

Breach response case study

Public sector company

# Enterprise falls to Ryuk ransomware



**Atos**

Ransomware is dangerous, complex, and constantly evolving. But it can be stopped.

In this incident, the organization was compromised by a ransomware attack because they had a low-security profile, no MFA, improper segmentation, no security monitoring, and no in-house security talent or a managed security vendor to fill the gaps in their defense.

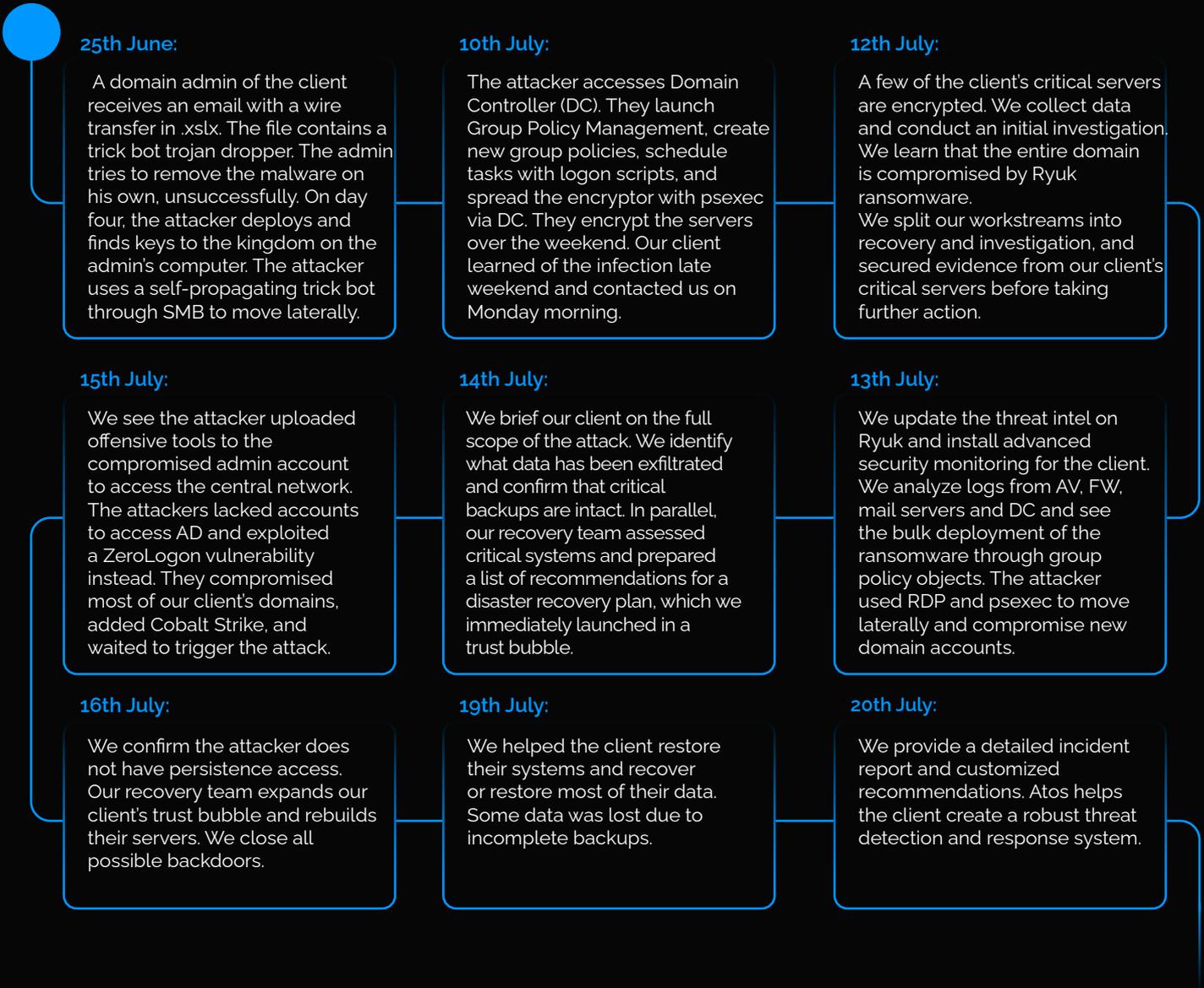
Thankfully, we could still respond successfully to this incident and stop the attack before they suffered significant harm.

To show you how we stopped this attack and how you could too, we will outline:

- A detailed timeline of the incident and our response
- How to successfully prevent, detect, and respond against attacks like this
- How you can develop the ability to stop attacks like this

## What happened: Timeline of the attack and our response

Here's what happened during the attack and how we evicted the attacker.



## Lessons learned: How to stop this attack

To keep your organization safe against attacks like this, you must take a few fundamental actions:

### Prevention

- Establish Multi-Factor Authentication and Zero Trust segmentation
- Perform fundamental security hygiene and vulnerability management
- Close unnecessary connections from high-risk attack pathways, such as SMB
- Establish and maintain comprehensive security monitoring tools
- Maintain complete and timely backups of all critical data
- Develop in-house security talent or contract. 24x7 MSSP or MDR provider

### Detection

- ◇ Don't ignore commodity malware and threats
- ◇ Use MDR and EDR for TTP monitoring
- ◇ Focus on Active Directory to prevent lateral movement
- ◇ Combine threat intelligence, threat hunting, auto-containment, and SOC
- ◇ Establish visibility into your supply chain and manage it
- ◇ Ensure proper logging to perform an effective investigation
- ◇ Be aware of your threat landscape

### Response

- Maintain an incident response playbook and perform tabletop exercises
- Create a crisis team and streamline communication channels with stakeholders
- Use trusted bubbles and build a recovery on top of the investigation
- Accelerate breach containment and management with a mature CMDB and asset management process
- Prepare and test your backup and recovery plan before a breach
- Implement post-incident recommendations from your IR team

## An ounce of prevention: Prepare to stop this attack ransomware

These security lessons are simple, but they can be challenging to bring to life. This is why Atos has put together a comprehensive framework for Ransomware defense aligned to the NIST framework. You can download this complimentary e-book here: <https://atos.net/en/lp/ransomware-defense-2022>

To learn more about Atos security solutions, Schedule a no-obligation consultation with an Atos Digital Security expert and begin to build or augment your ransomware defense.



# About Atos

Atos is a global leader in digital transformation with 112,000 employees and annual revenue of c. € 11 billion.

European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries.

A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients.

Atos is a SE (Societas Europaea), listed on Euronext Paris and included in the CAC 40 ESG and Next 20 Paris Stock indexes.

The [purpose of Atos](#) is to help design the future of the information space.

Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

[Find out more about us](#)

[atos.net](https://atos.net)

[atos.net/career](https://atos.net/career)

Let's start a discussion together



For more information: [breachresponse@atos.net](mailto:breachresponse@atos.net)

Atos is a registered trademark of Atos SE, August 2022.  
© Copyright 2022, Atos SE. Confidential Information owned by Atos group, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval of Atos.