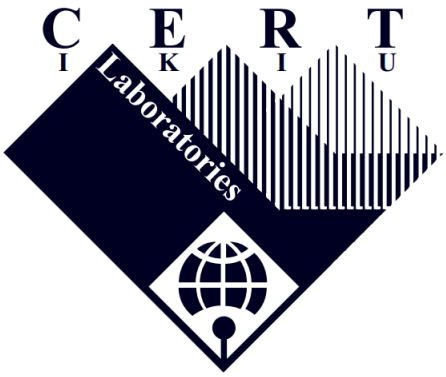


آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

خبرنامه تحلیلی رویدادهای امنیتی (روزانه)

دوشنبه ۸ بهمن ماه ۱۳۹۷

سوءاستفاده حملات بدافزاری از ماکروسافت وُرد[1]

نسخه ۱,۰,۰

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

[1] Microsoft Word is a word processor developed by Microsoft. It was first released on October 25, 1983 under the name Multi-Tool Word for Xenix systems.

انتشار باج‌افزار گَندکِراب[۱] و ویروس اورسنیف[۲] از طریق ماکروهای[۳] ماکروسافت آفیس وُرد

تاریخ: ۲۸ / ژانویه / ۲۰۱۹

بررسی اجمالی :

اخیرا محققان حوزه امنیت دو گروه سایبری در حوزه حملات بدافزاری را در سطح اینترنت کشف کرده‌اند. یکی از آنها «تروجان سرقت‌داده[۴] اورسنیف» و دیگری «باج‌افزار گَندکِراب» نام دارد. با وجود قرارگیری هر دو حمله بدافزاری در دو گروه مجزا از جرائم سایبری، شباهت‌های زیادی نیز در آن‌ها مشاهده می‌شود. یکی از این موارد انتشار از طریق پست‌های الکترونیکی فیشینگ[۵] حاوی سند مخرب مایکروسافت وُرد است. این فایل دارای ماکروهای مخربی بوده که از پاورشِل[۶] برای ارائه «بدافزار بدون فایل»[۷] استفاده می‌کنند [۱].

سیستم‌های آسیب‌پذیر [۱] :

- رایانه‌های متصل به شبکه

[1] GandCrab ransomware is a file locker that was first introduced in early 2018, and within a year managed to earn a name as one of the most prolific cyber infections around the world.
[2] Ursnif is a Trojan horse that steals information from the compromised computer.
[3] A macro is a series of commands and instructions that you group together as a single command to accomplish a task automatically.
[4] Data-stealing trojan
[5] 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
[6] PowerShell is a task automation and configuration management framework from Microsoft, consisting of a command-line shell and associated scripting language.
[7] Fileless malware is a variant of computer related malicious software that exists exclusively as a computer memory-based artifact i.e. in RAM.

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 : **بالا**

راه‌های نفوذ:

- مهندسی اجتماعی و پست‌الکترونیکی فیشینگ[1]

اهداف:

- بدست آوردن اعتبارنامه و اطلاعات حساس قربانیان
- باج‌خواهی

توضیحات فنی :

بتازگی محققان حوزه امنیت اطلاعات موفق به کشف دو گروه از حملات بدافزاری به نام‌های «تروجان سرقت داده اورسنیف» و «باج‌افزار گَندکِراب» شده‌اند. اورسنیف توانایی انجام فعالیت‌های زیر را داراست [۱]:

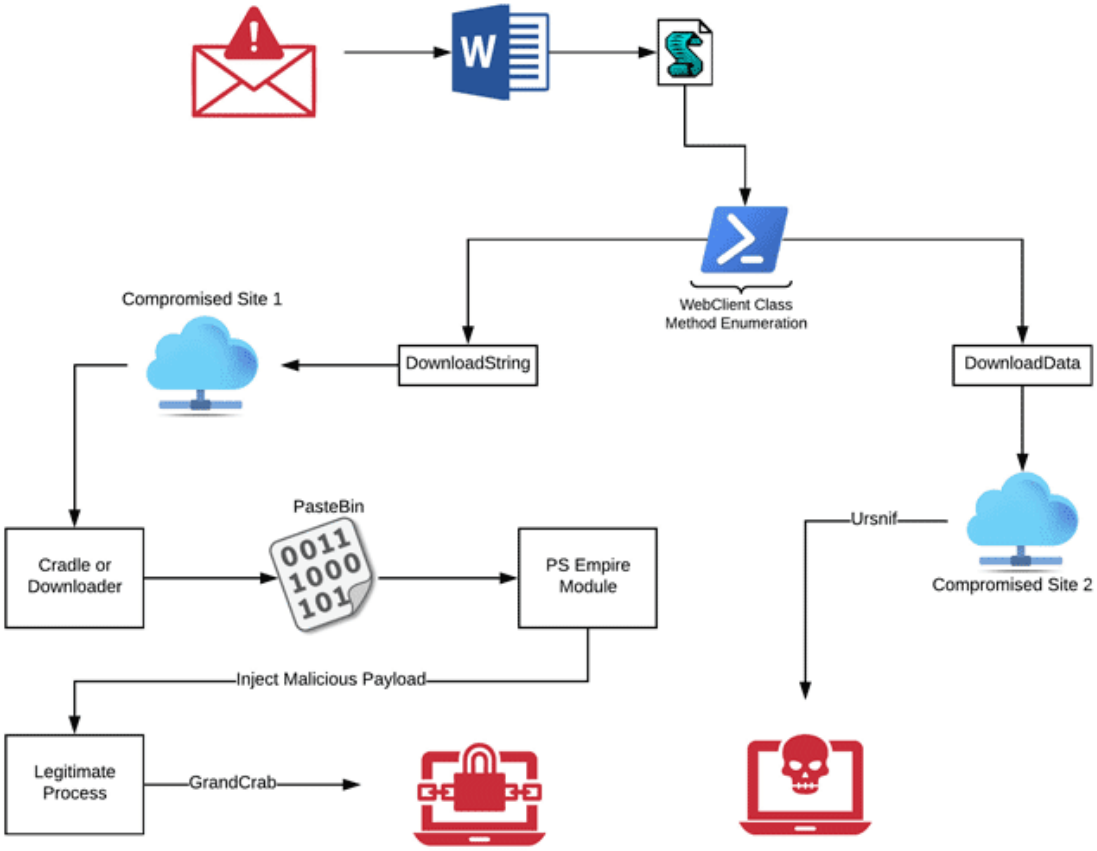
- جمع‌آوری اعتبارنامه‌های بانکی
- مرور فعالیت‌ها
- جمع‌آوری ضربه‌کلیدها و اطلاعات سیستم و فرآیند
- گسترش درِ پشتی[2] اضافی

[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.
[2] A backdoor is a technique in which a system security mechanism is bypassed undetectably to access a computer or its data.

گَندکِراب نیز مانند هر باج‌افزار دیگر در بازار فایل‌ها را بر روی سیستم آلوده رمزنگاری کرده و از قربانی جهت رمزگشایی آنها پولِ دیجیتال درخواست می‌کند. معمولا تقاضای پرداخت باج از طریق ارز دیجیتال دَش[1]- به دلیل پیچیدگی ردیابی آن- می‌باشد [۱].

اسناد ماکروسافت + ماکروهای وی.بی.اِس[2] = آلودگی گَندکِراب و اورسنیف

اولین گروه حملات بدافزاری مورد بحث توسط محققان حوزه امنیت اطلاعات شرکت کاربُن بِلَک[3] کشف شد. آنها برای این کار حدود ۱۸۰ نوع از اسناد ماکروسافت وُرد مخرب (دارای ماکروهای وی.بی.اِس) را در سطح اینترنت شناسایی کردند [۱]. ماکروهای وی.بی.اِس مخرب از طریق اجرای اسکریپت پاورشِل و برخی تکنیک‌های دیگر به دریافت و اجرای اورسنیف یا گَندکِراب روی سیستم هدف می‌پرداختند (شکل ۱) [۱].



شکل ۱: مراحل آلوده سازی سیستم توسط دو گروه حمله بدافزای جدید [۱]

[1] Dash is an open source cryptocurrency and is a form of decentralized autonomous organization run by a subset of users, called "masternodes". It is an altcoin that was forked from the Bitcoin protocol. The currency permits fast transactions that can be untraceable.

[2] VBScript is an Active Scripting language developed by Microsoft that is modeled on Visual Basic. It allows Microsoft Windows system administrators to generate powerful tools for managing computers with error handling, subroutines, and other advanced programming constructs.

[3] Carbon Black, Inc. is a cybersecurity company based in Waltham, Massachusetts.

اسکریپت پاورشل (کدگذاری شده در بیس۶۴[1]) پس از اجرا در سیستم قربانی به بارگیری محموله‌ی بدافزار اصلی می‌پردازد. اولین محموله- پاورشِل تک خطی[2]- پس از بررسی معماری سیستم یک محموله دیگر را از تارنمای پِیست‌بین[3] دریافت می‌کند. محموله‌ای که با اجرا در حافظه توسط ضد ویروس‌های سنتی قابل شناسایی نیست. هدف نهایی این فرآیند نصب نوعی باج‌افزار گَندکِراب بر روی سیستم قربانی و رمزنگاری فایل‌ها جهت دریافت باج است.

دومین گروه حملات بدافزای توسط محققان حوزه امنیت شرکت سیسکو تالوس[4] کشف شد. در این حملات اسناد ماکروسافت وُرد -حاوی ماکروهای وی.بی.اِس مخرب- به منظور ارائه نوع دیگری از بدافزارهای اورسیف به کار گرفته شده و سیستم را طی چند مرحله تحت اختیار می‌گیرد. در این حملات نیز با پست الکترونیکی فیشینگ فرمان‌های پاورشِل و ارائه بدافزار بدون فایل آغاز و در ادامه بدافزار اورسنیف دریافت و نصب می‌شود. بدافزار مذکور هنگام اجرا بر روی رایانه قربانی اطلاعات را از سیستم قربانی جمع‌آوری و در فرمت فایل سی.اِی.بی[5] قرار می‌دهد. این اطلاعات در انتها به سرور فرمان و کنترل با اتصال امن اچ.تی.تی.پی.اِس[6] ارسال می‌شود [۱].

پیشنهادات [۱]:

- احتیاط نسبت به پست‌های الکترونیکی دریافتی از منابع ناشناس
- توجه به لیست منتشر شده (آی.اُ.اِس)[7] توسط شرکت تالوس جهت تشخیص و جلوگیری از فعالیت بدافزارهای اورسنیف (ین لیست حاوی مشخصات رایانه‌های تحت تاثیر به همراه محموله‌های بارگذاری‌شده در آن است)

منابع :

1. TheHackerNews Website
https://thehackernews.com/2019/01/microsoft-gandcrab-ursnif.html?m=1

[1] Base64 is a group of similar binary-to-text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation.
[2] one-liner
[3] A pastebin or text storage site is a type of online content hosting service where users can store plain text, e.g. to source code snippets for code review via Internet Relay Chat (IRC). The first pastebin was the eponymous pastebin.com.
[4] Cisco Talos:the Talos Security Intelligence and Research Group (Talos) is made up of leading threat researchers supported by sophisticated systems to create threat intelligence for Cisco products that detects, analyzes and protects against both known and emerging threats.
[5] Cabinet(CAB) is an archive-file format for Microsoft Windows that supports lossless data compression and embedded digital certificates used for maintaining archive integrity. Cabinet files have .cab filename extensions and are recognized by their first 4 bytes MSCF. Cabinet files were known originally as Diamond files.
[6] Hypertext Transfer Protocol Secure is an extension of the Hypertext Transfer Protocol for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security, or, formerly, its predecessor, Secure Sockets Layer.
[7] Indicator of compromise (IOC) — in computer forensics is an artifact observed on a network or in an operating system that with high confidence indicates a computer intrusion.