



IT NATION™

SECURE

hosted by  CONNECTWISE™

Acronis

MSPs on the Edge: Advanced Security with EDR

June 7, 2023



Dimitri Korahais

Senior Solutions Engineer



Justin Ceballos

Strategic Partner Executive

#CyberFit

The new world of threats



Natural disasters

- Only 6% of outages are caused by natural disasters⁽¹⁾
- Affects facilities and infrastructure



Pandemics

- Requires a different kind of planning scenario
- Affects people



Hardware failure, software corruption

Up to 30M SMBs are vulnerable to IT failure without comprehensive monitoring⁽²⁾



Accidental data deletion

14% of data loss is caused by human error, such as deleting or overwriting files⁽³⁾



Cyberattacks

- 93% of businesses were attacked within the past three years⁽²⁾
- Malware attacks increased by 25% in 2019⁽⁴⁾
- By 2021 cybercrimes will cost \$6 trillion per year⁽⁴⁾

Natural

Human

(1) Actual Tech Media, (2) IDC, (3) Tech Radar, (4) Symantec 2019 ISTR

```
uu$$$$$$$$$$$$uu
uu$$$$$$$$$$$$uu
u$$$$$$$$$$$$u
u$$$$$$$$$$$$u
u$$$$$$$$$$$$u
u$$$$$$$$$$$$u
u$$$$$$$$$$$$u
u$$$$$$$$$$$$u
u$$$$$$$$$$$$u
```

Ransomware is a type of malicious software used by cybercriminals that is designed to **extort money from their victims**, by

- **Encrypting data** on the disk
- **Blocking access to the system**
- **Exfiltrating data**

```
u$$$$uu$$$$$$$$uu **$$$$$$$$$$$$uu$$$$
$$$$$$$$$$$$*** **$$$$$$$$$$$$*
*$$$$* **$$$$**
$$$* PRESS ANY KEY! $$$*
```

The threat landscape is becoming more complex



80%

of companies reported to have been attacked in H2, 2021



57%

of attacks are missed by traditional antivirus solutions



69%

of MSPs spend more time managing tools than defending against threats

Sources: Acronis Cyberthreats Report 2022, Acronis Cyber Readiness Report, 2020, FBI

What if you could rely on just one integrated solution?



Cut
cyber protection
costs by up to 50%



Boost
your monthly
recurring revenue



Deliver
unmatched cyber
protection

Advanced Security – Quick Overview

A complete endpoint security solution to protect various types of workloads, based on a combination of classic signature-based engine as well as next-gen set of modern technologies

Full-stack endpoint security

Acronis Active Protection (Anti-ransomware), enhanced with exploit prevention, URL filtering, anti-malware detection for backed-up data, and improved detection rate to catch more threats faster

Security automation and management

Smart protection plans, auto-allow list custom apps, automatic malware scans, and AV definitions updates as part of the recovery process help deliver services effortlessly

Integrated with backup & DR

Immediate data recovery in case of ransomware attack as well as backup capabilities within forensic data brings unique value-added functionality and fastest time-to-recovery

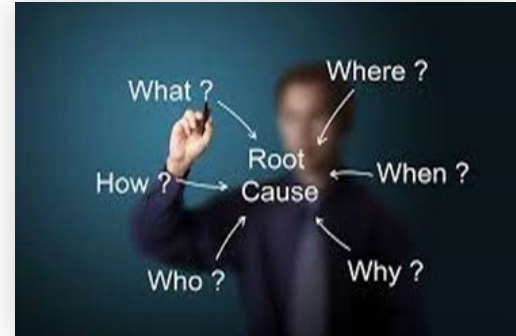
What is EDR?

EDR (Endpoint Detection and Response)

is an event correlation security platform, capable of identifying **advanced threats or in-progress attacks** – and then doing something about it.

Gartner - Primary EDR capabilities:

- Detect security incidents
- Contain the incident at the endpoint
- Investigate security incidents
- Provide remediation guidance



The need for EDR



Only advanced security can combat advanced attacks

More than 60% of breaches **involve some form of hacking**

On average, it takes organizations **207 days** to identify a breach



Breach is inevitable – you need to be prepared

70 days to contain a breach

USD 4.35 million – average total cost of a data breach

76% of security and IT teams struggle with **no common view** over applications and assets



For many – compliance is mandatory

Regulations require organizations to **report security incidents** within a strict time-frame – e.g. 72 hours for GDPR

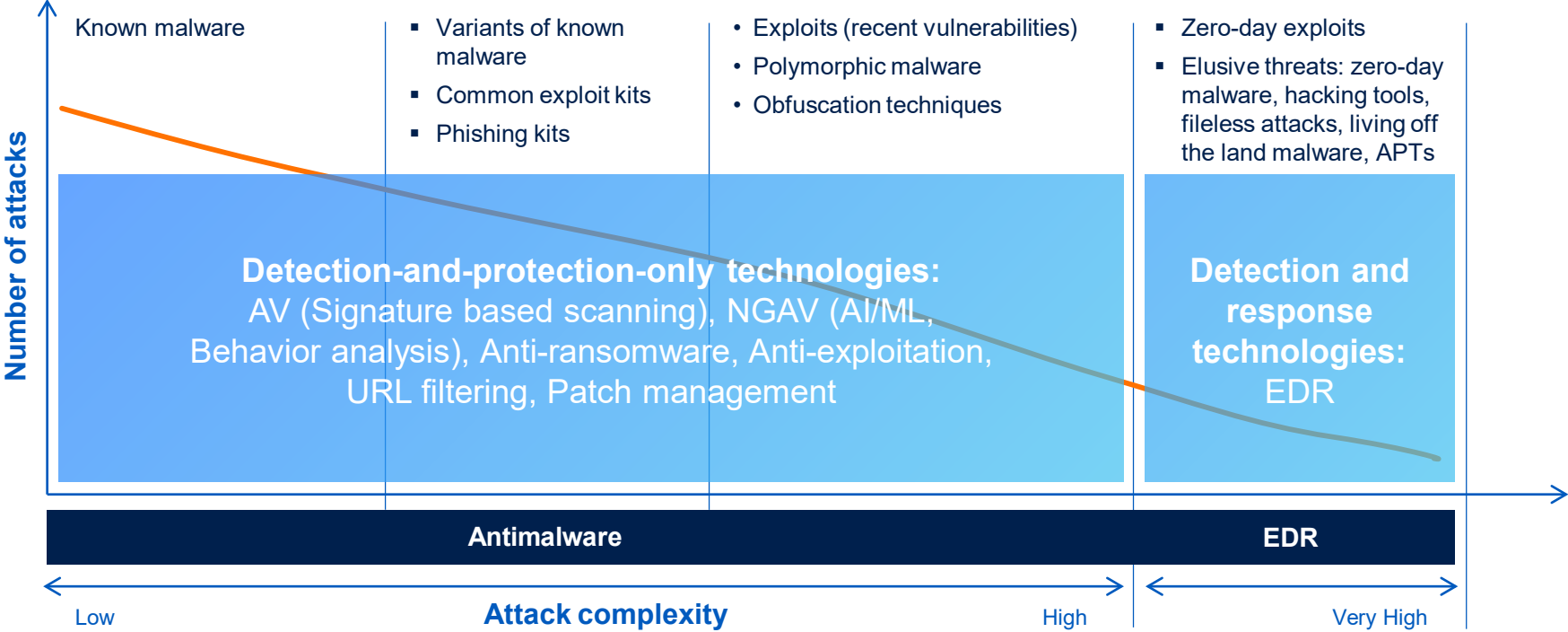
70% of breaches involve PII (post-incident analysis required for reporting for regulatory purposes)

Sources: "Data Breach Investigations Report", Verizon, 2022"; "Cost of data breach report", 2022, IBM Security & Ponemon Institute; "Costs and Consequences of Gaps in Vulnerability Response," ServiceNow, 2020, Investigation or Exasperation? The State of Security Operations", IDC

Comparing Antimalware vs EDR

Category	Antimalware	EDR
Focus	Block/prevent attack	Post-incident detection and response
Detection Technology	Detects and stops “ known bad ” files, processes or behaviors	Detects “ intent ” by <i>correlating a series of actions</i> an attacker performs to be successful at achieving its objective
Visibility into attacks	Low Shows only detected and blocked threats.	High – broader scope of incidents Maps steps of the attack to show: <ul style="list-style-type: none">• How did it get in?• How did it hide its tracks?• What did it harm?• How did it spread?
Response capabilities	Automatically blocks “known bad” processes and quarantines threats	Provides response capabilities to: <ul style="list-style-type: none">• Contain the incident at the endpoint• Investigate security incidents• Provide remediation

How EDR helps to protect against threats



Acronis Advanced Security + EDR Functionality

1 Rapid attack prioritization and analysis

2 Integrated remediation options

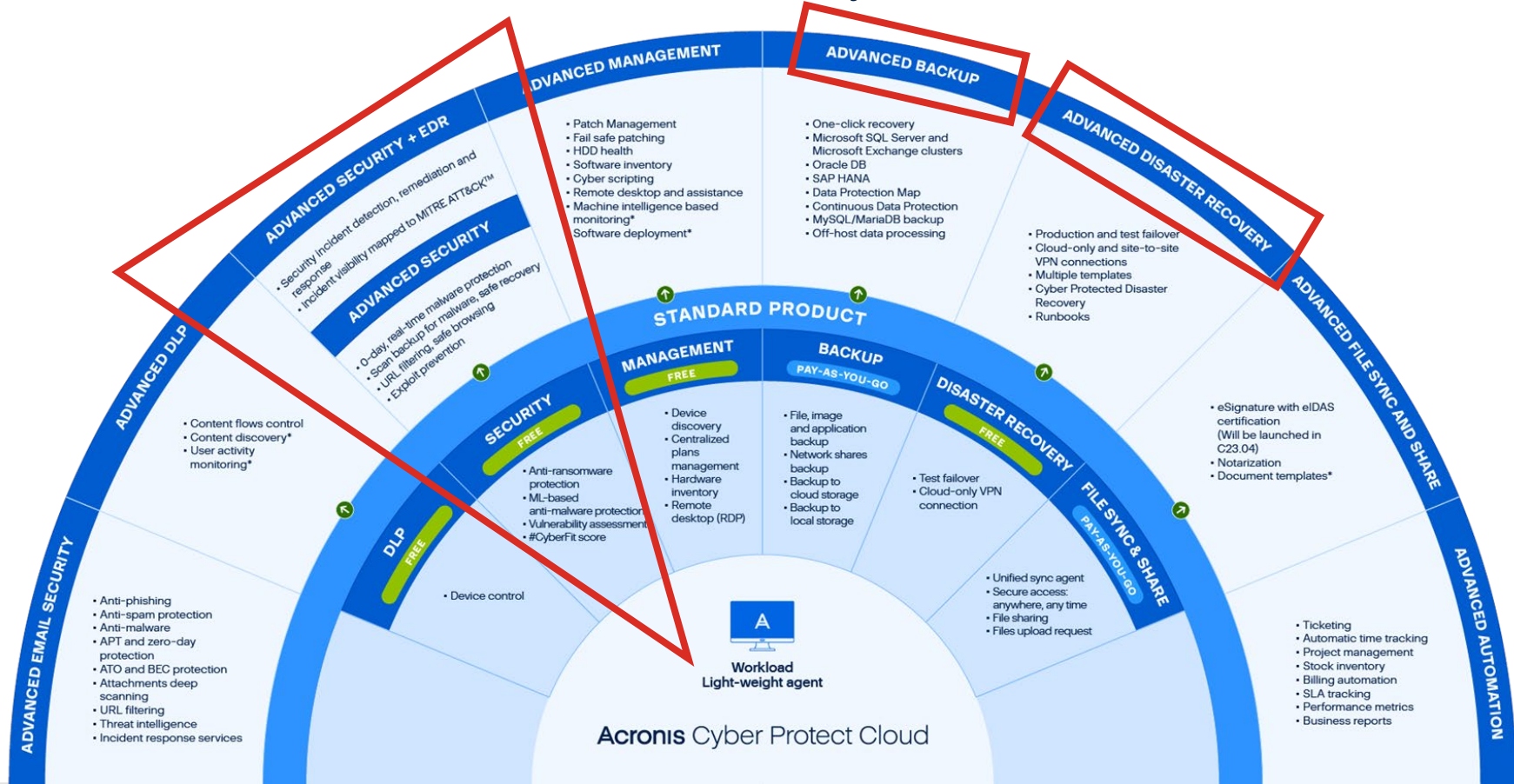
3 Unified scalable platform

The screenshot displays the Acronis Advanced Security + EDR interface for an incident analysis. The top navigation bar shows the incident status as 'Mitigated' with a severity of 'MEDIUM'. The incident was created on Jan 01, 2022, at 01:59:59:000 AM +02:00 and updated on Jan 01, 2022, at 01:59:59:000 AM +02:00. The investigation state is 'Investigating' and the priority level is '1.2 / 10'. There are options to 'Post comment' and 'Remediate entire incident'.

The main area is divided into several sections:

- Legend:** A list of categories and their counts: Workload (1), Process (10), File (51), Domain (51), Registry (6), Involved (43), Suspicious activity (20), Malicious threat (14), and Incident trigger (60).
- Attack stages:** A list of stages with their counts: Execution (0), Defense Evasion (0), Command And Control (0), and Collection (0).
- Attack Stages Details:**
 - Execution:** Jun 15, 2021, 09:38:11:374395 AM +03:00. User pbeesly, with standard privileges, on workload SCRANTON, executes a suspicious file (cmd_3akak.exe).
 - Defense Evasion:** Jun 15, 2021, 09:38:11:374395 AM +03:00. To trick user pbeesly, the file was masquerading as a benign doc file, by the name (rcs3akak.doc).
 - Command And Control:** Jun 15, 2021, 09:38:11:374395 AM +03:00. To control workload SCRANTON, once (cmd_3akak.exe) is executed, a TCP connection is established on an unusual port 1234 to a unknown domain 192.168.0.5.
 - Collection:** Jun 15, 2021, 09:38:52:669601 AM +03:00. The adversary collects files containing sensitive information credit card numbers, social security numbers and more from ServUsersPROFILE and compresses them into an archive (draft.zip) via a powershell script.
- Activity Flow Diagram:** A central diagram showing the sequence of events: 'SCRANTON' (Create process) leads to 'cmd_3akak.exe' (Create process), which leads to 'cmd.exe' (Create process), which leads to 'powershell.exe' (Create process). The 'powershell.exe' process then performs several actions: 'Create file' (Draft.zip), 'Set registry value' (powershell.exe), 'Create file' (mankey.png), 'Create process' (csrsshost.exe), 'Create process' (cmd.exe), 'Set registry value' (powershell.exe), 'Create process' (powershell.exe), and 'Set registry value' (powershell.exe).
- Process Details (powershell.exe):** A detailed view of the powershell.exe process, showing its type (Process), name (powershell.exe), PID (7156), state (Running), path (C:\Windows\System32\WindowsPowerShell\v1.0), command line (powershell), username (pbeesly), integrity level (MDS), and MD5 (7353F60B1739074EB17C5F4D06F239).
- Security analysis:** A section providing an overview of the security analysis, including the verdict (Suspicious activity), severity (MEDIUM), file found on (10 Workloads), attack objective (Collection), techniques (T1560), reason of detection (Suspicious Activity - unknown process collects files containing sensitive information and compresses them into an archive), and detection date (Jun 15, 2021, 09:38:51:983576 AM +03:00).
- Reputation:** A section showing the reputation of the file, including VirusTotal (Go to VirusTotal, Score: 3.57 / 10, Last seen: Jun 28, 2021, 08:45:23:111 AM +02:00) and Google (Go to Google).

EDR as Part of Acronis Cyber Protect Cloud



Builds on functionalities of Advanced Security



Next-generation anti-malware:
Prevent threats with signature- and behavior-based endpoint protection



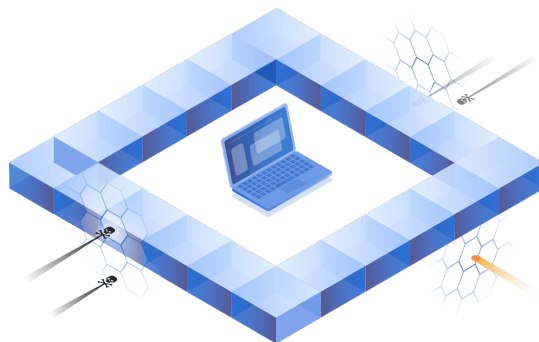
URL filtering: Extend cyber protection to web browsing to prevent attacks from malicious websites



Exploit prevention:
Reduce the risks of exploits and malware taking advantage of clients' software vulnerabilities



Smart protection plans: Auto-adjust patching, scanning and backing-up based on threat alarms from Acronis Cyber Protection Operations Centers



Forensic backup:
Enable forensic investigations by collecting digital evidence in image-based backups



Better protection with fewer resources:
Protect backups against malware and enable more aggressive scans by offloading data to central storage, including the cloud



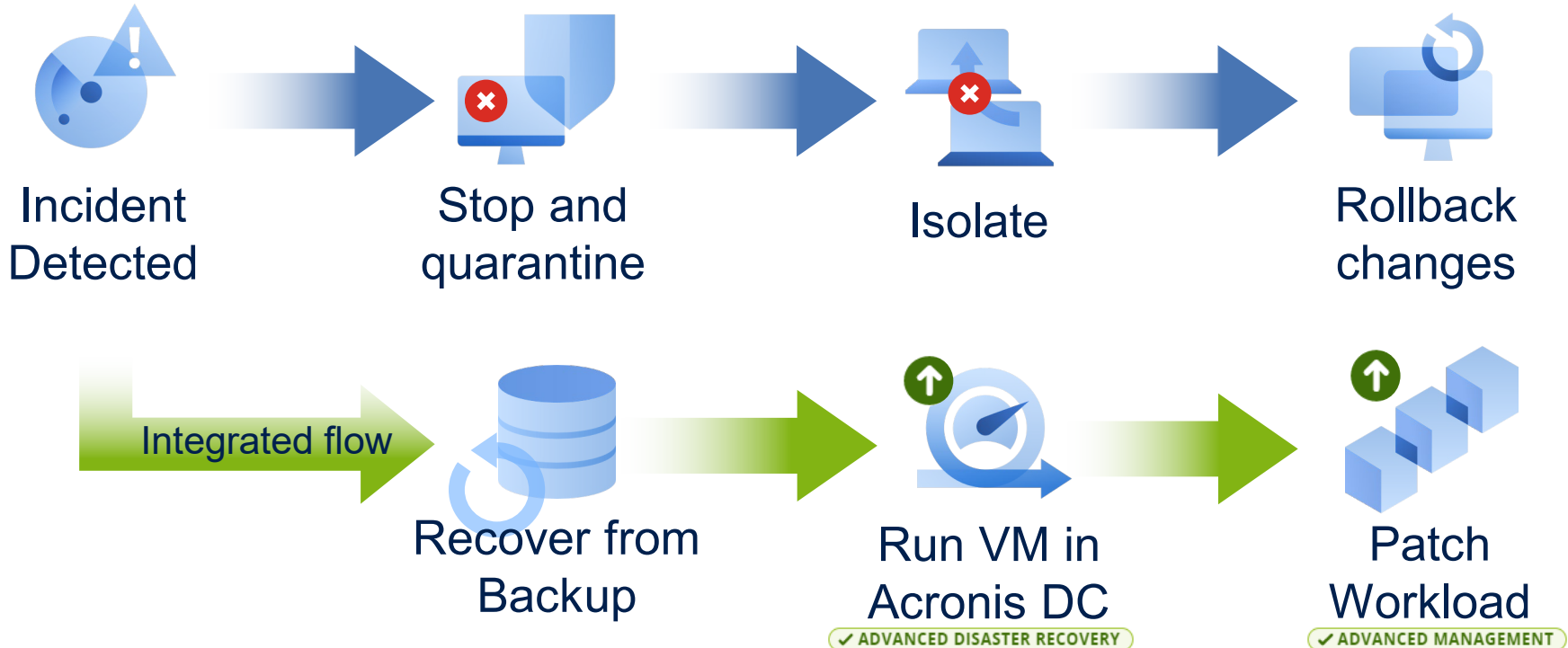
Safe recovery:
Prevent threat recurrence by integrating anti-malware scans of backups and antivirus database updates into the recovery process



Global and local allowlists:
Created from backups to support more aggressive heuristics, preventing false detections

Respond & Remediate

Take advantage of Integrated flow



Analyze attacks in minutes

Analyze attacks with ease and speed:

- **Prioritized visibility of suspicious activities** across endpoints – not a flat list of all alerts
- **Visibility into the attack chain evolution** – mapped to the MITRE framework
 - How did it get in?
 - How did it hide its tracks?
 - How did it cause harm?
 - How did it spread?
- **Save money and time**
Reduce need for specialized training and expertise

Incidents > 6

Threat status: **Mitigated** (yellow) | Severity: **Medium** (orange) | Created: Jan 01, 2022, 01:59:59:00 AM +02:00 | Updated: Jan 01, 2022, 01:59:59:00 AM +02:00 | Investigation state: **Investigating** (blue) | Positively resolved: 1.2 / 1.0

CYBER KILL CHAIN | **ACTIVITIES**

Legend: Workload, Process, File, Domain, Registry, Involved, Suspicious activity, Malicious threat, Incident trigger

Attack stages

- **Execution**
 - Jun 15, 2021, 09:38:11:374395 AM +03:00
User pbeesly, with standard SCRANTON, executes a suspicious file **[?jcod.3aka3.scr]**
- **Defense Evasion**
 - Jun 15, 2021, 09:38:11:374395 AM +03:00
To trick user pbeesly, the file is masquerading as a benign doc file, by the name **[rcs.3aka.doc]**
- **Command And Control**
 - Jun 15, 2021, 09:38:11:374395 AM +03:00
To control workload SCRANTON, once **[?jcod.3aka3.scr]** is executed, a TCP connection is established on an unusual port 1234 to a unknown domain 192.168.0.5
- **Collection**
 - Jun 15, 2021, 09:38:52:669601 AM +03:00
The adversary collects **[*.doc,*.xps,*.xls,*.ppt,*.pps,*.wps,*.wpd,*.ods,*.odt,*.lwp,*.jtd,*.p...]** files containing sensitive information credit card numbers, social security numbers and more from \$env:USERPROFILE and compresses them into an archive **[draft.zip]** via a powershell script

powerShell.exe

OVERVIEW | SCRIPTING ACTIVITIES (71) | RESPONDED

Security analysis

Verdict: **Suspicious activity** (orange)

Severity: **Medium** (orange)

File found on: **13 Workloads**

Attack objective: **Collection**

Techniques: **11960**

Reason for detection: **Suspicious Activity - unknown process collects files containing sensitive information and compresses them into an archive**

Detection date: Jun 15, 2021, 09:38:51:983796 AM +03:00

Reputation

VirusTotal: [Go to VirusTotal](#)
Score: **> 5.7 / 10**
Last seen: Jun 28, 2021, 08:45:23:111 AM +02:00

Google: [Go to Google](#)

Details

Type: **Process**

Name: **powerShell.exe**

PID: **7156**

State: **Running**

Path: **C:\Windows\System32\WindowsPowerShell**

Command Line: **powershell**

Username: **pbeesly**

Integrity level: **System**

MCS: **7353F6081739074B817C3FD0D0FE239**

Stop the breach

- Investigate further using remote connection and forensic backup
- Contain threats: Isolate the machine from the network
- Remediate: Kill malware processes, quarantine threats, and roll back changes.
- Prevent recurrence: Apply matches and block analyzed threats from execution
- Ensure business continuity: Use integrated recovery capabilities, including attack-specific rollback, file- or image-level recovery, and disaster recovery

Select actions and take action with a single click.

Remediate entire incident ✕

Analyst verdict
 True positive False positive

Remediation actions

- Step 1 – Stop threats
Stops all processes related to the threat.
- Step 2 – Quarantine threats
After being stopped, all malicious or suspicious processes and files are quarantined.
- Step 3 – Rollback changes
Rollback first deletes any new registry entries or files created by the threat (and any of its children threats). Next, rollback reverts any modifications made by the threat (or its children) to the registry and/or files existing on the workload prior to the attack.
Affected items: [Show \(4\)](#)

Recover workload
If any of the above selected remediation steps fail completely or partially.

Recover workload from backup Disaster recovery failover

Recovery point: [Select](#)

Items to be recovered: Entire workload

Prevention actions

- Add to blocklist**
Adds all threats from the incident to the blocklist in the selected protection plans. This action will prevent these threats from future executions.
Protection plan: [EDR protection plan \(Active on "WIN-H8EDQLM611"\)](#)
- Patch workload**
Prevents further attacks by patching software that contain vulnerabilities used by attackers in order to get a foothold on the workload.
- Change investigation state of the incident to: Closed**

Comment

Acronis EDR demo

Advanced Security + EDR: Top 4 use cases



Detect and block attack before breach

- **Monitor and correlate events** on endpoints
- **Block common threats** with award-winning endpoint protection
- **Detect advanced threats** and analyze in minutes



Respond before damage is done

- **True business continuity** with pre-integrated recovery
- **Reduce impact** – quarantine processes, isolate workloads
- **Limit attack surface** for future protection



Enable compliance and cyber insurance

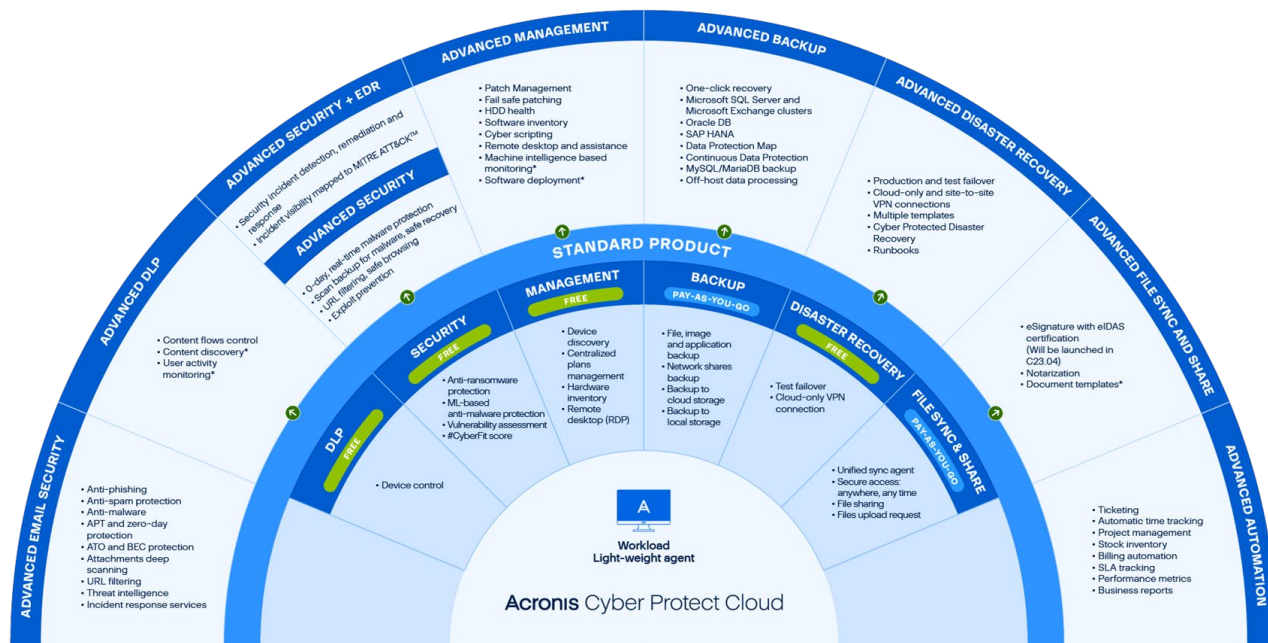
- **Report on incidents across endpoints** based on MITRE ATT&CK®
- **Classify sensitive data**
- **Collect forensic data** in backups



Consolidate solutions

- **Rapidly launch & scale through** an MSP-class platform
- **Reduce costs with** unified service management

Best-in-breed backup combined with integrated security and management



Optimize for every workload

Rapidly launch services

Consolidate vendors

Q&A

Visit Acronis Booth 504 for an in-depth demo!

Acronis Cyber Foundation

Building a more knowledgeable future

**Create, spread and protect
knowledge with us!**

- Building new schools
- Providing educational programs
- Publishing books

www.acronis.org

#CyberFit



Don't forget to fill out your

SESSION SURVEY