آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

خبرنامه تحلیلی رویدادهای امنیتی (روزانه)

چهارشنبه پانزدهم اسفند ماه ۱۳۹۷

سوءاستفاده از ریکَپچا[1] گوگل برای انتقال بدافزار[2]

نسخه ۱,۰,۰

نویسنده: نغمه محمدی **سردبیر:** محمد پیشدار

[1] reCAPTCHA is a CAPTCHA-like system designed to establish that a computer user is human and, at the same time, assist in the digitization of books.

[2] Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network

کشف نوعی کلاهبرداری فیشینگ که از ریکَپچا گوگل[1] برای انتقال بدافزار سوءاستفاده می‌کند

تاریخ: ۵ / مارس / ۲۰۱۹

بررسی اجمالی :

اخیرا محققان حوزه امنیت اطلاعات نوعی کلاهبرداری جدید فیشینگ[2] را کشف کرده که مهاجمان در آن به سوءاستفاده از سیستم ریکَپچای گوگل (رویکردی برای تشخیص ربات‌ها از انسان در فضای سایبری) جهت مخفی‌سازی صفحات مخرب[3] استفاده می‌کنند. در واقع مهاجمان در این حملات خود را شرکت گوگل به موسسات بانکی و کاربران آنها معرفی کرده و از طریق بدافزاری به نام بانک‌بات[4] سعی بر سرقت اعتبارنامه‌های بانکی آنها می‌کنند [۱و۲].

سیستم‌های آسیب‌پذیر [۱] :

- دستگاه‌های اندروید (به دلیل طراحی بدافزار بانک‌بات برای اندروید)

شدت خطر :

در دولت

- سازمان‌های بزرگ و متوسط در دولت : **بالا**
- سازمان‌های کوچک دولتی : **بالا**

[1] Google LLC is an American multinational technology company that specializes in Internet-related services and products, which include online advertising technologies, search engine, cloud computing, software, and hardware. It is considered one of the Big Four technology companies, alongside Amazon, Apple and Facebook.
[2] Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.
[3] In online marketing, a landing page, sometimes known as a "lead capture page", "static page", or a "destination page", is a single web page that appears in response to clicking on a search engine optimized search result, marketing promotion, marketing email, or an online advertisement.
[4] Malicious mobile BankBot Trojan injected into everyday apps, taking advantage of unknowing users whose banking apps could be compromised.

در تجارت

- سازمان های تجاری بزرگ و متوسط : **بالا**
- سازمان‌های کوچک تجاری : **بالا**
- کاربران خانگی : **بالا**

راه‌های نفوذ:

- از طریق حملات فیشینگ با سوءاستفاده از رویکرد ریکَپچای گوگل جهت فریب قربانیان

اهداف:

- سرقت اعتبارنامه و اطلاعات بانکی
- سرقت اطلاعات شخصی کاربران

توضیحات فنی :

به گفته محققان شرکت سوکِری[1] به تازگی یک بانک لهستانی و کاربران آن مورد حملات فیشینگ از طریق پست های الکترونیکی قرار گرفته است. مهاجمان در این حملات از طریق جعل سیستم ریکَپچا گوگل به ترغیب کاربران جهت کلیک بر روی یک پیوند مخرب (یک فایل پی.اِچ.پی[2]جاسازی شده در پست الکترونیکی) پرداخته‌اند. هدف از این کار انتقال بدافزاری با نام بانک‌بات بر روی سیستم قربانی بوده است [۱و۲].

پیام‌های ارسالی به قربانیان شامل درخواست‌های «تایید» تراکنش‌های ناشناخته گوگل از طریق کلیک بر روی یک پیوند است. نوآوری این حملات به اتفاقات پس از کلیک بر روی این پیوند مخرب اختصاص دارد. در واقع با عدم تشخیص پیام جعلی توسط قربانی و کلیک بر روی پیوند مخرب به جای صفحه جعلی بانک با یک کُد پی.اِچ.پی شامل

[1] Sucuri:A website security & protection platform that delivers peace of mind. Stop worrying about website security threats and get back to building your online brand.

[2] PHP: Hypertext Preprocessor is a general-purpose programming language originally designed for web development. It was originally created by Rasmus Lerdorf in 1994; the PHP reference implementation is now produced by The PHP Group.

ریکَپچای جعلی (با استفاده از عناصر اِچ.تی.اِم.اِل [1] و جاوا اِسکریپت[2]) روبرو خواهد شد. این ریکَپچا با وجود ظاهری قانونی به دلیل ساختار ایستا تا زمانِ تغییر کُد ثابت مانده و حتی برخلاف نسخه اصلی قابلیت پخش صوتی را نیز پشتیبانی نمی‌کند [۱]. بدافزار بانک‌بات پس از استقرار می‌تواند علاوه بر اطلاعات بانکی موارد خصوصی مختلفی نظیر پیام‌کوتاه، گزارشات تماس، لیست مخاطبین و حتی موقعیت جغرافیایی را برداشت کند [۱و۲].

پیشنهادات [۱]:

- عدم کلیک بر روی هر گونه پیوند مشکوک موجود در پست‌های الکترونیکی (به خصوص از منابع ناشناس)

منابع :

1. Threat Post Website
   https://threatpost.com/phishing-scam-malware-google-recaptcha/142142/
2. ZDNET Website
   https://www.zdnet.com/article/fake-google-recaptcha-used-to-hide-bank-malware/

[1] Hypertext Markup Language(HTML) is the standard markup language for creating web pages and web applications. With Cascading Style Sheets and JavaScript, it forms a triad of cornerstone technologies for the World Wide Web.

[2] JavaScript, often abbreviated as JS, is a high-level, interpreted programming language that conforms to the ECMAScript specification. It is a programming language that is characterized as dynamic, weakly typed, prototype-based and multi-paradigm.