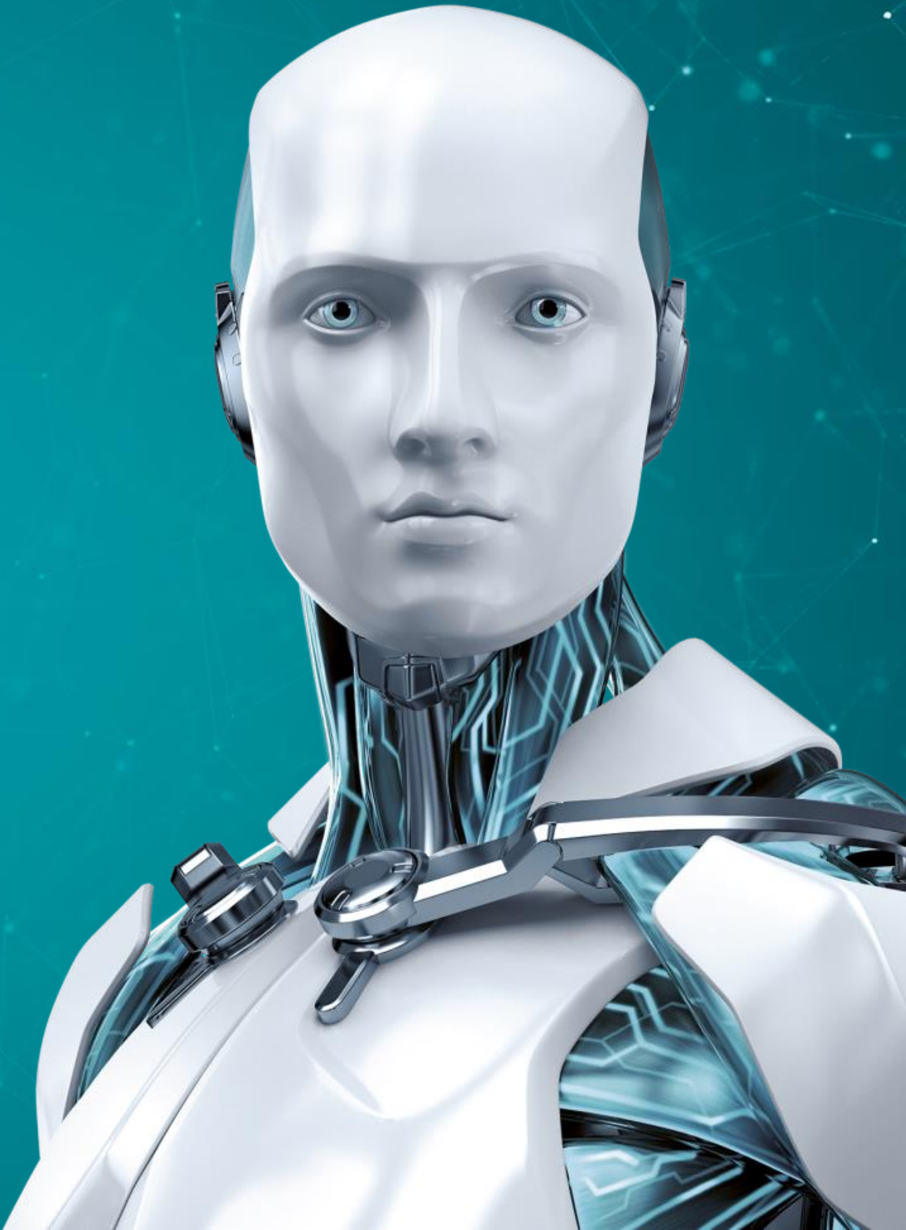
ENJOY SAFER TECHNOLOGY™

Modern threats require modern solutions

Jakub Debski / ESET



Modern threats – what are they?

0 day exploits?

Rootkits hidden in firmware?

Hardware implants?

Bloomberg Businessweek
October 8, 2018
The Big Hack

Smart attackers

… who understand your security stack

Yttrium

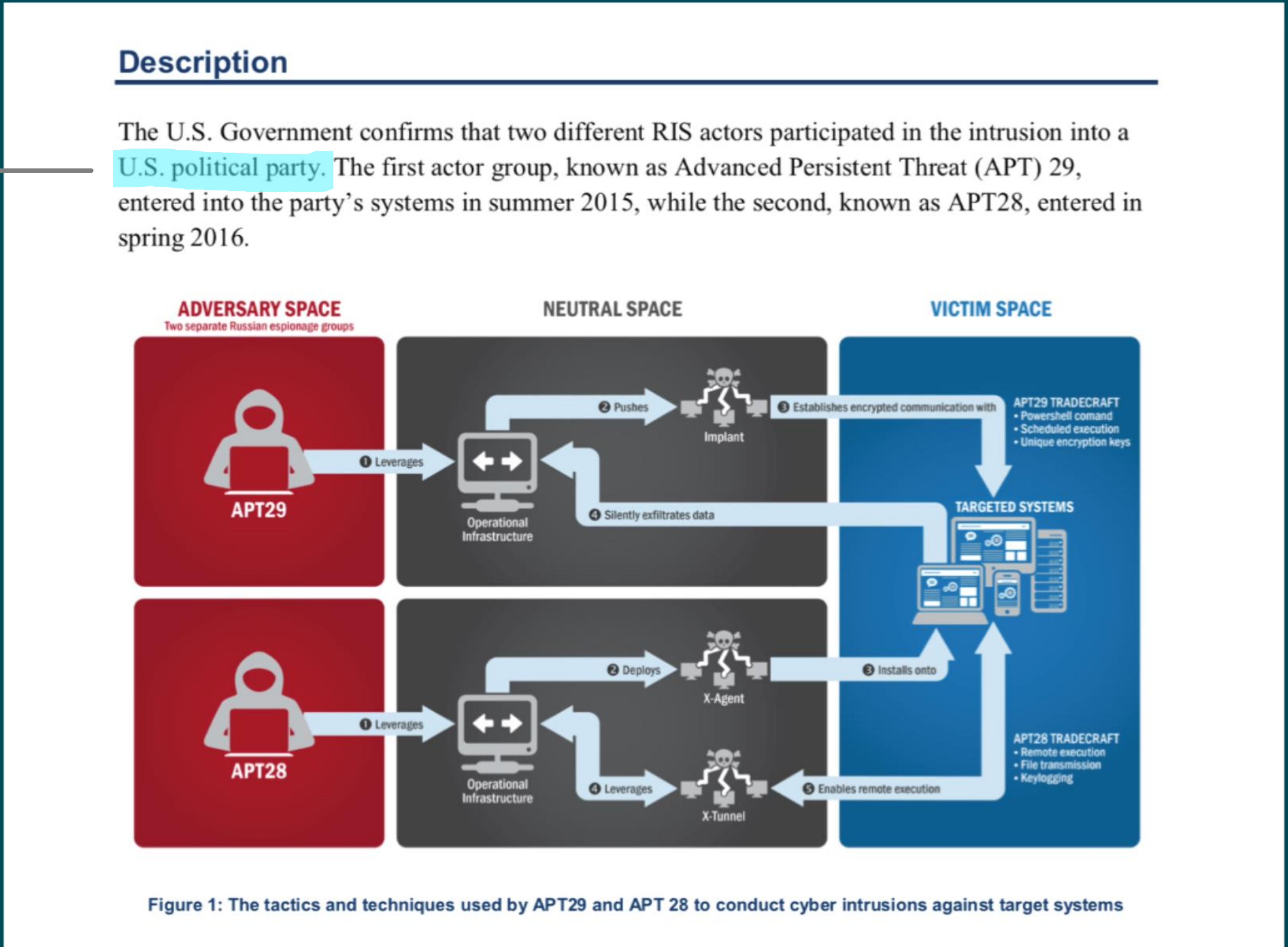
Cozy Bear

“The Dukes”

APT29

Democratic National Committee

GRIZZLY STEPPE (2015/2016)

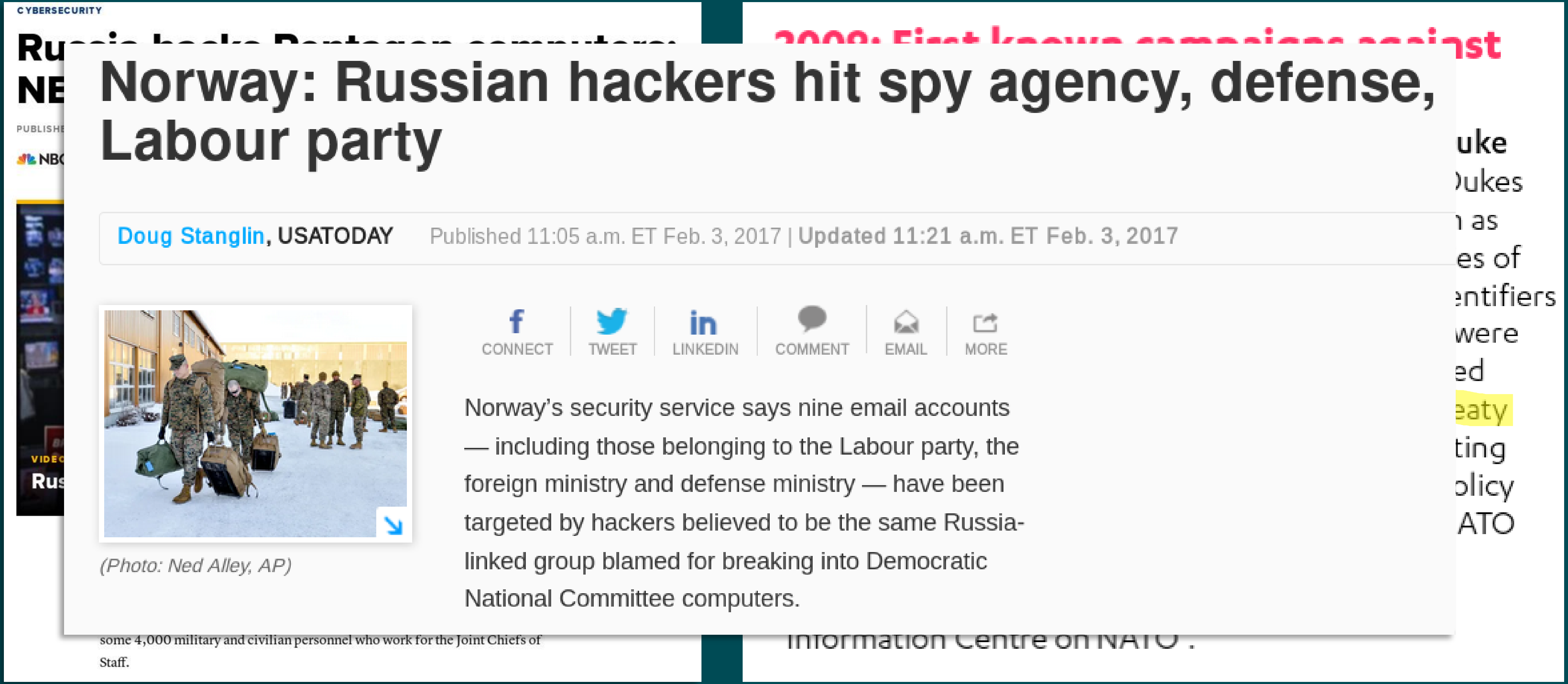


Description

The U.S. Government confirms that two different RIS actors participated in the intrusion into a U.S. political party. The first actor group, known as Advanced Persistent Threat (APT) 29, entered into the party's systems in summer 2015, while the second, known as APT28, entered in spring 2016.

ADVERSARY SPACE
Two separate Russian espionage groups
NEUTRAL SPACE
VICTIM SPACE
APT29
❶ Leverages
Operational Infrastructure
❷ Pushes
Implant
❸ Establishes encrypted communication with
❹ Silently exfiltrates data
APT29 TRADECRAFT
• Powershell comand
• Scheduled execution
• Unique encryption keys
TARGETED SYSTEMS
APT28
❶ Leverages
Operational Infrastructure
❷ Deploys
X-Agent
❸ Installs onto
❹ Leverages
X-Tunnel
❺ Enables remote execution
APT28 TRADECRAFT
• Remote execution
• File transmission
• Keylogging

Figure 1: The tactics and techniques used by APT29 and APT 28 to conduct cyber intrusions against target systems



CYBERSECURITY

Ru NE

PUBLISHE

NBC

VIDEO

Rus

2009: First known campaigns against

Norway: Russian hackers hit spy agency, defense, Labour party

Doug Stanglin, USATODAY Published 11:05 a.m. ET Feb. 3, 2017 | Updated 11:21 a.m. ET Feb. 3, 2017

(Photo: Ned Alley, AP)

Norway's security service says nine email accounts — including those belonging to the Labour party, the foreign ministry and defense ministry — have been targeted by hackers believed to be the same Russia-linked group blamed for breaking into Democratic National Committee computers.

some 4,000 military and civilian personnel who work for the Joint Chiefs of Staff.

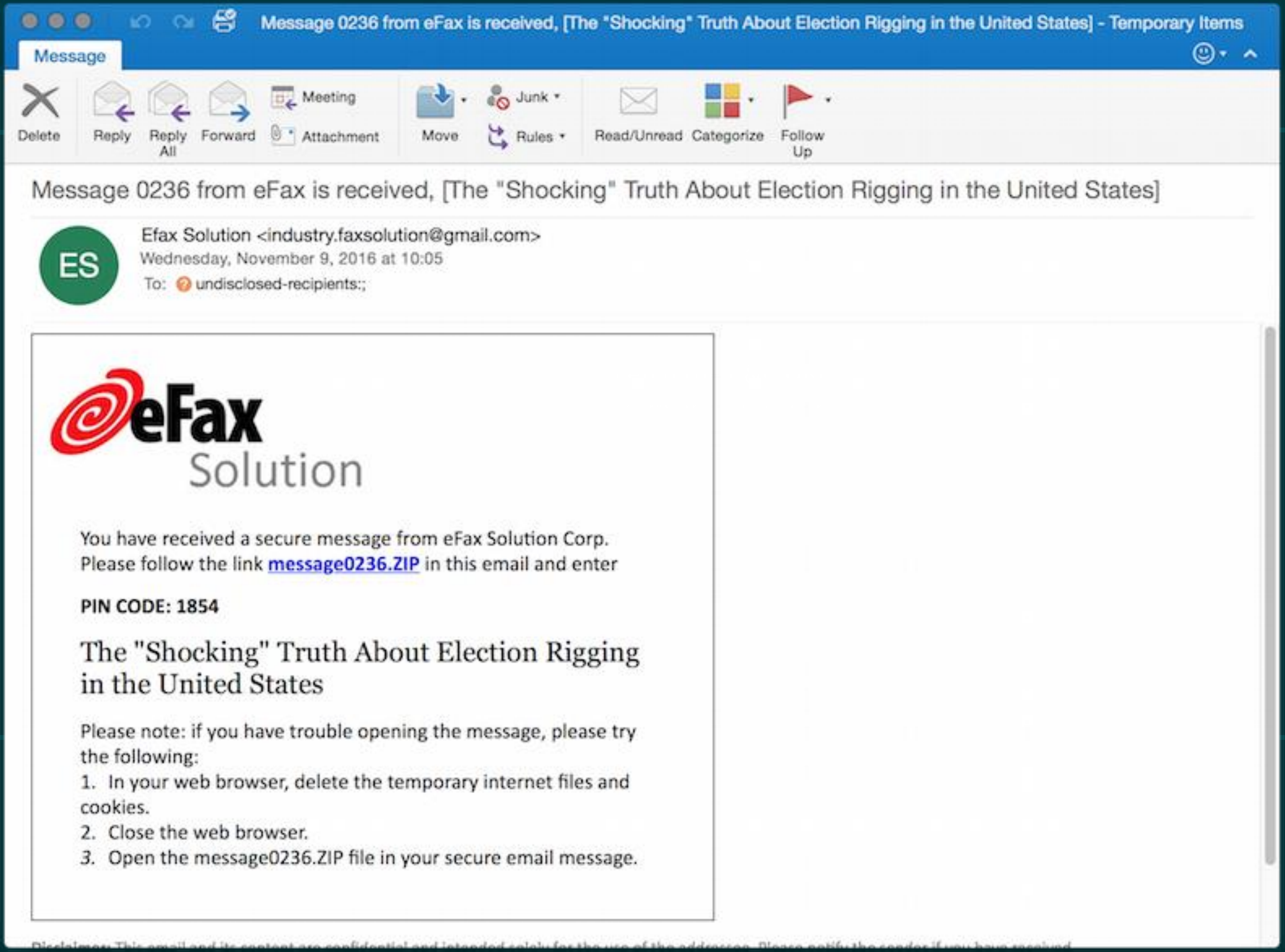
uke
Dukes
as
es of
entifiers
were
ed
eaty
ting
olicy
ATO

Information Centre on NATO".

After 2017 ?

How this research started

- Started ~ 18 months ago
- We analyzed three different malware families that were not apparently linked
- They were found in the same networks



Message 0236 from eFax is received, [The "Shocking" Truth About Election Rigging in the United States] - Temporary Items

Message 0236 from eFax is received, [The "Shocking" Truth About Election Rigging in the United States]

ES Efax Solution <industry.faxsolution@gmail.com>
Wednesday, November 9, 2016 at 10:05
To: undisclosed-recipients:;

You have received a secure message from eFax Solution Corp.
Please follow the link message0236.ZIP in this email and enter

PIN CODE: 1854

The "Shocking" Truth About Election Rigging in the United States

Please note: if you have trouble opening the message, please try the following:

1. In your web browser, delete the temporary internet files and cookies.
2. Close the web browser.
3. Open the message0236.ZIP file in your secure email message.

Disclaimer: This email and its content are confidential and intended solely for the use of the addressee. Please notify the sender if you have received

Use of Documents with macros to bypass **filetype filtering on Mail/Web Gateway** level

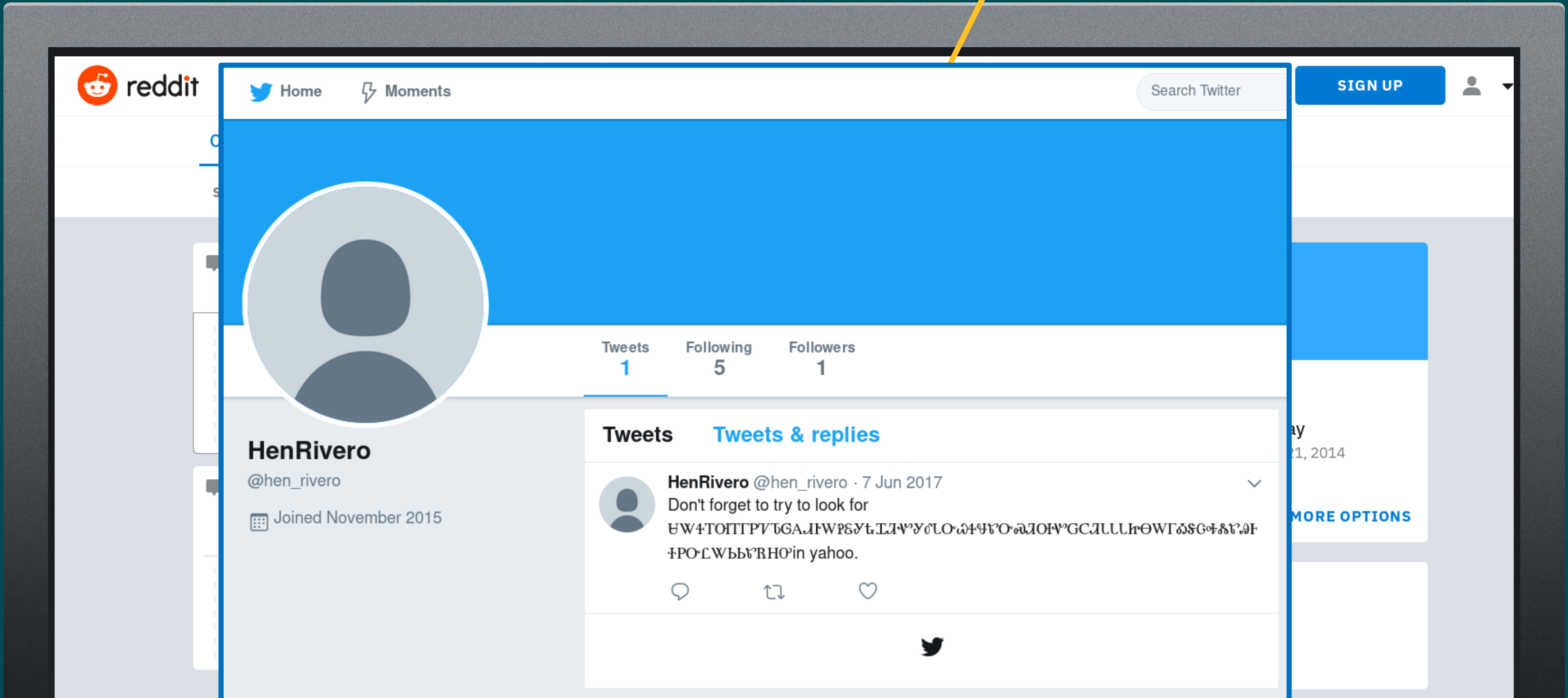
Splitting malware into multiple components

- prevents **behavioral detection**
- leaves some components undetected
- components can run on different devices

Downloading from valid domains like **Imgur, Twitter, Reddit** or **Dropbox** to bypass **URL Filtering** and **Network Anomaly Detection**

STAGE 3

http://www.coachandcook[.]at/error/307-temporary-redirect.php



HenRivero
@hen_rivero
Joined November 2015

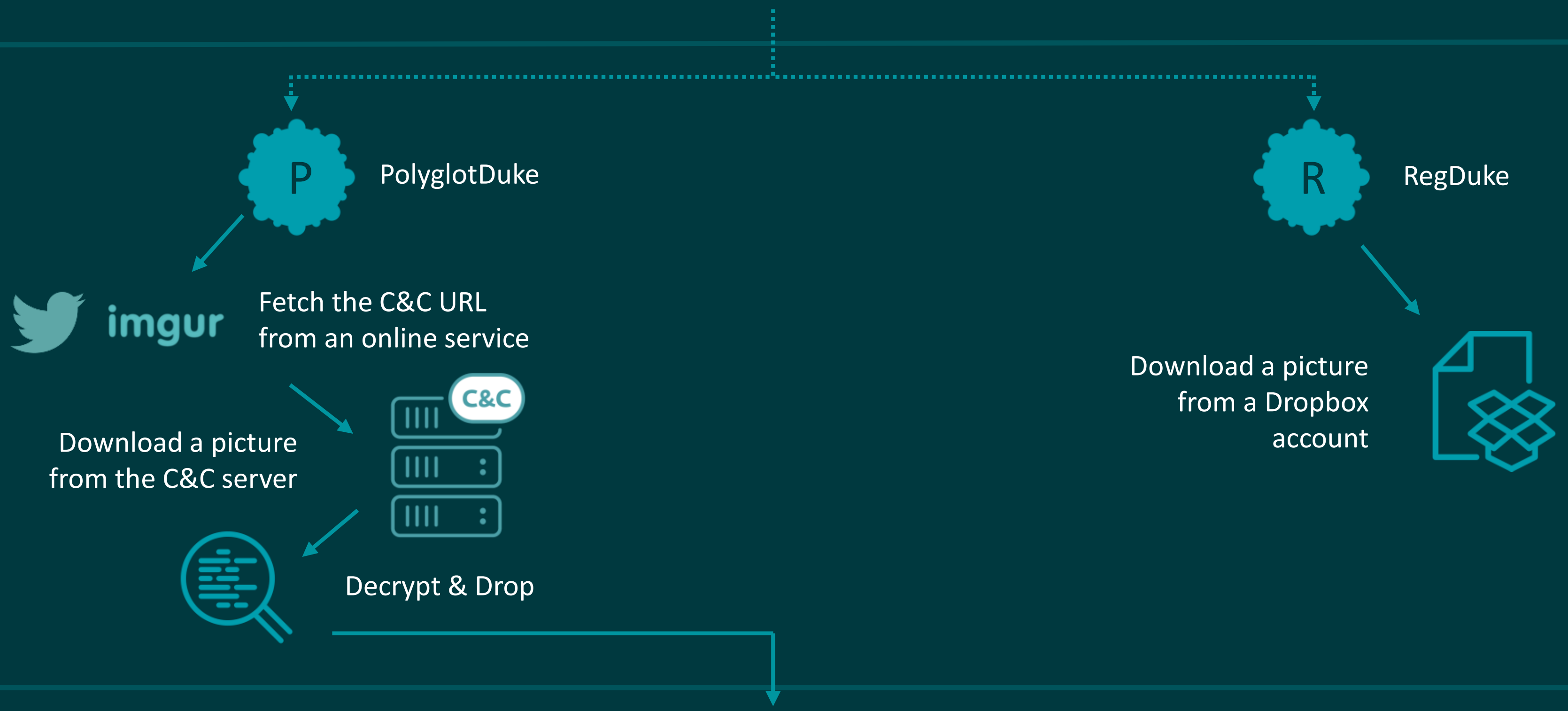
HenRivero @hen_rivero · 7 Jun 2017

Don't forget to try to look for ᏌᎳᏎᎢᏅᎢᎱᏢᏙᏏᏩᎪᏭᏔᏊᏋᏨᏆᎫᏁᎮᏕᏫᏓᏂᏗᏉᎨᏣᏝᏓᎵᎰᏔᎱᏍᏜᏲᏑᏕᏯᏆᏈᏬᏑᏬᏒᏡᏩᏏᏑᏑᏊᎡᎻᎰ in yahoo.

INITIAL COMPROMISE

Malicious document sent by email

Stolen credentials + lateral movement



STAGE 1

PolyglotDuke

Fetch the C&C URL from an online service

Download a picture from the C&C server

Decrypt & Drop

RegDuke

Download a picture from a Dropbox account

STAGE 2

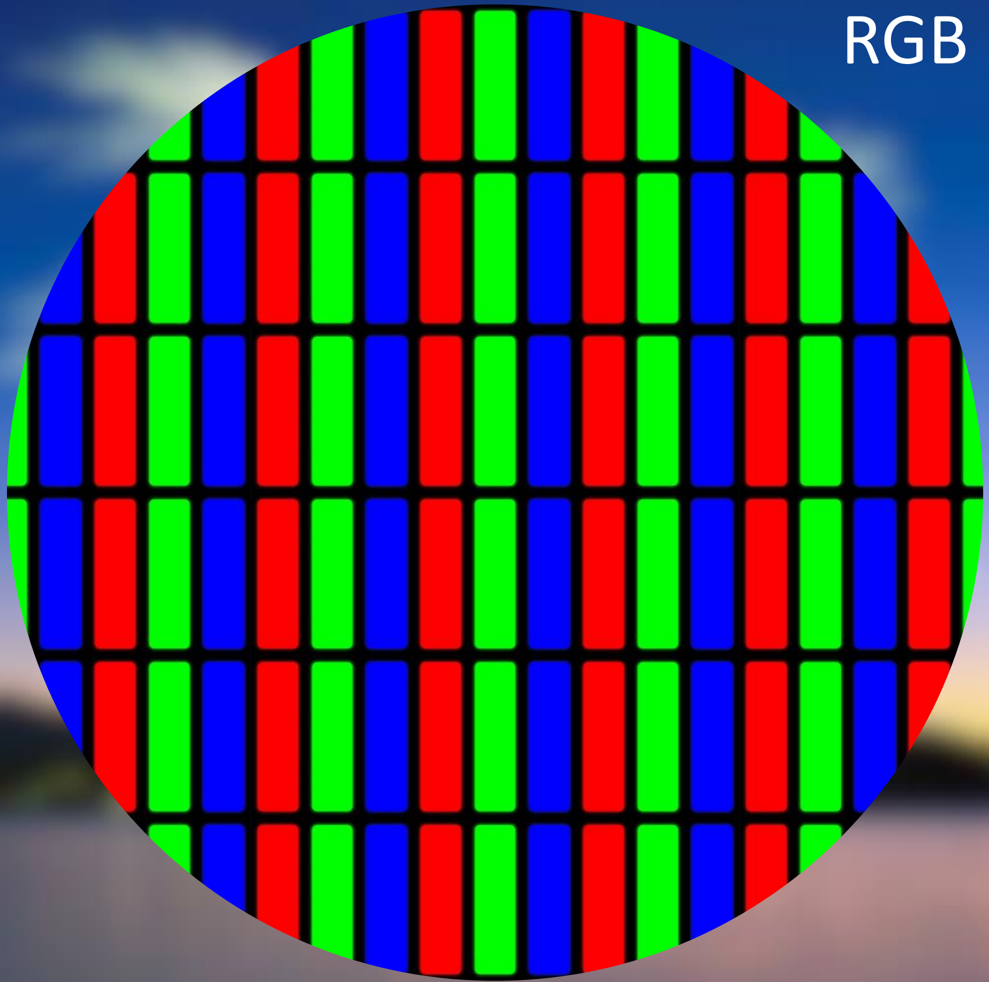
STAGE 3

Hiding 1 byte of data in every pixel

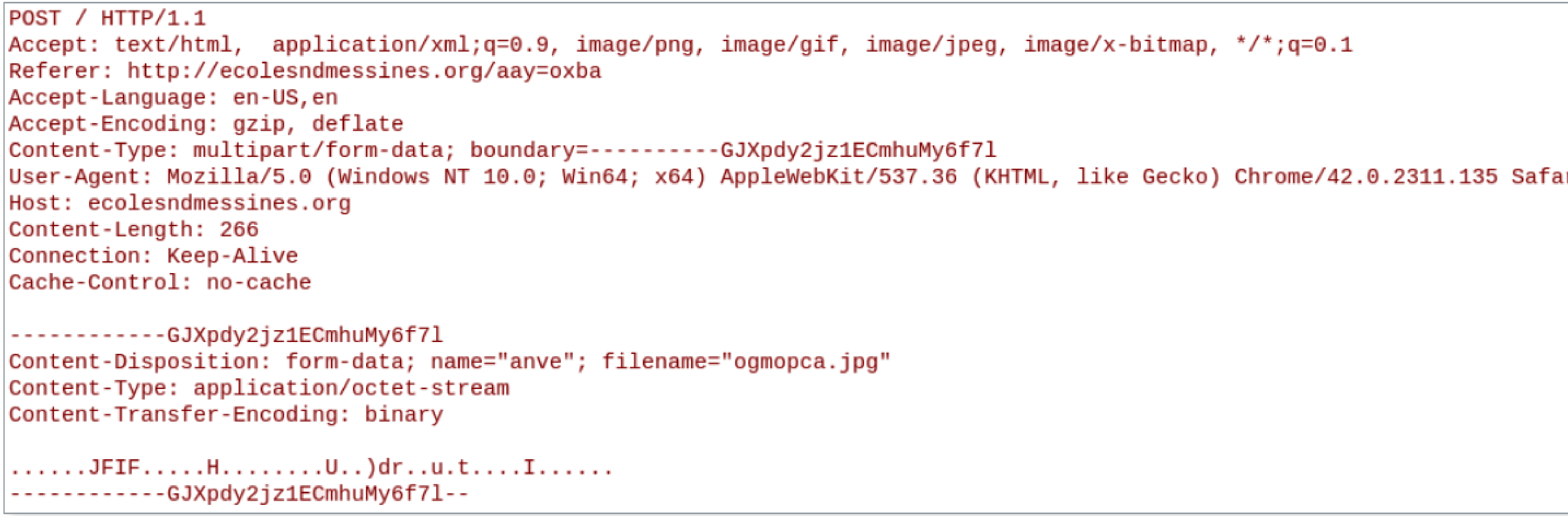
🟥	0	1	0	1	0	1	1	0
🟩	1	1	1	1	0	0	1	0
🟦	0	1	1	1	0	0	0	1

1	0	0	1	0	0	0	1

145



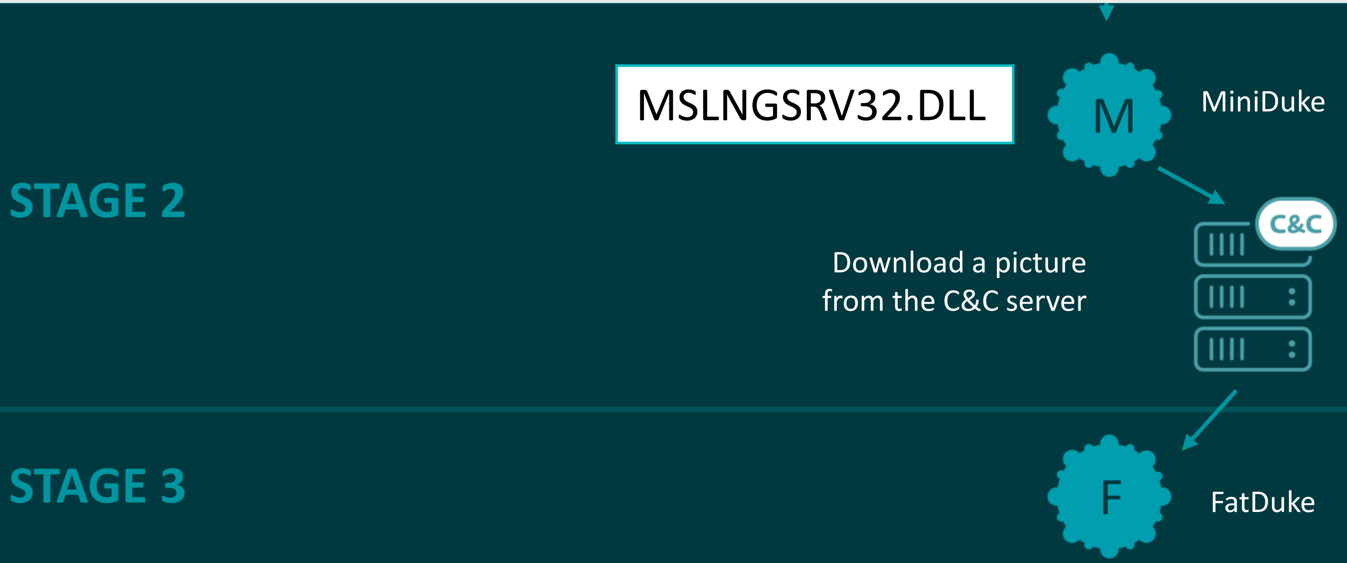
RGB



```
POST / HTTP/1.1
Accept: text/html,  application/xml;q=0.9, image/png, image/gif, image/jpeg, image/x-bitmap, */*;q=0.1
Referer: http://ecolesndmessines.org/aay=oxba
Accept-Language: en-US,en
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----------GJXpdy2jz1ECmhuMy6f7l
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safa
Host: ecolesndmessines.org
Content-Length: 266
Connection: Keep-Alive
Cache-Control: no-cache

------------GJXpdy2jz1ECmhuMy6f7l
Content-Disposition: form-data; name="anve"; filename="ogmopca.jpg"
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary

......JFIF.....H........U..)dr..u.t....I......
------------GJXpdy2jz1ECmhuMy6f7l--
```



Encryption and **steganography** hide malicious content from **network level scanners** (IPS/IDS) and **gateway sandboxes**

MiniDuke backdoor in communication with C&C server uses GET/POST methods with **JPEG header** to avoid **network IPS/IDS**

- Executable has **embedded components and strings from clean apps** to avoid static **machine learning classifiers**

ESET Research White papers // October 2019

OPERATION GHOST

The Dukes aren’t back — they never left

Matthieu Faou
Mathieu Tartare
Thomas Dupuy

Elements of „standard” IT security stack

GRC	Governance, Risk Managment, Compliance
Information & Event Management	SIEM + Threat Intelligence feeds
Data Security	Encryption, DLP
Application Security	Application Control, Patching, DB security
Host Security	Antimalware, Vulnerability Scanning, Exploit Prevention, HIPS
Gateway Security	URL/IP filtering, Email scanning, Sandboxing
Identity & Access	Access Control, 2FA/MFA
Network Security	Firewall, IPS/IDS, Anomaly Detection

Bypassing „standard” IT security stack

GRC	
Information & Event Management	Avoiding monitoring, Uniqueness against TI feeds
Data Security	Use of valid storages (OneDrive, Dropbox)
Application Security	Use of built in tools, Powershell, WMI, DLLs
Host Security	Targeted unique malware, Splitting malware
Gateway Security	Use of valid domains, Use of valid filetypes (gfx, doc)
Identity & Access	Stolen credentials, Lateral movement, Phishing
Network Security	Steganography, Encryption, Imitating packet headers

What's next in making Encrypted DN

Selena Dec

In 20

HTTPS

Firefox

been s

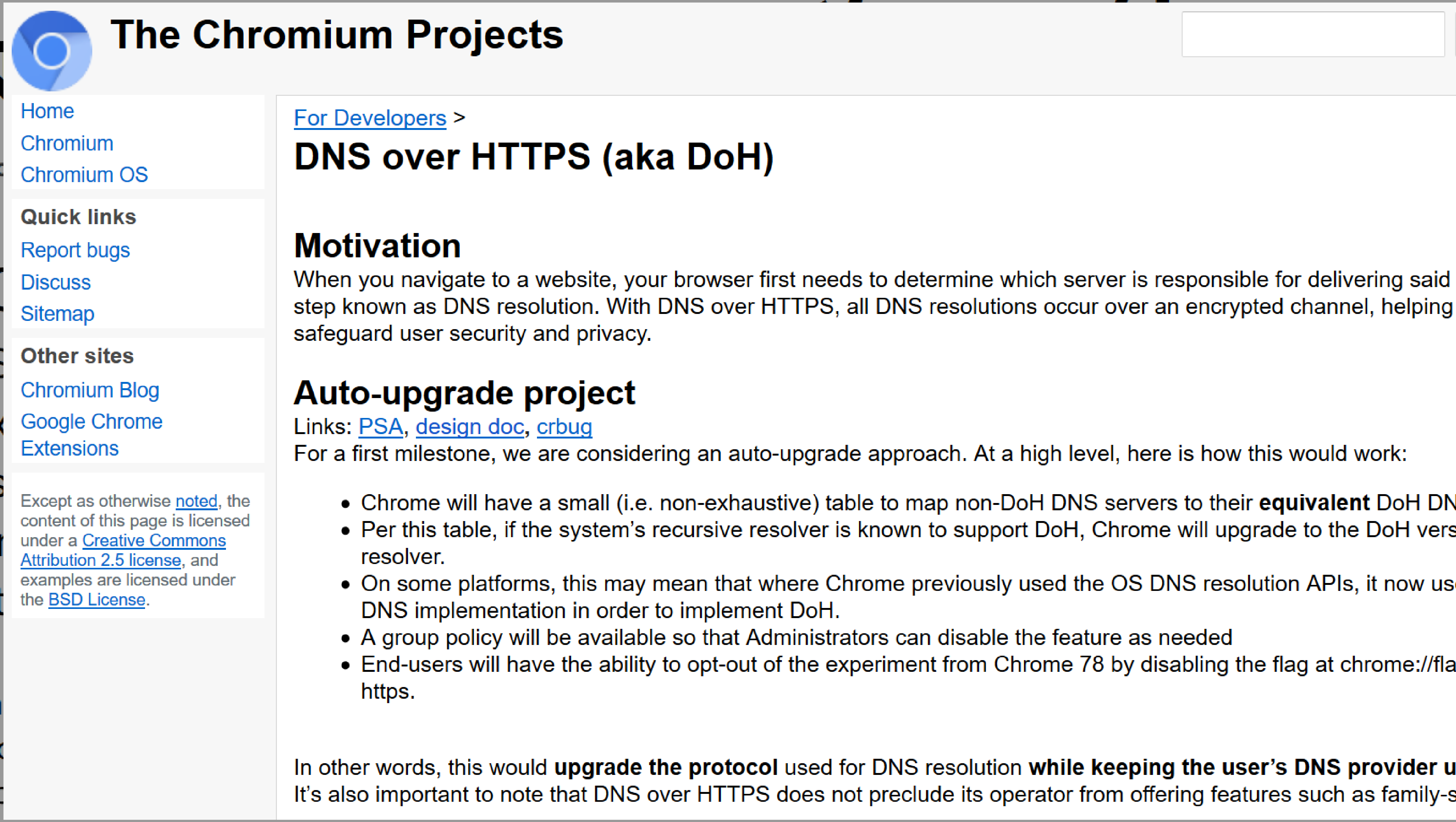
chosen

close t

After ma

that we c

greater p



The Chromium Projects

For Developers >

DNS over HTTPS (aka DoH)

Motivation

When you navigate to a website, your browser first needs to determine which server is responsible for delivering said step known as DNS resolution. With DNS over HTTPS, all DNS resolutions occur over an encrypted channel, helping safeguard user security and privacy.

Auto-upgrade project

Links: PSA, design doc, crbug

For a first milestone, we are considering an auto-upgrade approach. At a high level, here is how this would work:

- Chrome will have a small (i.e. non-exhaustive) table to map non-DoH DNS servers to their **equivalent** DoH DN
- Per this table, if the system's recursive resolver is known to support DoH, Chrome will upgrade to the DoH vers resolver.
- On some platforms, this may mean that where Chrome previously used the OS DNS resolution APIs, it now us DNS implementation in order to implement DoH.
- A group policy will be available so that Administrators can disable the feature as needed
- End-users will have the ability to opt-out of the experiment from Chrome 78 by disabling the flag at chrome://fla https.

In other words, this would **upgrade the protocol** used for DNS resolution **while keeping the user's DNS provider u** It's also important to note that DNS over HTTPS does not preclude its operator from offering features such as family-s

Modern solutions

Endpoint Detection and Response

EDR solution helps you to answer:

Active components

Fileless attacks

Back to the root

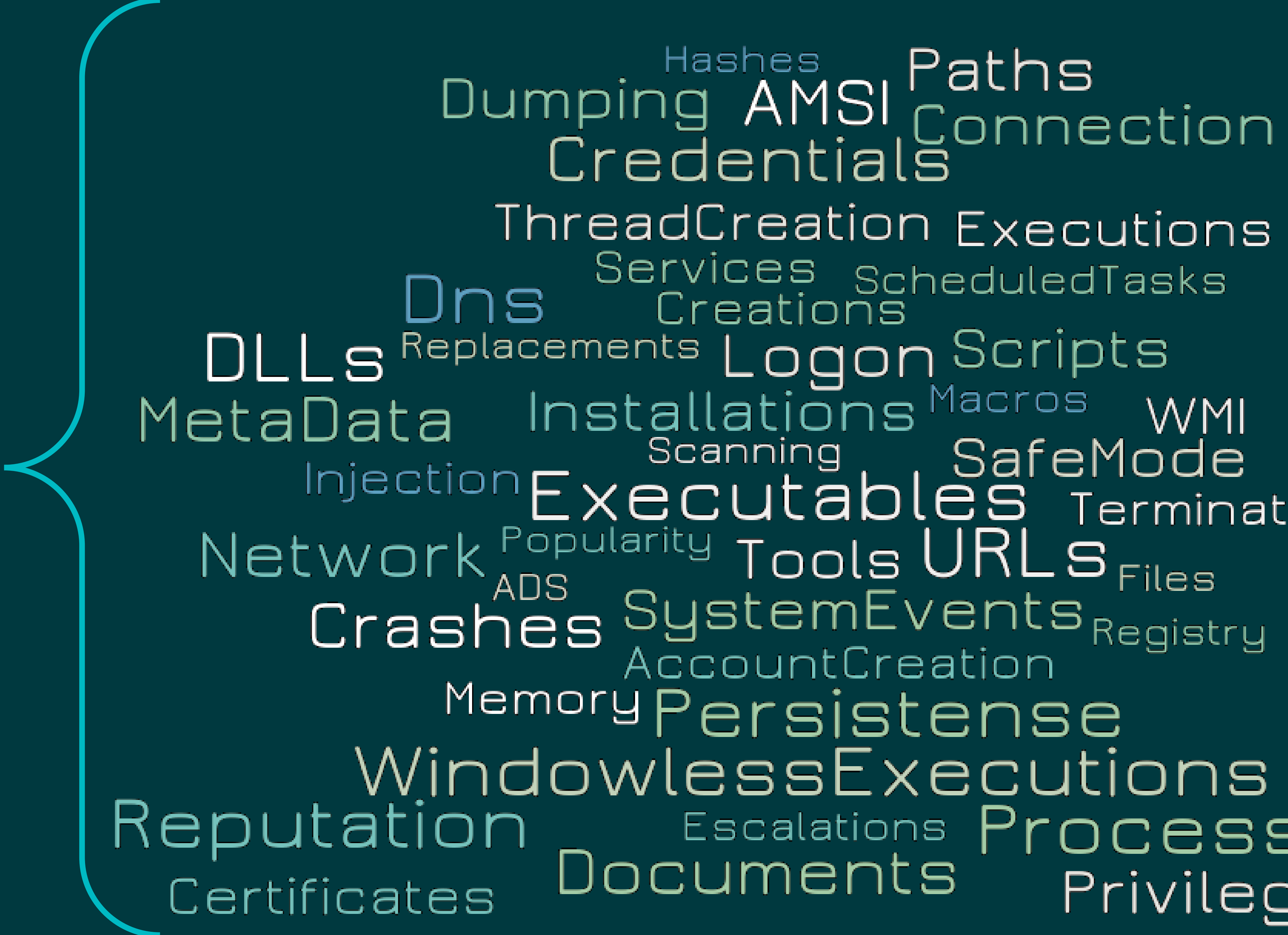
Lateral movement

Data affected

Techniques used

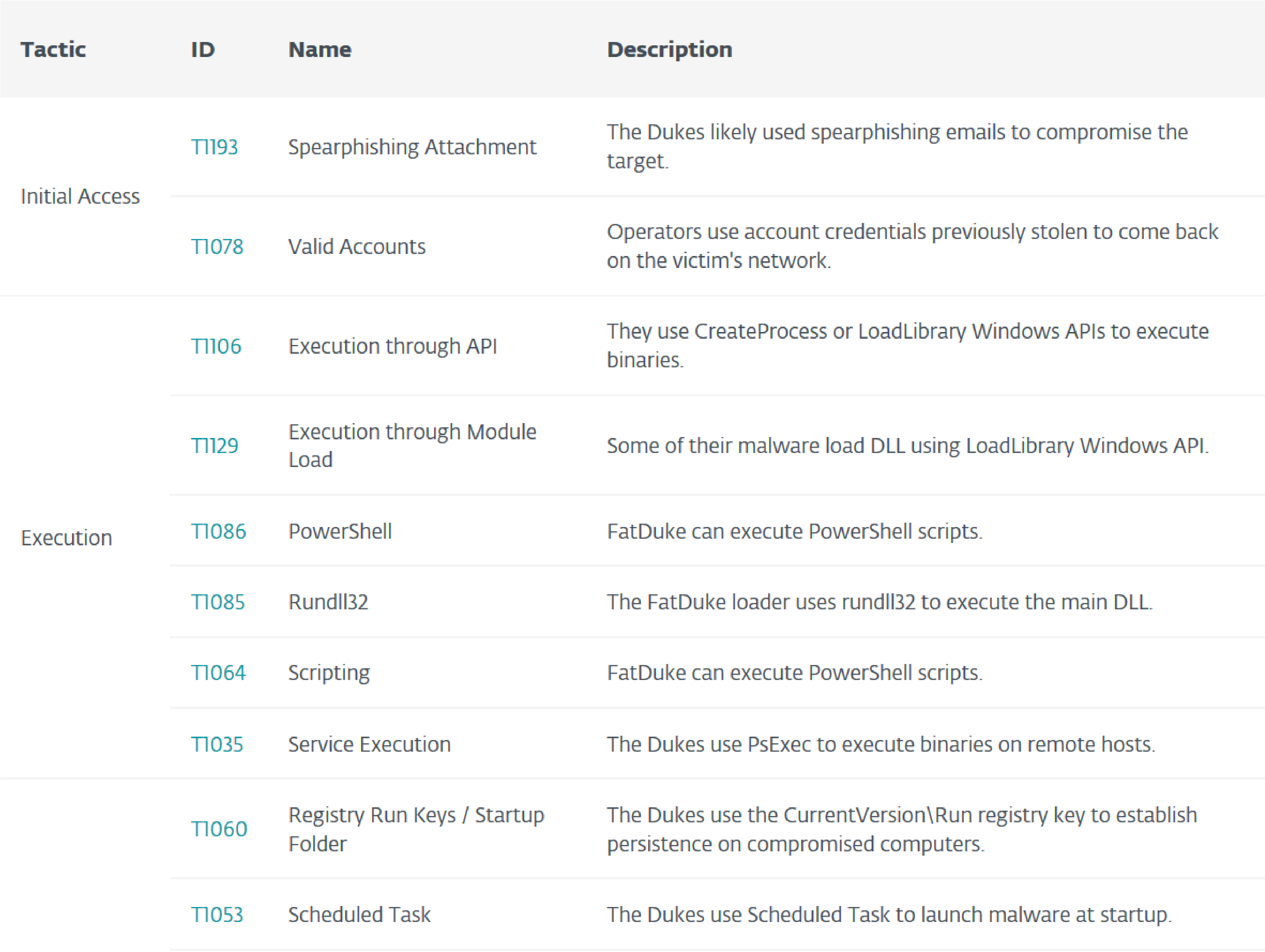
EDR

monitoring
collecting
detecting



EDR base on Indicators of Attack

techniques used by the attacker

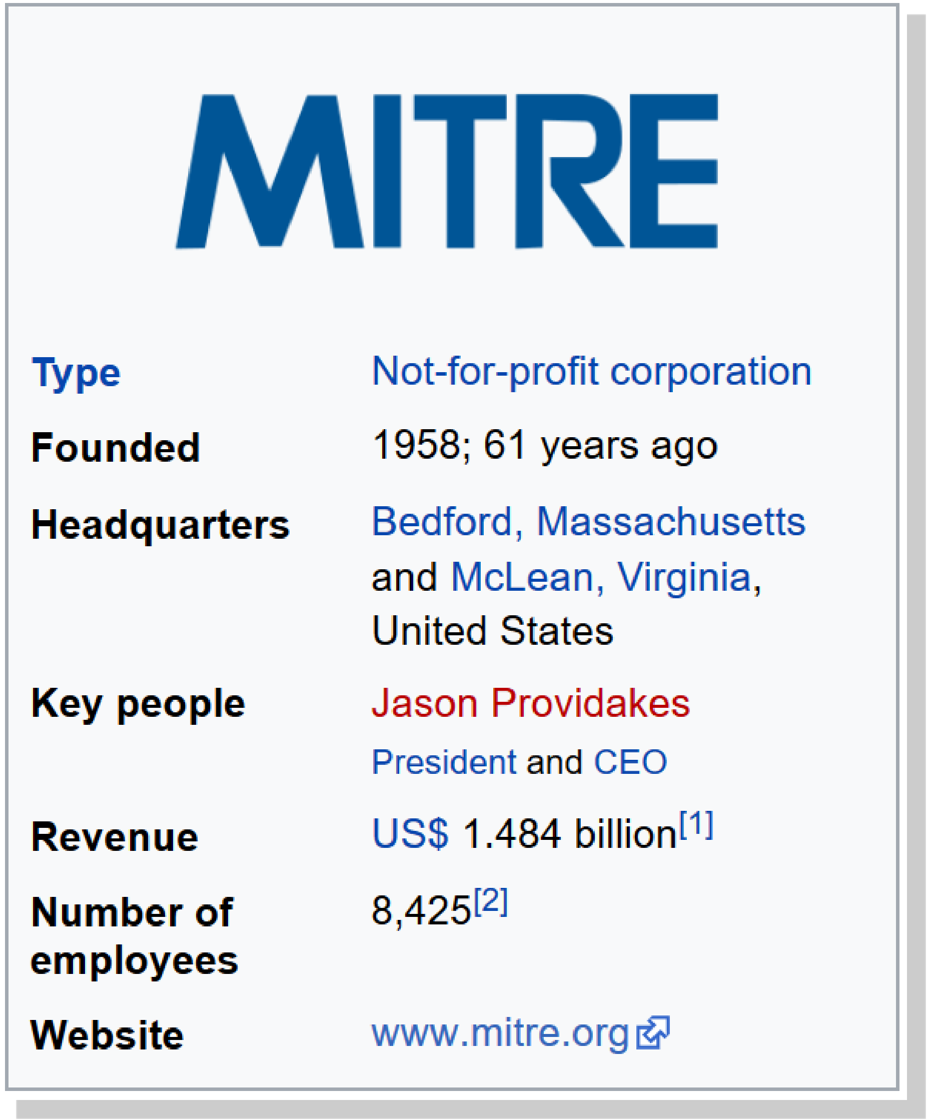


Tactic	ID	Name	Description
Initial Access	T1193	Spearphishing Attachment	The Dukes likely used spearphishing emails to compromise the target.
	T1078	Valid Accounts	Operators use account credentials previously stolen to come back on the victim's network.
Execution	T1106	Execution through API	They use CreateProcess or LoadLibrary Windows APIs to execute binaries.
	T1129	Execution through Module Load	Some of their malware load DLL using LoadLibrary Windows API.
	T1086	PowerShell	FatDuke can execute PowerShell scripts.
	T1085	Rundll32	The FatDuke loader uses rundll32 to execute the main DLL.
	T1064	Scripting	FatDuke can execute PowerShell scripts.
	T1035	Service Execution	The Dukes use PsExec to execute binaries on remote hosts.
	T1060	Registry Run Keys / Startup Folder	The Dukes use the CurrentVersion\Run registry key to establish persistence on compromised computers.
	T1053	Scheduled Task	The Dukes use Scheduled Task to launch malware at startup.

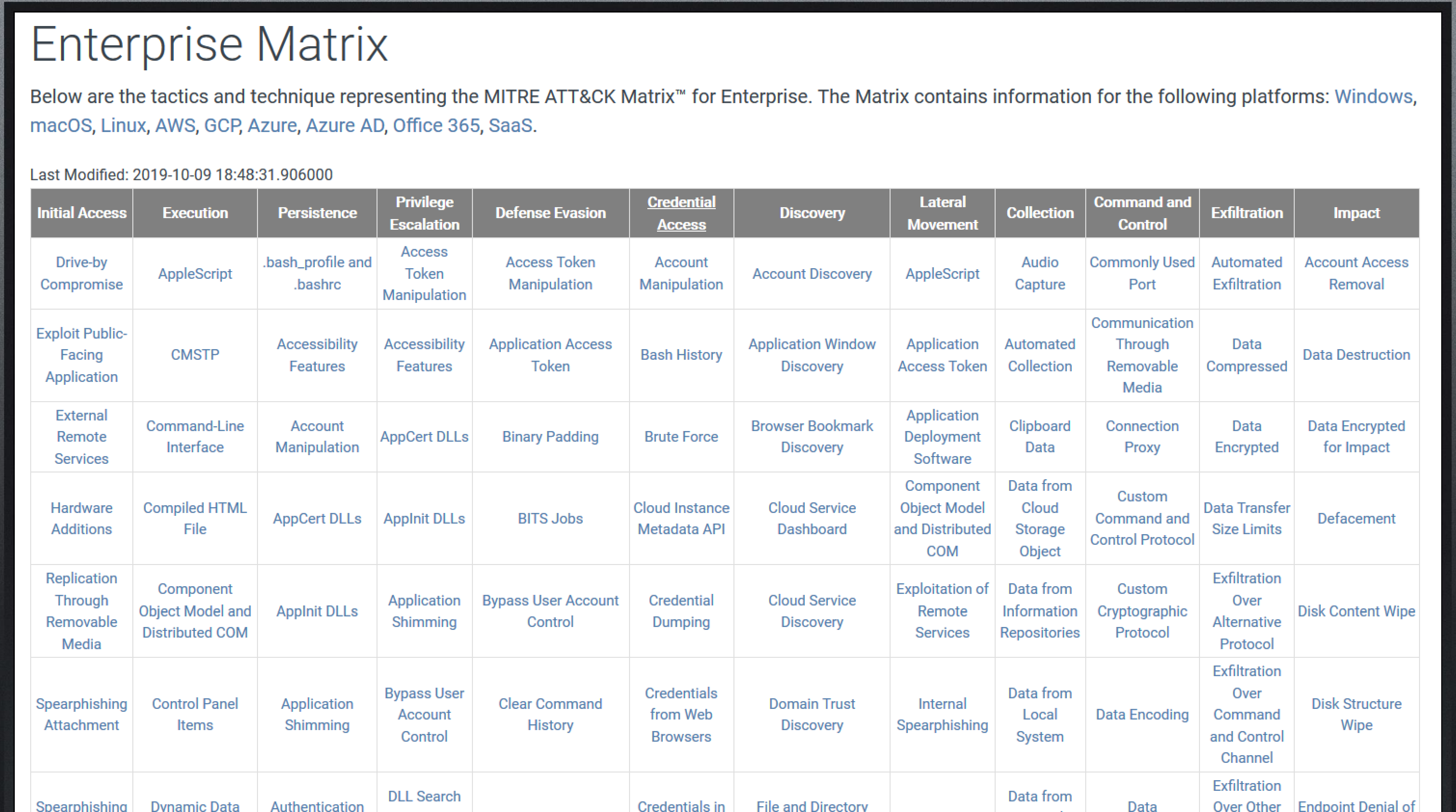
MITRE ATT&CK framework

Adversarial Tactics Techniques and Common Knowledge

What your security stack is able to detect?



Type	Not-for-profit corporation
Founded	1958; 61 years ago
Headquarters	Bedford, Massachusetts and McLean, Virginia, United States
Key people	Jason Providakes President and CEO
Revenue	US$ 1.484 billion[1]
Number of employees	8,425[2]
Website	www.mitre.org

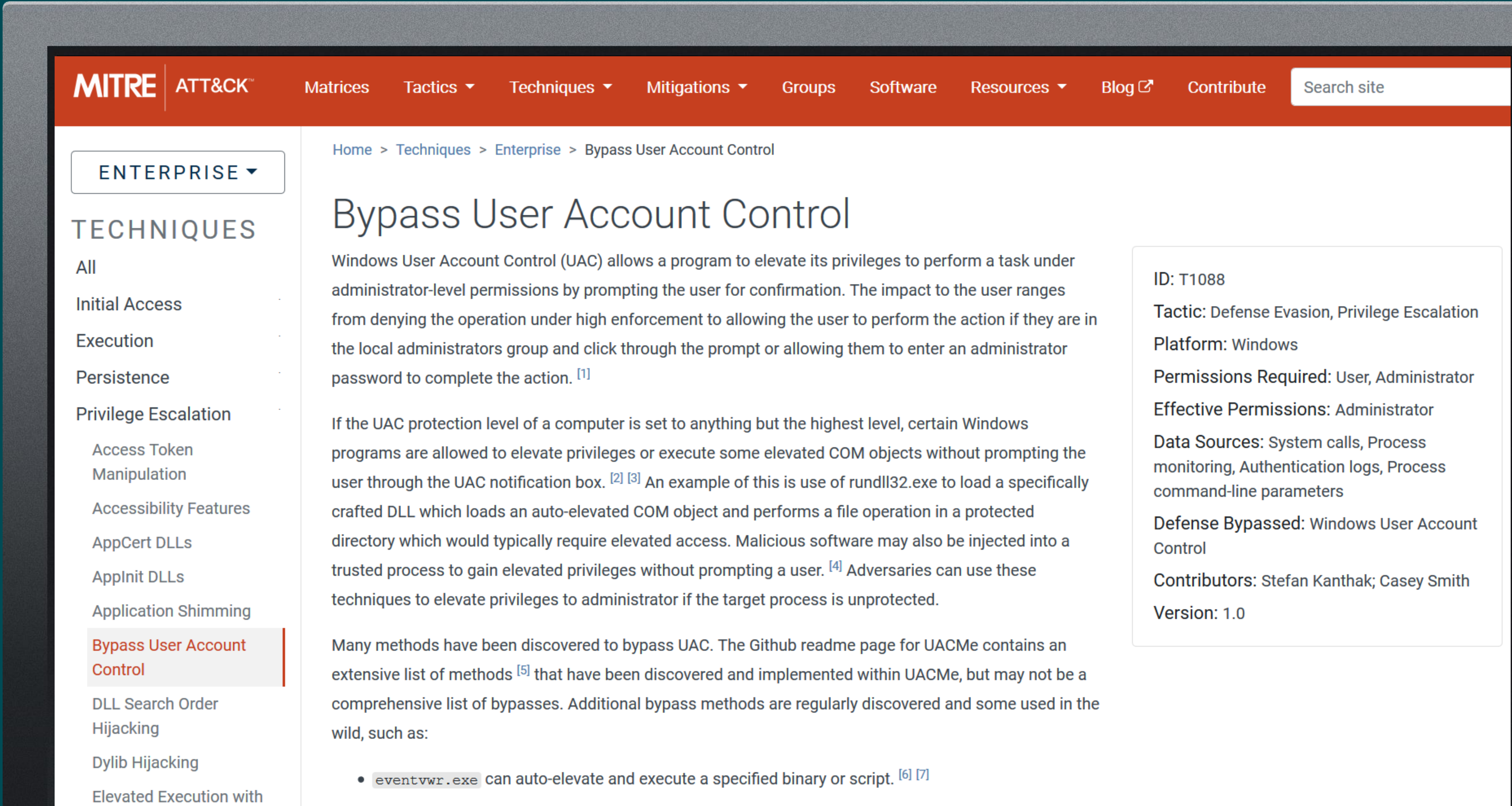


Enterprise Matrix

Below are the tactics and technique representing the MITRE ATT&CK Matrix™ for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS.

Last Modified: 2019-10-09 18:48:31.906000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and Distributed COM	Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Bypass User Account Control	Credential Dumping	Cloud Service Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command History	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing	Dynamic Data	Authentication	DLL Search		Credentials in	File and Directory		Data from	Data	Exfiltration Over Other	Endpoint Denial of



Home > Techniques > Enterprise > Bypass User Account Control

Bypass User Account Control

Windows User Account Control (UAC) allows a program to elevate its privileges to perform a task under administrator-level permissions by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action. [1]

If the UAC protection level of a computer is set to anything but the highest level, certain Windows programs are allowed to elevate privileges or execute some elevated COM objects without prompting the user through the UAC notification box. [2] [3] An example of this is use of rundll32.exe to load a specifically crafted DLL which loads an auto-elevated COM object and performs a file operation in a protected directory which would typically require elevated access. Malicious software may also be injected into a trusted process to gain elevated privileges without prompting a user. [4] Adversaries can use these techniques to elevate privileges to administrator if the target process is unprotected.

Many methods have been discovered to bypass UAC. The Github readme page for UACMe contains an extensive list of methods [5] that have been discovered and implemented within UACMe, but may not be a comprehensive list of bypasses. Additional bypass methods are regularly discovered and some used in the wild, such as:

- `eventvwr.exe` can auto-elevate and execute a specified binary or script. [6] [7]

ID: T1088

Tactic: Defense Evasion, Privilege Escalation

Platform: Windows

Permissions Required: User, Administrator

Effective Permissions: Administrator

Data Sources: System calls, Process monitoring, Authentication logs, Process command-line parameters

Defense Bypassed: Windows User Account Control

Contributors: Stefan Kanthak; Casey Smith

Version: 1.0

How can you check your security stack? (or EDR solution)

Open source and paid „attack simulation” tools

MITRE CALDERA

Infection Monkey
powered by Guardicore

PRAETORIAN

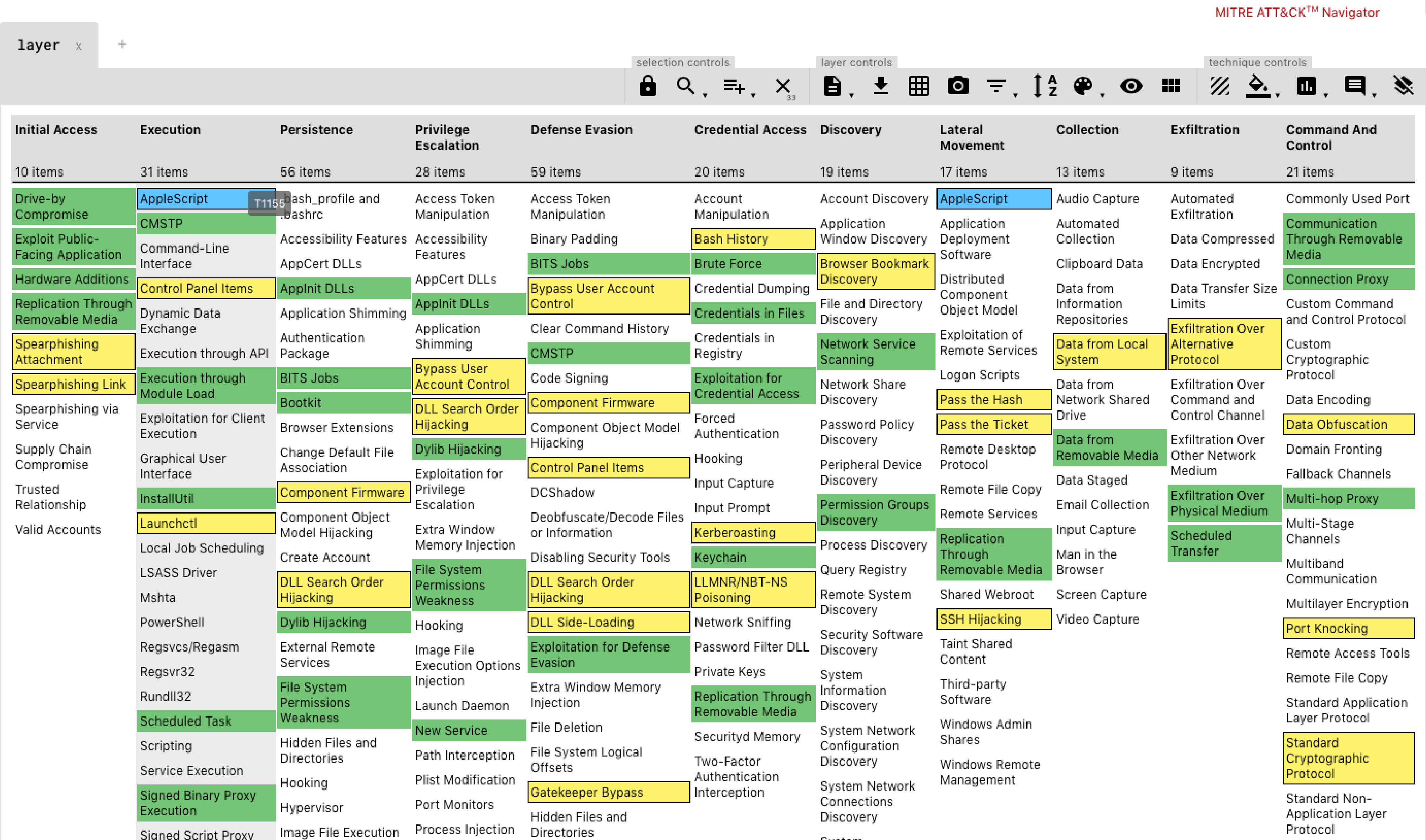
RTA
Red Team Automation

Atomic Red Team

CYMULATE
BREACH & ATTACK SIMULATION

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

COVENANT



Initial Access

10 items

- Drive-by Compromise
- Exploit Public-Facing Application
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution

31 items

- AppleScript
- CMSTP
- Command-Line Interface
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- Launchctl
- Local Job Scheduling
- LSASS Driver
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Scheduled Task
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script Proxy

Persistence

56 items

- .bash_profile and .bashrc
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Component Firmware
- Component Object Model Hijacking
- Create Account
- DLL Search Order Hijacking
- Dylib Hijacking
- External Remote Services
- File System Permissions Weakness
- Hidden Files and Directories
- Hooking
- Hypervisor
- Image File Execution

Privilege Escalation

28 items

- Access Token Manipulation
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Bypass User Account Control
- DLL Search Order Hijacking
- Dylib Hijacking
- Exploitation for Privilege Escalation
- Extra Window Memory Injection
- File System Permissions Weakness
- Hooking
- Image File Execution Options Injection
- Launch Daemon
- New Service
- Path Interception
- Plist Modification
- Port Monitors
- Process Injection

Defense Evasion

59 items

- Access Token Manipulation
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- Clear Command History
- CMSTP
- Code Signing
- Component Firmware
- Component Object Model Hijacking
- Control Panel Items
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- DLL Search Order Hijacking
- DLL Side-Loading
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File Deletion
- File System Logical Offsets
- Gatekeeper Bypass
- Hidden Files and Directories

Credential Access

20 items

- Account Manipulation
- Bash History
- Brute Force
- Credential Dumping
- Credentials in Files
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Input Capture
- Input Prompt
- Kerberoasting
- Keychain
- LLMNR/NBT-NS Poisoning
- Network Sniffing
- Password Filter DLL
- Private Keys
- Replication Through Removable Media
- Securityd Memory
- Two-Factor Authentication Interception

Discovery

19 items

- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System

Lateral Movement

17 items

- AppleScript
- Application Deployment Software
- Distributed Component Object Model
- Exploitation of Remote Services
- Logon Scripts
- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol
- Remote File Copy
- Remote Services
- Replication Through Removable Media
- Shared Webroot
- SSH Hijacking
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- Windows Remote Management

Collection

13 items

- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Man in the Browser
- Screen Capture
- Video Capture

Exfiltration

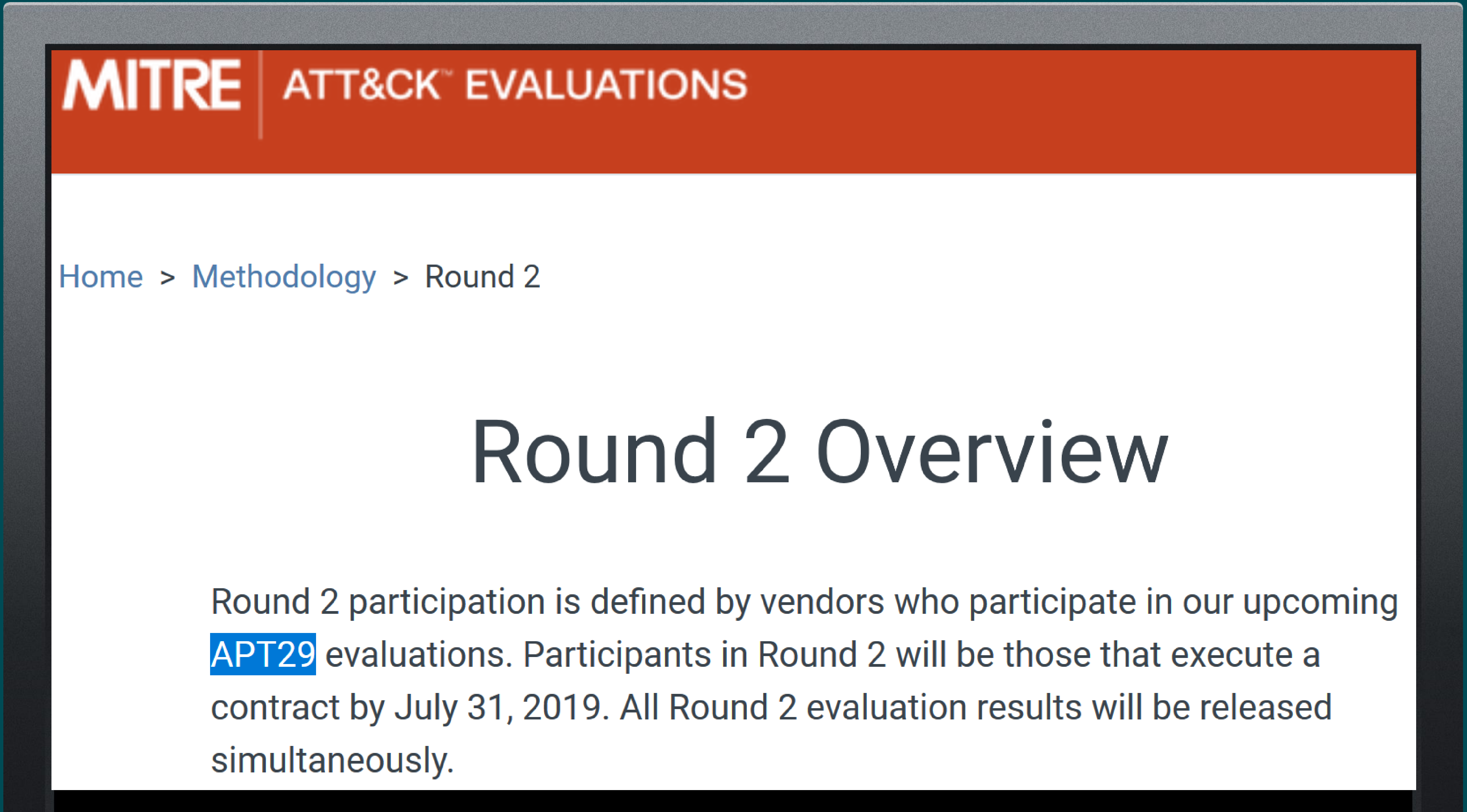
9 items

- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Scheduled Transfer

Command And Control

21 items

- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Fallback Channels
- Multi-hop Proxy
- Multi-Stage Channels
- Multiband Communication
- Multilayer Encryption
- Port Knocking
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol



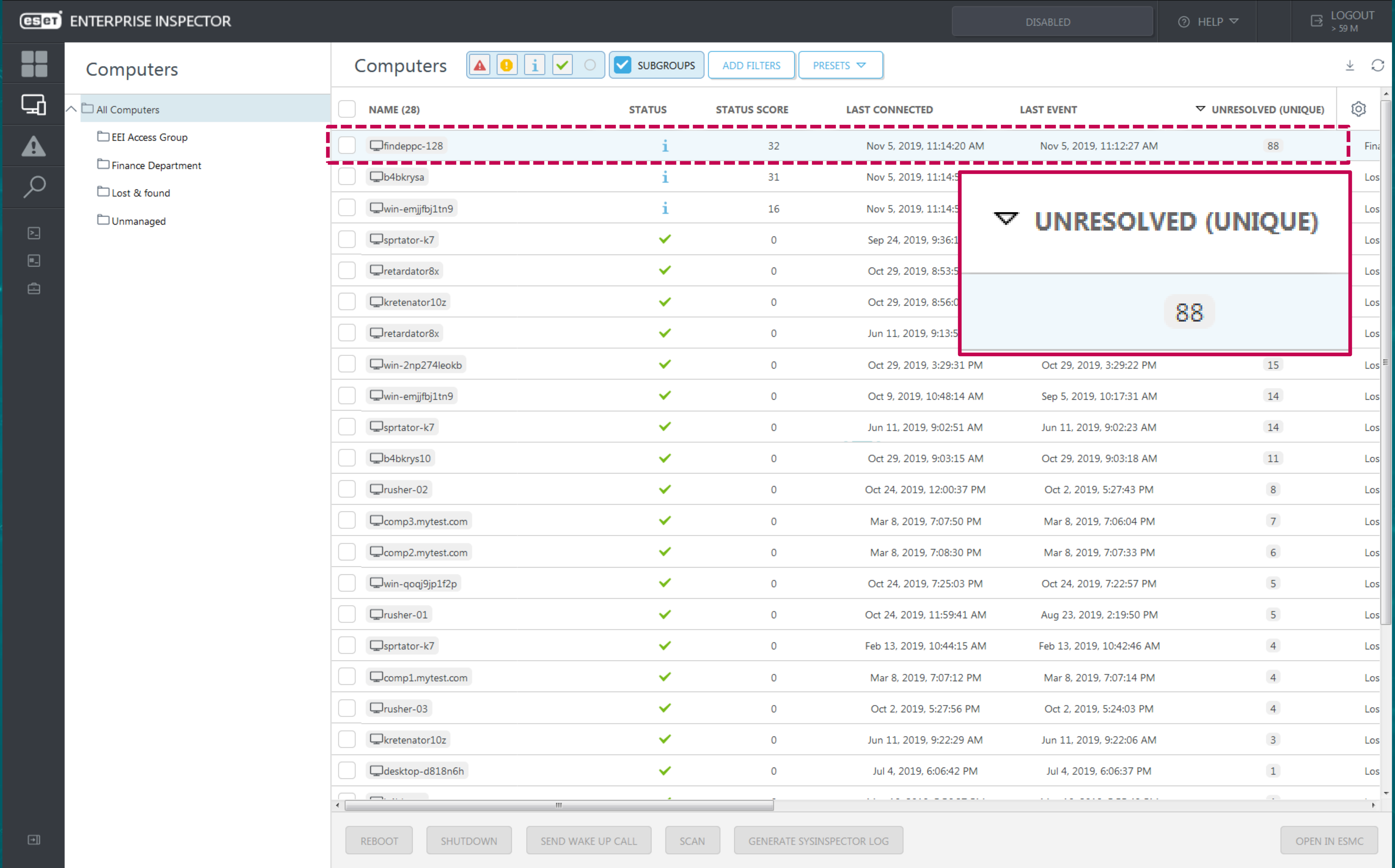
Round 2 Overview

Round 2 participation is defined by vendors who participate in our upcoming APT29 evaluations. Participants in Round 2 will be those that execute a contract by July 31, 2019. All Round 2 evaluation results will be released simultaneously.

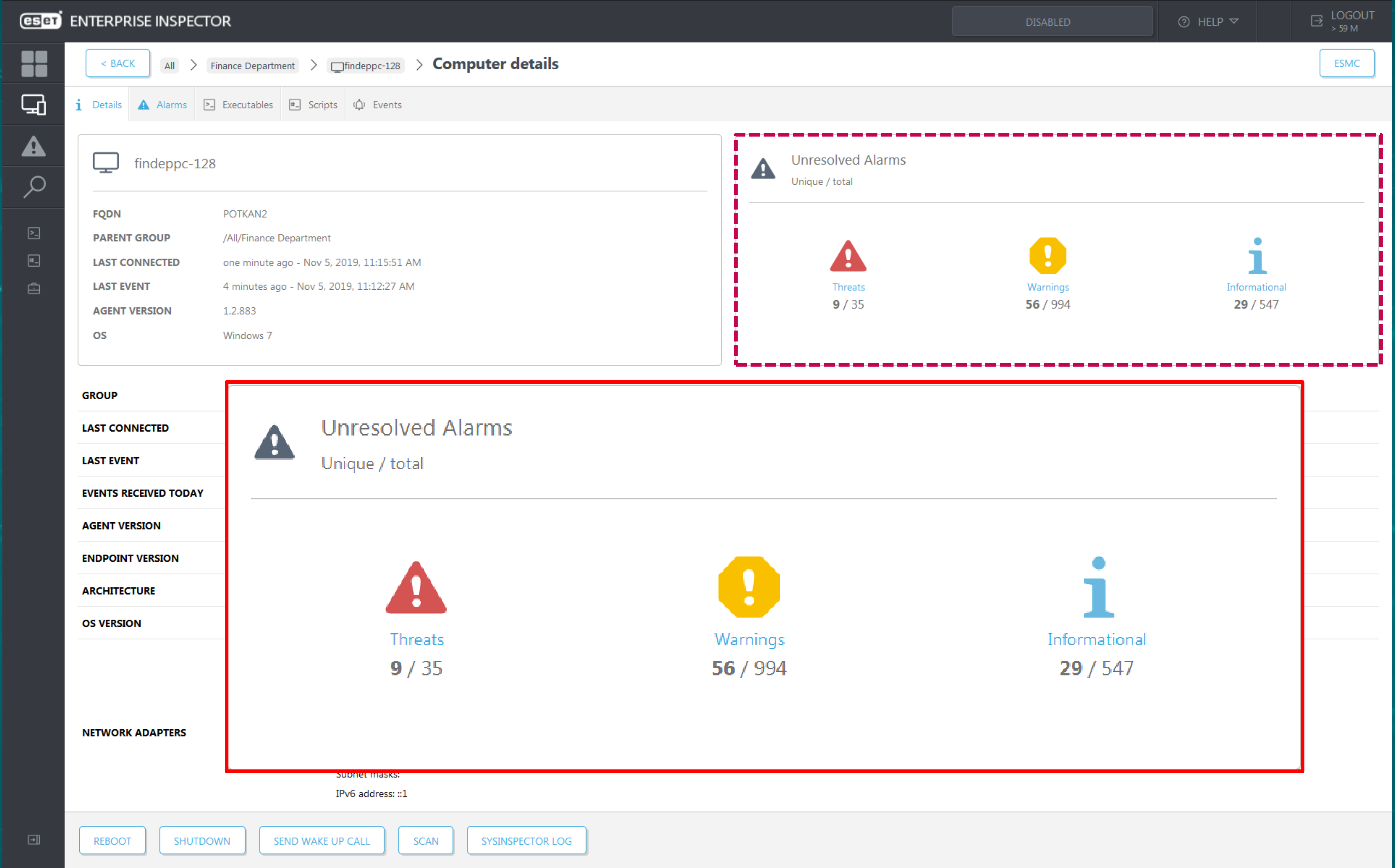
Operation Ghost/APT29 in **ESET Enterprise Inspector**

Initial Compromise

Targeted Email + Word Document + Dropper



NAME (28)	STATUS	STATUS SCORE	LAST CONNECTED	LAST EVENT	UNRESOLVED (UNIQUE)	
findeppc-128	i	32	Nov 5, 2019, 11:14:20 AM	Nov 5, 2019, 11:12:27 AM	88	Fina
b4bkrysa	i	31	Nov 5, 2019, 11:14:5			Los
win-emjjfbj1tn9	i	16	Nov 5, 2019, 11:14:5			Los
sprtator-k7	✓	0	Sep 24, 2019, 9:36:1			Los
retardator8x	✓	0	Oct 29, 2019, 8:53:5			Los
kretenator10z	✓	0	Oct 29, 2019, 8:56:0			Los
retardator8x	✓	0	Jun 11, 2019, 9:13:5			Los
win-2np274leokb	✓	0	Oct 29, 2019, 3:29:31 PM	Oct 29, 2019, 3:29:22 PM	15	Los
win-emjjfbj1tn9	✓	0	Oct 9, 2019, 10:48:14 AM	Sep 5, 2019, 10:17:31 AM	14	Los
sprtator-k7	✓	0	Jun 11, 2019, 9:02:51 AM	Jun 11, 2019, 9:02:23 AM	14	Los
b4bkrys10	✓	0	Oct 29, 2019, 9:03:15 AM	Oct 29, 2019, 9:03:18 AM	11	Los
rusher-02	✓	0	Oct 24, 2019, 12:00:37 PM	Oct 2, 2019, 5:27:43 PM	8	Los
comp3.mytest.com	✓	0	Mar 8, 2019, 7:07:50 PM	Mar 8, 2019, 7:06:04 PM	7	Los
comp2.mytest.com	✓	0	Mar 8, 2019, 7:08:30 PM	Mar 8, 2019, 7:07:33 PM	6	Los
win-qoqj9jp1f2p	✓	0	Oct 24, 2019, 7:25:03 PM	Oct 24, 2019, 7:22:57 PM	5	Los
rusher-01	✓	0	Oct 24, 2019, 11:59:41 AM	Aug 23, 2019, 2:19:50 PM	5	Los
sprtator-k7	✓	0	Feb 13, 2019, 10:44:15 AM	Feb 13, 2019, 10:42:46 AM	4	Los
comp1.mytest.com	✓	0	Mar 8, 2019, 7:07:12 PM	Mar 8, 2019, 7:07:14 PM	4	Los
rusher-03	✓	0	Oct 2, 2019, 5:27:56 PM	Oct 2, 2019, 5:24:03 PM	4	Los
kretenator10z	✓	0	Jun 11, 2019, 9:22:29 AM	Jun 11, 2019, 9:22:06 AM	3	Los
desktop-d818n6h	✓	0	Jul 4, 2019, 6:06:42 PM	Jul 4, 2019, 6:06:37 PM	1	Los



Computer details

findeppc-128

FQDN POTKAN2
PARENT GROUP /All/Finance Department
LAST CONNECTED one minute ago - Nov 5, 2019, 11:15:51 AM
LAST EVENT 4 minutes ago - Nov 5, 2019, 11:12:27 AM
AGENT VERSION 1.2.883
OS Windows 7

Unresolved Alarms
Unique / total

Threats
9 / 35

Warnings
56 / 994

Informational
29 / 547

GROUP
LAST CONNECTED
LAST EVENT
EVENTS RECEIVED TODAY
AGENT VERSION
ENDPOINT VERSION
ARCHITECTURE
OS VERSION
NETWORK ADAPTERS

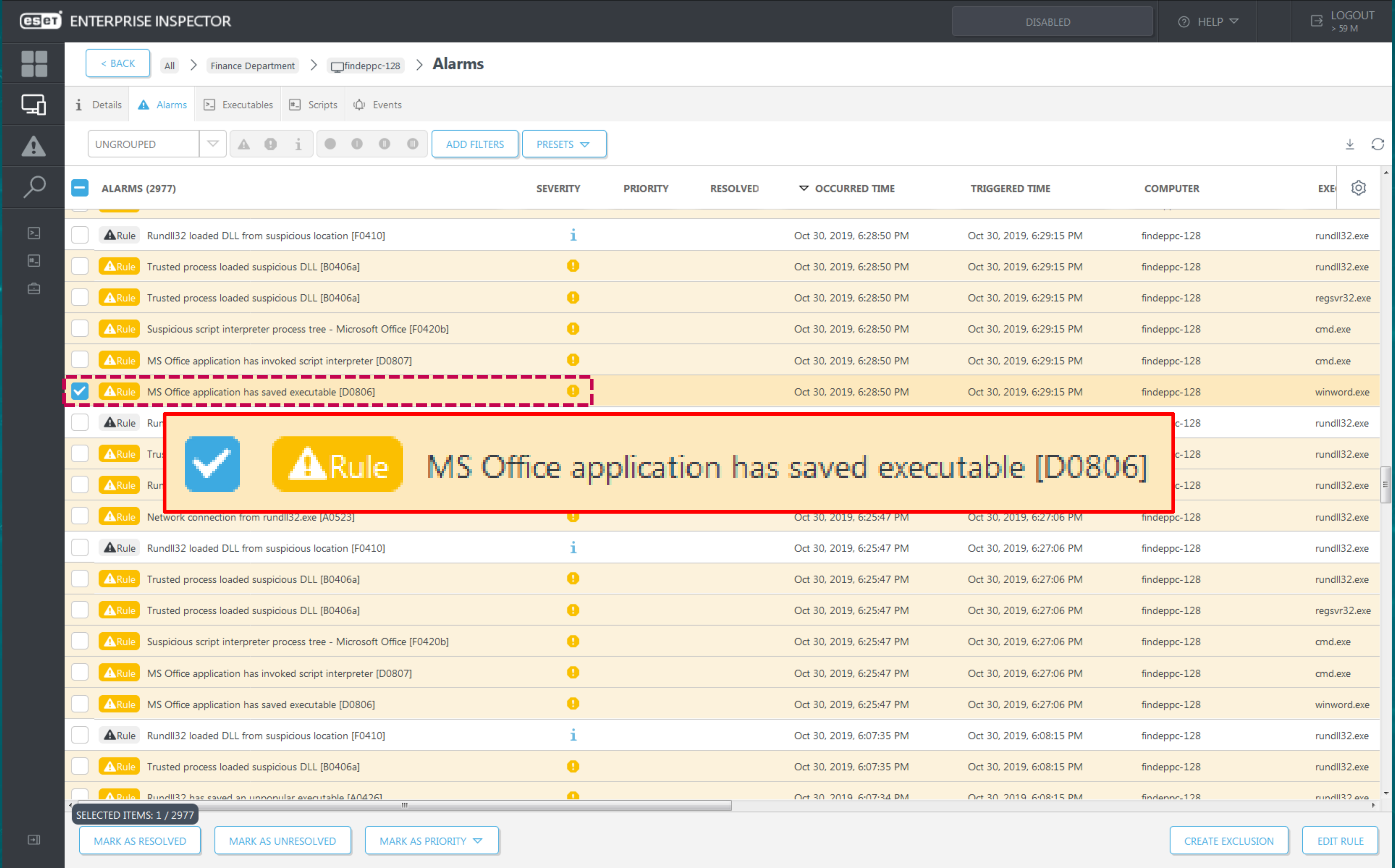
Subnet masks:
IPv6 address: ::1

Unresolved Alarms
Unique / total

Threats
9 / 35

Warnings
56 / 994

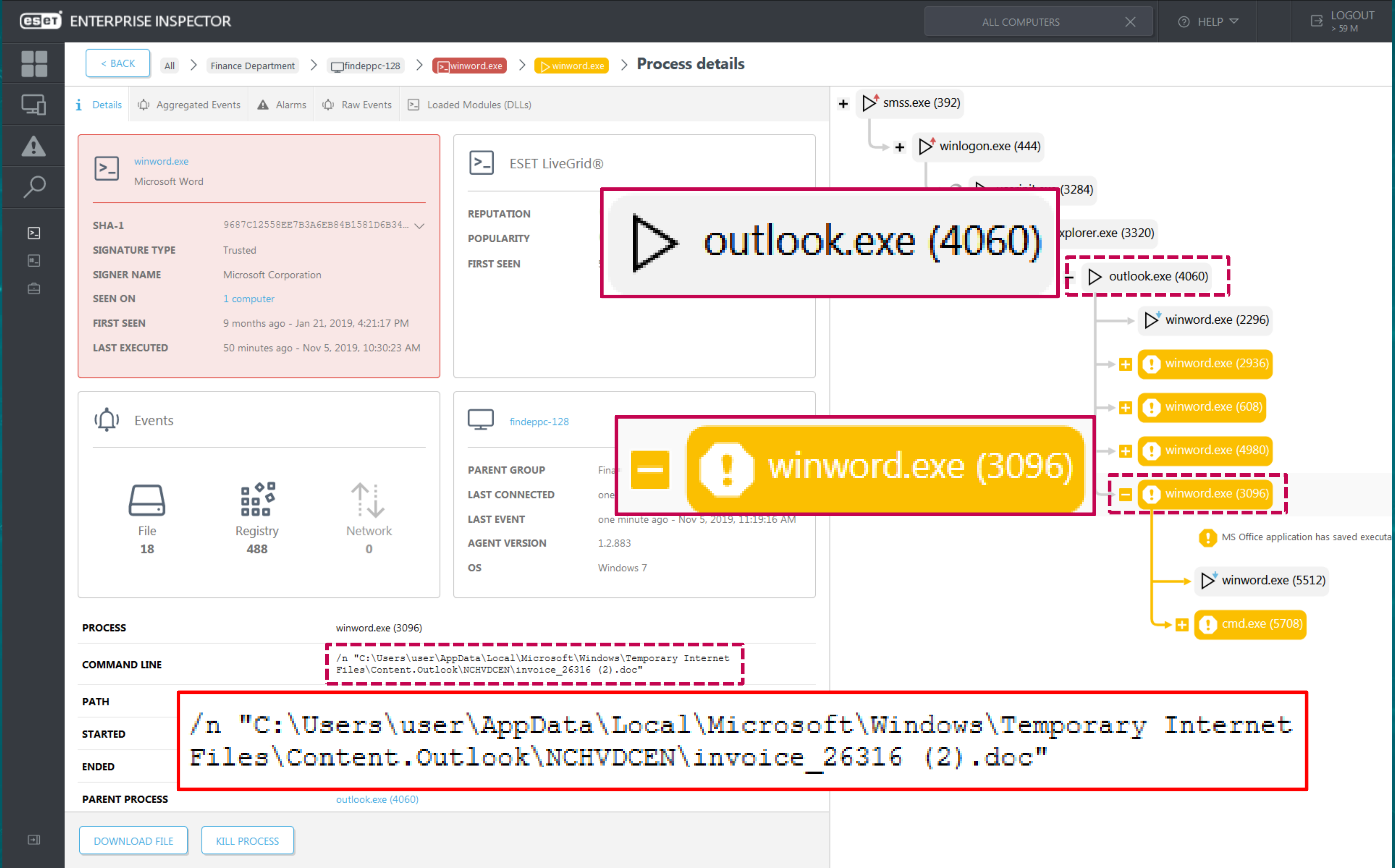
Informational
29 / 547



☐	ALARMS (2977)	SEVERITY	PRIORITY	RESOLVED	OCCURRED TIME	TRIGGERED TIME	COMPUTER	EXE
☐	Rule Rundll32 loaded DLL from suspicious location [F0410]	i			Oct 30, 2019, 6:28:50 PM	Oct 30, 2019, 6:29:15 PM	findeppc-128	rundll32.exe
☐	Rule Trusted process loaded suspicious DLL [B0406a]	!			Oct 30, 2019, 6:28:50 PM	Oct 30, 2019, 6:29:15 PM	findeppc-128	rundll32.exe
☐	Rule Trusted process loaded suspicious DLL [B0406a]	!			Oct 30, 2019, 6:28:50 PM	Oct 30, 2019, 6:29:15 PM	findeppc-128	regsvr32.exe
☐	Rule Suspicious script interpreter process tree - Microsoft Office [F0420b]	!			Oct 30, 2019, 6:28:50 PM	Oct 30, 2019, 6:29:15 PM	findeppc-128	cmd.exe
☐	Rule MS Office application has invoked script interpreter [D0807]	!			Oct 30, 2019, 6:28:50 PM	Oct 30, 2019, 6:29:15 PM	findeppc-128	cmd.exe
☑	Rule MS Office application has saved executable [D0806]	!			Oct 30, 2019, 6:28:50 PM	Oct 30, 2019, 6:29:15 PM	findeppc-128	winword.exe
☐	Rule Run						-128	rundll32.exe
☐	Rule Tru						-128	rundll32.exe
☐	Rule Run						-128	rundll32.exe
☐	Rule Network connection from rundll32.exe [A0523]	!			Oct 30, 2019, 6:25:47 PM	Oct 30, 2019, 6:27:06 PM	findeppc-128	rundll32.exe
☐	Rule Rundll32 loaded DLL from suspicious location [F0410]	i			Oct 30, 2019, 6:25:47 PM	Oct 30, 2019, 6:27:06 PM	findeppc-128	rundll32.exe
☐	Rule Trusted process loaded suspicious DLL [B0406a]	!			Oct 30, 2019, 6:25:47 PM	Oct 30, 2019, 6:27:06 PM	findeppc-128	rundll32.exe
☐	Rule Trusted process loaded suspicious DLL [B0406a]	!			Oct 30, 2019, 6:25:47 PM	Oct 30, 2019, 6:27:06 PM	findeppc-128	regsvr32.exe
☐	Rule Suspicious script interpreter process tree - Microsoft Office [F0420b]	!			Oct 30, 2019, 6:25:47 PM	Oct 30, 2019, 6:27:06 PM	findeppc-128	cmd.exe
☐	Rule MS Office application has invoked script interpreter [D0807]	!			Oct 30, 2019, 6:25:47 PM	Oct 30, 2019, 6:27:06 PM	findeppc-128	cmd.exe
☐	Rule MS Office application has saved executable [D0806]	!			Oct 30, 2019, 6:25:47 PM	Oct 30, 2019, 6:27:06 PM	findeppc-128	winword.exe
☐	Rule Rundll32 loaded DLL from suspicious location [F0410]	i			Oct 30, 2019, 6:07:35 PM	Oct 30, 2019, 6:08:15 PM	findeppc-128	rundll32.exe
☐	Rule Trusted process loaded suspicious DLL [B0406a]	!			Oct 30, 2019, 6:07:35 PM	Oct 30, 2019, 6:08:15 PM	findeppc-128	rundll32.exe
☐	Rule Rundll32 has saved an unpopular executable [A0426]	!			Oct 30, 2019, 6:07:34 PM	Oct 30, 2019, 6:08:15 PM	findeppc-128	rundll32.exe

☑ Rule MS Office application has saved executable [D0806]

SELECTED ITEMS: 1 / 2977



Process details

winword.exe
Microsoft Word

SHA-1	9687C12558EE7B3A6EB84B1581D6B34...
SIGNATURE TYPE	Trusted
SIGNER NAME	Microsoft Corporation
SEEN ON	1 computer
FIRST SEEN	9 months ago - Jan 21, 2019, 4:21:17 PM
LAST EXECUTED	50 minutes ago - Nov 5, 2019, 10:30:23 AM

ESET LiveGrid®

REPUTATION
POPULARITY
FIRST SEEN

Events

File	Registry	Network
18	488	0

findeppc-128

PARENT GROUP	Fina
LAST CONNECTED	one
LAST EVENT	one minute ago - Nov 5, 2019, 11:19:16 AM
AGENT VERSION	1.2.883
OS	Windows 7

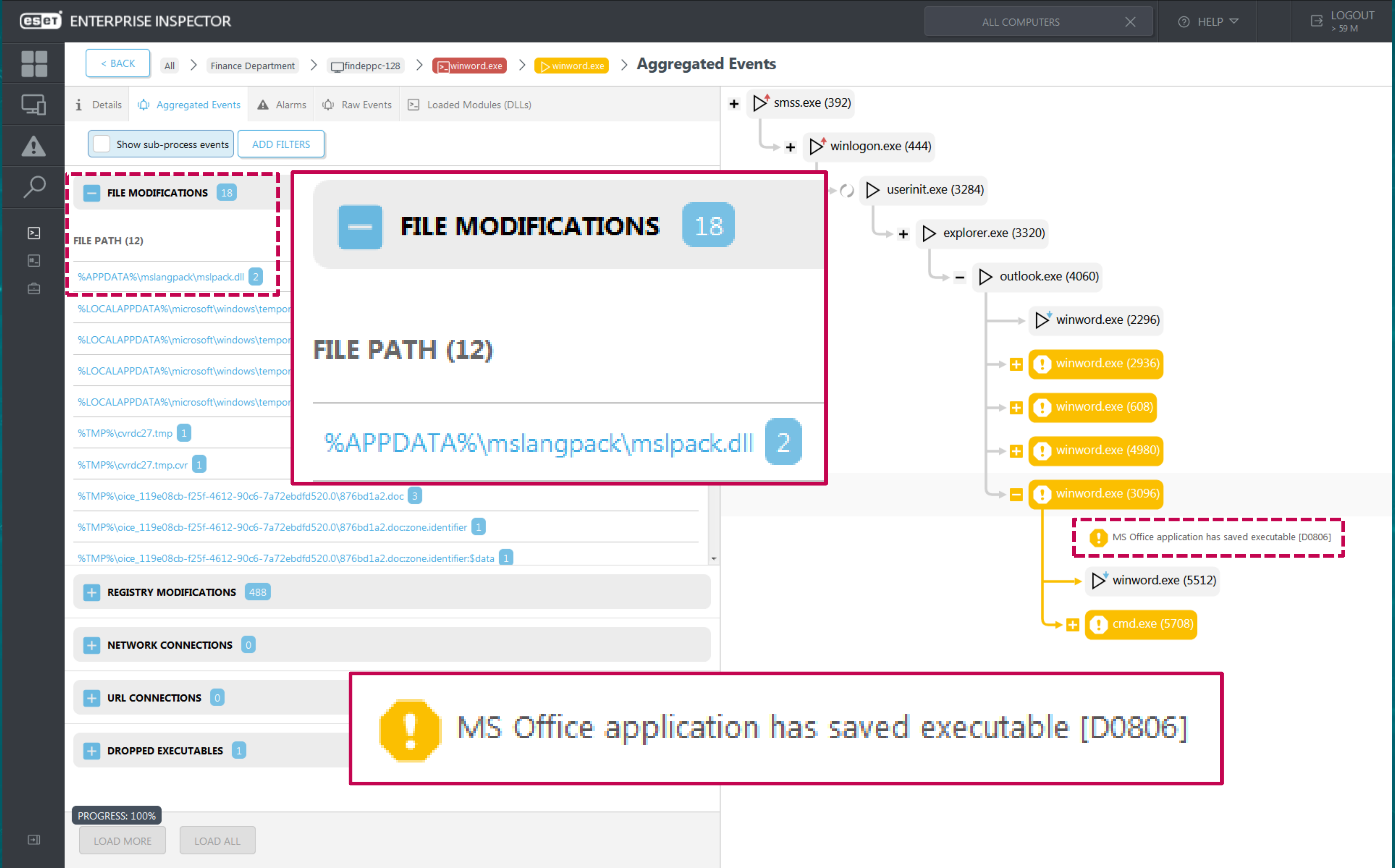
PROCESS	winword.exe (3096)
COMMAND LINE	/n "C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\NCHVDCEN\invoice_26316 (2).doc"
PATH	
STARTED	
ENDED	
PARENT PROCESS	outlook.exe (4060)

smss.exe (392)
winlogon.exe (444)
(3284)
xplorer.exe (3320)
outlook.exe (4060)
winword.exe (2296)
winword.exe (2936)
winword.exe (608)
winword.exe (4980)
winword.exe (3096)
MS Office application has saved executa
winword.exe (5512)
cmd.exe (5708)

outlook.exe (4060)

winword.exe (3096)

/n "C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\NCHVDCEN\invoice_26316 (2).doc"



ENTERPRISE INSPECTOR

ALL COMPUTERS

HELP

LOGOUT > 59 M

< BACK | All > Finance Department > findeppc-128 > winword.exe > winword.exe > **Aggregated Events**

Details | Aggregated Events | Alarms | Raw Events | Loaded Modules (DLLs)

□ Show sub-process events | ADD FILTERS

FILE MODIFICATIONS 18

FILE PATH (12)

%APPDATA%\mslangpack\mslpack.dll	2
%LOCALAPPDATA%\microsoft\windows\tempor	
%LOCALAPPDATA%\microsoft\windows\tempor	
%LOCALAPPDATA%\microsoft\windows\tempor	
%LOCALAPPDATA%\microsoft\windows\tempor	
%TMP%\cvrdc27.tmp	1
%TMP%\cvrdc27.tmp.cvr	1
%TMP%\oice_119e08cb-f25f-4612-90c6-7a72ebdfd520.0\876bd1a2.doc	3
%TMP%\oice_119e08cb-f25f-4612-90c6-7a72ebdfd520.0\876bd1a2.doc:zone.identifier	1
%TMP%\oice_119e08cb-f25f-4612-90c6-7a72ebdfd520.0\876bd1a2.doc:zone.identifier:$data	1

REGISTRY MODIFICATIONS 488

NETWORK CONNECTIONS 0

URL CONNECTIONS 0

DROPPED EXECUTABLES 1

PROGRESS: 100%

LOAD MORE | LOAD ALL

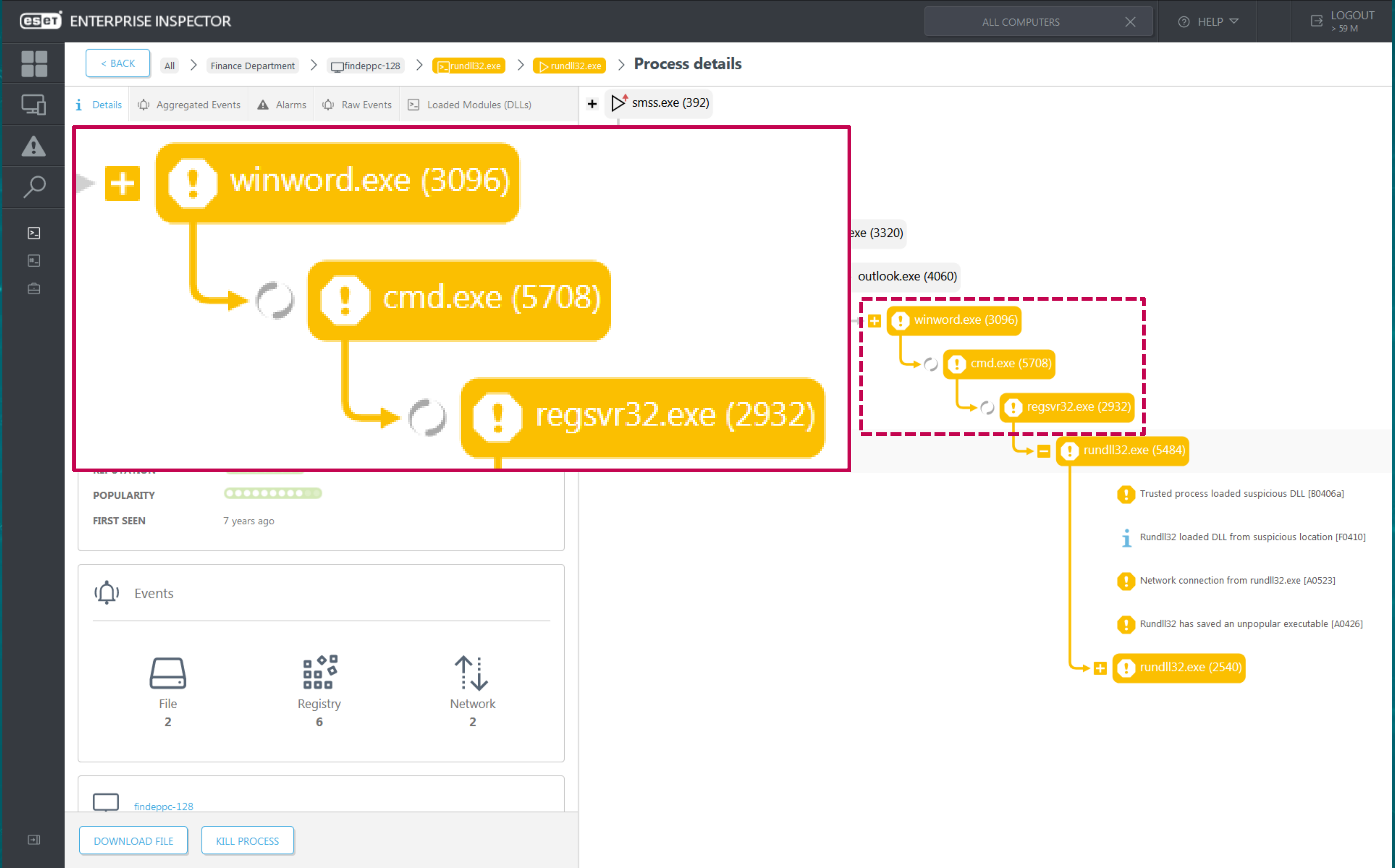
smss.exe (392)
- winlogon.exe (444)
  - userinit.exe (3284)
    - explorer.exe (3320)
      - outlook.exe (4060)
        - winword.exe (2296)
        - winword.exe (2936)
        - winword.exe (608)
        - winword.exe (4980)
        - winword.exe (3096)
          - MS Office application has saved executable [D0806]
          - winword.exe (5512)
          - cmd.exe (5708)

FILE MODIFICATIONS 18

FILE PATH (12)

%APPDATA%\mslangpack\mslpack.dll 2

MS Office application has saved executable [D0806]



ESET ENTERPRISE INSPECTOR

ALL COMPUTERS

HELP

LOGOUT
> 59 M

< BACK

All > Finance Department > findeppc-128 > rundll32.exe > rundll32.exe > Process details

Details | Aggregated Events | Alarms | Raw Events | Loaded Modules (DLLs)

smss.exe (392)

exe (3320)

outlook.exe (4060)

winword.exe (3096)

cmd.exe (5708)

regsvr32.exe (2932)

rundll32.exe (5484)

Trusted process loaded suspicious DLL [B0406a]

Rundll32 loaded DLL from suspicious location [F0410]

Network connection from rundll32.exe [A0523]

Rundll32 has saved an unpopular executable [A0426]

rundll32.exe (2540)

POPULARITY

FIRST SEEN 7 years ago

Events

File 2

Registry 6

Network 2

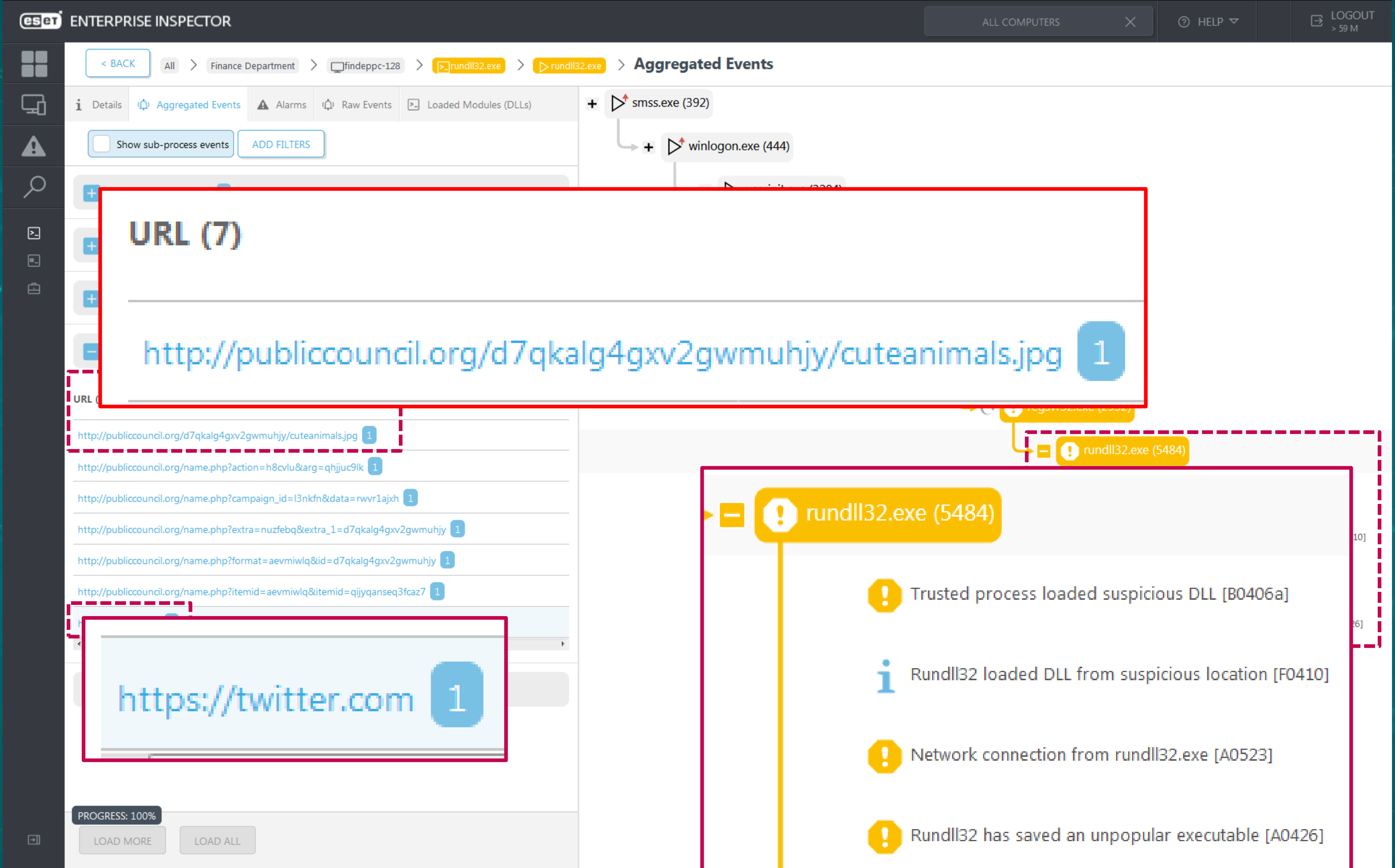
findeppc-128

DOWNLOAD FILE

KILL PROCESS

Stage 1 – PolyglotDuke

Twitter C&C + Picture downloader + Dropper



URL (7)

http://publiccouncil.org/d7qkalg4gxv2gwmuhjy/cuteanimals.jpg 1

http://publiccouncil.org/name.php?action=h8cvlu&arg=qhjjuc9lk 1

http://publiccouncil.org/name.php?campaign_id=l3nkfn&data=rwvr1ajxh 1

http://publiccouncil.org/name.php?extra=nuzfebq&extra_1=d7qkalg4gxv2gwmuhjy 1

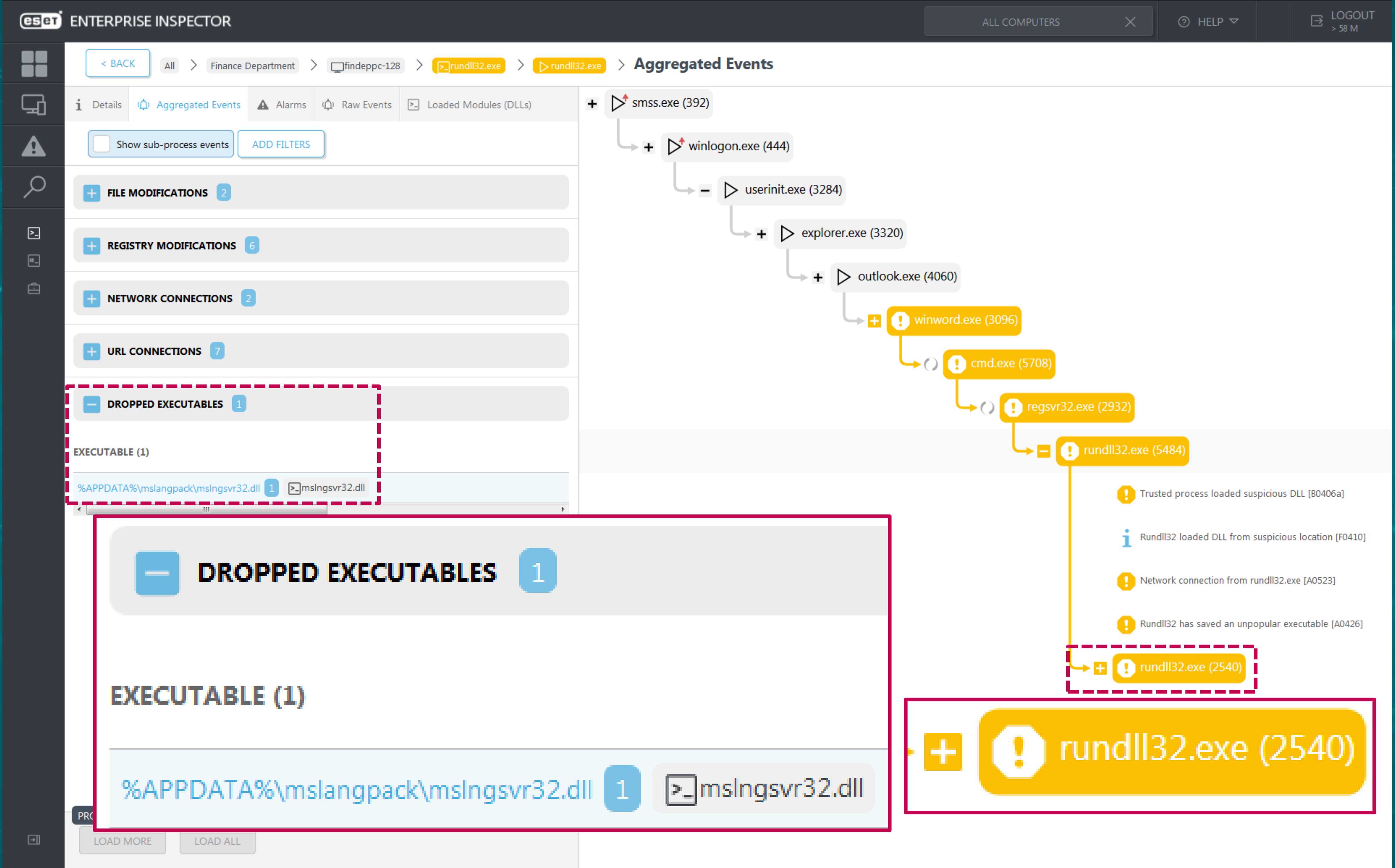
http://publiccouncil.org/name.php?format=aevmiwlq&id=d7qkalg4gxv2gwmuhjy 1

http://publiccouncil.org/name.php?itemid=aevmiwlq&itemid=qijyqanseq3fcaz7 1

https://twitter.com 1

rundll32.exe (5484)

- Trusted process loaded suspicious DLL [B0406a]
- Rundll32 loaded DLL from suspicious location [F0410]
- Network connection from rundll32.exe [A0523]
- Rundll32 has saved an unpopular executable [A0426]



ENTERPRISE INSPECTOR

ALL COMPUTERS

HELP

LOGOUT
> 58 M

< BACK

All > Finance Department > findeppc-128 > rundll32.exe > rundll32.exe > **Aggregated Events**

Details | Aggregated Events | Alarms | Raw Events | Loaded Modules (DLLs)

□ Show sub-process events

ADD FILTERS

FILE MODIFICATIONS 2

REGISTRY MODIFICATIONS 6

NETWORK CONNECTIONS 2

URL CONNECTIONS 7

DROPPED EXECUTABLES 1

EXECUTABLE (1)

%APPDATA%\mslangpack\mslngsvr32.dll 1 mslngsvr32.dll

LOAD MORE

LOAD ALL

- smss.exe (392)
  - winlogon.exe (444)
    - userinit.exe (3284)
      - explorer.exe (3320)
        - outlook.exe (4060)
          - winword.exe (3096)
            - cmd.exe (5708)
              - regsvr32.exe (2932)
                - rundll32.exe (5484)
                  - Trusted process loaded suspicious DLL [B0406a]
                  - Rundll32 loaded DLL from suspicious location [F0410]
                  - Network connection from rundll32.exe [A0523]
                  - Rundll32 has saved an unpopular executable [A0426]
                  - rundll32.exe (2540)

DROPPED EXECUTABLES 1

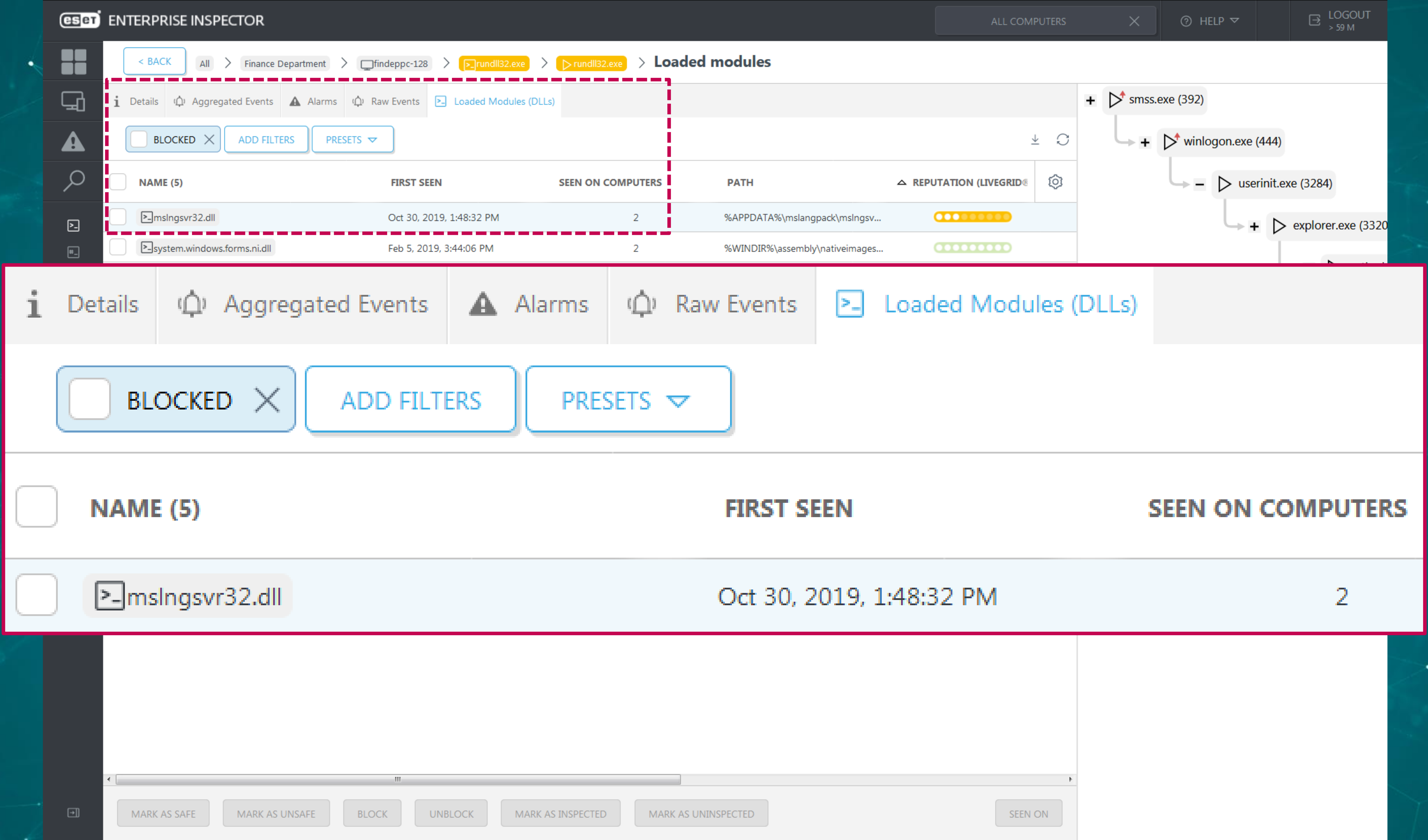
EXECUTABLE (1)

%APPDATA%\mslangpack\mslngsvr32.dll 1 mslngsvr32.dll

rundll32.exe (2540)

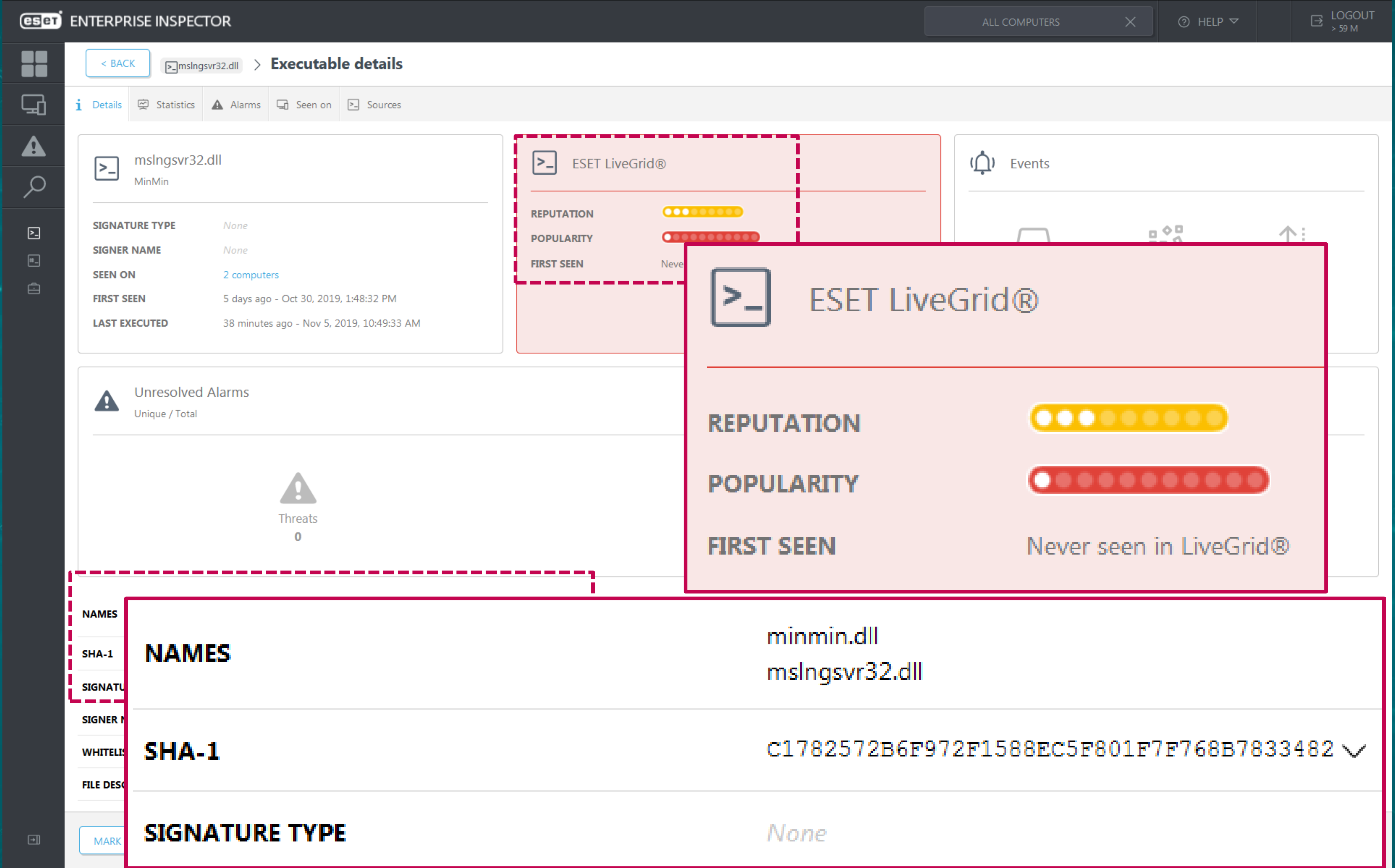
Stage 2 – MiniDuke

Backdoor + Lateral movement



NAME (5)	FIRST SEEN	SEEN ON COMPUTERS	PATH	REPUTATION (LIVEGRID®
mslngsvr32.dll	Oct 30, 2019, 1:48:32 PM	2	%APPDATA%\mslangpack\mslngsv...	
system.windows.forms.ni.dll	Feb 5, 2019, 3:44:06 PM	2	%WINDIR%\assembly\nativeimages...	

NAME (5)	FIRST SEEN	SEEN ON COMPUTERS
mslngsvr32.dll	Oct 30, 2019, 1:48:32 PM	2



Executable details

mslngsvr32.dll
MinMin

SIGNATURE TYPE	None
SIGNER NAME	None
SEEN ON	2 computers
FIRST SEEN	5 days ago - Oct 30, 2019, 1:48:32 PM
LAST EXECUTED	38 minutes ago - Nov 5, 2019, 10:49:33 AM

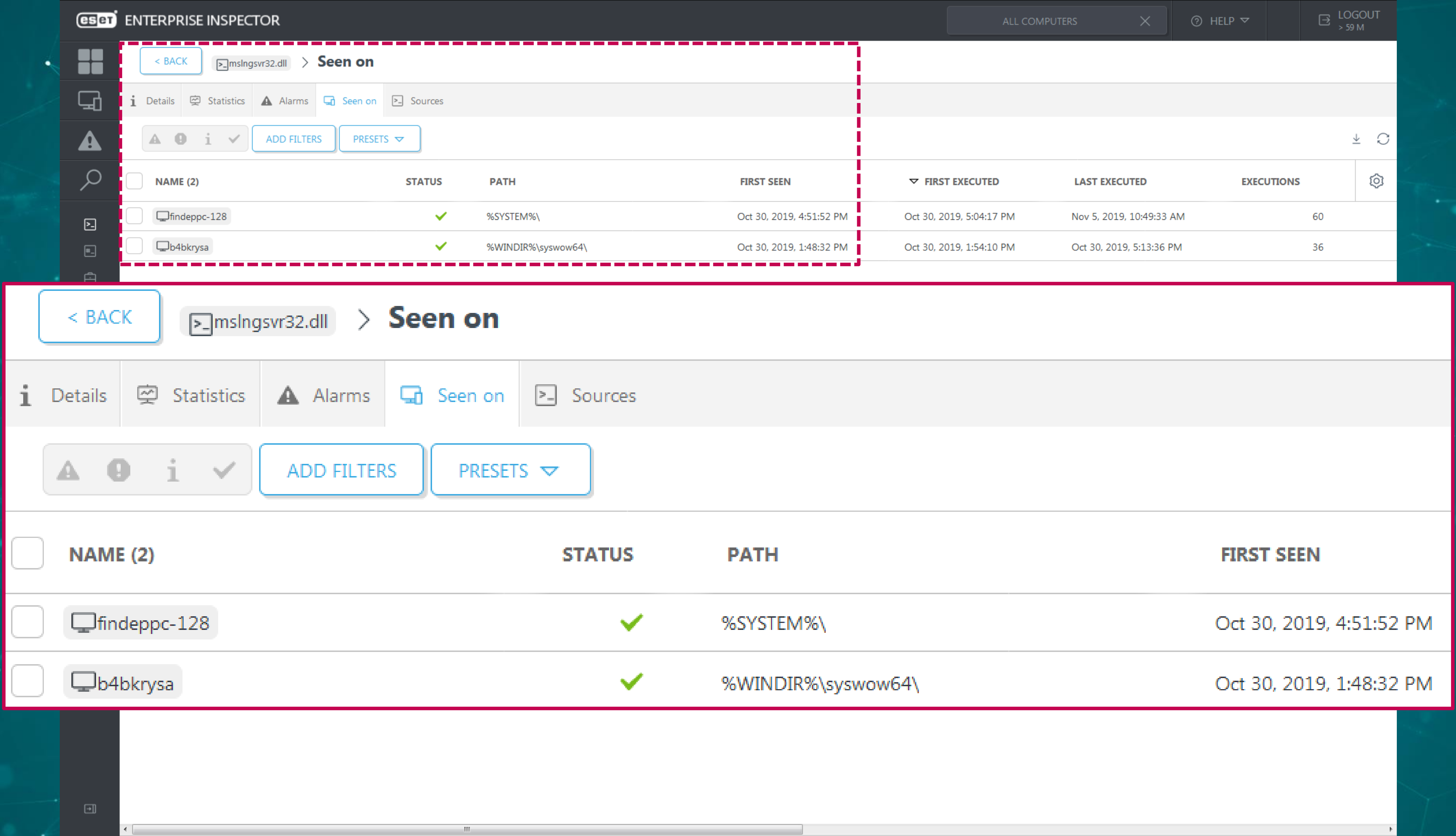
Unresolved Alarms
Unique / Total

Threats
0

ESET LiveGrid®

REPUTATION	●●●○○○○○○
POPULARITY	●○○○○○○○○○○
FIRST SEEN	Never seen in LiveGrid®

NAMES	minmin.dll mslngsvr32.dll
SHA-1	C1782572B6F972F1588EC5F801F7F768B7833482
SIGNATURE TYPE	None



mslngsvr32.dll > Seen on

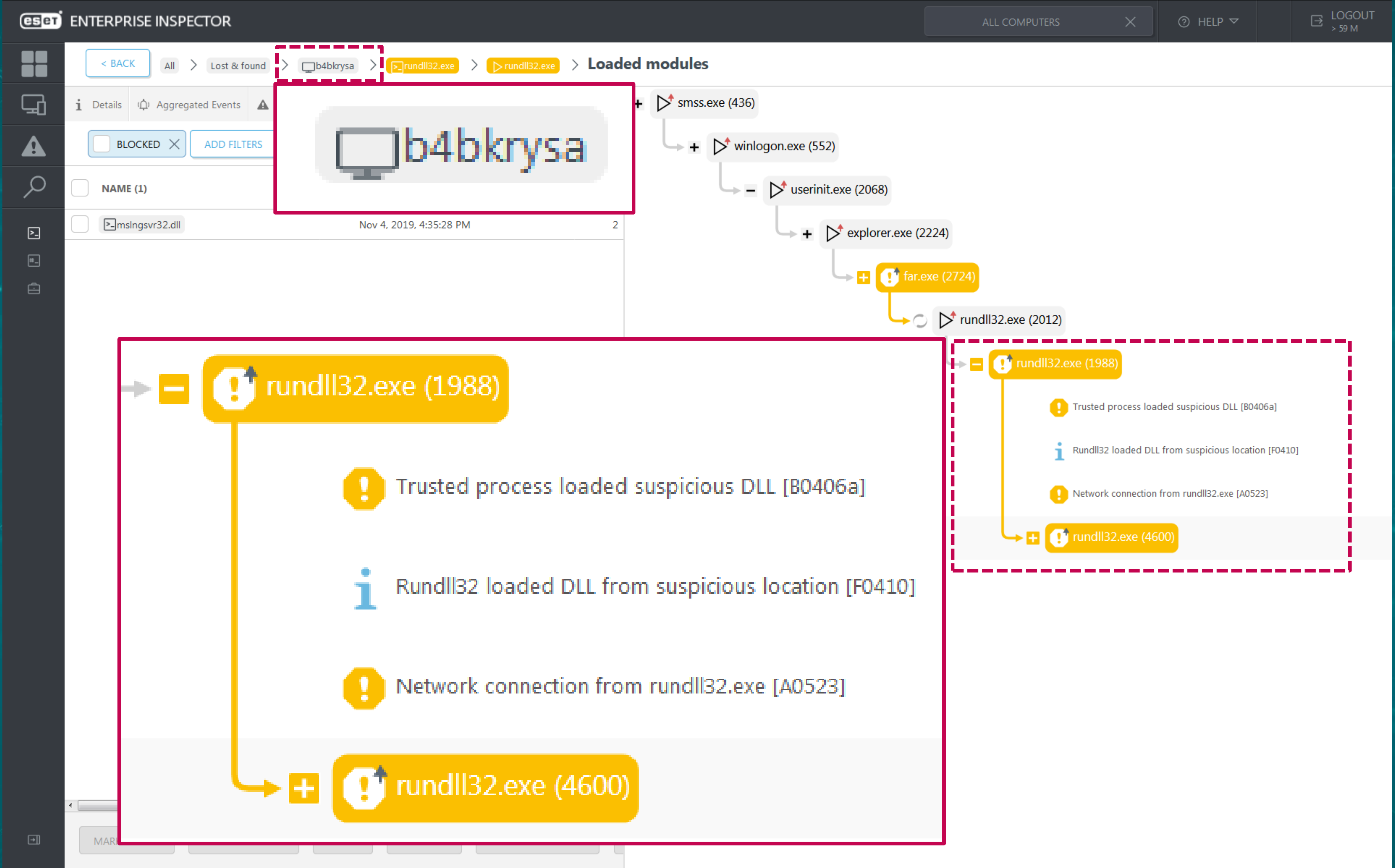
NAME (2)	STATUS	PATH	FIRST SEEN	FIRST EXECUTED	LAST EXECUTED	EXECUTIONS
findeppc-128	✓	%SYSTEM%\	Oct 30, 2019, 4:51:52 PM	Oct 30, 2019, 5:04:17 PM	Nov 5, 2019, 10:49:33 AM	60
b4bkrysa	✓	%WINDIR%\syswow64\	Oct 30, 2019, 1:48:32 PM	Oct 30, 2019, 1:54:10 PM	Oct 30, 2019, 5:13:36 PM	36

< BACK mslngsvr32.dll > Seen on

Details Statistics Alarms Seen on Sources

ADD FILTERS PRESETS

NAME (2)	STATUS	PATH	FIRST SEEN
findeppc-128	✓	%SYSTEM%\	Oct 30, 2019, 4:51:52 PM
b4bkrysa	✓	%WINDIR%\syswow64\	Oct 30, 2019, 1:48:32 PM



Loaded modules

NAME (1)		
mslngsvr32.dll	Nov 4, 2019, 4:35:28 PM	2

- smss.exe (436)
  - winlogon.exe (552)
    - userinit.exe (2068)
      - explorer.exe (2224)
        - far.exe (2724)
          - rundll32.exe (2012)
            - rundll32.exe (1988)
              - Trusted process loaded suspicious DLL [B0406a]
              - Rundll32 loaded DLL from suspicious location [F0410]
              - Network connection from rundll32.exe [A0523]
              - rundll32.exe (4600)

b4bkrysa

rundll32.exe (1988)

Trusted process loaded suspicious DLL [B0406a]

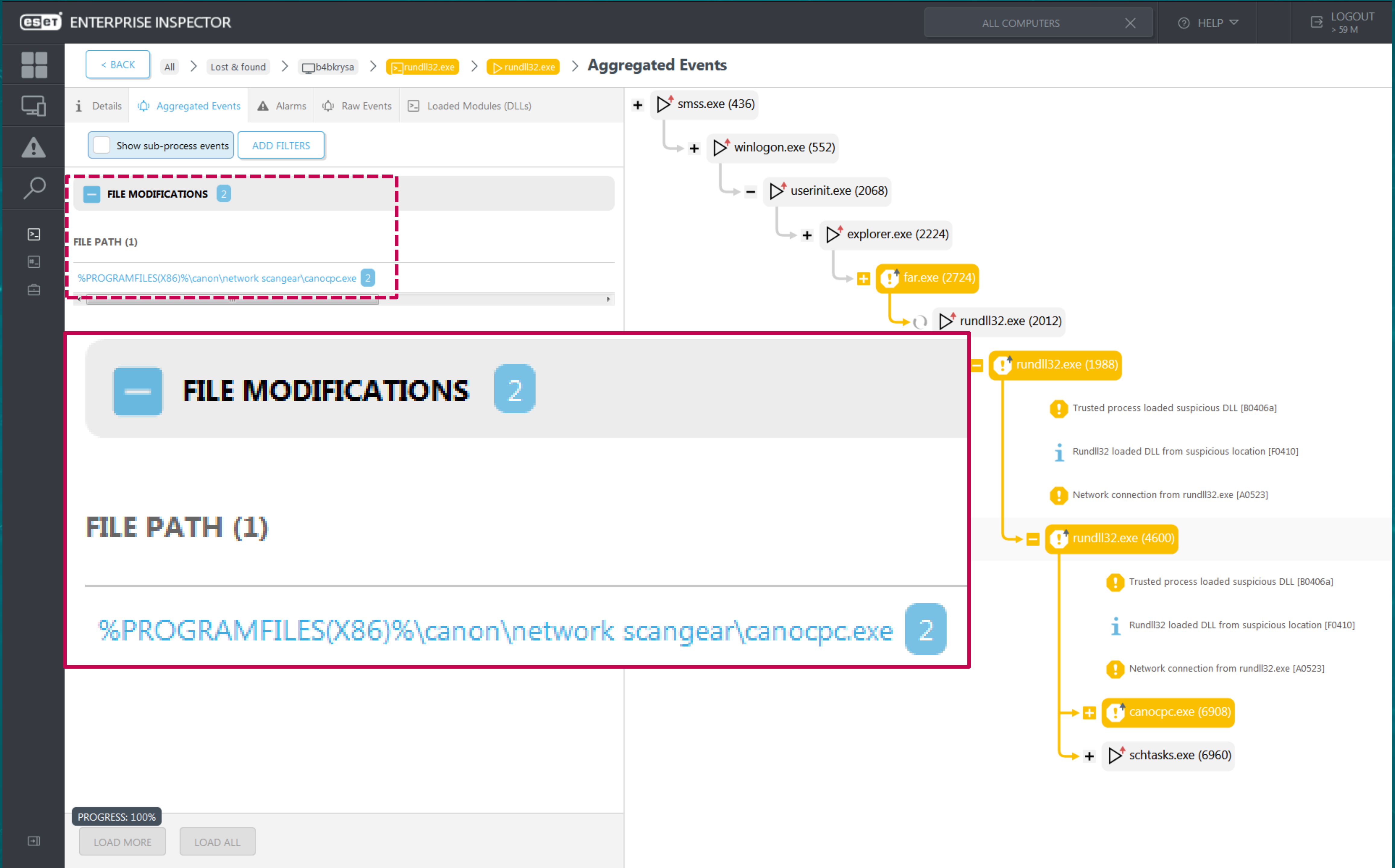
Rundll32 loaded DLL from suspicious location [F0410]

Network connection from rundll32.exe [A0523]

rundll32.exe (4600)

Stage 3 – FatDuke

Backdoor + Malicious activity



FILE MODIFICATIONS 2

FILE PATH (1)

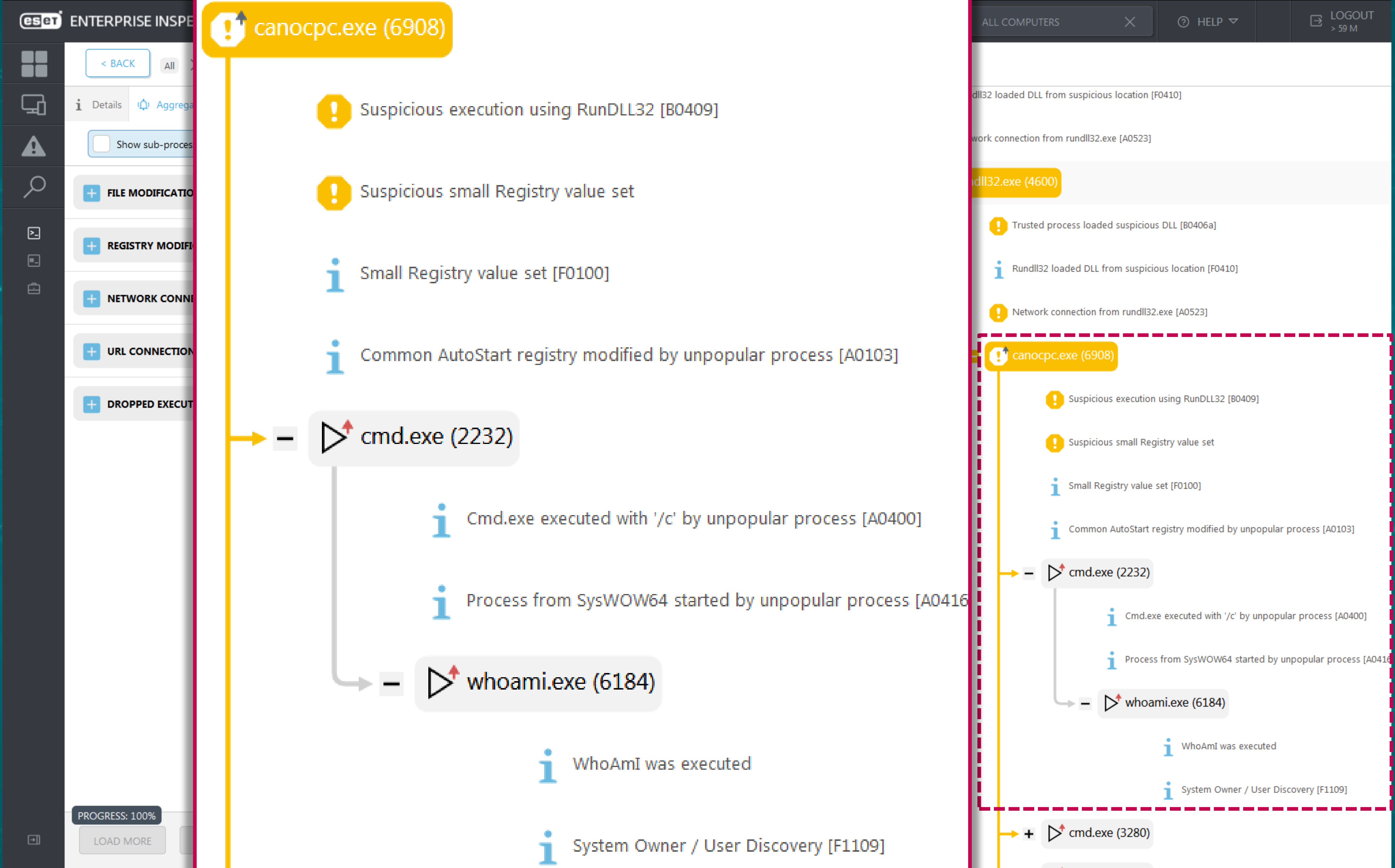
%PROGRAMFILES(X86)%\canon\network scangear\canocpc.exe 2

FILE MODIFICATIONS 2

FILE PATH (1)

%PROGRAMFILES(X86)%\canon\network scangear\canocpc.exe 2

smss.exe (436)
winlogon.exe (552)
userinit.exe (2068)
explorer.exe (2224)
far.exe (2724)
rundll32.exe (2012)
rundll32.exe (1988)
Trusted process loaded suspicious DLL [B0406a]
Rundll32 loaded DLL from suspicious location [F0410]
Network connection from rundll32.exe [A0523]
rundll32.exe (4600)
Trusted process loaded suspicious DLL [B0406a]
Rundll32 loaded DLL from suspicious location [F0410]
Network connection from rundll32.exe [A0523]
canocpc.exe (6908)
schtasks.exe (6960)



canocpc.exe (6908)

Suspicious execution using RunDLL32 [B0409]

Suspicious small Registry value set

Small Registry value set [F0100]

Common AutoStart registry modified by unpopular process [A0103]

cmd.exe (2232)

Cmd.exe executed with '/c' by unpopular process [A0400]

Process from SysWOW64 started by unpopular process [A0416

whoami.exe (6184)

WhoAmI was executed

System Owner / User Discovery [F1109]

dll32 loaded DLL from suspicious location [F0410]

work connection from rundll32.exe [A0523]

dll32.exe (4600)

Trusted process loaded suspicious DLL [B0406a]

Rundll32 loaded DLL from suspicious location [F0410]

Network connection from rundll32.exe [A0523]

canocpc.exe (6908)

Suspicious execution using RunDLL32 [B0409]

Suspicious small Registry value set

Small Registry value set [F0100]

Common AutoStart registry modified by unpopular process [A0103]

cmd.exe (2232)

Cmd.exe executed with '/c' by unpopular process [A0400]

Process from SysWOW64 started by unpopular process [A0416

whoami.exe (6184)

WhoAmI was executed

System Owner / User Discovery [F1109]

cmd.exe (3280)

EDR solutions should also:

Quick response

Purge resistance

Snapshot

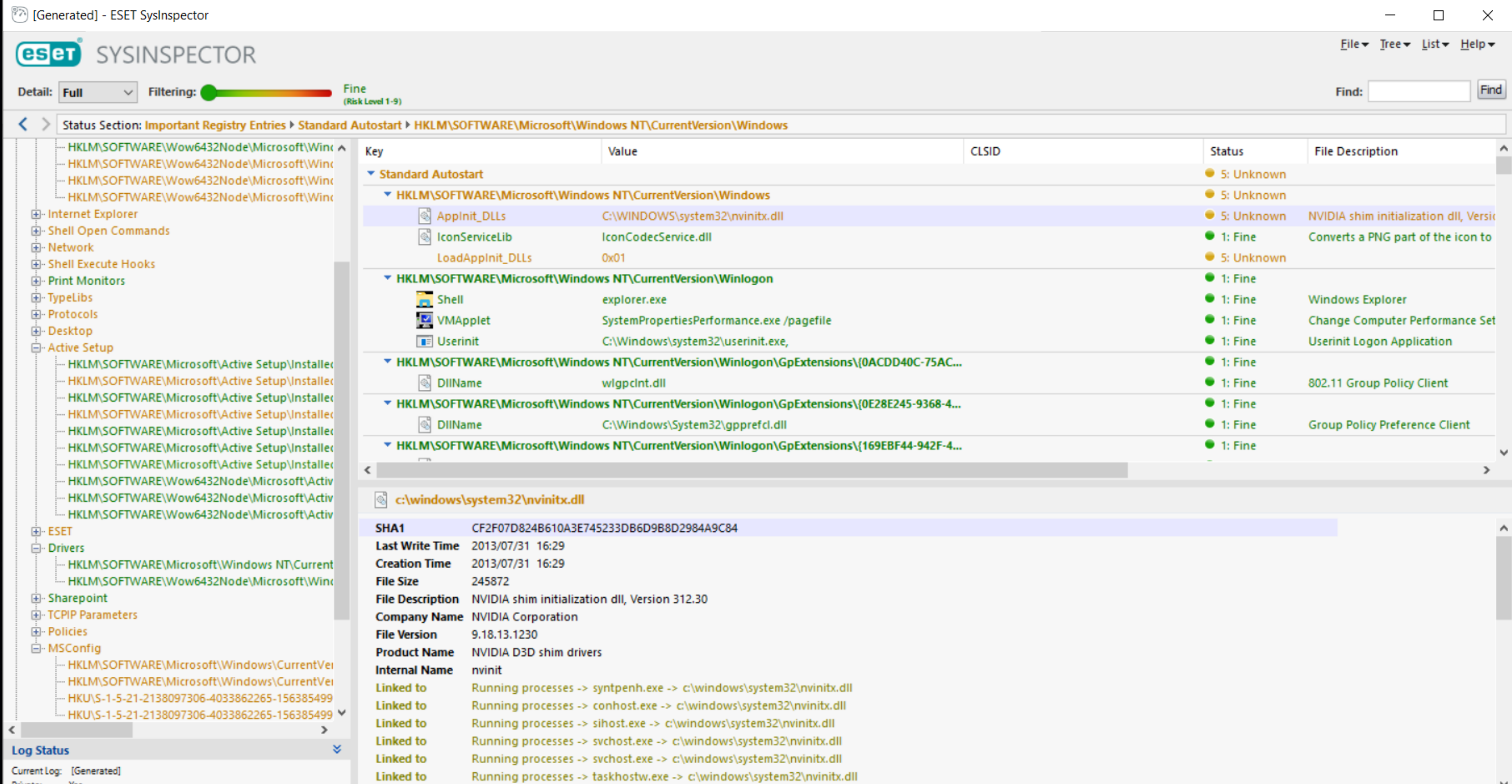
Multi-platform data

SIEM

AMSI

Automation

Security Snapshot – ESET SysInspector (also as free tool)



[Generated] - ESET SysInspector

Detail: Full Filtering: Fine (Risk Level 1-9) Find:

Status Section: Important Registry Entries ▸ Standard Autostart ▸ HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

- HKLM\SOFTWARE\Wow6432Node\Microsoft\Winc
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Winc
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Winc
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Winc
- Internet Explorer
- Shell Open Commands
- Network
- Shell Execute Hooks
- Print Monitors
- TypeLibs
- Protocols
- Desktop
- Active Setup
  - HKLM\SOFTWARE\Microsoft\Active Setup\Installec
  - HKLM\SOFTWARE\Microsoft\Active Setup\Installec
  - HKLM\SOFTWARE\Microsoft\Active Setup\Installec
  - HKLM\SOFTWARE\Microsoft\Active Setup\Installec
  - HKLM\SOFTWARE\Microsoft\Active Setup\Installec
  - HKLM\SOFTWARE\Microsoft\Active Setup\Installec
  - HKLM\SOFTWARE\Microsoft\Active Setup\Installec
  - HKLM\SOFTWARE\Wow6432Node\Microsoft\Activ
  - HKLM\SOFTWARE\Wow6432Node\Microsoft\Activ
  - HKLM\SOFTWARE\Wow6432Node\Microsoft\Activ
- ESET
- Drivers
  - HKLM\SOFTWARE\Microsoft\Windows NT\Current
  - HKLM\SOFTWARE\Wow6432Node\Microsoft\Winc
- Sharepoint
- TCPIP Parameters
- Policies
- MSConfig
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVe
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVe
  - HKU\S-1-5-21-2138097306-4033862265-156385499
  - HKU\S-1-5-21-2138097306-4033862265-156385499

Log Status

Current Log: [Generated]

Key	Value	CLSID	Status	File Description
Standard Autostart			● 5: Unknown	
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows			● 5: Unknown	
AppInit_DLLs	C:\WINDOWS\system32\nvinitx.dll		● 5: Unknown	NVIDIA shim initialization dll, Versic
IconServiceLib	IconCodecService.dll		● 1: Fine	Converts a PNG part of the icon to
LoadAppInit_DLLs	0x01		● 5: Unknown	
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon			● 1: Fine	
Shell	explorer.exe		● 1: Fine	Windows Explorer
VMApplet	SystemPropertiesPerformance.exe /pagefile		● 1: Fine	Change Computer Performance Set
Userinit	C:\Windows\system32\userinit.exe,		● 1: Fine	Userinit Logon Application
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GpExtensions\{0ACDD40C-75AC...			● 1: Fine	
DllName	wlgpclnt.dll		● 1: Fine	802.11 Group Policy Client
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GpExtensions\{0E28E245-9368-4...			● 1: Fine	
DllName	C:\Windows\System32\gpprefcl.dll		● 1: Fine	Group Policy Preference Client
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GpExtensions\{169EBF44-942F-4...			● 1: Fine	

c:\windows\system32\nvinitx.dll

SHA1	CF2F07D824B610A3E745233DB6D9B8D2984A9C84
Last Write Time	2013/07/31 16:29
Creation Time	2013/07/31 16:29
File Size	245872
File Description	NVIDIA shim initialization dll, Version 312.30
Company Name	NVIDIA Corporation
File Version	9.18.13.1230
Product Name	NVIDIA D3D shim drivers
Internal Name	nvinit
Linked to	Running processes -> syntpenh.exe -> c:\windows\system32\nvinitx.dll
Linked to	Running processes -> conhost.exe -> c:\windows\system32\nvinitx.dll
Linked to	Running processes -> sihost.exe -> c:\windows\system32\nvinitx.dll
Linked to	Running processes -> svchost.exe -> c:\windows\system32\nvinitx.dll
Linked to	Running processes -> svchost.exe -> c:\windows\system32\nvinitx.dll
Linked to	Running processes -> taskhostw.exe -> c:\windows\system32\nvinitx.dll

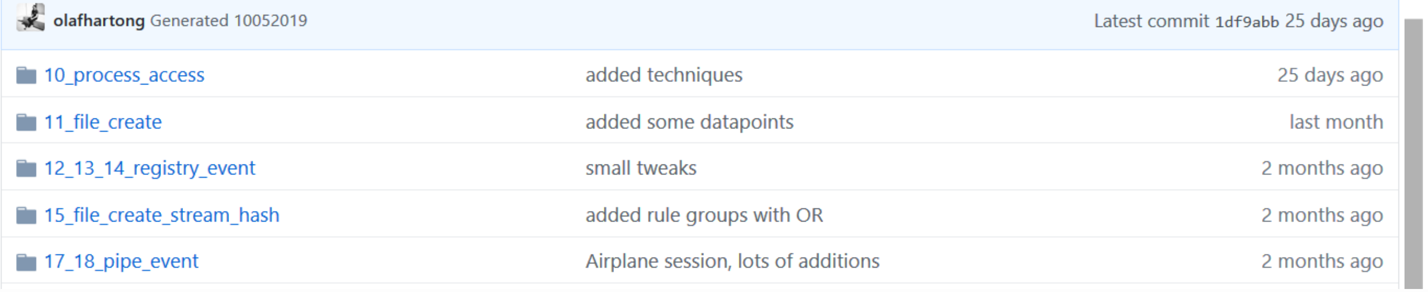
Any free alternatives to EDR?

SysMon v10 + a lot of manual work

github.com/olafhartong/sysmon-modular

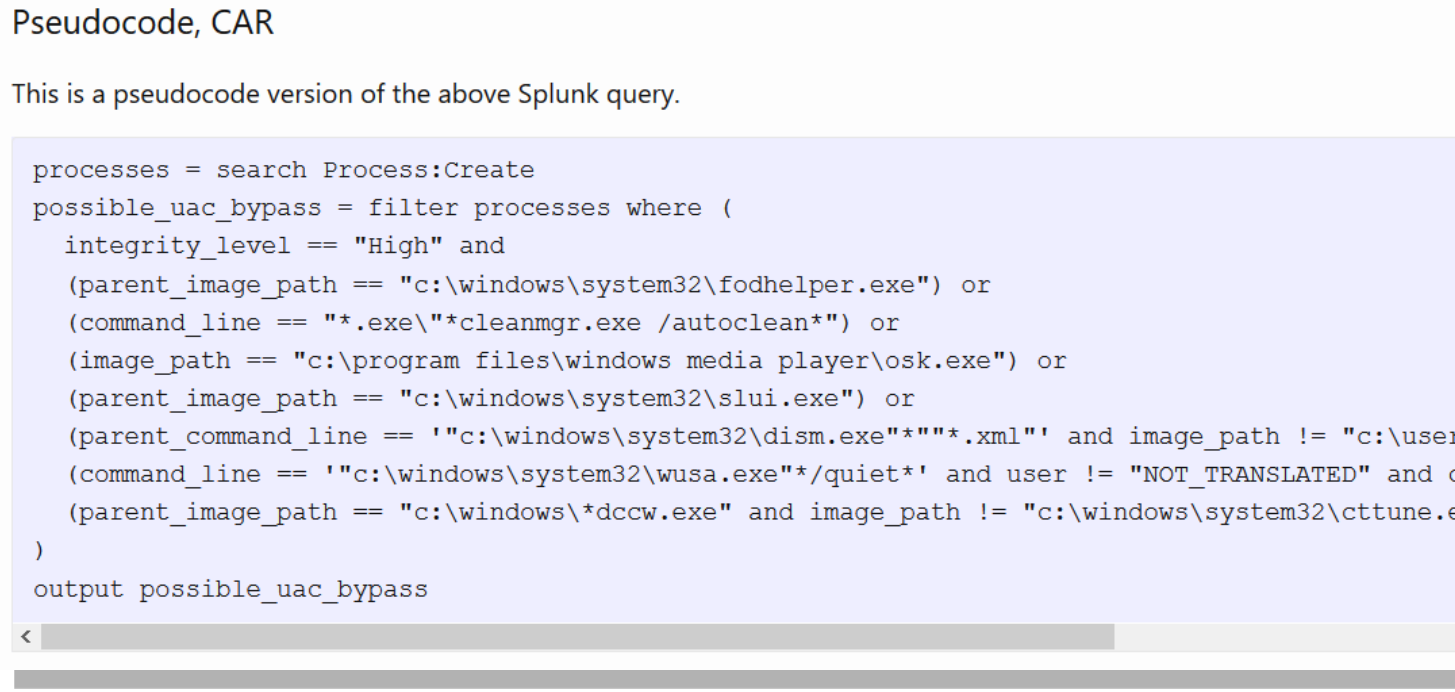
Other drawbacks:

- Single platform
- Reactive
- Limited to what SysMon can monitor
- Resource heavy
- Storage issues (no pre-filtering)
- Requires SIEM for detection rules



olafhartong Generated 10052019 — Latest commit 1df9abb 25 days ago

10_process_access	added techniques	25 days ago
11_file_create	added some datapoints	last month
12_13_14_registry_event	small tweaks	2 months ago
15_file_create_stream_hash	added rule groups with OR	2 months ago
17_18_pipe_event	Airplane session, lots of additions	2 months ago



Pseudocode, CAR

This is a pseudocode version of the above Splunk query.

```
processes = search Process:Create
possible_uac_bypass = filter processes where (
  integrity_level == "High" and
  (parent_image_path == "c:\windows\system32\fodhelper.exe") or
  (command_line == "*.exe\"*cleanmgr.exe /autoclean*") or
  (image_path == "c:\program files\windows media player\osk.exe") or
  (parent_image_path == "c:\windows\system32\slui.exe") or
  (parent_command_line == '"c:\windows\system32\dism.exe"*""*.xml"' and image_path != "c:\user
  (command_line == '"c:\windows\system32\wusa.exe"*/quiet*' and user != "NOT_TRANSLATED" and
  (parent_image_path == "c:\windows\*dccw.exe" and image_path != "c:\windows\system32\cttune.e
)
output possible_uac_bypass
```

Thank you