Threatle - predicting the future of threats in 6 steps

Judgement Day, Slovakia, May 2023

@vanjasvajcer

Who am I?

Vanja Svajcer

Security Researcher at Cisco Talos

- Automated analysis
- Mobile malware
- WinDBG
- Telemetry analysis

Based in Croatia

Threatle – predicting the future of threats in 6 steps

1. Defender teams
2. Defender tools
3. Adversary
4. Threats
5. Technology

Cisco Security Research

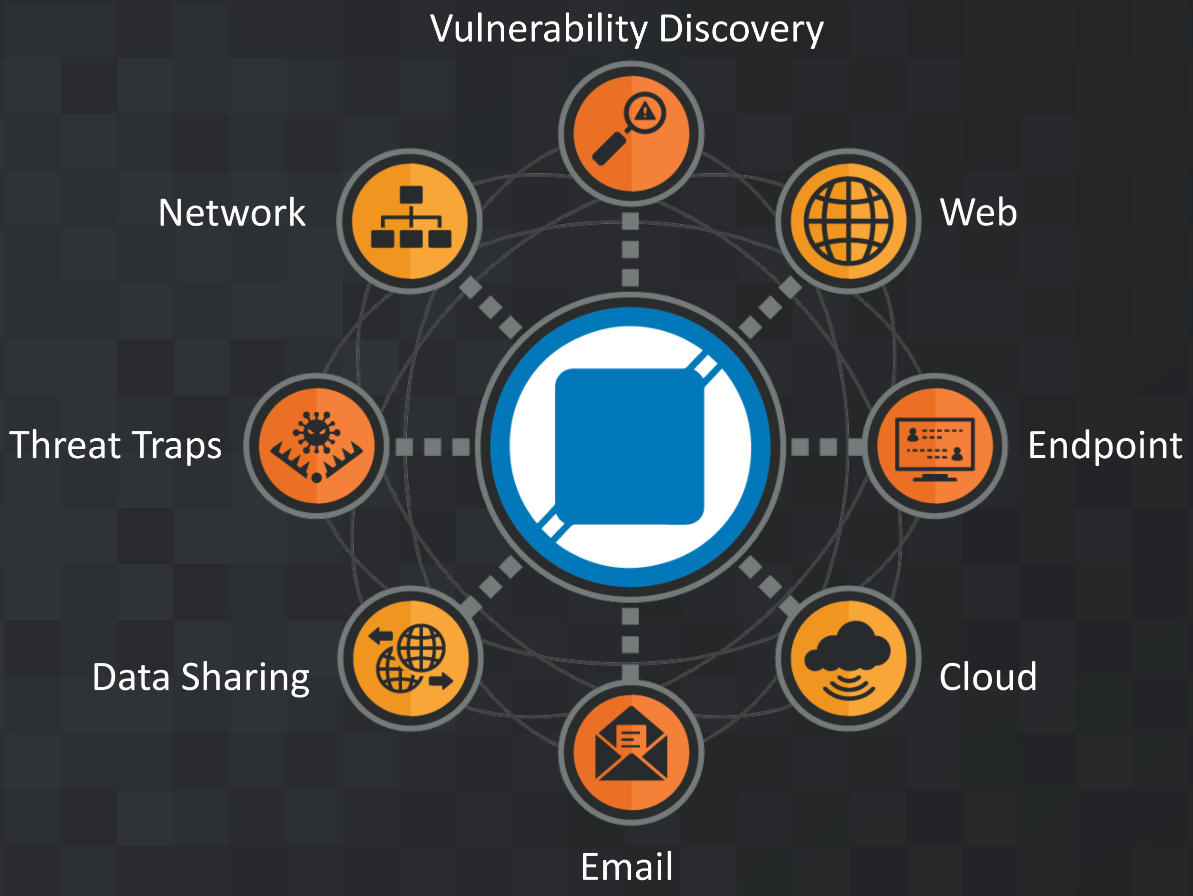
T	R	E	A	T
T	A	I	N	T
T	A	L	L	Y
T	A	C	O	S
T	A	L	O	S

Talos

Talos Role at Cisco

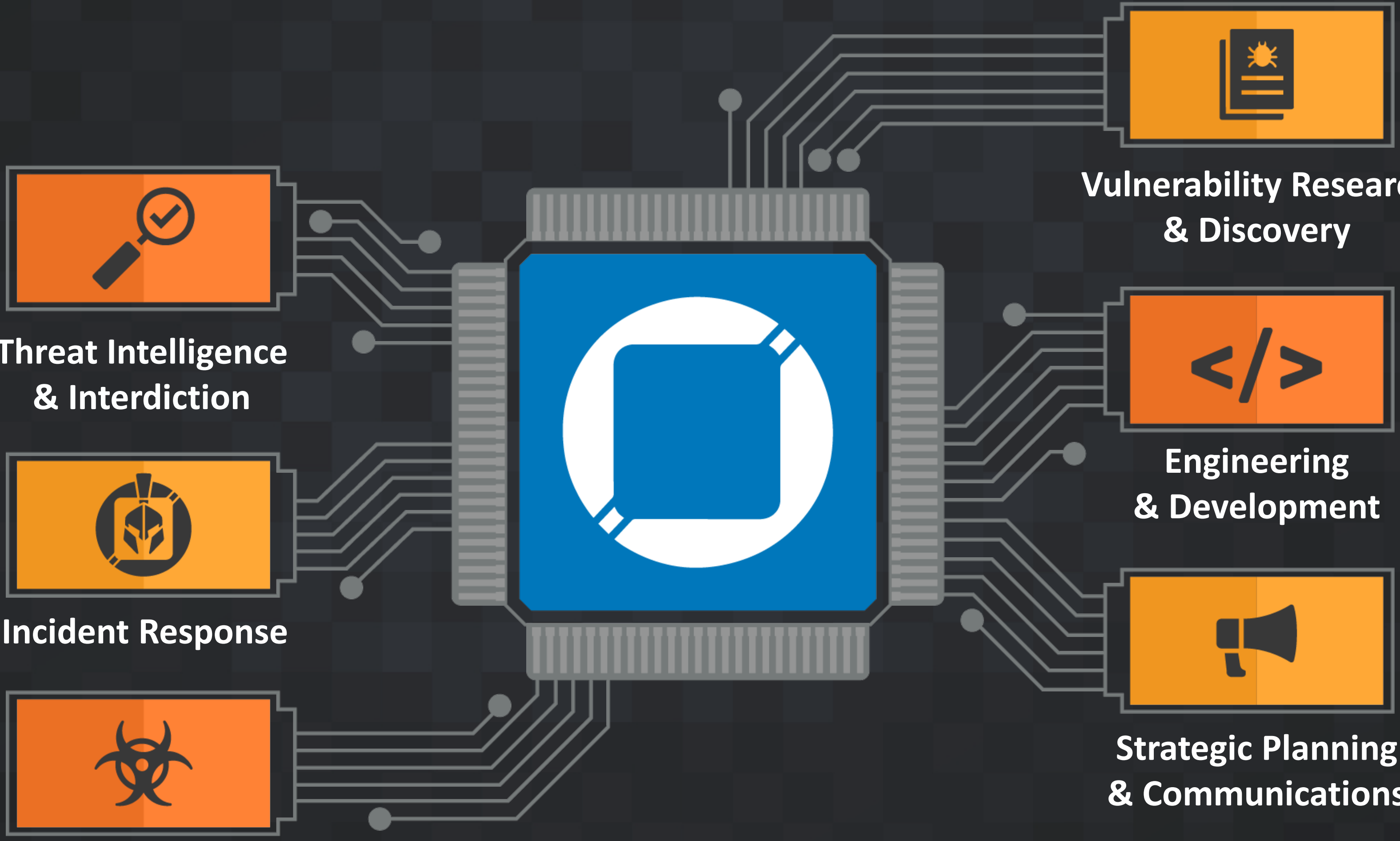
Protecting Customers.

- Build new detection logic to improve Cisco products (block, behavior analysis, and reputation/categorization)
- Work with national security and law enforcement partners to keep the world safe
- Gather intelligence & first-person research on cyber threat actors, tools, and techniques.
- Communicate findings through blog posts, intel bulletins to customers and sharing with industry partners



Our job is protecting your network

Talos is the threat intelligence group at Cisco. We are here to fight the good fight — we work to keep our customers, and users at large, safe from malicious actors.



Threat Intelligence & Interdiction

Incident Response

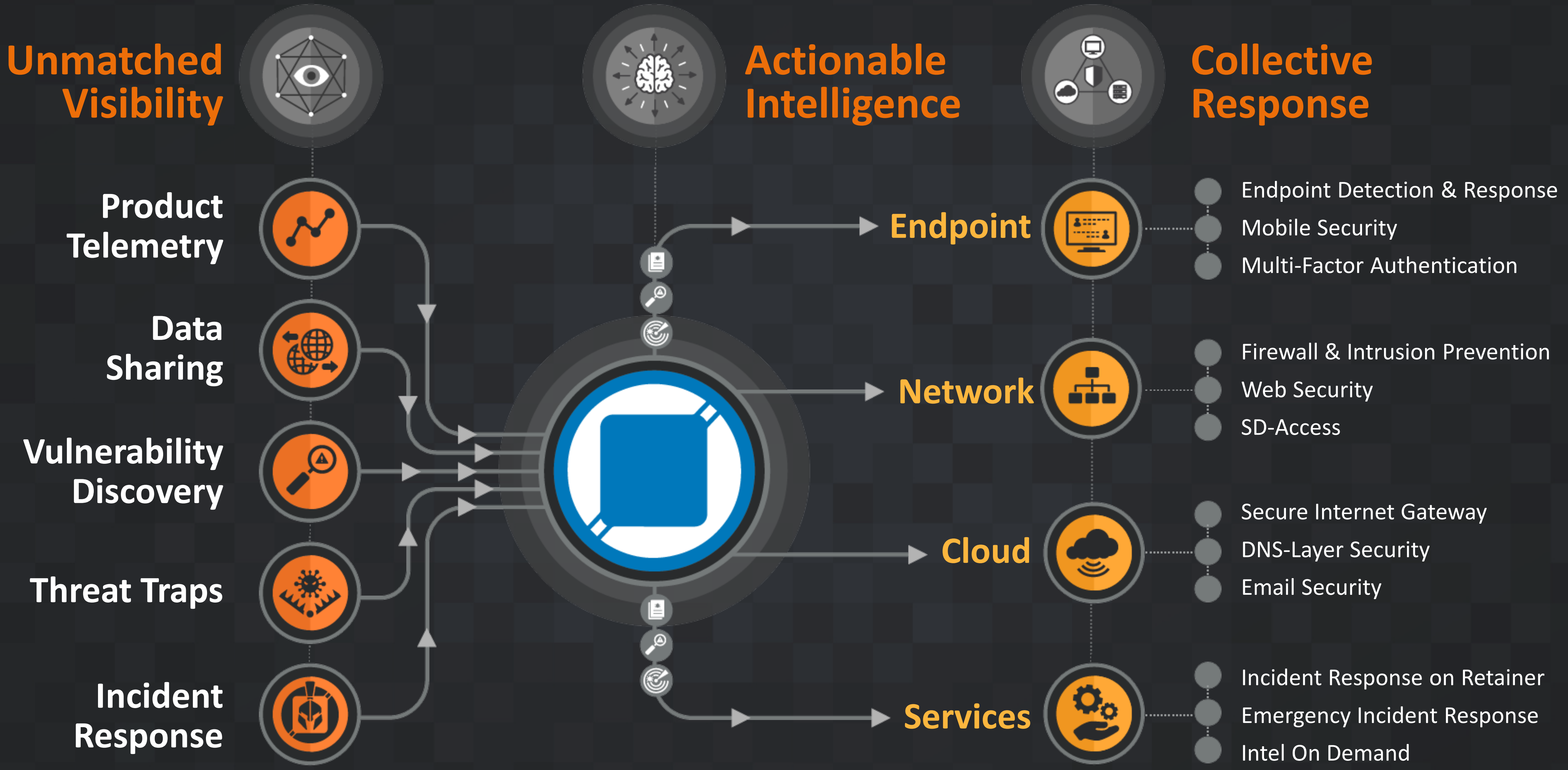
Detection Research

Vulnerability Research & Discovery

Engineering & Development

Strategic Planning & Communications

From Unknown to Understood



Unmatched Visibility

- Product Telemetry
- Data Sharing
- Vulnerability Discovery
- Threat Traps
- Incident Response

Actionable Intelligence

Collective Response

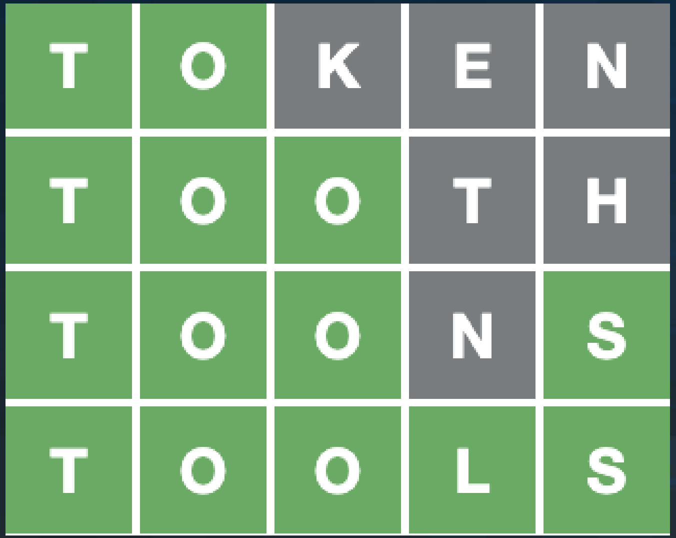
Endpoint
- Endpoint Detection & Response
- Mobile Security
- Multi-Factor Authentication

Network
- Firewall & Intrusion Prevention
- Web Security
- SD-Access

Cloud
- Secure Internet Gateway
- DNS-Layer Security
- Email Security

Services
- Incident Response on Retainer
- Emergency Incident Response
- Intel On Demand

CISCO | TALOS



T	O	K	E	N
T	O	O	T	H
T	O	O	N	S
T	O	O	L	S

Tools

Data analytics

- Log and telemetry ingestion
- Threat Intelligence platforms (big data)
- Machine learning and anomaly detection
- AI for classification

Threat analysis

- Large scale automated static and dynamic
- Similarity and clustering
- Graph based actor tracking
- ATT&CK
- Mature manual analysis tools and process

Detection Comes in Different Flavors

Malware Families

i.e. Emotet/Qbot/Trickbot

Technical Detection:

Indicated Threat

- NGIPS/NGFW Signature on
- Command and Control (C2) Activity
- ClamAV Signature for system activity
- C2 IP Address/Domain Blocked

Applicable to Specific Threat

Some detections are designed with a specific threat in mind, others are designed to catch malicious behavior

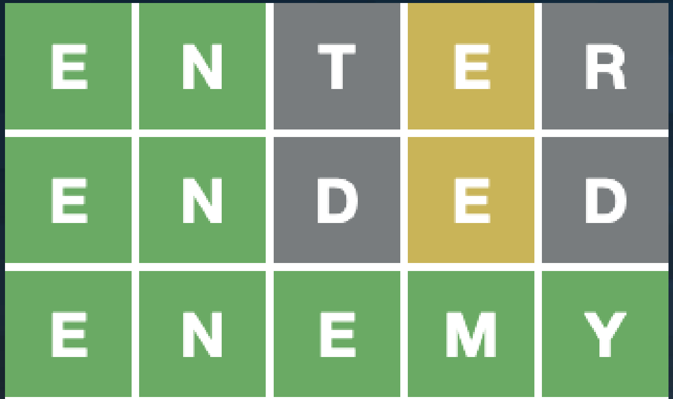
Behavioral Protections:

Indicated actor

- Bitsadmin used to download file
- Powershell used to disable EDR
- Scheduled Task Created
- Connection blocked to suspected phishing page

Applicable to all malicious activity

cisco | Talos



E	N	T	E	R
E	N	D	E	D
E	N	E	M	Y

Adversary

Commodity (common)

Ransomware & double extortion

Tools

- Emotet, Qbot and various Loaders
- Docs, Exec, PDFs, RTFs
- RaaS

Tactics

- Spam with embedded files
- Link based Spam
- Tor and Bitcoin/Crypto currency

Description

- Lots of Individual Actors
- Spray and Pray
- Disruptive Nuisance

Processes

- Encrypts files.
- Some contain lateral movement functionality or share encryption

TALOS

Infostealers (Redline)

Loss of sensitive or proprietary data, especially financial data

Exfiltrated data could be used for a wide range of malicious follow-on activity

Potentially indicative of a much larger security breach involving other malware families

Spamming botnets - Emotet

Tools

- Modular payloads including ransomware
- Multiple botnets distributing threat
- Network based propagation

Tactics

- Email Delivery Common (URL & Maldoc)
- Malware Downloaders Common (.DOCX, .XLSX, etc)
- Polymorphic/Sandbox Evasion

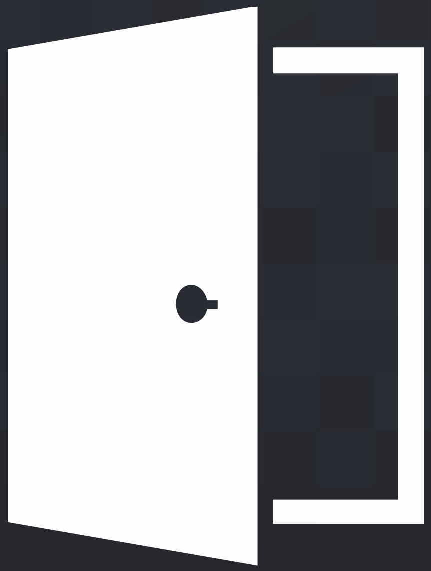
Description

- Banking Trojan + a lot more
- Modular Malware
- Widespread global distribution

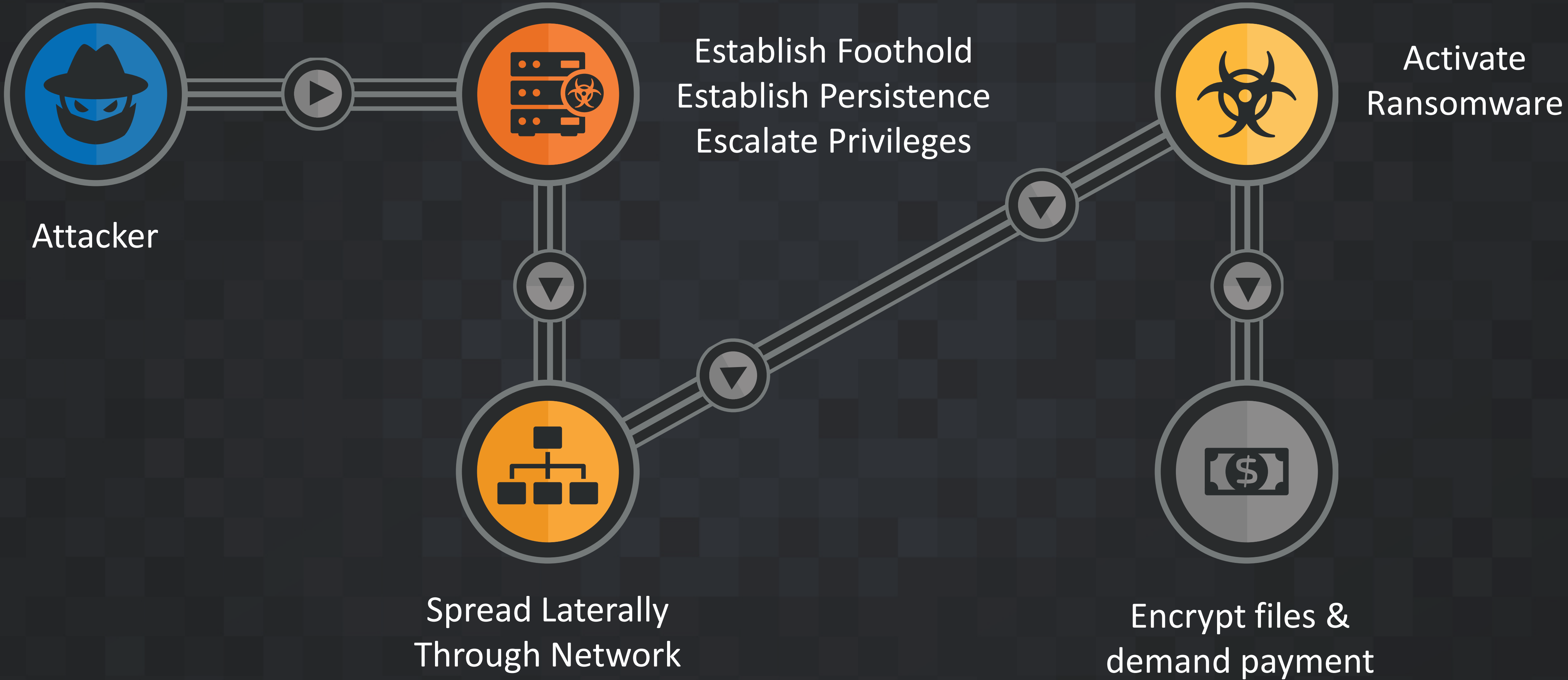
Processes

- Get foothold, gather information
- Base payload on highest ROI
- Sophisticated commodity malware

Opportunistic (Targeted)



“Big Game Hunting”



Attacker

Establish Foothold
Establish Persistence
Escalate Privileges

Spread Laterally
Through Network

Activate
Ransomware

Encrypt files &
demand payment

Cisco Security Research

Nation (APT)

Cisco Security Research

Cisco Talos & Ukraine

Previous assistance

- Six years in region
- On the ground during NotPetya
- Assisted with forensic analysis multiple events
- Assisted in monitoring of election infrastructure during 2019 presidential election

Partnerships

- State Special Communications Service of Ukraine (SSSCIP)
- Cyberpolice Department of the National Police of Ukraine
- National Coordination Center for Cybersecurity (NCCC at the NSDC of Ukraine)

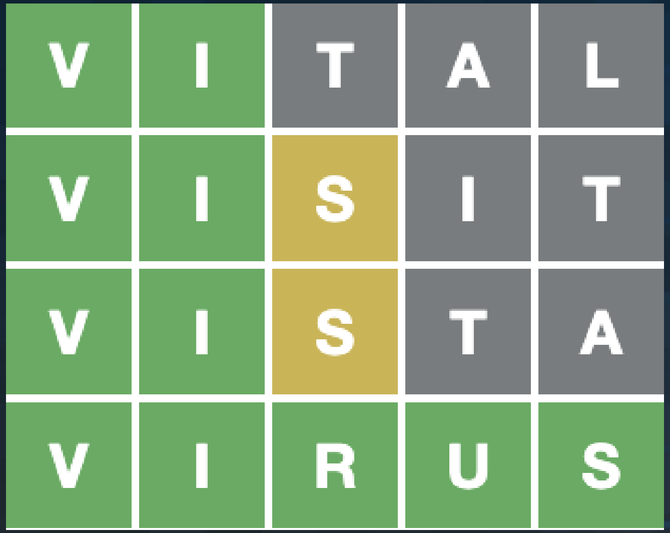
Current assistance

- Providing defensive guidance
- Assisting with forensic analysis
- Providing intelligence
- Assisting in hunting activities

ACTOR PROFILE

Gamaredon Group

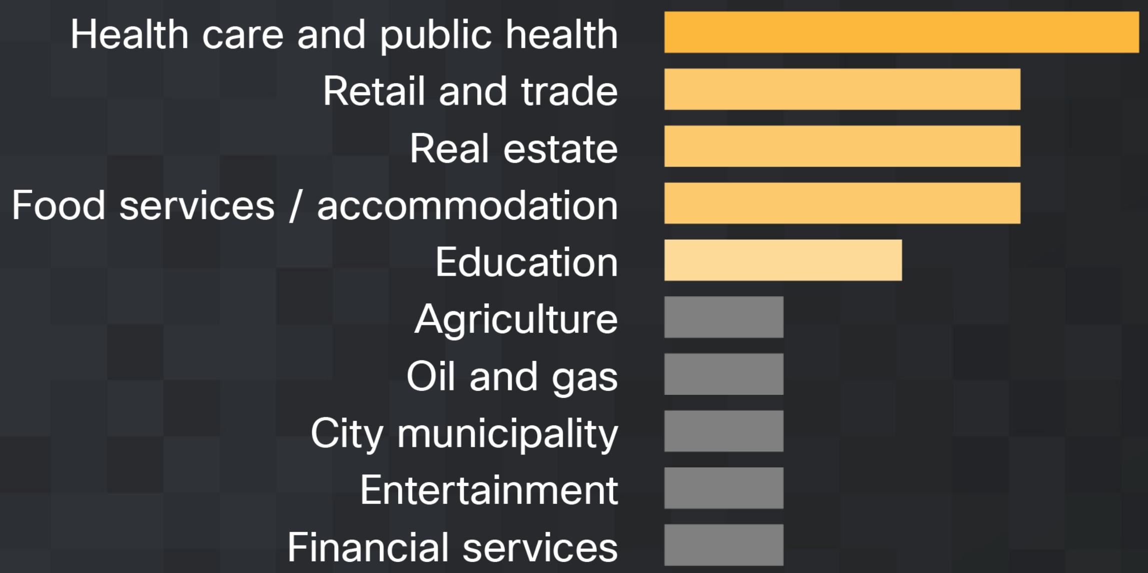
Aliases	Primitive Bear, Armageddon, Shuckworm, Winterflouder, BlueAlpha, BlueOtso, IronTiden, SectorC08, Callisto, Trident Ursa
Affiliations	Russia
Active since	2013
Goals	Espionage, data theft, establishing long-term access
Victimology	Actively targets Ukrainian entities, specifically government organizations, critical infrastructure and entities affiliated with Ukraine's defense, security and law enforcement apparatus. Secondary operations include broad targeting of entities in Europe and globally, including, government, military, humanitarian and non-profit organizations.
Notable TTPs	Social engineering techniques, spear-phishing, compromised domains and dynamic DNS, long-term access, data exfiltration, custom script-based malware.
Malware & tooling	Gamaredon employs a variety of custom, self-developed implants that are used exclusively by the adversary ranging from customized script-based malware to infostealers and backdoors. Notable malware families include GammaLoad, GammaSteel, Giddome, Powerpunch and Pterodo.



V	I	T	A	L
V	I	S	I	T
V	I	S	T	A
V	I	R	U	S

Threats – the daily reality

Attackers targeted health care and public health companies the most in the first quarter of 2023



Observed Trends

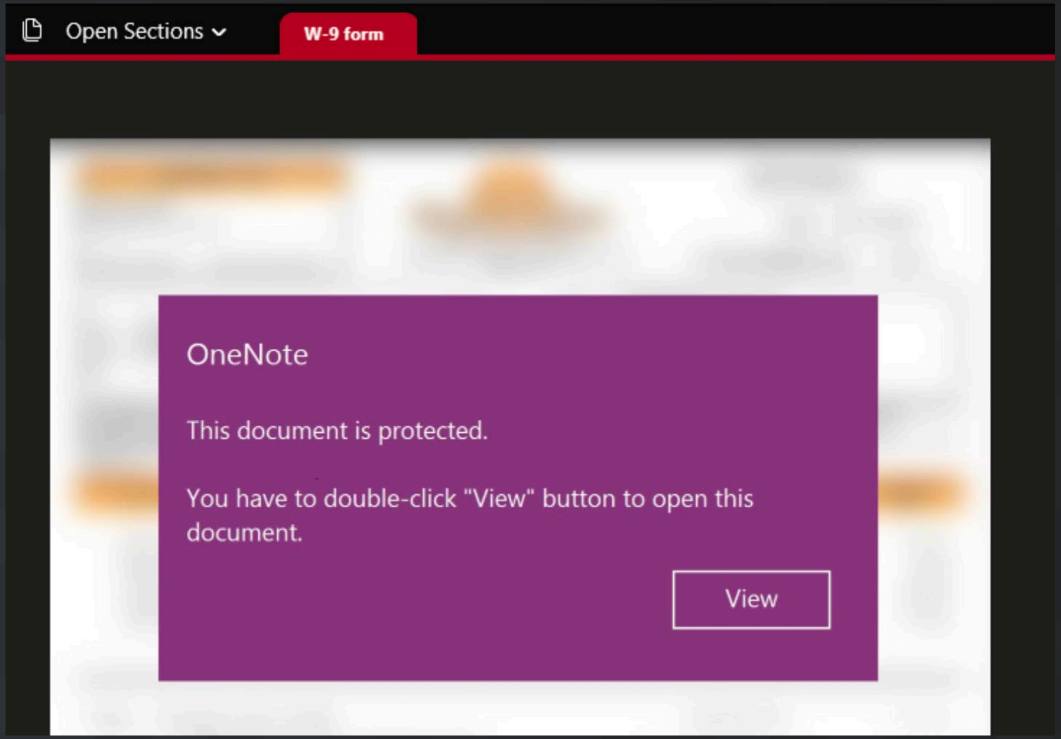
Most-observed threat was web shells

Top initial vector was exploitation of public-facing applications

Top weakness was lack of MFA

Malicious OneNote documents continue to be leveraged this quarter

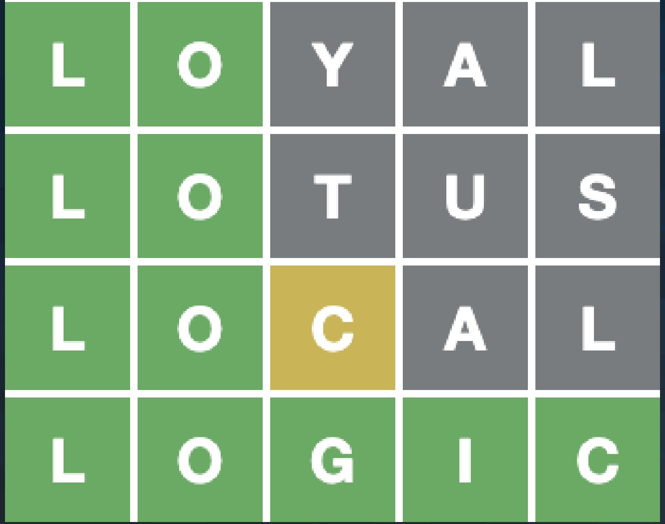
- Qakbot (Qbot) commodity loader
- Looking forward: Emotet



OneNote

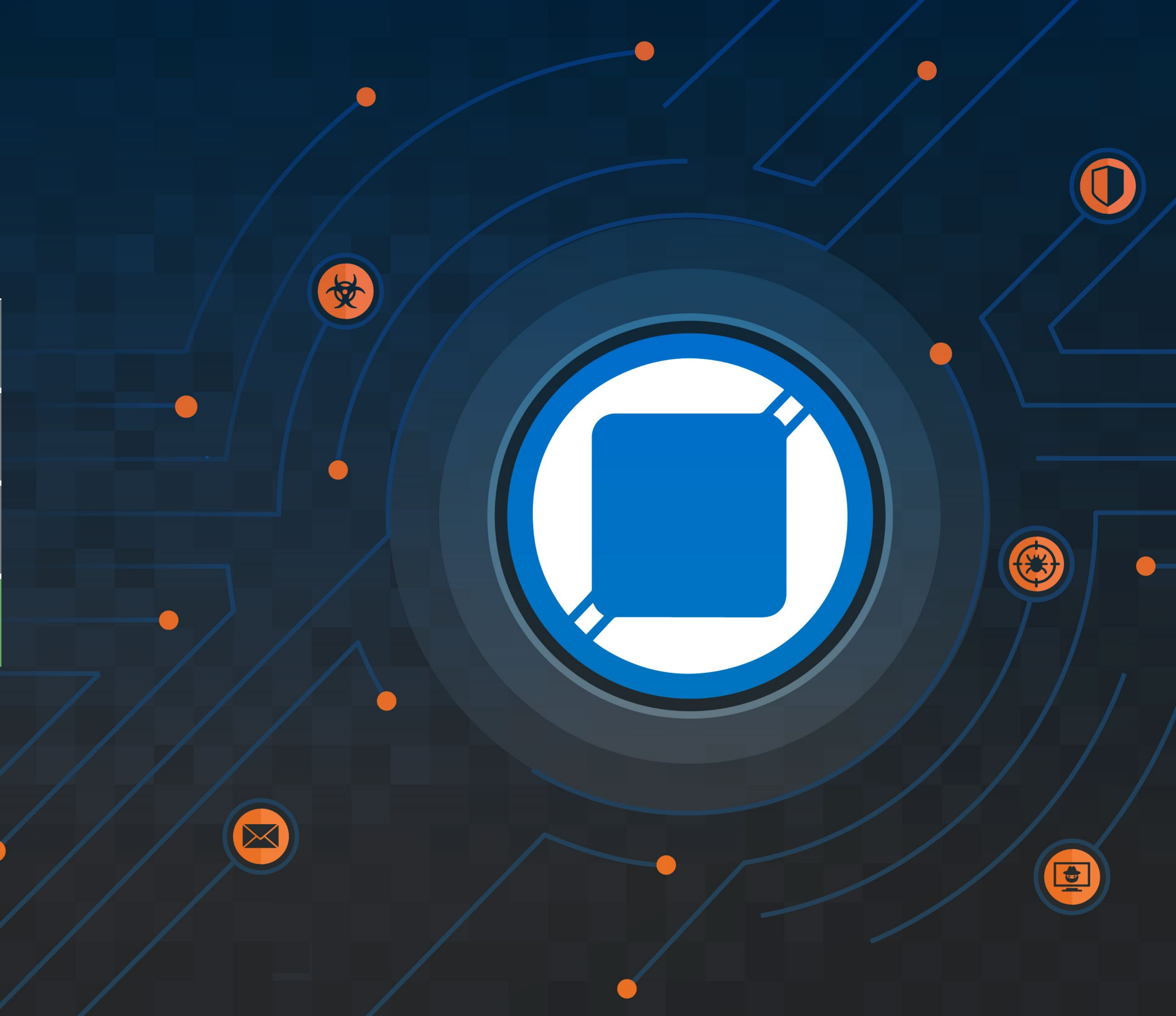
This document is protected.

You have to double-click "View" button to open this document.

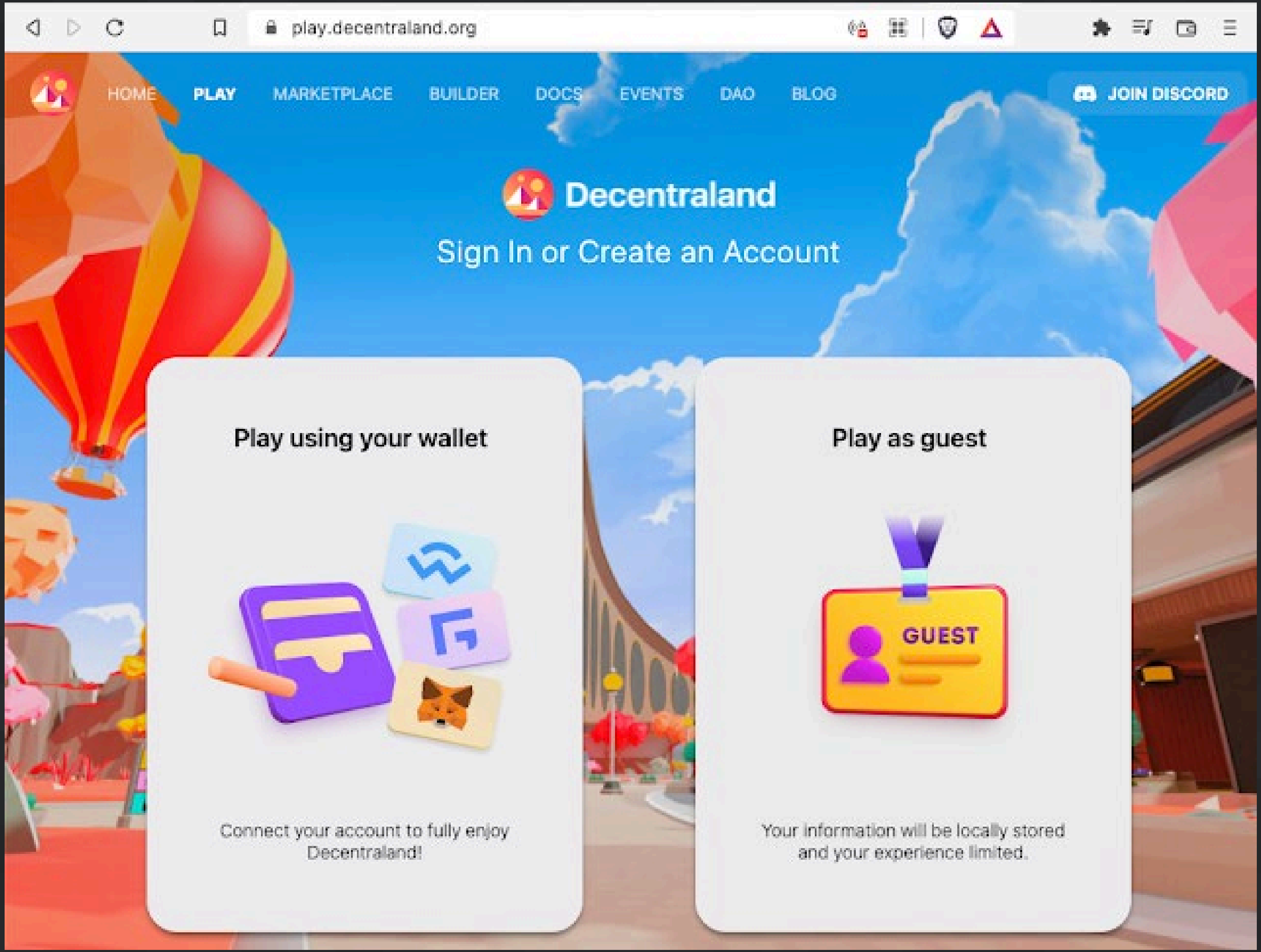


L	O	Y	A	L
L	O	T	U	S
L	O	C	A	L
L	O	G	I	C

Technology



Web 3.0 “revolution”



play.decentraland.org

Decentraland

Sign In or Create an Account

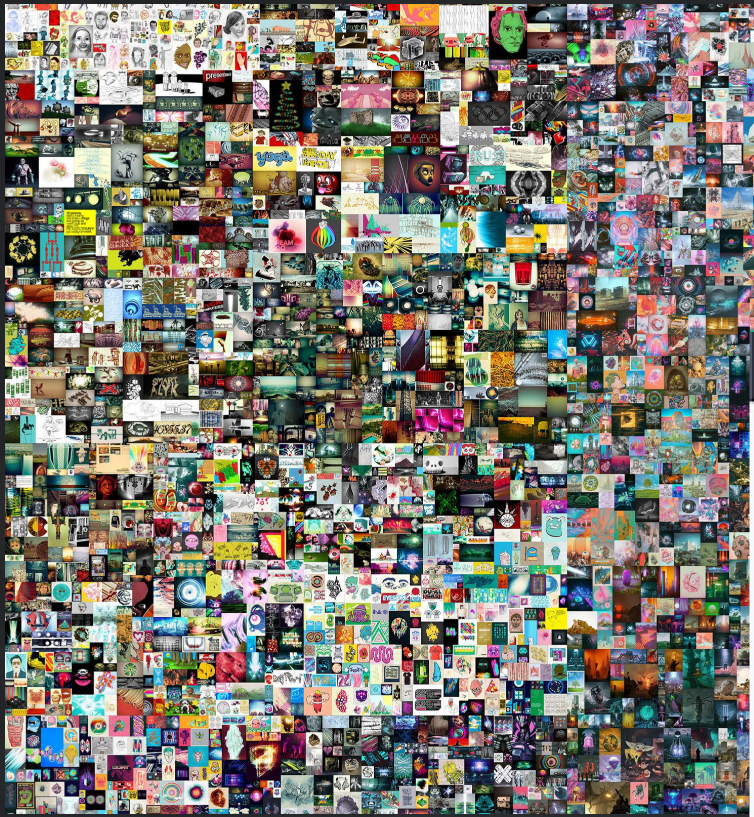
Play using your wallet

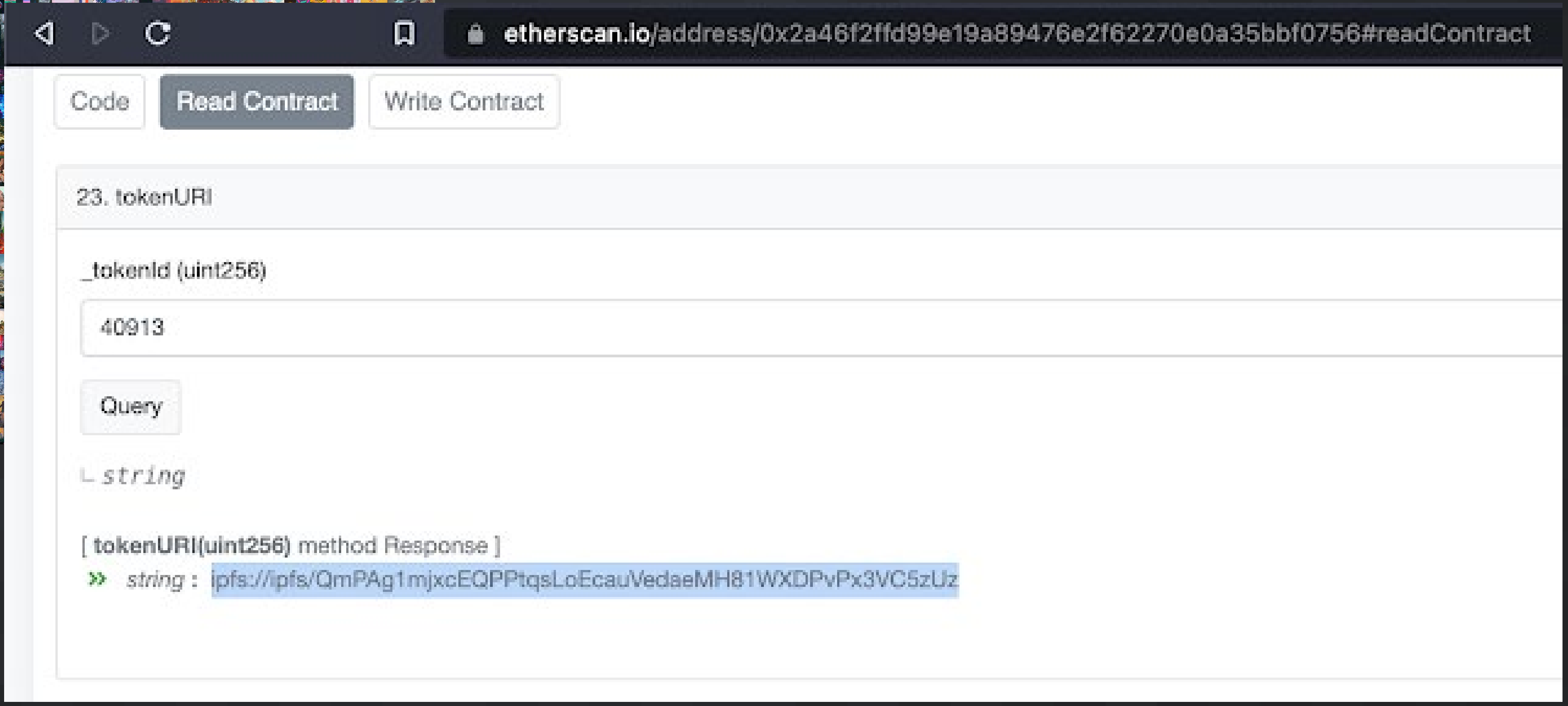
Connect your account to fully enjoy Decentraland!

Play as guest

Your information will be locally stored and your experience limited.

NFTs Use IPFS Too!





etherscan.io/address/0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756#readContract

23. tokenURI

_tokenId (uint256)

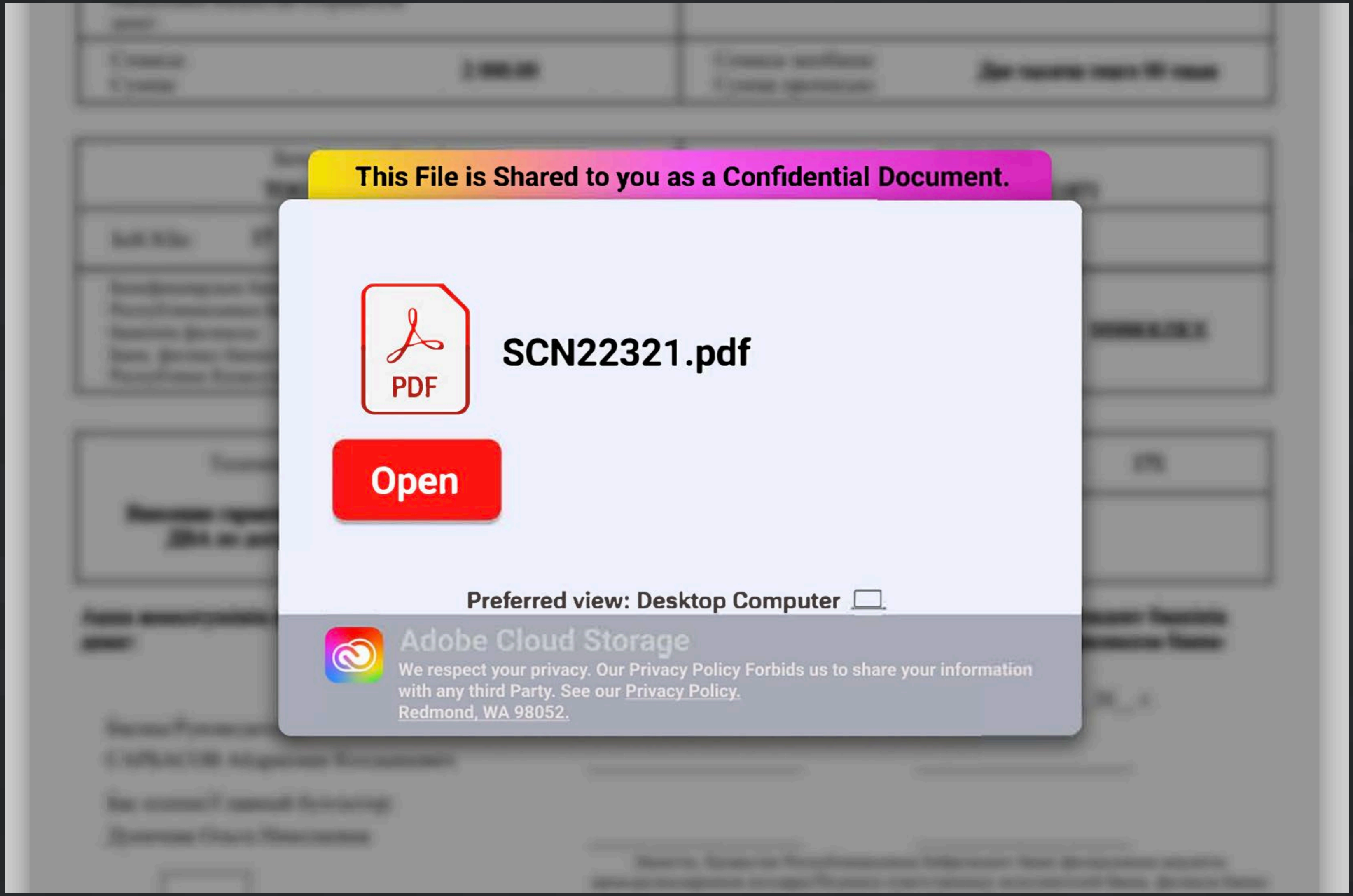
40913

└ *string*

[**tokenURI(uint256)** method Response]

» *string* : ipfs://ipfs/QmPAg1mjxcEQPPtqsLoEcauVedaeMH81WXDPvPx3VC5zUz

Email Attachment PDF



This File is Shared to you as a Confidential Document.

SCN22321.pdf

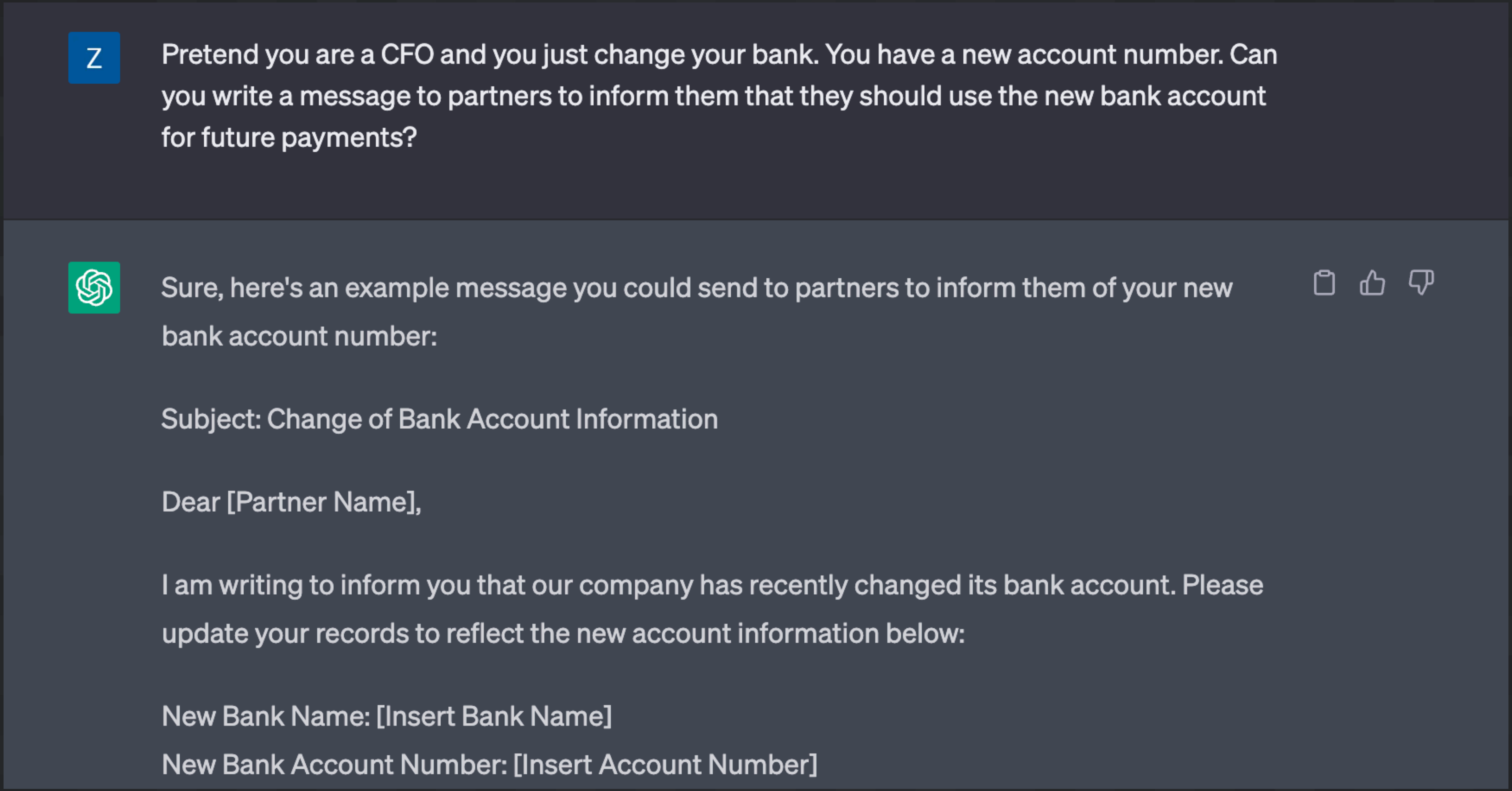
Preferred view: Desktop Computer

Adobe Cloud Storage

We respect your privacy. Our Privacy Policy Forbids us to share your information with any third Party. See our Privacy Policy.

Redmond, WA 98052.

Generative AI to rescue



Pretend you are a CFO and you just change your bank. You have a new account number. Can you write a message to partners to inform them that they should use the new bank account for future payments?

Sure, here's an example message you could send to partners to inform them of your new bank account number:

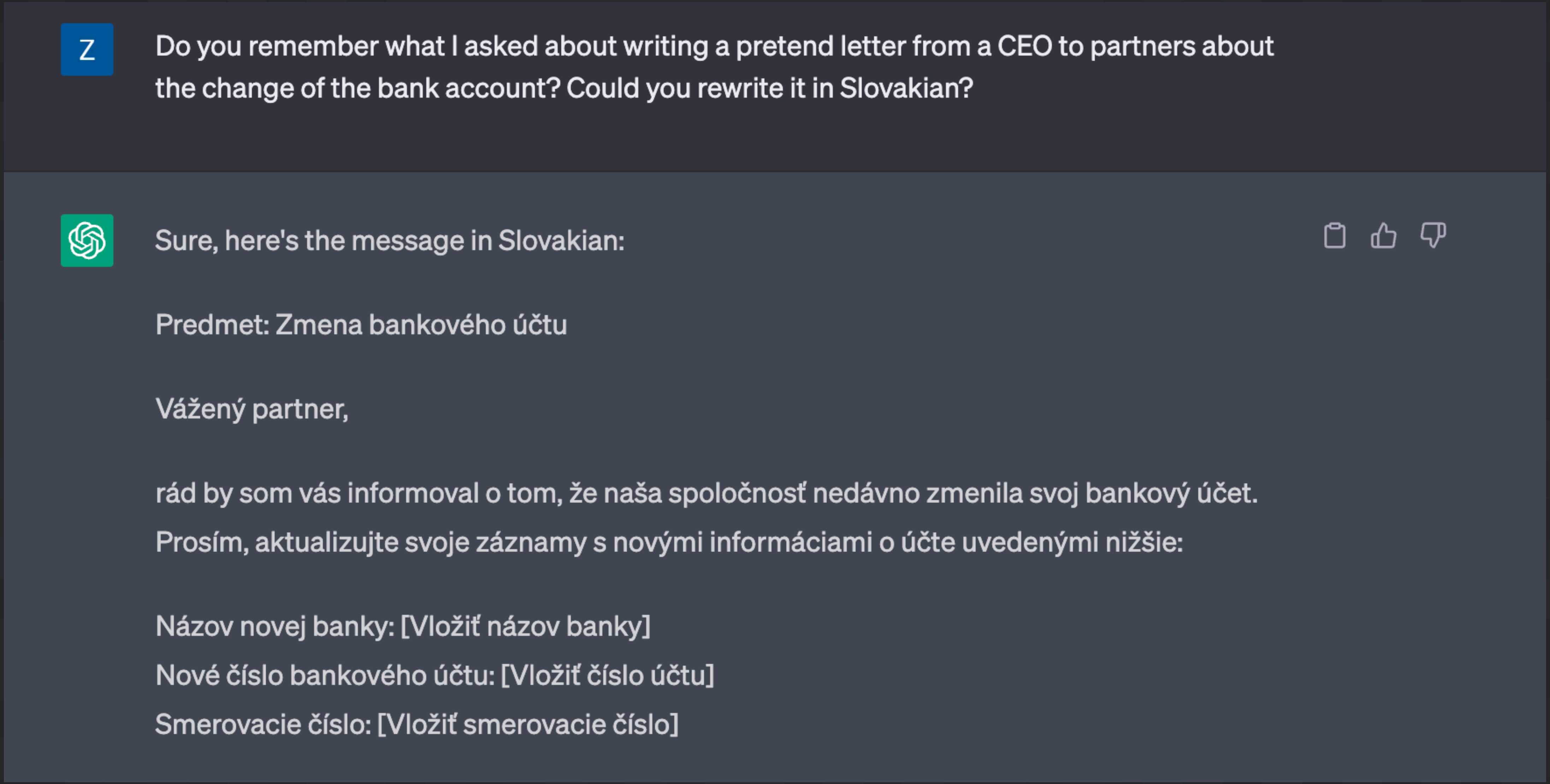
Subject: Change of Bank Account Information

Dear [Partner Name],

I am writing to inform you that our company has recently changed its bank account. Please update your records to reflect the new account information below:

New Bank Name: [Insert Bank Name]
New Bank Account Number: [Insert Account Number]

Generative AI to rescue



Z

Do you remember what I asked about writing a pretend letter from a CEO to partners about the change of the bank account? Could you rewrite it in Slovakian?

Sure, here's the message in Slovakian:

Predmet: Zmena bankového účtu

Vážený partner,

rád by som vás informoval o tom, že naša spoločnosť nedávno zmenila svoj bankový účet. Prosím, aktualizujte svoje záznamy s novými informáciami o účte uvedenými nižšie:

Názov novej banky: [Vložiť názov banky]
Nové číslo bankového účtu: [Vložiť číslo účtu]
Smerovacie číslo: [Vložiť smerovacie číslo]

The Future of threats

(It is all about the potential)

The future

- Maturing LLMs used by threat actors
- New trends and techniques discovered
- Supply chain attacks major threat
- Further down – automated discovery 0 days
- Same problems and same distance between the opponents

Q&A

TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity