

بسمه تعالی



وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات



مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

حمله بدافزاری هدفمند از نوع درب پشتی با استفاده از

PowerShell

گزارش بدافزار

شناسه سند MaherReports_14020214
نوع سند گزارش فنی
شماره نگارش ۰۱
تاریخ نگارش ۱۴۰۲/۰۲/۱۴
طبقه‌بندی سند **عادی**

تهران، خیابان شهید بهشتی - بین بزرگراه شهید مدرس و خیابان احمد قصیر - پلاک ۲۶۷



(۰۲۱) ۴۲۶۵۰۰۰۰



(۰۲۱) ۴۲۶۵۰۰۰۰





۱.....	مقدمه	۱
۱.....	جزئیات آسیب پذیری	2
۶.....	محصولات تحت تأثیر	۳
۶.....	توصیه‌های امنیتی	۴
۷.....	شاخصهای IOC	5
۷.....	منابع خبر	۶

۱ مقدمه

محققان Threatmon یک حمله بدافزاری هدفمند از نوع درب پشتی و با استفاده از PowerShell را از گروه جاسوسی APT41 شناسایی کردند که قادر است انواع روش‌های شناسایی را دور بزند و به مهاجمان اجازه می‌دهد در سیستم‌عامل ویندوز قربانی، دستوراتی را اجرا کنند، فایل دانلود یا آپلود کنند و اطلاعات حساس را جمع‌آوری کنند.

از سال ۲۰۱۲، گروه جاسوسی سایبری چینی APT41 (معروف به پاندای تبهکار) از تاکتیک‌ها، تکنیک‌ها و رویه‌های پیشرفته (TTPs) استفاده کرده است. آن‌ها از بدافزار اختصاصی و ابزارهایی مانند درب پشتی PowerShell در زرادخانه مخرب خود استفاده می‌کنند.

مایکروسافت ویندوز، زبان اسکریپت نویسی تعبیه شده‌ای به نام PowerShell دارد و می‌تواند پیکربندی‌های سیستم را مدیریت کرده و وظایف اجرایی را خودکار نماید.

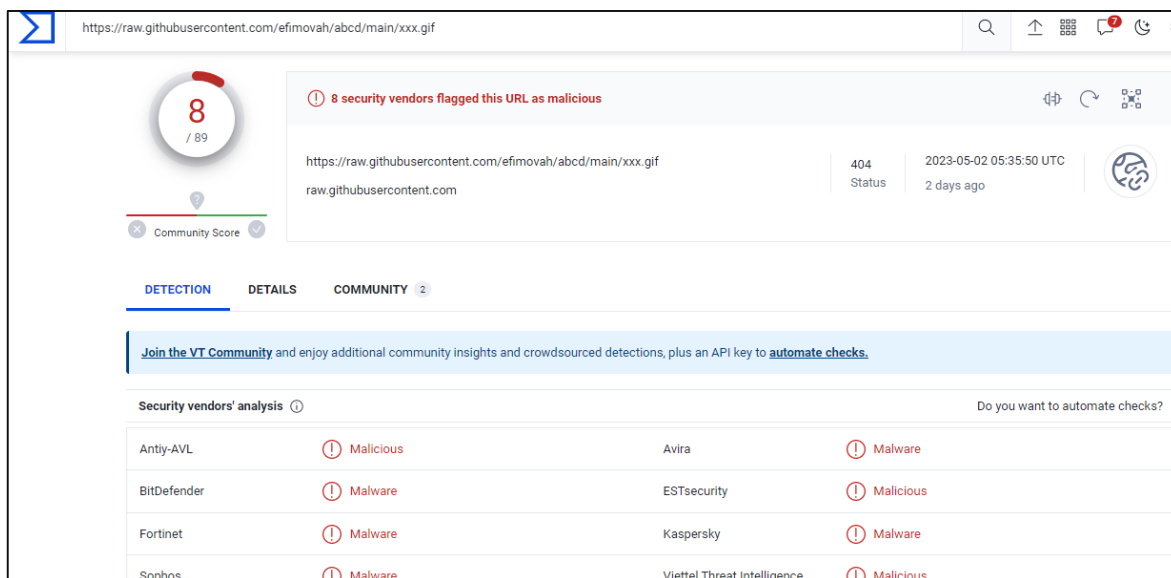
Alp Cihangir ASLAN و Seyit SIGIRCI، تحلیلگران بدافزار شرکت Threat Intelligence، ThreatMon، به سایت اخبار امنیت مجازی گزارش دادند که: «گروه APT41 با استفاده از درب پشتی PowerShell، اقدامات امنیتی متعارف را دور می‌زند که این امر، آن‌ها را قادر می‌سازد تا به سیستم‌های هدف نفوذ نماید.» «این گروه همچنین به دلیل استفاده از طیف گسترده‌ای از ابزارها و تکنیک‌های پیچیده، شامل بدافزار، حملات زنجیره‌ای و بهره‌برداری از آسیب‌پذیری‌ها در نرم‌افزار و سخت‌افزار معروف شده است.»

۲ جزئیات آسیب‌پذیری

به‌طور کلی بدافزار موردنظر به گروه جاسوسی سایبری اجازه می‌دهد تا دستورات را اجرا کند، فایل‌ها را دانلود و آپلود کند و اطلاعات را در پلتفرم‌های ویندوز جمع‌آوری کند. این گروه همچنین از بدافزارهای سفارشی، حملات زنجیره تامین و سایر آسیب‌پذیری‌های نرم‌افزاری پیشین برای حمله به اهداف با مشخصات بالا استفاده کرده است. درب پشتی PowerShell به APT41 اجازه می‌دهد تا اهداف را در مدت‌زمان طولانی به‌طور مخفیانه رصد کند. این بدافزار اغلب به‌عنوان یک بسته ثانویه در حملات هدفمند عمل می‌کند که نیاز به اقدامات امنیتی تقویت‌شده را برجسته می‌کند. PowerShell خود را با جاسازی payloads در رجیستری ویندوز اجرا می‌کند که اولین مورد آن "forfiles.exe" نام دارد. payload نهایی می‌تواند دستگاه‌های قابل جابجایی را آلوده کند و تلگرام را به‌عنوان یک سرور C2 ایجاد کند. این به Backdoor اجازه می‌دهد تا با استفاده از ip-API اطلاعات را به سرور C2 منتقل کند.

شاخص‌های IOC ذکر شده در سایت virustotal بررسی شدند که درهم سازی‌ها نتیجه‌ای تا زمان تهیه این مستند ثبت نشده بود اما `hXXps://raw.githubusercontent.com/efimovah/abcd/main/xxx.gif` و `hXXp://ip-api[.]com/json` بررسی شدند و نتایج آن در گزارش به شرح زیر می‌باشد:

در شکل ۱، در سایت `virustotal` `hXXps://raw.githubusercontent.com/efimovah/abcd/main/xxx.gif` را به‌عنوان بدافزار و مخرب تشخیص داده اما نوع آن را شناسایی نکرده است.



شکل ۱. تشخیص بدافزار

دسته‌بندی این url و درواقع محتوای دامنه موردبررسی بدین صورت هست که حوزه تهدیدش فناوری اطلاعات می‌باشد و به‌عنوان بدافزار و نرم‌افزار جاسوسی شناسایی شده که سرورش از حوزه ارتباطات سیار می‌باشد.

Categories	
Forcepoint ThreatSeeker	information technology
Sophos	spyware and malware
Xcitiium Verdict Cloud	mobile communications

شکل ۲. دسته‌بندی url

داده‌های جمع‌آوری شده از ارتباطات http هنگام بررسی url به شرح زیر می‌باشد:

لینک آدرس و آدرس ip ذخیره شده به شرح زیر می‌باشند که کد وضعیت ۴۰۴ است که به کاربر وب می‌گوید صفحه درخواستی موجود نیست و به این معنی است که سرور نمی‌تواند صفحه وب درخواستی کلاینت را پیدا کند و درواقع موجود نبوده است. همچنین سایز body و درهم سازی آن مطابق شکل ۳ می‌باشد.

HTTP Response ①	
Final URL	https://raw.githubusercontent.com/efimovah/abcd/main/xxx.gif
Serving IP Address	185.199.108.133
Status Code	404
Body Length	14 B
Body SHA-256	d5558cd419c8d46bdc958064cb97f963d1ea793866414c025906ec15033512ed

شکل ۳. سایز body و درهم سازی url

اطلاعات هدر به شرح زیر می‌باشند:

فیلتر XSS را فعال می‌کند کرده که در صورت شناسایی حمله، مرورگر به جای پاک‌سازی صفحه، از نمایش صفحه جلوگیری می‌کند. از Xcache که یک opcode cache منبع باز است، استفاده کرده به این معنی که عملکرد PHP را در سرورها تسریع می‌کند. XCache با حذف زمان کامپایل اسکریپت‌های PHP با ذخیره کردن حالت کامپایل شده آن‌ها در SHM (RAM) عملکرد را بهینه می‌کند. همچنین، XCache از نسخه کامپایل شده مستقیماً از RAM استفاده می‌کند، که زمان تولید صفحه را تا ۵ برابر افزایش می‌دهد، همچنین جنبه‌های مختلف اسکریپت‌های PHP را بهینه می‌کند و بار سرور را کاهش می‌دهد. Cache Hit زمانی رخ می‌دهد که یک برنامه یا نرم‌افزار اطلاعات را درخواست کند. ابتدا، CPU به دنبال داده‌ها در نزدیک‌ترین مکان حافظه خود، که معمولاً cache اولیه است، می‌گردد. اگر داده‌های درخواستی در cache یافت شوند، به‌عنوان یک cache hit در نظر گرفته می‌شوند. از connection:keep alive استفاده کرده که ارتباط بین یک کلاینت و سرور را حفظ می‌کند و زمان موردنیاز برای ارائه فایل‌ها را کاهش می‌دهد. اتصال دائمی همچنین تعداد درخواست‌های اتصال TCP و SSL/TLS را کاهش می‌دهد که منجر به کاهش زمان رفت‌و برگشت (RTT) می‌شود. هدف ارتباطات سریع و افزایش عملکرد جهت پیش برد سریع مقصود بوده است. از Varnish استفاده کرده تا داده را بروی virtual memory ذخیره کند و فایل‌های استاتیک و anonymous page-views را بسیار سریع‌تر و در حجم‌های بالاتر از آپاچی پردازش می‌کند. همچنین جلوی اجرا در محیط sandbox را گرفته است. هدر X-Content-Type-Options روی nosniff تنظیم‌شده و به مرورگر دستور می‌دهد که همیشه از نوع MIME که در هدر Content-Type تعریف‌شده است استفاده کند نه اینکه سعی کند نوع MIME را بر اساس محتوای فایل تعیین کند. Vary به‌صورت Authorization, Accept-Encoding, Origin تنظیم‌شده که هدف اصلی آن این است که به مرورگرها اطلاع دهد که کلاینت می‌تواند نسخه فشرده وبسایت را مدیریت کند.

xFrameOptions: DENY تنظیم شده که این هدر، هدری است که صفحه را از نمایش در یک فریم منع می‌کند و صفحه ورود به سیستم شما مجاز به بارگیری کدهای جاسازی ارائه‌شده توسط Credo که از عنصر iframe HTML استفاده می‌کنند، نخواهد بود در واقع امکان استفاده از کد جاسازی‌شده از مکان دیگر را غیرفعال کرده است. سایر اطلاعات هدر اعم از اندازه، زمان منقضی شدن، شناسه درخواست و ... نیز مطابق شکل ۴ می‌باشد:

Headers	
Content-Length	14
X-XSS-Protection	1; mode=block
X-Cache	HIT
Accept-Ranges	bytes
Strict-Transport-Security	max-age=31536000
Source-Age	0
Connection	keep-alive
Via	1.1 varnish
X-Cache-Hits	1
Access-Control-Allow-Origin	*
Expires	Tue, 02 May 2023 05:40:51 GMT
X-Served-By	cache-chi-klot8100157-CHI
Content-Security-Policy	default-src 'none'; style-src 'unsafe-inline'; sandbox
X-Content-Type-Options	nosniff
X-GitHub-Request-Id	EDFA:9897:15B37D:19A54A:6450A137
X-Timer	S1683005752.787697,VS0,VE0
Vary	Authorization,Accept-Encoding,Origin
X-Fastly-Request-ID	2a16eb5d8052d28380285e17f56031f2f96ddd3a
Date	Tue, 02 May 2023 05:35:51 GMT
Content-Type	text/plain; charset=utf-8
X-Frame-Options	deny

شکل ۴. سایر اطلاعات هدر

در بررسی `hXXp://ip-api[.]com/json` در سایت `virustotal`، مطابق شکل ۵ مخرب شناخته‌نشده است و تاکنون عملکرد نامتعارفی تشخیص داده نشده است.

http://ip-api.com/json

No security vendors flagged this URL as malicious

http://ip-api.com/json
ip-api.com

200 Status
2023-05-01 06:45:37 UTC
3 days ago

DETECTION DETAILS COMMUNITY 13+

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AICC (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
AlphaSOC	Clean	Antiy-AVL	Clean

شکل ۵. بررسی سایت virustotal در hXXp://ip-api[.]com/json

حمله درب پشتی پیشرفته PowerShell گروه APT41، بر اهمیت اقدامات امنیتی قوی برای سازمان‌ها به منظور مقابله با تهدیدات پیشرفته می‌افزاید.

حملات سایبری مشهور مانند نقض داده‌های Equifax در سال ۲۰۱۷، هوشمندی و توانمندی‌های این گروه مهاجم را نشان می‌دهد.

برای گریز از تشخیص و جلوگیری از آلوده شدن مجدد، این بدافزار از یک تاکتیک هوشمندانه استفاده می‌کند به این طریق که یک mutex به نام "v653Bmua-53JCY7Vq-tgSAaiwC-SSq3D4b6" قبل از اجرا ایجاد می‌کند.

باین حال اگر ایجاد mutex ناموفق باشد، با بازگشت دادن مقدار ۱، اجرا خاتمه می‌یابد.

```
int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int
{
    if ( !CreateMutexA(0, 0, "v653Bmua-53JCY7Vq-tgSAaiwC-SSq3D4b6") )
        return 1;
    if ( (unsigned __int8)sub_401000() )
        Sleep(0x3E8u);
    return 0;
}
```

شکل ۶. کد mutex

بدافزار، فرآیند اجرای خود را با قرار دادن سیستماتیک بارهای خود در رجیستری ویندوز آغاز می‌کند. اولین بار (payload)، با استفاده از یک LOLBin به نام "forfiles.exe" پیاده‌سازی می‌شود.

تمام این «living-off-the-land-binaries» یا Lolbin ها ابزارهای سیستمی اصلی هستند که عوامل تهدید، از آن‌ها برای انجام فعالیت‌های غیرقانونی استفاده می‌کنند

```
if ( RegOpenKeyExA(HKEY_CURRENT_USER, "Environment", 0, '\x0F\0?', &phkResult) )
    return 0;
if ( RegSetValueExA(
    phkResult,
    "UserInitMprLogonScript",
    0,
    1u,
    "C:\\Windows\\system32\\forfiles.exe /p c:\\windows\\system32 /m notepad.exe /c \"cmd.exe /c whoami >> %appdata%
    \"\\z.abcd && %appdata%\\z.abcd && del %appdata%\\z.abcd && exit\"",
    strlen("C:\\Windows\\system32\\forfiles.exe /p c:\\windows\\system32 /m notepad.exe /c \"cmd.exe /c whoami >> %a
    \"ppdata%\\z.abcd && %appdata%\\z.abcd && del %appdata%\\z.abcd && exit\"")
    + 1)

```

شکل ۷. کد Lolbin

ابزار Forfiles که عمدتاً برای جستجو استفاده می‌شود، می‌تواند دستوراتی را نیز اجرا کند و آن را به هدفی برای AV bypass با استفاده از LOLBins تبدیل کند.

یک دستور به‌طور خودکار در هنگام ورود به سیستم از طریق کلید HKCU\\Environment\\UserInitMprLogonScript به‌منظور ماندگاری اجرا می‌شود.

سپس تحت "HKEY_CLASSES_ROOT\\abcdfile\\shell\\open\\command\\abcd" بار رمزگذاری شده PowerShell با استفاده از LOLBin دیگری ساخته می‌شود:

● SyncAppPublishingServer.vbs

بار نهایی، یک درب پشتی غیرمتعارف PowerShell است که می‌تواند دستگاه‌های قابل جابجایی را آلوده کند و از تلگرام به‌عنوان سرور C2 استفاده کند.

اکنون درب پشتی، اطلاعات سیستم و آدرس IP را با اهرم ip-API، به سرور C2 منتقل می‌کند.

۳ محصولات تحت تأثیر

مایکروسافت ویندوز

۴ توصیه‌های امنیتی

تحلیلگران امنیت سایبری در ThreatMon تأکید کردند که اقدامات امنیتی پیشگیرانه برای سازمان‌ها ضروری است تا از تاکتیک‌های مخرب در حال تکامل پیشی بگیرند.

۵ شاخص‌های IOC

- **SHA-256 HASH:** *bb3d35cba3434f053280fc2887a7e6be703505385e184da4960e8db533cf4428*
- **SHA-256 HASH:** *d71f6fbc9dea34687080a2e12bf326966f6841d51294bd665261e07281459eeb*
- **URL:** *hXXps://raw.githubusercontent.com/efimovah/abcd/main/xxx.gif*
- **URL:** *hXXp://ip-api.com/json*

شکل ۸. شاخص‌های IOC

۶ منابع خبر

[1] <https://cybersecuritynews.com/apt41s-powershell-backdoor/>