Stealing Identities and Privilege Escalation

The Real-World Story of a Ransomware Attack

identiverse

#identiverse

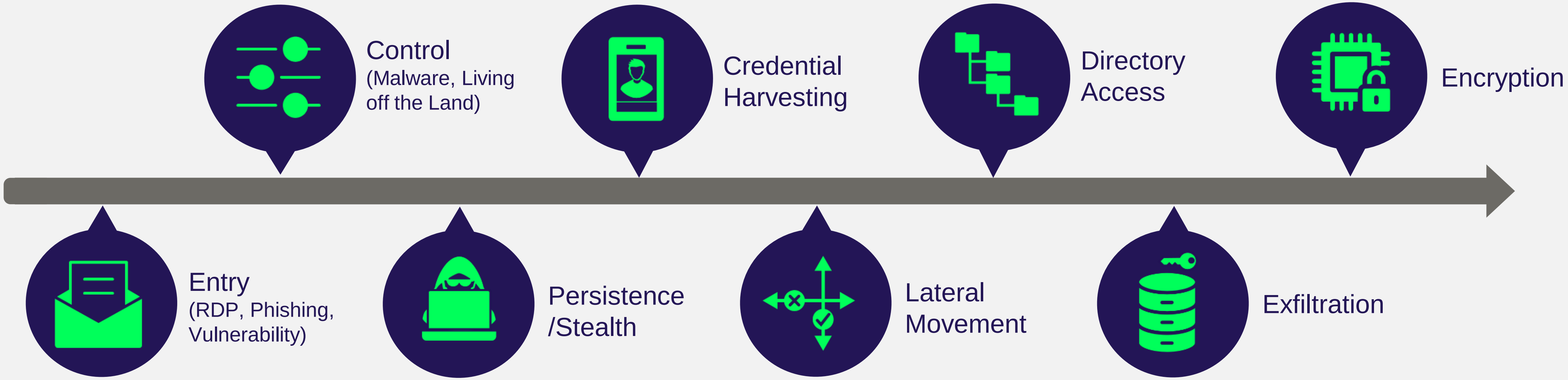
Joseph Carson

Chief Security Scientist & Advisory CISO

Delinea

High Risks from Over Privileged Identities

Common Attack Path



Entry
(RDP, Phishing, Vulnerability)

Control
(Malware, Living off the Land)

Persistence
/Stealth

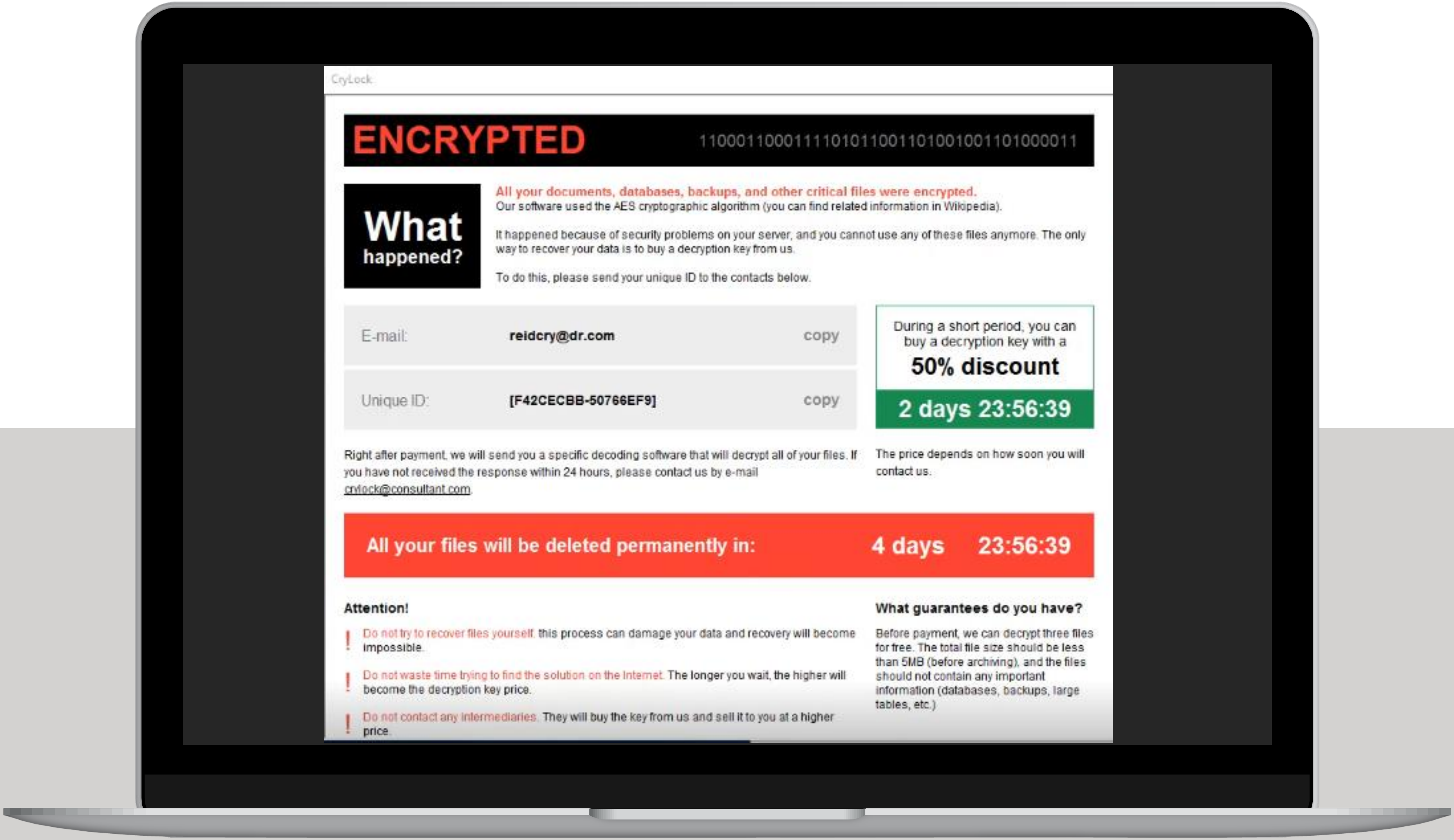
Credential Harvesting

Lateral Movement

Directory Access

Exfiltration

Encryption



ENCRYPTED 1100011000111101011001101001001101000011

What happened?

All your documents, databases, backups, and other critical files were encrypted.
Our software used the AES cryptographic algorithm (you can find related information in Wikipedia).

It happened because of security problems on your server, and you cannot use any of these files anymore. The only way to recover your data is to buy a decryption key from us.

To do this, please send your unique ID to the contacts below.

E-mail: **reidcry@dr.com** copy

Unique ID: **[F42CECBB-50766EF9]** copy

During a short period, you can buy a decryption key with a

50% discount

2 days 23:56:39

Right after payment, we will send you a specific decoding software that will decrypt all of your files. If you have not received the response within 24 hours, please contact us by e-mail crylock@consultant.com.

The price depends on how soon you will contact us.

All your files will be deleted permanently in: 4 days 23:56:39

Attention!

! Do not try to recover files yourself, this process can damage your data and recovery will become impossible.

! Do not waste time trying to find the solution on the Internet. The longer you wait, the higher will become the decryption key price.

! Do not contact any intermediaries. They will buy the key from us and sell it to you at a higher price.

What guarantees do you have?

Before payment, we can decrypt three files for free. The total file size should be less than 5MB (before archiving), and the files should not contain any important information (databases, backups, large tables, etc.)

You’ll most likely be notified of a breach by an OUTSIDER!

- Law Enforcement
- Third Parties including customers
- Attackers contact you
- Social Media
- Employees
- Security Researchers

Be Incident Response Ready

- Time Format and Naming?
- Policies (HR, Legal, Law Enforcement)
- Evidence Gathering (Logs, Images)
- Identities and User Access
- Service Accounts (Privileged Access, Rotate)
- Go Bag (Everything you might need)
- Communications Alternative (OOB)
- Helpdesk Ready
- Incident Response Plan
- Incident Response Practice Drills

If you do become a victim of Ransomware

RESTORE BACKUP or

PAY RANSOM or

DO NOTHING
AND HOPE TO REBUILD

What did the attackers have access to and how did they do it?

- Domain Admin and DC
- All Systems
- All Data
- All Applications?
- On-Premise or Cloud?
- How long?
- What tools did they use?
- Did they leave any backdoors?
- What data did they take and how?
- What is the timeline of events?
- What evidence is remaining?

Following the attackers’ footprints
ATTACK PATH

LIVE WALKTHROUGH OF ATTACK

What can we do to reduce the risks?

Top tips to reduce Ransomware risks and avoid becoming a victim

- Education & Cyber Hygiene
- Backup & Test
- Zero-Trust & Least Privilege
- Privileged Access Management
- Application Control
- Patch and Update Security

THANK YOU!