



**SECURITY
DAYS**

BEZPEČNOSTNÉ RIEŠENIA PRE OCHRANU KONCOVÝCH STANÍC A FIREMNEJ INFRAŠTRUKTÚRY



ENJOY SAFER TECHNOLOGY™



**SECURITY
DAYS**

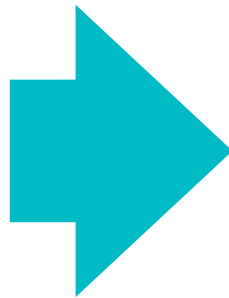
ESET Security Management Center



ENJOY SAFER TECHNOLOGY™



REMOTE
ADMINISTRATOR



SECURITY
MANAGEMENT
CENTER

ESMC?



Enterprise Inspector
a Dynamic Threat
Defense



sieťový
troubleshooting



hardware
inventory

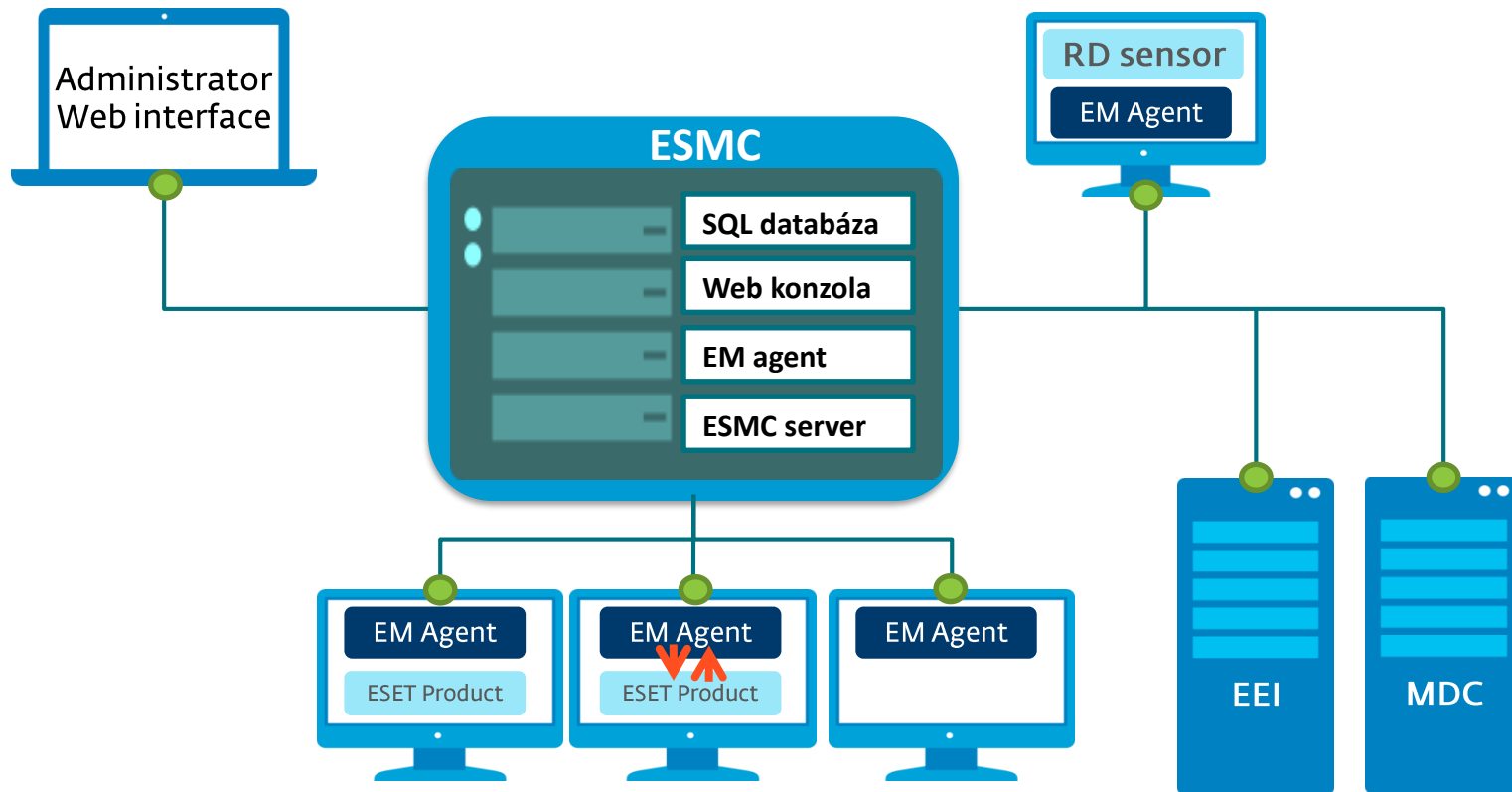


preddefinované
riadenie a scenáre



podrobný
reporting
a notifikácie

Schéma ESMC



Using unencrypted connection! Please configure the webserver to use HTTPS

eset SECURITY MANAGEMENT CENTER

Login

- Log into Domain
- Allow session in multiple tabs

[LOG IN](#) [Change password](#)



[Open Help](#)

© 1992 - 2017 ESET, spol. s r.o. - All rights reserved.

Dashboard

eset SECURITY MANAGEMENT CENTER

Search computer name | QUICK LINKS | HELP | ADMINISTRATOR | >9 MIN

Dashboard

Overview | Incidents Overview | Computers | Security Management Center Server | Antivirus threats | Firewall threats | ESET applications

Total number of devices: 2

Ok: 0

Attention required: 1

Security risks: 1

Device status

Desktops

Ok	0
Attention required	1
Security risk	0
Total	1

Connection Status

One day	1
> 7 days	1

Product version status

Category	Up to date	Outdated
Agent	0%	100%
Endpoint	0%	100%
Server	100%	0%
Mobile	0%	0%

Management status

Managed & Protected	2	0	15
Managed	2	0	15
Unmanaged	0	0	15
Rogue	0	0	15

RSS feed

ESET Support News

ESET Endpoint Antivirus and ESET Endpoint Security hotfix version 6.5.2123.8 has been released

THU AUG 02 2018 15:01:09 GMT+0200 (CENTRAL EUROPE DAYLIGHT TIME)
http://support.eset.com/news6918/?locale=en_US&viewlocale=en_US

ESET Endpoint Antivirus and ESET Endpoint Security hotfix version 6.5.2123.8 has been released and is

Windows Taskbar: 12:33, 16.8.2018

Skupiny

The screenshot displays the ESET Security Management Center web interface. The browser address bar shows the URL `https://localhost/era/webconsole/#id=GROUP_TEMPLATES`. The page title is "ESET SECURITY MANAGEMENT CENTER". The left sidebar contains a navigation menu with categories: Groups, Dynamic Group Templates (selected), Submitted Files, Quarantine, License Management, ACCESS RIGHTS, Users, Permission Sets, CERTIFICATES, Peer Certificates, Certification Authorities, SERVER, Server Tasks, and Server Settings. The main content area is titled "Dynamic Group Templates" and features a table with two columns: "TEMPLATE NAME" and "TEMPLATE DESCRIPTION". The table lists 17 different operating system and device conditions, each with a checkbox in the "TEMPLATE NAME" column. At the bottom of the table, there are buttons for "NEW TEMPLATE...", "EDIT TEMPLATE...", "DELETE", "DUPLICATE...", and "MOVE ACCESS GROUP". The top right of the interface includes a search bar, "QUICK LINKS", "HELP", and user information for "ADMINISTRATOR". The Windows taskbar at the bottom shows the system tray with the date "16.8.2018" and time "12:52".

TEMPLATE NAME	TEMPLATE DESCRIPTION
<input type="checkbox"/> Operating system is MS Windows	Operating system identifies itself as Microsoft Windows family
<input type="checkbox"/> Operating system is MS Windows Client (Agent-less)	Operating system identifies itself as Microsoft Windows for Client / Workstations family (non-Server) & machine is protected by "agent-less protection" (VMware vShield / NSX)
<input type="checkbox"/> Operating system is MS Windows Client (Agent Installed)	Operating system identifies itself as Microsoft Windows for Client / Workstations family (non-Server) & ESET Management Agent is installed on the system
<input type="checkbox"/> Operating system is MS Windows Server (Agent-less)	Operating system identifies itself as Microsoft Windows Servers family & machine is protected by "agent-less protection" (VMware vShield / NSX)
<input type="checkbox"/> Operating system is MS Windows Server (Agent Installed)	Operating system identifies itself as Microsoft Windows Servers family & ESET Management Agent is installed on the system
<input type="checkbox"/> Operating system is MS Windows (Client)	Operating system identifies itself as Microsoft Windows for Client / Workstations family (non-Server)
<input type="checkbox"/> Operating system is MS Windows (Server)	Operating system identifies itself as Microsoft Windows Server
<input type="checkbox"/> Operating system is Linux	Operating system identifies itself as Linux family
<input type="checkbox"/> Operating system is Mac OS	Operating system identifies itself as Mac OS family
<input type="checkbox"/> Operating system is Google Android	Operating system identifies itself as Google Android family
<input type="checkbox"/> Operating system is Apple iOS	Operating system identifies itself as Apple iOS family
<input type="checkbox"/> Operating system is Apple iOS using the Device Enrollment Program	Operating system identifies itself as Apple iOS family
<input type="checkbox"/> Computer type is mobile device	Managed computer identifies itself as a mobile device
<input type="checkbox"/> Operating system is not up to date	Operating system indicates that more recent updates are available and not installed yet
<input type="checkbox"/> Product modules are not up to date	Security product indicates that modules have not been updated recently
<input type="checkbox"/> Computer is idle	Agent indicates that the computer is in idle state
<input type="checkbox"/> Computer has reported a problem	Agent indicates that operating system or managed product is in problematic state
<input type="checkbox"/> Not activated security product	Security product indicates that it is not activated

Hrozby

The screenshot shows the ESET Security Management Center web console. The browser address bar indicates the URL is `https://localhost/era/webconsole/#id=THREATS`. The page title is "ESET SECURITY MANAGEMENT CENTER".

The left sidebar contains the following navigation items: DASHBOARD, COMPUTERS, THREATS (selected), Reports, Client Tasks, Installers, Policies, Computer Users, Notifications, Status Overview, and More.

The main content area is titled "Threats" and features a "Groups" dropdown menu with the following options: All (0 problems), EDTD, Lost & found, New Static Group, Windows computers (expanded), Linux computers, Mac computers, Computers with outdated modules, Computers with outdated operating systems, Problematic computers, Not activated security product, and Mobile devices.

At the top of the main content area, there are several filter buttons: SHOW SUBGROUPS (checked), COMPUTER MUTED (unchecked), THREAT RESOLVED (unchecked), and OCCURRED (Between 7 day(s) ago and Future). There are also buttons for ADD FILTER and PRESETS.

Below the filters is a table with the following columns: THREAT TYPE, RESOLVED, COMI, CAUSE, ACTIC, OBJECT, PROCESS NAME, and USER. The table is currently empty, displaying "NO DATA AVAILABLE".

At the bottom of the main content area, there are buttons for SCAN COMPUTERS, MARK AS RESOLVED, MARK AS NOT RESOLVED, and ACTIONS.

The Windows taskbar at the bottom shows the system tray with the date and time: SLK 12:37 16.8.2018 US.

Reporty

eset SECURITY MANAGEMENT CENTER

Categories & Templates | Scheduled Reports

Templates | ACCESS GROUP | Select | [Search] | [Filter] | [Share]

Antivirus threats

- Active threats**
Active antivirus threats that weren't handled. To resolve an active threat, a scan covering its path must be executed or a full in-depth scan must be initiated from the console. Persisting active threats will change their status to unresolved after 24 hours.
- Active threats by IPv4 subnet**
Counts of unresolved antivirus threats grouped by IPv4 subnet
- Active threats by IPv6 subnet**
Counts of unresolved antivirus threats grouped by IPv6 subnet
- Agentless virtual machine last scan**
Agentless virtual machines counts grouped by time elapsed since scan
- Antivirus threats in last 30 days grouped by scanner**
Antivirus threats in last 30 days detected by ESET detection engine, grouped by scanner that detected them
- Blocked files in last 30 days grouped by reason for blocking**
Chart showing blocked files by ESET security products in last 30 days grouped by reason for blocking
- Daily summary of threat events in last 30 days**
Overview of antivirus threats detected in last 30 days counted per day
- High severity scans in last 30 days**
Scans with unresolved antivirus threats performed in last 30 days
- High severity threat events in last 7 days**
Unresolved antivirus threat detected in last 7 days
- Last scan**
Computer counts grouped by time elapsed since last computer scan
- Mobile device last scan**
Mobile devices counts grouped by time elapsed since last mobile device scan
- Scans in last 30 days**
Scans performed in last 30 days
- Threat events by IPv4 subnet in last 7 days**
Count of all antivirus threats detected in last 7 days grouped by IPv4 subnets
- Threat events by IPv6 subnet in last 7 days**
Count of all antivirus threats detected in last 7 days grouped by IPv6 subnets
- Threat events in last 7 days**
All antivirus threats detected in last 7 days
- Threats in last 30 days grouped by action taken**
Threats and detected security incidents in last 30 days grouped by action that was taken upon detection
- Threats in last 30 days grouped by detection method**
Threats and detected security incidents in last 30 days grouped by detection method
- Top active threats**
Most frequent unresolved antivirus threats
- Top agentless virtual machines with threat events in last 7 days**
Agentless virtual machines with most detected antivirus threats in last 7 days
- Top computers with active threats**
Computers with most detected unresolved antivirus threats
- Top computers with threat events in last 7 days**
Computers with most detected antivirus threats in last 7 days
- Top mobile devices with threat events in last 7 days**
Mobile devices with most detected antivirus threats in last 7 days
- Top threats in last 7 days**
Most frequent antivirus threats detected in last 7 days
- Top users with threat events in last 7 days**
Users with most detected antivirus threats in last 7 days
- Unresolved high severity threat events in last 7 days**
Severe antivirus threats detected in last 7 days, not marked as resolved

NEW REPORT TEMPLATE | NEW CATEGORY | IMPORT REPORT TEMPLATES

COLLAPSE

Search computer name | QUICK LINKS | HELP | ADMINISTRATOR | >9 MIN

Windows Taskbar: 12:38, 16.8.2018

Prehľad HW a SW

The screenshot displays the ESET Security Management Center interface. The top navigation bar includes the ESET logo, 'SECURITY MANAGEMENT CENTER', a search bar, and user information for 'JANKECH'. The left sidebar contains navigation options: DASHBOARD, COMPUTERS, THREATS, Reports, Client Tasks, Installers, Policies, Computer Users, Notifications, Status Overview, and More. The main content area is titled 'nbjankech-sony.hq.eset.com' and shows the following details:

- Overview:** nbjankech-sony.hq.eset.com (Michal Jankech Physical Laptop Replicator). FQDN: NBJANKECH-SONY.hq.eset.com. Parent Group: /All/Lost & found. IP: 10.1.1.20.185. Applied Policies Count: 5.
- Operating System:** Microsoft Windows 7 Enterprise 32-bit. Manufacturer: Sony Corporation, Model: VGN-Z21XN_B, S/N: 28281860-5000392.
- Hardware:** Intel(R) Core(TM)2 Duo CPU P9500 @ 2.53GHz, RAM: 4 GB, Storage: 250 GB.
- Alerts:** Attention required. Alerts: No alerts. Unresolved Threats Count: 0. Last Connected Time: 2017 Aug 23 22:43:50. Detection Engine: 15964 (20170823). Updated: Updated.
- Products & Licenses:**

Product Name	Version
ESET Remote Administrator Agent	7.0.135.0 (Up-to-date version)
ESET Endpoint Antivirus	6.6.2046.1 (Up-to-date version)
338-HJ3-W37 ESET Endpoint Antivirus	2018 Jan 31 13:00:00
- Users:**

Assigned Users	Logged users
n/a (+ Add)	HQjankech

At the bottom, there are buttons for 'CLOSE', 'COMPUTER', and 'SAVE'.

Karanténa

https://localhost/era/webconsole/#id=QUARANTINE

ESET SECURITY MANAGEMENT CENTER

ADMINISTRATOR >9 MIN

ADD FILTER PRESETS

HASH	THREAT TYPE	THREAT NAME	THREAT FLAGS	USER REASON	RESTORABLE	EXCLUDABLE	COMPUTERS	HITS	FIRST OCCURRED	LAST OCCURRED
NO DATA AVAILABLE										

DELETE RESTORE

SLK US 12:57 16.8.2018

Notifikácie

eset SECURITY MANAGEMENT CENTER Search computer na... QUICK LINKS ? HELP JANKECH > 1 H

Edit Notification

Notifications > Edit Notification

- Basic
- Configuration
- Advanced Settings - Throttling
- Distribution

EMAIL ADDRESS **NAME (OPTIONAL)**

jankech@eset.sk @ New email Add user Duplicate

+ ADD EMAIL + ADD USER IMPORT CSV... COPY & PASTE Remove All

Message preview

Subject
Malware Outbreak Alert!

Content
Number of threat detection events in 10 minutes has reached defined threshold (100 events). Please log-in to your ESET Security Management Center and navigate to Threats view for more details.

+ Add variable Or start typing \$ to display list of variables

SAVE CANCEL

General

Language
English

Customized message content will not be translated into selected language.

Timezone
(UTC+00:00) United Kingdom Time (United Kingdom) Adjust for daylight saving time automatically

FINISH SAVE AS... CANCEL

- Add variable
- Computer name
- Time of occurrence
- Threat type
- Threat name
- Scanner
- Detection engine
- Object type
- Object URI
- Action performed
- Action error
- Threat handled
- Restart required
- User
- Process name
- Circumstances
- First seen time
- Hash of detected file
- Notification name

Politiky

The screenshot displays the ESET Security Management Center web console. The browser address bar shows the URL `https://localhost/era/webconsole/#id=POLICIES;pcz=(p=0)`. The console interface includes a top navigation bar with the ESET logo, 'SECURITY MANAGEMENT CENTER', and user information (ADMINISTRATOR, >9 MIN). A left sidebar contains navigation options: DASHBOARD, COMPUTERS, THREATS, Reports, Client Tasks, Installers, Policies (selected), Computer Users, Notifications, Status Overview, and More. The main content area is titled 'Policies' and shows a tree view of policy categories. Under 'Built-in Policies', 'EDTD aktivacia' is selected. The right pane displays 'EDTD aktivacia - Assigned to' with a table of assigned targets.

Assigned to	Applied on	Settings	Summary
<input type="checkbox"/>	TARGET NAME		TARGET DESCRIPTION
<input type="checkbox"/>	WIN7PC1		
<input type="checkbox"/>	EDTD		

At the bottom of the console, there are buttons for 'POLICIES', 'NEW POLICY', 'ASSIGN GROUP(S)', 'ASSIGN CLIENT(S)', and 'UNASSIGN'. The Windows taskbar at the bottom shows the system tray with the date and time: 12:41, 16.8.2018.

Tasky pre koncové stanice

The screenshot displays the ESET Security Management Center web console. The browser address bar shows the URL `https://localhost/era/webconsole/#id=CLIENT_TASKS`. The page title is "ESET SECURITY MANAGEMENT CENTER". The left sidebar contains navigation options: DASHBOARD, COMPUTERS, THREATS, Reports, Client Tasks, Installers, Policies, Computer Users, Notifications, Status Overview, and More. The main content area is titled "Client Tasks" and shows a list of tasks under the "All Tasks" view. The tasks are as follows:

TASK NAME	PROGRESS	TYPE	TASK DESCRIPTION	TARGETS	MODIFICATION T	LAST
Modules Update		Modules Update	Modules of the installed security product wil...		2018 May 31 09:154...	2018 Aug
Install File Server		Software Install			2018 Jun 8 13:04:03	2018 Jun 1
EDTD		Product Activation	aktivacia		2018 Jun 26 16:47:5...	2018 Jun 2
Activation Klient		Product Activation			2018 Jun 22 10:39:5...	2018 Jun 2
File security activation		Product Activation			2018 Jun 12 08:36:3...	2018 Jun 1

At the bottom of the console, there are buttons for "NEW...", "EDIT...", "DUPLICATE...", "DELETE", and "MOVE ACCESS GROUP". The Windows taskbar at the bottom shows the system tray with the date and time: 12:40, 16.8.2018.

EDTD (ESET Dynamic Threat Defense)

The screenshot displays the ESET Security Management Center interface. The top navigation bar includes the ESET logo, "SECURITY MANAGEMENT CENTER", a search field, "QUICK LINKS", "HELP", "ADMINISTRATOR", and a session timer showing ">9 MIN". The left sidebar contains a navigation menu with categories like Groups, Analyzed Files, Quarantine, License Management, ENCRYPTION, ACCESS RIGHTS, CERTIFICATES, and SERVER. The main content area is titled "file.exe - File Details" and has tabs for OVERVIEW and BEHAVIOR. Two summary cards are shown: "Malicious" with status "Finished" and "file.exe" with origin "NBIJANKECH" and user "michal.jankech". Below these is an "ANALYSIS" section with a table of details.

ANALYSIS	
STATUS	Malicious
STATE	Finished
SENT ON	22 Sep 2017 12:00:00
PROCESSED ON	22 Sep 2017 11:58:00
ORIGIN	
ORIGIN	NBIJANKECH
USER	michal.jankech
REASON	Manual submission
SOURCE	Dynamic Threat Defense
FILE	
HASH	1872A482C41DC305DFB0A95CCD9811B4E82AFD2C
FILE	file.exe
SIZE	5 KB
CATEGORY	Executable

Uživatelia a oprávnenia

The screenshot shows the ESET Security Management Center web console. The browser address bar indicates the URL is `https://localhost/era/webconsole/#id=COMPETENCES`. The page title is "ESET SECURITY MANAGEMENT CENTER".

The left sidebar contains a navigation menu with the following items:

- Groups
- Dynamic Group Templates
- Submitted Files
- Quarantine
- License Management
- ACCESS RIGHTS
- Users
- Permission Sets** (selected)
- CERTIFICATES
- Peer Certificates
- Certification Authorities
- SERVER
- Server Tasks
- Server Settings

The main content area is divided into two panels:

- Permission Sets:** A list of permission sets with a search bar and a "Select" button. The list includes:
 - Administrator permission set (selected)
 - Reviewer permission set
 - Server assisted installation permission set
- Permission Set Details:** A detailed view of the "Administrator permission set".

The "Permission Set Details" panel shows the following information:

- Name:** Administrator permission set
- Description:**
- Static Group Access:** All
- Functionality Access:**

Groups & Computers	Read, Use, Write
Permission Sets	Read, Use, Write
Domain Groups	Read, Use, Write
Native Users	Read, Use, Write
Agent Deployment	Use
Certificates	Read, Use, Write
Server Tasks & Triggers	Read, Use, Write
Notifications	Read, Write
Client Tasks	Read, Use, Write
Dynamic Groups Templates	Read, Use, Write
Reports and Dashboard	Read, Use, Write
Policies	Read, Use, Write
Send Email	Use
Send SNMP Trap	Use
Export report to file	Use
Licenses	Read, Use, Write
Server Settings	Read, Write
Stored Installers	Read, Use, Write
Enterprise Inspector User	Read, Write
Enterprise Inspector Administrator	Write
- Client tasks related access:**
- Server tasks related access:**
- User Group Access:** All Groups Read, Use, Write
- Mapped Domain Security Groups:**
- Assigned Native Users:** Administrator

At the bottom of the details panel, there are "NEW..." and "EDIT..." buttons. The bottom of the console shows a "CLOSE" button and a "PERMISSION SETS" dropdown menu.

The Windows taskbar at the bottom shows the system tray with the date and time: 12:59, 16.8.2018.

Správa licencií

The screenshot displays the ESET Security Management Center interface. The browser address bar shows the URL `https://localhost/era/webconsole/#id=LICENSES`. The application title is "ESET SECURITY MANAGEMENT CENTER". The user is logged in as "ADMINISTRATOR".

The main content area is titled "License Management" and shows a list of licenses. The table has the following columns: PUBLIC ID, PRODUCT NAME, STAT, UNITS, SUBUNITS, VALIDITY, OWNER NAME, and CONTACT. Two licenses are listed:

PUBLIC ID	PRODUCT NAME	STAT	UNITS	SUBUNITS	VALIDITY	OWNER NAME	CONTACT
3AD-P7A-2XX	ESET Dynamic Threat Defense	✓	NFR	Business	2018 Sep 26 14:00:00	Ondrej	krajc@eset.sk
33B-V3K-78F	ESET Secure Enterprise	✓	NFR	Business	2020 May 13 14:00:00	Krajc	krajc@eset.sk

The interface includes a left sidebar with navigation options: Groups, Dynamic Group Templates, Submitted Files, Quarantine, License Management (selected), ACCESS RIGHTS, Users, Permission Sets, CERTIFICATES, Peer Certificates, Certification Authorities, SERVER, Server Tasks, and Server Settings. The bottom of the interface has buttons for "ADD LICE...", "REMOVE LICE...", "SYNCHRONIZE LICENSES", and "OPEN". The Windows taskbar at the bottom shows the system tray with the date and time: 12:58, 16.8.2018.

Ucelený přehľad

The screenshot displays the ESET Security Management Center (SMC) Status Overview dashboard. The interface is organized into a grid of status cards, each representing a different system component. A left-hand navigation pane lists various management areas, and a top navigation bar includes search and user information. The status cards use color-coding: yellow for warnings, green for success, and red for errors.

Navigation and Header:

- Browser: https://localhost/era/webconsole/#id=STATUS_OVERVIEW
- Page Title: SECURITY MANAGEMENT CENTER
- User: ADMINISTRATOR
- Session: >7 MIN

Navigation Menu:

- DASHBOARD
- COMPUTERS
- THREATS
- Reports
- Client Tasks
- Installers
- Policies
- Computer Users
- Notifications
- Status Overview (Active)
- More

Status Overview Cards:

- Users:** Create native users and configure their permissions to allow different levels of management in ESET Security Management Center. It's not recommended to use Administrator account created during installation.
 - Warning: Backup user not set up
- Certificates:** Certificates are used to digitally sign encrypted communications between ESET Security Management Center components.
 - Available certification authorities: 1
 - Available agent certificates: 2
 - Server certificate is valid
- Licenses:** Licenses are essential to activate ESET Security Products and to enable updates for ESET Security Management Center. At least one entered license is needed to ensure ESMC Server receives updates.
 - Available licenses: 5
- Computers:** Add devices to groups in ESET Security Management Center to deploy ESET Management Agent or enroll mobile devices.
 - Available computers: 2
 - Warning: Rogue computers found: 15
 - Synchronization task is either scheduled for execution or already finished
- Agents:** ESET Management Agent is required for the management of computers and ESET products using ESET Security Management Center.
 - No unmanaged computer was found.
- Products:** ESET provides a large variety of security applications for all different platforms. You can easily install them using ESET Security Management Center.
 - Warning: No repository available or no software in repository
 - Computers without any product installed: 0
- Invalid Objects:** Tasks & notifications execution is dependent on internal & external parameters (like computers, groups, installers from repository etc.). If objects are no longer accessible tasks & notifications will not work.
 - Warning: Client tasks containing inaccessible objects: 1
 - Server tasks containing inaccessible objects: 0
 - Warning: Notifications containing inaccessible objects: 28
- External Services:** To function properly, ESET Security Management Center regularly connects to the ESET Repository so that ESET Software installation and Update Servers use up-to-date modules. For e-mail notifications, SMTP configuration is essential.
 - Repository is connected
 - Update server is connected
 - Warning: SMTP server is not configured
- Questions:** Some decisions cannot be handled automatically and need the attention of the Administrator. They should be made as soon as possible to avoid incorrect behavior.
 - Computer connection questions: 0

System Information:

- OS: Windows
- Language: SLK
- Time: 12:52
- Date: 16.8.2018

- DASHBOARD
- COMPUTERS
- THREATS
- Reports
- Client Tasks
- Installers
- Policies
- Computer Users
- Notifications
- Status Overview
- More

< BACK Computers > nbjankech-sony.hq.eset.com Last Connected Time: 2017 Aug 23 22:43:50

- i OVERVIEW**
- CONFIGURATION
- LOGS
- TASK EXECUTIONS
- INSTALLED APPLICATIONS
- ALERTS
- THREATS AND QUARANTINE
- DETAILS

nbjankech-sony.hq.eset.com

Michal Jankech Physical Laptom Replicator

FQDN NBJANKECH-SONY.hq.eset.com

Parent Group /All/Lost & found

IP 10.1.120.185

Applied Policies Count 5

Microsoft Windows 7 Enterprise 32-bit

Manufacturer Model S/N Sony Corporation VGN-Z21XN_B 28281860-5000392

Intel(R) Core(TM)2 Duo CPU P9500 @ 2.53GHz

RAM 4 GB

Storage 250 GB

Attention required

Alerts	No alerts
Unresolved Threats Count	0
Last Connected Time	2017 Aug 23 22:43:50
Detection Engine	15964 (20170823)
Updated	Updated

Products & Licenses

ESET Remote Administrator Agent 7.0.135.0	Up-to-date version
ESET Endpoint Antivirus 6.6.2046.1	Up-to-date version
33B-HJ3-W37 ESET Endpoint Antivirus	2018 Jan 31 13:00:00

Users

Assigned Users	Logged users
n/a	HQ\jankech
+ Add	



**SECURITY
DAYS**

ESET Dynamic Threat Defense

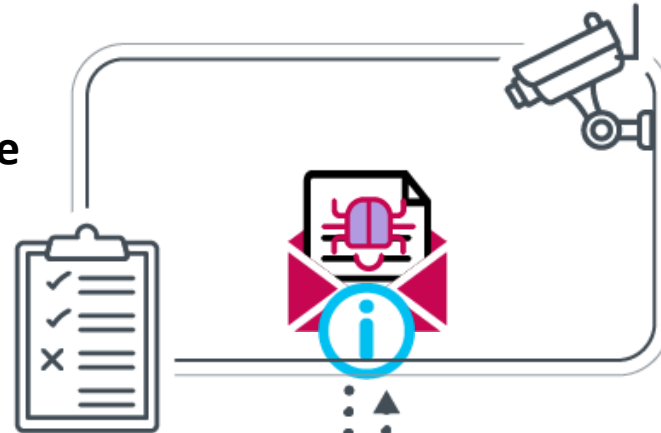
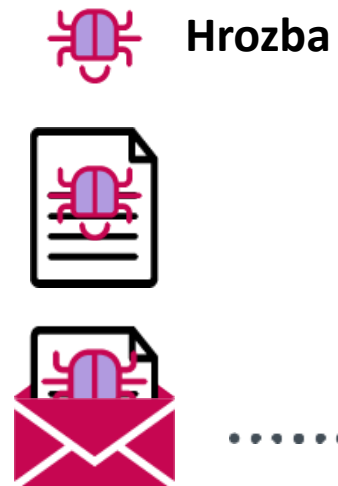


ENJOY SAFER TECHNOLOGY™

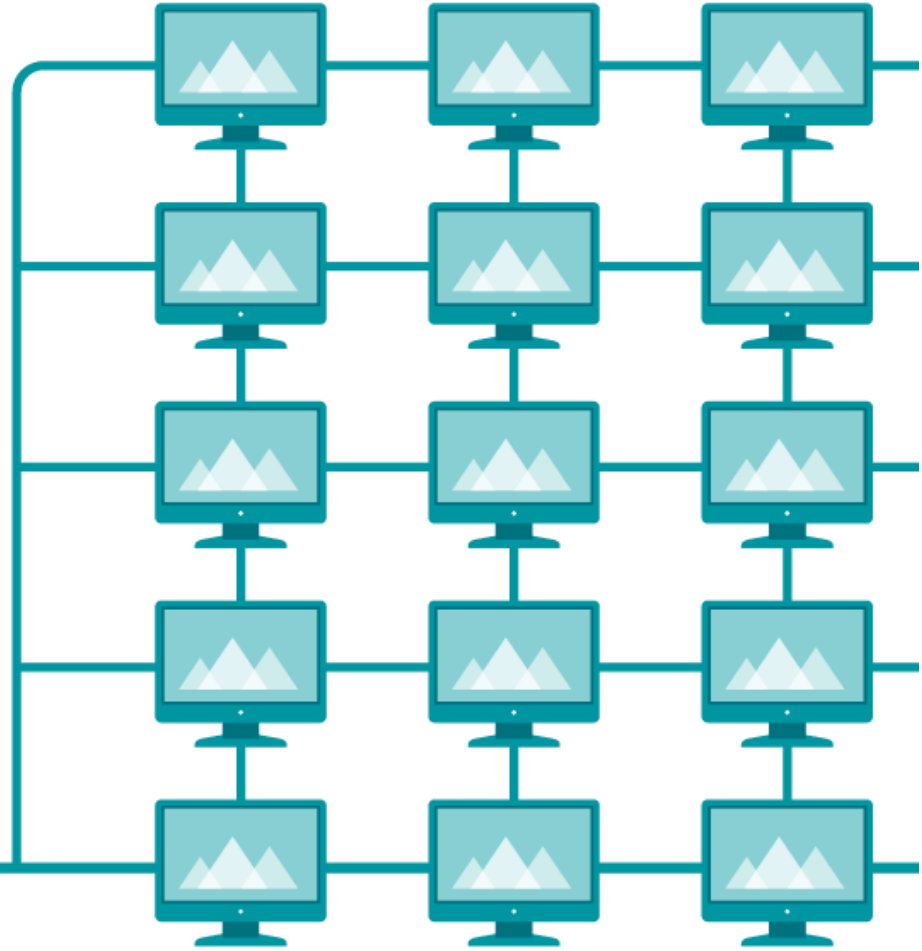
Čo je to ESET Dynamic Threat Defense (EDTD)

- Cloudová technológia sandboxingu
- Využíva pokročilé detekčné techniky
- Platený produkt (služba)
- Od 200 vyššie

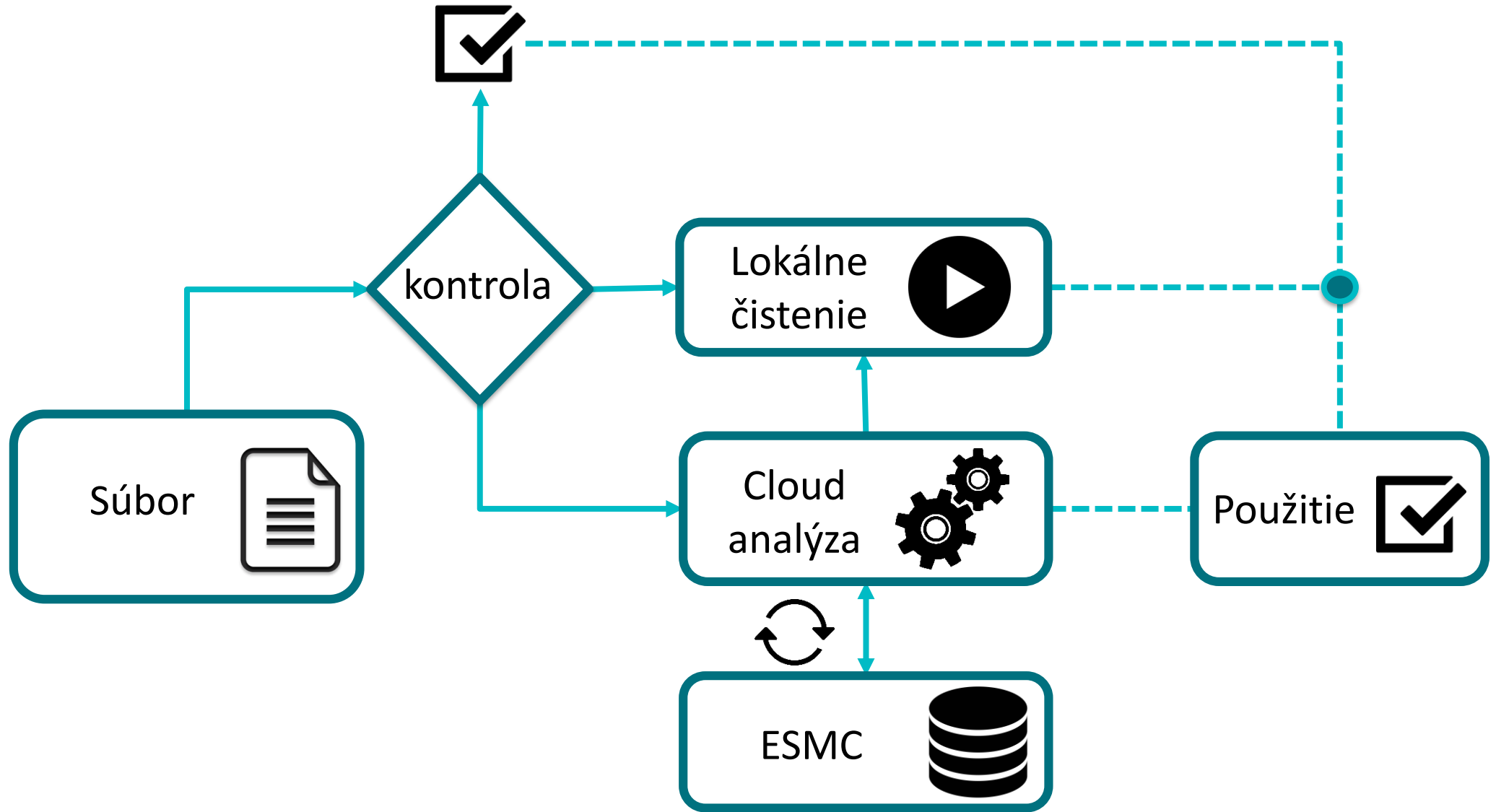
ESET Dynamic Threat Defense



Server
EMS s EDTD



Endpoint



Hlavné výhody

1. Automatická ochrana proti 0-day zraniteľnostiam
2. Viacvrstvová ochrana s metódami strojového učenia
3. Kompletný prehľad o odoslaných súboroch do ESETu
4. Podpora staníc aj mimo vnútornej siete
5. Bez nutností doinštalovať iné SW
6. Jednoduché výstupy v podobe reportov

Podporované verzie OS a ESET produktov

Endpoint:

- ESET Endpoint Antivirus 7 OS Vista a novšie
- ESET Endpoint Security 7 OS Vista a novšie


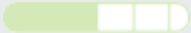
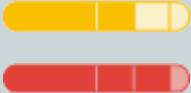

Server:

- ESET Mail Security 7 pre OS Windows server 2008
- ESET File Security pre Windows Server pre OS Windows server 2008

ESMC:

- ESET Security Management Center 7

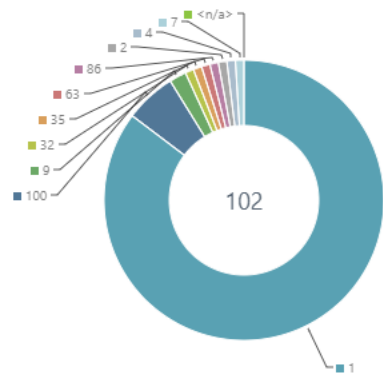
Stav a výsledky

Ikona	Status	Popis
	Neznámy	Súbor zatiaľ nebol analyzovaný
	Neškodný	Detekčné jadro nevyhodnotilo analyzovaný súbor ako škodlivý
	Veľmi podozrivý Podozrivý	Detekčné jadro vyhodnotilo zachytenú aktivitu súboru ako podozrivú, avšak nie ako jednoznačne škodlivú
	Škodlivý	Súbor je na základe zachytenej aktivity vyhodnotený ako škodlivý

Dashboard

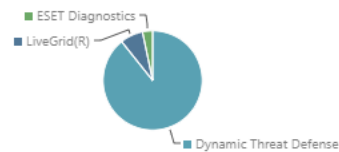
- Overview
- Incidents Overview**
- Computers
- Security Management Center Server
- Antivirus threats
- Firewall threats
- ESET applications
- EDTD ⚙️ +

Files analyzed by ESET Dynamic Threat Defense in last 30 days grouped by the resul...



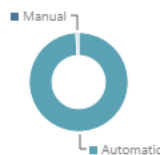
Generated 1 minute ago

Files submitted to ESET Dynamic Threat Defense and ESET LiveGrid in last 30 days g...



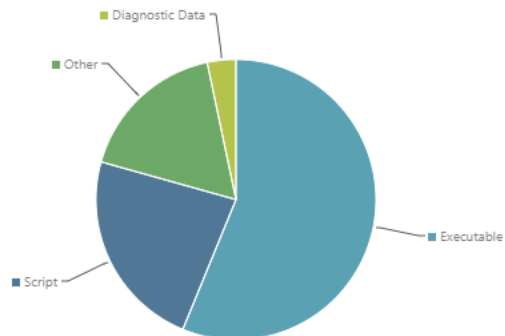
Generated 1 minute ago

Files submitted to ESET Dynamic Threat Defense and ESET LiveGrid in last 30 days g...



Generated 1 minute ago

Files submitted to ESET Dynamic Threat Defense and ESET LiveGrid in last 30 days g...



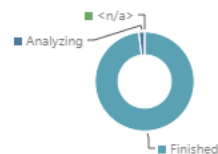
Generated 1 minute ago

Manually submitted samples to ESET Dynamic Threat Defense in last 30 days

Computer name	User name	Object URI	Time of occurrence
ESET Endpoint	EDTDPM\Administrator	file:///C:/Program Files/F...	2018 Mar 14 10:43:07

Generated 1 minute ago

Files submitted to ESET Dynamic Threat Defense and ESET LiveGrid in last 30 days g...



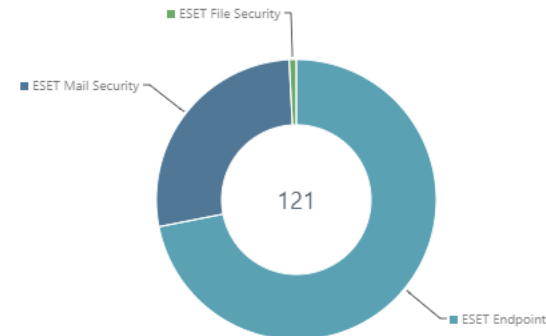
Generated 1 minute ago

Files submitted to ESET Dynamic Threat Defense and ESET Live Grid in last 30 days

Group by (Hash)	Group by (File category)	Group by (Reason of submission)	Group by (State of analysis)	Group by (Score)	Maximum (Timestamp of analysis)
1E4A4BBEC5E4...	Script	Automatic	Finished	1	2018 Mar 15 1...
0DA7BD177B9...	Script	Automatic	Finished	1	2018 Mar 15 1...
3F37A0BC29E6...	Other	Automatic	Finished	100	2018 Mar 14 1...
F5C4208E1A5...	Executable	Automatic	Finished	1	2018 Mar 14 1...
1E135AF20993...	Executable	Automatic	Finished	100	2018 Mar 14 1...
C21680CADA1...	Executable	Automatic	Finished	1	2018 Mar 14 1...
C21680CADA1...	Executable	Manual	Finished	1	2018 Mar 14 1...
83E5CF148819...	Executable	Automatic	Finished	1	2018 Mar 14 1...
F541CDDDA17...	Other	Automatic	Finished	1	2018 Mar 14 0...
2E534EAD8CF...	Executable	Automatic	Finished	1	2018 Mar 13 1...
2420FCADF9C...	Script	Automatic	Finished	86	2018 Mar 13 1...
88F65621A6E9...	Executable	Automatic	Finished	1	2018 Mar 13 0...
262CA94379F6...	Executable	Automatic	Finished	1	2018 Mar 13 0...
64CF454F2481...	Executable	Automatic	Finished	1	2018 Mar 13 0...
070EAA0C0AE3...	Script	Automatic	Finished	1	2018 Mar 13 0...

Generated 1 minute ago

Top 10 computers with file submissions to ESET Dynamic Threat Defense and ESET L...



Generated 1 minute ago

Submitted Files



ADD FILTER

PRESETS



<input type="checkbox"/>	FILE	STATUS	STATE	FIRST SENT ON	LAST PROCESSED ON	COMPUTER	CATEGORY	REASON	SENT TO	HASH	SIZE	
<input type="checkbox"/>	file:///	<div style="width: 100%; height: 10px; background-color: #28a745;"></div>	Finished	2018 Mar 14 08:48:52	2018 Mar 14 08:56:19	ESET Mail Security	Other	Automatic	Dynamic Threat Defense	F541CDDDA17CBE59D487CAE434...	2 KB	
<input type="checkbox"/>	mailto:?to=<edt..._suspicious.bat	<div style="width: 100%; height: 10px; background-color: #ffc107;"></div>	Finished	2018 Mar 13 12:32:20	2018 Mar 13 15:50:01	ESET Mail Security	Script	Automatic	Dynamic Threat Defense	2420FCADF9C358872212DD92232...	147 B	
<input type="checkbox"/>	file:///ø	<div style="width: 100%; height: 10px; background-color: #28a745;"></div>	Finished	2018 Mar 13 12:15:16	2018 Mar 13 17:39:59	ESET Mail Security	Executable	Automatic	Dynamic Threat Defense	2E534EAD8CFB3FAA593E1006E02...	5 MB	
<input type="checkbox"/>	file:///ekrn_1478f780_1d04.mdmp	<div style="width: 100%; height: 10px; background-color: #6c757d;"></div>		2018 Mar 13 10:42:34		ESET Mail Security	Diagnostic Data	Automatic	ESET Diagnostics	30968D266C5A2148041F4410EE3...	297 KB	
<input type="checkbox"/>	file:///C:/Prog...e/Builder3D.exe	<div style="width: 100%; height: 10px; background-color: #28a745;"></div>	Finished	2018 Mar 13 03:07:14	2018 Mar 13 09:06:21	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	64CF454F2481C1616FEC226FED5A...	17 MB	
<input type="checkbox"/>	file:///C:/Prog...rceResolver.exe	<div style="width: 100%; height: 10px; background-color: #28a745;"></div>	Finished	2018 Mar 13 03:07:12	2018 Mar 13 09:08:24	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	88F65621A6E946D927C7BF7244C...	10 KB	
<input type="checkbox"/>	file:///C:/Prog...e/Lib3mfUAP.dll	<div style="width: 100%; height: 10px; background-color: #28a745;"></div>	Finished	2018 Mar 13 03:07:09	2018 Mar 13 09:06:52	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	262CA94379F60D9F08B344B7F1C...	198 KB	
<input type="checkbox"/>	file:///C:/Prog...e_installer.exe	<div style="width: 100%; height: 10px; background-color: #6c757d;"></div>	Sent to LiveGrid®	2018 Mar 12 16:16:22		ESET Mail Security	Executable	Automatic	LiveGrid(R)	04FD23DAAC8872CF59E53A93E4F...	161 KB	
<input type="checkbox"/>	file:///C:/Prog...ng/bootstrap.js	<div style="width: 100%; height: 10px; background-color: #28a745;"></div>	Finished	2018 Mar 12 02:03:27	2018 Mar 12 02:06:10	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	878E449C94F31D4B6FDCAE304A...	20 KB	
<input type="checkbox"/>	file:///C:/Prog...tising/vpaid.js	<div style="width: 100%; height: 10px; background-color: #28a745;"></div>	Finished	2018 Mar 12 02:03:26	2018 Mar 12 02:06:06	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	23A3A4A2DF71835917392AAB131...	24 KB	
<input type="checkbox"/>	file:///C:/Prog...tising/ormma.js	<div style="width: 100%; height: 10px; background-color: #28a745;"></div>	Finished	2018 Mar 12 02:03:26	2018 Mar 12 02:06:07	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	A1DCB407F777AB105E0985104A8...	31 KB	
<input type="checkbox"/>	file:///C:/work...120552974d78f9f	<div style="width: 100%; height: 10px; background-color: #dc3545;"></div>	Finished	2018 Mar 9 13:36:52	2018 Mar 9 13:43:41	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	CA1C8C8A6BB11365A0FE32E6D12...	1 MB	
<input type="checkbox"/>	file:///C:/work...ff173d8f5621bc3	<div style="width: 100%; height: 10px; background-color: #6c757d;"></div>	Sent to LiveGrid®	2018 Mar 9 13:33:40		ESET Endpoint	Executable	Automatic	LiveGrid(R)	EF6990FAE665C4B2E1A0C8D36FF1...	508 KB	
<input type="checkbox"/>	file:///C:/work...oder_crysis.exe	<div style="width: 100%; height: 10px; background-color: #dc3545;"></div>	Finished	2018 Mar 9 13:06:24	2018 Mar 9 13:11:26	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	FED6A67C97B461A0DF1332AF61A...	426 KB	
<input type="checkbox"/>	file:///C:/work...ng Invoices.doc	<div style="width: 100%; height: 10px; background-color: #dc3545;"></div>	Finished	2018 Mar 9 12:58:08	2018 Mar 9 13:01:49	ESET Endpoint	Other	Automatic	Dynamic Threat Defense	062A180A5A7C9854E605BA87E6C...	246 KB	
<input type="checkbox"/>	file:///C:/work...d Installer.exe	<div style="width: 100%; height: 10px; background-color: #28a745;"></div>	Finished	2018 Mar 9 12:39:42	2018 Mar 9 12:44:46	ESET Endpoint	Executable	Automatic	Dynamic Threat Defense	DA61EA7363F23626C044023E2A3...	1 MB	
<input type="checkbox"/>	file:///C:/User.../8df804ba[1].js	<div style="width: 100%; height: 10px; background-color: #28a745;"></div>	Finished	2018 Mar 9 12:28:10	2018 Mar 9 12:32:33	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	0BE08A96802453391E381FDC58C...	18 KB	
<input type="checkbox"/>	file:///C:/User.../7c687813[1].js	<div style="width: 100%; height: 10px; background-color: #28a745;"></div>	Finished	2018 Mar 9 12:28:07	2018 Mar 9 12:31:55	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	0EC53AB1670DF0A004CD57ACB2...	162 KB	
<input type="checkbox"/>	file:///C:/User.../2fd3c36c[1].js	<div style="width: 100%; height: 10px; background-color: #28a745;"></div>	Finished	2018 Mar 9 12:28:06	2018 Mar 9 12:31:55	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	2E08190DEEF03F33718043589486...	506 B	
<input type="checkbox"/>	file:///C:/User.../7ca2a944[1].js	<div style="width: 100%; height: 10px; background-color: #28a745;"></div>	Finished	2018 Mar 9 12:28:05	2018 Mar 9 12:32:02	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	04CDB462F4D38AA65AA471DD6D...	42 KB	
<input type="checkbox"/>	file:///C:/User.../437e8126[1].js	<div style="width: 100%; height: 10px; background-color: #28a745;"></div>	Finished	2018 Mar 9 12:28:04	2018 Mar 9 12:31:55	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	EF6CC5F5AD4F46D1D026CCCB299...	12 KB	
<input type="checkbox"/>	file:///C:/User.../6f2db999[1].js	<div style="width: 100%; height: 10px; background-color: #28a745;"></div>	Finished	2018 Mar 9 12:28:03	2018 Mar 9 12:31:24	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	D276BEF785A933621F3A8B6D3EA...	44 KB	
<input type="checkbox"/>	file:///C:/User.../8636b4dd[1].js	<div style="width: 100%; height: 10px; background-color: #28a745;"></div>	Finished	2018 Mar 9 12:28:02	2018 Mar 15 15:08:16	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	1E4A48BEC5E408C9258B30FEFA2F...	92 KB	
<input type="checkbox"/>	file:///C:/User.../916eb510[1].js	<div style="width: 100%; height: 10px; background-color: #28a745;"></div>	Finished	2018 Mar 9 12:28:02	2018 Mar 9 12:31:55	ESET Endpoint	Script	Automatic	Dynamic Threat Defense	EB32997E4D108F578820D57903E...	15 KB	

ADD EXCLUSION TO POLICY



[< BACK](#)[Submitted Files](#) > [mailto:?to=<e...uspicious.bat - File Details](#)

Suspicious

Status	Suspicious
State	Finished
Last processed on	2018 Mar 13 15:50:01
Sent on	2018 Mar 13 12:32:20
Behaviors	View behavior



mailto:?to=&from=edtdp... suspicious.bat_

Computer	ESET Mail Security
User	NT AUTHORITY\NETWORK SERVICE
Reason	Automatic
Sent to	Dynamic Threat Defense
Hash	2420FCADF9C358B72212DD922321E53CC4C39D5F

Analysis

Status



Suspicious

State

Finished

Sent on

2018 Mar 13 12:32:20

Last processed on

2018 Mar 13 15:50:01

Origin

Computer

ESET Mail Security

User

NT AUTHORITY\NETWORK SERVICE

Reason

Automatic

Sent to

Dynamic Threat Defense

File

File

[CLOSE](#)[VIEW BEHAVIOR](#)[ADD EXCLUSION TO POLICY](#)

✓ STATUS	Clean
SHA-1	A1DCB407F777AB105E0985104A8AA4BB192B4A6D
SIZE	32361B
CATEGORY	Script

Detected Behaviors

BEHAVIOR	Network communication
EXPLANATION	Sample has tried to contact another computer over a network or listen for connections from other computers
BENIGN CAUSES	Clean samples are using network communication to download content
MALICIOUS CAUSES	Sample tried to download additional parts or communicate with malicious servers
BEHAVIOR	Hidden code detection
EXPLANATION	Sample contains hidden code to hide its functionality
BENIGN CAUSES	This is standard behavior when author does not want others to reverse-engineer the file
MALICIOUS CAUSES	Malware tried to hide its presence
BEHAVIOR	Script execution
EXPLANATION	Sample has executed a script (BAT, VBS, JS)
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware may have attempted to run other parts of the sample

! STATUS	Suspicious
SHA-1	2420FCADF9C358B72212DD922321E53CC4C39D5F
SIZE	147B
CATEGORY	Script

Detected Behaviors

BEHAVIOR	Suspicious DLL load
EXPLANATION	Sample has loaded a DLL library in an uncommon way
BENIGN CAUSES	Usually triggered by printer installation or print-to-pdf tools
MALICIOUS CAUSES	Malware tried to hide its presence
BEHAVIOR	Network communication
EXPLANATION	Sample has tried to contact another computer over a network or listen for connections from other computers
BENIGN CAUSES	Clean samples are using network communication to download content
MALICIOUS CAUSES	Sample tried to download additional parts or communicate with malicious servers
BEHAVIOR	Executed file moved by sample
EXPLANATION	Sample has executed another file and then moved it
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware tried to hide its presence
BEHAVIOR	Script execution
EXPLANATION	Sample has executed a script (BAT, VBS, JS)
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware may have attempted to run other parts of the sample
BEHAVIOR	Executed file deleted by sample
EXPLANATION	Sample has executed a file and deleted it afterward
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	This behavior could be caused by malware trying to hide its presence
BEHAVIOR	Analyzed sample moved
EXPLANATION	Sample has been moved to a different location
BENIGN CAUSES	This is standard behavior for some uninstalls
MALICIOUS CAUSES	Malware tried to hide its presence

! STATUS	Malicious
SHA-1	FED6A67C97B461A0DF1332AF61A89EA9FB5A540F
SIZE	436736B
CATEGORY	Executable

Detected Behaviors

BEHAVIOR	Malware detected after execution
EXPLANATION	Sample has been detected as malicious after execution
BENIGN CAUSES	Clean applications should not do this
MALICIOUS CAUSES	Malware detected with ESET scanning engine after execution
BEHAVIOR	New files created in the Windows folder
EXPLANATION	Sample has created new files in the Windows folder
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware tried to hide its presence
BEHAVIOR	Analyzed sample copied
EXPLANATION	Sample has been copied to a different location
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware tried to hide its presence
BEHAVIOR	Startup list modified
EXPLANATION	Sample has added a new entry to the Windows Startup application list
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware wants to run after a system reboot
BEHAVIOR	Machine Learning detection
EXPLANATION	Sample behaves very similarly to known malware
BENIGN CAUSES	Clean applications should not do this
MALICIOUS CAUSES	Malware has been detected by Neural network Machine Learning
BEHAVIOR	New files in Program Files folder created
EXPLANATION	Sample has created new files in the Windows Program Files folder
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Sample may be a Potentially Unwanted Application



**SECURITY
DAYS**

ESET Enterprise Inspector



ENJOY SAFER TECHNOLOGY™

PREDICT

POLICY

PREVENT

NEW ESET Threat Intelligence
ESET Virus Radar
WeLive Security

ESET Endpoint Security
ESET Virtualization Security
ESET Security Management Center
ESET Secure Authentication
ESET Encryption

**CLOSING
THE LOOP**

ESET Security Management Center

NEW ESET Enterprise Inspector

NEW ESET Dynamic Threat Defense

ESET Endpoint Security
ESET Security Management Center
ESET Enterprise Inspector **NEW**
ESET Dynamic Threat Defense **NEW**

RESPOND

COMPLIANCE

DETECT

Problém: Cílené útoky a APT

- Modifikácia hrozieb aby obchádzali detekciu
- Doba nepozorovaného parazitovania
- Na útoky sú použité aj iné ako spustiteľné súbory

Riešenie: ESET Enterprise Inspector



Detekcia

**Detekcia
anomalíí**



Prehľad

- Čo
- Ako
- Kedy



Reakcia

- **Blokovanie**
- **Odstránenie**

Nutné predpoklady

- Incident management proces
- IT security tím
- Patch management

Princípy fungovania?

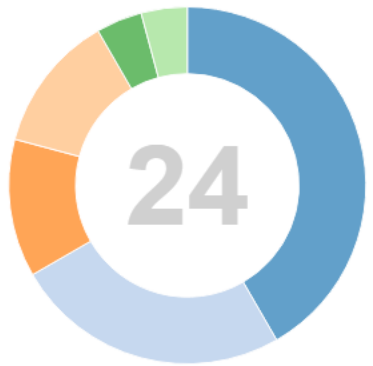
- Zaznamenávanie aktuálnych udalostí v systémoch
- Rozsiahle filtrovanie
- Reputácia na základe ESET technológií
- Vytváranie vlastných notifikačných pravidiel YARA
- Blokovanie a odstránenie

Dashboard

Alarms Executables Computer Computers & Alerts Server Status

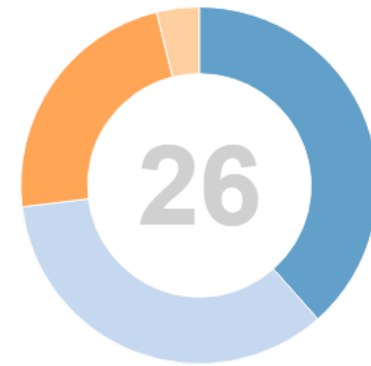
ADD FILTER

Top 10 Threat and Warning Alarms



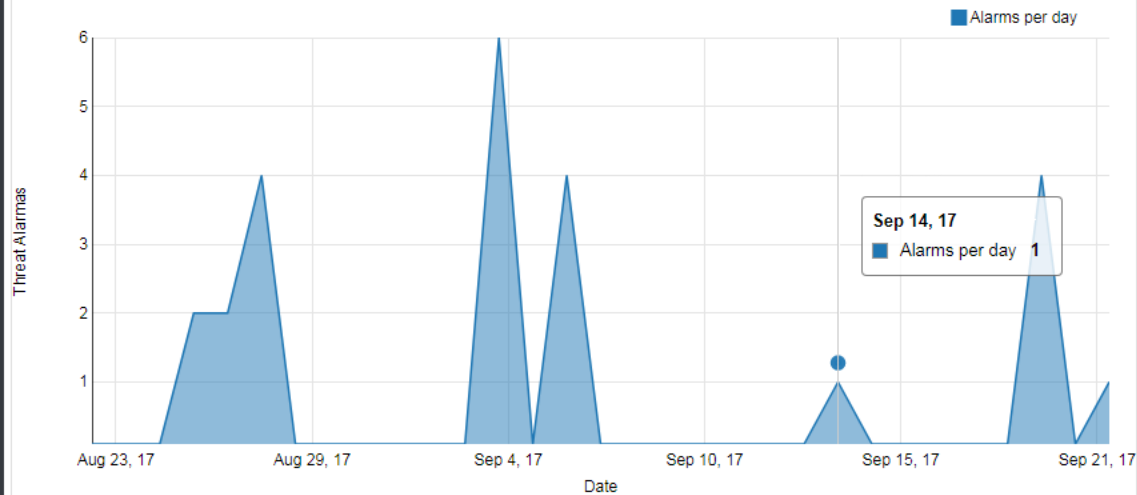
- Detected by ESET Endpoint Security product (10)
- Non-System process with system process name has started [Z0400]...
- Common AutoStart registry modified by unpopular process [A0103] ...
- Unpopular process has started from %Temp% [Z0402] (3)
- Windows Firewall rules manipulation [B0202] (1)
- EXE patching or dropping [B0304] (1)

Top 10 Informational Alarms

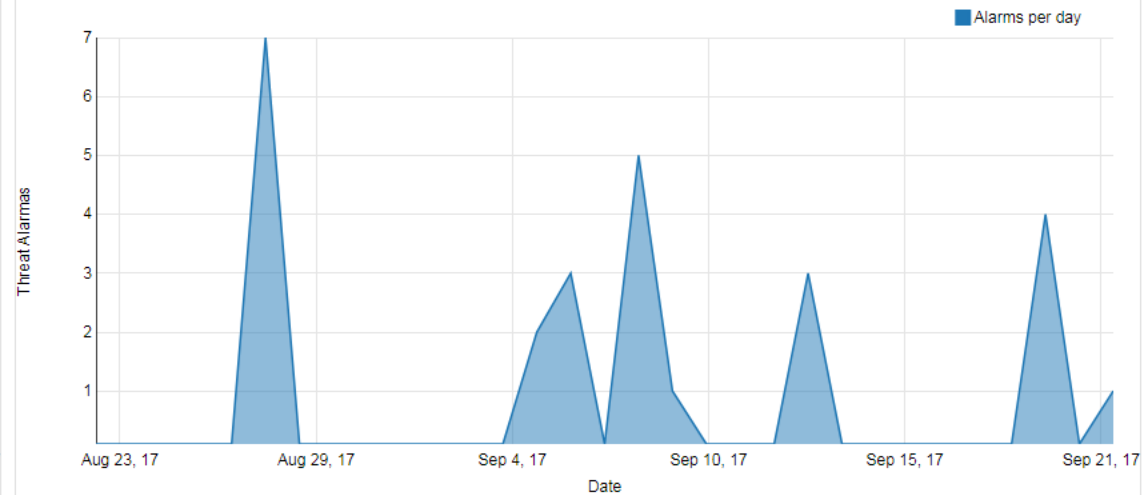


- System utility was executed test [A0403] (10)
- Unpopular process has started from %AppData%/ProgramData% [Z04...
- Cmd.exe executed with '/c' by unpopular process [A0400] (6)
- Service installation or modification [B0402] (1)

Threat and Warning Alarms



Informational Alarms



- DASHBOARD
- ALARMS**
- EXECUTABLES
- SCRIPTS
- COMPUTERS
- ADMIN

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 i
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 f
Rule Unpopular process has started from %AppData%\%ProgramData% [Z				2 weeks ago	JANKECH-TVM5	AEMAgent.exe	AEMAgent.exe (4304)	Unpopular process f
Rule Unpopular process has started from %AppData%\%ProgramData% [Z				2 weeks ago	JANKECH-TVM2	AEMAgent.exe	AEMAgent.exe (3648)	Unpopular process f
Rule Unpopular process has started from %AppData%\%ProgramData% [Z				2 weeks ago	jankech-tvm8	AEMAgent.exe	AEMAgent.exe (6812)	Unpopular process f
Rule Unpopular process has started from %AppData%\%ProgramData% [Z				2 weeks ago	Jankech-tvm11	AEMAgent.exe	AEMAgent.exe (8932)	Unpopular process f
Rule Unpopular process has started from %AppData%\%ProgramData% [Z				2 weeks ago	JANKECH-TVM3	AEMAgent.exe	AEMAgent.exe (6940)	Unpopular process f
Rule Common AutoStart registry modified by unpopular process [A0103]				2 weeks ago	JANKECH-TVM5	badexe.exe	epic.exe (3764)	Common AutoStart i
Rule EXE patching or dropping [B0304]				2 weeks ago	JANKECH-TVM5	badexe.exe	epic.exe (3764)	EXE patching or dro
Rule Common AutoStart registry modified by unpopular process [A0103]				2 weeks ago	JANKECH-TVM5	badexe.exe	bla.exe (3988)	Common AutoStart i
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 f
Rule Unpopular process has started from %AppData%\%ProgramData% [Z				2 weeks ago	Jankech-tvm11	AEMAgent.exe	AEMAgent.exe (3180)	Unpopular process f

MARK AS RESOLVED
MARK AS UNRESOLVED
MARK AS NO PRIORITY
MARK AS PRIORITY I
MARK AS PRIORITY II
MARK AS PRIORITY III
EDIT RULE

DASHBOARD

ALARMS

EXECUTABLES

SCRIPTS

COMPUTERS

ADMIN

< BACK Alarm details

Unpopular process has started from %Tem...

SOURCE Rule: Unpopular process has started from %Temp% [Z0402]
CATEGORY Suspicious process creation and process manipulation
OCCURED Sep 20, 2017, 12:41:25 PM
PRIORITY 0

eei_demo.exe

SIGNATURE TYPE None
SIGNER NAME None
SEEN ON 1 computer
FIRST SEEN 4 weeks ago - Aug 25, 2017, 5:40:11 AM
LAST EXECUTED 2 days ago - Sep 20, 2017, 12:41:25 PM

ESET LiveGrid®

REPUTATION
POPULARITY
FIRST SEEN 3 months ago

JANKECH-TVM3

PARENT GROUP Desktops
LAST CONNECTED Sep 22, 2017, 3:54:36 PM
LAST EVENT Sep 22, 2017, 3:51:50 PM
AGENT VERSION 1.0.505
OS Windows 10

TYPE	Rule
INFO	Rule was activated
SOURCE	Rule: Unpopular process has started from %Temp% [Z0402]
OCCURED	Sep 20, 2017, 12:41:25 PM
PRIORITY	0
SEVERITY	Warning
RESOLVED	No
PROCESS	eei_demo.exe (7580) +
COMPUTER	JANKECH-TVM3 View alarms on this computer
EXECUTABLE	eei_demo.exe +
CATEGORY	Suspicious process creation and process manipulation
EXPLANATION	Unpopular process executed process from %temp% folder.
MALICIOUS CAUSES	Popular folder location for malware
BENIGN CAUSES	Various installers
RECOMMENDED ACTIONS	Evaluate executed process, its commandline and execution chain. Check for presence of new/non-standard processes on computer. Start incident response process if suspicious (e.g. disconnect computer, update AV and scan, send sample to analysis, block module)

MARK AS RESOLVED

MARK AS NO PRIORITY

MARK AS PRIORITY I

MARK AS PRIORITY II

MARK AS PRIORITY III

EDIT RULE

- DASHBOARD
- ALARMS
- EXECUTABLES
- SCRIPTS
- COMPUTERS
- ADMIN

Executables EXE DLI ⚠ ! ! ✓ BLOCKED SAFE ADD FILTER

NAME (8235)	STATUS	EXECUTED ON COMPUTERS	REPUTATION (LIVEGRID®)	POPULARITY (LIVEGRID®)	FIRST SEEN (LIVEGRID®)	SIGNATURE TYPE	SIGNER NAME	FILE DESC
apt.4.0.exe	⚠	0	●●●●●●●●	●●●●●●●●	7 years ago	None	None	None
eset-testfile.exe	⚠	0	●●●●●●●●	●●●●●●●●	2 years ago	None	None	None
badexe.exe	!	1	●●●●●●●●	●●●●●●●●	6 months ago	None	None	BadExe
eei_demo.exe	!	1	●●●●●●●●	●●●●●●●●	3 months ago	None	None	None
cmd.exe	!	1	●●●●●●●●	●●●●●●●●	2 years ago	Valid	Microsoft Windows	Windows Co
potentiallyunwanted.exe	!	0	●●●●●●●●	●●●●●●●●	2 years ago	Trusted	ESET, spol. s r.o.	None
InstHelper.exe	!	1	●●●●●●●●	●●●●●●●●	Not seen	Valid	ESET, spol. s r.o.	ESET Install
cmd.exe	!	8	●●●●●●●●	●●●●●●●●	5 years ago	Trusted	Microsoft Windows	Windows Co
cmd.exe	!	1	●●●●●●●●	●●●●●●●●	5 years ago	Trusted	Microsoft Windows	Windows Co
cmd.exe	!	2	●●●●●●●●	●●●●●●●●	one year ago	Trusted	Microsoft Windows	Windows Co
cmd.exe	!	1	●●●●●●●●	●●●●●●●●	one year ago	Trusted	Microsoft Windows	Windows Co
regedit.exe	!	1	●●●●●●●●	●●●●●●●●	2 years ago	Valid	Microsoft Windows	Registry Cor
AEMAgent.exe	!	5	●●●●●●●●	●●●●●●●●	2 weeks ago	Trusted	Autotask International Holdings Limited	AEM Agent
61.0.3163.79_60.0.3112.113_chrome_updater.exe	!	1	●●●●●●●●	●●●●●●●●	2 weeks ago	Trusted	Google Inc	Google Chr
AEMAgent.exe	!	5	●●●●●●●●	●●●●●●●●	one week ago	Trusted	Autotask International Holdings Limited	AEM Agent
smss.exe	✓	0	●●●●●●●●	●●●●●●●●	one month ago	Trusted	Microsoft Windows	Windows Se
csrss.exe	✓	8	●●●●●●●●	●●●●●●●●	7 years ago	Trusted	Microsoft Windows	Client Serve
wininit.exe	✓	8	●●●●●●●●	●●●●●●●●	7 years ago	Trusted	Microsoft Windows	Windows St
winlogon.exe	✓	8	●●●●●●●●	●●●●●●●●	2 years ago	Trusted	Microsoft Windows	Windows Lo
services.exe	✓	8	●●●●●●●●	●●●●●●●●	2 years ago	Trusted	Microsoft Windows	Services anc
lsass.exe	✓	8	●●●●●●●●	●●●●●●●●	one month ago	Trusted	Microsoft Windows	Local Secur
lsm.exe	✓	8	●●●●●●●●	●●●●●●●●	5 years ago	Trusted	Microsoft Windows	Local Sessio
svchost.exe	✓	8	●●●●●●●●	●●●●●●●●	7 years ago	Trusted	Microsoft Windows	Host Proces
dipsrv.exe	✓	9	●●●●●●●●	●●●●●●●●	6 months ago	Trusted	DESlock Limited	DESlock+ Se
vmacthlp.exe	✓	7	●●●●●●●●	●●●●●●●●	one year ago	Trusted	VMware, Inc.	VMware Act
LogonUI.exe	✓	8	●●●●●●●●	●●●●●●●●	5 years ago	Trusted	Microsoft Windows	Windows Lc
spoolsv.exe	✓	8	●●●●●●●●	●●●●●●●●	5 years ago	Trusted	Microsoft Windows	Spooler Sub
EPA Agent.exe	✓	0	●●●●●●●●	●●●●●●●●	6 months ago	Trusted	ESET spol. s r.o.	ESET Remot

MARK AS SAFE MARK AS UNSAFE BLOCK UNBLOCK COMPUTERS

DASHBOARD

ALARMS

EXECUTABLES

SCRIPTS

COMPUTERS

ADMIN

< BACK eei_demo.exe - Executable details

Details Statistics Alarms Computers Droppers

eei_demo.exe

SIGNATURE TYPE	None
SIGNER NAME	None
SEEN ON	1 computer
FIRST SEEN	4 weeks ago - Aug 25, 2017, 5:40:11 AM
LAST EXECUTED	2 days ago - Sep 20, 2017, 12:41:25 PM

ESET LiveGrid®

REPUTATION	
POPULARITY	
FIRST SEEN	3 months ago

Events

File	36540
Registry	20
Network	12922

Alarms (unresolved)
Unique / total

Threats	0
Warnings	3 / 4
Informational	1 / 1

SHA-1 8D349F798541B4361C899D585D50F1F7164704E5

SIGNATURE TYPE None

SIGNER NAME None

WHITELIST TYPE None

FILE DESCRIPTION None

FILE VERSION None

COMPANY NAME None

PRODUCT NAME None

PRODUCT VERSION None

INTERNAL NAME None

ORIGINAL FILE NAME None

PACKER NAME UPX v13_m2








SFX NAME None

FILE SIZE 40.5 KB (41472 bytes)

FIRST SEEN 4 weeks ago - Aug 25, 2017, 5:40:11 AM

FIRST EXECUTED 4 weeks ago - Aug 25, 2017, 5:40:11 AM

MARK AS SAFE BLOCK DOWNLOAD FILE

-  DASHBOARD
-  ALARMS
-  EXECUTABLES
-  **SCRIPTS**
-  COMPUTERS
-  ADMIN
-  COLLAPSE MENU

Scripts UNGROUPED SAFE ADD FILTER

PROCESS NAME (ID) (32)	COMPUTER	STATUS	SAFE	UNRESOLVED ALARMS (UNIQUE)	RESOLVED ALARMS	USER	STARTED	ENDED	PARENT NAME
powershell.exe (137420)	JANKECH.hq.eset.com	✓		0	0	va.scanner	Sep 20, 2017, 1:12:30 PM	Sep 20, 2017, 1:12:33 PM	cmd.exe
AEMAgent.exe (1352)	jankech-tvm8	✓		0	0	system	Sep 15, 2017, 3:20:16 AM		CagService.exe
AEMAgent.exe (3516)	JANKECH-TVM3	✓		0	0	system	Sep 14, 2017, 8:52:18 AM		CagService.exe
AEMAgent.exe (748)	jankech-tvm8	✓		0	0	system	Sep 14, 2017, 4:16:40 AM	Sep 15, 2017, 3:14:12 AM	CagService.exe
powershell.exe (97940)	JANKECH.hq.eset.com	✓		0	0	va.scanner	Sep 13, 2017, 1:09:04 PM	Sep 13, 2017, 1:09:09 PM	cmd.exe
AEMAgent.exe (5376)	JANKECH-TVM2	✓		0	0	system	Sep 13, 2017, 12:10:36 PM		CagService.exe
AEMAgent.exe (4044)	JANKECH-TVM5	✓		0	0	system	Sep 13, 2017, 4:26:14 AM	Sep 14, 2017, 3:44:23 AM	CagService.exe
AEMAgent.exe (2664)	Jankech-1vrn11	✓		0	0	system	Sep 13, 2017, 4:16:37 AM		CagService.exe
msic42e.tmp (75936)	JANKECH.hq.eset.com	✓		0	0	system	Sep 9, 2017, 6:11:57 PM	Sep 9, 2017, 6:12:04 PM	msiexec.exe
msibe8f.tmp (77508)	JANKECH.hq.eset.com	✓		0	0	system	Sep 9, 2017, 6:11:55 PM	Sep 9, 2017, 6:11:55 PM	msiexec.exe
install.exe (72884)	JANKECH.hq.eset.com	✓		0	0	system	Sep 9, 2017, 6:11:54 PM	Sep 9, 2017, 6:12:05 PM	silverlight.exe
AEMAgent.exe (5152)	JANKECH-TVM2	✓		0	0	system	Sep 9, 2017, 1:37:17 PM	Sep 13, 2017, 8:54:05 AM	CagService.exe
AEMAgent.exe (1832)	JANKECH-TVM5	✓		0	0	system	Sep 9, 2017, 1:37:05 PM	Sep 13, 2017, 4:16:59 AM	CagService.exe
AEMAgent.exe (5116)	Jankech-tvm11	✓		0	0	system	Sep 9, 2017, 1:36:09 PM		CagService.exe
AEMAgent.exe (8160)	jankech-tvm8	ⓘ		1	0	system	Sep 9, 2017, 1:16:34 PM	Sep 14, 2017, 4:06:22 AM	CagService.exe
AEMAgent.exe (8104)	JANKECH-TVM3	✓		0	0	system	Sep 9, 2017, 12:53:36 PM	Sep 14, 2017, 8:38:04 AM	CagService.exe
AEMAgent.exe (3648)	JANKECH-TVM2	ⓘ		1	0	system	Sep 8, 2017, 1:36:42 PM	Sep 9, 2017, 1:36:06 PM	CagService.exe
AEMAgent.exe (6812)	jankech-tvm8	ⓘ		1	0	system	Sep 8, 2017, 12:55:45 PM	Sep 9, 2017, 1:15:19 PM	CagService.exe
AEMAgent.exe (8932)	Jankech-tvm11	ⓘ		1	0	system	Sep 8, 2017, 12:55:39 PM	Sep 9, 2017, 1:34:55 PM	CagService.exe
AEMAgent.exe (4304)	JANKECH-TVM5	ⓘ		1	0	system	Sep 8, 2017, 12:55:29 PM	Sep 9, 2017, 1:35:30 PM	CagService.exe
AEMAgent.exe (6940)	JANKECH-TVM3	ⓘ		1	0	system	Sep 8, 2017, 12:42:48 PM	Sep 9, 2017, 12:52:27 PM	CagService.exe
AEMAgent.exe (3280)	JANKECH-TVM5	✓		0	0	system	Sep 6, 2017, 1:31:05 PM	Sep 8, 2017, 12:55:10 PM	CagService.exe
powershell.exe (59028)	JANKECH.hq.eset.com	✓		0	0	va.scanner	Sep 6, 2017, 1:08:49 PM	Sep 6, 2017, 1:08:53 PM	cmd.exe
AEMAgent.exe (4520)	JANKECH-TVM2	✓		0	0	system	Sep 6, 2017, 10:36:23 AM	Sep 8, 2017, 1:35:58 PM	CagService.exe
AEMAgent.exe (5228)	JANKECH-TVM3	✓		0	0	system	Sep 6, 2017, 9:57:54 AM	Sep 8, 2017, 12:42:11 PM	CagService.exe
AEMAgent.exe (5416)	jankech-tvm8	✓		0	0	system	Sep 6, 2017, 9:20:33 AM	Sep 8, 2017, 12:55:04 PM	CagService.exe
SETUP.EXE (10164)	Jankech-tvm11	✓		0	1	admin	Sep 6, 2017, 1:04:45 AM	Sep 6, 2017, 1:18:04 AM	61.0.3163.75
SETUP.EXE (4320)	Jankech-tvm11	✓		0	1	admin	Sep 6, 2017, 1:04:45 AM	Sep 6, 2017, 1:18:04 AM	SETUP.EXE

MARK AS SAFE MARK AS UNSAFE

DASHBOARD

ALARMS

EXECUTABLES

SCRIPTS

COMPUTERS

ADMIN

< BACK All > HQ - Bratislava > Desktops > Jankech-tvm11 > 61.0.3163.79_60.0.3112.113_chrome_updater.exe > 61.0.3163.79_60.0.3112.113_chrome_updater.exe - Process details

Details Aggregated Events Alarms Raw Events Loaded Modules (DLLs)

61.0.3163.79_60.0.3112.113_chrome_updater.exe
Google Chrome Installer

SIGNATURE TYPE	Trusted
SIGNER NAME	Google Inc
SEEN ON	1 computer
FIRST SEEN	2 weeks ago - Sep 6, 2017, 1:04:35 AM
LAST EXECUTED	2 weeks ago - Sep 6, 2017, 1:04:40 AM

ESET LiveGrid®

REPUTATION	●●●●●●
POPULARITY	●●●●●●
FIRST SEEN	2 weeks ago

Jankech-tvm11

PARENT GROUP	Desktops
LAST CONNECTED	Sep 22, 2017, 4:11:16 PM
LAST EVENT	Sep 22, 2017, 4:11:07 PM
AGENT VERSION	1.0.503
OS	Windows 7

Events

File
6

Registry
1

Network
0

PROCESS 61.0.3163.79_60.0.3112.113_chrome_updater.exe (3228)

COMMAND LINE "c:\users\admin\appdata\local\google\update\install\{ad95bcab-3cfc-42ed-8a69-65220924176f}\61.0.3163.79_60.0.3112.113_chrome_updater.exe" --verbose-logging --do-not-launch-chrome

PATH %LOCALAPPDATA%\google\update\install\{ad95bcab-3cfc-42ed-8a69-65220924176f}\

USER admin

STARTED Sep 6, 2017, 1:04:40 AM

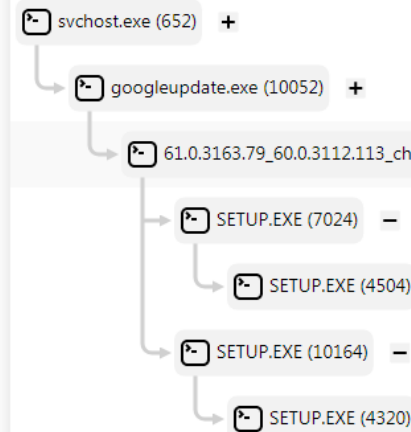
ENDED Sep 6, 2017, 1:18:04 AM

PARENT PROCESS googleupdate.exe (10052)

COMPUTER Jankech-tvm11

DOWNLOAD FILE

KILL PROCESS



- ALARMS
- EXECUTABLES
- SCRIPTS
- COMPUTERS
- ADMIN

Alarm rules Blocked hashes

⚠️ ⓘ ⓘ ADD FILTER

<input type="checkbox"/>	RULE NAME (172) ▾	AUTHOR	ENABLED	VALID	SEVERITY	CATEGORY
<input type="checkbox"/>	🔍 .NET appx_process registry modified [A0111]	ESET	true	true	⚠️	Persistence
<input type="checkbox"/>	🔍 .NET profiler registry modified [A0109]	ESET	true	true	ℹ️	Persistence
<input type="checkbox"/>	🔍 .NET winappxrt.dll file modified [A0110]	ESET	true	true	⚠️	Persistence
<input type="checkbox"/>	🔍 Accessibility Features file modified [A0304]	ESET	true	true	ℹ️	File system
<input type="checkbox"/>	🔍 Active Setup autostart registry entry modified [A0100]	ESET	true	true	ℹ️	Persistence
<input type="checkbox"/>	🔍 ADS written by unpopular process [A0300]	ESET	true	true	⚠️	File system
<input type="checkbox"/>	🔍 AppInit registry entry was created [A0101]	ESET	true	true	⚠️	Persistence
<input type="checkbox"/>	🔍 Autorun.inf file was created/modified [A0301]	ESET	true	true	ℹ️	File system
<input type="checkbox"/>	🔍 Autorun.inf file was deleted [A0301]	ESET	true	true	ℹ️	File system
<input type="checkbox"/>	🔍 Bad extension - filecoders (ext. A - C) [C0607]	ESET	true	true	⚠️	Filecoders
<input type="checkbox"/>	🔍 Bad extension - filecoders (ext. D - L) [C0608]	ESET	true	true	⚠️	Filecoders
<input type="checkbox"/>	🔍 Bad extension - filecoders (ext. M - Z) [C0609]	ESET	true	true	⚠️	Filecoders
<input type="checkbox"/>	🔍 Bad extension - filecoders (ext. spec., num.) [C0606]	ESET	true	true	⚠️	Filecoders
<input type="checkbox"/>	🔍 Browser Helper Objects registry modified by unpopular proces	ESET	true	true	ℹ️	Persistence
<input type="checkbox"/>	🔍 Chrome executing suspicious extension [B0703]	ESET	true	true	⚠️	Web browser related
<input type="checkbox"/>	🔍 Chrome renaming [B0702]	ESET	true	true	⚠️	Web browser related
<input type="checkbox"/>	🔍 Chrome updates disabling [B0701]	ESET	true	true	⚠️	Web browser related
<input type="checkbox"/>	🔍 Clearing event logs [B1001]	ESET	true	true	⚠️	Removing evidence
<input type="checkbox"/>	🔍 cmd.exe executed under different name [B0404]	ESET	true	true	⚠️	Suspicious process creation and proces
<input type="checkbox"/>	🔍 Cmd.exe executed with '/c' by unpopular process [A0400]	ESET	true	true	ℹ️	Suspicious process creation and proces
<input type="checkbox"/>	🔍 Common AutoStart registry modified by unpopular process [A	ESET	true	true	⚠️	Persistence
<input type="checkbox"/>	🔍 Connection to malicious site - Wauchos [Z0501]	ESET	true	true	⚠️	Communication
<input type="checkbox"/>	🔍 Credential Providers registry modified by unpopular process [A	ESET	true	true	⚠️	Persistence
<input type="checkbox"/>	🔍 cscript executed under different name [D0409]	ESET	true	true	⚠️	Suspicious process creation and proces

DASHBOARD

ALARMS

EXECUTABLES

SCRIPTS

COMPUTERS

ADMIN

< BACK Bad extension - filecoders (ext. A - C) [C0607] Edit rule

```

1 <?xml version="1.0" encoding="utf-8"?>
2 <rule>
3   <description>
4     <explanation>Process writes files with suspicious extensions. The rule contains list of common extensions used by ransomware starting with A-C. Seldom the rule may trigger on clean application (e. g. while
performing backup of encrypted files).</explanation>
5     <maliciousCauses>Filecoder is encrypting files.</maliciousCauses>
6     <benignCauses>Backup process or administrator is copying encrypted files.</benignCauses>
7     <recommendedActions>1. Scan the related process with AV.
8     2. If not detected then submit the executable for analysis.
9     3. Search for encrypted files. Shares on network may be affected.
10    4. Restore encrypted files from backup (backup encrypted files for future decryption)
11  </recommendedActions>
12  <category>Filecoders</category>
13  <guid>86a47275-746e-4b38-8b7a-4509d033349a </guid>
14  <name>Bad extension - filecoders (ext. A - C) [C0607]</name>
15  <severity>Threat</severity>
16 </description>
17 <definition>
18 <!-- rev 20170825 -->
19 <Process>
20   <operator type="AND">
21     <condition component="LiveGrid" condition="less" property="Reputation" value="8"/>
22   </operator>
23 </Process>
24 <operations>
25   <operation type="WriteFile">
26     <operator type="OR">
27       <!-- only extensions with size more than 3 are included starting with A-C -->
28       <!-- extensions without comments are gathered from external resources -->
29       <!-- Win32/Filecoder.FV -->
30       <condition component="FileItem" condition="ends" property="Extension" value="A1crypt"/>
31       <!-- MSIL/Filecoder.C/AC/BU -->
32       <condition component="FileItem" condition="ends" property="Extension" value="adamlars"/>
33       <!-- more variants use this -->
34       <condition component="FileItem" condition="ends" property="Extension" value="AES256"/>
35       <!-- Win32/Filecoder.AESNI -->
36       <condition component="FileItem" condition="ends" property="Extension" value="aes_ni"/>
37       <condition component="FileItem" condition="ends" property="Extension" value="aes_ni_0day"/>
38       <!-- Win32/Filecoder.NKP -->
39       <condition component="FileItem" condition="ends" property="Extension" value="aleta"/>
40       <!-- Win32/Filecoder.AU -->
41       <condition component="FileItem" condition="ends" property="Extension" value="amba"/>
42       <!-- Win32/Filecoder.Crysis -->
43       <condition component="FileItem" condition="ends" property="Extension" value="arena"/>
44       <!-- Win32/Filecoder.FS -->
45       <condition component="FileItem" condition="ends" property="Extension" value="badnews"/>
46       <condition component="FileItem" condition="ends" property="Extension" value="bart"/>
47       <!-- Win32/Filecoder.ED -->
48       <condition component="FileItem" condition="ends" property="Extension" value="better_call_saul"/>
49       <condition component="FileItem" condition="ends" property="Extension" value="bitcrypt"/>
50       <condition component="FileItem" condition="ends" property="Extension" value="bitstak"/>
51       <condition component="FileItem" condition="ends" property="Extension" value="bleepYourFiles"/>
52       <condition component="FileItem" condition="ends" property="Extension" value="bloccatto"/>
53       <!-- MSIL/Filecoder.C/AC/BU -->
54       <condition component="FileItem" condition="ends" property="Extension" value="block"/>
55       <!-- Win32/Filecoder.RotoCrypt -->
56       <condition component="FileItem" condition="ends" property="Extension" value="blockage42"/>
57       <!-- more variants use this -->
58       <condition component="FileItem" condition="ends" property="Extension" value="blocked"/>

```

Syntax Reference

The general structure of rule looks like this:

```

<rule>
  <name>example's name </name>
  <process />
  <operations />
</rule>

```

Process element defines which processes meet the rule conditions. Similarly, operations element defines operations which need to be executed by a process to meet the rule conditions. Both these elements are optional but one of them needs to be present in the rule. If there is no process element operations of all processes in the system are checked. If there is no operations element rule become active as soon as process which meets condition is started. If both are present a process needs to execute operations described by operations element to activate the rule. Conditions are defined using operator and condition elements. Operator element is a logical OR or AND operator. Condition element checks if a property has a required value.

```

<process>
  <operator type="AND">
    <condition component="FileItem" pr
    <condition component="FileItem" pr
  </operator>
</process>

```

This example checks if process with a name svchost was started from temp folder or its subfolders. Currently the following components and properties are supported: FileItem (Name, Extension, Path), Executable (SHA-1), LiveGrid@ (Age, Reputation, Popularity), Enterprise (Popularity), NetworkAddress (RemoteAddressIPv4, RemotePort) The condition attribute can be: is, isnot, starts, notstarts, contains, notcontains, less, lessOrEqual, greater, greaterOrEqual. Operations element contains one or more operation elements. Operation element has a type attribute and body which defines condition for this operation's argument. Here is an example checking if VBS file was written to the disk:

```

<operations>
  <operation type="WriteFile">
    <condition component="FileItem" pr
  </operation>
</operations>

```

The following operation types are supported: WriteFile, DeleteFile, RenameFile, CreateNewFile, TcpIpConnect, TcpIpAccept, RegSetValue.

FINISH CHECK SYNTAX CLOSE DELETE SAVE AS

EXPORT

COLLAPSE MENU



**SECURITY
DAYS**

Otázky?



ENJOY SAFER TECHNOLOGY™



**SECURITY
DAYS**



/ESET



@ESET



+esetglobal

#ESETDay