Orange
Cyberdefense

Enhanced malware detection

Reduce the risk of introducing a malware in your internal network

orange™

40% of

the 30k confirmed incidents were **malwares***

Malware is any malicious software, script, or code running on a device that alters its state or function without the owner’s informed consent.

***Source: Orange Cyberdefense Security Navigator Report 2023**

Challenge

Malwares proliferating, limited resources and expertise.

How to…

… ensure that files are safe before entering my network?

… automate files analysis and make it seamless for my employees?

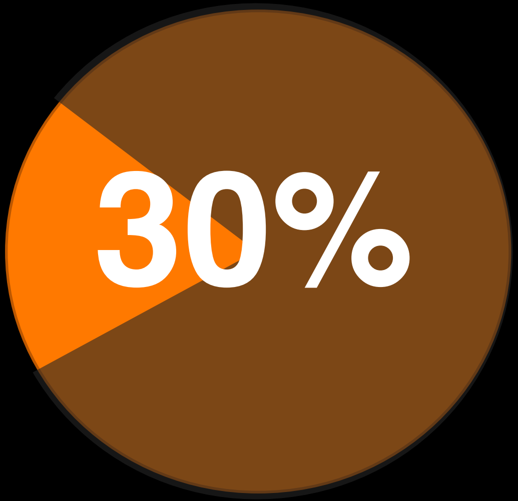
… maintain the confidentiality of the data analysed?

… detect malwares that are still unknown by antivirus?

Enhanced malware detection

Complementarity is key

… ensure that files are safe before entering my network?



is the detection rate of

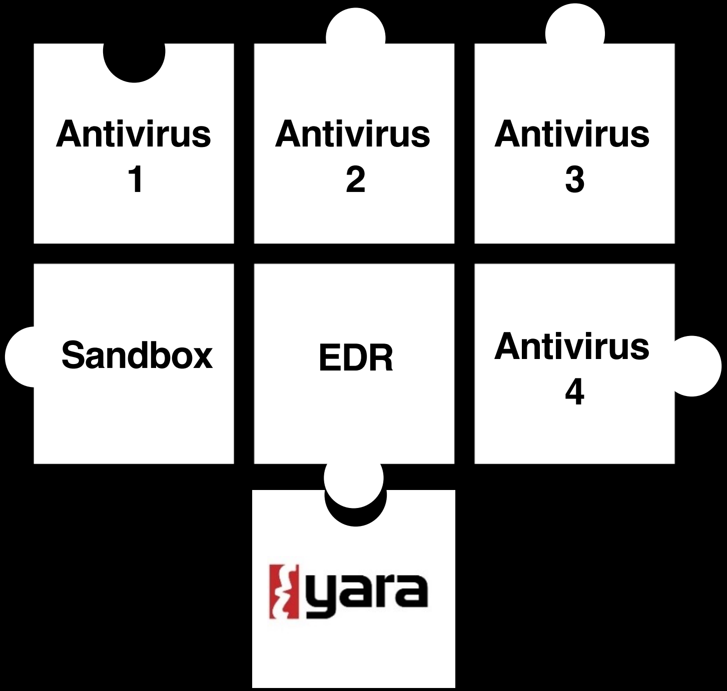
The best antivirus* in the market

*offline

... ensure that files are safe before entering my network?

Enhanced malware detection

Combining tools to improve your detection rate



Antivirus 1

Antivirus 2

Antivirus 3

Sandbox

EDR

Antivirus 4

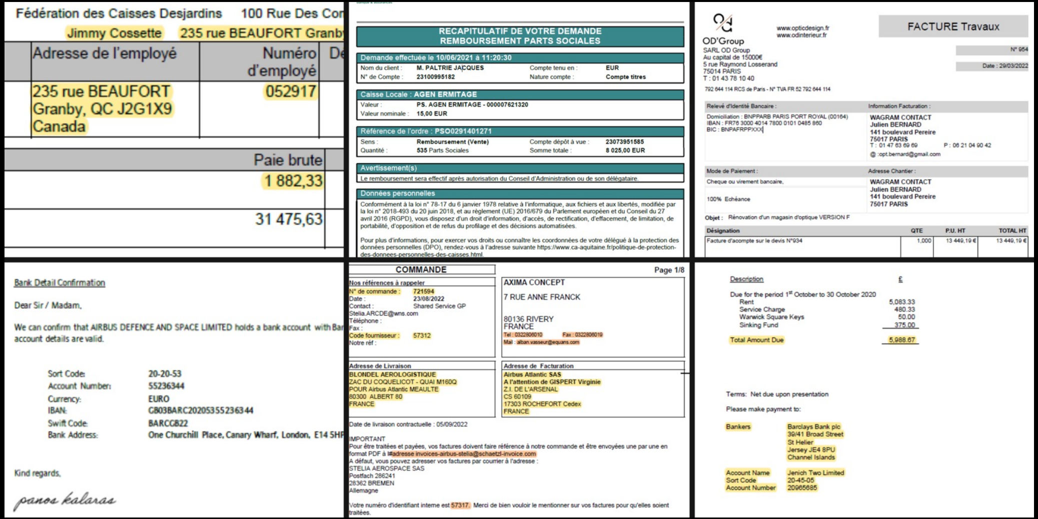
yara

Enhanced malware detection

Confidentiality is key

… maintain the confidentiality of the data analysed?

Misuse of security tools can turn against you:



Fédération des Caisses Desjardins 100 Rue Des Cor

Jimmy Cossette 235 rue BEAUFORT Granb

	Adresse de l'employé	Numéro d'employé	De
	235 rue BEAUFORT Granby, QC J2G1X9 Canada	052917	

Paie brute
1 882,33
31 475,63

RECAPITULATIF DE VOTRE DEMANDE
REMBOURSEMENT PARTS SOCIALES

Demande effectuée le 10/06/2021 à 11:20:30

Nom du client :	M. PALTRIE JACQUES	Compte tenu en :	EUR
N° de Compte :	23100995182	Nature compte :	Compte titres

Caisse Locale : AGEN ERMITAGE

Valeur :	PS. AGEN ERMITAGE - 000007621320
Valeur nominale :	15,00 EUR

Référence de l'ordre : PSO0291401271

Sens :	Remboursement (Vente)	Compte dépôt à vue :	23073951585
Quantité :	535 Parts Sociales	Somme totale :	8 025,00 EUR

Avertissement(s)

Le remboursement sera effectif après autorisation du Conseil d'Administration ou de son délégataire.

Données personnelles

Conformément à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018, et au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD), vous disposez d'un droit d'information, d'accès, de rectification, d'effacement, de limitation, de portabilité, d'opposition et de refus du profilage et des décisions automatisées.

Pour plus d'informations, pour exercer vos droits ou connaître les coordonnées de votre délégué à la protection des données personnelles (DPO), rendez-vous à l'adresse suivante https://www.ca-aquitaine.fr/politique-de-protection-des-donnees-personnelles-des-caisses.html.

OD'Group
SARL OD Group
Au capital de 15000€
5 rue Raymond Losserand
75014 PARIS
T : 01 43 78 10 40

www.opticdesign.fr
www.odinterieur.fr

FACTURE Travaux

N° 954

Date : 29/03/2022

792 644 114 RCS de Paris - N° TVA FR 52 792 644 114

Relevé d'Identité Bancaire :	Information Facturation :
Domiciliation : BNPPARB PARIS PORT ROYAL (00164) IBAN : FR76 3000 4014 7800 0101 0485 860 BIC : BNPAFRPPXXX	WAGRAM CONTACT Julien BERNARD 141 boulevard Pereire 75017 PARIS T : 01 47 63 69 69 P : 06 21 04 90 42 @ :opt.bernard@gmail.com

Mode de Paiement :	Adresse Chantier :
Cheque ou virement bancaire. 100% Echéance	WAGRAM CONTACT Julien BERNARD 141 boulevard Pereire 75017 PARIS

Objet : Rénovation d'un magasin d'optique VERSION F

Désignation	QTE	P.U. HT	TOTAL HT
Facture d'acompte sur le devis N°934	1,000	13 449,19 €	13 449,19 €

Bank Detail Confirmation

Dear Sir / Madam,

We can confirm that AIRBUS DEFENCE AND SPACE LIMITED holds a bank account with Bar
account details are valid.

Sort Code:	20-20-53
Account Number:	55236344
Currency:	EURO
IBAN:	GB03BARC20205355236344
Swift Code:	BARCGB22
Bank Address:	One Churchill Place, Canary Wharf, London, E14 5HP

Kind regards,

panos kalaras

COMMANDE

Page 1/8

Nos références à rappeler

N° de commande :	721594
Date :	23/08/2022
Contact :	Shared Service GP
Stelia.ARCDE@wns.com	
Téléphone :	
Fax :	
Code fournisseur :	57312
Notre réf :	

AXIMA CONCEPT
7 RUE ANNE FRANCK
80136 RIVERY
FRANCE
Tel : 0322806010 Fax : 0322806019
Mail : alban.vasseur@equans.com

Adresse de Livraison
BLONDEL AEROLOGISTIQUE
ZAC DU COQUELICOT - QUAI M160Q
POUR Airbus Atlantic MEAULTE
80300 ALBERT 80
FRANCE

Adresse de Facturation
Airbus Atlantic SAS
A l'attention de GISPERT Virginie
Z.I. DE L'ARSENAL
CS 60109
17303 ROCHEFORT Cedex
FRANCE

Date de livraison contractuelle : 05/09/2022

IMPORTANT
Pour être traitées et payées, vos factures doivent faire référence à notre commande et être envoyées une par une en format PDF à l#adresse invoices-airbus-stelia@schaetzl-invoice.com
A défaut, vous pouvez adresser vos factures par courrier à l'adresse :
STELIA AEROSPACE SAS
Postfach 286241
28362 BREMEN
Allemagne

Votre numéro d'identifiant interne est 57317. Merci de bien vouloir le mentionner sur vos factures pour qu'elles soient traitées.

Description	£
Due for the period 1st October to 30 October 2020	
Rent	5,083.33
Service Charge	480.33
Warwick Square Keys	50.00
Sinking Fund	375.00
Total Amount Due	5,988.67

Terms: Net due upon presentation

Please make payment to:

Bankers	Barclays Bank plc 39/41 Broad Street St Helier Jersey JE4 8PU Channel Islands
Account Name	Jenich Two Limited
Sort Code	20-45-05
Account Number	20965685

Keep your data private!

The "Perfect" Cybercrime

Researchers Explore Hacking VirusTotal to Find Stolen Credentials

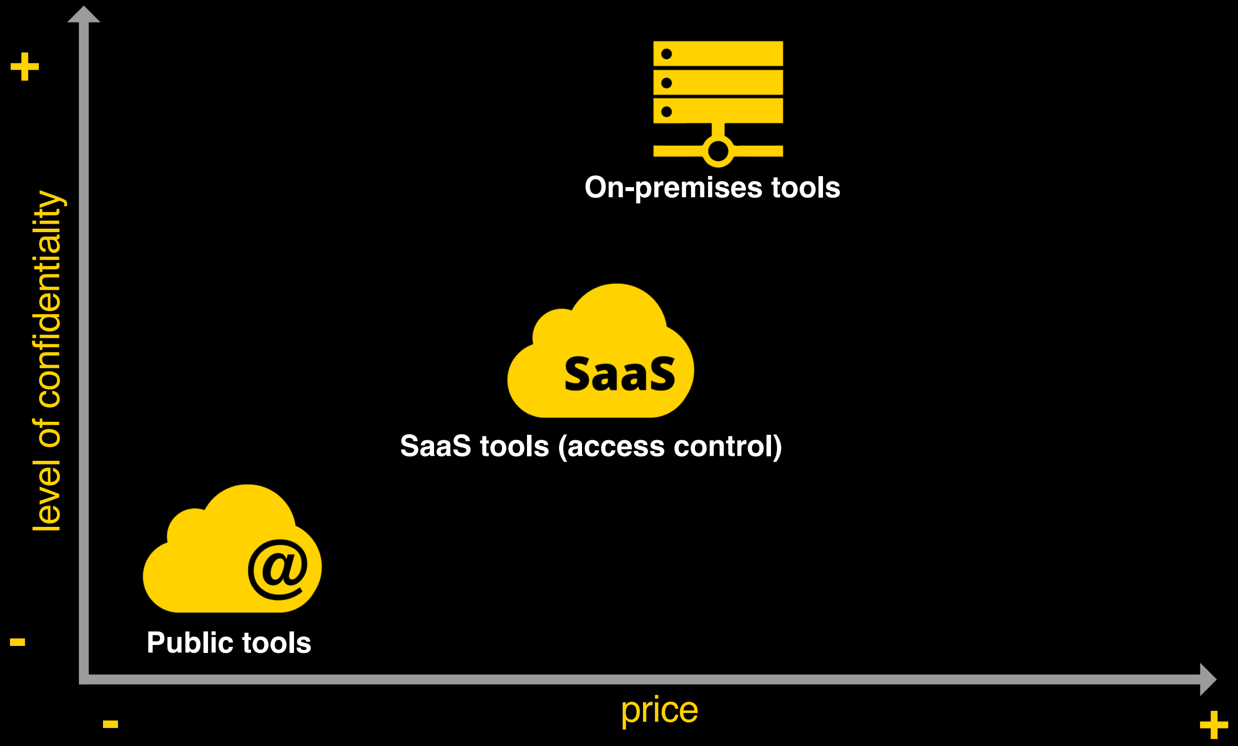
https://www.darkreading.com/threat-intelligence/researchers-explore-hacking-virustotal-to-find-stolen-credentials

- Clients information
- Invoices
- Bank details
- Passwords
- Mail adresses
- IBAN

Enhanced malware detection

Select the right tool according to the level of confidentiality needed

… maintain the confidentiality of the data analysed?



… automate files analysis and make it seamless for my employees?

47%

of the confirmed incidents are caused by **internal sources***

End-user devices

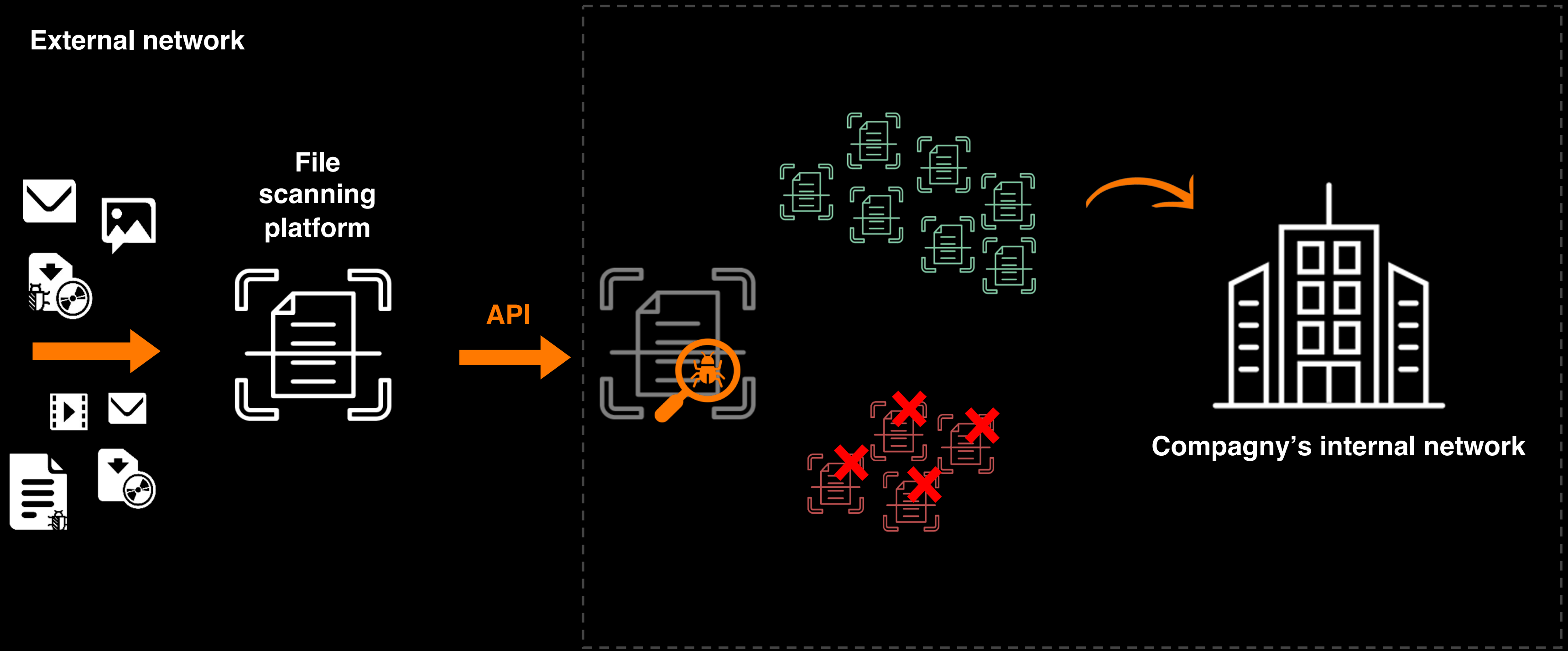
is the **most targeted** endpoint*

*Source: Orange Cyberdefense Security Navigator Report 2023

Enhanced malware detection

Automate files analysis in your workflow

… automate files analysis and make it seamless for my employees?



External network

File scanning platform

API

Compagny’s internal network

80%

malwares are packed and ½ of them are repacked versions of existing malwares

Packed malwares

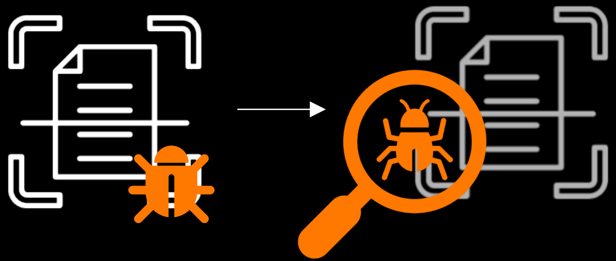
cannot be detected by antivirus

*Source: Dr. Mafaz Mohsin Khalil Al-Anezi

Enhanced malware detection

Two levels of analysis to not miss any malware

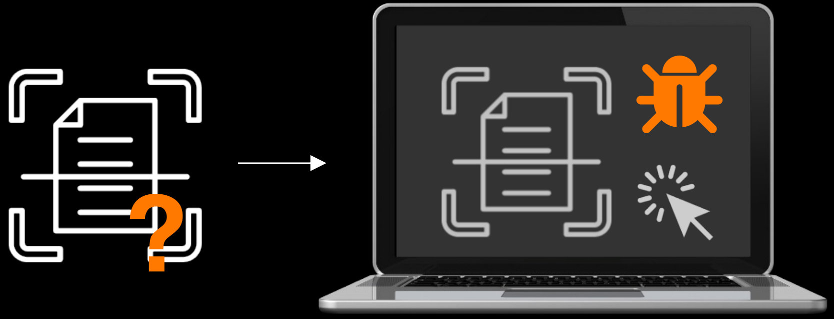
… detect malwares that are still unknown by antivirus?



Static analysis

Based on antivirus signatures

For **known threats**



Dynamic analysis

Sandbox to execute the file

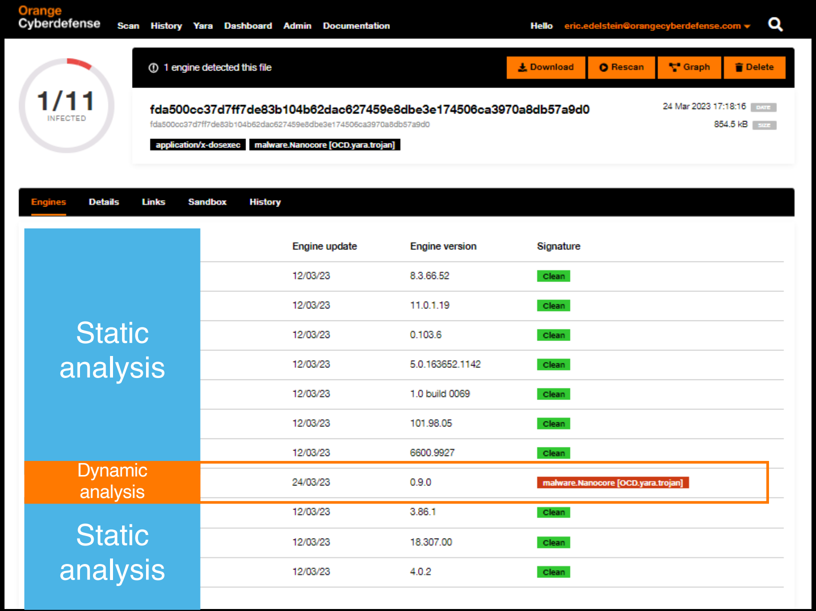
For **unknown threats**

Enhanced malware detection

Sandboxing solutions can help you detect advanced threats

… detect malwares that are still unknown by antivirus?

21/03/2023



1/11 INFECTED

1 engine detected this file

fda500cc37d7ff7de83b104b62dac627459e8dbe3e174506ca3970a8db57a9d0
fda500cc37d7ff7de83b104b62dac627459e8dbe3e174506ca3970a8db57a9d0

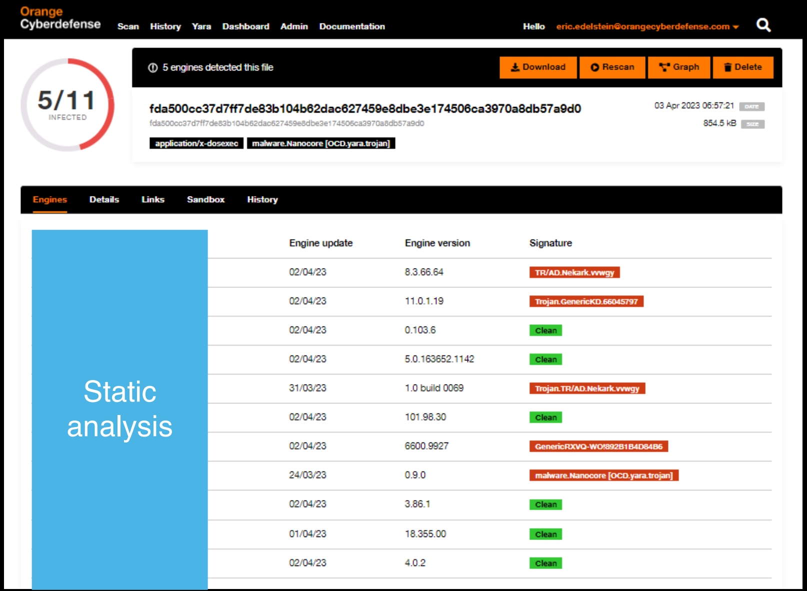
24 Mar 2023 17:18:16
854.5 kB

application/x-dosexec | malware.Nanocore [OCD.yara.trojan]

	Engine update	Engine version	Signature
Static analysis	12/03/23	8.3.66.52	Clean
	12/03/23	11.0.1.19	Clean
	12/03/23	0.103.6	Clean
	12/03/23	5.0.163652.1142	Clean
	12/03/23	1.0 build 0069	Clean
	12/03/23	101.98.05	Clean
	12/03/23	6600.9927	Clean
Dynamic analysis	24/03/23	0.9.0	malware.Nanocore [OCD.yara.trojan]
Static analysis	12/03/23	3.86.1	Clean
	12/03/23	18.307.00	Clean
	12/03/23	4.0.2	Clean

Dynamic analysis match

03/04/2023



5/11 INFECTED

5 engines detected this file

fda500cc37d7ff7de83b104b62dac627459e8dbe3e174506ca3970a8db57a9d0
fda500cc37d7ff7de83b104b62dac627459e8dbe3e174506ca3970a8db57a9d0

03 Apr 2023 06:57:21
854.5 kB

application/x-dosexec | malware.Nanocore [OCD.yara.trojan]

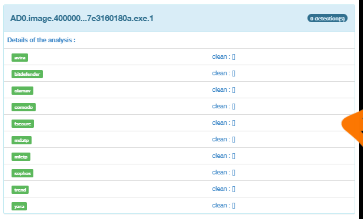
	Engine update	Engine version	Signature
Static analysis	02/04/23	8.3.66.64	TR/AD.Nekark.vvwgy
	02/04/23	11.0.1.19	Trojan.GenericKD.66045797
	02/04/23	0.103.6	Clean
	02/04/23	5.0.163652.1142	Clean
	31/03/23	1.0 build 0069	Trojan.TR/AD.Nekark.vvwgy
	02/04/23	101.98.30	Clean
	02/04/23	6600.9927	GenericRXVQ-WO!892B1B4D84B6
	24/03/23	0.9.0	malware.Nanocore [OCD.yara.trojan]
	02/04/23	3.86.1	Clean
	01/04/23	18.355.00	Clean
	02/04/23	4.0.2	Clean

Dynamic + static analysis match

Enhanced malware detection

How to detect a packed malware thanks to the dynamic analysis

… detect malwares that are still unknown by antivirus?



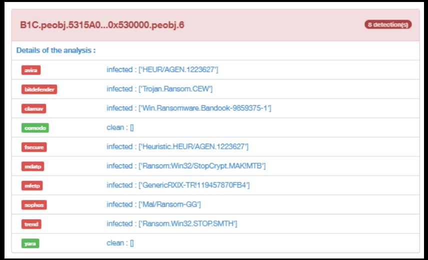
AD0.image.400000...7e3160180a.exe.1

Details of the analysis :

avira	clean : []
bitdefender	clean : []
clamav	clean : []
comodo	clean : []
fsecure	clean : []
mdatp	clean : []
mfetp	clean : []
sophos	clean : []
trend	clean : []
yara	clean : []

Strain compressed and encrypted by a packer,
Antivirus software does not detect the malicious strain.

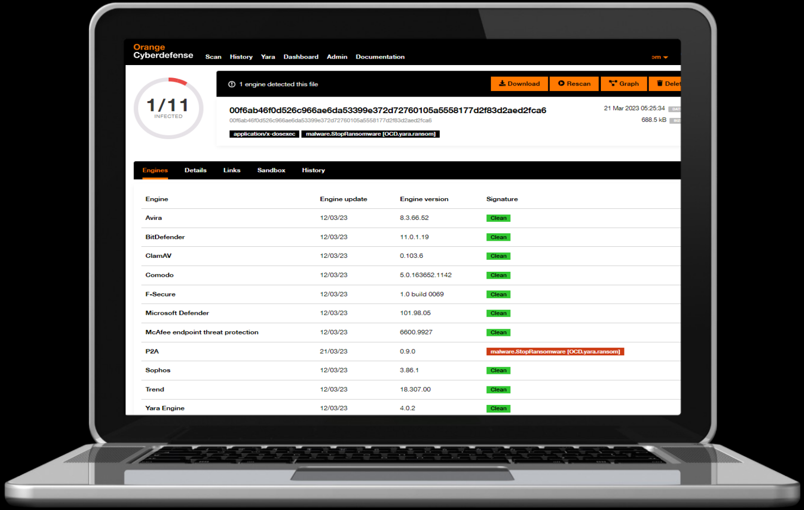
- Sandbox execution,
- In-memory decryption and decompression,
- Capture of memory snapshots for MFD detection



B1C.peobj.5315A0...0x530000.peobj.6

Details of the analysis :

avira	infected : ['HEUR/AGEN.1223627']
bitdefender	infected : ['Trojan.Ransom.CEW']
clamav	infected : ['Win.Ransomware.Bandook-9859375-1']
comodo	clean : []
fsecure	infected : ['Heuristic.HEUR/AGEN.1223627']
mdatp	infected : ['Ransom:Win32/StopCrypt.MAK!MTB']
mfetp	infected : ['GenericRXIX-TR!119457870FB4']
sophos	infected : ['Mal/Ransom-GG']
trend	infected : ['Ransom.Win32.STOP.SMTH']
yara	clean : []



1/11
INFECTED

1 engine detected this file

00f6ab46f0d526c966ae6da53399e372d72760105a5558177d2f83d2aed2fca6
00f6ab46f0d526c966ae6da53399e372d72760105a5558177d2f83d2aed2fca6

application/x-dosexec | malware.StopRansomware [OCD.yara.ransom]

21 Mar 2023 05:25:34
688.5 kB

Engine	Engine update	Engine version	Signature
Avira	12/03/23	8.3.66.52	Clean
BitDefender	12/03/23	11.0.1.19	Clean
ClamAV	12/03/23	0.103.6	Clean
Comodo	12/03/23	5.0.163652.1142	Clean
F-Secure	12/03/23	1.0 build 0069	Clean
Microsoft Defender	12/03/23	101.98.05	Clean
McAfee endpoint threat protection	12/03/23	6600.9927	Clean
P2A	21/03/23	0.9.0	malware.StopRansomware [OCD.yara.ransom]
Sophos	12/03/23	3.86.1	Clean
Trend	12/03/23	18.307.00	Clean
Yara Engine	12/03/23	4.0.2	Clean

Dynamic analysis is crucial in the process of analyzing malicious code

Enhanced malware detection

Case studies

I’m Elina Muna, CISO of an insurance company.
Employees of an insurance company are receiving a lot of attachments by email and I want to make sure that all attachments are automatically analysed before entering the internal network.
I’ve integrated the solution in my workflow using the API.

I’m Olivier Rigal, Head of the CyberSOC of a manufacturing company.
My team is doing reverse engineering on malwares and they needed an advanced tool to be more efficient.
We’re using the sandbox and are able to fully customize the testing environment and make the malware execute faster for instance.

Orange Cyberdefense