آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

خبرنامه تحلیلی رویدادهای امنیتی (روزانه)

یکشنبه بیست و پنجم اسفند ماه ۱۳۹۸

انتقال بدافزار[1] با پیام‌های هشدار امنیتی

نسخه ۱,۰,۰

نویسنده : مونا رضا زاده **سردبیر :** محمد پیشدار

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

مهاجمان سایبری با ساخت یک پیام فیشینگ[1] بر اساس هشدارهای امنیتی به انتقال بدافزارها می‌پردازند

تاریخ: ۰۵/ مارس/ ۲۰۲۰

بررسی اجمالی :

بر اساس برخی گزارش‌ها اخیرا یک گروه سایبری با یک روش فیشینگ جدید اقدام به انتشار بدافزارهای تروجان و درب پشتی[3] در سیستم برخی افراد کرده‌اند. در این روش مهاجم سایبری با فریب قربانیان خود (مدیران وبگاه‌ها) به نصب گواهینامه امنیتی[4] یک بدافزار جاسوسی را به سیستم وی منتقل می‌کند [۱].

نگاه کلی :

سیستم‌های آسیب‌پذیر	سیستم‌عامل ویندوز
راه‌های نفوذ	از طریق پیام فیشینگ
هدف مهاجمان	انتقال بدافزار

توضیحات بیشتر :

گواهینامه‌های امنیتی اِس.اِس.اِل/تی.اِل.اِس[5] توسط مراکز ارائه این نوع گواهینامه صادر می‌شوند. این اطلاعات به منظور رمزنگاری کانال‌های ارتباطی بین مرورگر و خدمات‌رسان و حتی اعتبار سنجی هویت کاربران استفاده می‌گردد. بدین طریق تبادلات در بستر اینترنت به خصوص در سرویس‌های تجارت الکترونیک بصورت امن صورت می‌گیرد. از زمان پیدایش رویکرد مذکور مهاجمان سایبری نیز در جهت یافتن راه‌حلی برای جعل گواهینامه‌های امنیتی حرکت کرده‌اند. به

[1]-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

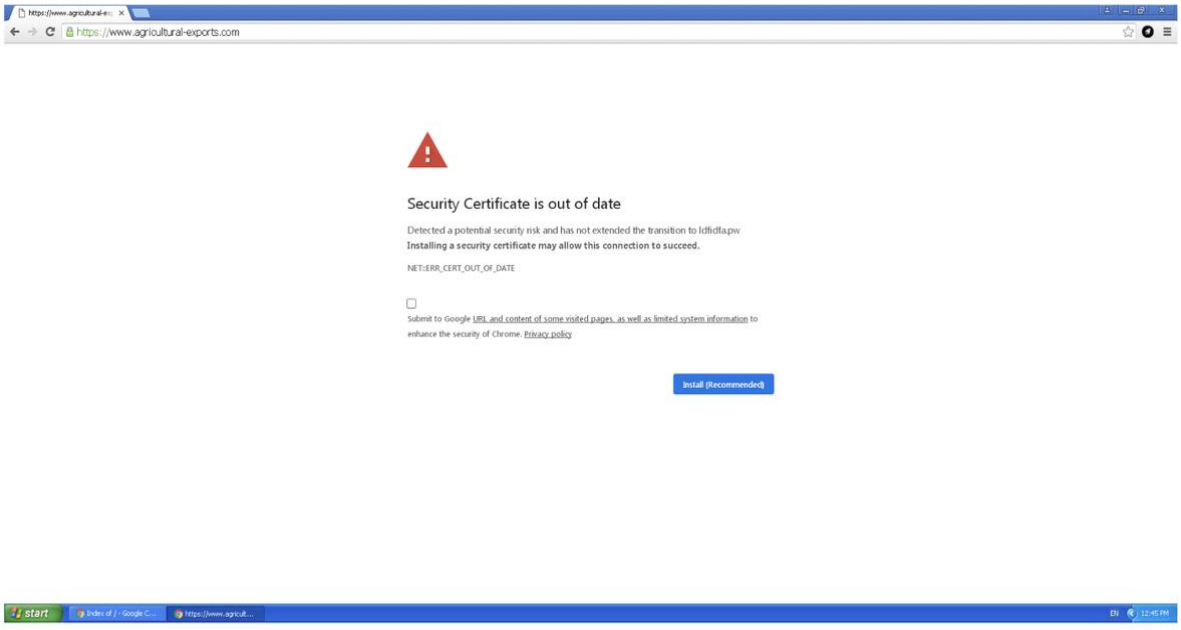
[3]-A backdoor is a method, often secret, of bypassing normal authentication or encryption in a computer system, a product, or an embedded device, or its embodiment, e.g. as part of a cryptosystem, an algorithm, a chipset, or a "homunculus computer" —a tiny computer-within-a-computer.

[4]- In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.

[5]-Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network.

عنوان مثال در یکی از مشهورترین حملات این نوع، مهاجم سایبری با معرفی خود به عنوان مدیر شرکت‌های معروف اقدام به دریافت چندین گواهینامه از این مراجع و توزیع آن در بدافزارهای خود می‌کند.

اخیرا مهاجمان با ارسال یک پیام فیشینگ به قربانیان خود موفق به فریب آن‌ها جهت نصب بدافزارها شده‌اند [۱،۲]. در این کار ابتدا پیامی حاوی انقضاء گواهینامه وبگاه (شکل ۱) به کاربر نمایش داده شده و از وی (صاحب دامنه) درخواست نصب بروزرسانی گواهینامه امنیتی می‌گردد. این پیام در قاب‌های داخلی صفحه[۱] قرار گرفته و محتوای آن توسط یک اسکریپت جی.کوئری[۲] در سرور فرمان و کنترل[۳] مهاجم فراخوانی می‌شود. اما از آنجایی که در نوار آدرس، نشانی دامنه اصلی نمایش داده شده قربانی به این پیام اعتماد می‌کند. به بیان دیگر به جای نمایش محتوای صفحه اصلی وبگاه، کاربر با یک پیام جعلی نصب بروزرسانی گواهینامه روبرو خواهد شد. به محض کلیک کاربر بر روی دکمه نصب فرآیند دریافت فایل Certificate_Update_v02.2020.exe آغاز شده که با اجرای آن یکی از دو بدافزار مُوکِس[۴] یا بوراک[۵] به سیستم قربانی منتقل می‌گردد [۱،۲].



شکل ۱: نمایش پیام انقضاء گواهینامه امنیتی به قربانی

[1]- The *HTML* <iframe></iframe> element creates an inline frame that contains another document.
[2]- jQuery is a JavaScript library designed to simplify HTML DOM tree traversal and manipulation, as well as event handling, CSS animation, and Ajax.
[3]-A command and control server (C&C server) is a computer that issues directives to digital devices that have been infected with rootkits or other types of malware, such as ransomware.
[4]-Mokes
[5]-Buerak

مُوکِس به عنوان یک بدافزار درب پشتی برای سیستم‌های عامل مَک[1] و ویندوز قادر به اجرای کد، تصویربرداری و سرقت اطلاعات از سیستم قربانی است. این بدافزار ضمن ماندگاری در دستگاه قربانی جهت مخفی‌سازی اقدامات مخربانه خود از رمزگذاری اِی.ای.اِس[2].۲۵۶ استفاده می‌کند. در مقابل بوروک یک تروجان مبتنی بر ویندوز بوده که اجرای کُد، دستکاری در فرایندهای قابل اجرا، سرقت محتوا، حفظ پایداری از طریق کلیدهای ریجستری و شناسایی روش‌های تحلیلی از جمله قابلیت‌های آن است [۱].

پیوست اجرایی:

- با دریافت هر گونه پیام مشکوک حتما از صحت ادعای موجود در متن پیام مطمئن شوید.
- تنها از طریق مراکز معتبر اقدام به دریافت گواهینامه امنیتی کنید.
- زمان پایان اعتبار گواهینامه امنیتی سامانه خود را به خاطر داشته باشید.

منابع :

1. Zdnet Website
   https://www.zdnet.com/article/backdoor-malware-is-being-spread-through-fake-security-certificate-alerts/
2. Securelist Website
   https://securelist.com/mokes-and-buerak-distributed-under-the-guise-of-security-certificates/96324/

[1]-macOS is a series of graphical operating systems developed and marketed by Apple Inc. since 2001. It is the primary operating system for Apple's Mac family of computers.

[2]-The Advanced Encryption Standard (AES), also known by its original name Rijndael is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST).