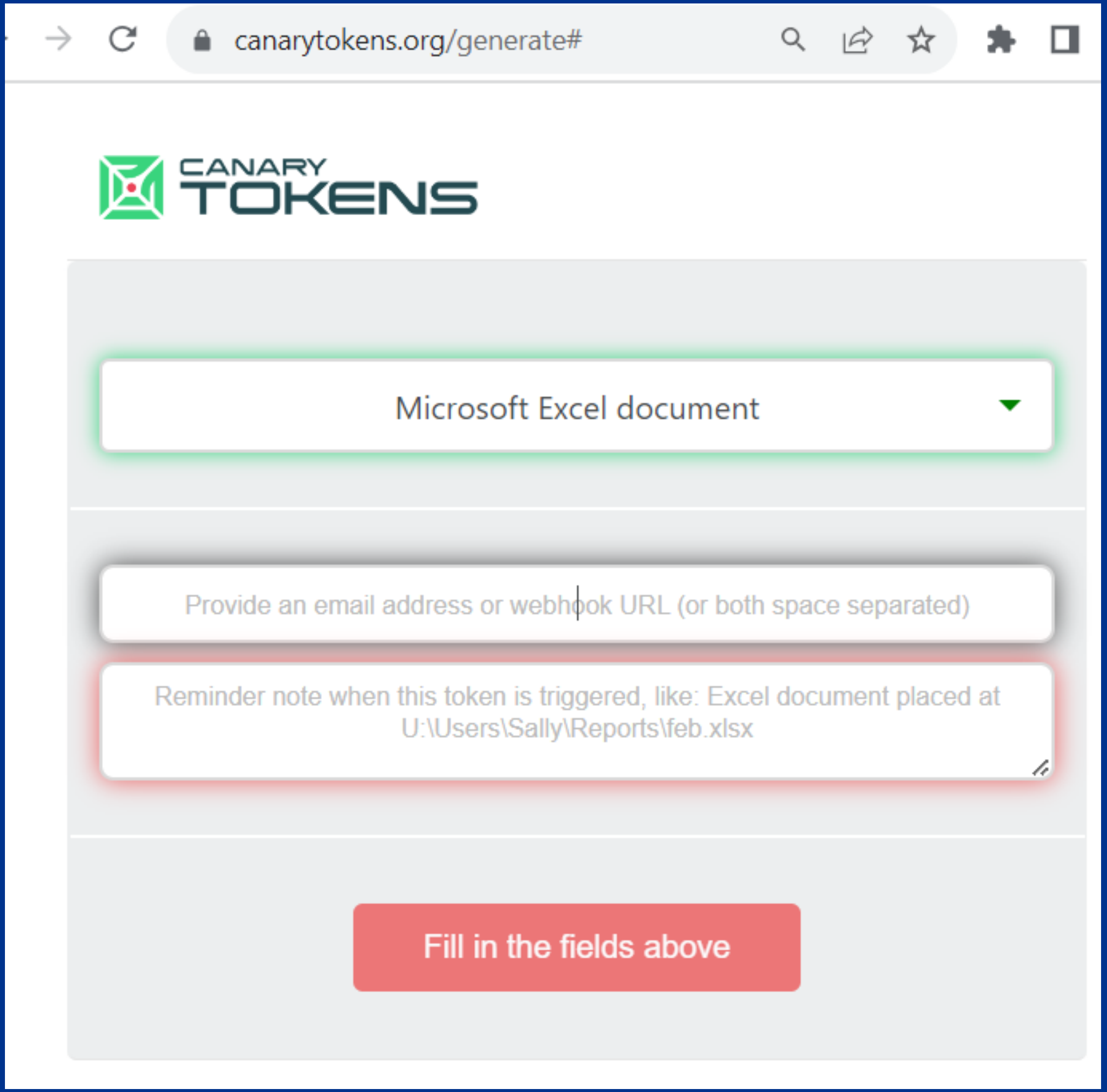
Detection using Deception

Matt Dri – KPMG, Partner Cyber Response

Agenda

- Challenges
- Threat landscape
- Detection Ideation
- Power Up



canarytokens.org/generate#

CANARY TOKENS

Microsoft Excel document

Provide an email address or webhook URL (or both space separated)

Reminder note when this token is triggered, like: Excel document placed at U:\Users\Sally\Reports\feb.xlsx

High fidelity detection

Low to no cost

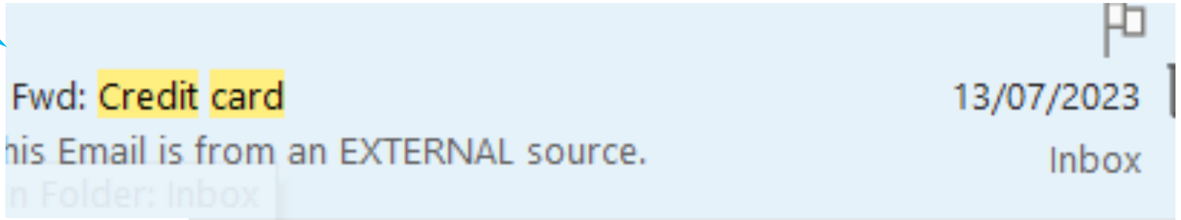
Easy to deploy

Building blocks for automation

Early detection

Deception may lead to adversary mistrust and paranoia

Fake credit card in mailbox

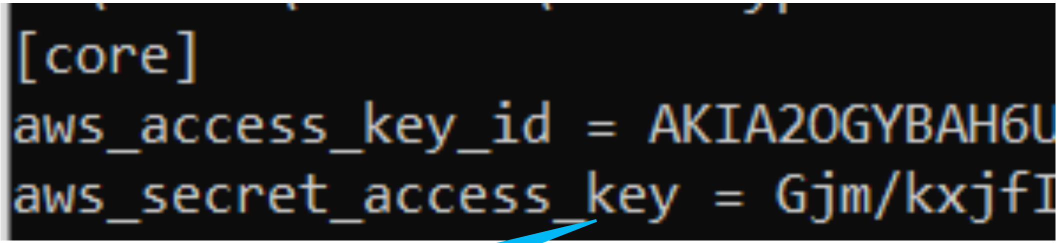


Fwd: Credit card 13/07/2023

his Email is from an EXTERNAL source. Inbox

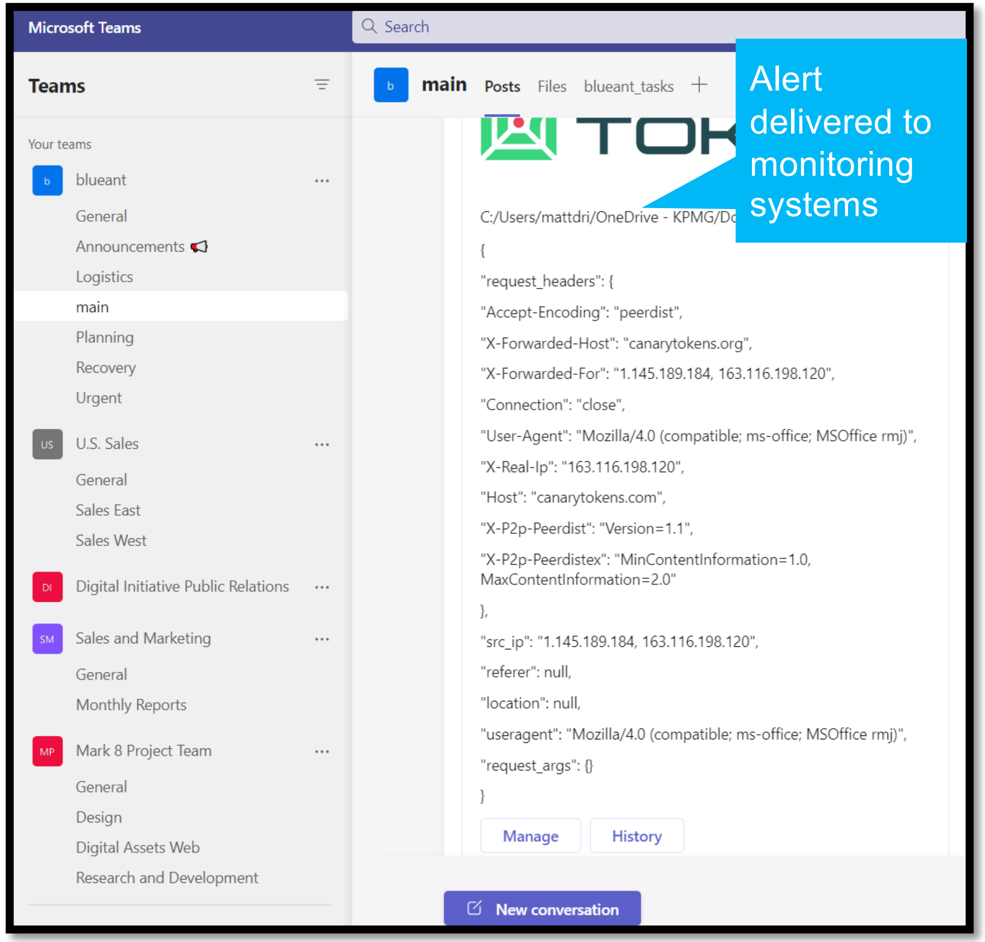
n Folder: Inbox

Fake documents



```
[core]
aws_access_key_id = AKIA2OGYBAH6U
aws_secret_access_key = Gjm/kxjfI
```

Fake credentials

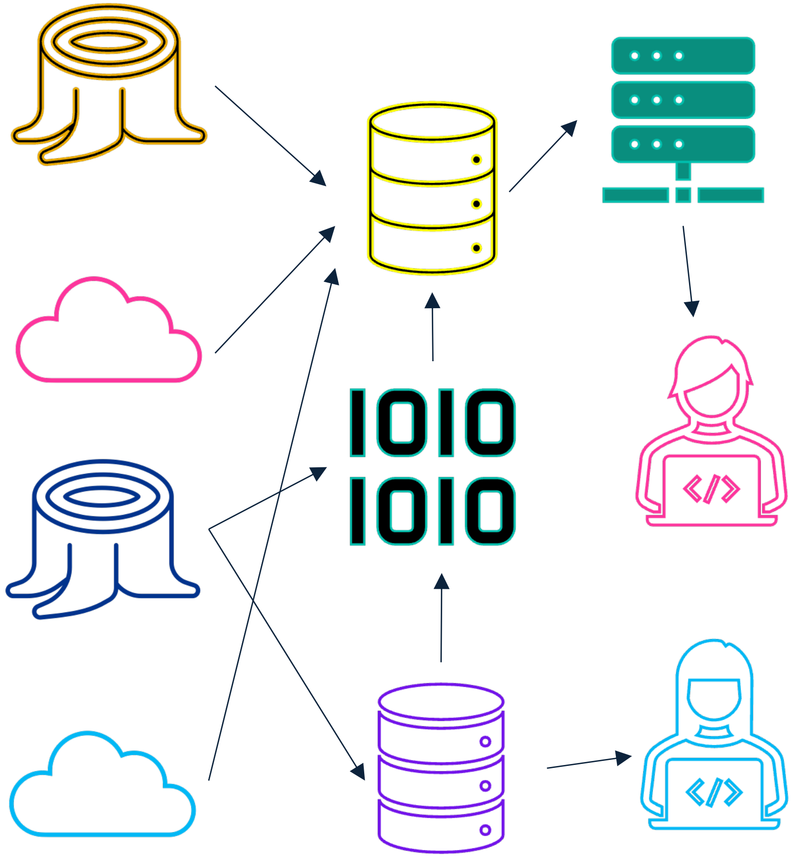


C:/Users/mattdri/OneDrive - KPMG/Dc

```
{
"request_headers": {
"Accept-Encoding": "peerdist",
"X-Forwarded-Host": "canarytokens.org",
"X-Forwarded-For": "1.145.189.184, 163.116.198.120",
"Connection": "close",
"User-Agent": "Mozilla/4.0 (compatible; ms-office; MSOffice rmj)",
"X-Real-Ip": "163.116.198.120",
"Host": "canarytokens.com",
"X-P2p-Peerdist": "Version=1.1",
"X-P2p-Peerdistex": "MinContentInformation=1.0,
MaxContentInformation=2.0"
},
"src_ip": "1.145.189.184, 163.116.198.120",
"referer": null,
"location": null,
"useragent": "Mozilla/4.0 (compatible; ms-office; MSOffice rmj)",
"request_args": {}
}
```

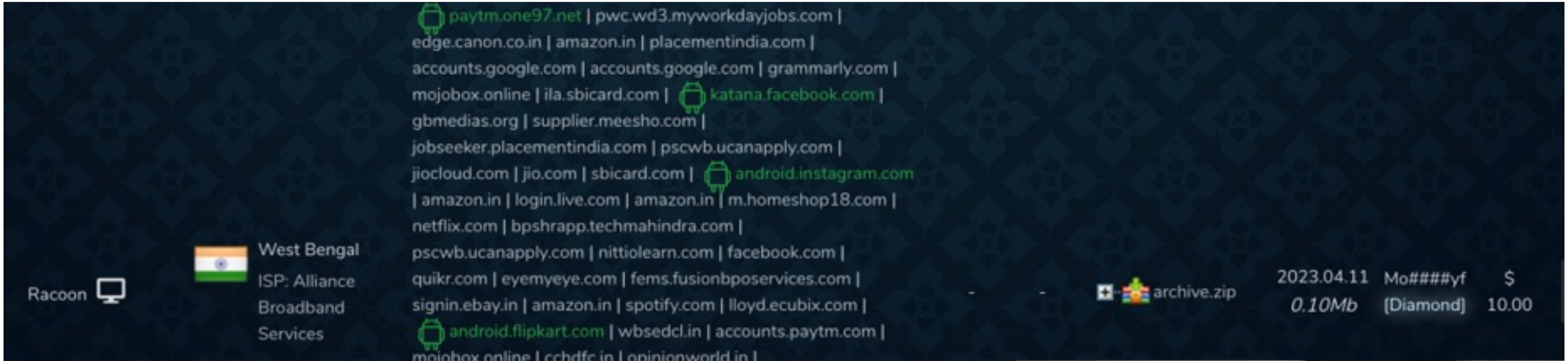
Alert delivered to monitoring systems

Detection Engineering Challenges

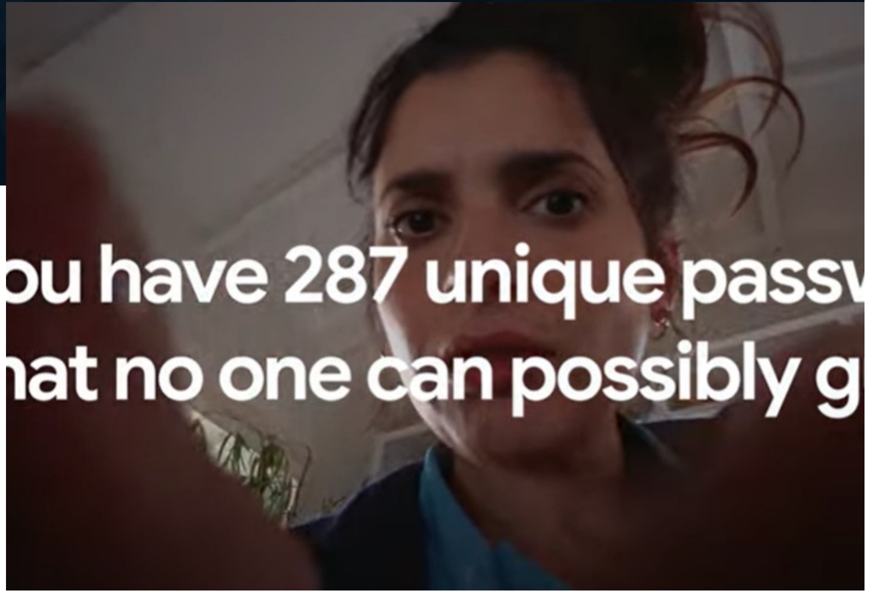


- Lag time in the pipeline
- Increasing number of external providers
- Lack of logging standards
- Inconsistent integrations
- Schema/ data model mapping
- Building high confidence alerts
- Interpretation of alerts
- Large volumes of benign detections
- Log retention and data volume
- Duplication of logs across business silos
- Cost of SIEM, SOAR and people

Stealer Scenario



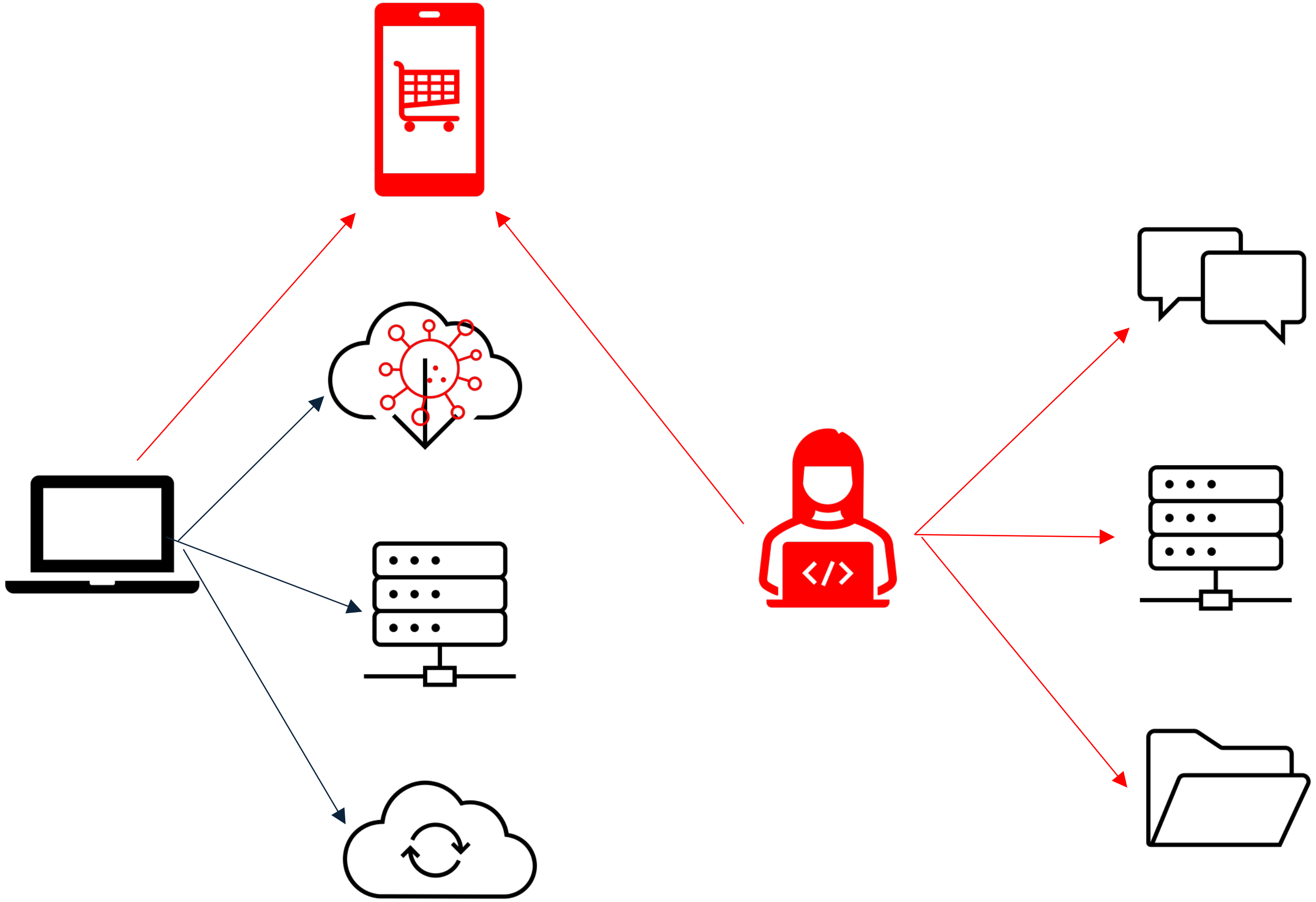
Racoon 🖥	West Bengal ISP: Alliance Broadband Services	paytm.one97.net | pwc.wd3.myworkdayjobs.com | edge.canon.co.in | amazon.in | placementindia.com | accounts.google.com | accounts.google.com | grammarly.com | mojobox.online | ila.sbicard.com | katana.facebook.com | gbmedias.org | supplier.meesho.com | jobseeker.placementindia.com | pscwb.ucanapply.com | jiocloud.com | jio.com | sbicard.com | android.instagram.com | amazon.in | login.live.com | amazon.in | m.homeshop18.com | netflix.com | bpshrapp.techmahindra.com | pscwb.ucanapply.com | nittiolearn.com | facebook.com | quikr.com | eyemyeye.com | fems.fusionbposervices.com | signin.ebay.in | amazon.in | spotify.com | lloyd.ecubix.com | android.flipkart.com | wbsedcl.in | accounts.paytm.com | mojobox.online | cchdfc.in | opinionworld.in | api.sh.mysmitch.com | lloyd.ecubix.com | reg.ebay.in | careers-wipro.icims.com | ysc123.com | m.facebook.com | timesheet.techmahindra.com | jiosaavn.com | yesforyou.darwinbox.in | yesforyou.darwinbox.in |	-	-	archive.zip	2023.04.11 0.10Mb	Mo####yf [Diamond]	$ 10.00



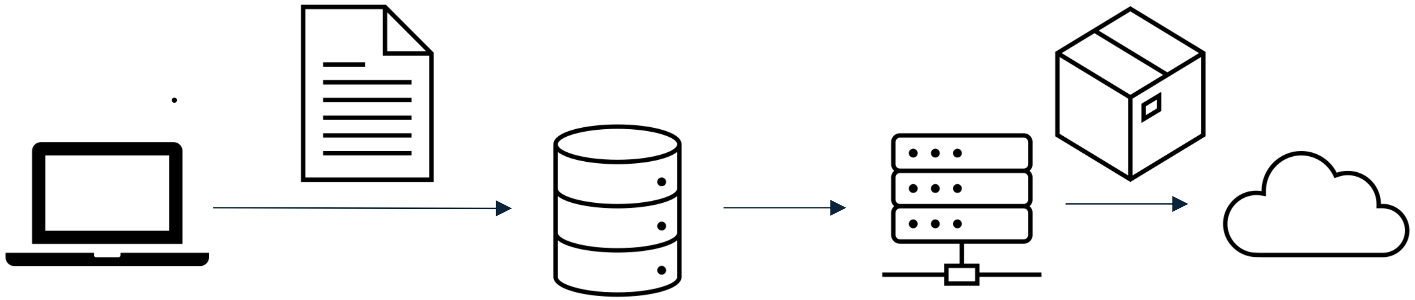
Document Classification: KPMG Confidential

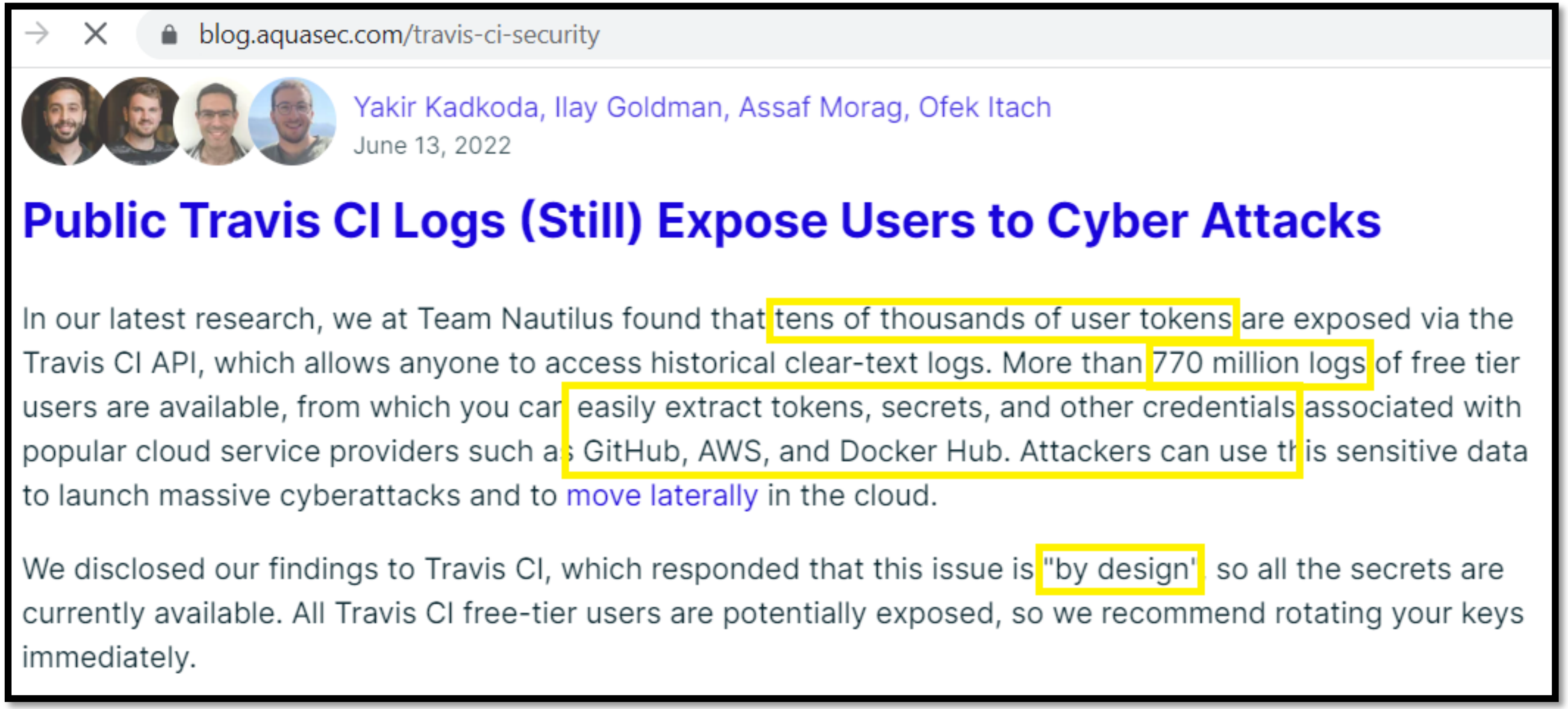
Liability limited by a scheme approved under Professional Standards Legislation.

Stealer Scenario



CI/CD





blog.aquasec.com/travis-ci-security

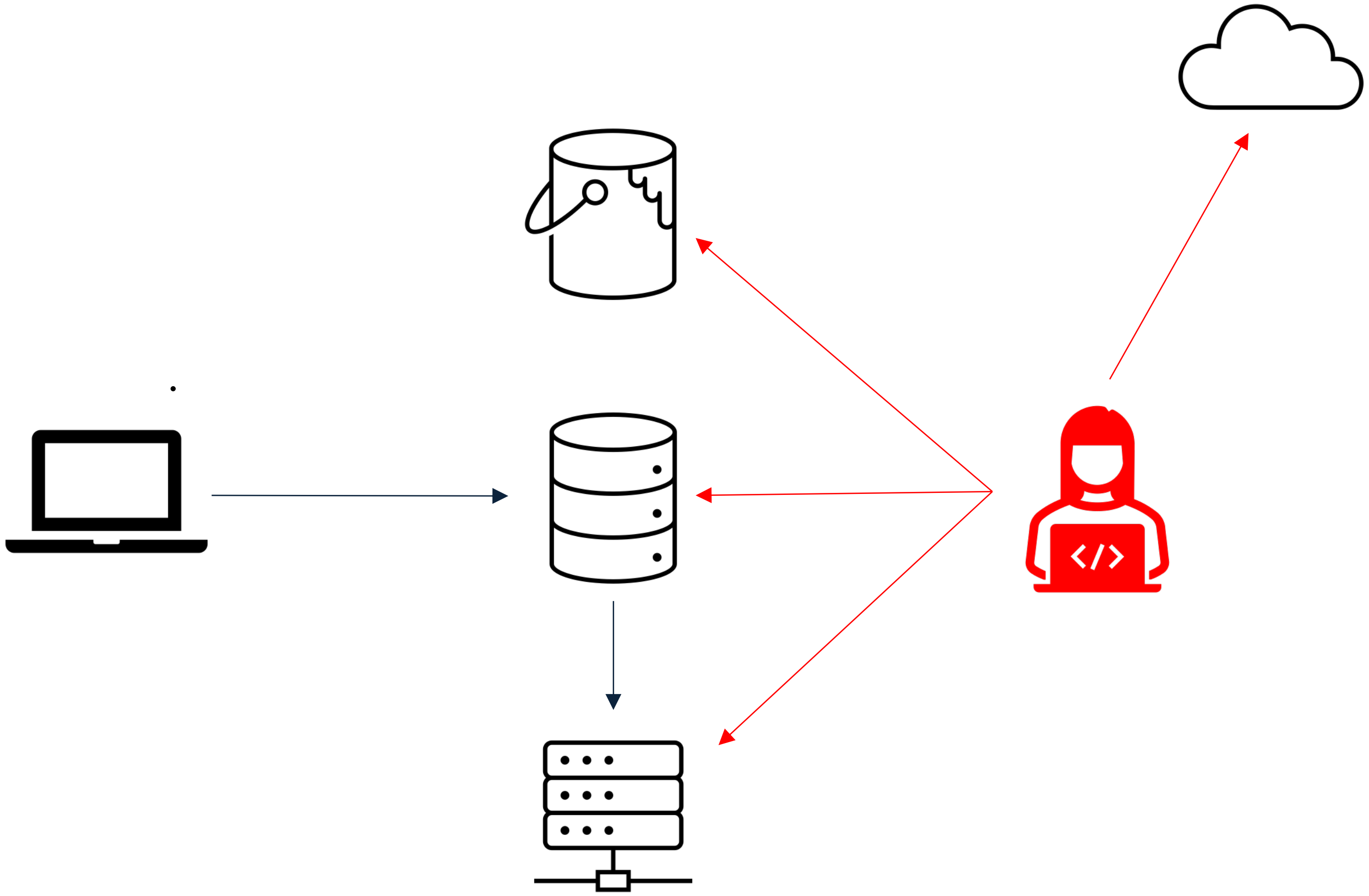
Yakir Kadkoda, Ilay Goldman, Assaf Morag, Ofek Itach
June 13, 2022

Public Travis CI Logs (Still) Expose Users to Cyber Attacks

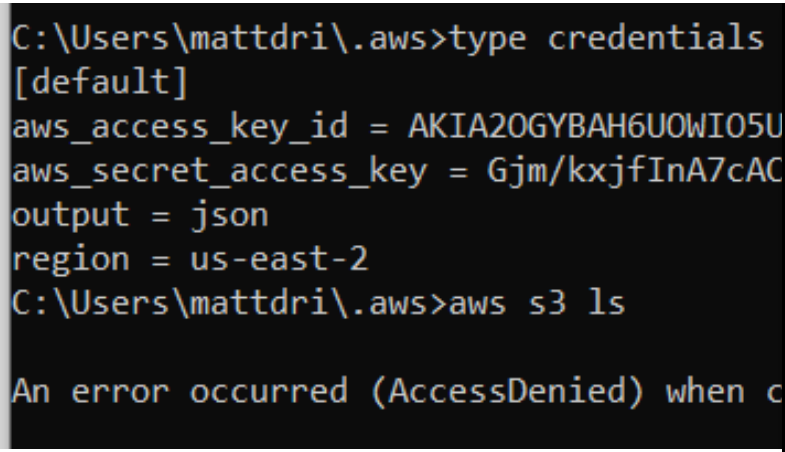
In our latest research, we at Team Nautilus found that tens of thousands of user tokens are exposed via the Travis CI API, which allows anyone to access historical clear-text logs. More than 770 million logs of free tier users are available, from which you can easily extract tokens, secrets, and other credentials associated with popular cloud service providers such as GitHub, AWS, and Docker Hub. Attackers can use this sensitive data to launch massive cyberattacks and to move laterally in the cloud.

We disclosed our findings to Travis CI, which responded that this issue is "by design", so all the secrets are currently available. All Travis CI free-tier users are potentially exposed, so we recommend rotating your keys immediately.

CI/CD Scenario

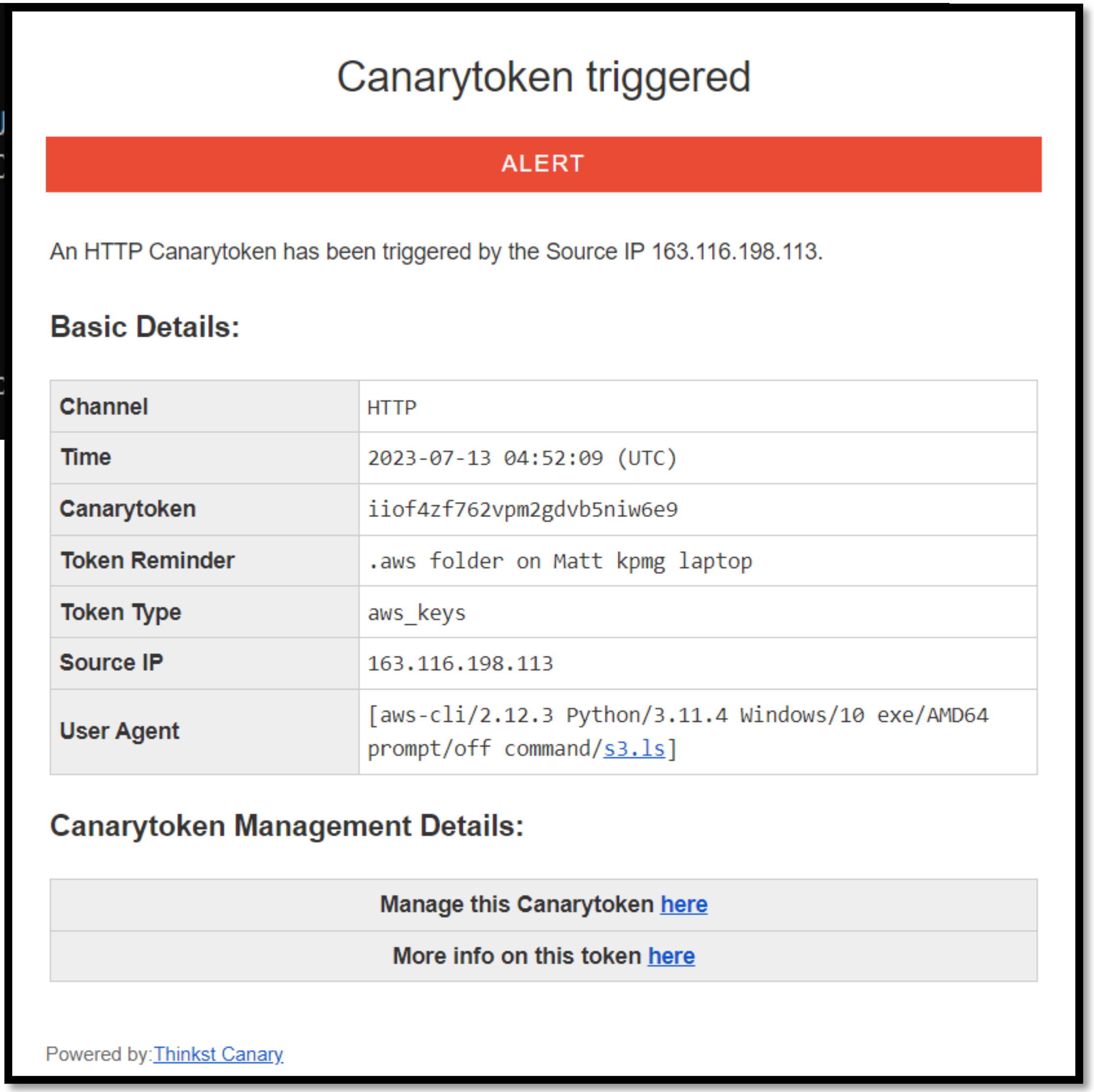


Example Email Alert



```
C:\Users\mattdri\.aws>type credentials
[default]
aws_access_key_id = AKIA2OGYBAH6UOWIO5U
aws_secret_access_key = Gjm/kxjfInA7cAC
output = json
region = us-east-2
C:\Users\mattdri\.aws>aws s3 ls

An error occurred (AccessDenied) when c
```



Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP 163.116.198.113.

Basic Details:

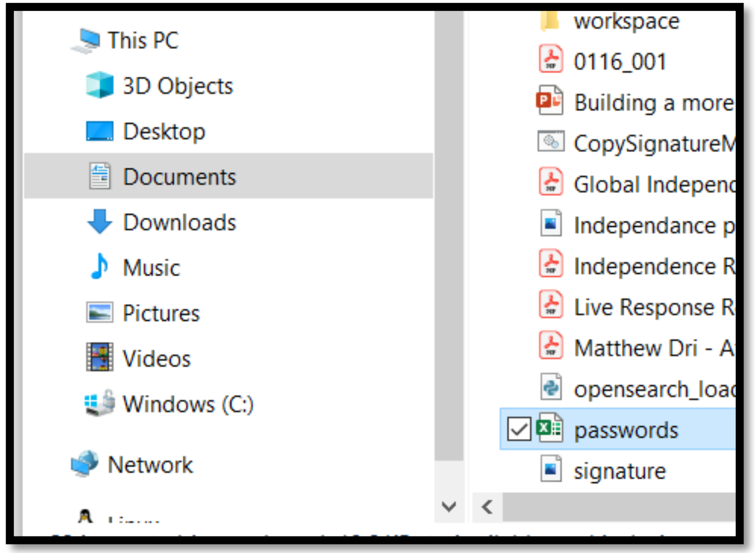
Channel	HTTP
Time	2023-07-13 04:52:09 (UTC)
Canarytoken	iiof4zf762vpm2gdvb5niw6e9
Token Reminder	.aws folder on Matt kpmg laptop
Token Type	aws_keys
Source IP	163.116.198.113
User Agent	[aws-cli/2.12.3 Python/3.11.4 Windows/10 exe/AMD64 prompt/off command/s3.ls]

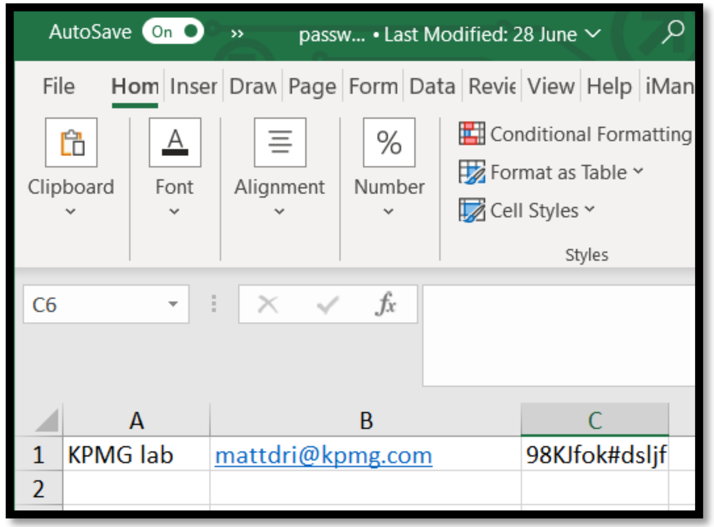
Canarytoken Management Details:

Manage this Canarytoken here
More info on this token here

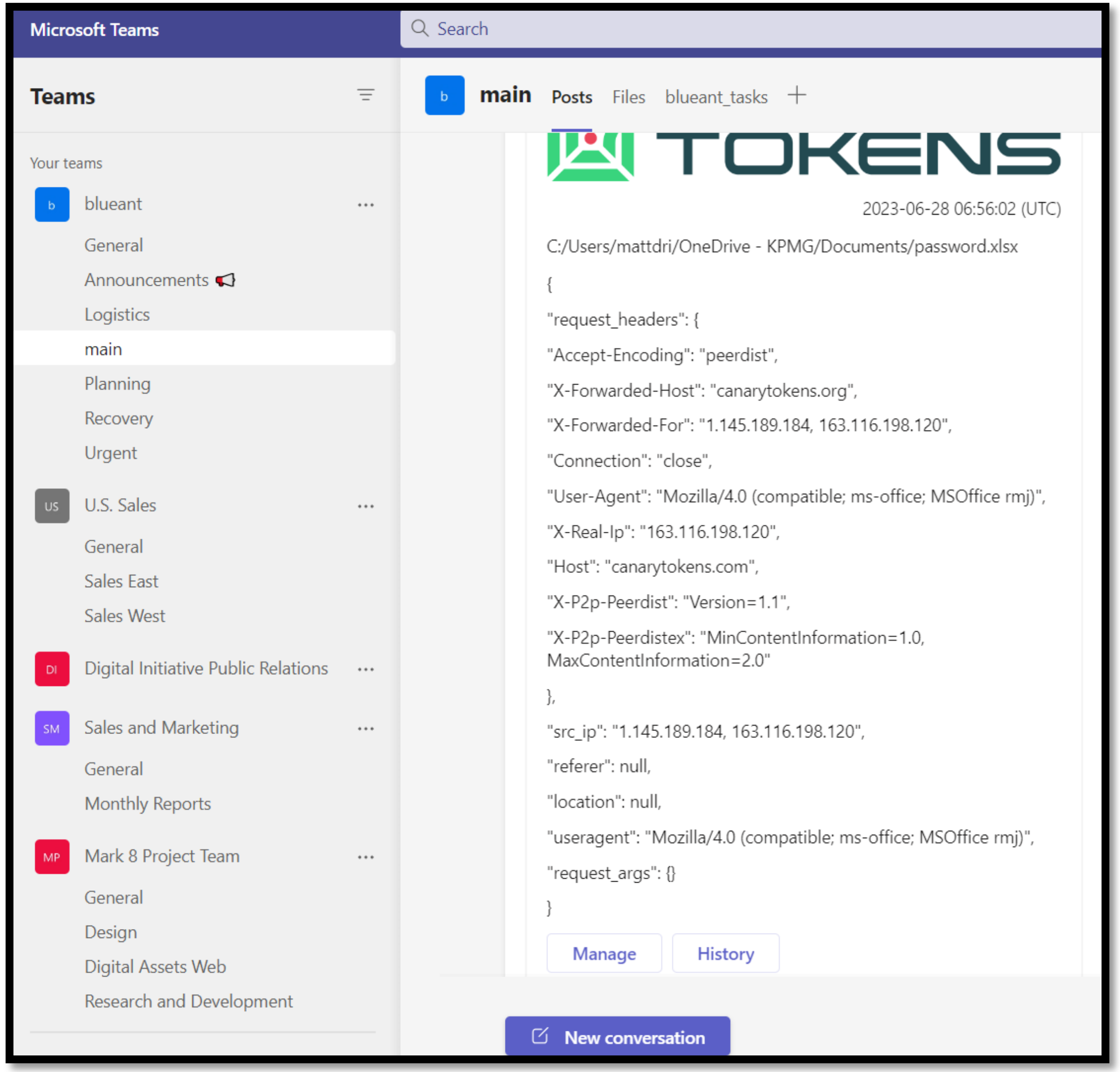
Powered by: Thinkst Canary

Example Teams Alert





	A	B	C
1	KPMG lab	mattdri@kpmg.com	98KJfok#dsljf
2			



2023-06-28 06:56:02 (UTC)

C:/Users/mattdri/OneDrive - KPMG/Documents/password.xlsx

```
{
"request_headers": {
"Accept-Encoding": "peerdist",
"X-Forwarded-Host": "canarytokens.org",
"X-Forwarded-For": "1.145.189.184, 163.116.198.120",
"Connection": "close",
"User-Agent": "Mozilla/4.0 (compatible; ms-office; MSOffice rmj)",
"X-Real-Ip": "163.116.198.120",
"Host": "canarytokens.com",
"X-P2p-Peerdist": "Version=1.1",
"X-P2p-Peerdistex": "MinContentInformation=1.0,
MaxContentInformation=2.0"
},
"src_ip": "1.145.189.184, 163.116.198.120",
"referer": null,
"location": null,
"useragent": "Mozilla/4.0 (compatible; ms-office; MSOffice rmj)",
"request_args": {}
}
```

Cyber Kill Chain - Credential focus

Reconnaissance

- Attack surface scanning
- Harvesting credentials
- Open-source intelligence
- Dark markets

Weaponisation

- Phishing infrastructure prepared
- Preparation for credential attack
- Remote access setup

Delivery

- Sending phishing emails
- Execution of credential attacks
- Social engineering

Exploitation

- Use of credentials
- Password reset flow exploitation
- Credential stuffing
- Brute force

Installation

- Creation of additional accounts

Command and Control

- Lateral movement

Actions on Objectives

- Theft
- Destruction
- Encryption
- Exfiltration

Detection Ideation

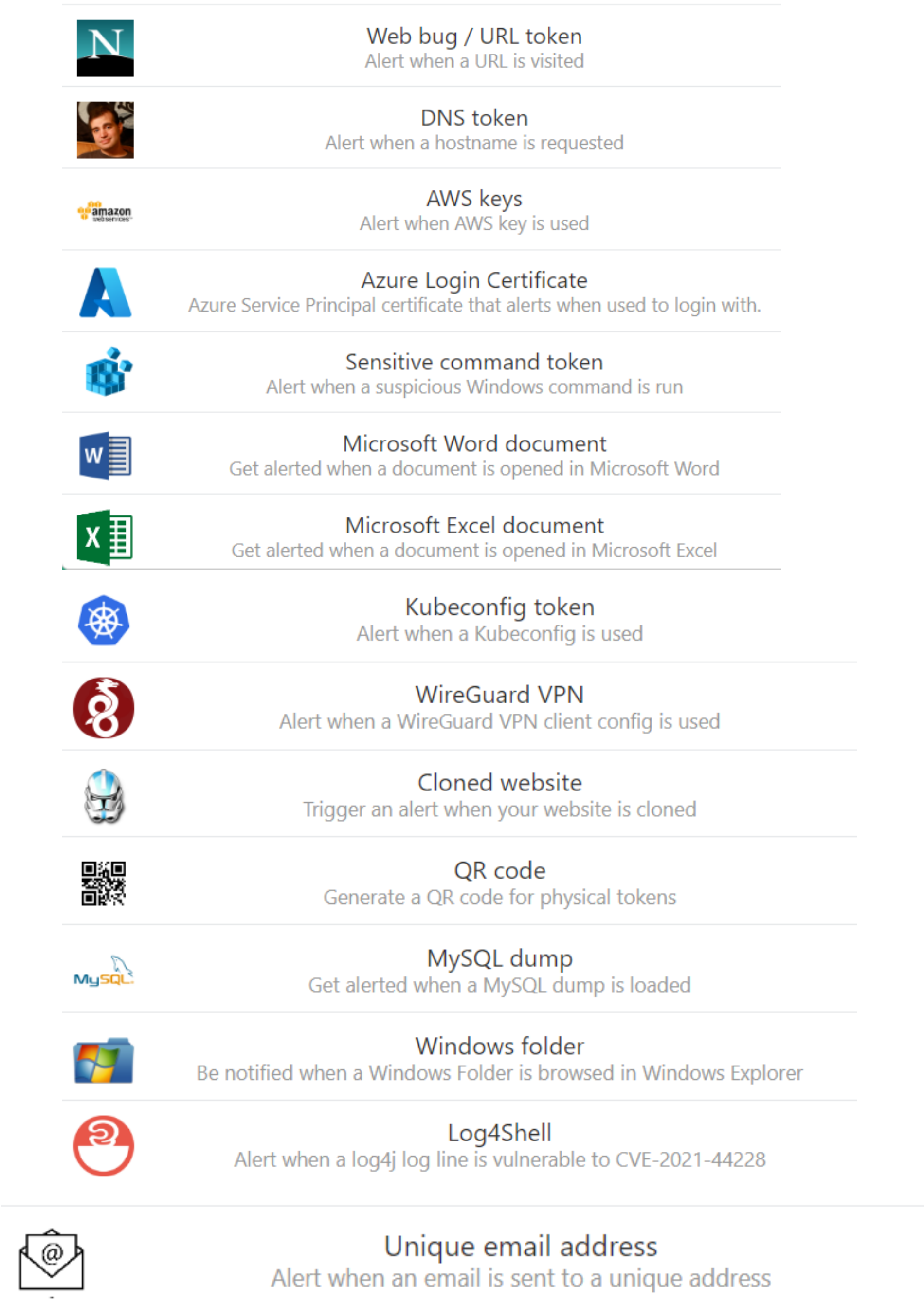
- Store Azure/AWS credentials within mailboxes
- Store VPN login instructions.docx in mailboxes
- Host “Admin credentials” documents in desktop support shared drives
- Fake cyber insurance policy document
- Inject credentials into public channels in Teams and Slack
- Expose AWS access keys to instances using environment variables
- Store AWS access keys and Azure credentials in S3 buckets / Azure storage
- Store AWS and Azure credentials within private code repositories
- Insert into web pages discovered via enumeration
- Create emails with luring subjects like “credit card” and embed URL/ image tokens

Power Up

- Strategic Canary deployment
  - Develop an understanding of how the team works
  - Perform threat modelling
  - Enable team members to build their own Canaries

- Use at risk credentials
  - Credentials get on sold and included in combination lists
  - Ingest the relevant logs and build detections
  - Use of at risk credentials could be the precursor to additional attacks

- Active Defence
  - Session invalidation
  - Host isolation
  - Incident escalation



Web bug / URL token
Alert when a URL is visited

DNS token
Alert when a hostname is requested

AWS keys
Alert when AWS key is used

Azure Login Certificate
Azure Service Principal certificate that alerts when used to login with.

Sensitive command token
Alert when a suspicious Windows command is run

Microsoft Word document
Get alerted when a document is opened in Microsoft Word

Microsoft Excel document
Get alerted when a document is opened in Microsoft Excel

Kubeconfig token
Alert when a Kubeconfig is used

WireGuard VPN
Alert when a WireGuard VPN client config is used

Cloned website
Trigger an alert when your website is cloned

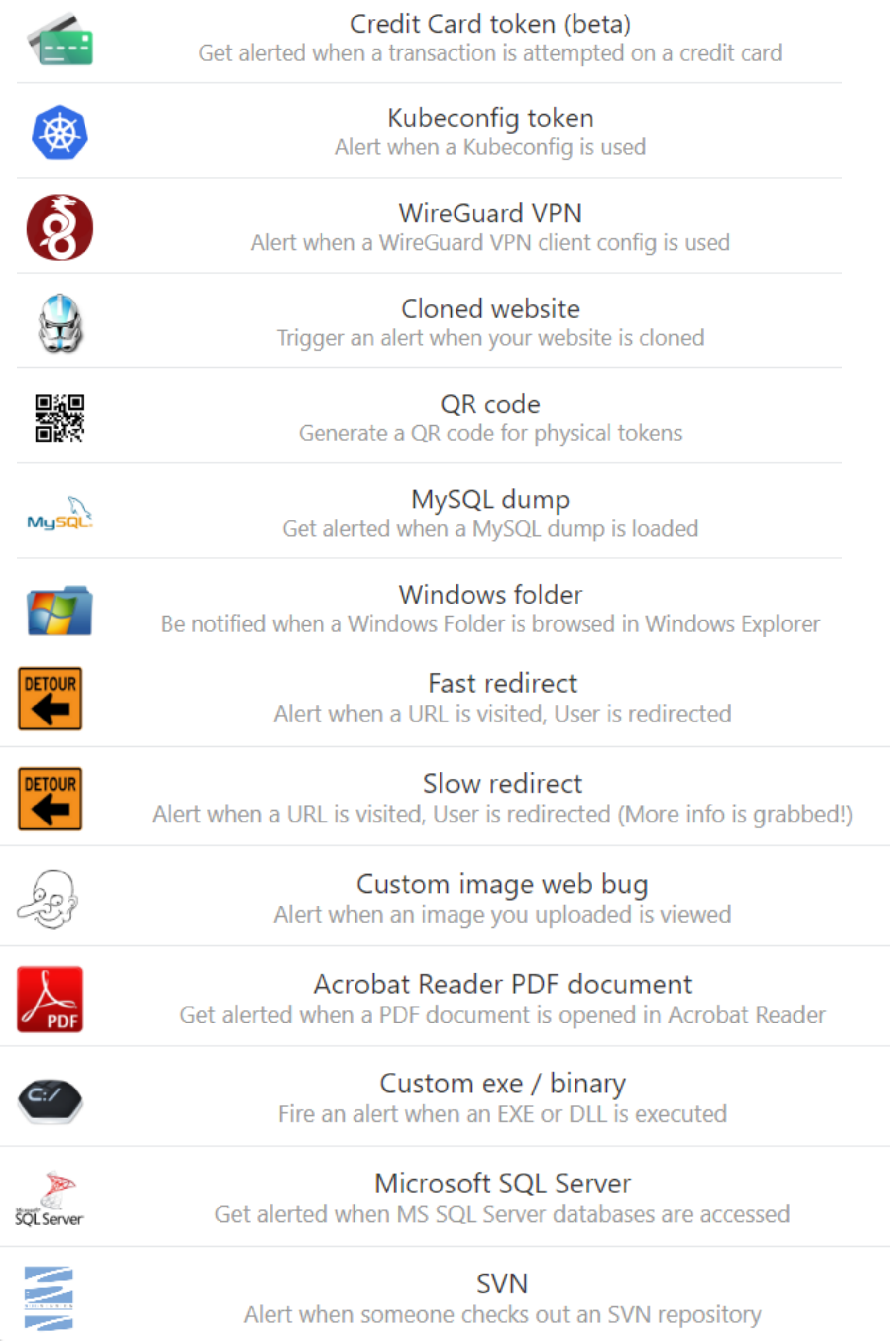
QR code
Generate a QR code for physical tokens

MySQL dump
Get alerted when a MySQL dump is loaded

Windows folder
Be notified when a Windows Folder is browsed in Windows Explorer

Log4Shell
Alert when a log4j log line is vulnerable to CVE-2021-44228

Unique email address
Alert when an email is sent to a unique address



Credit Card token (beta)
Get alerted when a transaction is attempted on a credit card

Kubeconfig token
Alert when a Kubeconfig is used

WireGuard VPN
Alert when a WireGuard VPN client config is used

Cloned website
Trigger an alert when your website is cloned

QR code
Generate a QR code for physical tokens

MySQL dump
Get alerted when a MySQL dump is loaded

Windows folder
Be notified when a Windows Folder is browsed in Windows Explorer

Fast redirect
Alert when a URL is visited, User is redirected

Slow redirect
Alert when a URL is visited, User is redirected (More info is grabbed!)

Custom image web bug
Alert when an image you uploaded is viewed

Acrobat Reader PDF document
Get alerted when a PDF document is opened in Acrobat Reader

Custom exe / binary
Fire an alert when an EXE or DLL is executed

Microsoft SQL Server
Get alerted when MS SQL Server databases are accessed

SVN
Alert when someone checks out an SVN repository