



Experiences from the attack on Lidingö city in 2019

Mimikatz

```
FILE EDIT VIEW SEARCH TERMINAL HELP
meterpreter > mimikatz_command -f samdump::hashes
Ordinateur : sathish-PC
BootKey    : 7edc62545ab8133464eb213b020caa26

Rid : 500
User : Administrator
LM :
NTLM : 31d6cfe0d16ae931b73c59d7e0c089c0

Rid : 501
User : Guest
LM :
NTLM :

Rid : 1000
User : sathish
LM :
NTLM : daadaf2f12980eb22e9eeca458ecf1da

Rid : 1004
User : arthar
LM :
NTLM : f932f72ba1e52155642c84361a366917
meterpreter > █
```




Illustration: Linux Digest, <https://sathisharthars.com/2014/07/09/dump-clear-text-password-with-mimikatz-using-metasploit/>

The cyber kill chain

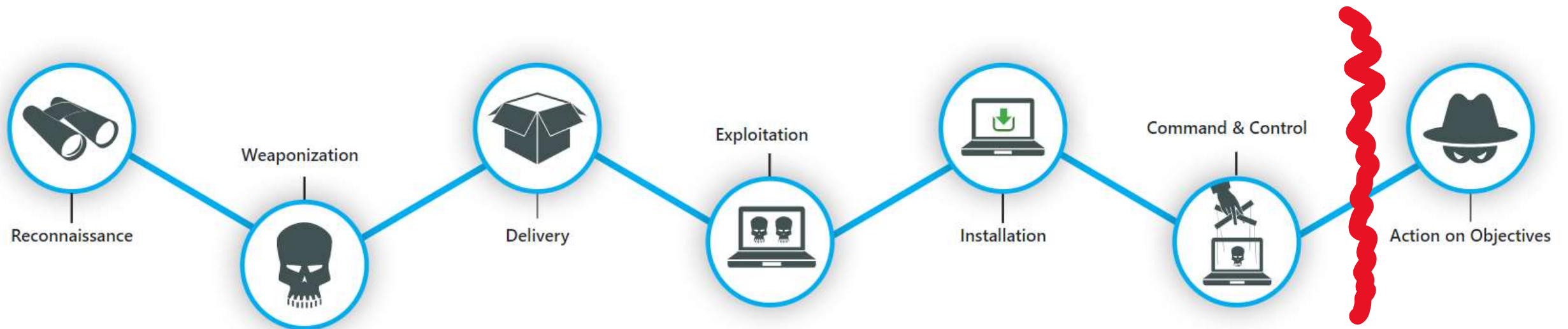


Illustration: www.lockheedmartin.com

199 emails on lidingo.se have been pwned in the Verifications.io data breach

- Får du för mycket e-post? Avsluta prenumerationen
- Översätt meddelandet till: Svenska | Översätt aldrig från: Engelska


H Have I Been Pwned <noreply@haveibeenpwned.com>
Sön 2019-03-10 04:33
Till: Per-Johan Gelotte



An email on a domain you're monitoring has been pwned

You signed up for notifications when emails on **lidingo.se** were pwned in a data breach and unfortunately, it's happened. Here's what's known about the breach:

Breach:	Verifications.io
Date of breach:	25 Feb 2019
Accounts found:	763,117,241
Your accounts:	199
Compromised data:	Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses

← Svava | ∨  Ta bort  Skräppost Blockera ...

Ev pågående spam attack?



Till: Per-Johan Gelotte
Kopia:

Hej,

Är lite smått orolig över en viss trendvarning ifrån Microsoft 365 Security & Compliance – Threat management, så tänkte flagga lite för det.

Bör nämnas att det är så pass nyligen som det aktiverades så svårt att säga hur pass ovanligt det är, men vi har gått ifrån ca 7 tusen spam mail om dagen, till runt 316 tusen i går och i dag.

Det mesta verkar fastna i filter, men en del slinker nog igenom.



Security State

Endpoint Protection Client Status

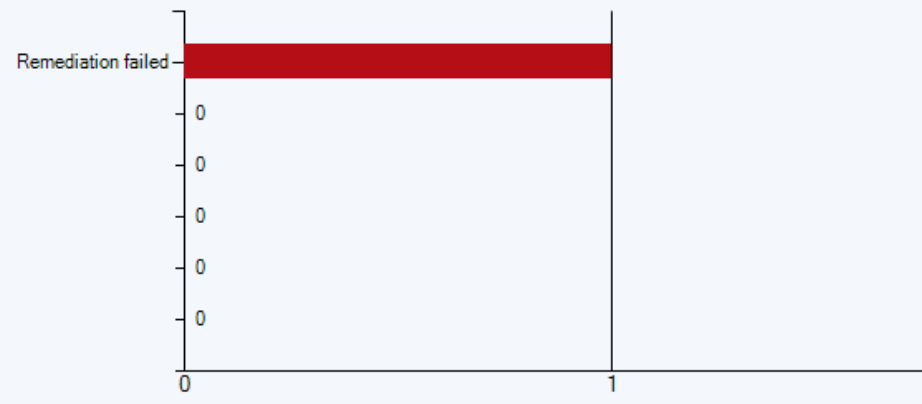
✔ Total active clients in this collection protected with Endpoint Protection: 97,1%

Endpoint Protection clients in this collection that are active: 1195

- ✔ Active clients protected with Endpoint Protection: 1160
- ✘ Active clients at risk: 35

Malware remediation status

✘ 1 /1472 affected by malware.



The chart displays a single red bar representing the number of remediation failures. The y-axis is labeled 'Remediation failed' and has tick marks at 0, 0, 0, 0, 0, 0, and 0. The x-axis has tick marks at 0 and 1. The bar extends to the value 1 on the x-axis.

Category	Count
Remediation failed	1

Security State

Endpoint Protection Client Status

Malware remediation status

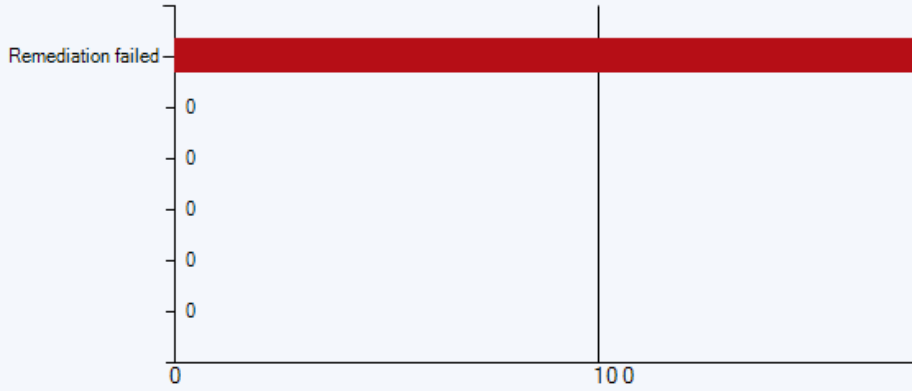
✔ Total active clients in this collection protected with Endpoint Protection: 97,1%

✘ 471 /1472 affected by malware.

Endpoint Protection clients in this collection that are active: 1195

✔ Active clients protected with Endpoint Protection: 1160

✘ Active clients at risk: 35



Category	Value
Total active clients protected with Endpoint Protection	97,1%
Active clients protected with Endpoint Protection	1160
Active clients at risk	35
Malware remediation status (affected)	471 / 1472

10 objects detected

Select action for found objects:

Copy all to quarantine Neutralize all Skip all Restore default actions

HEUR:Trojan.Win32.Scar.gen

@Filesystem[dbe44e4d-68f5-0314-9a55-cba5087038df]/Program Files (x86)/Profdoc/PMOClient/PMOWinHook.dll

Trojan program

MD5: 273EB5D1E31C709BD4C50B8A8A553C1A

SHA256: 486A3EED20F5E25B9A3B616AC35474252C5CBEC38C9B4D2C0C92068CCF4F6AC0

HEUR:Trojan.Script.Alien.gen

@Filesystem[dbe44e4d-68f5-0314-9a55-cba5087038df]/Users/bsk/AppData/Roaming/flashplayer.tmp

Trojan program

MD5: 17891737D9970812FE875D0B95580E15

SHA256: D5F4F04F00D874973BC5C9F166C6ECCAF635FC22657E418EE616ADF243E95601

HEUR:Trojan.Script.Alien.gen

@Filesystem[dbe44e4d-68f5-0314-9a55-cba5087038df]/Users/Default/AppData/Roaming/flashplayer.tmp

Trojan program

MD5: 17891737D9970812FE875D0B95580E15

SHA256: D5F4F04F00D874973BC5C9F166C6ECCAF635FC22657E418EE616ADF243E95601

HEUR:Trojan.Script.Alien.gen

@Filesystem[dbe44e4d-68f5-0314-9a55-cba5087038df]/Users/defaultuser0/AppData/Roaming/flashplayer.tmp

Trojan program

MD5: 17891737D9970812FE875D0B95580E15

SHA256: D5F4F04F00D874973BC5C9F166C6ECCAF635FC22657E418EE616ADF243E95601

HEUR:Trojan.Script.Alien.gen

@Filesystem[dbe44e4d-68f5-0314-9a55-cba5087038df]/Users/jati/AppData/Roaming/flashplayer.tmp

Trojan program

MD5: 17891737D9970812FE875D0B95580E15

SHA256: D5F4F04F00D874973BC5C9F166C6ECCAF635FC22657E418EE616ADF243E95601

HEUR:Trojan.Script.Alien.gen

@Filesystem[dbe44e4d-68f5-0314-9a55-cba5087038df]/Users/jatiinstall/AppData/Roaming/flashplayer.tmp

Trojan program

MD5: 17891737D9970812FE875D0B95580E15

SHA256: D5F4F04F00D874973BC5C9F166C6ECCAF635FC22657E418EE616ADF243E95601

HEUR:Trojan.Script.Alien.gen

@Filesystem[dbe44e4d-68f5-0314-9a55-cba5087038df]/Users/jony/AppData/Roaming/flashplayer.tmp

Trojan program

MD5: 17891737D9970812FE875D0B95580E15

SHA256: D5F4F04F00D874973BC5C9F166C6ECCAF635FC22657E418EE616ADF243E95601

HEUR:Trojan.Script.Alien.gen

@Filesystem[dbe44e4d-68f5-0314-9a55-cba5087038df]/Users/lal/AppData/Roaming/flashplayer.tmp

Trojan program

MD5: 17891737D9970812FE875D0B95580E15



Lidingö
stad



What worked well

- Crisis management
- "Sleeping" incident personnel
- External reviewer
- Continuity plans
- Information classification
- Solitary equipment for water and sewage, access systems etc

In the eye of the incident, "small" things have great significance

- Use the terms of crisis management
- Follow the routines/plans
- Nutrition



Photo: Per-Johan Gelotte

What worked **less well**

→ No automated actions
Automatic isolation

→ Permissive segmentation

→ Low awareness in the organization

IT and information security training for all managers
Fake phishing etc



2 Failed messages to you

Till: Per-Johan Gelotte

Office 365

Our server has detected some errors delivering 2 new messages to your inbox due to the synchronization delay.

Click on View Returned Messages below to retrieve these messages.

[View Returned Messages](#)

Result

→900 computers reinstalled/checked

→Incident personnel SEK 900,000

→Went out of incident mode after just over seven days

		RECEIVE TIME	TYPE	SEVERITY	FILE N
		10:47:28	vulnerability	high	getuse
		10:42:57	vulnerability	high	getuse
		10:39:02	vulnerability	high	getuse
		10:37:11	vulnerability	high	getuse
		10:31:03	vulnerability	high	getuse
		10:21:07	vulnerability	high	getuse
		10:11:04	vulnerability	high	getuse
		09:45:35	vulnerability	medium	leb.lidi

Per-Johan Gelotte



[linkedin.com/in/per-johan-gelotte](https://www.linkedin.com/in/per-johan-gelotte)



per-johan.gelotte@lidingo.se