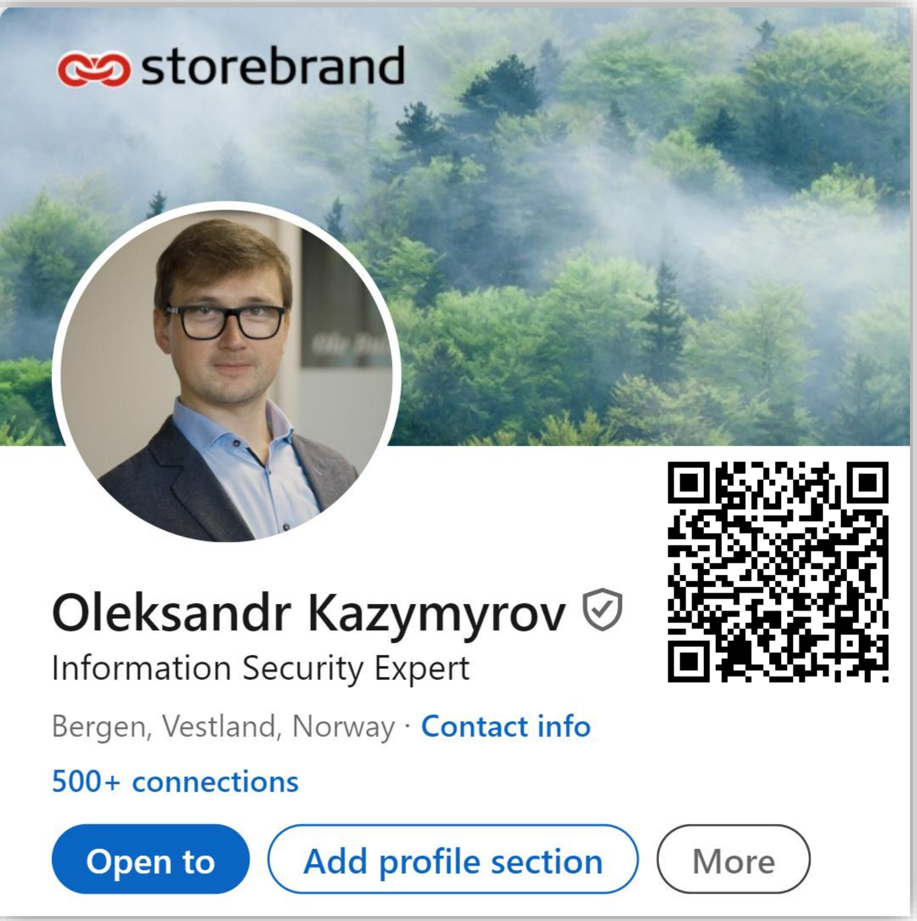
Storebrand

An offensive kill chain to reveal client's financial status

Oleksandr Kazymyrov

Booster 2024

Who am I?

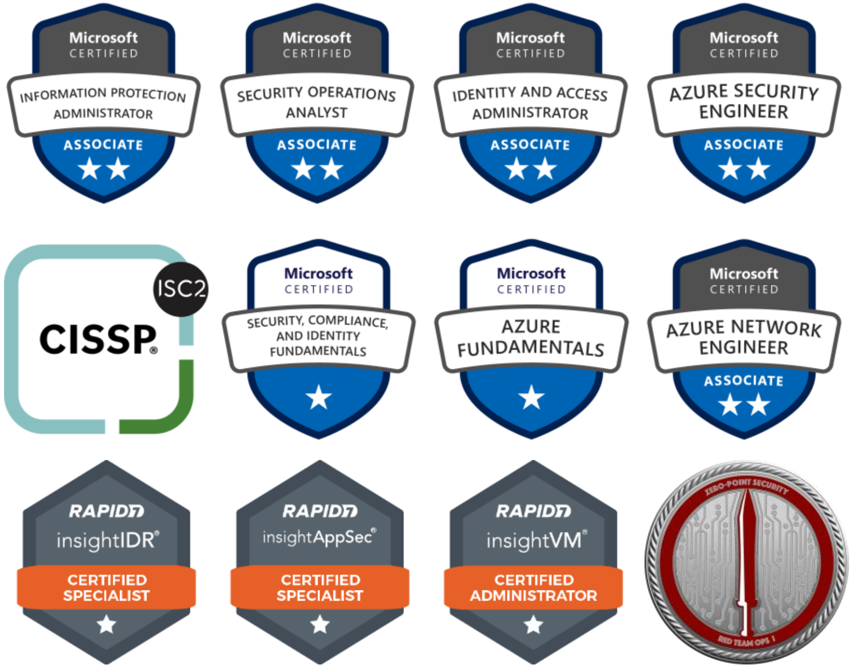

storebrand

Oleksandr Kazymyrov

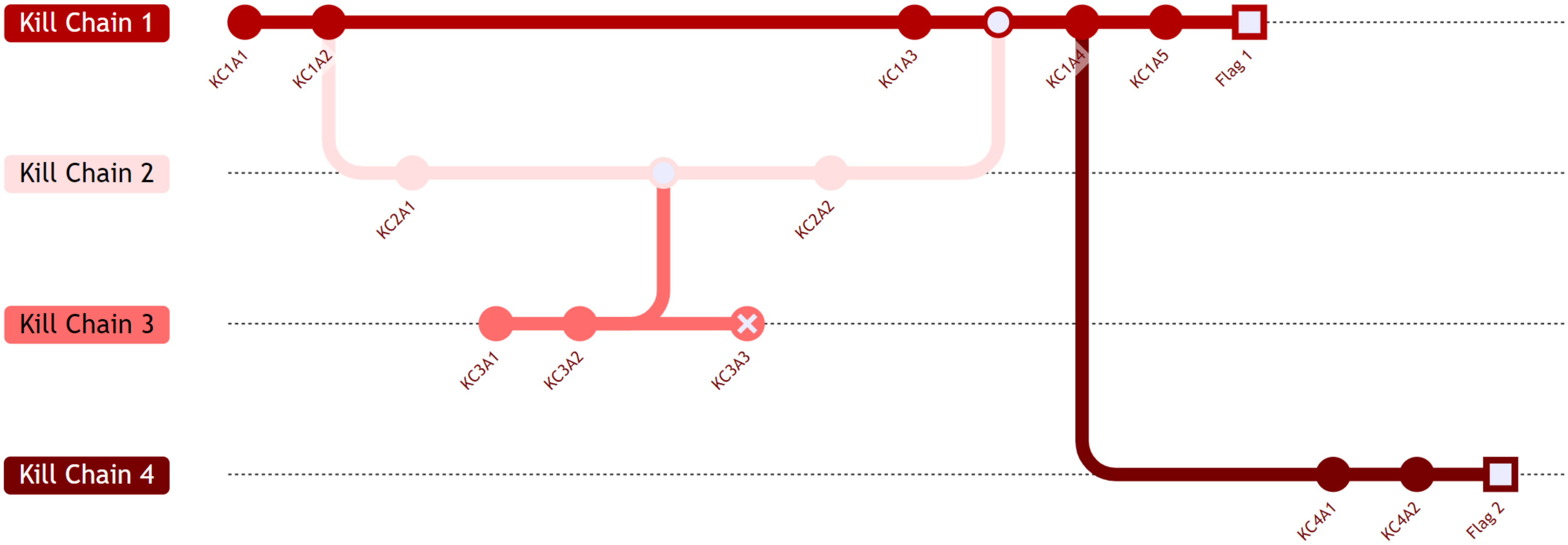
Information Security Expert

Bergen, Vestland, Norway · Contact info

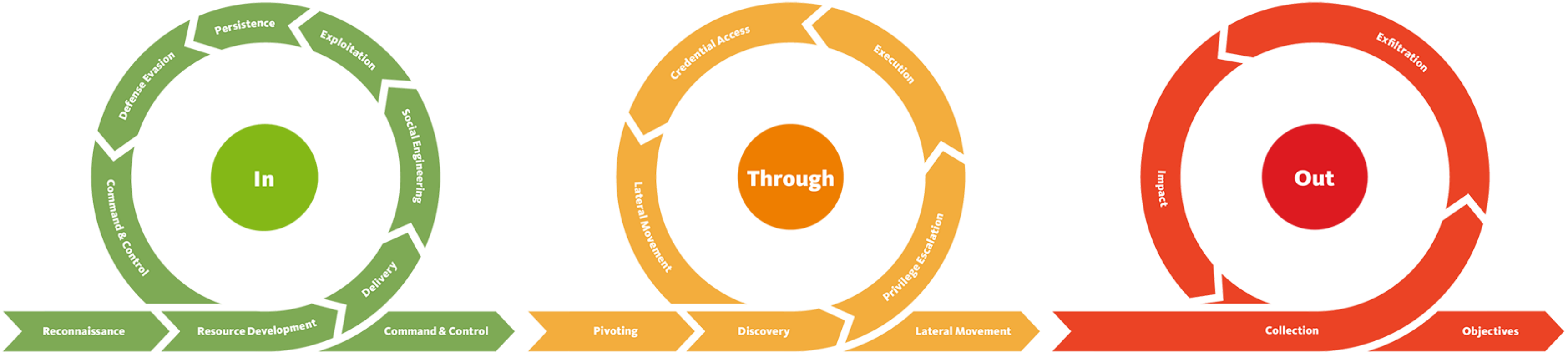
500+ connections



What is a cyber kill chain?

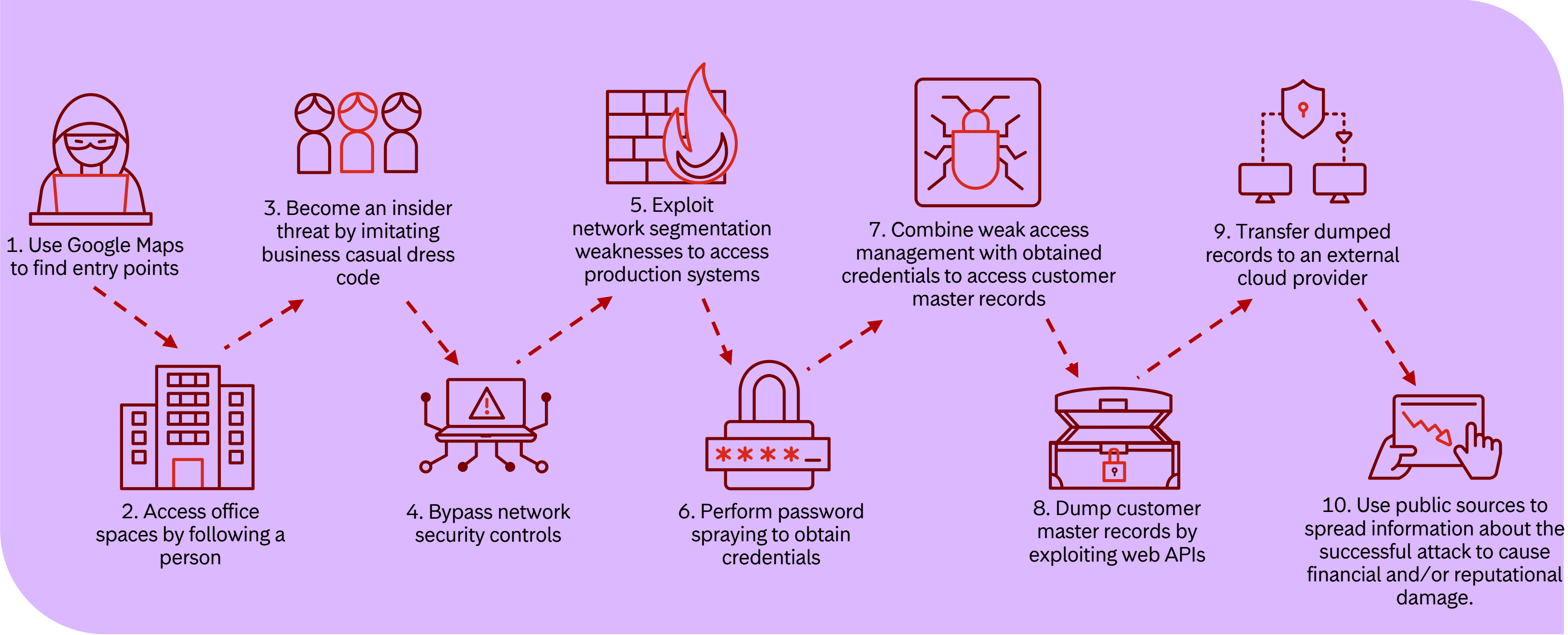


The unified kill chain



Source: https://www.unifiedkillchain.com/

Kill chain: from shared food courts to falling stocks



1. Use Google Maps to find entry points

2. Access office spaces by following a person

3. Become an insider threat by imitating business casual dress code

4. Bypass network security controls

5. Exploit network segmentation weaknesses to access production systems

6. Perform password spraying to obtain credentials

7. Combine weak access management with obtained credentials to access customer master records

8. Dump customer master records by exploiting web APIs

9. Transfer dumped records to an external cloud provider

10. Use public sources to spread information about the successful attack to cause financial and/or reputational damage.

Tactics, techniques and impact

Initial Access (In)

Reconnaissance

Tailgating

Insider threat

Lateral Movement (Through)

Network access

Exploit segmentation

Credential Access

Collection and exfiltration (Out)

Exploit web apps

Collection

Exfiltration

Impact

Malware

Supply chain attacks

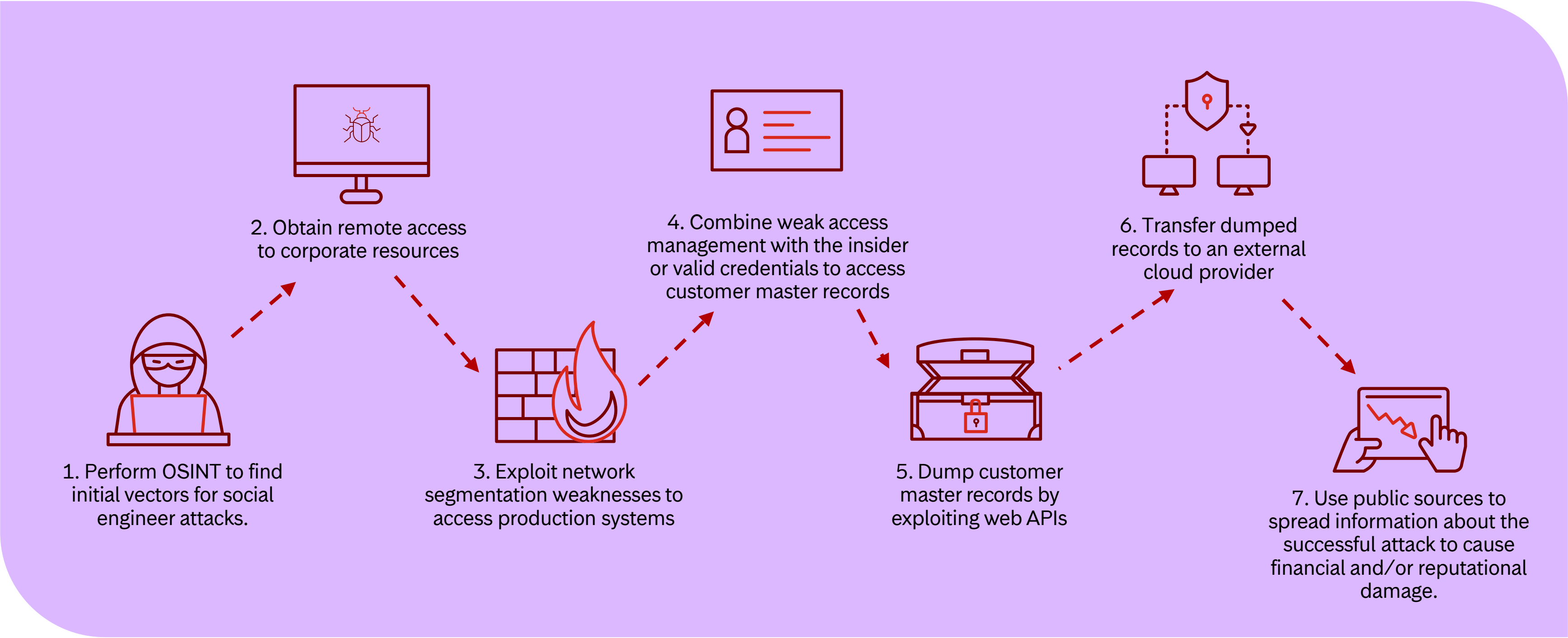
Lateral movement

Reputational and financial losses

Ransomware

Identity thief

Kill chain to reveal client's financial status



1. Perform OSINT to find initial vectors for social engineer attacks.

2. Obtain remote access to corporate resources

3. Exploit network segmentation weaknesses to access production systems

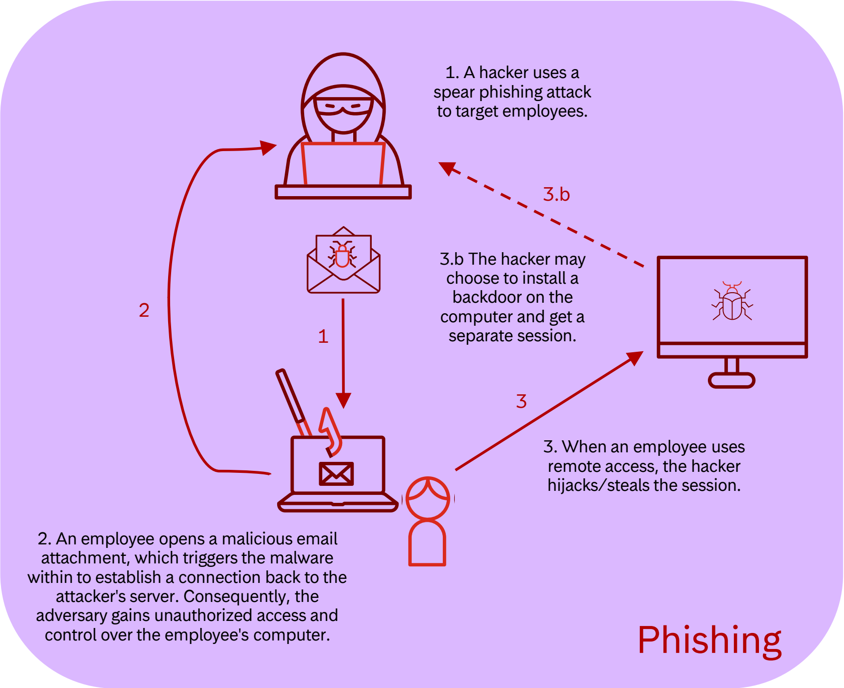
4. Combine weak access management with the insider or valid credentials to access customer master records

5. Dump customer master records by exploiting web APIs

6. Transfer dumped records to an external cloud provider

7. Use public sources to spread information about the successful attack to cause financial and/or reputational damage.

Threat scenarios for remote access



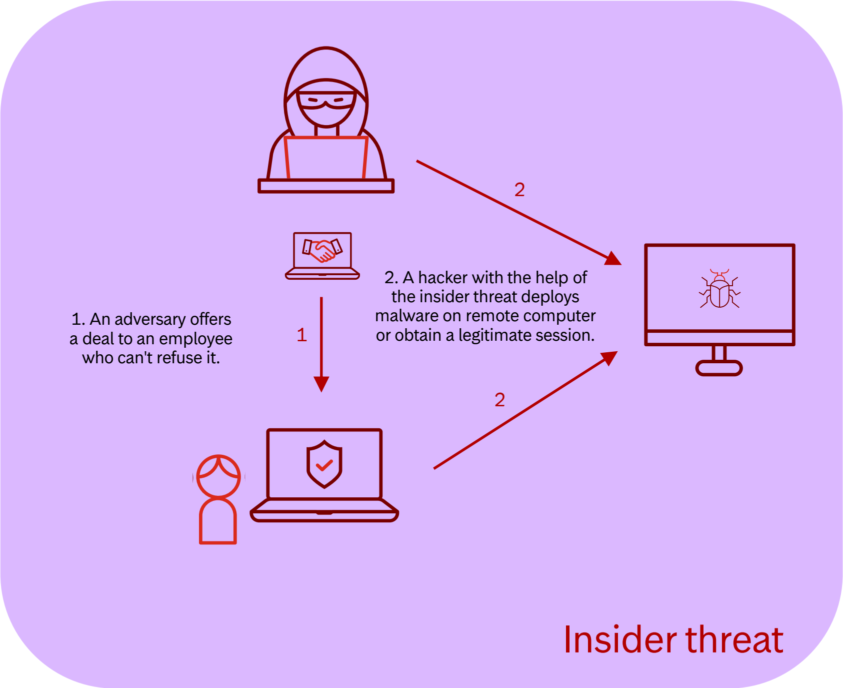
1. A hacker uses a spear phishing attack to target employees.

2. An employee opens a malicious email attachment, which triggers the malware within to establish a connection back to the attacker's server. Consequently, the adversary gains unauthorized access and control over the employee's computer.

3. When an employee uses remote access, the hacker hijacks/steals the session.

3.b The hacker may choose to install a backdoor on the computer and get a separate session.

Phishing



1. An adversary offers a deal to an employee who can't refuse it.

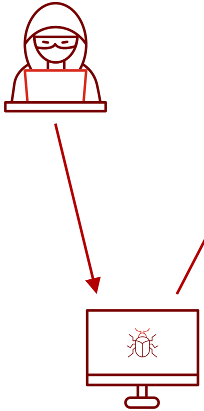
2. A hacker with the help of the insider threat deploys malware on remote computer or obtain a legitimate session.

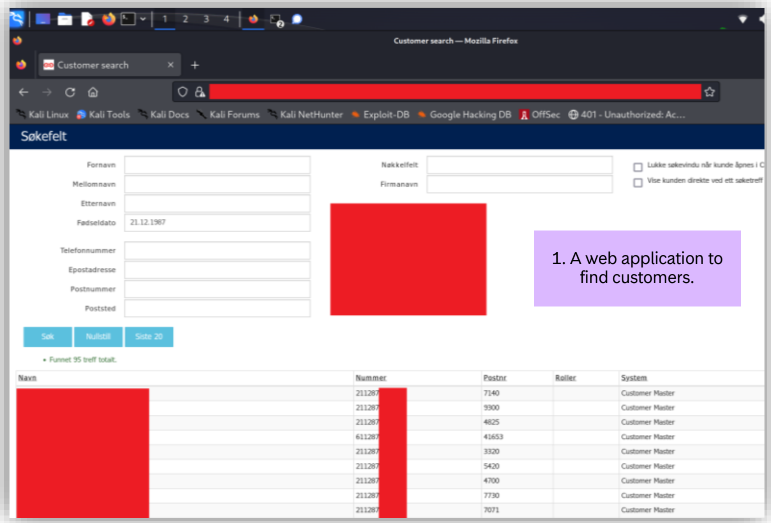
Insider threat

Kill chain: customer master records

Vulnerability

Access control was implemented on an external/internal basis. No roles or further segregation in the internal network.





Søkefelt

Fornavn		Nøkkelfelt	
Mellomnavn		Firmanavn	
Etternavn			
Fødseldato	21.12.1987		
Telefonnummer			
Epostadresse			
Postnummer			
Poststed			

□ Lukke søkevindu når kunde åpnes i C

□ Vise kunden direkte ved ett søketreff

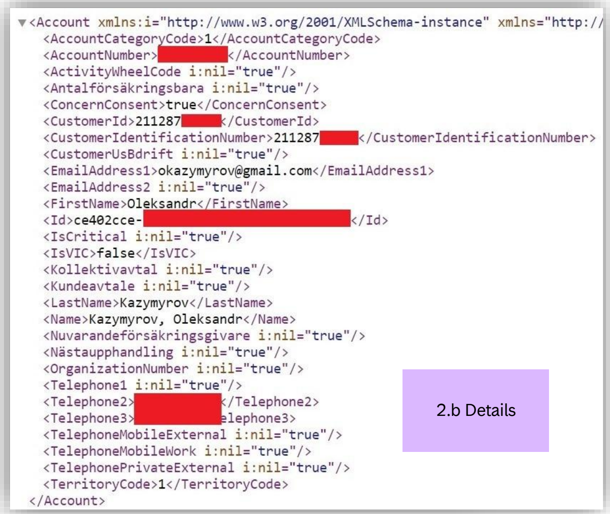
[redacted]

- Funnet 95 treff totalt.

Navn	Nummer	Postnr	Roller	System
[redacted]	211287[redacted]	7140		Customer Master
[redacted]	211287[redacted]	9300		Customer Master
[redacted]	211287[redacted]	4825		Customer Master
[redacted]	611287[redacted]	41653		Customer Master
[redacted]	211287[redacted]	3320		Customer Master
[redacted]	211287[redacted]	5420		Customer Master
[redacted]	211287[redacted]	4700		Customer Master
[redacted]	211287[redacted]	7730		Customer Master
[redacted]	211287[redacted]	7071		Customer Master

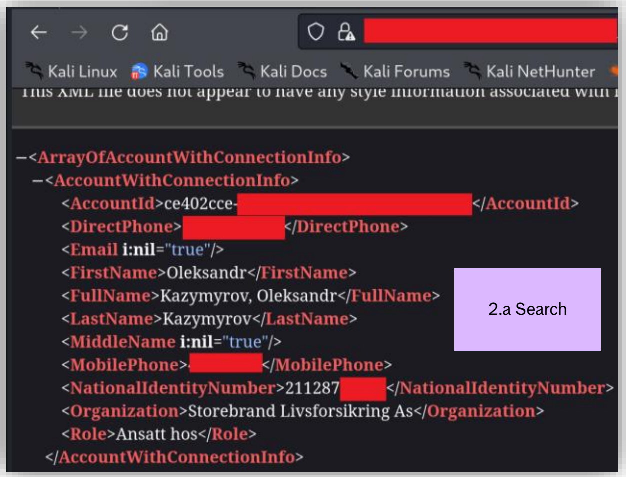
1. A web application to find customers.

2. APIs used in the customer search web application. The hacker could dump CM data of all Storebrand's customers.



```
▼<Account xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://
   <AccountCategoryCode>1</AccountCategoryCode>
   <AccountNumber>[redacted]</AccountNumber>
   <ActivityWheelCode i:nil="true"/>
   <Antalförsäkringsbara i:nil="true"/>
   <ConcernConsent>true</ConcernConsent>
   <CustomerId>211287[redacted]</CustomerId>
   <CustomerIdentificationNumber>211287[redacted]</CustomerIdentificationNumber>
   <CustomerUsBdrift i:nil="true"/>
   <EmailAddress1>okazymyrov@gmail.com</EmailAddress1>
   <EmailAddress2 i:nil="true"/>
   <FirstName>Oleksandr</FirstName>
   <Id>ce402cce-[redacted]</Id>
   <IsCritical i:nil="true"/>
   <IsVIC>false</IsVIC>
   <Kollektivavtal i:nil="true"/>
   <Kundeavtale i:nil="true"/>
   <LastName>Kazymyrov</LastName>
   <Name>Kazymyrov, Oleksandr</Name>
   <Nuvarandeförsäkringsgivare i:nil="true"/>
   <Nästaupphandling i:nil="true"/>
   <OrganizationNumber i:nil="true"/>
   <Telephone1 i:nil="true"/>
   <Telephone2>[redacted]</Telephone2>
   <Telephone3>[redacted]elephone3>
   <TelephoneMobileExternal i:nil="true"/>
   <TelephoneMobileWork i:nil="true"/>
   <TelephonePrivateExternal i:nil="true"/>
   <TerritoryCode>1</TerritoryCode>
</Account>
```

2.b Details



This XML file does not appear to have any style information associated with i

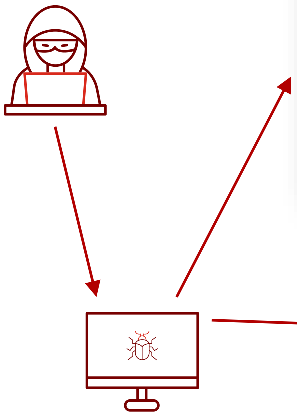
```
–<ArrayOfAccountWithConnectionInfo>
  –<AccountWithConnectionInfo>
     <AccountId>ce402cce-[redacted]</AccountId>
     <DirectPhone>[redacted]</DirectPhone>
     <Email i:nil="true"/>
     <FirstName>Oleksandr</FirstName>
     <FullName>Kazymyrov, Oleksandr</FullName>
     <LastName>Kazymyrov</LastName>
     <MiddleName i:nil="true"/>
     <MobilePhone>[redacted]</MobilePhone>
     <NationalIdentityNumber>211287[redacted]</NationalIdentityNumber>
     <Organization>Storebrand Livsforsikring As</Organization>
     <Role>Ansatt hos</Role>
  </AccountWithConnectionInfo>
```

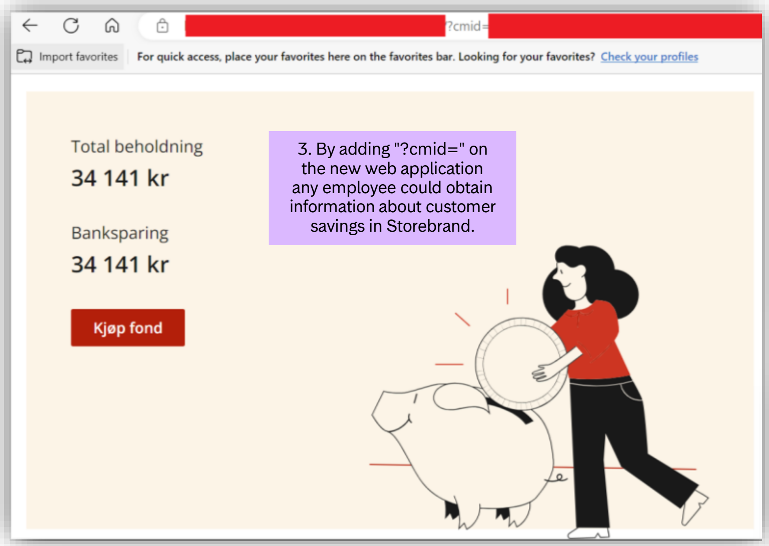
2.a Search

Attack vectors: targeting new platforms in the cloud

Vulnerability

Lift and shift migrations without continuous security tests of changes.





[redacted]?cmid=[redacted]

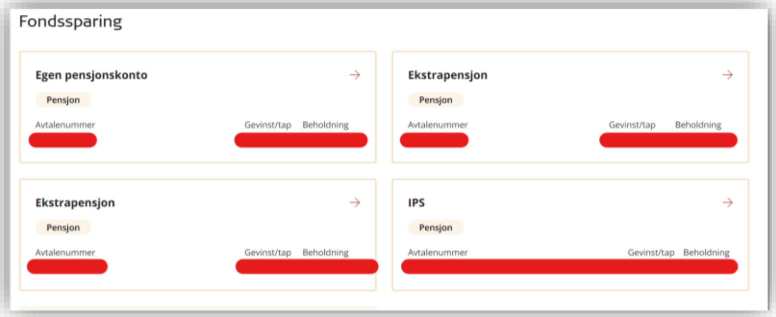
For quick access, place your favorites here on the favorites bar. Looking for your favorites? Check your profiles

Total beholdning
34 141 kr

Banksparing
34 141 kr

3. By adding "?cmid=" on the new web application any employee could obtain information about customer savings in Storebrand.

4. The combination of several services provides even more information about the savings and financial status of any client.



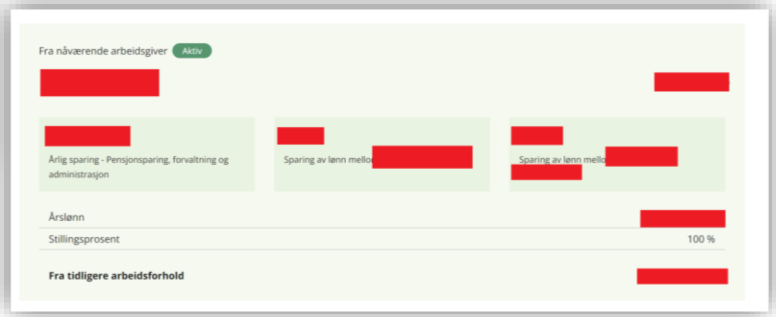
Fondssparing

Egen pensjonskonto
Pensjon
Avtalenummer [redacted]
Gevinst/tap Beholdning [redacted]

Ekstrapensjon
Pensjon
Avtalenummer [redacted]
Gevinst/tap Beholdning [redacted]

Ekstrapensjon
Pensjon
Avtalenummer [redacted]
Gevinst/tap Beholdning [redacted]

IPS
Pensjon
Avtalenummer Gevinst/tap Beholdning [redacted]



Fra nåværende arbeidsgiver Aktiv

[redacted] [redacted]

[redacted]
Årlig sparing - Pensjonsparing, forvaltning og administrasjon

[redacted]
Sparing av lønn mello[redacted]

[redacted]
Sparing av lønn mello[redacted]
[redacted]

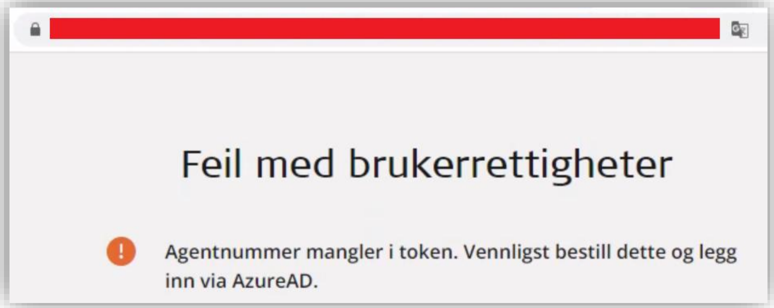
Årslønn	[redacted]
Stillingsprosent	100 %

Fra tidligere arbeidsforhold [redacted]

Attack vectors: extracting information after a quick fix

Vulnerability

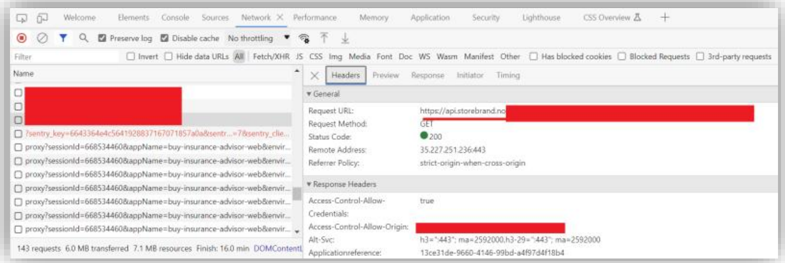
Fire fighting is the main approach to improve security. Many security updates have been implemented during the cloud migration, but some fundamental security issues (such as secure development or application/API security) are still ongoing.



[redacted]

Feil med brukerrettigheter

Agentnummer mangler i token. Vennligst bestill dette og legg inn via AzureAD.



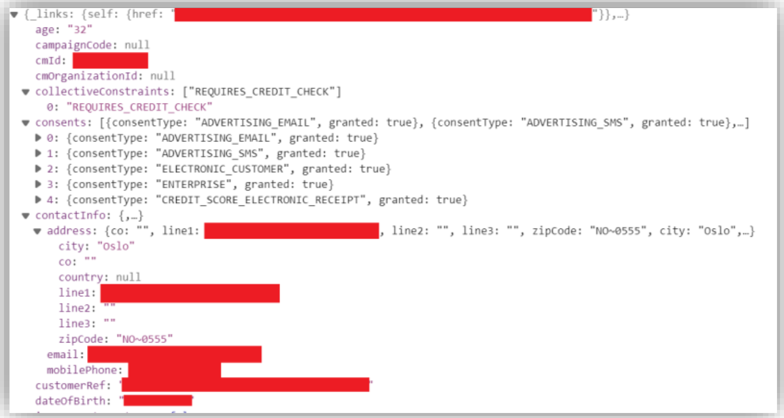
☑ Preserve log ☑ Disable cache No throttling

Filter □ Invert □ Hide data URLs All Fetch/XHR JS CSS Img Media Font Doc WS Wasm Manifest Other □ Has blocked cookies □ Blocked Requests □ 3rd-party requests

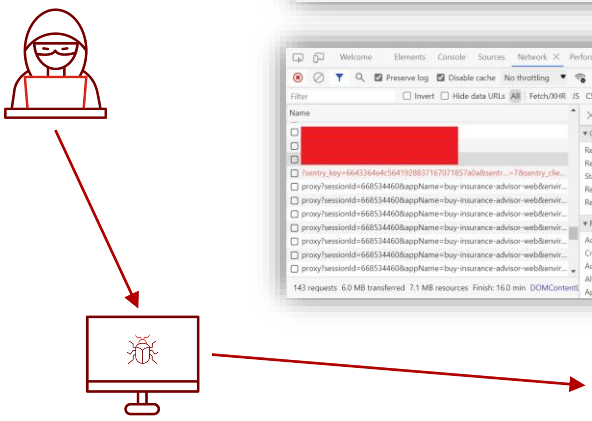
```
Name
[redacted]
?sentry_key=6643364e4c5641928837167071857a0a&sentr...=7&sentry_clie...
proxy?sessionId=668534460&appName=buy-insurance-advisor-web&envir...
proxy?sessionId=668534460&appName=buy-insurance-advisor-web&envir...
proxy?sessionId=668534460&appName=buy-insurance-advisor-web&envir...
proxy?sessionId=668534460&appName=buy-insurance-advisor-web&envir...
proxy?sessionId=668534460&appName=buy-insurance-advisor-web&envir...
proxy?sessionId=668534460&appName=buy-insurance-advisor-web&envir...
proxy?sessionId=668534460&appName=buy-insurance-advisor-web&envir...
143 requests  6.0 MB transferred  7.1 MB resources  Finish: 16.0 min  DOMContentL
```

Headers Preview Response Initiator Timing

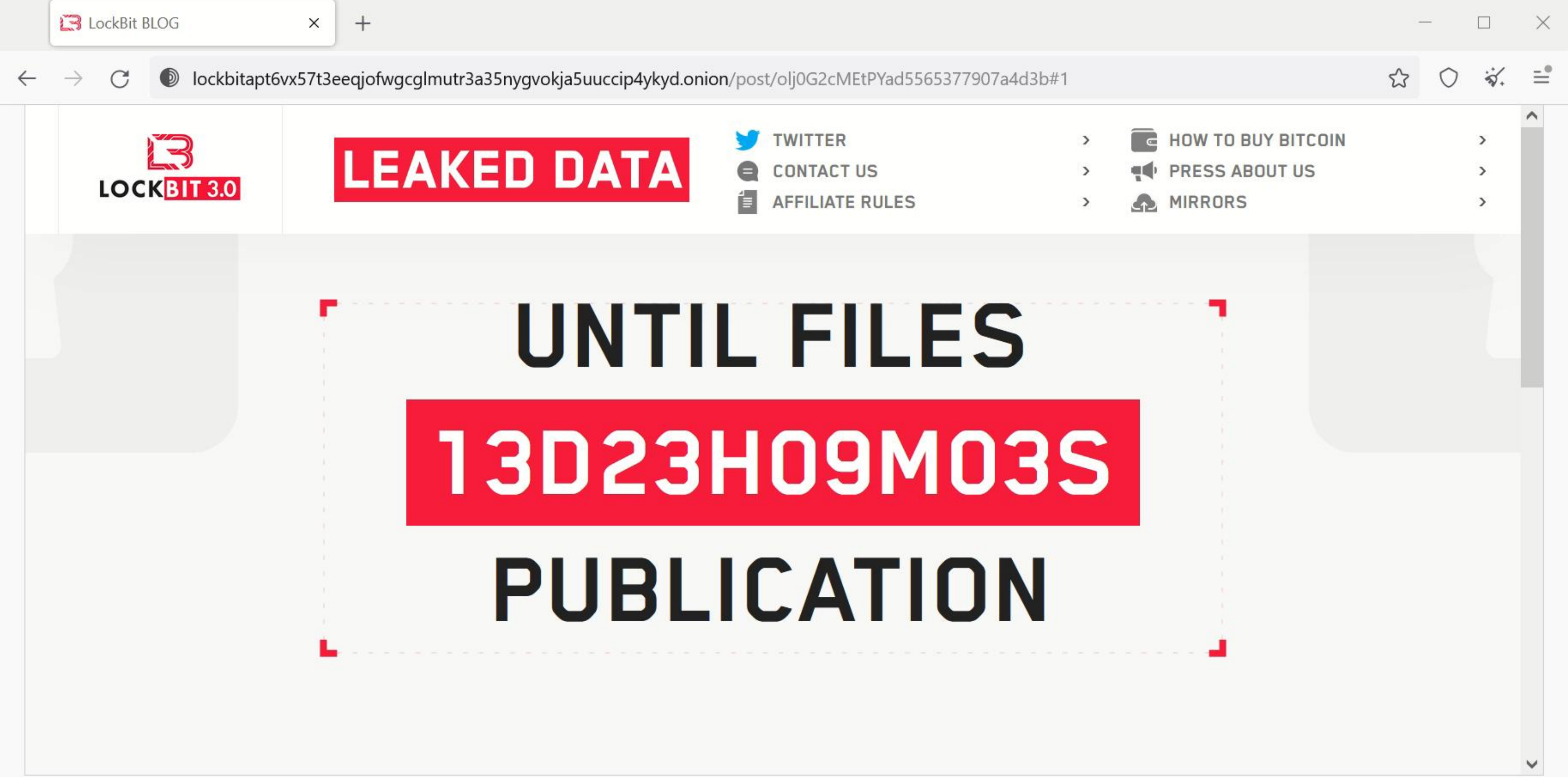
```
▾ General
Request URL:                  https://api.storebrand.no[redacted]
Request Method:               GET
Status Code:                  ● 200
Remote Address:               35.227.251.236:443
Referrer Policy:              strict-origin-when-cross-origin
▾ Response Headers
Access-Control-Allow-
Credentials:                  true
Access-Control-Allow-Origin:  [redacted]
Alt-Svc:                      h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Applicationreference:         13ce31de-9660-4146-99bd-a4f97d4f18b4
```



```
▼ {_links: {self: {href: "[redacted]"}},…}
   age: "32"
   campaignCode: null
   cmId: [redacted]
   cmOrganizationId: null
 ▼ collectiveConstraints: ["REQUIRES_CREDIT_CHECK"]
     0: "REQUIRES_CREDIT_CHECK"
 ▼ consents: [{consentType: "ADVERTISING_EMAIL", granted: true}, {consentType: "ADVERTISING_SMS", granted: true},…]
   ▶ 0: {consentType: "ADVERTISING_EMAIL", granted: true}
   ▶ 1: {consentType: "ADVERTISING_SMS", granted: true}
   ▶ 2: {consentType: "ELECTRONIC_CUSTOMER", granted: true}
   ▶ 3: {consentType: "ENTERPRISE", granted: true}
   ▶ 4: {consentType: "CREDIT_SCORE_ELECTRONIC_RECEIPT", granted: true}
 ▼ contactInfo: {,…}
   ▼ address: {co: "", line1: [redacted], line2: "", line3: "", zipCode: "NO~0555", city: "Oslo",…}
       city: "Oslo"
       co: ""
       country: null
       line1: [redacted]
       line2: ""
       line3: ""
       zipCode: "NO~0555"
     email: [redacted]
     mobilePhone: [redacted]
   customerRef: "[redacted]"
   dateOfBirth: "[redacted]
```



5. An insider could obtain customer master records and other product-related information through the API (backend) even if the browser (frontend) throws an error.



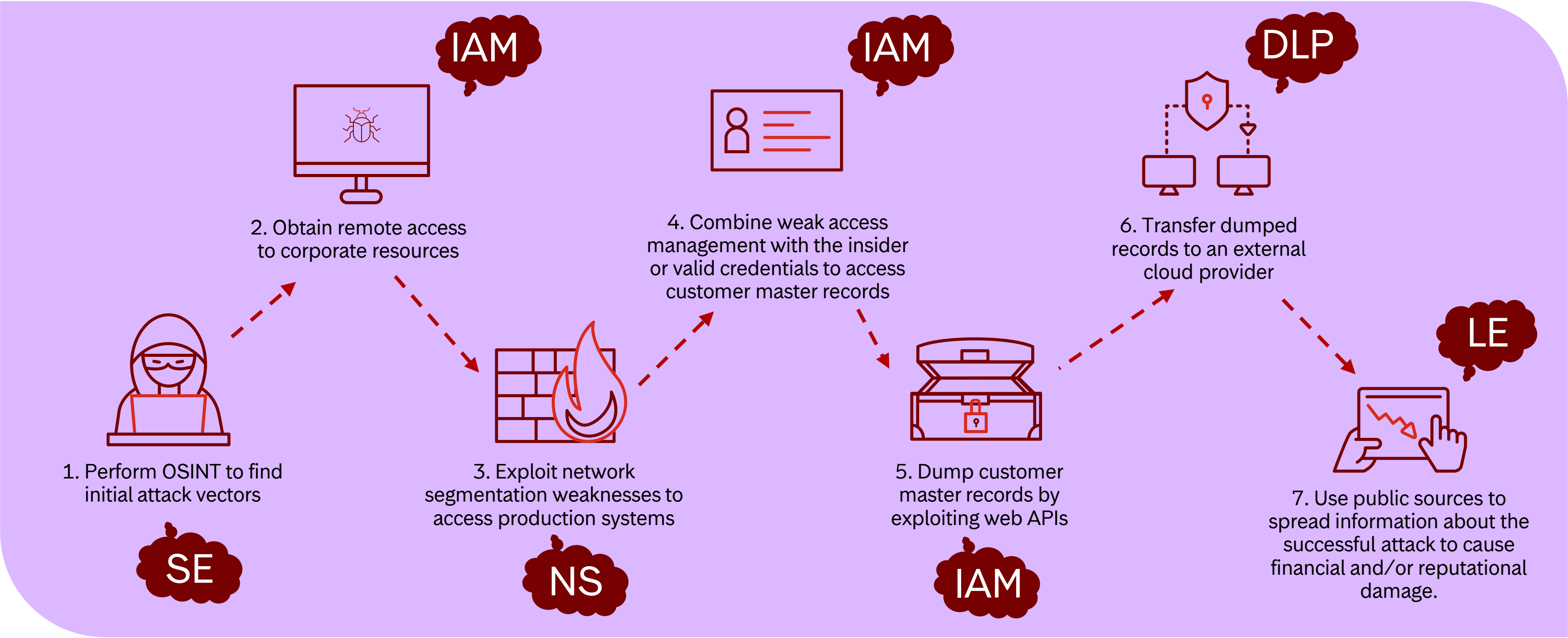
lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion/post/olj0G2cMEtPYad5565377907a4d3b#1

UNTIL FILES

13D23H09M03S

PUBLICATION

Mapping to cybersecurity domains



1. Perform OSINT to find initial attack vectors

SE

2. Obtain remote access to corporate resources

IAM

3. Exploit network segmentation weaknesses to access production systems

NS

4. Combine weak access management with the insider or valid credentials to access customer master records

IAM

5. Dump customer master records by exploiting web APIs

IAM

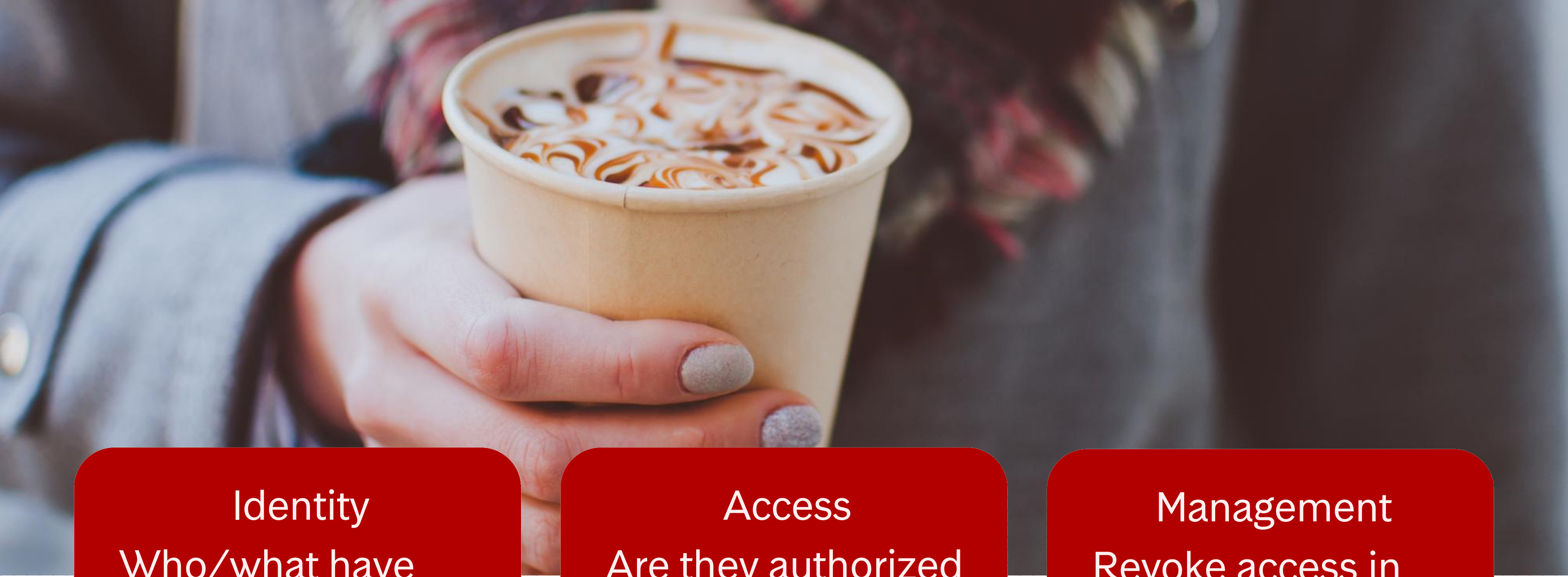
6. Transfer dumped records to an external cloud provider

DLP

7. Use public sources to spread information about the successful attack to cause financial and/or reputational damage.

LE

SE: social engineering; IAM: identity and access management; NS: network segmentation; DLP: data loss prevention; LE: law enforcement.



Identity

Who/what have access to resources?

01

Access

Are they authorized to interact with the resources?

02

Management

Revoke access in swiftly manner.

03

Storebrand

Investor i fremtiden