Antivir vs EDR = historie vs budoucnost

Jakub Karvánek
Sales Director

FREEDIVISION
for safety reasons

NALÉHAVÝ PROBLÉM

Aktuální situace v českém zdravotnictví

- Častokrát jediná ochrana koncových zařízení je AV
- Různé AV a aktualizace v rámci jedné organizace
- Poddimenzované IT oddělení
- Zastaralá HW technika
- ČASTÝM TERČEM KYBERNETICKÝCH ÚTOKŮ.

+ Obdobná situace je i ve světě

Přední výzkum

Gartner

“Běžná antivirová řešení neposkytují **dostatečnou ochranu** před dnešními pokročilými hrozbami, **postrádají rychlou odezvu** a nejsou schopná **odhalit příčinu nebo rozsah škody.**”

Gartner

REAQTA

Zdroj: Market Guide for Endpoint Detection and Response Solutions (Gartner, 2019)

NALÉHAVÝ PROBLÉM

Mnoho organizací není připraveno na zvládání složitých situací

Tradiční ochrana a lidské týmy *nejsou schopné držet krok s pokročilými hrozbami*

ŠPATNÁ VIDITELNOST A SLEDOVÁNÍ

Špatná viditelnost v tradičních nástrojích znemožňuje vyhodnocení a reakci. Nemůžeme pracovat s rizikem, které ani nevidíme.

OMEZENÉ VYHLEDÁVÁNÍ A REAKCE

Tradiční přístup se opírá o vyhledávání již známého. Útočníci ale oběti nenapadají „známým“ (např. známé signatury), ale „neznámým“ (např. fileless/ransomware útoky) .

LIDÉ STĚŽÍ UDRŽÍ KROK

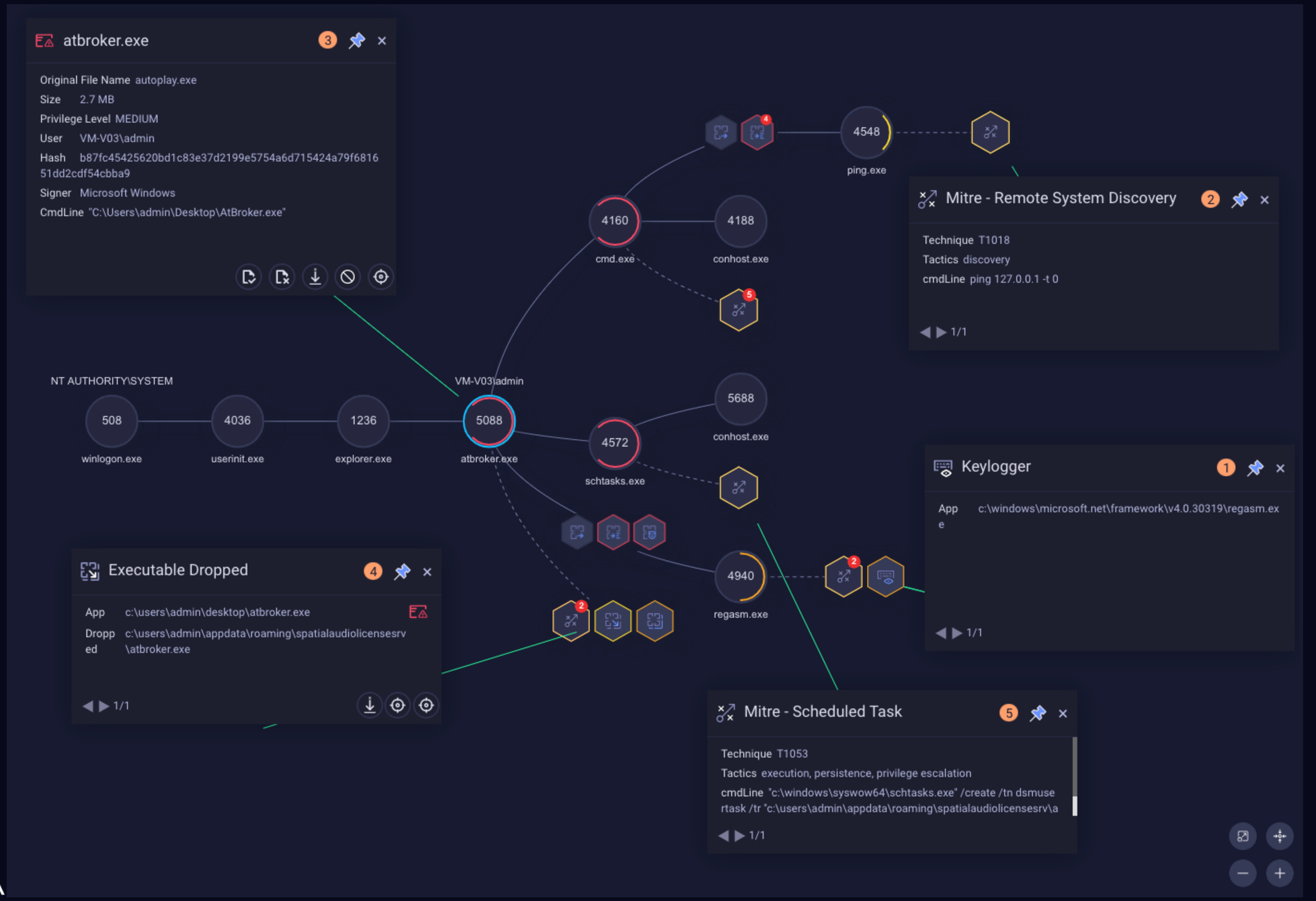
Současné hrozby jsou nesmírně složité a automatizované. Lidé neumí vyhodnocovat situace s mnoha pohyblivými částmi.

REAQTA

ARCHITEKTURA

Dejte Vaší bezpečnosti **nové super-schopnosti**

REAQTA


atbroker.exe
3
Original File Name autoplay.exe
Size 2.7 MB
Privilege Level MEDIUM
User VM-V03\admin
Hash b87fc45425620bd1c83e37d2199e5754a6d715424a79f681651dd2cdf54cbba9
Signer Microsoft Windows
CmdLine "C:\Users\admin\Desktop\AtBroker.exe"
4548
ping.exe
4160
cmd.exe
4188
conhost.exe
Mitre - Remote System Discovery
2
Technique T1018
Tactics discovery
cmdLine ping 127.0.0.1 -t 0
1/1
NT AUTHORITY\SYSTEM
VM-V03\admin
508
winlogon.exe
4036
userinit.exe
1236
explorer.exe
5088
atbroker.exe
4572
schtasks.exe
5688
conhost.exe
Keylogger
1
App c:\windows\microsoft.net\framework\v4.0.30319\regasm.exe
1/1
Executable Dropped
4
App c:\users\admin\desktop\atbroker.exe
Dropped c:\users\admin\appdata\roaming\spatialaudiolicensesrv\atbroker.exe
1/1
4940
regasm.exe
Mitre - Scheduled Task
5
Technique T1053
Tactics execution, persistence, privilege escalation
cmdLine "c:\windows\syswow64\schtasks.exe" /create /tn dsmusertask /tr "c:\users\admin\appdata\roaming\spatialaudiolicensesrv\a
1/1

REAQTA

INFRASTRUCTURE ARTIFACTS (3)

locky.exe

SHA256 70d06bd4e6a91b60bc8515e327fa1f9fb7ac82125e3c8a06359b5bb3f96e48f3

Seen in 3 other endpoints	Last Seen
FD-001 (192.168.71.8)	2020-12-08 14:03:13
MMALWARE (10.0.2.15)	2021-02-05 11:50:59
KMYRANSOMWARE2 (10.0.2.15)	2021-02-10 12:36:53

EXPORT RESULTS

Happened At	Endpoint	Type	Description	Has Alert
2021-03-15 10:37:17	REAQTA-RANSOMWA	File Deleted	cmd.exe deleted sys79a3.tmp from filesystem	
2021-03-15 10:37:17	REAQTA-RANSOMWA	Process Terminated	jarda.exe terminated	
2021-03-15 10:37:17	REAQTA-RANSOMWA	File Read	jarda.exe read file staticcache.dat	
2021-03-15 10:37:16	REAQTA-RANSOMWA	File Renamed	jarda.exe renamed file jarda.exe to sys79a3.tmp	
2021-03-15 10:37:16	REAQTA-RANSOMWA	File Created	jarda.exe created file sys79a3.tmp	
2021-03-15 10:37:16	REAQTA-RANSOMWA	Registry Value Set	jarda.exe set a persistency key called @{microsoft.windows....ces/appfriendlyname}	
2021-03-15 10:37:15	REAQTA-RANSOMWA	File Read	jarda.exe read file desktop.ini	
2021-03-15 10:37:15	REAQTA-RANSOMWA	File Read	jarda.exe read file desktop.ini	
2021-03-15 10:37:14	REAQTA-RANSOMWA	Registry Value Set	jarda.exe set a persistency key called wallpaper	
2021-03-15 10:37:14	REAQTA-RANSOMWA	Registry Value Set	jarda.exe set a persistency key called tilewallpaper	
2021-03-15 10:37:14	REAQTA-RANSOMWA	Registry Value Set	jarda.exe set a persistency key called wallpaperstyle	
2021-03-15 10:37:14	REAQTA-RANSOMWA	File Written	jarda.exe wrote content into ykcol.bmp	
2021-03-15 10:37:14	REAQTA-RANSOMWA	File Created	jarda.exe created file ykcol.bmp	
2021-03-15 10:37:14	REAQTA-RANSOMWA	File Written	jarda.exe wrote content into ykcol.htm	
2021-03-15 10:37:14	REAQTA-RANSOMWA	File Created	jarda.exe created file ykcol.htm	
2021-03-15 10:37:14	REAQTA-RANSOMWA	File Written	jarda.exe wrote content into 4qkk73yy-f83f-8664-2f806a71-5e5cf0f7133d.ykcol	

REAQTA

DOPORUČENÍ

SHRNUTÍ:

Zajištění kontinuity provozu

Využitelnost nástrojů vs kapacita IT

Automatizované analytické nástroje

Centrální dohled nad všemi zařízeními

Zajištění auditní stopy

FREEDIVISION
for safety reasons

DĚKUJI ZA POZORNOST

Jakub Karvánek
JAKUB.KARVANEK@FREEDIVISION.COM