Ransomware attack: lessons learned

Francesco De Luca (CISSP®) – CSI-RT
We are one of the most important Italian tech companies.

We create digital services for public administrations, used daily by citizens and businesses.
A COMPLETE OFFER OF INFRASTRUCTURES, NETWORKS AND SERVICES

- certified data centre TIA-942 Rating 3
- certified cloud service
- regional CSIRT team accredited
- regional connectivity network
- smart data platform for big data that is unique in Italy
How do we protect our data?

DEFENSE IN DEPTH
DEFENSE IN DEPTH

several layers of defense
  • technology
  • human resources
  • operations
DEFENSE IN DEPTH
Uses technical controls such as

• Intrusion detection/protection systems
• Web application firewalls
• Configuration management
• Web scanners

• Two-factor authentication
• Timed access
• Virtual private networks
• At rest encryption
To be continued...
Ransomware attack: lessons learned

Dedicated to those who have not experienced a ransomware attack.

Paolo Cravero – CSI-RT
In previous attacks we handled user accounts that had fallen victim of CryptoLocker on local disks and mounted network drives (2014). Our first large-scale ransomware attack was in 2021.

The victim has a hybrid configuration:

- Email platform in cloud, no visibility
- Internal Network devices, no visibility
- Firewalls, partly managed by us
- Active Directory, managed by us
- Endpoint Security, managed by us
• Both commercial vendors and free platforms monitor Internet-facing systems for risk vectors like
  • TLS/SSL configurations
    • Insecure protocols SSLv2, SSLv3, TLSv1.0, TLSv1.1
    • Weak TLS cipher suite
  • Unpatched or Outdated Systems
  • Open and unsecured ports
  • Missing security Web Application Headers
• Other services offer reports of outgoing traffic towards malicious IPs
• Those sources are extremely useful to assess and reduce your exposure! But they were not enough ...
So, how did they get in?

• RCE? No. 0-day? No. CVE exploit? No.
• Through **ONE** stolen RDS credential.

The Human Factor bypassed k€/k$/k£ worth of defense technologies.

Then the actor followed step-by-step the Conti playbook (that was already available as OSINT source).
From the analysis of lateral movement and the attack timeline we learned that:

• The first use of stolen credentials was two days before the weekend break (Thursday or Wednesday depending on your geolocation)

• Reconnaissance took place during working hours.

• Encryption was finally launched on Saturday evening.
• Ever heard the statistic that a % of servers is «forgotten» every year? Well, that applies to endpoints, too!

• When you handle 10k seats, even 1%/year means a lot!

• First systems to be exploited were «personal – under the desk – servers» powered up 24/7

• Followed by other endpoints running 24/7
  • Because they had to (think of a public safety service)
  • Because of lazy assignee (and they waste electricity)

• Attacker’s success was the combination of weekend and unattended EP
Lessons from the Reaction Phase.

- Monday, 8AM: first reports of inaccessible files. Within 30 minutes the spread was stopped.

- Work From Home was a plus:
  - No limits to the number of expertise that can be involved in matter of seconds, no need for everyone to get to the office building.
  - 20+ people around a table but only one speaks, no background noise from sidetalks (that occur in text or in separate chats).
  - But the information gets spread across several chats: use your own notepad, better if tamper-resistant pen & paper!
Lessons from the Reaction Phase.

• The reaction task force was composed of senior IT staff with 10+ experience within our company and customers:
  • We knew the infrastructure by heart: any lookup is much faster in human memory than searching on a tool (and cannot be compromised)
  • Customer’s AD infrastructure was scheduled for update as part of the continuous evolution of IT
  • Everyone knew his/her role; some hatchets were buried

• Years long relationship with our customers allowed us to limit temporarily their operations (Human Factor, again 😊)

• Enterprise-grade backups greatly limited the damage 💡
Prevention from further attacks.

• Need to develop a sixth-sense for anomalies in user activities
• Re-evaluate the importance of existing alerts
• Ingest more logs and build meaningful alerts on top of them
• Do red&blue team training and activities as there are many free resources available
• Define what OSINT to monitor and adopt CLOSINT source(s)
Thank you for your attention!

You can reach us at csirt@csi.it

CSI-RT of CSI Piemonte – Torino – Italy