آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

خبرنامه تحلیلی رویدادهای امنیتی (روزانه)

دوشنبه نوزدهم شهریور ماه ۱۳۹۷

دریافت بدافزاری جدید در صندوق پست الکترونیک[1]

نسخه ۱,۰,۰

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

[1] E-Mailbox

اخیرا دریافت یک بدافزار[1] جدید در پست‌الکترونیک برخی شرکت‌ها مشاهده شده است

تاریخ: ۷ / سپتامبر / ۲۰۱۸

بررسی اجمالی :

از اوایل جولای ۲۰۱۸، محققان امنیت اطلاعات شرکت کَسپِراسکای[2] شاهد ارسال بدافزاری جدید به پست‌الکترونیک برخی شرکت‌ها و سازمان‌های تجاری بوده‌اند. این بدافزار در قالب یک هرزنامه شامل فایلی با پسوند ایزو[3] منتشر می‌گردید. محققان کسپراسکای نامی با عنوان لُکی‌بات[4] را به این بدافزار نسبت داده و ماموریت آن را سرقت اطلاعات حساس در مرورگرها[5]، پیام‌رسان‌ها، پست‌های‌الکترونیکی، کاربران اف.تی.پی[6] و حتی کیف‌های پول ارز دیجیتال[7] عنوان کرده‌اند. متن هرزنامه‌های شامل این بدافزار اطلاعیه‌های جعلی شرکت‌های معروف به همراه اسناد مالی، سفارشات و پیشنهادات دروغین گزارش شده است [۱].

سیستم‌های آسیب‌پذیر [۱] :

- پست الکترونیک اشخاص، شرکت‌ها و سازمان‌ها

[1] Malware is any software intentionally designed to cause damage to a computer, server or computer network.
[2] Kaspersky Lab is a Russian security software and services company with a presence in 200 countries and territories around the world.
[3] An ISO image is a disk image of an optical disc. In other words, it is an archive file that contains everything that would be written to an optical disc, sector by sector, including the optical disc file system.
[4] Loki Bot
[5] A web browser is a software application for accessing information on the World Wide Web.
[6] FTP: The File Transfer Program is a standard network protocol used for the transfer of computer files between a client and server on a computer network.
[7] A cryptocurrency wallet stores the public and private keys which can be used to receive or spend a cryptocurrency. A wallet can contain multiple public and private key pairs.

شدت خطر:

در دولت

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

در تجارت

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

توضیحات فنی :

از اوایل جولای ۲۰۱۸، محققان امنیت اطلاعات شرکت کَسپِراسکای شاهد ارسال بدافزاری جدید به پست‌الکترونیک برخی شرکت‌ها و سازمان‌های تجاری بوده‌اند. این بدافزار در قالب یک هرزنامه شامل فایلی با پسوند ایزو منتشر می‌گردید. محققان کسپراسکای نامی با عنوان لُکی‌بات را به این بدافزار نسبت داده و ماموریت آن را سرقت اطلاعات حساس در مرورگرها، پیام‌رسان‌ها، پست‌های‌الکترونیکی، کاربران اف.تی.پیو حتی کیف‌های پول ارز دیجیتال عنوان کرده‌اند [۱].

فایل با پسوند ایزو، یک کپی یا تصویر از دیسک نوری[1] با توانایی نصب در درایو دی.وی.دی یا سی.دی مجازی[2] است. اطلاعات این فایل می‌تواند همانند دیسک‌نوری اصلی مورد استفاده قرار گیرد [۲,۱]. در گذشته برای مشاهده فایل‌های ایزو نیاز به نرم‌افزارهای خاصی بود اما امروزه سیستم‌های‌عامل خود توانایی پشتیبانی از این فرمت را دارند. در واقع مهاجمان برای انتقال بدافزار لُکی‌بات از این نوع فایل به عنوان یک ظرف استفاده می‌کنند. ظرفی که می‌تواند فایل‌های این بدافزار را از چشم ابزارهای امنیتی (به ویژه در صندوق‌های پستی) مخفی نگاه دارد.

[1] An optical disc is an electronic data storage medium that can be written to and read using a low-powered laser beam.
[2] The Virtual DVD/CD Control Panel utility enables users of Windows XP, Vista, and 7 to mount ISO disk image files as virtual CD-ROM drives.

پست‌های الکترونیکی حاوی این فایل ارسالی شامل موارد زیر بوده‌اند [۱]:

- اطلاعیه‌های جعلی از طرف شرکت‌های مشهور:

امروزه ارسال پیام‌های جعلی از طرف شرکت‌های مشهور، محبوب‌ترین ترفند مهندسی اجتماعی برای حملات فیشینگ[1] به شمار می‌آید. در گذشته پست‌های‌الکترونیکی جعلی تنها به کاربران و مشتریان معمولی ارسال می‌گردید در حالی که امروزه حتی خود شرکت‌ها نیز مستقیما مورد حمله قرار می‌گیرند.

- اطلاعیه‌های جعلی شامل اسناد مالی:

در این روش مهاجمان یک فایل مخرب را به جای اسناد مالی نظیر فاکتورها، تراکنش‌ها، پرداخت‌ها منتقل می‌کنند. معمولا بدنه پیام‌های این حملات کوتاه و بیشتر تمرکز بر دریافت فایل‌های مخرب توسط قربانیان است. فایل‌هایی که به صورت اسناد جعلی در پیوست قابل دریافت هستند.

- سفارشات و پیشنهادات جعلی:

در این روش مهاجمان به جای مشتری اصلی به ثبت سفارش و یا ارائه پیشنهاد به فروشنده محصولات یا خدمات می‌پردازند. در واقع با این استراتژی سعی بر ترغیب قربانیان به دریافت فایل‌های مخرب موجود در پیوست می‌گردد.

به طور کلی مهاجمان از طریق فیشینگ یا هرزنامه‌های دارای فایل مخرب به جستجوی اطلاعات محرمانه شرکت‌ها از جمله مالکیت معنوی، اطلاعات احراز هویت، پایگاه‌های‌داده و حساب‌های بانکی می‌پردازند. متاسفانه در سال‌های اخیر آمار این حملات با گسترش قابل توجهی همراه بوده است [۱].

پیشنهادات [۱]:

- استفاده از ابزارهای امنیتی بروز و کارآمد (بررسی استفاده غیرمجاز از منابع سیستم)
- آموزش کارکنان شرکت در رابطه با حملات فیشینگ

منابع :

1. The Secure List (https://securelist.com/loki-bot-stealing-corporate-passwords/۸۷۵۹۵/)
2. Wikipedia Website (https://en.wikipedia.org/wiki/ISO_image)

[1] Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.