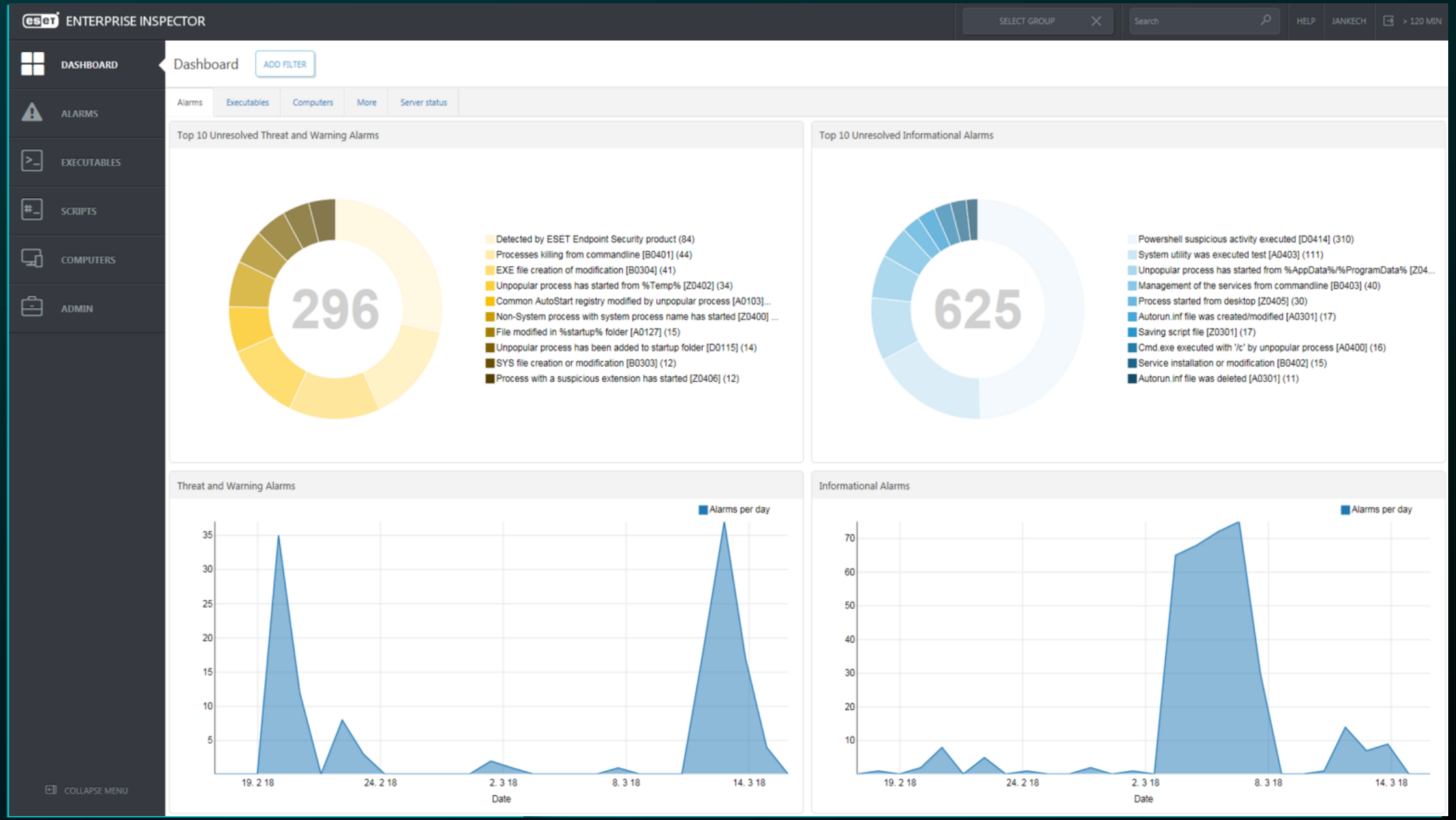
BEZPEČNOSTNÍ IT EXPERTI
NA VAŠEJ STRANE

Nedajte šancu hrozbám vďaka sofistikovaným EDR nástrojom

Július Selecký

Senior Technical Pre-Sales Representative

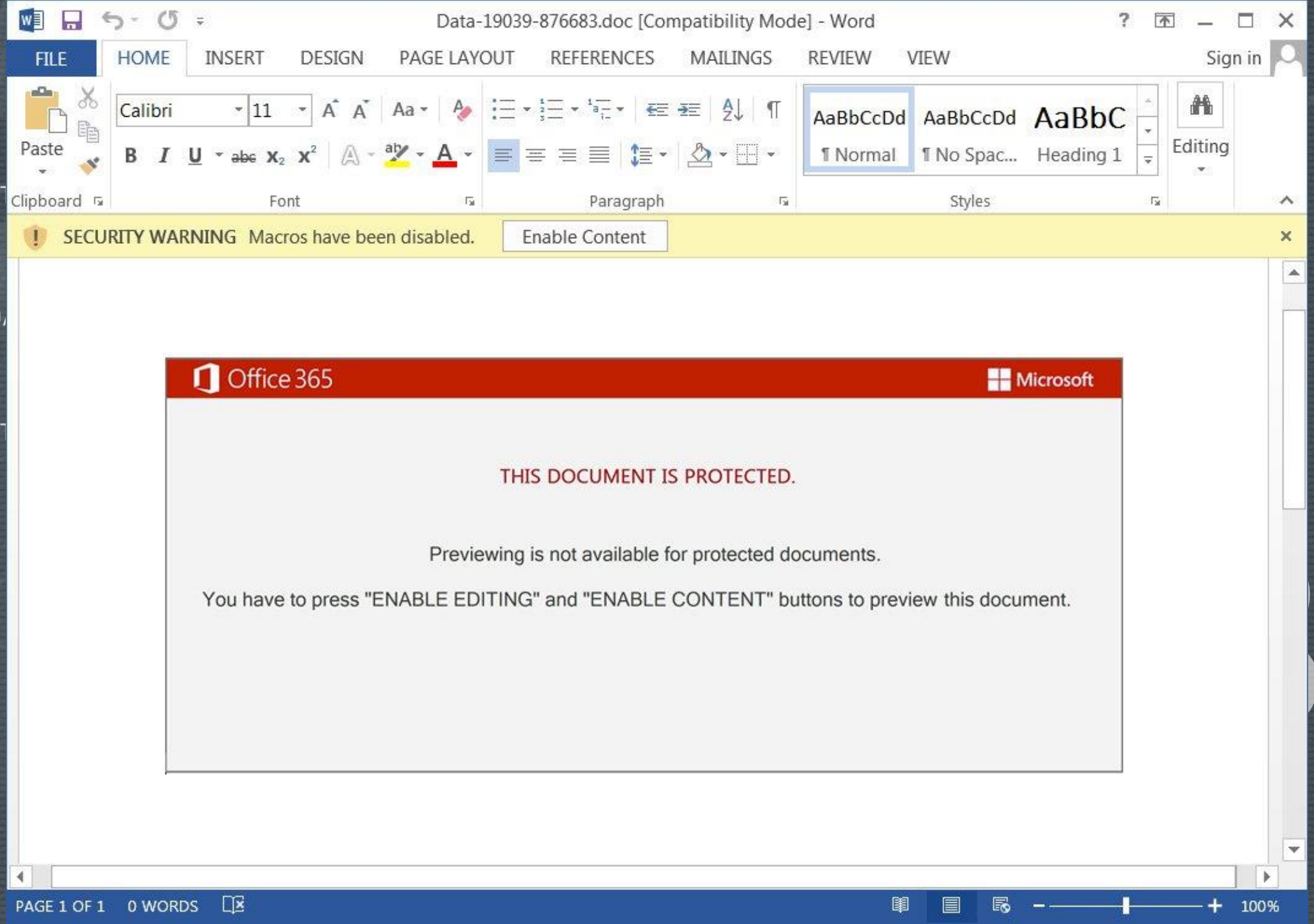
julius.selecky@eset.sk


ENTERPRISE INSPECTOR
SELECT GROUP
Search
HELP
JANKECH
> 120 MIN
DASHBOARD
ALARMS
EXECUTABLES
SCRIPTS
COMPUTERS
ADMIN
COLLAPSE MENU
Dashboard
ADD FILTER
Alarms
Executables
Computers
More
Server status
Top 10 Unresolved Threat and Warning Alarms
296
Detected by ESET Endpoint Security product (84)
Processes killing from commandline [B0401] (44)
EXE file creation of modification [B0304] (41)
Unpopular process has started from %Temp% [Z0402] (34)
Common AutoStart registry modified by unpopular process [A0103]...
Non-System process with system process name has started [Z0400] ...
File modified in %startup% folder [A0127] (15)
Unpopular process has been added to startup folder [D0115] (14)
SYS file creation or modification [B0303] (12)
Process with a suspicious extension has started [Z0406] (12)
Top 10 Unresolved Informational Alarms
625
Powershell suspicious activity executed [D0414] (310)
System utility was executed test [A0403] (111)
Unpopular process has started from %AppData%/%ProgramData% [Z04...
Management of the services from commandline [B0403] (40)
Process started from desktop [Z0405] (30)
Autorun.inf file was created/modified [A0301] (17)
Saving script file [Z0301] (17)
Cmd.exe executed with '/c' by unpopular process [A0400] (16)
Service installation or modification [B0402] (15)
Autorun.inf file was deleted [A0301] (11)
Threat and Warning Alarms
Alarms per day
35
30
25
20
15
10
5
19. 2 18
24. 2 18
2. 3 18
8. 3 18
14. 3 18
Date
Informational Alarms
Alarms per day
70
60
50
40
30
20
10
19. 2 18
24. 2 18
2. 3 18
8. 3 18
14. 3 18
Date

ESET THREAT REPORT

- Published every quarter
- Summaries of latest ESET research
- Exclusive ESET research updates
- Trends in a wide variety of threat categories
- Insight into ESET telemetry
- Commentary by ESET threat analysts

ENJOY SAFER TECHNOLOGY™


Data-19039-876683.doc [Compatibility Mode] - Word
FILE
HOME
INSERT
DESIGN
PAGE LAYOUT
REFERENCES
MAILINGS
REVIEW
VIEW
Sign in
Paste
Calibri
11
Clipboard
Font
Paragraph
AaBbCcDd
¶ Normal
AaBbCcDd
¶ No Spac...
AaBbC
Heading 1
Styles
Editing
SECURITY WARNING Macros have been disabled.
Enable Content
Office 365
Microsoft
THIS DOCUMENT IS PROTECTED.
Previewing is not available for protected documents.
You have to press "ENABLE EDITING" and "ENABLE CONTENT" buttons to preview this document.
PAGE 1 OF 1
0 WORDS
100%

Endpoint Detection & Response (EDR)

- Detekcia pokročilých pretrvávajúcich hrozieb
- Zastavenie bezsúborových útokov
- Blokovanie zero-day hrozieb
- Ochrana pred ransomware
- Zachytenie porušovania bezpečnostných politík
- Detekcia incidentov (analýza príčin vzniku)
- Úplná sieťová izolácia

< 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®

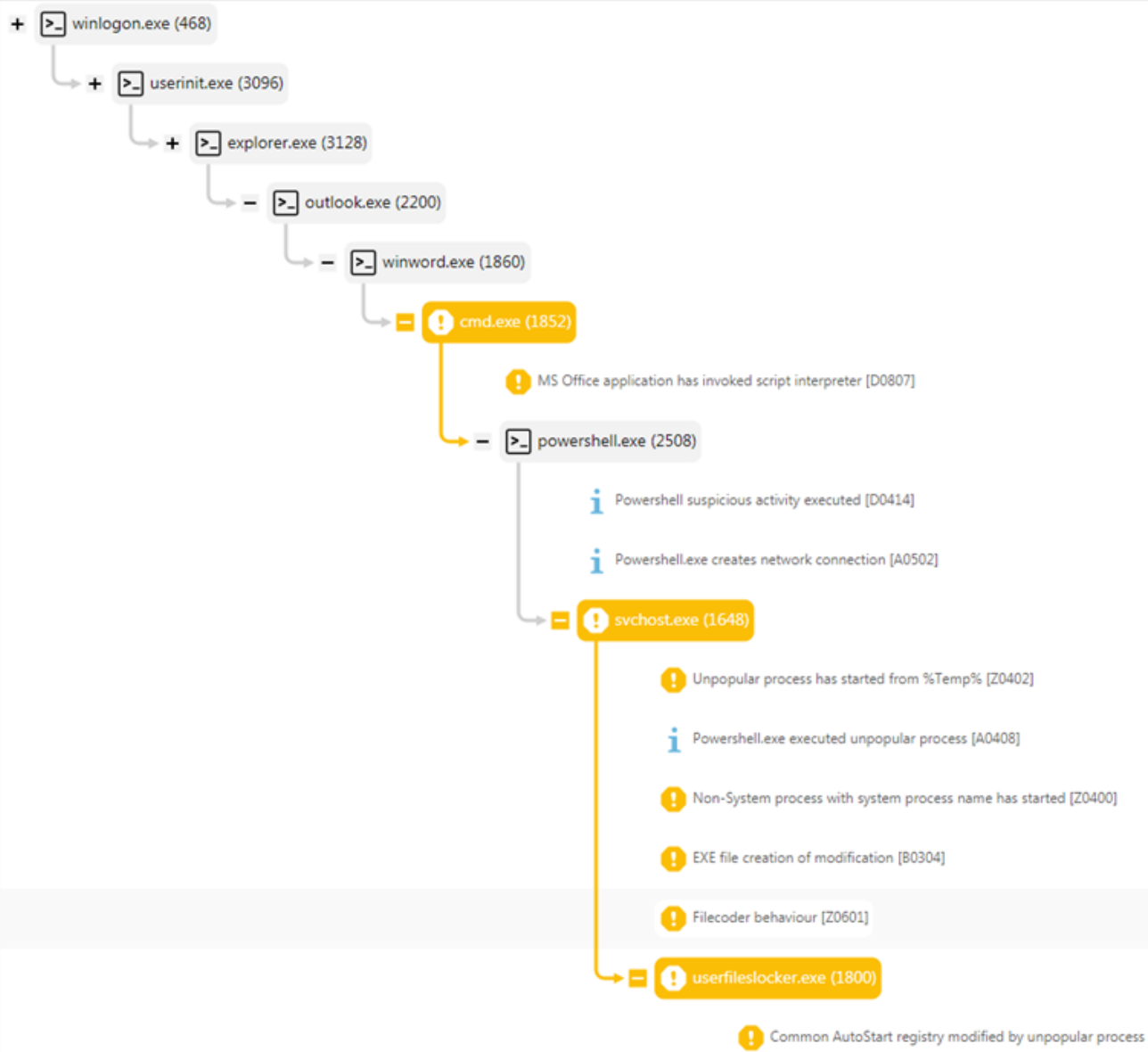
REPUTATION	
POPULARITY	
FIRST SEEN	one year ago

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



69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

§ 24 Hlásenie kybernetických bezpečnostných incidentov

- povinnosť hlásiť každý závažný kybernetický bezpečnostný incident
- kategória závažnosti
- dĺžka trvania kybernetického bezpečnostného incidentu

CSIRT.SK

- typ závažného incidentu (nežiadúci obsah, škodlivý kód, získavanie informácií, pokus o prienik do systému, nedostupnosť, neoprávnený prístup, podvod, zraniteľnosť...)
- časové údaje zistenia a vzniku incidentu
- detailný opis a priebeh incidentu
- rozsah škôd
- prvotné zasiahnuté aktíva
- stav riešenia závažného kybernetického incidentu

BEZPEČNOSTNÍ IT EXPERTI
NA VAŠEJ STRANE

Ďakujem za pozornosť.