BEZPEČNOSTNÍ IT EXPERTI
NA VAŠEJ STRANE

Ako efektívne "loviť" hrozby a vyšetriť incidenty

Július Selecký

Senior Technical Pre-Sales Representative

julius.selecky@eset.sk

Zákazník

- **verejná správa**
- **prevádzkovateľ základnej služby**
- **problém?**
  - phishingové útoky
  - hrozby priamo zvnútra spoločnosti
  - zákon č.69/2018 Z.z. o kybernetickej bezpečnosti

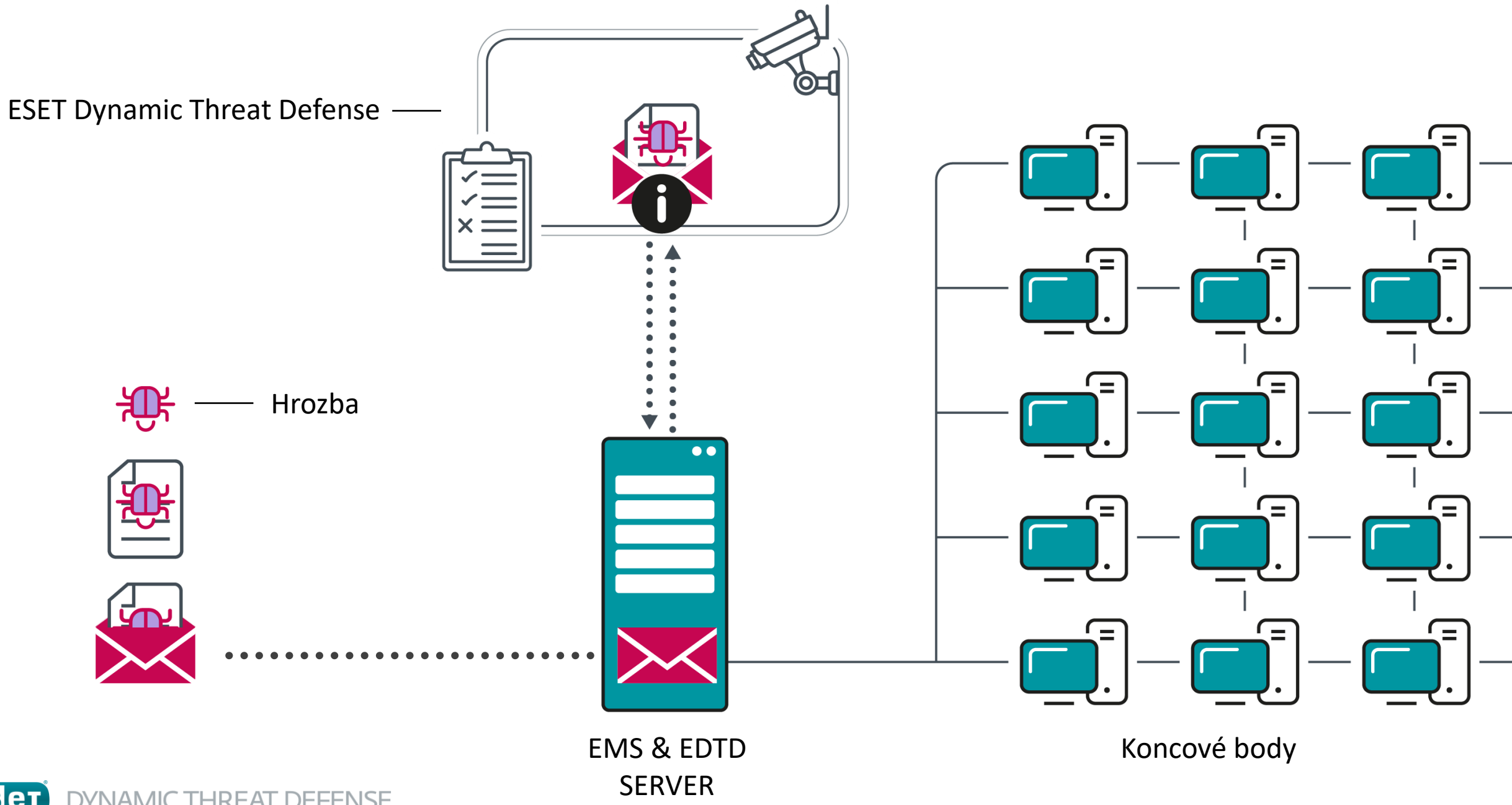
Phishing správy s malvérom

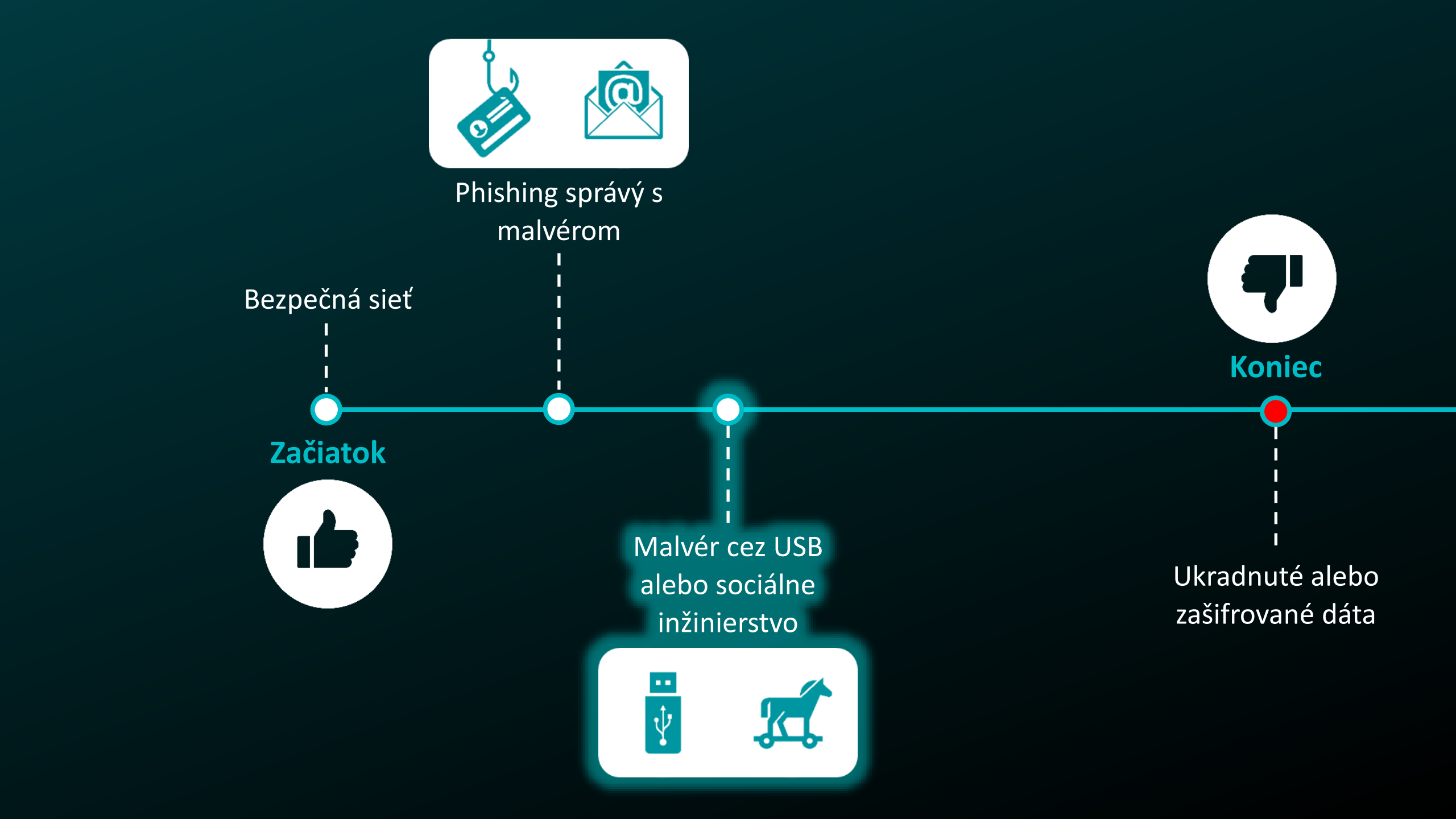
Bezpečná sieť

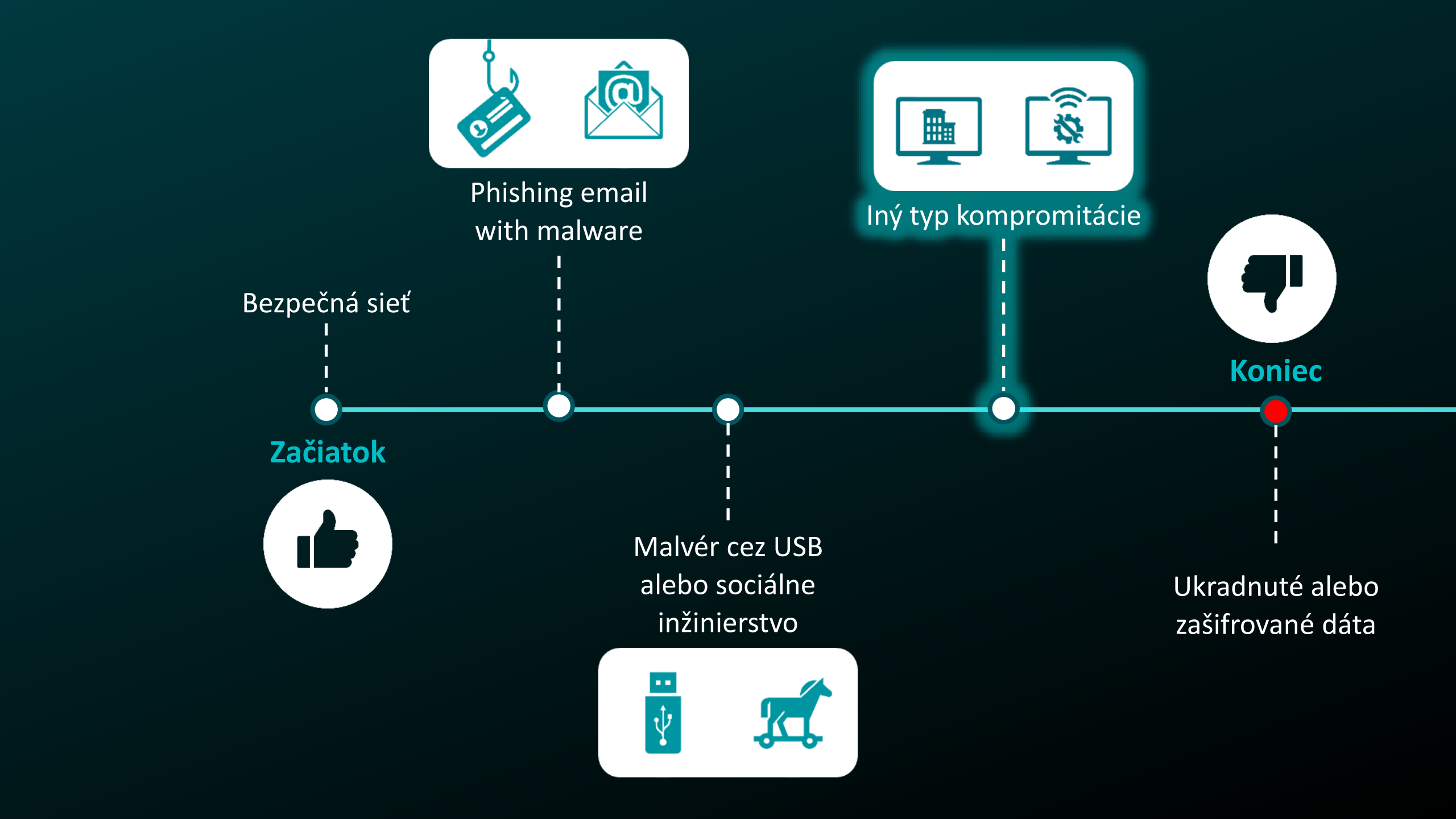
Začiatok

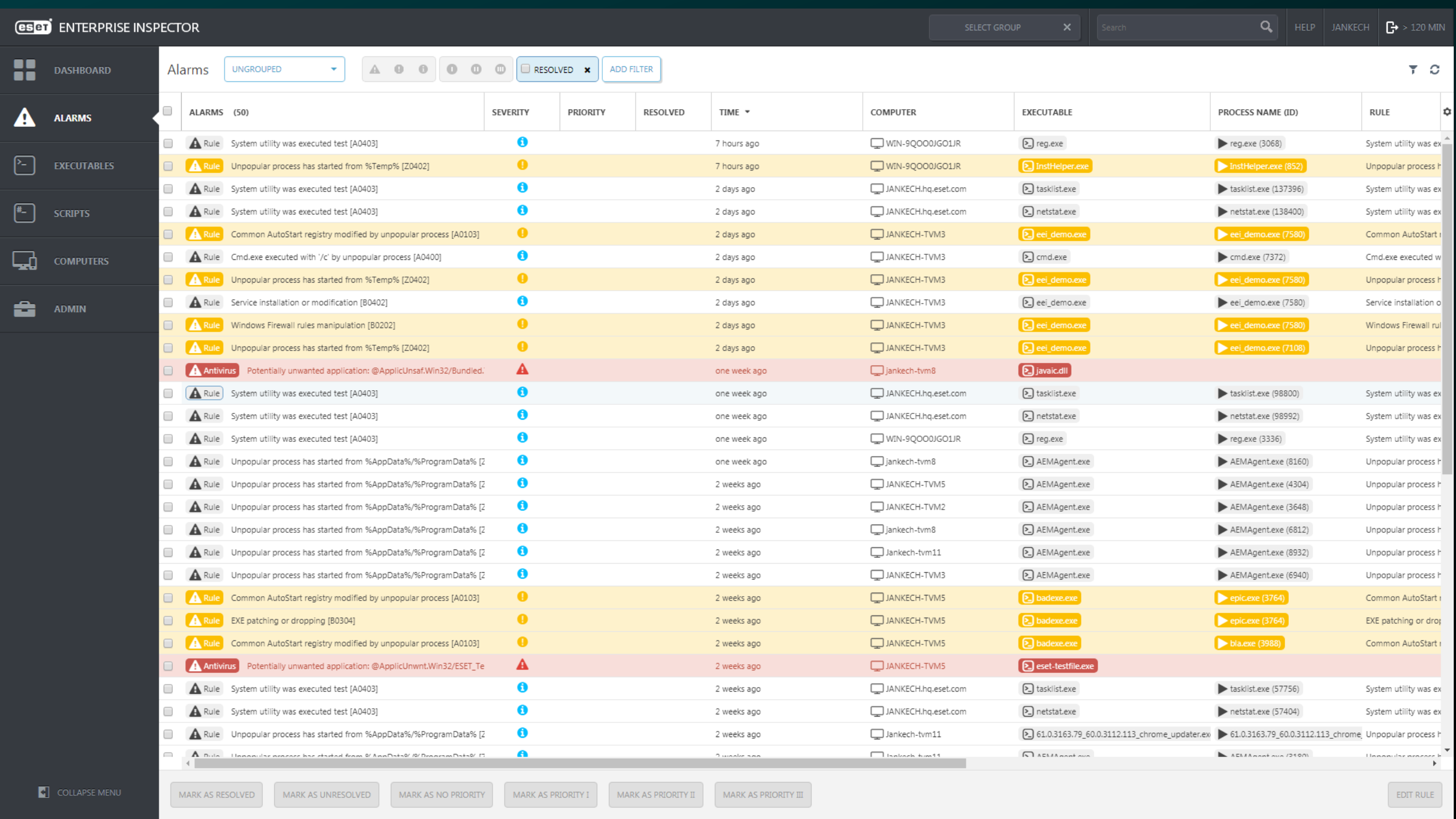
Koniec

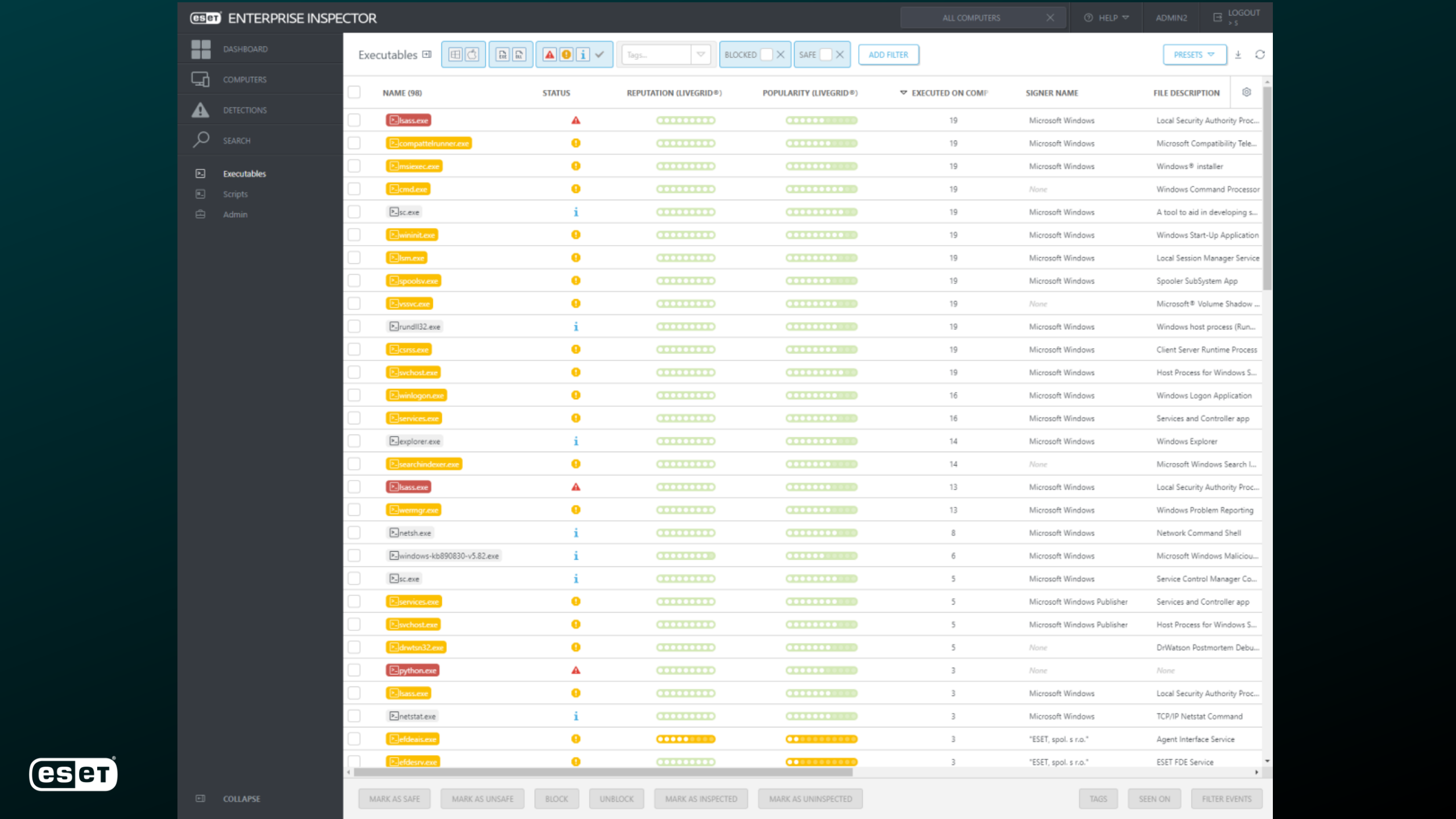
Ukradnuté alebo zašifrované dáta


ESET Dynamic Threat Defense
Hrozba
EMS & EDTD
SERVER
Koncové body


Phishing správý s malvérom
Bezpečná sieť
Koniec
Začiatok
Malvér cez USB alebo sociálne inžinierstvo
Ukradnuté alebo zašifrované dáta


Phishing email
with malware
Iný typ kompromitácie
Bezpečná sieť
Koniec
Začiatok
Malvér cez USB
alebo sociálne
inžinierstvo
Ukradnuté alebo
zašifrované dáta


ENTERPRISE INSPECTOR
SELECT GROUP
Search
HELP
JANKECH
> 120 MIN
DASHBOARD
ALARMS
EXECUTABLES
SCRIPTS
COMPUTERS
ADMIN
COLLAPSE MENU
Alarms
UNGROUPED
RESOLVED
ADD FILTER
ALARMS (50)
SEVERITY
PRIORITY
RESOLVED
TIME
COMPUTER
EXECUTABLE
PROCESS NAME (ID)
RULE
Rule System utility was executed test [A0403] 7 hours ago WIN-9QOO0JGO1JR reg.exe reg.exe (3068) System utility was ex
Rule Unpopular process has started from %Temp% [Z0402] 7 hours ago WIN-9QOO0JGO1JR InstHelper.exe InstHelper.exe (852) Unpopular process h
Rule System utility was executed test [A0403] 2 days ago JANKECH.hq.eset.com tasklist.exe tasklist.exe (137396) System utility was ex
Rule System utility was executed test [A0403] 2 days ago JANKECH.hq.eset.com netstat.exe netstat.exe (138400) System utility was ex
Rule Common AutoStart registry modified by unpopular process [A0103] 2 days ago JANKECH-TVM3 eei_demo.exe eei_demo.exe (7580) Common AutoStart
Rule Cmd.exe executed with '/c' by unpopular process [A0400] 2 days ago JANKECH-TVM3 cmd.exe cmd.exe (7372) Cmd.exe executed w
Rule Unpopular process has started from %Temp% [Z0402] 2 days ago JANKECH-TVM3 eei_demo.exe eei_demo.exe (7580) Unpopular process h
Rule Service installation or modification [B0402] 2 days ago JANKECH-TVM3 eei_demo.exe eei_demo.exe (7580) Service installation o
Rule Windows Firewall rules manipulation [B0202] 2 days ago JANKECH-TVM3 eei_demo.exe eei_demo.exe (7580) Windows Firewall rul
Rule Unpopular process has started from %Temp% [Z0402] 2 days ago JANKECH-TVM3 eei_demo.exe eei_demo.exe (7108) Unpopular process h
Antivirus Potentially unwanted application: @ApplicUnsaf.Win32/Bundled. one week ago jankech-tvm8 javaic.dll
Rule System utility was executed test [A0403] one week ago JANKECH.hq.eset.com tasklist.exe tasklist.exe (98800) System utility was ex
Rule System utility was executed test [A0403] one week ago JANKECH.hq.eset.com netstat.exe netstat.exe (98992) System utility was ex
Rule System utility was executed test [A0403] one week ago WIN-9QOO0JGO1JR reg.exe reg.exe (3336) System utility was ex
Rule Unpopular process has started from %AppData%/%ProgramData% [Z one week ago jankech-tvm8 AEMAgent.exe AEMAgent.exe (8160) Unpopular process h
Rule Unpopular process has started from %AppData%/%ProgramData% [Z 2 weeks ago JANKECH-TVM5 AEMAgent.exe AEMAgent.exe (4304) Unpopular process h
Rule Unpopular process has started from %AppData%/%ProgramData% [Z 2 weeks ago JANKECH-TVM2 AEMAgent.exe AEMAgent.exe (3648) Unpopular process h
Rule Unpopular process has started from %AppData%/%ProgramData% [Z 2 weeks ago jankech-tvm8 AEMAgent.exe AEMAgent.exe (6812) Unpopular process h
Rule Unpopular process has started from %AppData%/%ProgramData% [Z 2 weeks ago Jankech-tvm11 AEMAgent.exe AEMAgent.exe (8932) Unpopular process h
Rule Unpopular process has started from %AppData%/%ProgramData% [Z 2 weeks ago JANKECH-TVM3 AEMAgent.exe AEMAgent.exe (6940) Unpopular process h
Rule Common AutoStart registry modified by unpopular process [A0103] 2 weeks ago JANKECH-TVM5 badexe.exe epic.exe (3764) Common AutoStart
Rule EXE patching or dropping [B0304] 2 weeks ago JANKECH-TVM5 badexe.exe epic.exe (3764) EXE patching or drop
Rule Common AutoStart registry modified by unpopular process [A0103] 2 weeks ago JANKECH-TVM5 badexe.exe bla.exe (3988) Common AutoStart
Antivirus Potentially unwanted application: @ApplicUnwnt.Win32/ESET_Te 2 weeks ago JANKECH-TVM5 eset-testfile.exe
Rule System utility was executed test [A0403] 2 weeks ago JANKECH.hq.eset.com tasklist.exe tasklist.exe (57756) System utility was ex
Rule System utility was executed test [A0403] 2 weeks ago JANKECH.hq.eset.com netstat.exe netstat.exe (57404) System utility was ex
Rule Unpopular process has started from %AppData%/%ProgramData% [Z 2 weeks ago Jankech-tvm11 61.0.3163.79_60.0.3112.113_chrome_updater.ex 61.0.3163.79_60.0.3112.113_chrome Unpopular process h
MARK AS RESOLVED
MARK AS UNRESOLVED
MARK AS NO PRIORITY
MARK AS PRIORITY I
MARK AS PRIORITY II
MARK AS PRIORITY III
EDIT RULE


ENTERPRISE INSPECTOR
ALL COMPUTERS
HELP
ADMIN2
LOGOUT
DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
Executables
Scripts
Admin
COLLAPSE
Executables
Tags...
BLOCKED
SAFE
ADD FILTER
PRESETS
NAME (98)
STATUS
REPUTATION (LIVEGRID®)
POPULARITY (LIVEGRID®)
EXECUTED ON COMP
SIGNER NAME
FILE DESCRIPTION
lsass.exe 19 Microsoft Windows Local Security Authority Proc...
compattelrunner.exe 19 Microsoft Windows Microsoft Compatibility Tele...
msiexec.exe 19 Microsoft Windows Windows® installer
cmd.exe 19 None Windows Command Processor
sc.exe 19 Microsoft Windows A tool to aid in developing s...
wininit.exe 19 Microsoft Windows Windows Start-Up Application
lsm.exe 19 Microsoft Windows Local Session Manager Service
spoolsv.exe 19 Microsoft Windows Spooler SubSystem App
vssvc.exe 19 None Microsoft® Volume Shadow ...
rundll32.exe 19 Microsoft Windows Windows host process (Run...
csrss.exe 19 Microsoft Windows Client Server Runtime Process
svchost.exe 19 Microsoft Windows Host Process for Windows S...
winlogon.exe 16 Microsoft Windows Windows Logon Application
services.exe 16 Microsoft Windows Services and Controller app
explorer.exe 14 Microsoft Windows Windows Explorer
searchindexer.exe 14 None Microsoft Windows Search I...
lsass.exe 13 Microsoft Windows Local Security Authority Proc...
wermgr.exe 13 Microsoft Windows Windows Problem Reporting
netsh.exe 8 Microsoft Windows Network Command Shell
windows-kb890830-v5.82.exe 6 Microsoft Windows Microsoft Windows Maliciou...
sc.exe 5 Microsoft Windows Service Control Manager Co...
services.exe 5 Microsoft Windows Publisher Services and Controller app
svchost.exe 5 Microsoft Windows Publisher Host Process for Windows S...
drwtsn32.exe 5 None DrWatson Postmortem Debu...
python.exe 3 None None
lsass.exe 3 Microsoft Windows Local Security Authority Proc...
netstat.exe 3 Microsoft Windows TCP/IP Netstat Command
efdeais.exe 3 "ESET, spol. s r.o." Agent Interface Service
efdesrv.exe 3 "ESET, spol. s r.o." ESET FDE Service
MARK AS SAFE
MARK AS UNSAFE
BLOCK
UNBLOCK
MARK AS INSPECTED
MARK AS UNINSPECTED
TAGS
SEEN ON
FILTER EVENTS

< BACK

Alarm details

Filecoder behaviour [Z0601]

SOURCE	Filecoder behaviour [Z0601]
CATEGORY	Filecoders
OCCURED	11 minutes ago - Mar 7, 2018, 4:57:39 PM
PRIORITY	0

svchost.exe

SIGNATURE TYPE	None
SIGNER NAME	None
SEEN ON	2 computers
FIRST SEEN	one day ago - Mar 6, 2018, 2:55:50 PM
LAST EXECUTED	11 minutes ago - Mar 7, 2018, 4:57:38 PM

ESET LiveGrid®

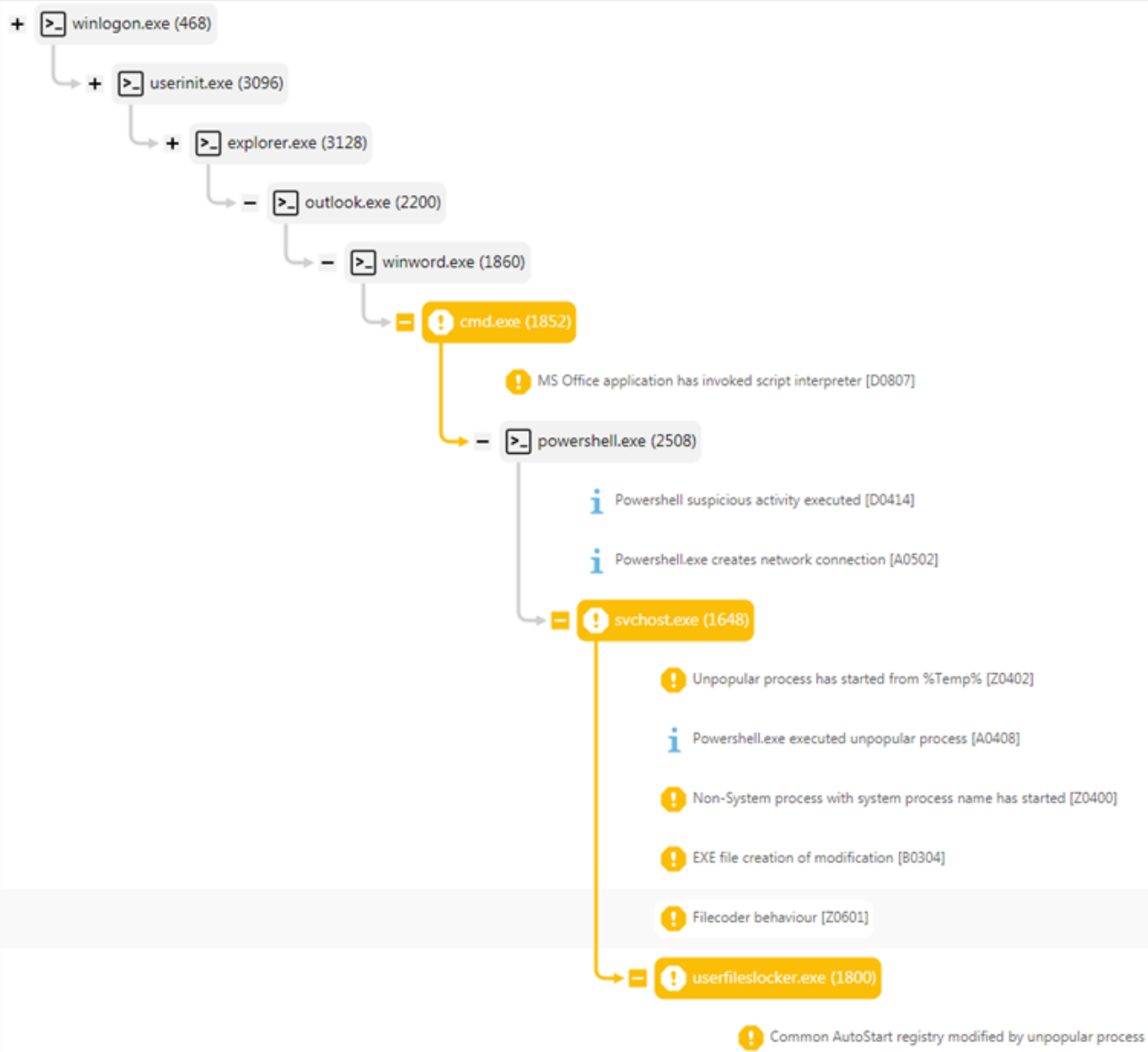
REPUTATION	
POPULARITY	
FIRST SEEN	one year ago

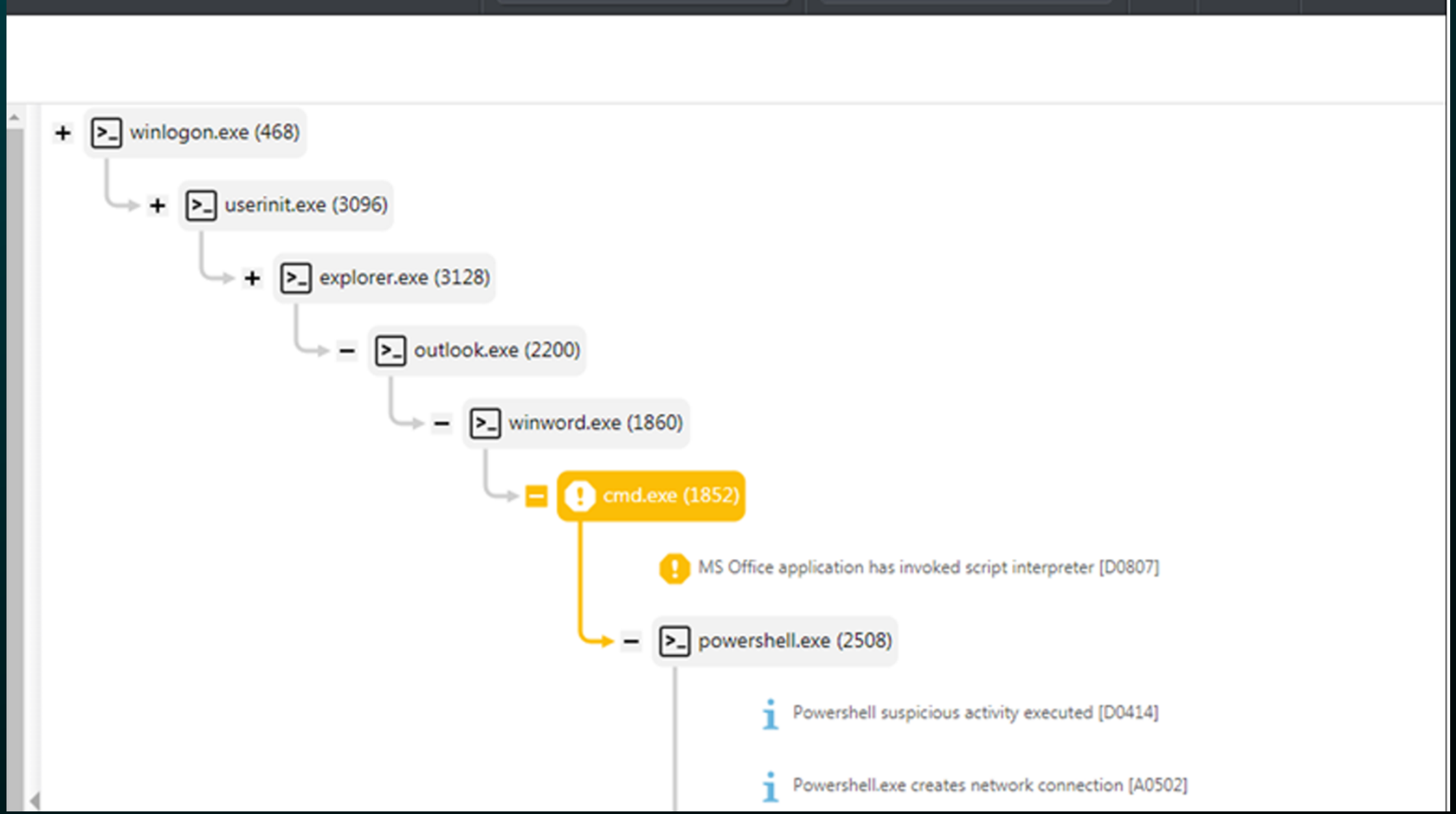
findeppc-128

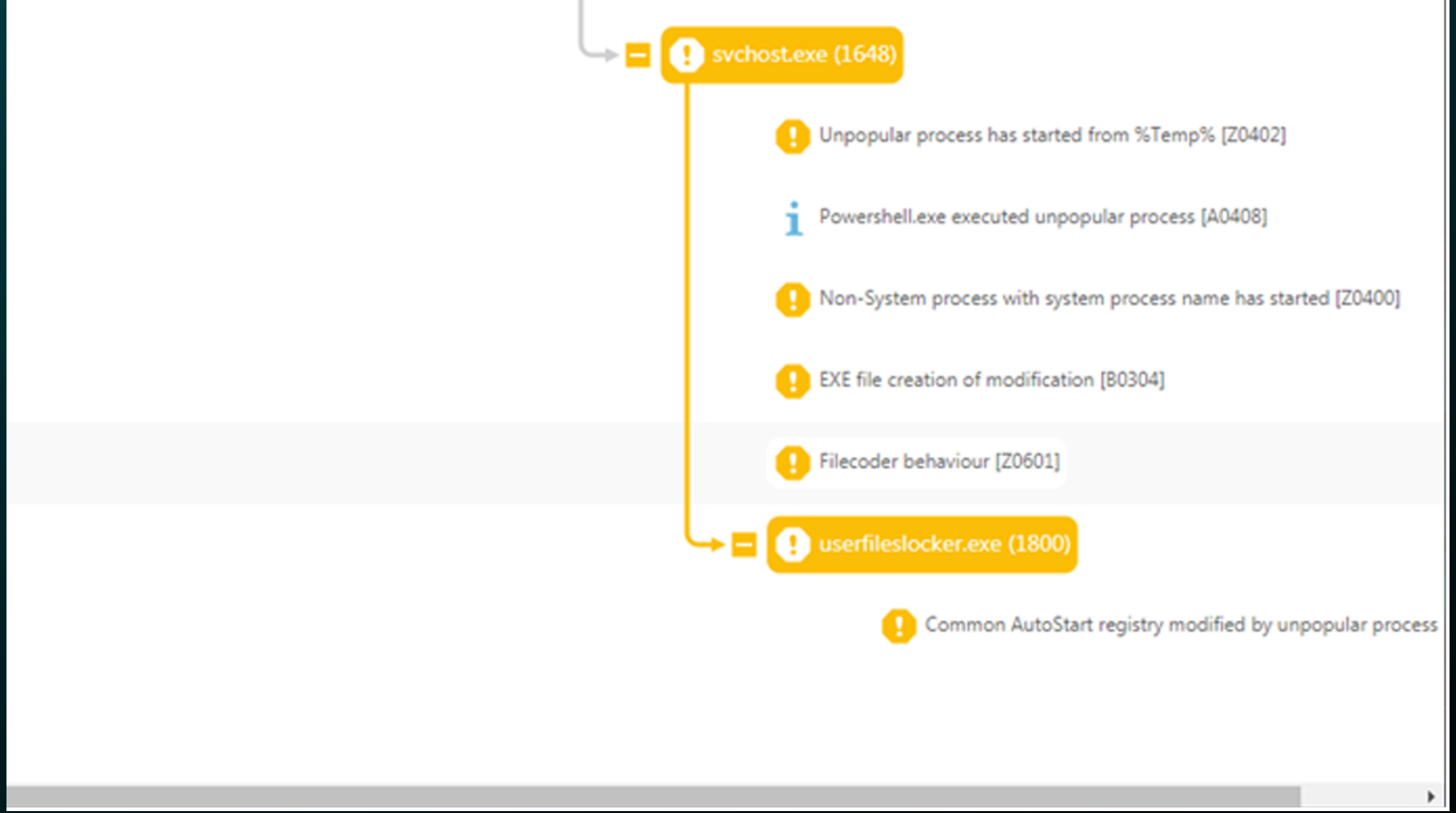
PARENT GROUP	Finance Department
LAST CONNECTED	3 minutes ago - Mar 7, 2018, 5:05:32 PM
LAST EVENT	4 minutes ago - Mar 7, 2018, 5:05:02 PM
AGENT VERSION	1.2.649
OS	Windows 7

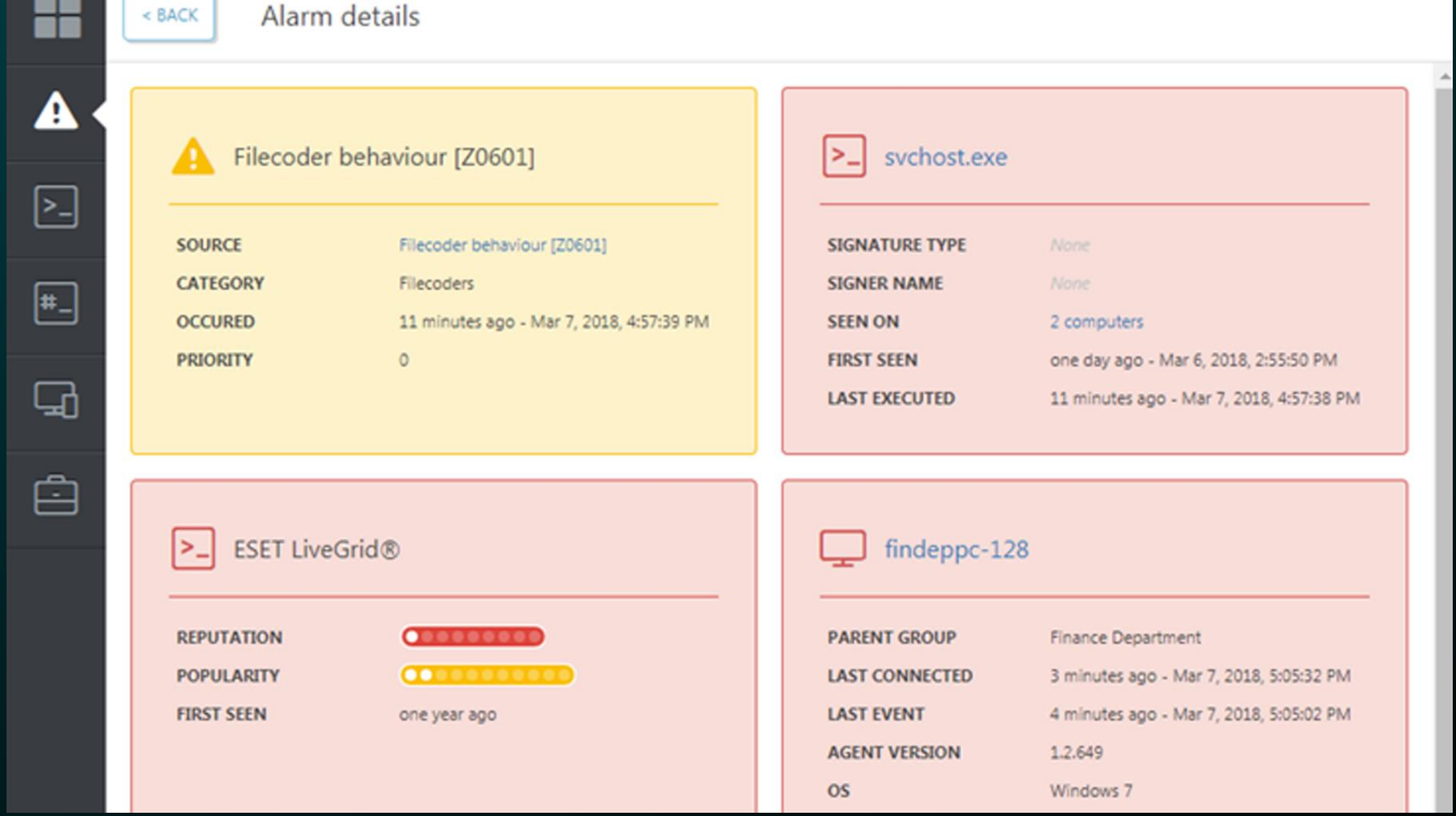
CATEGORY	Filecoders
EXPLANATION	File with a duplicate extension created on top of a popular file extension (such as .jpg.lock) has been created. That may indicate activity of ransomware encrypting files.
MALICIOUS CAUSES	Generated by ransomware when encrypting files.
BENIGN CAUSES	Sometimes used by legitimate program to "lock"/ensure exclusive access to some file. Usually used only on one or few files.
RECOMMENDED ACTIONS	Check the count of files with changed extension and content of such changed files. Are they encrypted? Is there any reason for adding a duplicate extension? Scan the reported program by AV. If not detected then submit the executable for analysis. Locate encrypted files (find out extent of damage). Shares on network may be affected. Investigate how the program reached your company and how was it was executed.
ALARM TYPE	Rule was activated
SOURCE RULE	Filecoder behaviour [Z0601]
OCCURRED	11 minutes ago - Mar 7, 2018, 4:57:39 PM
TRIGGERED	10 minutes ago - Mar 7, 2018, 4:58:31 PM

MARK AS RESOLVED | MARK AS PRIORITY | COMPUTER | KILL PROCESS | EXECUTABLE | CREATE EXCLUSION | EDIT RULE



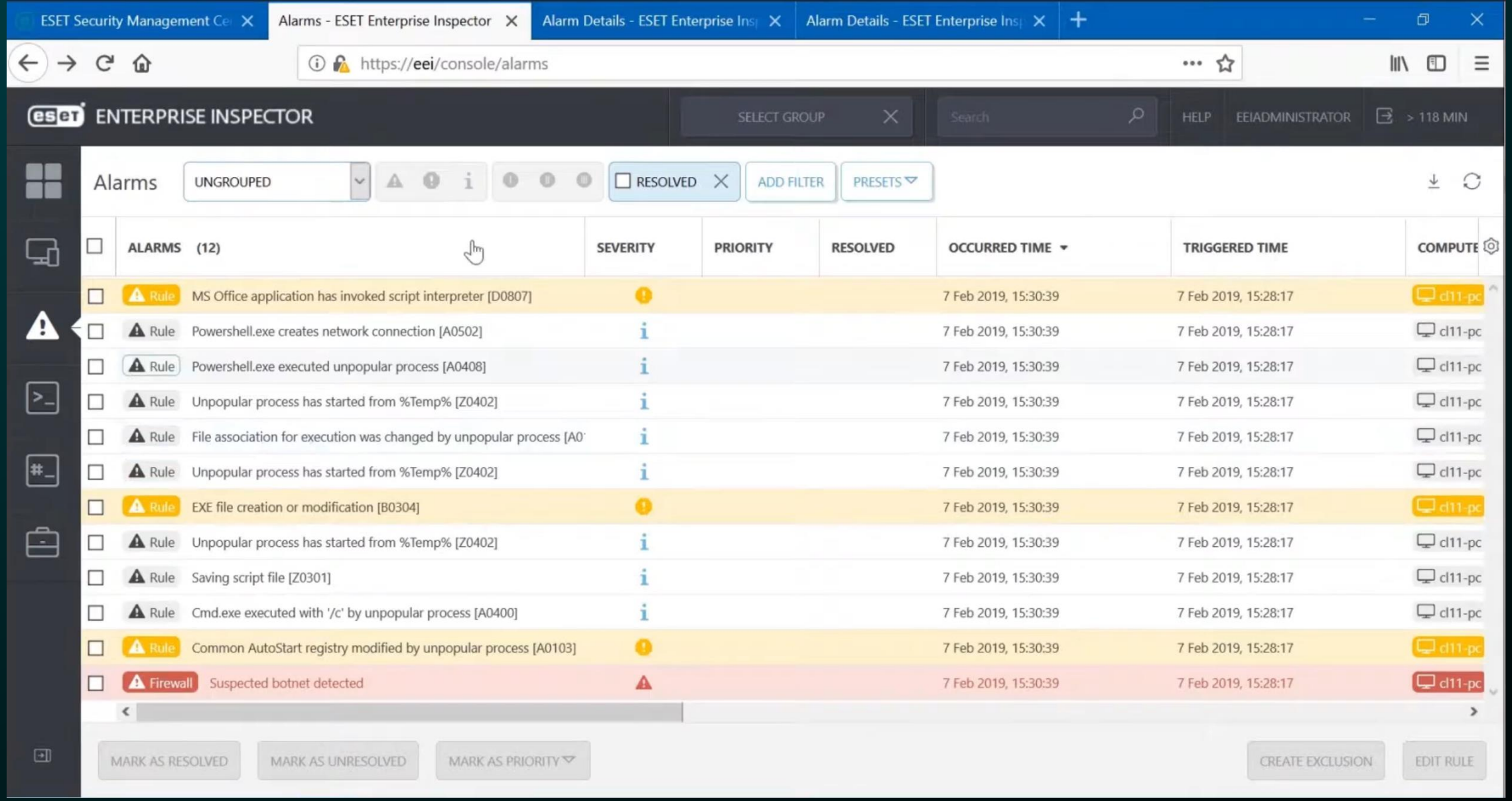

winlogon.exe (468)
userinit.exe (3096)
explorer.exe (3128)
outlook.exe (2200)
winword.exe (1860)
cmd.exe (1852)
MS Office application has invoked script interpreter [D0807]
powershell.exe (2508)
Powershell suspicious activity executed [D0414]
Powershell.exe creates network connection [A0502]

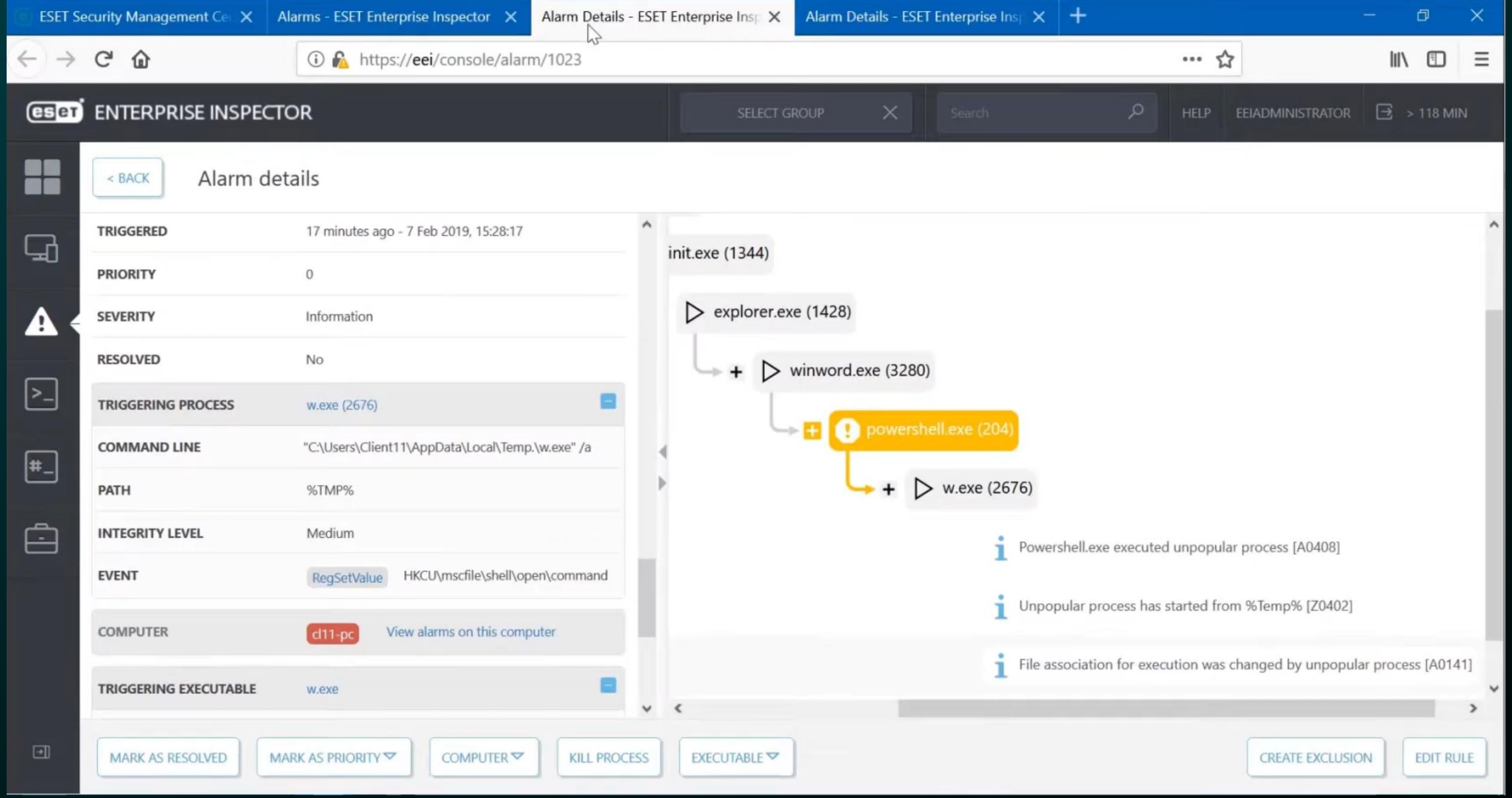

svchost.exe (1648)
Unpopular process has started from %Temp% [Z0402]
Powershell.exe executed unpopular process [A0408]
Non-System process with system process name has started [Z0400]
EXE file creation of modification [B0304]
Filecoder behaviour [Z0601]
userfileslocker.exe (1800)
Common AutoStart registry modified by unpopular process

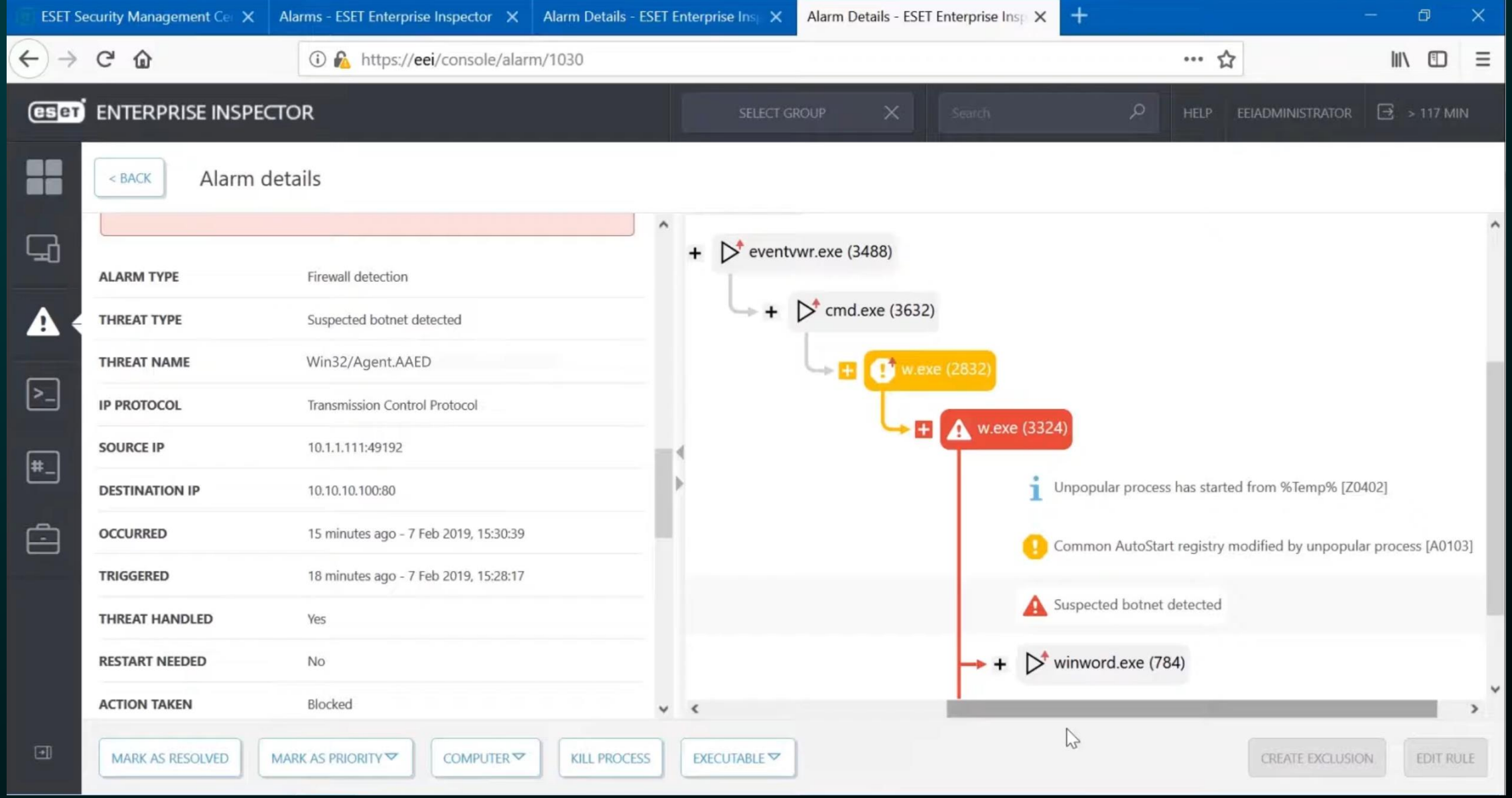

< BACK
Alarm details
Filecoder behaviour [Z0601]
SOURCE
Filecoder behaviour [Z0601]
CATEGORY
Filecoders
OCCURED
11 minutes ago - Mar 7, 2018, 4:57:39 PM
PRIORITY
0
svchost.exe
SIGNATURE TYPE
None
SIGNER NAME
None
SEEN ON
2 computers
FIRST SEEN
one day ago - Mar 6, 2018, 2:55:50 PM
LAST EXECUTED
11 minutes ago - Mar 7, 2018, 4:57:38 PM
ESET LiveGrid®
REPUTATION
POPULARITY
FIRST SEEN
one year ago
findeppc-128
PARENT GROUP
Finance Department
LAST CONNECTED
3 minutes ago - Mar 7, 2018, 5:05:32 PM
LAST EVENT
4 minutes ago - Mar 7, 2018, 5:05:02 PM
AGENT VERSION
1.2.649
OS
Windows 7

CATEGORY	Filecoders
EXPLANATION	File with a duplicate extension created on top of a popular file extension (such as .jpg.lock) has been created. That may indicate activity of ransomware encrypting files.
MALICIOUS CAUSES	Generated by ransomware when encrypting files.
BENIGN CAUSES	Sometimes used by legitimate program to "lock"/ensure exclusive access to some file. Usually used only on one or few files.
RECOMMENDED ACTIONS	Check the count of files with changed extension and content of such changed files. Are they encrypted? Is there any reason for adding a duplicate extension? Scan the reported program by AV. If not detected then submit the executable for analysis. Locate encrypted files (find out extent of damage). Shares on network may be affected. Investigate how the program reached your company and how was it was executed.
ALARM TYPE	Rule was activated
SOURCE RULE	Filecoder behaviour [Z0601]
OCCURRED	11 minutes ago - Mar 7, 2018, 4:57:39 PM
TRIGGERED	10 minutes ago - Mar 7, 2018, 4:58:31 PM

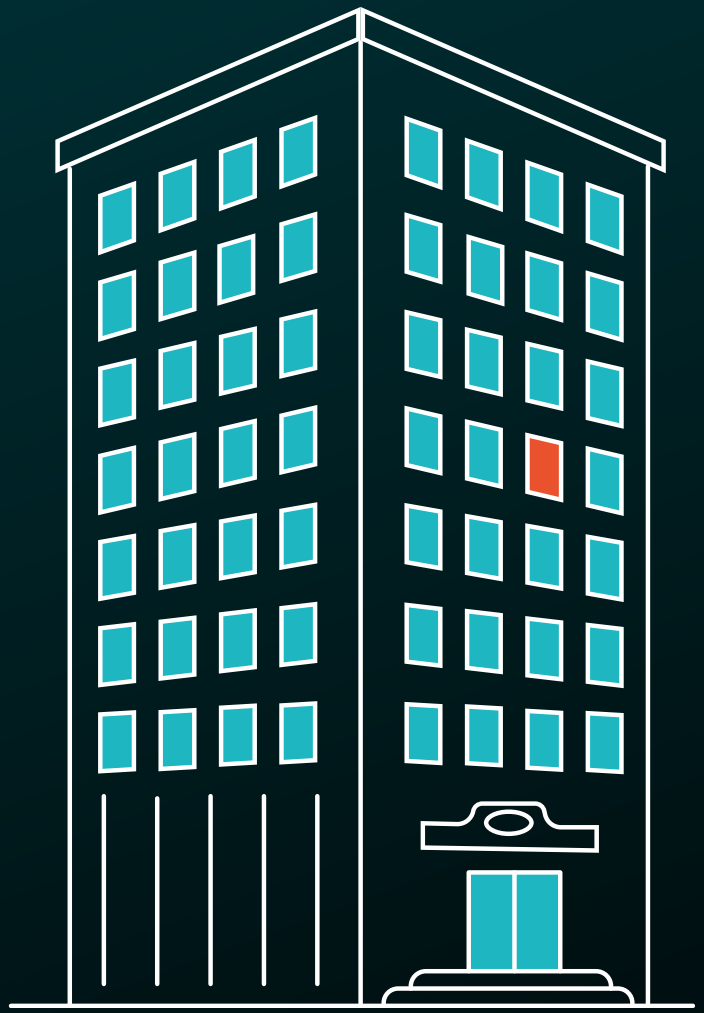
MARK AS RESOLVED | MARK AS PRIORITY | COMPUTER | KILL PROCESS | EXECUTABLE | CREATE EXCLUSION | EDIT RULE


ESET Security Management Ce
Alarms - ESET Enterprise Inspector
Alarm Details - ESET Enterprise Insp
Alarm Details - ESET Enterprise Insp
https://eei/console/alarms
ENTERPRISE INSPECTOR
SELECT GROUP
Search
HELP
EEIADMINISTRATOR
> 118 MIN
Alarms
UNGROUPED
RESOLVED
ADD FILTER
PRESETS
ALARMS (12)
SEVERITY
PRIORITY
RESOLVED
OCCURRED TIME
TRIGGERED TIME
COMPUTE
Rule MS Office application has invoked script interpreter [D0807] 7 Feb 2019, 15:30:39 7 Feb 2019, 15:28:17 cl11-pc
Rule Powershell.exe creates network connection [A0502] 7 Feb 2019, 15:30:39 7 Feb 2019, 15:28:17 cl11-pc
Rule Powershell.exe executed unpopular process [A0408] 7 Feb 2019, 15:30:39 7 Feb 2019, 15:28:17 cl11-pc
Rule Unpopular process has started from %Temp% [Z0402] 7 Feb 2019, 15:30:39 7 Feb 2019, 15:28:17 cl11-pc
Rule File association for execution was changed by unpopular process [A0 7 Feb 2019, 15:30:39 7 Feb 2019, 15:28:17 cl11-pc
Rule Unpopular process has started from %Temp% [Z0402] 7 Feb 2019, 15:30:39 7 Feb 2019, 15:28:17 cl11-pc
Rule EXE file creation or modification [B0304] 7 Feb 2019, 15:30:39 7 Feb 2019, 15:28:17 cl11-pc
Rule Unpopular process has started from %Temp% [Z0402] 7 Feb 2019, 15:30:39 7 Feb 2019, 15:28:17 cl11-pc
Rule Saving script file [Z0301] 7 Feb 2019, 15:30:39 7 Feb 2019, 15:28:17 cl11-pc
Rule Cmd.exe executed with '/c' by unpopular process [A0400] 7 Feb 2019, 15:30:39 7 Feb 2019, 15:28:17 cl11-pc
Rule Common AutoStart registry modified by unpopular process [A0103] 7 Feb 2019, 15:30:39 7 Feb 2019, 15:28:17 cl11-pc
Firewall Suspected botnet detected 7 Feb 2019, 15:30:39 7 Feb 2019, 15:28:17 cl11-pc
MARK AS RESOLVED
MARK AS UNRESOLVED
MARK AS PRIORITY
CREATE EXCLUSION
EDIT RULE


ESET Security Management Ce
Alarms - ESET Enterprise Inspector
Alarm Details - ESET Enterprise Insp
Alarm Details - ESET Enterprise Insp
https://eei/console/alarm/1023
ENTERPRISE INSPECTOR
SELECT GROUP
Search
HELP
EEIADMINISTRATOR
> 118 MIN
< BACK
Alarm details
TRIGGERED
17 minutes ago - 7 Feb 2019, 15:28:17
PRIORITY
0
SEVERITY
Information
RESOLVED
No
TRIGGERING PROCESS
w.exe (2676)
COMMAND LINE
"C:\Users\Client11\AppData\Local\Temp.\w.exe" /a
PATH
%TMP%
INTEGRITY LEVEL
Medium
EVENT
RegSetValue
HKCU\mscfile\shell\open\command
COMPUTER
cl11-pc
View alarms on this computer
TRIGGERING EXECUTABLE
w.exe
init.exe (1344)
explorer.exe (1428)
winword.exe (3280)
powershell.exe (204)
w.exe (2676)
Powershell.exe executed unpopular process [A0408]
Unpopular process has started from %Temp% [Z0402]
File association for execution was changed by unpopular process [A0141]
MARK AS RESOLVED
MARK AS PRIORITY
COMPUTER
KILL PROCESS
EXECUTABLE
CREATE EXCLUSION
EDIT RULE

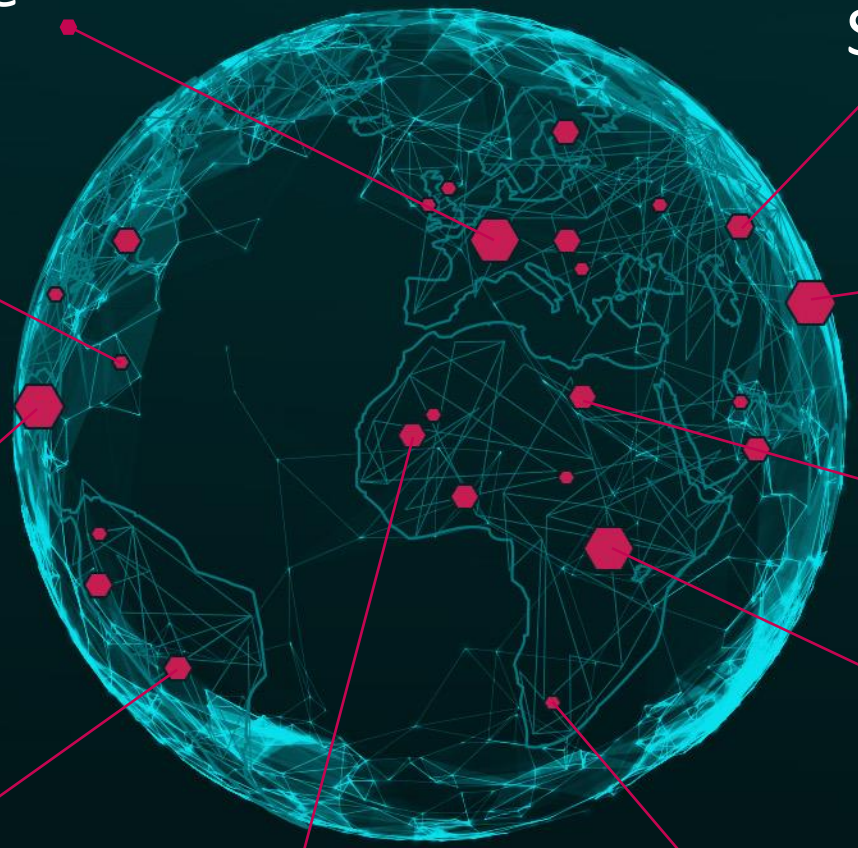

ESET Security Management Ce
Alarms - ESET Enterprise Inspector
Alarm Details - ESET Enterprise Insp
Alarm Details - ESET Enterprise Insp
https://eei/console/alarm/1030
ENTERPRISE INSPECTOR
SELECT GROUP
Search
HELP
EEIADMINISTRATOR
> 117 MIN
< BACK
Alarm details
ALARM TYPE
Firewall detection
THREAT TYPE
Suspected botnet detected
THREAT NAME
Win32/Agent.AAED
IP PROTOCOL
Transmission Control Protocol
SOURCE IP
10.1.1.111:49192
DESTINATION IP
10.10.10.100:80
OCCURRED
15 minutes ago - 7 Feb 2019, 15:30:39
TRIGGERED
18 minutes ago - 7 Feb 2019, 15:28:17
THREAT HANDLED
Yes
RESTART NEEDED
No
ACTION TAKEN
Blocked
eventvwr.exe (3488)
cmd.exe (3632)
w.exe (2832)
w.exe (3324)
Unpopular process has started from %Temp% [Z0402]
Common AutoStart registry modified by unpopular process [A0103]
Suspected botnet detected
winword.exe (784)
MARK AS RESOLVED
MARK AS PRIORITY
COMPUTER
KILL PROCESS
EXECUTABLE
CREATE EXCLUSION
EDIT RULE

Bezpečnostní špecialisti potrebujú chrániť kompletne **celý perimeter**



Útočníkom stačí nájsť **jedno slabé miesto**

Svet sa mení a rovnako aj ESET



Cielené útoky

Súlad

Analýza hrozieb

Detekcia správania

Strojové učenie

Ransomware

Bezsúborové útoky

UEFI

IoT

Kybernetická vojna

BEZPEČNOSTNÍ IT EXPERTI
NA VAŠEJ STRANE

Ďakujem za pozornosť.