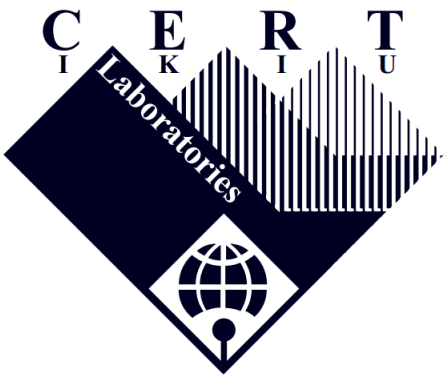


آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

هفته نامه تحلیلی رویدادهای امنیتی

شنبه سیزدهم مرداد ماه ۱۳۹۷

نسخه ۱,۰,۰

بنام خداوند بخشنده و مهربان

یادداشت سردبیر

مهاجمان رایانه‌ای حرفه‌ای امروزه اهداف خاص‌تر را به جای قربانیان گسترده ترجیح می‌دهند. دلیل این امر مزایای مهمی است که این رویکرد می‌تواند برای آن‌ها به همراه داشته باشد. برخی از این مزایا در لیست زیر قابل مشاهده است.

۱. جلب توجه کمتر و تاخیر در واکنش شرکت‌های امنیتی
۲. انتخاب بررسی شده قربانیان برای افزایش احتمال تامین منافع مهاجم

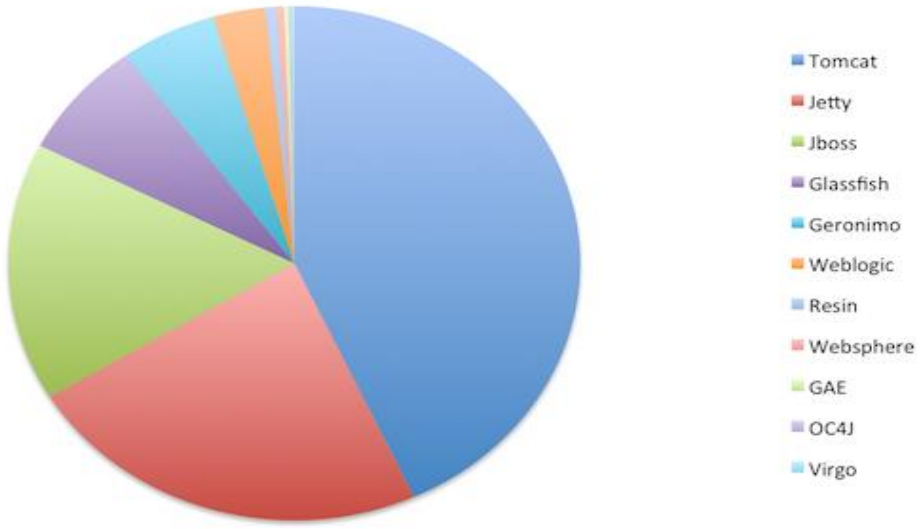
نمونه‌ی بارز این موضوع را می‌توان در اخبار این هفته مشاهده کرد. جایی که طراحان باج‌افزار سَم‌سَم به جای گسترش بدافزار خود و افزایش تعداد قربانیان بر روی اهداف ویژه تمرکز کرده‌اند. افرادی که حاضر به پرداخت هزینه‌های سنگین برای بازگشت اطلاعات خود به شرایط عادی هستند. این باج‌افزار به همین ترتیب توانسته بیش از ۶ میلیون دلار اتنها از ۲۳۶ قربانی کسب کند.

مورد دیگر به استفاده از بدافزار جاسوسی پگاسوس[1] ساخته‌ی شرکت اسرائیلی اِن.اِس.او[2] بر ضد فعالان حقوق بشر برمی‌گردد. حملاتی که مهندسی اجتماعی خاص قربانی نقش پررنگی را در انتقال این بدافزار به سیستم قربانی ایفا کرده است. بسیار جالب است که مهاجمان در هر دو حمله بالا به جای روش‌های پیچیده تنها از بی‌توجهی قربانیان به موارد ساده امنیتی استفاده کرده‌اند.

آخرین خبر هفته گذشته نیز به انتشار وصله امنیتی جدید برای آپاچی تامکَت[3] برمی‌گردد. مهم‌ترین آسیب‌پذیری رفع شده در این وصله، امکان شنود غیرمجاز ارتباطات بین کاربر و سرور است. نقصی که از مدیریت ناصحیح آپاچی تامکَت در

[1]-Pegasus is spy software installable on devices running certain versions of iOS, Apple's mobile operating system, and android Mobiles developed by the Israeli cyberarms firm, NSO Group
[2]-NSO Group Technologies is an Israeli firm that works in the world of cyber intelligence.
[3]-Apache Tomcat is an open-source Java Servlet Container developed by the Apache Software Foundation (ASF).

خاتمه ارتباطات نشأت می‌گیرد. تامکَت از سرورهای مهم بازار سروهای برنامه کاربردی محسوب می‌گردد. این امر در شکل شماره ۱ قابل مشاهده است.



شکل ۱ : سهم بازار مربوط به انواع سرور برنامه‌های کاربردی (plumbr.io)

محمد پیشدار

فهرست مطالب

خبر شماره ۱ تاریخ انتشار : ۹۷/۰۵/۰۷

انتشار وصله امنیتی جدید برای آپاچی تامکَت[1]

خلاصه

آپاچی تامکَت یک وب سرور محبوب برای پروتکل اچ.تی.تی.پی[2] با قابلیت اجرای کدهای جاوا[3] است. اخیرا بنیاد نرم‌افزار آپاچی[4] به عنوان پشتیبان و سازنده این نوع وب‌سرور یک بسته بروزرسانی برای رفع چند آسیب‌پذیری امنیتی منتشر کرده است. آسیب‌پذیری‌هایی که حتی می‌توانند دستیابی غیرمجاز به اطلاعات حساس سرور را ممکن سازند. این اطلاعات مقدمه‌ای برای طراحی حملات دیگر به سرور تامکَت است. حملاتی که حتی ممکن است کنترل غیرمجاز سرور را برای مهاجمان فضای سایبری در پی داشته باشد. علاوه بر این، بروزرسانی مذکور برخی آسیب‌پذیری‌های دیگر را نیز رفع می‌نماید. از مهمترین این موارد می‌توان به امکان اجرای حملات انکار سرویس با استفاده از سرریز بافر اشاره کرد.

برای مشاهده متن کامل خبر می‌توانید به آدرس زیر مراجعه نمایید.

https://cert.ikiu.ac.ir/news-view.php?nid=76

مرجع اصلی خبر:

The Hacker News Website (https://thehackernews.com/2018/07/apache-tomcat-server.html)

[1]- Apache Tomcat is an open-source Java Servlet Container developed by the Apache Software Foundation (ASF).
[2]- The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, and hypermedia information systems.
[3]- Java is a general-purpose computer-programming language that is concurrent, class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible.
[4]- The Apache Software Foundation (ASF) is an American non-profit corporation in the United States to support Apache software projects, including the Apache HTTP Server

خبر شماره ۲ تاریخ انتشار : ۹۷/۰۵/۱۰

رشد گسترده قربانیان باج‌افزار سَم.سمَ[1]

خلاصه

امروزه باج‌افزارها کم کم در حال تبدیل به یک بازار چند میلیون دلاری برای مهاجمان فضای سایبری هستند. یکی از بارزترین مثال‌های این موضوع باج‌افزار سَم.سَم است. باج‌افزاری که اخیرا در یک پژوهش دریافتی‌های آن از قربانیان حدود ۶ میلیون دلار تخمین زده شده است. بازه زمانی مورد مطالعه در این پژوهش سال ۲۰۱۵، زمان شروع توزیع گسترده این بدافزار تا کنون بوده است. محققان شرکت سوفوس[2] نتایج این پژوهش را با بررسی تراکنش‌های مربوط به آدرس‌های بیتکوین[3] (ارز دیجیتال[4]) در این باج‌افزار به دست آورده‌اند. در واقع طراحان سَم.سَم پس از رمزنگاری اطلاعات قربانی وجهی را بر اساس پول الکترونیکی بیتکوین در قبال بازگرداندن شرایط به قبل طلب می‌کنند. این وجه از سایر باج‌افزارهای مشابه بسیار بیشتر بوده به طوریکه مبلغ ۶ میلیون دلار مذکور تنها از طریق ۲۳۳ قربانی دریافت شده است. مبلغی که همچنان در حال گسترش بوده و ماهانه حدود ۳ میلیون دلار به درآمد طراحان این بدافزار می‌افزاید.

برای مشاهده متن کامل خبر می‌توانید به آدرس زیر مراجعه نمایید.

https://cert.ikiu.ac.ir/news-view.php?nid=77

مرجع اصلی خبر:

The Hacker News Website (https://thehackernews.com/2018/07/samsam-ransomware-attacks.html)

[1]-SamSam Ransomware is a custom infection used in targeted attacks, often deployed using a wide range of exploits or brute-force tactics

[2]- Sophos Group plc is an English security software and hardware company. Sophos develops products for communication endpoint, encryption, network security, email security, mobile security and unified threat management

[3]- Bitcoin is a cryptocurrency, a form of electronic cash. It is a decentralized digital currency without a central bank or single administrator, though some researchers point at a trend towards centralization

[4]- Cryptocurrency (or crypto currency) is digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets

خبر شماره ۳ تاریخ انتشار : ۹۷/۰۵/۱۱

جاسوسی از فعالان حقوق بشر با بدافزارهای اسرائیلی

خلاصه

اخیرا سازمان عفو بین‌الملل[1] یکی از برجسته‌ترین سازمان‌های حقوق بشر در سطح جهان خبری مبنی بر کشف یک بدافزار پیشرفته با هدف جاسوسی از کارمندان این سازمان را منتشر کرده است. در این خبر از سازمان اِن.اِس.او اسرائیل به عنوان سازنده این بدافزار نام برده شده است. اِن.اِس.او شرکتی اسرائیلی است که عمدتا با ساخت نرم‌افزار های جاسوسی و بدافزارهای پیشرفته شناخته می‌شود. بدافزارهایی که بیشتر قابلیت نفوذ به دستگاههای آیفون و موبایل‌های اندرویدی را دارند. این بدافزارها معمولا برای حمله به سازمان‌های نظامی، ارگان‌های اطلاعاتی و دستگاه‌های مجری قانون مورد استفاده قرار می‌گیرند.

برای مشاهده متن کامل خبر می‌توانید به آدرس زیر مراجعه نمایید.

https://cert.ikiu.ac.ir/news-view.php?nid=78

مرجع اصلی خبر:

The Hacker News Website (https://thehackernews.com/2018/07/iphone-hacking-spyware.html)

[1]- Amnesty International is a London-based non-governmental organization focused on human rights.