

United Americas
Partner Conference 2025

Incident Response

From chaos to control

kaspersky



Fernando Andreazi

United Americas
Partner Conference 2025



“ Once upon a time...

There was a company that had the best security solutions:

- EDR with 99.9% detection rate.
- MDR/XDR service in place.
- Most awarded SIEM on the market.
- Anti-spam solution powered by AI.
- Strong password policies.
- Backups in place.
- Fully hardened servers and services.

Let's start with a little story

And then there was Bob, a system administrator.

Username: admin

Password: Manager@2025!



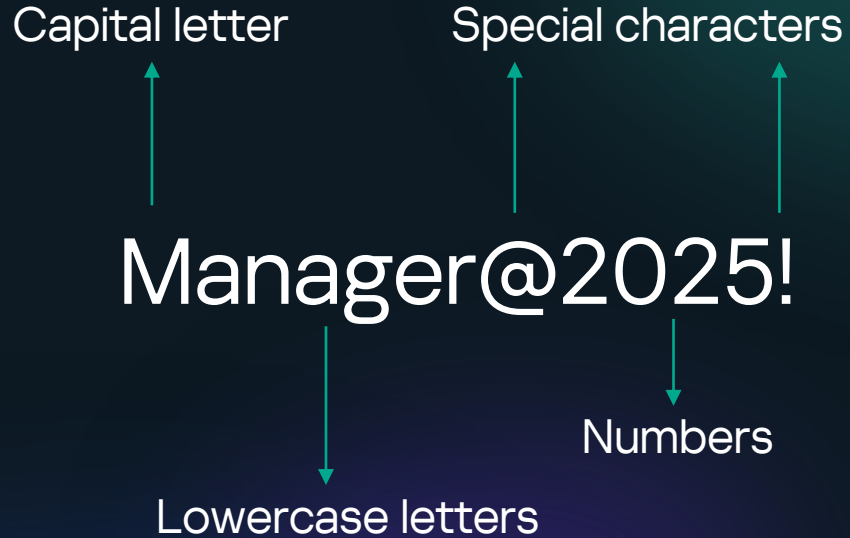
Wait, but you said the company
has strong password policies.

Strong is different from predictable.

A password can, at the same time, follow the best practices and still be guessable.

Let's start with a little story

7



Time to crack:

Manager@2025!

~ **3 hours**

IAmTheBestSysAdminInTheWorld

~ **523 million years**

In a ordinary day an incident occurs

It is Friday night and Bob receives a notification about servers with high I/O and CPU usage.

Bob started analyzing the systems.

The AV was disabled and everything was encrypted.

Bob immediately contacts the information security team.

The InfoSec team rapidly identify the source of the attack.

RDP connection from 45[.]9[.]148[.]99

Username: admin

Password: Manager@2025!

Incident containment

Several measures were adopted to contain and recover from the incident.

The malicious IP was blocked.

Backups were in place, so little information was lost.

A decryptor was available due to an algorithm flaw in the malware.

All passwords in the network were changed.

After 2 days...

All systems were stable ✓

The little information that was lost was recovered ✓

Passwords are now stronger and guessable terms are not allowed anymore ✓

Months passed by, the company was proud on how the handled the incident.

They were sure that similar situations would be handled even faster.

And then, another incident occurs

Similar patterns were identified, including the ransomware family.

However...

Many more systems were infected this time.

Backups were erased.

The previously used decryptor is not working anymore.

What went wrong this time?

Actually, we need to understand
what went wrong in **the first time**.

Recapitulating...

The malicious IP was blocked.

All passwords in the network were changed.

Backups were in place, so little information was lost.

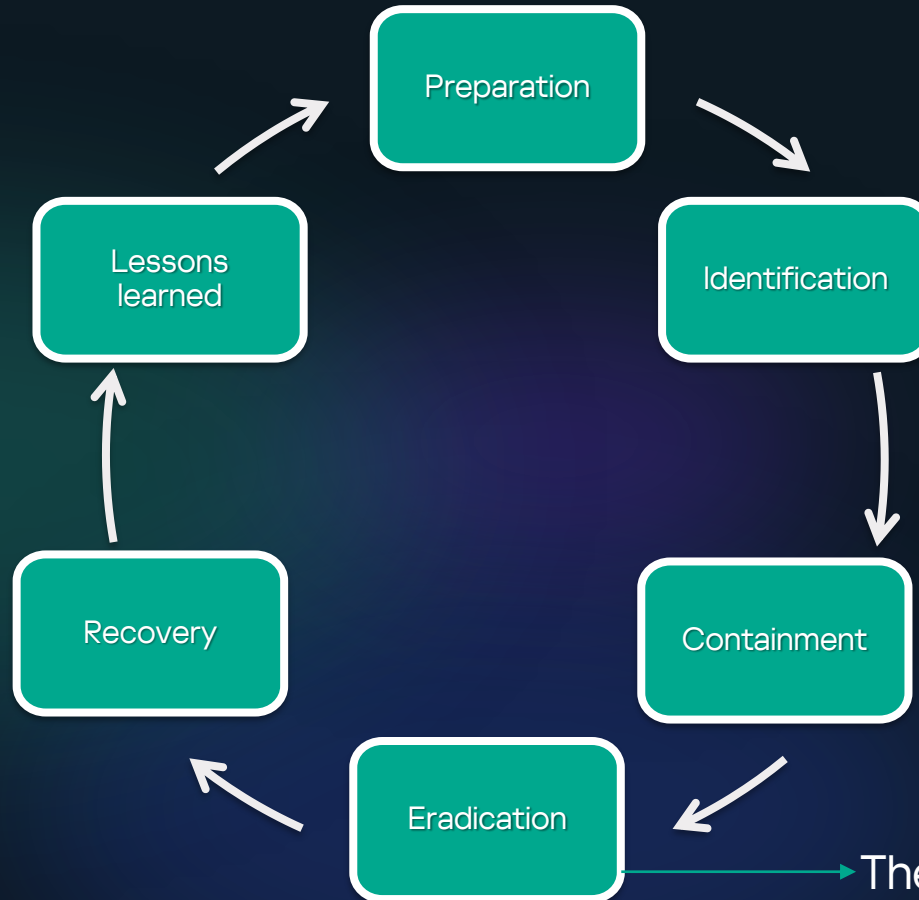
A decryptor was available due to an algorithm flaw in the malware.

So what failed?

The company missed crucial phases of incident response and started directly from the containment phase.

Let's start with a little story

18



They started here!

What they should have done?

Preparation: Map all assets, develop an IR plan.

Identification: Scope all machines infected by the attacker.

Containment: Isolate affected systems to prevent further spread.

Eradication: Remove the root cause of the incident.

Recovery: Restore systems to normal operation.

Lessons learned: Update the IR plan and apply improvements.

They decided to call Kaspersky and we:

Identified that the attacker was inside the network since the **first incident**.

He performed **lateral movement** to infect other machines and stay hidden.

The second ransomware execution had the encryption algorithm **fixed**.

The adversary was able to **exfiltrate sensitive information** to sell on the dark net.

In summary, improper IR procedures can lead to:

Delayed detection of threats, allowing the attackers more time to cause damage.

Incomplete containment, resulting in continued compromise or lateral movement.

Greater data exfiltration or corruption, increasing the impact on operations.

Loss of critical evidence, making forensic investigation difficult.

Failure to address root causes, resulting in persistent threats.

Reputational damage, eroding customer trust and stakeholder confidence.

Incident response statistics

In-depth analysis of cyberattacks

Key findings from Kaspersky's incident response report

United Americas
Partner Conference 2025



Geography of Kaspersky incident response service in 2024

Europe
11%

Americas
10%

Africa
5%

Russia and CIS
51%

Middle East
16%

Asia Pacific
7%





Industrial

24%



Government

16%



Financial

13%

Reasons for IR service in Americas:

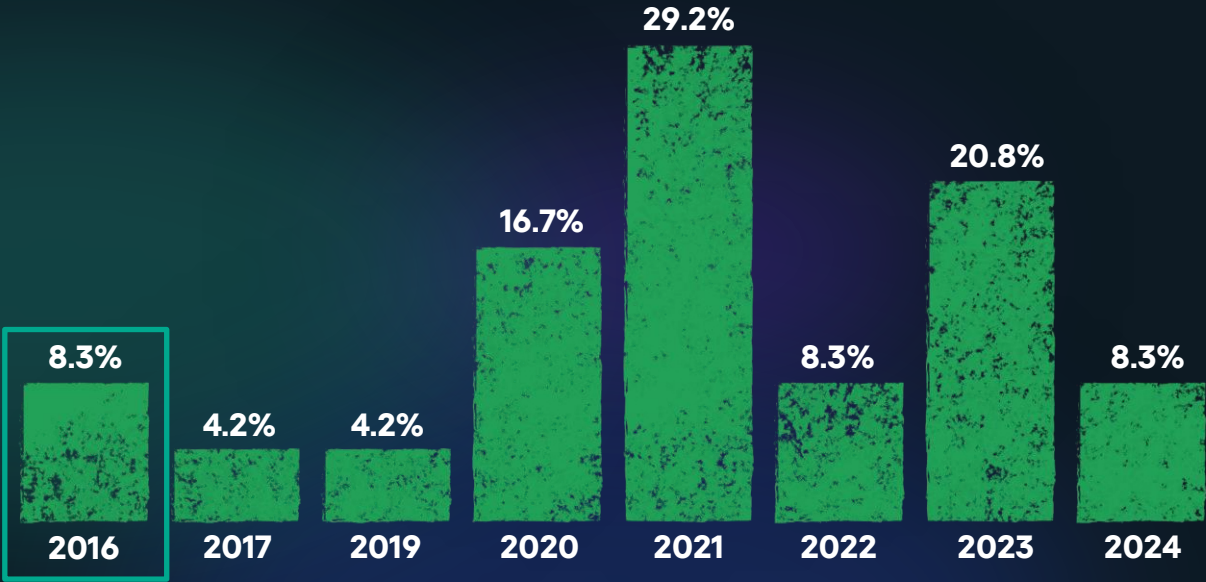
Encrypted files.

Unauthorized access.

Suspicious endpoint activities.

Suspicious network activities.

Vulnerabilities used:



Duration of attacks:



Rush

(hours and days)

44.5%

0 days

33h of IR



Average

(weeks)

20.3%

13 days

40h of IR



Long lasting

(Months)

35.2%

253 days

50h of IR

APT activities:



Industrial enterprises, financial and government institutions were **the most targeted by APTs**

APT activities:

APTs and targeted campaigns were responsible for **26.3%** of all attacks.

Third of that couldn't be attributed to specific known groups (stressing the **specially-crafted attacks**).

Frequent tools used by attackers:

Frequent, 8–22%

mimikatz psexec
softperfect network scanner
ngrok anydesk

Average, 4–8%

procdump powershell
impacket adrecon gs-netcat
advanced port scanner chisel
advanced ip scanner netscan.exe

Rare, 1–4%

bloodhound processhacker
nmap nssm lazagne
diskcryptor remcom
wmic gmer.exe

Incident response services by the GERT



Distributed team with world wide presence.

We speak different languages:
English, Russian, Spanish, Portuguese,
Arabic, French, Italian.

United Americas
Partner Conference 2025







File



Hash sum



URL, IP address, domain



Malicious
object



Analysis



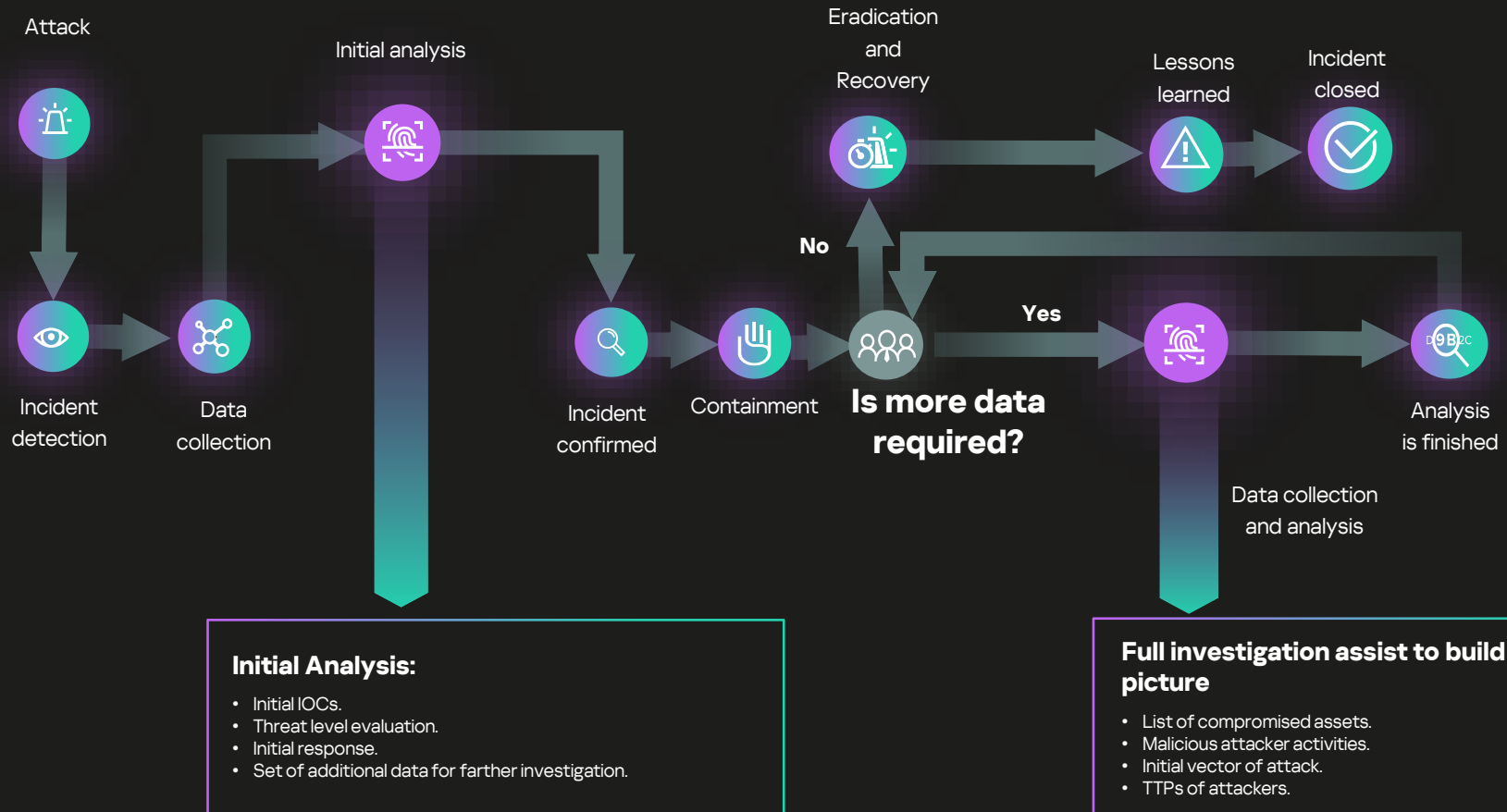
Report

Report contains:

- Metadata.
- Activities on file system.
- Network activities.
- Malicious behavior.
- Artifacts on the system.
- Recommendations for disinfection and recovery.

The process of investigation

35





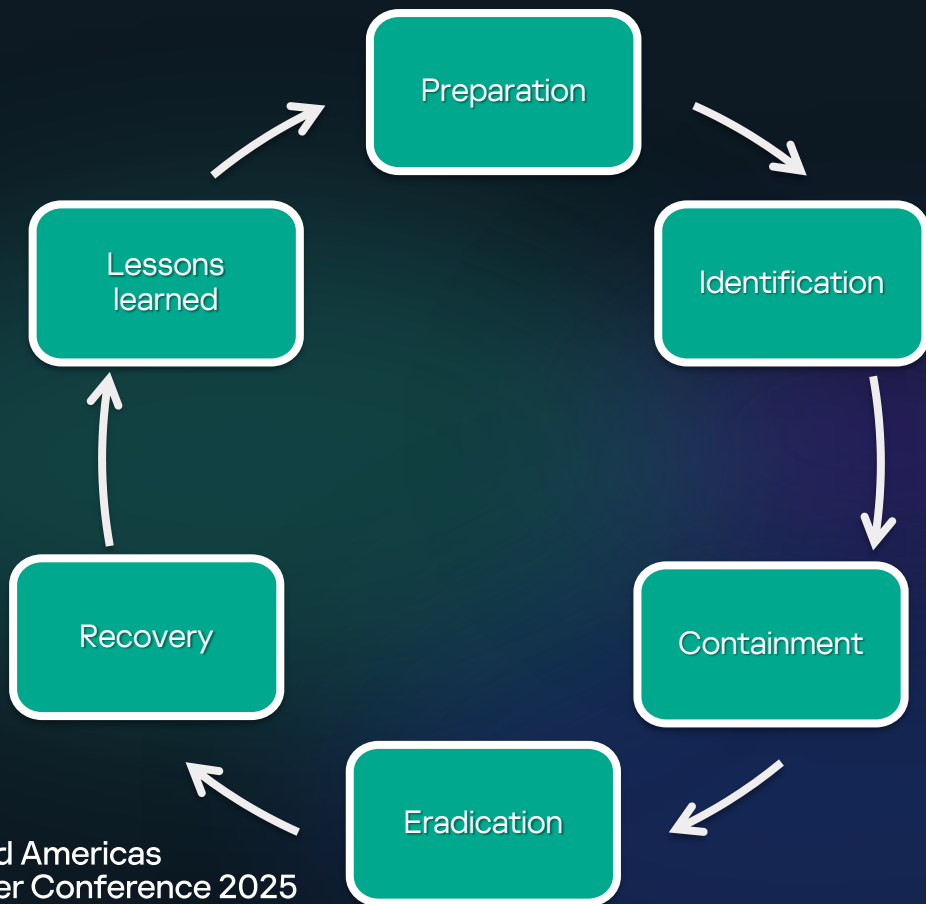
Incident Response Emergency

- No SLA.
- No allocated budget.
- No signed NDA and contract.
- No allocated resources in IR team.
- Unknown processes for response.
- Long reaction time.
- Big impact.



Incident Response Retainer

- SLA 24x7.
- All business docs signed.
- Ready to go IR team.
- Fast reaction time.
- Minimal impact.



Our services follow the best practices established by **NIST 800-61** and **SANS**.

Intelligent-driven incident response:

- Threat lookup.
- Crimeware intelligence reporting.
- Threat data feeds.
- ICS intelligence reporting.
- Digital Footprint Intelligence.
- Research sandbox and attribution engine.

Other services provided by GERT:

- Tabletop Exercises (TTX).
- Expert trainings.
 - Digital Forensics.
 - Incident Response.

Myths and fears:

“If we don’t have Kaspersky, we can’t hire the service.”

“I can’t install Kaspersky, so I won’t hire the IR service.”

“The reports are only in English.”

“I don’t need this; we don’t deal with anything that critical.”

“We’ve already investigated internally and don’t believe there’s any ongoing activity.”

“I don’t know how to collect evidence, I need someone on-site.”

Want to train your team?

Kaspersky Expert Trainings

Want user awareness?

Kaspersky Automated Security Awareness Platform

Want to simulate an incident?

Tabletop Exercise (TTX)

Want a SOC?

Managed Detection and Response (MDR)

An incident occurred?

Incident Response / Digital Forensics

Have a suspicious file?

Ask the analyst

General recommendations

United Americas
Partner Conference 2025

- ✓ Implement a robust password policy and multifactor authentication.
- ✓ Remove management ports from public access.
- ✓ Adopt secure development practices to avoid insecure code in production environments.
- ✓ Establish a zero-tolerance policy for patch management or compensation measures for public-facing applications.
- ✓ Ensure that employees maintain a high level of security.

- ✓ Implement rules for the detection of pervasive tools used by adversaries.
- ✓ Conduct frequent, regular compromise assessment activities.
- ✓ Employ a security tool stack with EDR-like telemetry.
- ✓ Constantly test reaction times of security operations with offensive exercises.
- ✓ Prohibit the use of any software being used within the corporate network that's listed as being used by adversaries.

- ✓ Back up your data.
- ✓ Work with an Incident Response Retainer partner to address incidents with fast SLAs.
- ✓ Implement strict security programs for applications with PII.
- ✓ Implement security access control over important data with DLP.
- ✓ Continuously train your incident response team to maintain their expertise and stay up to speed with the changing threat landscape.

“

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

Sun Tzu

Thank you!

Check our annual IR report at:



kaspersky

