EDR V PROSTREDÍ NUKLEÁRNEJ MEDICÍNY

Ing. Tomáš Antonič

Digital Security
Progress. Protected.

&

konferencie

iServices

Inštitút nukleárnej a molekulárnej medicíny

Prostredie **bez** adekvátnej antivírusovej/antimalwarovej ochrany
(len natívne prostriedky Windowsu)

Inštitút absolvoval **audit** podľa **Zákona č. 69/2018 Z.z.**
o kybernetickej bezpečnosti

Nálezy auditu iniciovali nasadenie komplexnej ochrany
ESET Protect Enterprise, ktorého súčasťou je aj **EDR**

Inštitút nukleárnej a molekulárnej medicíny

- **EDR** implementované na **Windows Server**
- centrálna **MySQL databáza** na tom istom serveri
- **56** klientských **staníc** pre EDR, bez roamingových klientov
- implementácia vrátane vyladenia pravidiel trvala **1 mesiac**
- cca **150.000** eventov **denne** za pracovnú stanicu
- priemer **100** eventov **za sekundu** počas pracovného času
- peaky **800** sprocesovaných **eventov za sekundu**

Inštitút nukleárnej a molekulárnej medicíny

EDR generovalo a generuje štandardné hlásenia a výstrahy ako

- **SMTP** komunikácia na non-standard portoch
- Spúšťaný **TeamViewer** na pracovných staniciach
- **GoogleUpdate** credential dumping
- Spustenie **putty.exe**
- HTTP komunikácia na **neštandardnom** porte
- **FTP** komunikácia
- suspicious **DLL loading** – nepodpísané knižnice s nízkou reputáciou

Inštitút nukleárnej a molekulárnej medicíny

Špecifikum, nemocničný systém **LCS**

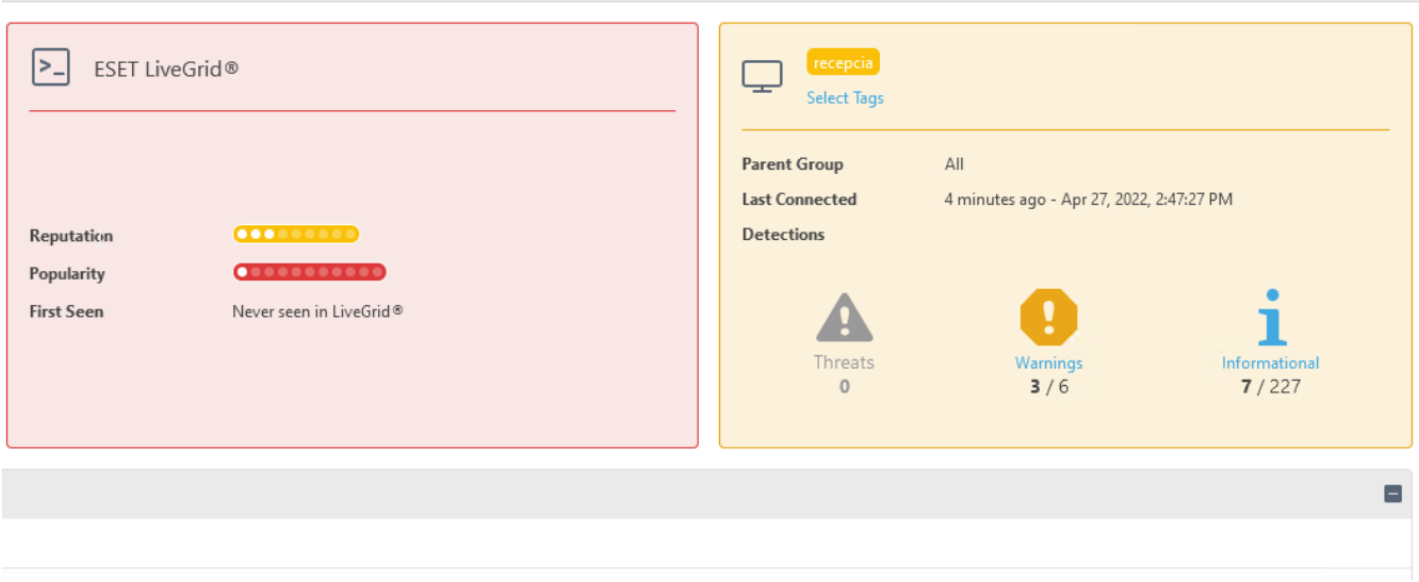
Nemocničný systém sa spúšta pomocou **lcs_launcher.exe** a načítava si rôzne moduly napr. **lcs_tyto.exe**

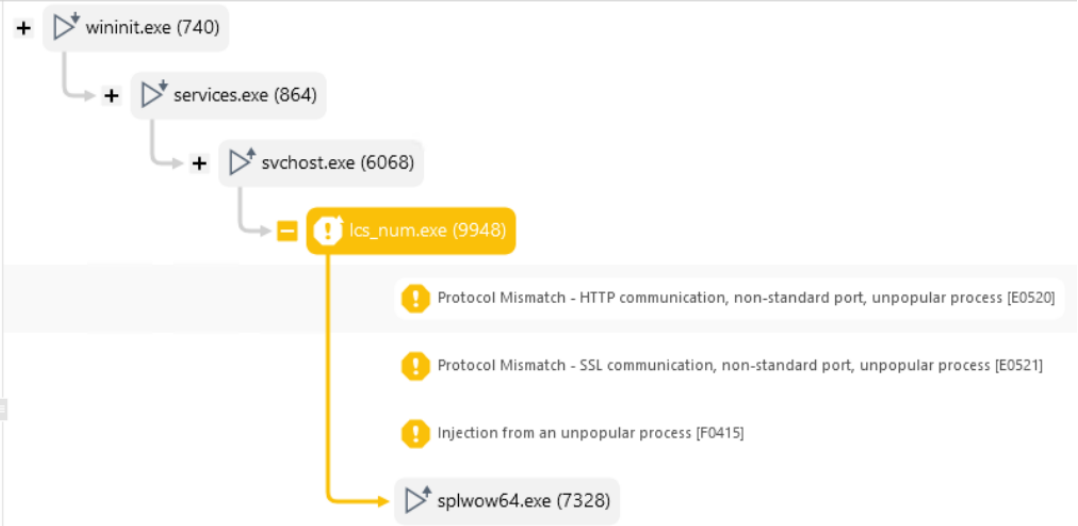
Samotný lcs_launcher spúšťa alert : **Injection into trusted process**

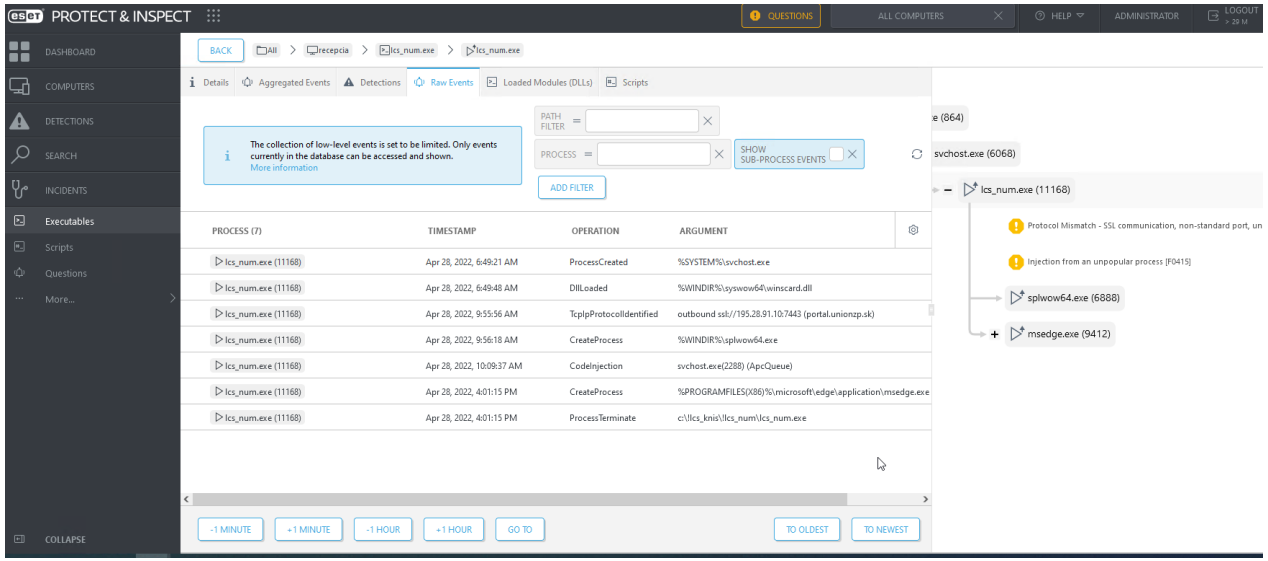
Moduly LCS napr. alerty typu:

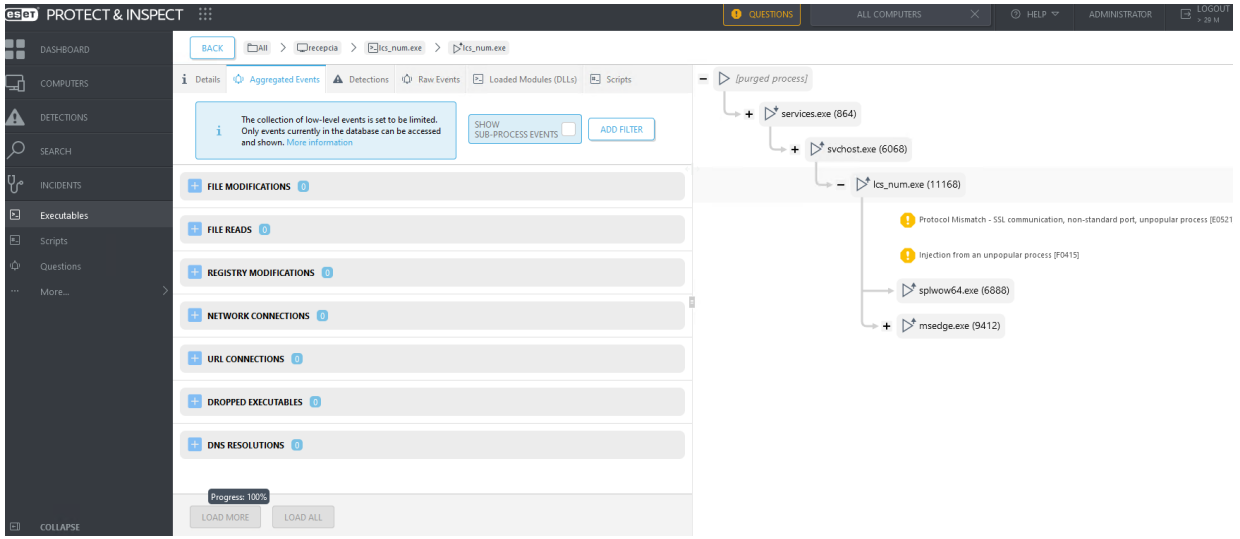
- Protocol Mismatch - HTTP communication, **non-standard port**, unpopular process
- Protocol Mismatch - SSL communication, **non-standard port**, unpopular process
- **Injection into** email client **process**
- **Injection from** an unpopular process

Takisto súbory sú označené na webe **Virustotal** rôznymi výrobcami ako **malicious**.


ESET LiveGrid®
Reputation
Popularity
First Seen
Never seen in LiveGrid®
recepcia
Select Tags
Parent Group
All
Last Connected
4 minutes ago - Apr 27, 2022, 2:47:27 PM
Detections
Threats
0
Warnings
3 / 6
Informational
7 / 227


wininit.exe (740)
services.exe (864)
svchost.exe (6068)
lcs_num.exe (9948)
Protocol Mismatch - HTTP communication, non-standard port, unpopular process [E0520]
Protocol Mismatch - SSL communication, non-standard port, unpopular process [E0521]
Injection from an unpopular process [F0415]
splwow64.exe (7328)


PROTECT & INSPECT
QUESTIONS
ALL COMPUTERS
HELP
ADMINISTRATOR
DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
INCIDENTS
Executables
Scripts
Questions
More...
COLLAPSE
BACK
Details
Aggregated Events
Detections
Raw Events
Loaded Modules (DLLs)
Scripts
The collection of low-level events is set to be limited. Only events currently in the database can be accessed and shown.
More information
PATH FILTER
PROCESS
SHOW SUB-PROCESS EVENTS
ADD FILTER
PROCESS (7)
TIMESTAMP
OPERATION
ARGUMENT
lcs_num.exe (11168) Apr 28, 2022, 6:49:21 AM ProcessCreated %SYSTEM%\svchost.exe
lcs_num.exe (11168) Apr 28, 2022, 6:49:48 AM DllLoaded %WINDIR%\syswow64\winscard.dll
lcs_num.exe (11168) Apr 28, 2022, 9:55:56 AM TcpIpProtocolIdentified outbound ssl://195.28.91.10:7443 (portal.unionzp.sk)
lcs_num.exe (11168) Apr 28, 2022, 9:56:18 AM CreateProcess %WINDIR%\splwow64.exe
lcs_num.exe (11168) Apr 28, 2022, 10:09:37 AM CodeInjection svchost.exe(2288) (ApcQueue)
lcs_num.exe (11168) Apr 28, 2022, 4:01:15 PM CreateProcess %PROGRAMFILES(X86)%\microsoft\edge\application\msedge.exe
lcs_num.exe (11168) Apr 28, 2022, 4:01:15 PM ProcessTerminate c:\!lcs_knis\!lcs_num\lcs_num.exe
-1 MINUTE
+1 MINUTE
-1 HOUR
+1 HOUR
GO TO
TO OLDEST
TO NEWEST
svchost.exe (6068)
lcs_num.exe (11168)
Protocol Mismatch - SSL communication, non-standard port, un
Injection from an unpopular process [F0415]
splwow64.exe (6888)
msedge.exe (9412)


PROTECT & INSPECT
QUESTIONS
ALL COMPUTERS
HELP
ADMINISTRATOR
DASHBOARD
COMPUTERS
DETECTIONS
SEARCH
INCIDENTS
Executables
Scripts
Questions
More...
COLLAPSE
BACK
Details
Aggregated Events
Detections
Raw Events
Loaded Modules (DLLs)
Scripts
The collection of low-level events is set to be limited. Only events currently in the database can be accessed and shown. More information
SHOW SUB-PROCESS EVENTS
ADD FILTER
FILE MODIFICATIONS
FILE READS
REGISTRY MODIFICATIONS
NETWORK CONNECTIONS
URL CONNECTIONS
DROPPED EXECUTABLES
DNS RESOLUTIONS
Progress: 100%
LOAD MORE
LOAD ALL
[purged process]
services.exe (864)
svchost.exe (6068)
lcs_num.exe (11168)
Protocol Mismatch - SSL communication, non-standard port, unpopular process [E0521
Injection from an unpopular process [F0415]
splwow64.exe (6888)
msedge.exe (9412)

c05ab652ed9aa367416f102c146513919371bd5265cea124b9270517009832c8

Sign in | Sign up

3 / 67

Community Score

3 security vendors and no sandboxes flagged this file as malicious

c05ab652ed9aa367416f102c146513919371bd5265cea124b9270517009832c8
lcs_launcher.exe
direct-cpu-clock-access | peexe | runtime-modules

3.14 MB
Size

2022-03-11 15:17:30 UTC
1 month ago

EXE

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Security Vendors' Analysis

Cybereason	Malicious.9a49b9	MaxSecure	Trojan.Malware.300983.susgen
SecureAge APEX	Malicious	Acronis (Static ML)	Undetected
Ad-Aware	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	ClamAV	Undetected

3792d5b0004b50749e7bcbaf485a519e6f0ffdf4d8d503785b7a5146ad2f5b11

Sign in

4
/ 69

Community Score

4 security vendors and no sandboxes flagged this file as malicious

3792d5b0004b50749e7bcbaf485a519e6f0ffdf4d8d503785b7a5146ad2f5b11
lcs_tyto.exe

assembly | detect-debug-environment | direct-cpu-clock-access | peexe | runtime-modules

210.00 KB
Size

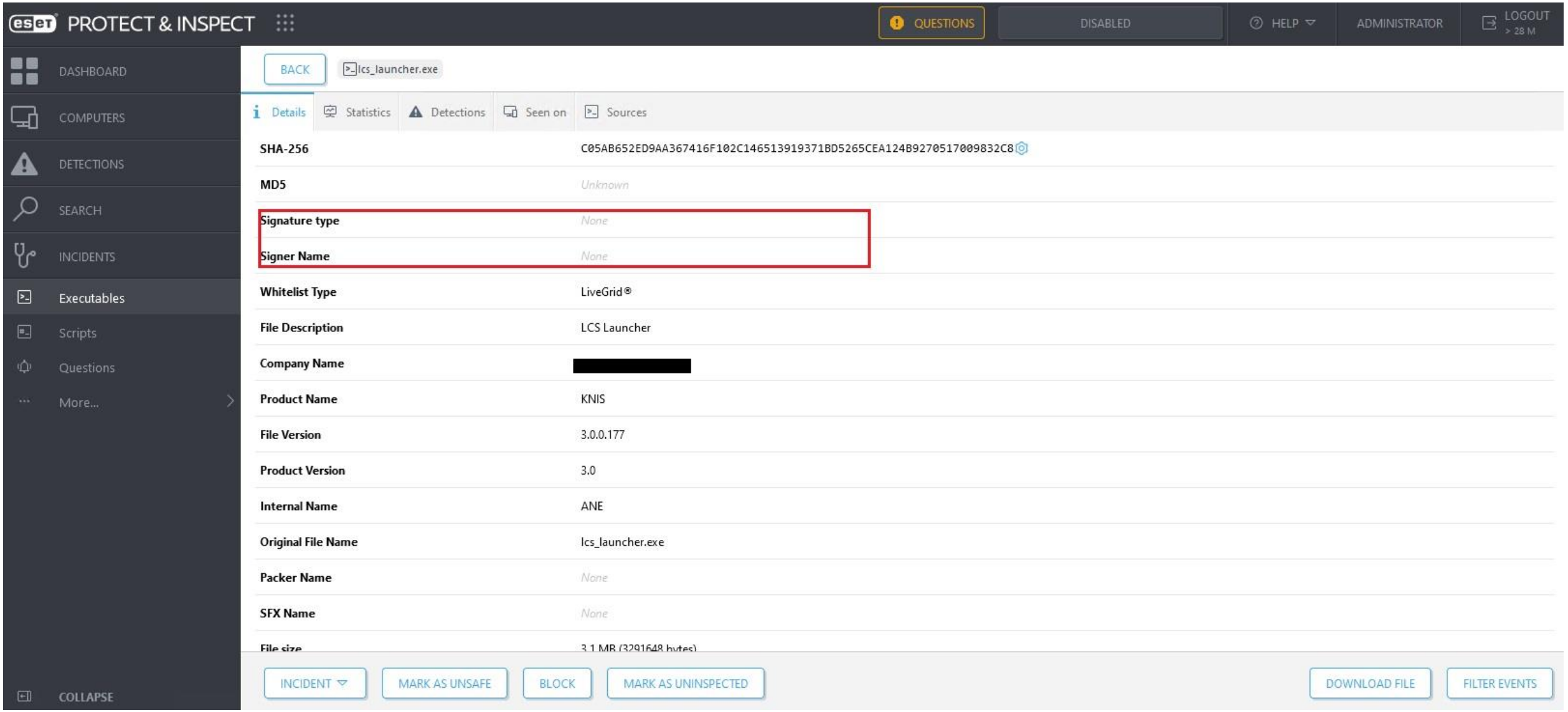
2022-04-15 01:10:59 UTC
12 days ago

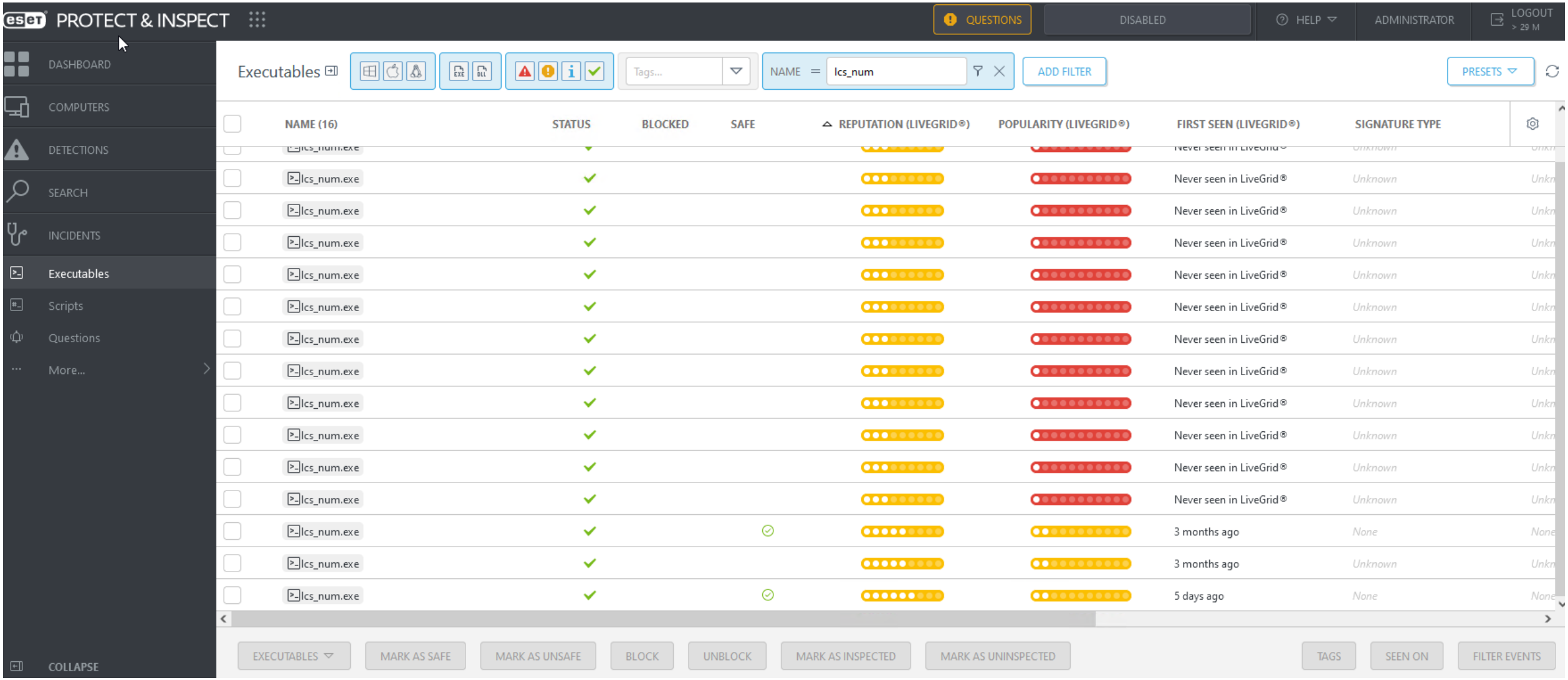
EXE

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Security Vendors' Analysis

MaxSecure	Trojan.Malware.300983.susgen	SecureAge APEX	Malicious
SentinelOne (Static ML)	Static AI - Suspicious PE	Trapmine	Malicious.high.ml.score
Acronis (Static ML)	Undetected	Ad-Aware	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected





ESET SECURITY DAYS

iServices

Ďakujem za pozornosť

ESET Digital Security Progress. Protected. & HN konferencie