SECURITY SUMMIT

14-15-16 marzo 2023

Security Summit

Clusit Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

L’Intelligenza Artificiale per proteggere i dispositivi da ransomware e malware

Delia La Volpe, Senior Security Technical Specialist Manager, IBM

Pier Luigi Rotondo, Security Technical Specialist, IBM

15 marzo 2023 - 14.00-14.40

IBM

Delia La Volpe

SENIOR SECURITY TECHNICAL SPECIALIST MANAGER, IBM

Pier Luigi Rotondo

SECURITY TECHNICAL SPECIALIST, IBM

MEMBRO DEL COMITATO SCIENTIFICO DEL CLUSIT

Evolving threat landscape in Europe

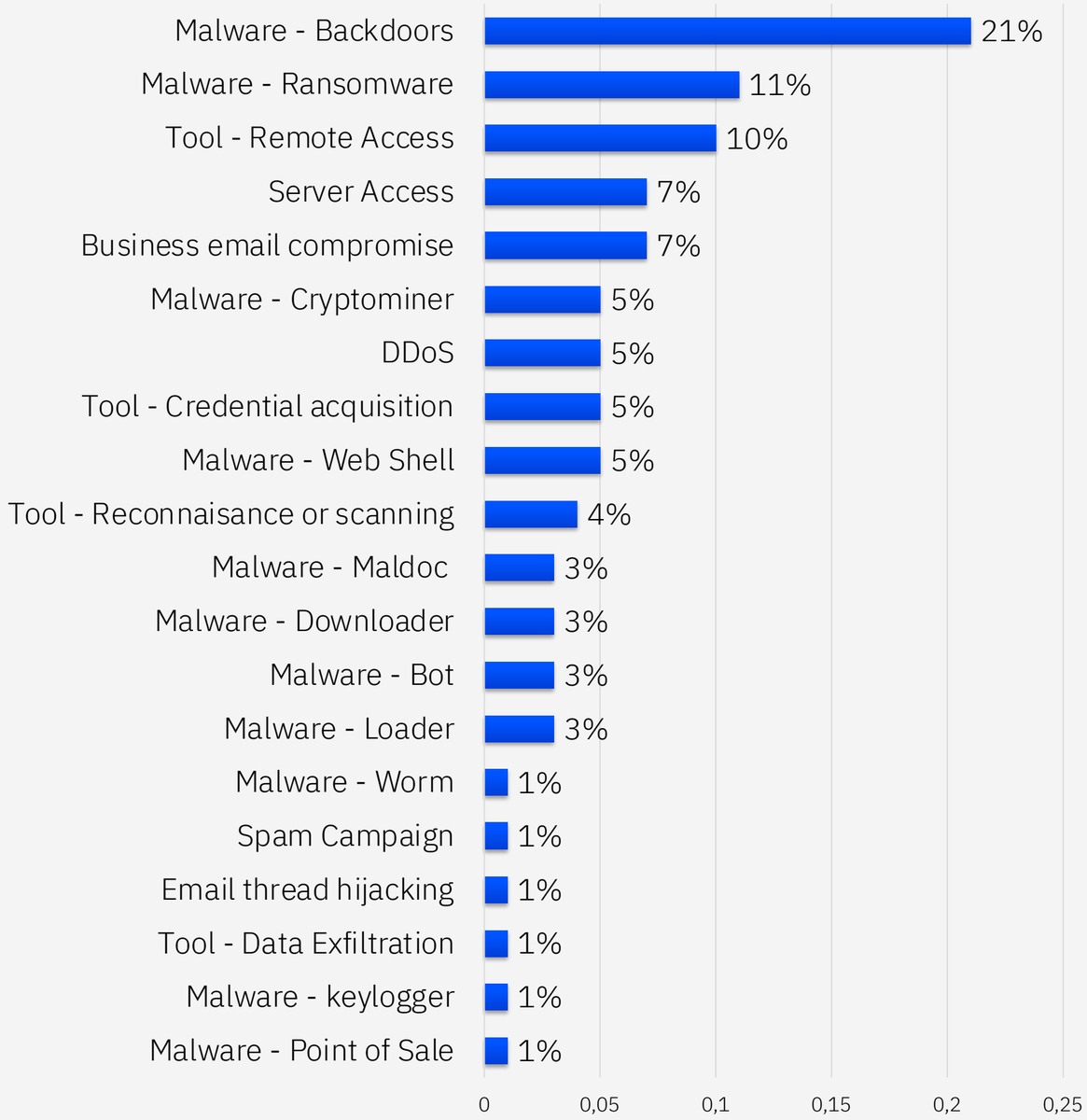
#2

Europe was the second-most attacked geography worldwide in 2022

28%

of attacks in 2022 occurred in the European region, up from 24% in 2021

Top actions on objectives



Sources: 2023 IBM X-Force Threat Intelligence Report;

Endpoint security: more timely, more challenges

- Traditional antimalware approaches rely on finding what's known (known signatures)
- Attackers target unknown (fileless/ransomware)
- Poor visibility and zero-day attacks
- Attackers are manipulating legitimate software and files to hide their presence
- Rise in complexity of malicious and automated cyber activity

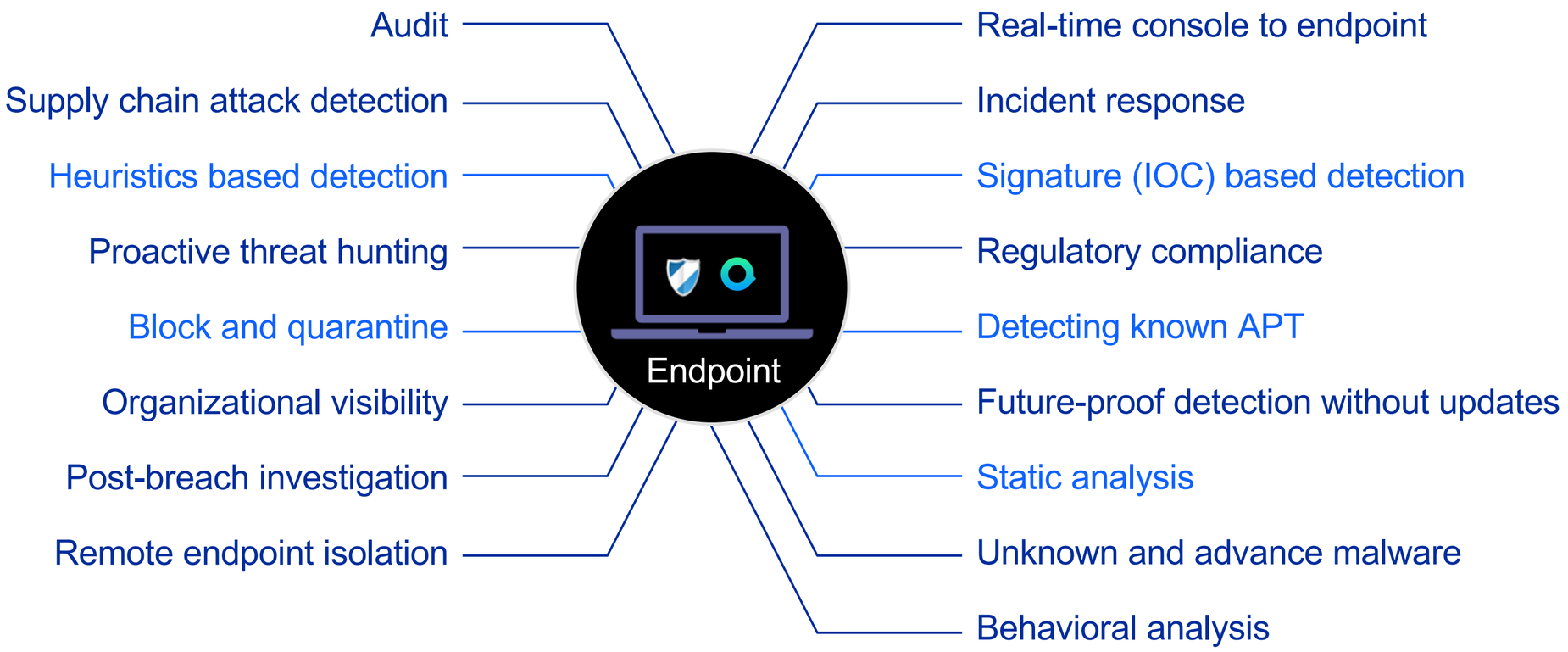
"Endpoint security continues to be one of the most requested core topic coverage areas… because the endpoint is often a target of attack, attacks becoming more sophisticated, and endpoints getting more and more diversified."

Gartner, Guide to Endpoint Security Concepts, Dec. 2020

Why Endpoint Detection & Response?

ANTI VIRUS + **BEST-IN-CLASS EDR**

Basic Protection	Behavioral Analysis	Threat Hunting	Risk and Compliance	CERT	IT Audit

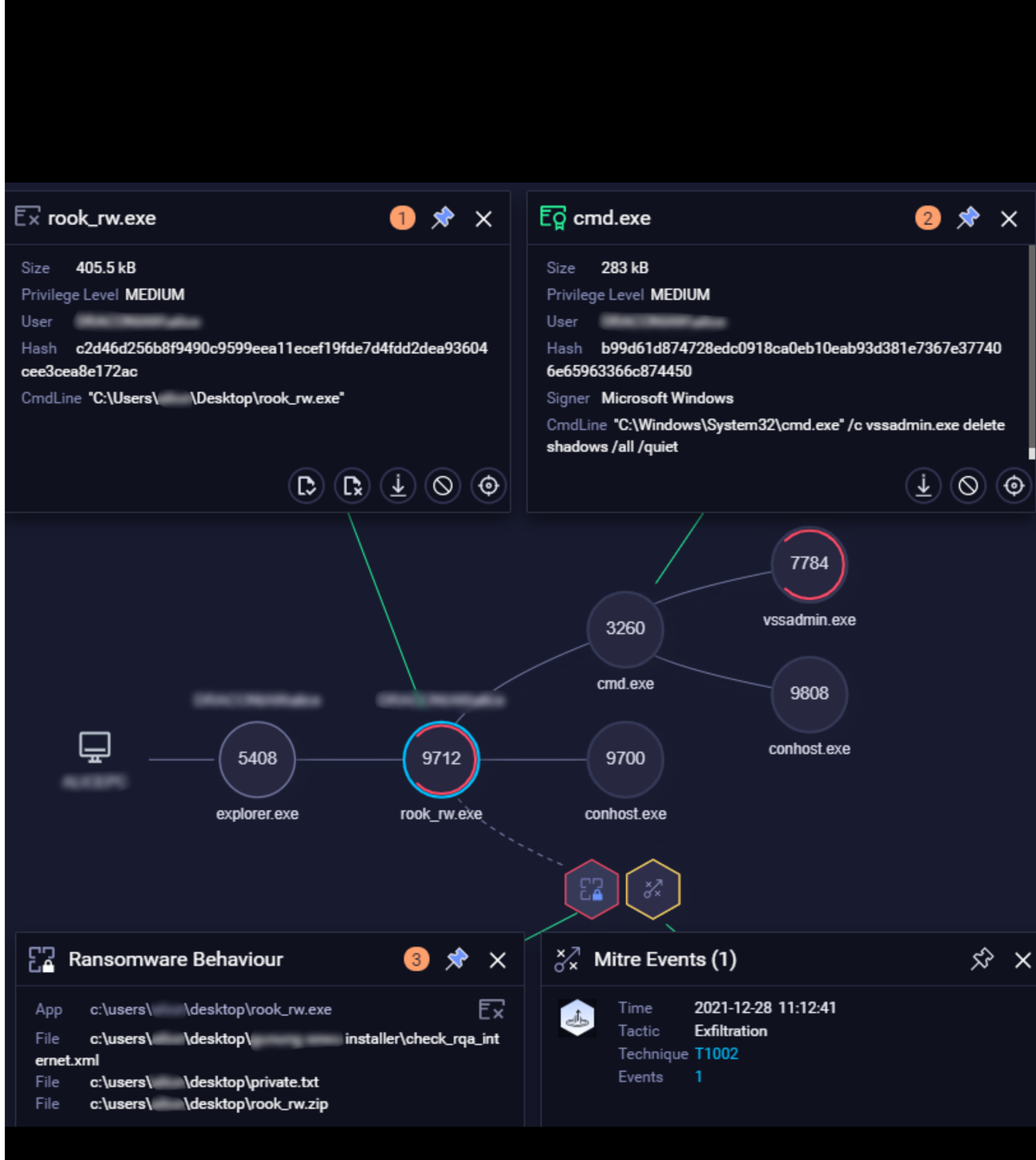


IBM Security ReaQta in action: Early detection of malware

By leveraging AI and automation directly on the endpoint, ReaQta helps in detecting a wide range of malware/ransomware and actively mitigate in near real-time

Key capabilities

- Detects unknown malware/ransomware variants using a behavioral engine
- Analyzes file activities and access, if an encryption attempt is detected and the process chain is suspicious, the process is blocked, and the encrypted files are restored in real-time



THREAT HUNT | ALERTS | ENDPOINTS | POLICIES | DESTRA | REPORTS | ADMINISTRATION

HOME | TRENDS | MITRE ATT&CK™

X-Force Red & IR | All Groups

ALERTS BY SEVERITY

Last 30 Days

ALL	HIGH	MEDIUM	LOW
28	14	9	5

ENDPOINTS

Connected	13 /16
With Alerts	10
Isolated	0

ENDPOINTS TRIGGERED MOST EVENTS

Last 7 Days

TRENDING KEY EVENTS ON PROCESSES

Last 7 Days

services.exe	230	
onedrivesetup.exe	19	11
setup.exe	7	10

EVENT DISTRIBUTION TRENDING ENDPOINTS

Last 7 Days

ENDPOINTS TRIGGERED MOST ALERTS

Last 7 Days

MOST ACTIVE ALERT CONNECTIONS

Last 7 Days

United States of America	8

APPS TRIGGERED MOST ALERTS

Last 7 Days

MACHINE TYPE DISTRIBUTION

Last 7 Days

SERVER	9
VM	4
DC	4

What makes ReaQta a different endpoint protection solution?

Undetectable by Design

NANO OS

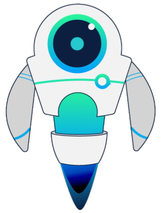
Live Hypervisor-based monitoring

Customized Threat Hunting

ADVANCED THREAT HUNTING

DeStra (Detection Strategy) scripting

Can Help Reduce False Positives by 80%+



CYBER ASSISTANT

One-shot learning system

Q&A

IL REPORT
X-FORCE THREAT INTELLIGENCE INDEX 2023
E' DISPONIBILE
AL DESK IBM SECURITY!