CYBERSECURITY

Orion Malware

SAFECARE event

2021/11/30

Securing Critical Business

AIRBUS

The threat of malware

As villains we have...

The WILLINGNESS

The CAPACITY

We are looking for..

The OPPORTUNITY

SODINOKIBI

EMOTET

RYUK

LOCKY

...

SOPHOS survey 2020 (2 500 companies, 26 countries)

51% of companies were hit by a ransomware

45% of attacks relied on malicious file

Ref.: https://www.sophos.com/en-us/medialibrary/gated-assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

Ransomware and Covid-related cybercrime 'biggest threats to UK security'

National Cyber Security Centre chief executive Lindy Cameron was speaking at Chatham House's Cyber 2021 Conference.

Cyber attacks hit two French hospitals in one week

Issued on: 16/02/2021 - 19:19

https://www.france24.com/en/europe/20210216-cyber-attacks-hit-two-french-hospitals-in-one-week

Foreign hacking group targets hospitals, clinics with ransomware attacks, says new report

BY NICOLE SGANGA, CATHERINE HERRIDGE, MUSADIQ BIDAR
UPDATED ON: OCTOBER 7, 2021 / 8:34 PM / CBS NEWS

https://www.cbsnews.com/news/cyberattacks-ransomware-hacking-hospitals-target-foreign-groups/

Israeli hospital hit with ransomware attack

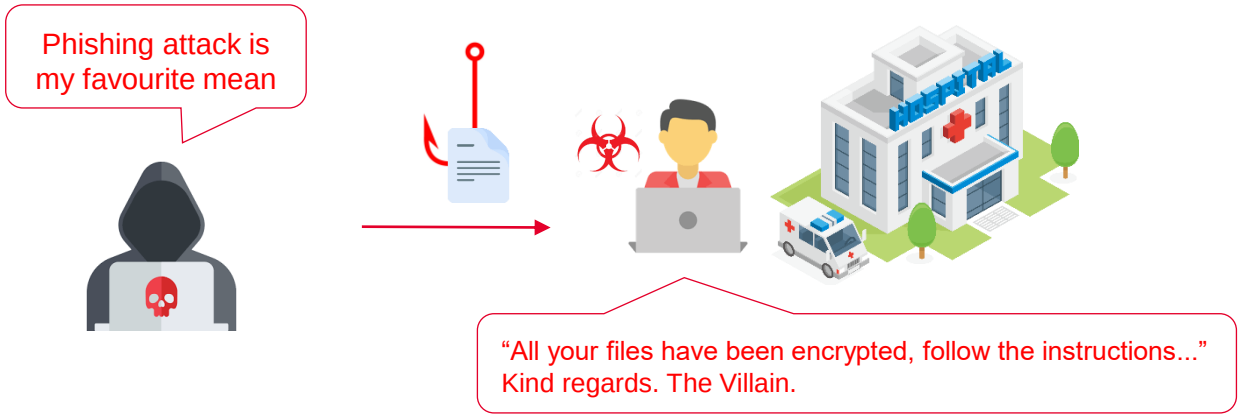
Hillel Yaffe Medical Center says it is able to keep operating, aside from non-urgent elective procedures, by switching to alternate computer systems

By STUART WINER
13 October 2021, 12:58 pm

Ref.: https://www.timesofisrael.com/israeli-hospital-hit-with-ransomware-attack/

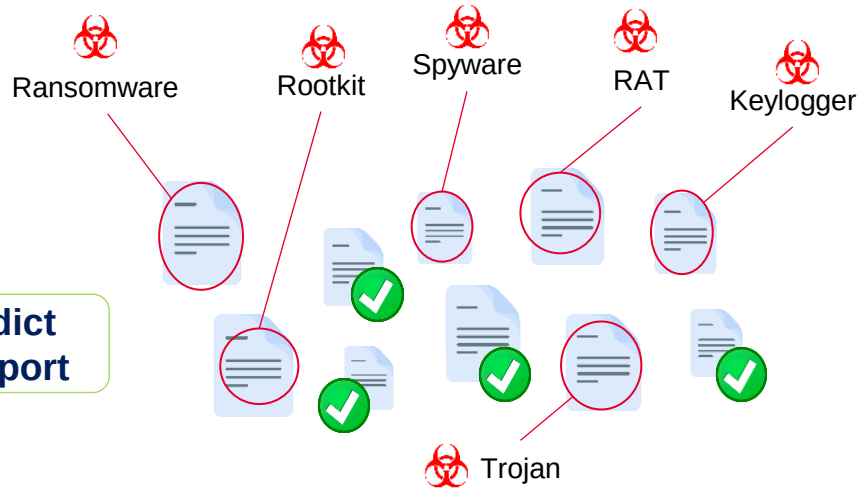
AIRBUS

Orion Malware helps you to prevent malware attacks



File

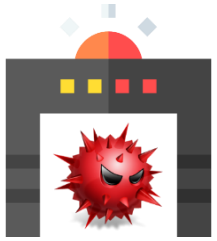
Verdict
+ Report



Orion Malware to DETECT & ANALYSE

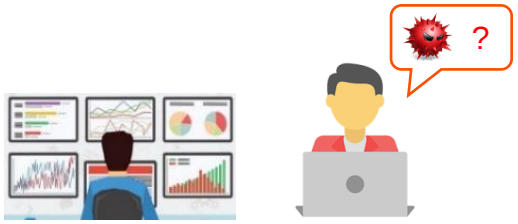
AIRBUS

Benefits of Orion Malware



DETECT MALWARE TO PREVENT ATTACKS

LEVERAGE THIRD PART EQUIPEMENT/SYSTEMS



Cybersecurity teams Users

HELP YOUR TEAMS TO MAKE THEIR DECISION

SAVE TIME

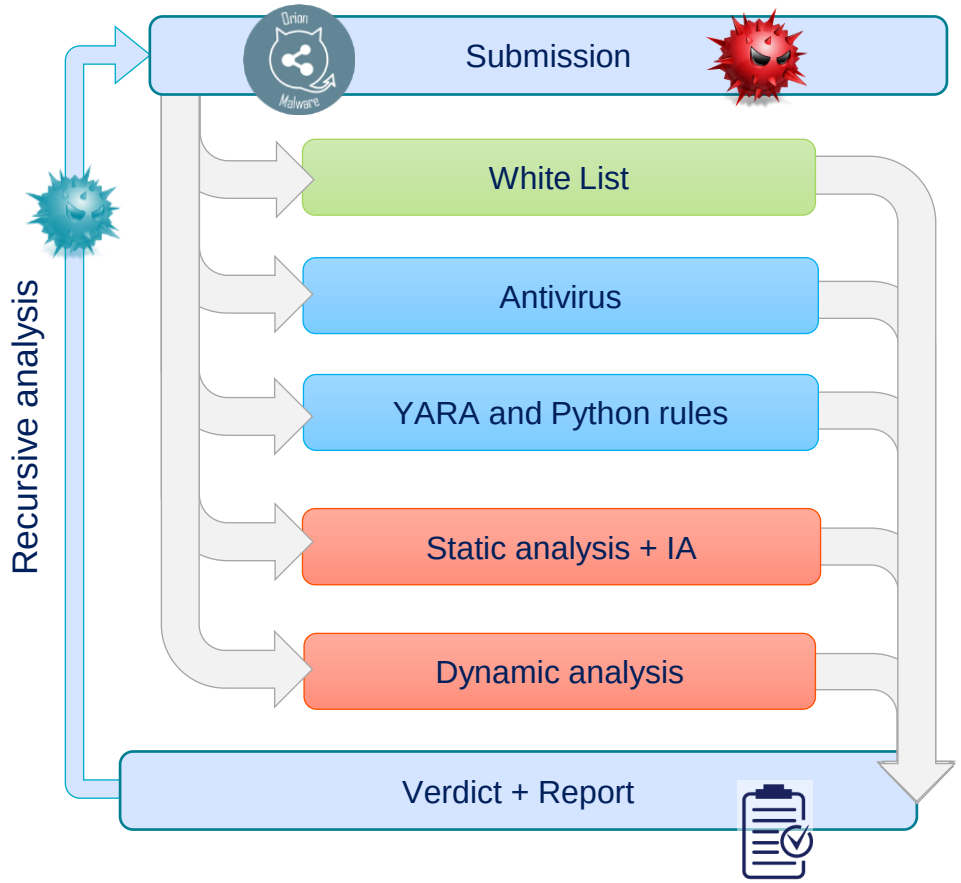
BOOST YOUR THREAT INTELLIGENCE

CUSTOM YOUR POLICY OF DETECTION

PROTECT YOUR INFRASTRUCTURE

AIRBUS

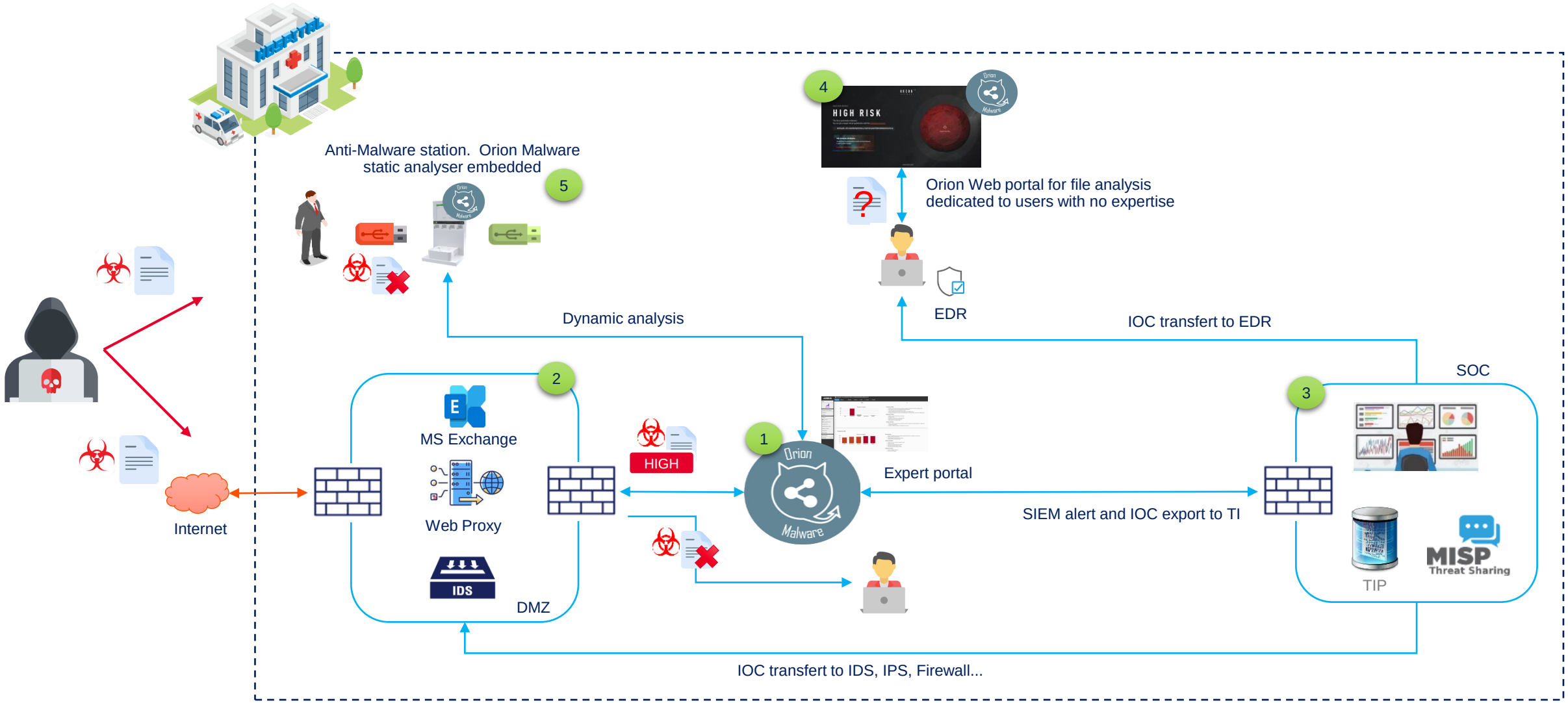
Orion Malware combines 5 static and dynamic analysis engines, heuristics and artificial intelligence



DESCRIPTION	BENEFITS
✓ Manual & automatic submissions ✓ Queueing & anti-burst	✓ Performance optimisation ✓ Low analysis redundancy
✓ NSRL files database	✓ Instant detection of **legitimate files** ✓ **False positive reduction**
✓ **5 Antivirus (**wide geographical cover)	✓ **KNOWN THREATS** detection
✓ Detection rules	✓ **KNOWN THREATS** detection
✓ AI :**Deep Learning, Machine Learning models** ✓ Heuristics ✓ **IOC** extraction	✓ **UNKNOWN THREATS** detection
✓ **Sandboxing** : Windows 10, 7, XP, Linux ✓ Anti-evasion and undetectable hooking ✓ **IOC** extraction ✓ User interaction	✓ **UNKNOWN THREATS** detection
✓ HTML, JSON, PDF formats ✓ **Mitre Att&CK** & **TimeLine** representation ✓ **Recursive analysis**	✓ **Decision** making ✓ **Tactics and technics** understanding ✓ **IOC** export

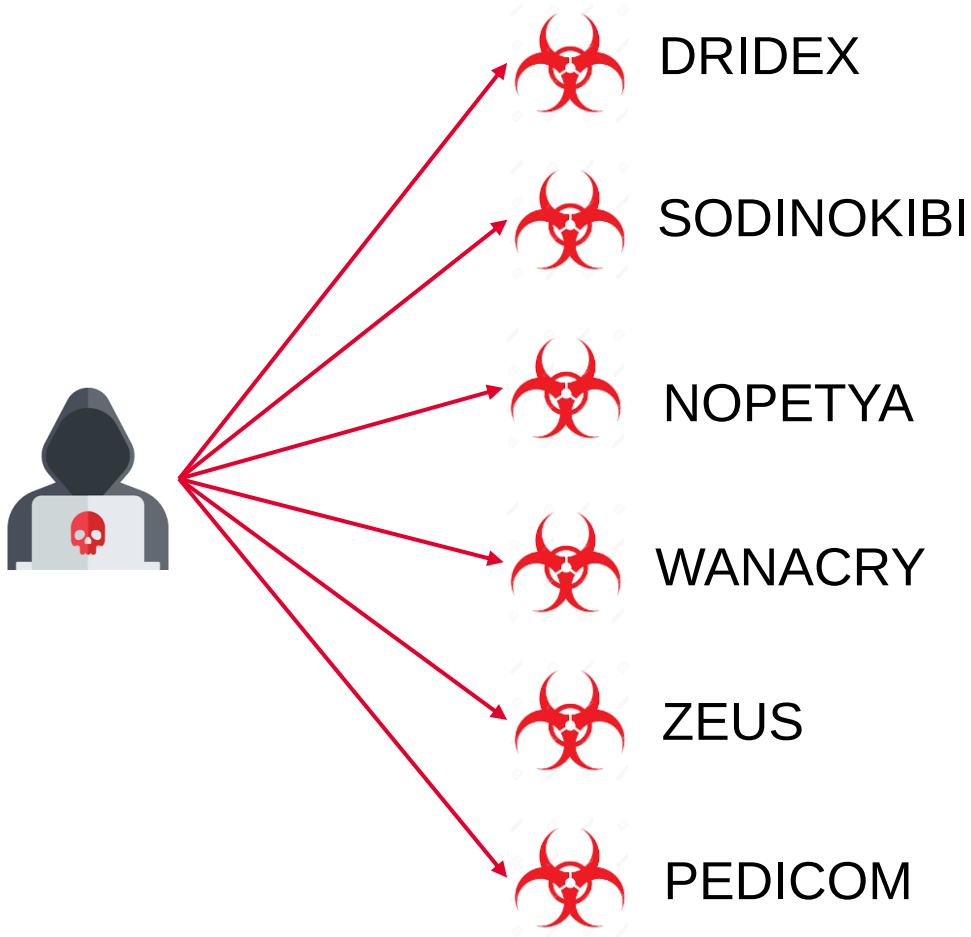
AIRBUS

Orion Malware in your context



AIRBUS

Demonstration



Orion Malware products and services

OMW Appliance

OMW SaaS

KUB & OMW

OMW Architecture to scale up and increase resilience.
Available for **Appliance** and **SaaS mode**

- ✓ Support
- ✓ Training
- ✓ Professional Services

AIRBUS

If you want to know more about Orion Malware

- Email : ewin.cannet@airbus.com

- Web site : https://airbus-cyber-security.com/
  - Menu : “Products & Service > Detect > Orion Malware”

We can provide :

- Further demonstration
- Trial period - POC

CYBERSECURITY

Thank you for attending
Your questions

This document and all information contained herein is the sole property of Airbus. No intellectual property rights are granted by the delivery of this document or the disclosure of its content. This document shall not be reproduced or disclosed to a third party without the expressed written consent of Airbus. This document and its content shall not be used for any purpose other than that for which it is supplied.

Airbus, it's logo and product names are registered trademarks.