THE DFIR REPORT

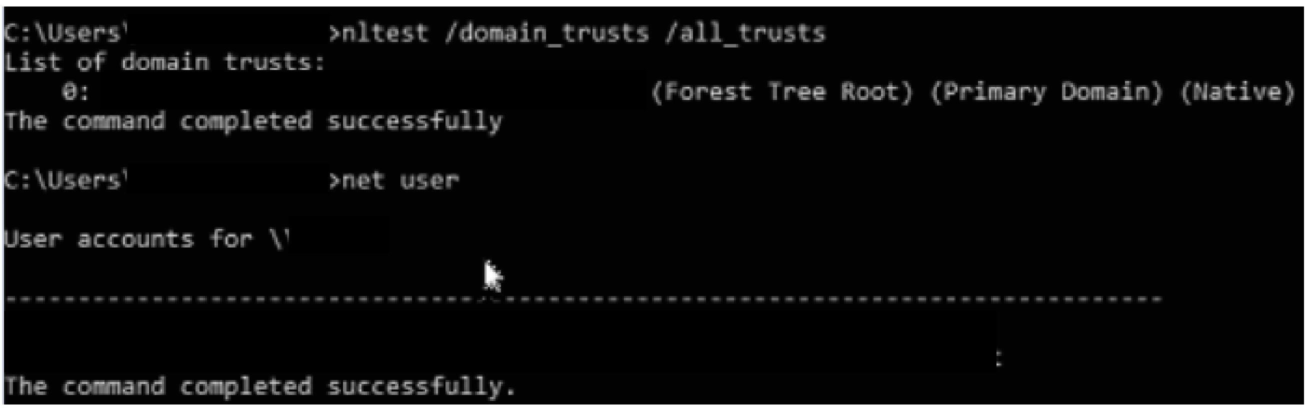
Real Intrusions by Real Attackers, The Truth Behind the Intrusion

rdp recon

AdFind Recon

May 8, 2020

A threat actor logged into the RDP honeypot from 217[.]182[.]242[.]13 (OVH) with a hostname of WORK9F3B. Within 20 seconds they opened a command prompt and issued the following commands



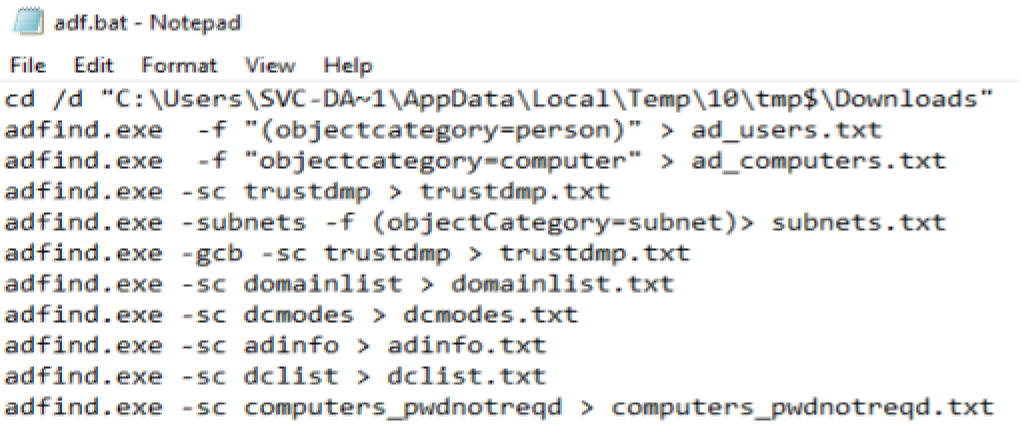
```
C:\Users\          >nltest /domain_trusts /all_trusts
List of domain trusts:
    0:                              (Forest Tree Root) (Primary Domain) (Native)
The command completed successfully

C:\Users\          >net user

User accounts for \\

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

The command completed successfully.
```

They then logged off and 15 minutes later logged back in from a hostname of MacBook-Pro (the resolution was a lot better compared to whatever they were using before 🙂). From there they ran whoami /upn and then dropped AdFind.

AdFind is described as the following:

> Command line Active Directory query tool. Mixture of ldapsearch, search.vbs, ldp, dsquery, and dsget tools with a ton of other cool features thrown in for good measure. This tool proceeded dsquery/dsget/etc by years though I did adopt some of the useful stuff from those tools.
>
> http://www.joeware.net/freetools/tools/adfind/

The threat actor then ran a batch file which ran AdFind commands and output them to txt files.



```
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
```

- objectcategory=person – Finds all person objects
- objectcategory=computer – Finds all computers in domain
- trustdmp – Dumps trust objects.
- objectcategory=subnet – Finds all subnets
- domainlist – Dumps all Domain NCs in forest in sorted DNS list format

Search Search

Sélectionner une langue ⌄
Fourni par Google Traduction

Subscribe

Register For Our Next CTF

Reports

Threat Intelligence

Detection Rules

- dcmodes – Shows modes of all DCs in forest from config
- adinfo – Shows Active Directory Info with whoami info.
- dclist – Dumps Domain Controllers FQDNs.
- computers_pwdnotreqd – Dumps users set with password not required.

AdFind usage can be found here.

The threat actors then added a local admin user named Adm.1c with a password of adm99!@. The actors were not seen again.

We’ve seen AdFind used numerous times for recon in the past and continue to see it today. Here are a few more examples of AdFind being used for recon:

- FireEye recently published an article on Maze ransomware TTPs which included the use of AdFind and a script to run and output files. Read more here.
- Cybereason put out an article last year on a Trickbot infection which used AdFind. Read more here.
- FireEye put out an article in April of 2019 which talked about a FIN6 intrusion which used AdFind. Read more here.
- Visa put out a Situational Intelligence Report on FIN6 activities in 2019 which included the use of AdFind. Read more here.

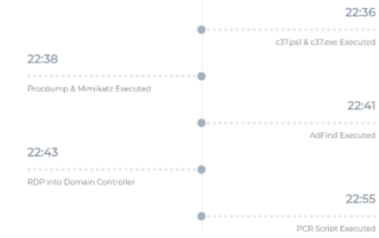
If you know of other instances where AdFind has been used for recon leading up to ransomware or other malicious activities please contact us so we can add it to the list.

Enjoy our report? Please consider donating $1 or more to the project using Patreon. Thank you for your support!

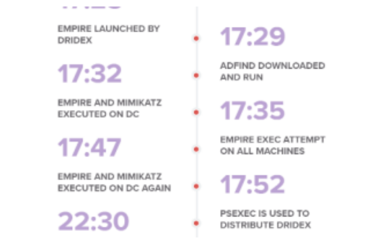
Share this:

Twitter | LinkedIn | Reddit | Facebook | WhatsApp

Related


22:36
c37.ps1 & c37.exe Executed
22:38
Procdump & Mimikatz Executed
22:41
AdFind Executed
22:43
RDP into Domain Controller
22:55
PCR Script Executed

NetWalker Ransomware in 1 Hour


EMPIRE LAUNCHED BY DRIDEX
17:29
17:32
ADFIND DOWNLOADED AND RUN
EMPIRE AND MIMIKATZ EXECUTED ON DC
17:35
17:47
EMPIRE EXEC ATTEMPT ON ALL MACHINES
EMPIRE AND MIMIKATZ EXECUTED ON DC AGAIN
17:52
22:30
PSEXEC IS USED TO DISTRIBUTE DRIDEX

Dridex – From Word to Domain Dominance

Ryuk in 5 Hours

« TRICKY PYXIE

LOCKBIT RANSOMWARE, WHY YOU NO SPREAD? »

DFIR Labs

Mentoring and Coaching