Questions:

- how does email from miroslav.jakabovic about browser extesion related? Was his account compromised, it was this game of chance? Because of 3 people that downloaded it, only david.jalovec got one with keylogger.

Executive Summary - still not clear to be updated!

Coolbank experienced multiple security incidents within a short time window, affecting on-prem infrastructure, cloud services, and user identities. Detailed forensic analysis determined that these events do not represent a single continuous intrusion, but rather two parallel and independent attack paths conducted by different threat actors using distinct initial access vectors, tooling, and objectives.

The primary incident involved a technically sophisticated infrastructure compromise that began with remote code execution (RCE) against a public-facing Apache Tomcat service on the loan application server. The attacker escalated privileges locally, harvested credentials, pivoted internally using tunneling tools, compromised DMZ and domain assets, deployed remote access tools, and ultimately executed Akira ransomware. In parallel, stolen AWS credentials were abused to provision cloud resources for cryptocurrency mining and to access sensitive S3 data.

Separately, a secondary but unrelated identity compromise affected the Office 365 account of lea.ciger@coolbank.eu. This incident originated from an infostealer (Vidar) infection on an end-user workstation, which occurred several days before the Tomcat exploitation. The attacker leveraged stolen credentials and authentication cookies to access email, grant application consent, and perform inbox rule manipulation consistent with email account abuse and potential business email compromise (BEC) activity. No technical indicators link this identity compromise to the infrastructure-focused attack chain.

While both incidents occurred within the same organizational environment and timeframe, no shared infrastructure, malware, credentials, or operational dependencies were identified. Treating these events as independent attack paths provides a more accurate reconstruction of attacker behavior and supports proportionate remediation and risk assessment.

Incident taxonomy

Incident ID	Classification
CB-2026-01	Infrastructure compromise via RCE (Primary incident)
CB-2026-02	Identity compromise via infostealer (Secondary, unrelated)

CB-2026-01 - Infrastructure compromise via RCE timeline

- `2026-01-15T16:40:13.887Z` - [Loan] attacker exploited tomcat11 RCE (CVE-2025-24813/Partial PUT) and downloaded payload `memory_test.sh` what contained remote shell from `192.20.253.137:8080`.
- `2026-01-15T16:40:53.983Z` - [Loan] attacker started reverse shell to `195.20.9.183:8443`.
- `2026-01-15T16:43:13.984Z` - [Loan] attacker escalated privileges by exploiting CVE-2025-32463 Local Privilege Escalation to Root via Sudo chroot in Linux.
- `2026-01-15T16:44:03.983Z` - [Loan] attacker obtained AWS access key and secret key for loan-apiuser from source code in Coolbank java application `/home/developer/projects/loan-app/src/main/java/eu/coolbank/loan/LoanApplicationServlet.java`.
- `2026-01-15T16:48:04.909Z` - [Loan] attacker exfiltrated collected AWS access key to Mega cloud storage provider `g.api.mega.co.nz`.
- `2026-01-15T16:49:11.907Z` - [Loan] attacker exfiltrated SSH private key from user `spravca` on Loan server a Mega.
- `2026-01-15T16:51:03.000Z` - [AWS] attacker logged to AWS from IP `138.199.21.200` using stolen access key `AKIATECIQI6O6Y3CBDOH` for `loan-apiuser`.
- `2026-01-15T16:52:18.000Z` - [AWS] attacker created AWS user `aws-testing` with access key `AKIATECIQI6O6U5P3WUZ` and attached access policy `arn:aws:iam::aws:policy/AdministratorAccess`.
- `2026-01-15T16:56:44.000Z` - [AWS] attacker listed objects in `loan-applicants` S3 bucket.
- `2026-01-15T16:58:14.000Z` - [AWS] attacker downloaded 7 objects from `loan-applicants` S3 bucket (see list of exfiltrated documets).
- `2026-01-15T17:00:29.000Z` - [AWS] loan-apiuser created ssh key pair (`testing_web_key/b4:f4:2a:90:b8:f8:fd:e4:0f:32:66:4a:bd:0c:00:63:ae:31:8b:bb`).

- `2026-01-15T17:02:02.000Z` - [AWS] loan-apiuser started EC2 instance i-06f9c69d1c1cb1ece with public IP 16.170.218.1.

- `2026-01-15T17:12:55.542Z` - [AWS] CryptoCurrency:EC2/BitcoinTool.B - The EC2 instance i-06f9c69d1c1cb1ece is communicating outbound with a known Bitcoin-related IP address 141.95.72.61.

- `2026-01-15T17:15:47.907Z` - [Loan] attacker installed pivoting and tunneling tool ligolo-ng.

- `2026-01-15T17:16:13.984Z` - [Loan] attacker started network discovery by running port scan across the DMZ network from the `loan` server.

- `2026-01-15T17:23:38.000Z` - [DMZ] attacker accessed `dmzFTP` using stolen ssh private key from `spravca`.

- `2026-01-15T17:28:40.743Z` - [DMZ] attacker installed `teamviewer` on `dmzFTP` server.

- `2026-01-15T17:29:48.348Z` - [DMZ] attacker created user `admfile` on `dmzFTP` server.

- `2026-01-15T17:45:12.020Z` - [DMZ] attacker created crontab task to establish persistence.

- `2026-01-15T18:54:38.000Z` - [DMZ] attacker performed lateral movement and accessed `velociraptor` server using stolen ssh private key from user `spravca`.

- `2026-01-15T19:12:57.376Z` - [DC] attacker created user `administratr` on ADC1ofc using Velociraptor and placed it into `Domain Admins` group.

- `2026-01-15T19:15:42.622Z` - [DC] attacker downloads AnyDesk.exe into C:\Users\Public\ on ADC2ofc using Velociraptor.

- `2026-01-15T19:20:38.416Z` - [DC] attacker installs AnyDesk.exe, configures to start silently with Windows and sets password.

- `2026-01-15T19:26:16.422Z` - [DC] attacker created a disk snapshot using Volume Shadow Copies, exposed it locally via a filesystem link, and extracted important system files `NTDS.dit`and `SYSTEM` into a temporary folder.

- `2026-01-15T19:31:31.956Z` - [DC] attacker deleted shadow copies on ADC2ofc to disable system recovery.

- `2026-01-15T19:32:02.932Z` - [DC] attacker created user `dominik.chrappe` in Windows AD and added him to `Group Policy Creator Owners` group.

- `2026-01-15T20:15:01.543Z` - [DMZ] attacker tried to exfiltrate data from `dmzFTP` server from /etc /home /var/www /root directories, but that appears to fail.

- `2026-01-15T20:52:45.599Z` - [DC] attacker started Akira ranwomware on ADC2ofc.

- `2026-01-15T21:18:33.000Z` - [AWS] An administrator (admin.stanko) while on vacation in Serbia, terminated the suspicious EC2 instance i-06f9c69d1c1cb1ece.

- `2026-01-15T22:12:56.965Z` - [EXT] attacker installs NodeJS server on officewin5/192.168.12.8 that listens on port `3000` and collects keylogger data.

- `2026-01-15T22:25:58.300Z` - [EXT] user `david.jalovec` downloads malicious browser extension `extension.zip` that is masked keylogger.

- `2026-01-15T22:40:11.346Z` - [EXT] O365 credentials of `david.jalovec` were stolen by keylogger.

- `2026-01-15T23:38:14.578Z` - [EXT] attacker used stolen O365 credentials from `david.jalovec` to login to One Outlook Web using eM Client.

- `2026-01-15T23:52:48.000Z` - [EXT] attacker created inbox rule in Outlook to forward incoming emails to `miloslav.dubnicka@coolbank.eu` and another rule to move email with subject containing `invoice` to Archive folder.

- `2026-01-16T00:40:12.00Z` - [EXT] attacker sent fake email with subject `faktura` to `david.jalovec@coolbank.eu` with intention to trick David paying fake invoice.

CB-2026-02 - Identity compromise via infostealer timeline

- `2026-01-12T01:03:45.000Z` - [HR] Initial infection of Lea's personal computer G2026/Windows 11, from where Vidal Stealer stole 17 unique password and persistent cookie ESTSAUTHPERSISTENT that could be used to attacker to access Lea's O365 account.
- `2026-01-15T20:13:13.971Z` - [HR] event with source `36.50.238.15` by `lea.ciger@coolbank.eu` created high alert Entra ID Protection - Risk Detection - Sign-in Risk. Lea logged in to Outlook Web from IP address located in `Singapore`, owned by VPN provider while usually she logs in from `37.58.4.198`. Further investigation showed that she logged from Chrome, while she usually used Edge and logged from IP. Her account was using single factor for authentication.
- `2026-01-15T20:23:44.000Z` - [HR] attacker tried to access Azure Portal but it failed due to requirement to enroll for second factor authentication.
- `2026-01-15T20:31:18.204Z` - [HR] attacker granted consent to 3rd party client (eM Client) to access Lea's account.

Impact Analysis

Credentials compromised

- AKIATECIQI6O6Y3CBDOH - loan-apiuser AWS access key.
- Lea Ciger (lea.ciger@coolbank.eu) - compromised O365 credentials.
- David Jalovec (david.jalovec@coolbank.eu) - stolen O365 credentials via keylogger.
- Miloslav Dubnicka (miloslav.dubnicka@coolbank.eu) -
- spravca - SSH private key `id_ed25519` and passphrase stolen from local user on loan server.

Sensitive documents exfiltrated

- applications/106db801-b157-4e17-a04e-c9b92a54ad04.json [407b]
- applications/6b6ee0a3-5f54-4a65-bef9-2858e7c89a44.json [433b]
- applications/43402e88-148b-4221-92a3-cd9e8c239a9a.json [423b]
- applications/cdc208d6-d601-4b75-8364-b5173b5e8e6a.json [420b]
- applications/6028eeec-d4d2-4002-9c04-63c252137e58.json [427b]
- applications/1ef41cd1-d150-45fc-bf3d-fc41abd0c22b.json [430b]
- applications/2648684d-7288-47bc-96fd-6d1348860cb3.json [435b]
- id_ed25519 (SSH private key)
- NTDS.dit,SYSTEM from ADC2ofc

Affected Assets

- List of hosts compromised:

    - Linux servers
        - loan/192.168.11.49
        - dmzFTP/192.168.11.26
        - velociraptor/192.168.11.7
    - Windows servers:

        - ADC1ofc/192.168.11.98
        - ADC2ofc/192.168.12.99
    - Worstations:
        - officewin1/192.168.12.4/david.jalovec
        - officewin3/192.168.12.6/zdenka.jakubcek
        - officewin5/192.168.12.8/miloslav.dubnicka
    - Cloud:
        - AWS account (loan-apiuser)
        - O365 tenant

- List of hosts impacted by ransomware:

    - ADC2ofc/192.168.12.99
        - C:\Users\Public\
        - C:\Users\Default\
        - C:\Users\administratr\
        - C:\Temp\EXCH\
        - C:\Temp\

Lessons learned

- **Gap Analysis**:
- **Recommendations for Improvement**:
    - storage of private key in user home directory
    - week private key passphrase

Indicators of Compromise (IoCs)

IOC type	IOC value	Comments
Malware	C:\Users\leuska\AppData\Local\Temp\11808150101\bDjqu09.exe	Vidar Sealer
IP	138.199.21.200	attacker loged to AWS using stolen loan-apiuser accesskey
Account	aws-testing	attacker created AWS user
sshkey	b4:f4:2a:90:b8:f8:fd:e4:0f:32:66:4a:bd:0c:00:63:ae:31:8b:bb	key fingerprint of aws-testing user
AWS KEY	AKIATECIQI6O6U5P3WUZ	AWS access key for aws-testing user
AWS KEY	AKIATECIQI6O6Y3CBDOH	compromised AWS access key used by legitimate loan-apiuser
SHA1	0b7fc40a15b5f471261dd76a16c6acd20e055373	sha1 hash of the malicious browser extension
File	extension.zip	name of the file containing malicious browser extension

IOC type	IOC value	Comments
IP	54.175.155.238	IP address from which malicious browser extension was downloaded
IP	84.252.113.67	attacker logged to O365 using stolen credentials from David Jalovec
UserAgent	eMClient/10.4.4209.0	UserAgent used by attacker duing logon
IP	176.9.15.89	IP address from which the tomcat11 RCE (CVE-2025-24813) was exploited
file	memory_test.sh	remote shell
IP	192.30.253.137	IP where attacker connected remote shell from loan
file	memory_test.sh	remote shell
Server	SimpleHTTP/0.6 Python/3.13.11	Server that hosted attackers reverse shell binary
file	cpu_test.sh	Local Privilege Escalation to Root via Sudo exploiting CVE-2025-32463
URL	https://github.com/nicocha30/ligolo-ng/releases/download/v0.8.2/ligolo-ng_agent_0.8.2_linux_amd64.tar.gz	Pivoting and tunneling tool used by many pentesters
Malware	teafortwo.exe	ransomware.akira/filecryptor
MD5	ae454079c93a7a1ce276756b9d62d196	teafortwo.exe ransomware.akira/filecryptor
Malware	backupTool.exe	Havoc C2 framework used to establish persistence
SHA256	c9a38fa7b619a1bc814fcf381a940245dfa8d24ae51e7ec22f9461eae288ede3	backupTool.exe Havoc C2 framework used to establish persistence
Account	administratr	User created by attacker to keep persistent access to compromised environment
IP	176.9.13.248	Havoc C2 infrastructure
Account	dominik.chrappe	User created by attacker to keep persistent access to compromised environment
Account	admfile	local user on dmzFTP server created by attacker

IOC type	IOC value	Comments
IP	200.98.8.82	C2 IP address where the crontab job from dmzFTP was regularly connecting
file	healthcheck	script that exfiltrated data from `/etc` `/home` `/var/www` `/root` and deleted all files under `/home` `/var/www` `/root`
string	H4ck3rM4n	Attacker signature left from the privilege escalation script