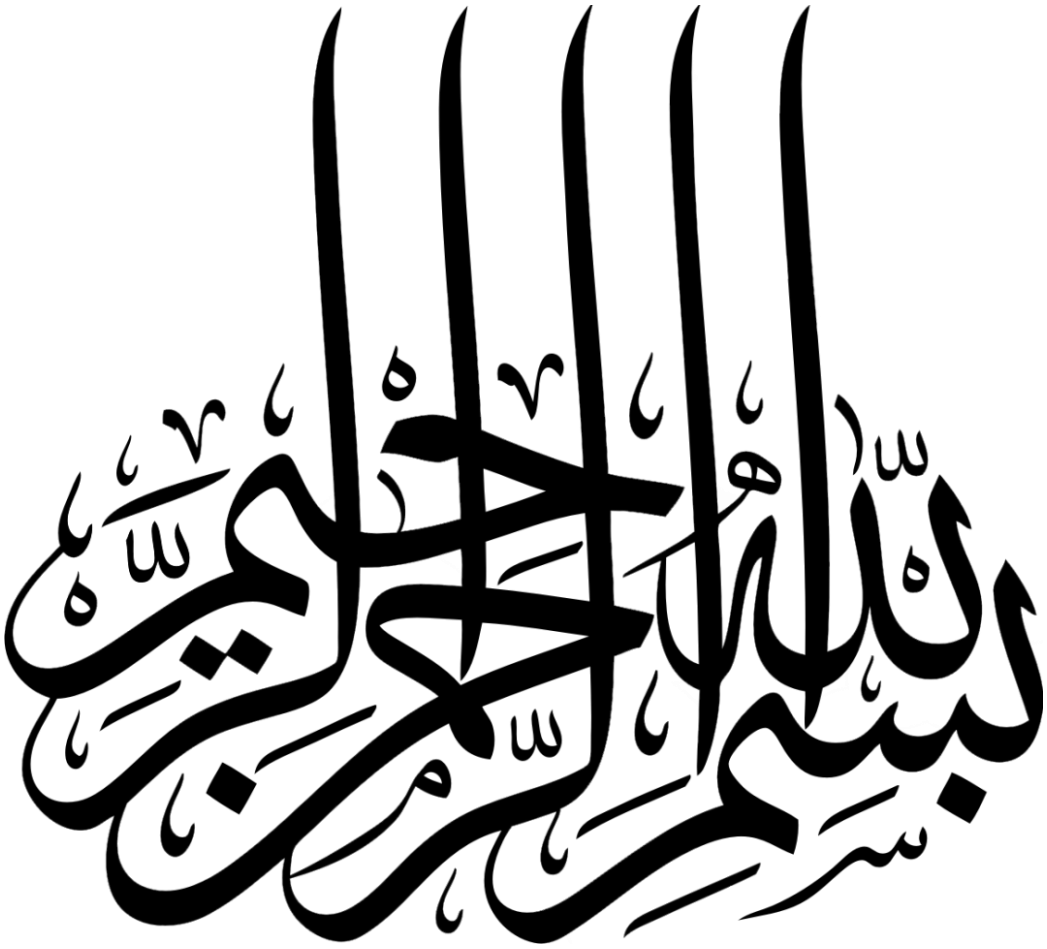
بسم الله الرحمن الرحیم

AdFind Recon

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو

فهرست مطالب

مقدمه

افزایش سوءاستفاده از دسترسی‌های RDP و ابزارهای قانونی ویندوز، به یکی از روش‌های رایج مهاجمان برای نفوذ و شناسایی شبکه‌های سازمانی تبدیل شده است. در این نوع حملات، مهاجمان بدون استفاده از بدافزارهای پیچیده، با تکیه بر ابزارهای خط فرمان و قابلیت‌های بومی سیستم‌عامل، اقدام به جمع‌آوری اطلاعات حساس و ایجاد دسترسی پایدار می‌کنند؛ موضوعی که شناسایی آن را برای تیم‌های امنیتی دشوارتر می‌سازد.

در یکی از نمونه‌های اخیر، مهاجمی از طریق سرویس RDP موفق به ورود به یک سیستم شد. وی ابتدا با استفاده از اجرای چند دستور خط فرمان اقدام به جمع آوری اطلاعات از سیستم نموده و خارج می شود. حدود پانزده دقیقه بعد، همان مهاجم با hostname جدیدی به نام MacBook-Pro مجدداً به سیستم متصل شد و با اجرای دستور whoami /upn تأیید کرد که سطح دسترسی خود را در محیط ویندوز بررسی کرده است.

در ادامه، این فرد ابزار AdFind را برای استخراج اطلاعات دامنه و ساختار Active Directory به کار گرفت.

هدف از این گزارش، مستندسازی و تحلیل فنی یک نمونه نفوذ واقعی مشاهده‌شده و افزایش درک نسبت به تاکتیک‌ها، تکنیک‌ها و رویه‌های (TTPs) مورد استفاده مهاجمان در مرحله شناسایی پس از دسترسی اولیه است. این گزارش تلاش می‌کند با بررسی نحوه استفاده از ابزار AdFind و الگوی رفتاری مهاجم در محیط Active Directory، به تیم‌های امنیتی در شناسایی زودهنگام چنین فعالیت‌هایی، بهبود مانیتورینگ، و تقویت کنترل‌های پیشگیرانه و تشخیصی در برابر حملات مشابه کمک کند.

توضیحات اولیه

یک مهاجم از آدرس 217.182.242.13 (OVH) و از طریق سرویس RDP با hostname به نام WORK9F3B وارد سیستم می‌شود.

adf.bat - Notepad

File Edit Format View Help

```
cd /d "C:\Users\SVC-DA~1\AppData\Local\Temp\10\tmp$\Downloads"
adfind.exe  -f "(objectcategory=person)" > ad_users.txt
adfind.exe  -f "objectcategory=computer" > ad_computers.txt
adfind.exe -sc trustdmp > trustdmp.txt
adfind.exe -subnets -f (objectCategory=subnet)> subnets.txt
adfind.exe -gcb -sc trustdmp > trustdmp.txt
adfind.exe -sc domainlist > domainlist.txt
adfind.exe -sc dcmodes > dcmodes.txt
adfind.exe -sc adinfo > adinfo.txt
adfind.exe -sc dclist > dclist.txt
adfind.exe -sc computers_pwdnotreqd > computers_pwdnotreqd.txt
```

ظرف ۲۰ ثانیه، آن‌ها یک Command Prompt باز کردند و دستورهای زیر را اجرا کردند:

```
C:\Users'             >nltest /domain_trusts /all_trusts
List of domain trusts:
    0:                                  (Forest Tree Root) (Primary Domain) (Native)
The command completed successfully

C:\Users'             >net user

User accounts for \'

-------------------------------------------------------------------------------

The command completed successfully.
```

سپس مهاجم خارج شد و ۱۵ دقیقه بعد دوباره وارد شد، این بار از یک hostname به نام MacBook-Pro پس از ورود، دستور whoami /upn را اجرا کردند و سپس AdFind را اجرا کردند.

AdFind یک ابزار خط فرمان برای پرس‌وجوی Active Directory و جمع آوری اطلاعات از آن است. AdFind، ترکیبی از ابزارهایی مثل dsquery, ldp, search.vbs, ldapsearch و dsget با ویژگی‌های جالب است.

این ابزار سال‌ها قبل از dsquery/dsget و ابزارهای مشابه آمده است. البته هرچند بخشی از ویژگی‌های مفید آن‌ها در این ابزار نیز استفاده شده است.

لینک ابزار AdFind

سپس مهاجم یک batch file اجرا کرد که دستورات AdFind درون آن قرار داشت و خروجی آن‌ها را در فایل‌های txt ذخیره می‌کرد.

adf.bat - Notepad

File Edit Format View Help

```
cd /d "C:\Users\SVC-DA~1\AppData\Local\Temp\10\tmp$\Downloads"
adfind.exe  -f "(objectcategory=person)" > ad_users.txt
adfind.exe  -f "objectcategory=computer" > ad_computers.txt
adfind.exe -sc trustdmp > trustdmp.txt
adfind.exe -subnets -f (objectCategory=subnet)> subnets.txt
adfind.exe -gcb -sc trustdmp > trustdmp.txt
adfind.exe -sc domainlist > domainlist.txt
adfind.exe -sc dcmodes > dcmodes.txt
adfind.exe -sc adinfo > adinfo.txt
adfind.exe -sc dclist > dclist.txt
adfind.exe -sc computers_pwdnotreqd > computers_pwdnotreqd.txt
```

دستورات مورد استفاده در این فایل عبارتند از:

- **objectcategory=person**: تمام اشیاء افراد را پیدا می‌کند.
- **objectcategory=computer**: تمام کامپیوترهای دامنه را پیدا می‌کند.
- **trustdmp**: اشیاء Trust دامنه را استخراج می‌کند.
- **objectcategory=subnet**: تمام ساب‌نت‌ها را پیدا می‌کند.
- **domainlist**: تمام اطلاعات Domain در Forest را در قالب لیست DNS مرتب شده نمایش می‌دهد.
- **dcmodes**: Modeهای تمام DC ها در Forest را نمایش می‌دهد.
- **adinfo**: اطلاعات Active Directory همراه با اطلاعات whoami را نشان می‌دهد.
- **dclist FQDN**: تمام Domain Controller ها را استخراج می‌کند.
- **computers_pwdnotreqd**: کاربران بدون نیاز به رمز عبور را استخراج می‌کند.

مهاجم سپس یک کاربر Local Admin به نام Adm.1c با رمز adm99!@ ایجاد می‌کند. بعد از آن، مهاجمان دیده نشدند.

ما AdFind را چندین بار در گذشته برای شناسایی شبکه (recon) مشاهده کرده‌ایم و هنوز هم استفاده می‌شود.

مثال‌های بیشتر از استفاده AdFind برای شناسایی

FireEye مقاله‌ای در مورد Maze ransomware TTPs منتشر کرد که شامل استفاده از AdFind و اسکریپتی برای اجرای دستورات و خروجی گرفتن بود.

Cybereason مقاله‌ای درباره نفوذ Trickbot منتشر کرد که در آن از AdFind استفاده شده بود.

FireEye در آوریل ۲۰۱۹ مقاله‌ای درباره نفوذ FIN6 منتشر کرد که از AdFind استفاده کرده بود.

Visa در گزارش Situational Intelligence درباره فعالیت‌های FIN6 در ۲۰۱۹، استفاده از AdFind را ذکر کرده بود.

منبع:

https://thedfirreport.com/2020/05/08/adfind-recon