدی آزادی‌های مدنی عمدا در یک لایحه اصلاحیه عادی پنهان شده تا آن را به‌سرعت و بدون بحث تصویب کنند». در پی حملات تروریستی چند سال اخیر، مقامات امنیتی و سیاسی اروپا خواستار دسترسی بیشتر به محتوای پیام‌های رمزگذاری‌شده هستند. در همین حال تلاش‌هایی از این دست برای دسترسی به اطلاعات پیش از رمزگذاری مورد توجه قرار گرفته است. در بریتانیا ترزا می، نخست‌وزیر و بوریس جانسون، وزیر امور خارجه کشور، گفته‌اند شرکت‌هایی که امکان رمزگذاری پیام‌های اینترنتی را ارائه می‌دهند، باید بیش از این به مقامات کمک کنند.

مدیر اجرائی «اپل»، از نگرانی کارگران درباره مهاجرت می‌گوید

الهام محسنی‌آهویی: هفته گذشته، رئیس‌جمهور ترامپ هفته فناوری را در کاخ سفید با برگزاری یک نشست با برخی از بزرگ‌ترین نام‌های صنعت فناوری، ازجمله مدیرعامل شرکت اپل تیم کوک، مدیرعامل شرکت مایکروسافت ساتیا نادلا و رئیس آمازون جف بیسوس آغاز کرد. به گزارش وب‌سایت «ری‌کد»، درحالی‌که رهبران بسیاری از شرکت‌های دره سیلیکون رئیس‌جمهور ترامپ را در دوره خود تحت فشار قرار داده بودند، در جلسه گذشته با «تاکتیک بیشتری» صحبت کردند، اریک اشمیت از شرکت «الفبا» حتی پیشنهاد کرد که ترامپ به ایجاد فرصت‌های جدید در افق پیش‌رو کمک کند. بااین‌حال، پیرو گزارش «ری‌کد» و دیگر رسانه‌ها، بحث فناوری در رابطه با سیاست‌های رئیس‌جمهور در زمینه توسعه در چندین موقعیت شکلی جدی به خود گرفت.

در ادامه نظر تکراری ترامپ که اصلاحات جمهوری‌خواهان برای برنامه سلامت به «قلبی دیگر» نیاز دارد، کوک موافقت خود را با رئیس‌جمهور ابراز و از او درخواست کرد تا همین رویه را درخصوص برنامه «داکا» DACA پیش بگیرد؛ برنامه‌ای در زمان اوباما که بزرگ‌سالانی را که در کودکی به آمریکا آورده شده‌اند، از دیپورت‌شدن مصون می‌داشت. طبق گفته سی‌ان‌بی‌سی، مدیرعامل شرکت اپل همچنین به رئیس‌جمهور تأکید کرد که موضعش درباره مهاجرت موجب نگرانی و اضطراب کارکنان بخش فناوری در مورد وضعیت و آینده خود در ایالات متحده شده است. وی سپس خاطرنشان کرد بهتر خواهد بود که ترامپ در این زمینه به آنها پیامی دهد. در پاسخ به نظرات کوک، رئیس‌جمهور نسبت به اعمال رویکردی جدید و جامع‌تر نسبت به مهاجرت ابراز تمایل کرده است («ری‌کد»، به نقل از اکسیوز). ترامپ از مدیران خواست تا با نمایندگان منتخب خود صحبت کنند. وی همچنین از نیاز به اصلاحات جامع در زمینه مهاجرت سخن گفت.

ملاقات دوشنبه هفته گذشته فقط آغاز هفته فناوری بود. رهبران فناوری همچنین فرصتی برای تأکید بر دیدگاه‌های خود در جلسه اعلام‌نشده پیشین خود با مشاوران ترامپ مانند استیو مِنوچین، وزیر خزانه‌داری رئیس‌جمهور و گری کوهن، مشاور اقتصادی ریاست‌جمهوری، داشتند.

مذاکرات به طور خاص بر مالیات‌هایی متمرکز بود که شرکت‌های فناوری پس از کسب ثروت در خارج از کشور و واردکردن آن به کشور می‌خواهند از آنها اجتناب کنند. اینکه آیا رهبران فناوری چنین پس‌اندازهایی را به طور منصفانه صرف شغل‌های جدید چه به صورت خصوصی، چه از طریق سیاست می‌کند یا خیر، ناشناخته است. در ادامه هفته فناوری در آمریکا، حامیان و فعالان زمینه پهبادها و اینترنت 5G نیز فرصتی برای بیان نظرات خود در کاخ سفید خواهند داشت.

بازار

تازه‌واردهای ال‌جی و ایسوس در بازار

G6 Pro و G6 Plus

درحالی‌که فقط چهار ماه از معرفی گوشی پرچمدار LG G6 در MWC 2017 می‌گذرد، در هفته‌های گذشته منابع خبری از ارائه نسخه‌های جدیدتری از این گوشی هوشمند با نام‌های G6 Plus و G6 Pro خبر می‌دادند. گوشی هوشمند جدید ال‌جی از نظر مشخصات سخت‌افزاری تفاوت عمده‌ای با نمونه قبلی خود ندارد. صفحه‌نمایش محصول جدید مانند نسخه پیشین، ۵.۷ اینچی با طراحی Full Vision، وضوح QHD+ و نسبت تصویر ۱۸:۹ است. گوشی هوشمند جدید مجهز به پروسسور چهارهسته‌ای Snapdragon 821 است؛ چیپ‌ستی که بسیاری از کارشناسان امیدوار بودند به Snapdragon 835 ارتقا یابد. G6 Plus مانند G6 از چهار گیگابایت رم بهره می‌برد، اما ظرفیت حافظه داخلی آن بهبود یافته و از ۶۴ گیگابایت به ۱۲۸ گیگابایت رسیده است. این گوشی همچون G6 با دوربین‌های دوگانه ۱۳مگاپیکسلی مجهز به فلش LED، امکان فیلم‌برداری 4K و عدسی‌های با زاویه‌دید معمولی و وسیع عرضه شده است. به علاوه، G6 Plus مجهز به دوربین جلوی پنج‌مگاپیکسلی با میدان دید صد درجه است. این گوشی هوشمند دارای باتری با ظرفیت سه‌هزارو ۳۰۰ میلی‌آمپر ساعت است که با اندروید ۷.۰ و رابط کاربری LG UX 6.0 ارائه خواهد شد. سایر ویژگی‌های این دستگاه ازجمله گزینه‌های ارتباطی نیز مشابه G6 است. ازجمله این قابلیت‌های جدید می‌توان به حسگر تشخیص چهره (Face Print) اشاره کرد. به کمک این ویژگی طبق ادعای ال‌جی، کاربر می‌تواند در کمتر از یک ثانیه با گرفتن گوشی در برابر صورت خود و بدون فشردن هیچ دکمه‌ای قفل گوشی را باز کند. به گفته ال‌جی، دوربین فقط هنگامی فعال می‌شود که گوشی مقابل چهره قرار گیرد، ازاین‌رو هنگام استفاده از این گزینه مصرف اضافه باتری وجود نخواهد داشت. سومین قابلیت ارتقایافته در G6 Plus به ویژگی Covered Lens در دوربین آن مرتبط است. از آنجا که میدان دید وسیع لنز یکی از دوربین‌های G6 سطح بزرگ‌تری را پوشش می‌دهد، ممکن است انگشت کاربر به طور ناخواسته در عکس ثبت شود. به کمک این قابلیت، در صورت وجود انگشتان کاربر در تصویر، پیش از فعال‌شدن شاتر دوربین، پیغام هشدار روی نمایشگر ظاهر می‌شود.

Zenfone ۳ و Zenfone ۳ Max

شرکت ایسوس از ارائه دو گوشی هوشمند جدید Zenfone 3 و Zenfone 3 Max به بازار خبر داد. هر دو مدل یادشده به رده میانی بازار تعلق دارند و از لحاظ مشخصات، مدل Zenfone 3 در جایگاه بالاتری قرار می‌گیرد. گوشی‌های سری Zenfone ایسوس از سال ۲۰۱۴ به بازار ارائه شدند و تا به امروز در مناطق مختلف به‌ویژه در آسیای شرقی و کشور ژاپن به بالاترین فروش دست پیدا کرده‌اند. زن‌فون۳ با نام کامل Zenfone 3 ZE520KL گوشی هوشمندی با دو لایه شیشه‌ای در پشت و روی دستگاه بوده و حسگر اثر انگشت آن نیز در بخش پشتی و زیر دوربین قرار دارد. این حسگر توانایی بازگشایی قفل دستگاه را تنها در ۰.۲ ثانیه داراست. چیپ‌ست پردازشی دستگاه از نوع Snapdragon 625 با فناوری ساخت ۱۴نانومتری است که نخستین گوشی هوشمند مجهز به این چیپ‌ست (در زمان معرفی جهانی دستگاه) به شمار می‌رود. صفحه‌نمایش گوشی یک نمونه ۵.۲ اینچی با وضوح ۱۹۲۰×۱۰۸۰ پیکسل یا فول اچ‌دی بوده که از طرفین ۲.۱ میلی‌متر حاشیه دارد و به گفته ایسوس نزدیک به ۷۵.۶ درصد از روی دستگاه را پوشانده است. دوربین اصلی گوشی ۱۶مگاپیکسلی با سنسور سونی IMX 298 و ابعاد پیکسل ۱.۱۲ میکرون است که در مقابل خود لنز با گشودگی دیافراگم حداکثر f/2.0 را می‌بیند. پوشش لنز سافایر، لرزه‌گیر اپتیکال چهارمحوره دست (OIS)، اتوفوکوس سریع لیزری، سنسور تصحیح رنگ (RGB sensor) و توانایی برداشت ویدئو با وضوح 4K دیگر مشخصات برجسته این دوربین که در کنار خود دو فلش LED را نیز می‌بیند تشکیل می‌دهند. دوربین دوم این گوشی نیز هشت مگاپیکسل وضوح دارد و دیافراگم آن از گشودگی f/2.0 برخوردار است. این گوشی دوسیم‌کارته از پورت اتصال USB Type-C برخوردار بوده و سه گیگابایت حافظه RAM و ۳۲ گیگابایت حافظه داخلی قابل ارتقا دارد. Zenfone 3 Max با نام مدل ZC553KL دیگر محصول جدید ایسوس است که با بدنه‌ای از جنس آلیاژ آلومینیوم با لبه‌های گرد و شیشه نمایشگر با انحنای 2.5D، طیف دیگری از مخاطبان را هدف قرار داده است. صفحه‌نمایش گوشی ۵.۵ اینچی با وضوح فول اچ‌دی یا ۱۹۲۰×۱۰۸۰ پیکسل بوده و سنسور اثر انگشت آن نیز همچون زن‌فون۳ در پشت دستگاه قرار دارد. دوربین اصلی این گوشی نیز ۱۶مگاپیکسلی با f/2.0 و مجهز به فوکوس لیزری و تشخیص فاز بوده و لرزه‌گیر اپتیکال مدل پیشین نیز جای خود را به تثبیت‌کننده الکترونیکی یا EIS در این مدل داده است. دوربین دوم این مدل هشت مگاپیکسل وضوح داشته و دیافراگم آن نیز حداکثر تا f/2.2 امکان گشودگی دارد. پردازش در Zenfone 3Max با چیپ هشت هسته‌ای Snapdragon 430 انجام شده و مثل زن‌فون۳ دارای ۳۲ گیگابایت حافظه داخلی و سه گیگابایت رم است.

دریچه

تهدید تلگرام با تروجان جاسوس‌افزار

● محققان امنیتی از شرکت دکتر وب یک تروجان اندرویدی را شناسایی کرده‌اند که مهاجمان سایبری برای مدیریت آن از پروتکل تلگرام استفاده می‌کنند. این تروجان می‌تواند اطلاعات حساس قربانیان را به سرقت برده و کدهای دلخواه مهاجم را روی سامانه قربانی اجرا کند. این تروجان Android.Spy.377.origin نام داشته و یک ابزار مدیریتی راه دور (RAT) است که در قالب برنامه‌های بی‌خطر توزیع می‌شود. این بدافزار کاربران ایرانی را هدف قرار داده است. این تروجان می‌تواند روی تلفن‌های هوشمند و تبلت‌های قربانیان با عنوان برنامه‌هایی مانند «اینستا پلاس»، «پروفایل چکر» و «کلینر پرو» نصب شود. این بدافزار پس از اجراشدن، به کاربر پیشنهاد می‌دهد تا محبوبیت مالک دستگاه را در بین سایر کاربران تلگرام بررسی کند. برای اجرای این کار، بدافزار از قربانی شناسه‌های خصوصی او را درخواست می‌کند. پس از اینکه قربانی اطلاعات درخواستی را در اختیار مهاجمان قرار می‌دهد، بدافزار Android.Spy.377.origin تعداد بازدیدها از پروفایل کاربر را نمایش می‌دهد. کمی پس از اجرای این عملیات، بدافزار آیکون میان‌بر خود را از صفحه خانگی حذف می‌کند تا عملیات مخرب خود را مخفی کند. این بدافزار یک جاسوس‌افزار کلاسیک است که می‌تواند دستورات موردنظر مهاجمان سایبری را اجرا کند. یکی از تفاوت‌هایی که این بدافزار با سایر تروجان‌های اندرویدی دارد، نحوه کنترل آن به وسیله مهاجمان سایبری است. مهاجمان برای کنترل این بدافزار از پروتکل تبادل پیام در پیام‌رسان برخط تلگرام استفاده می‌کنند. این اولین تروجان اندرویدی است که از پروتکل تلگرام استفاده می‌کند. این تروجان پس از حذف پرونده میان‌بر، اطلاعاتی را از فهرست مخاطبان، پیام‌های کوتاه دریافتی و ارسالی و داده‌های حساب‌های گوگل رونویسی می‌کند. در ادامه این داده‌ها در دایرکتور خود بدافزار اجرا می‌شود و آنها را در داخل یک پرونده متنی ذخیره می‌کند. علاوه بر اینها، تروجان با استفاده از دوربین جلویی دستگاه، از چهره مالک دستگاه عکس می‌گیرد. درنهایت نیز این تصویر و پرونده اطلاعات را روی کارگزار دستور و کنترل بارگذاری می‌کند و یک سیگنال به بات تلگرام نیز ارسال می‌شود تا نشان دهد دستگاه با موفقیت آلوده شده است.