Shut Up 'n Hide Yer Data

Luca Caviglione

PhD Summer School

Extreme-scale Big Data Analytics and Scientific Computing on Heterogeneous Platforms

Villa Grumello - Lake Como
September 26-30, 2022

EVEREST
DESIGN ENVIRONMENT
FOR EXTREME-SCALE BIG DATA ANALYTICS
ON HETEROGENEOUS PLATFORMS

imati

Outline

- A Short Introduction to Information Hiding
- Why are we Here?
- Part One: Hiding Data for Offending
- Part Two: Hiding Data for Defending
- Takeaway Messages
- Conclusions

Information Hiding

- **Information Hiding** is part of a wide spectrum of methods that are used to make secret data difficult to notice.
- **Steganography** is one of the most well-known subfields of Information Hiding.
- Steganography vs **Cryptography**:
  - Steganography: information is difficult to notice;
  - Cryptography: information is difficult to comprehend.
- Information Hiding and cryptography can be used **jointly!**

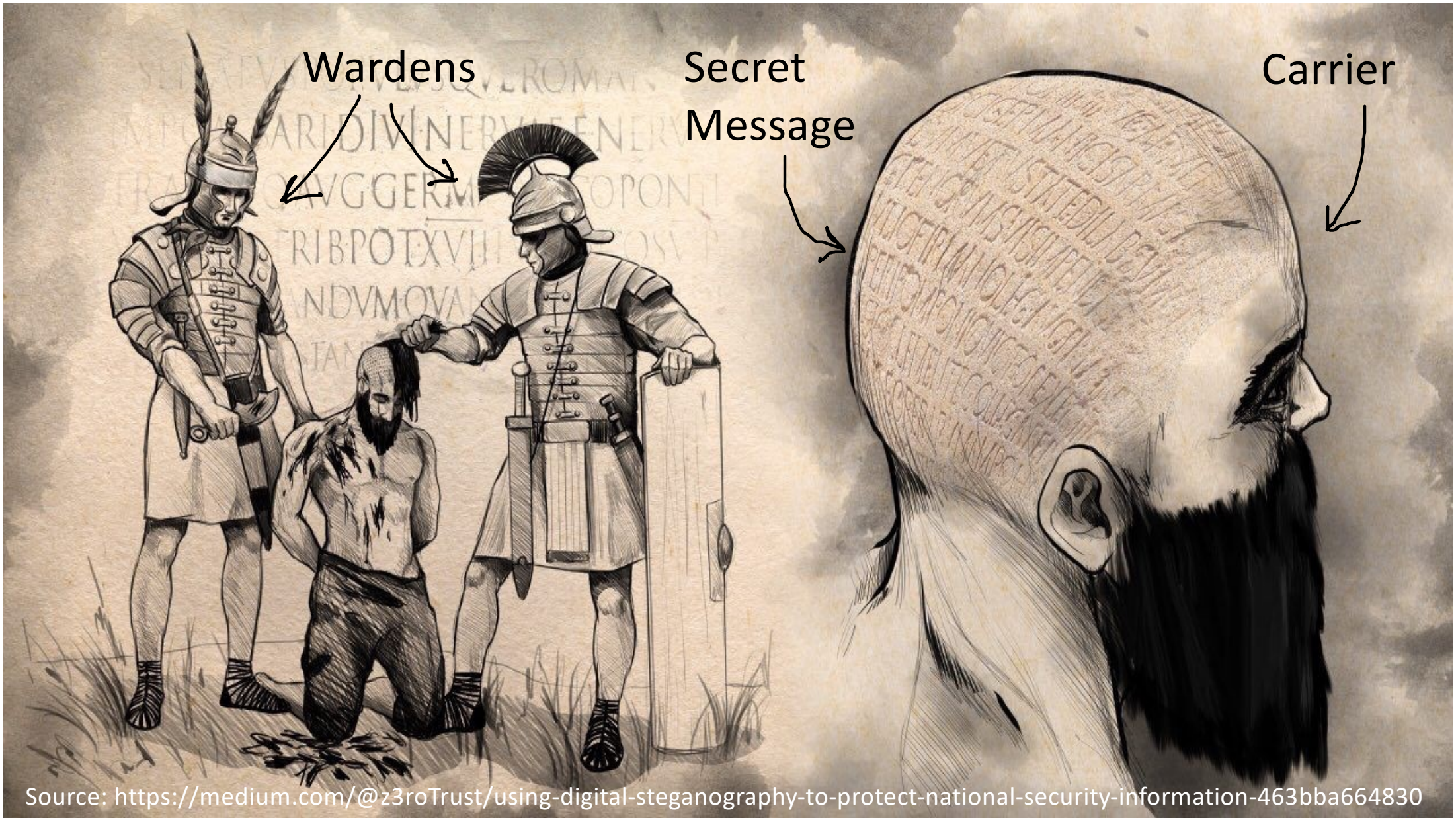
Steganography: roots

- The word steganography is the combination of:
  - *steganos* = covered, concealed;
  - *graphe* = writing.
- The first recorded use of the term:
  - in 1499 by Johannes Trithemius;
  - book “Steganographia”, i.e., an essay on cryptography and steganography.
- Mentioned in 440 BC by Herodotus in his Histories.
- **Cloak secret data into a suitable carrier.**

steganos (στεγᾰνός) + graphe (γραφή)

Steganography: principles

- To exchange secrets the involved parties must **agree on a pre-shared scheme**.
- The **most favourable carriers** for secret messages must have two features:
  - modifications of the carrier caused by the embedding of the secret data **should not be "visible"** to parties unaware of the steganographic procedure;
  - **they should be popular**: the used carrier should not be considered as an anomaly. The greater the carrier's popularity, the better its masking capacity.

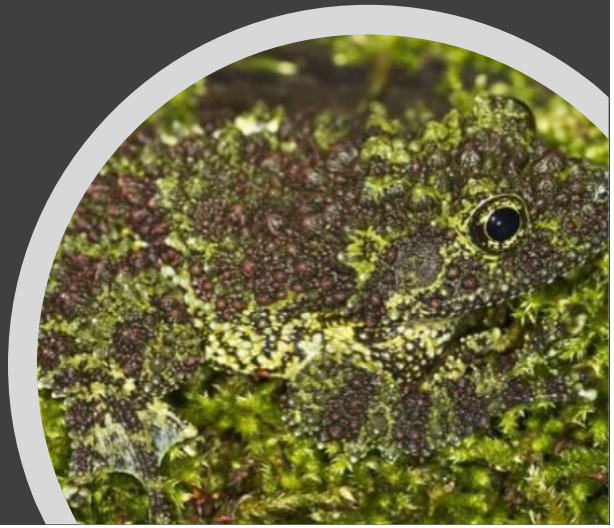


Source: https://medium.com/@z3roTrust/using-digital-steganography-to-protect-national-security-information-463bba664830

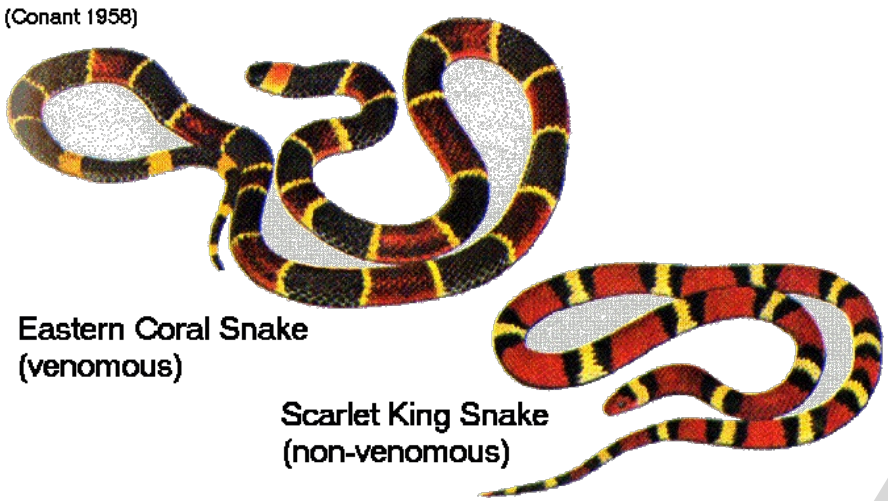
Information Hiding in Nature

- **Philippine tarsiers** (*Tarsius syrichta*): small nocturnal primates.
- They have a high-frequency auditory sensitivity limit of approximately **91 kHz** and are also able to vocalize with a dominant frequency of **70 kHz.**
- This is an example of **ultrasonic communication**.
- Philippine tarsiers implement a private **covert communication channel** that is undetectable by predators, preys, and competitors.

Information Hiding in Nature



- **Camouflage** exploits solutions utilizing features like the physical shape, texture, coloration, and illumination, to make animals hard to spot.
- As a result, the **information** about the exact location remains **ambiguous**.

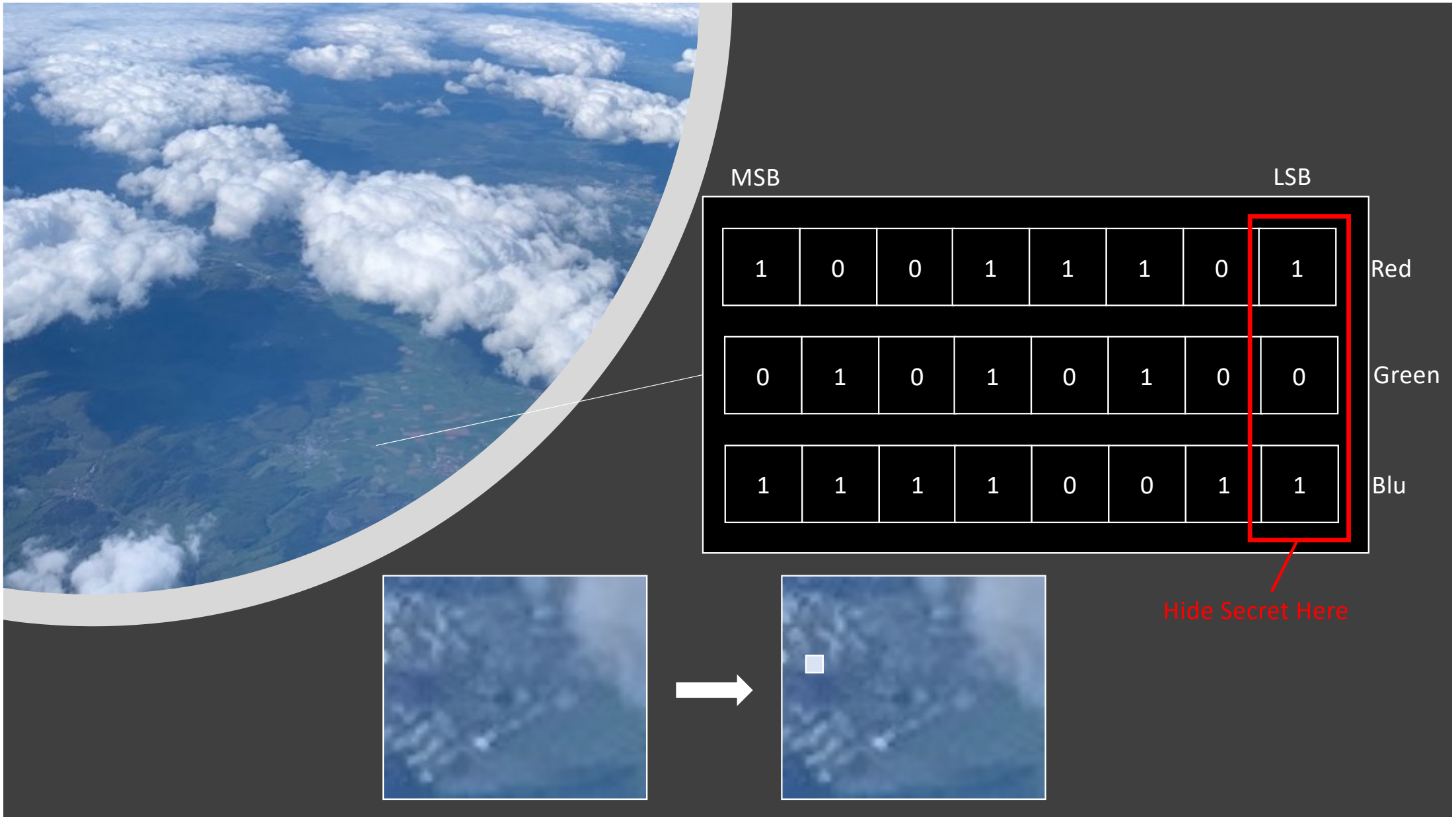


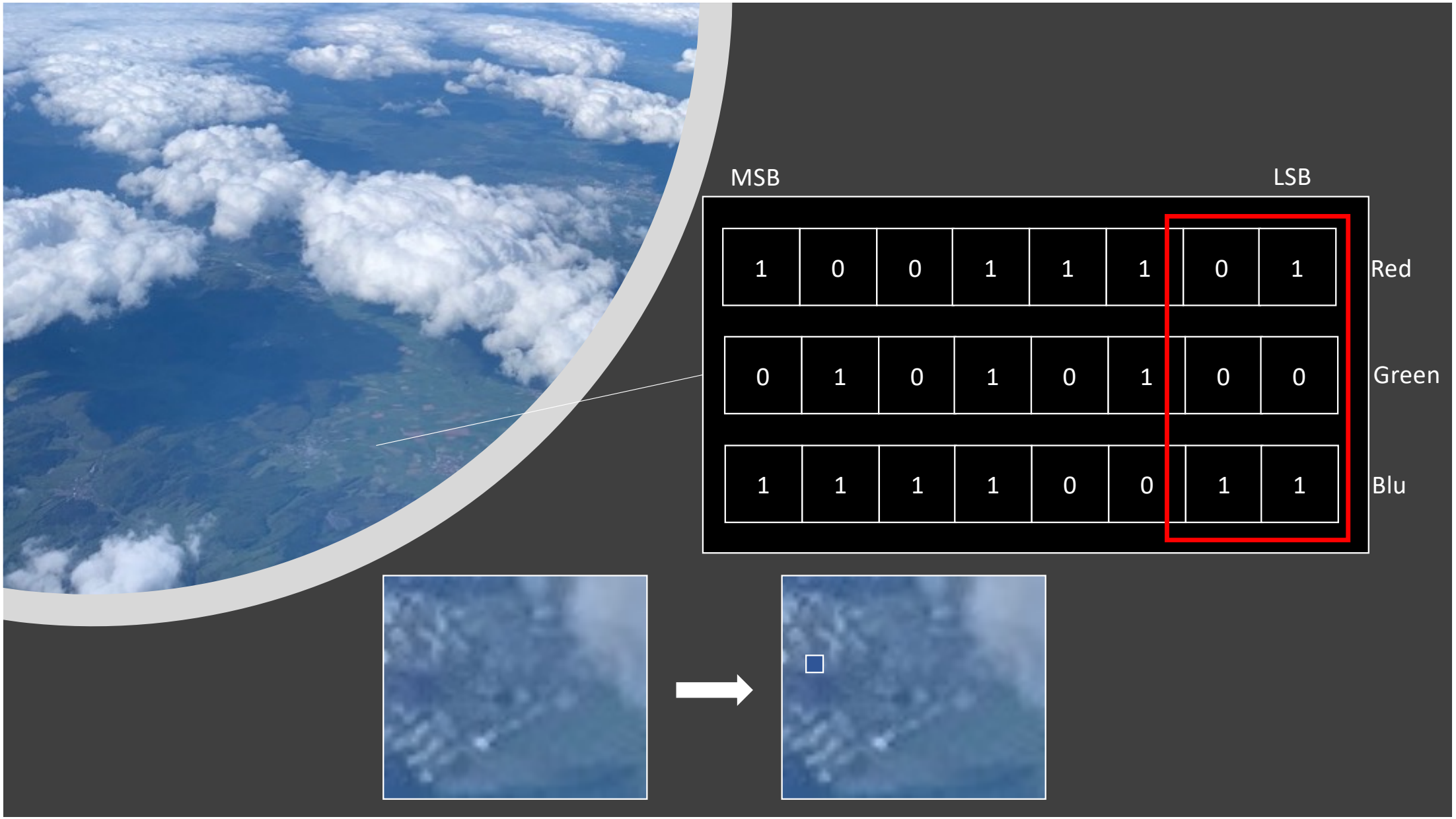
Information Hiding in Nature

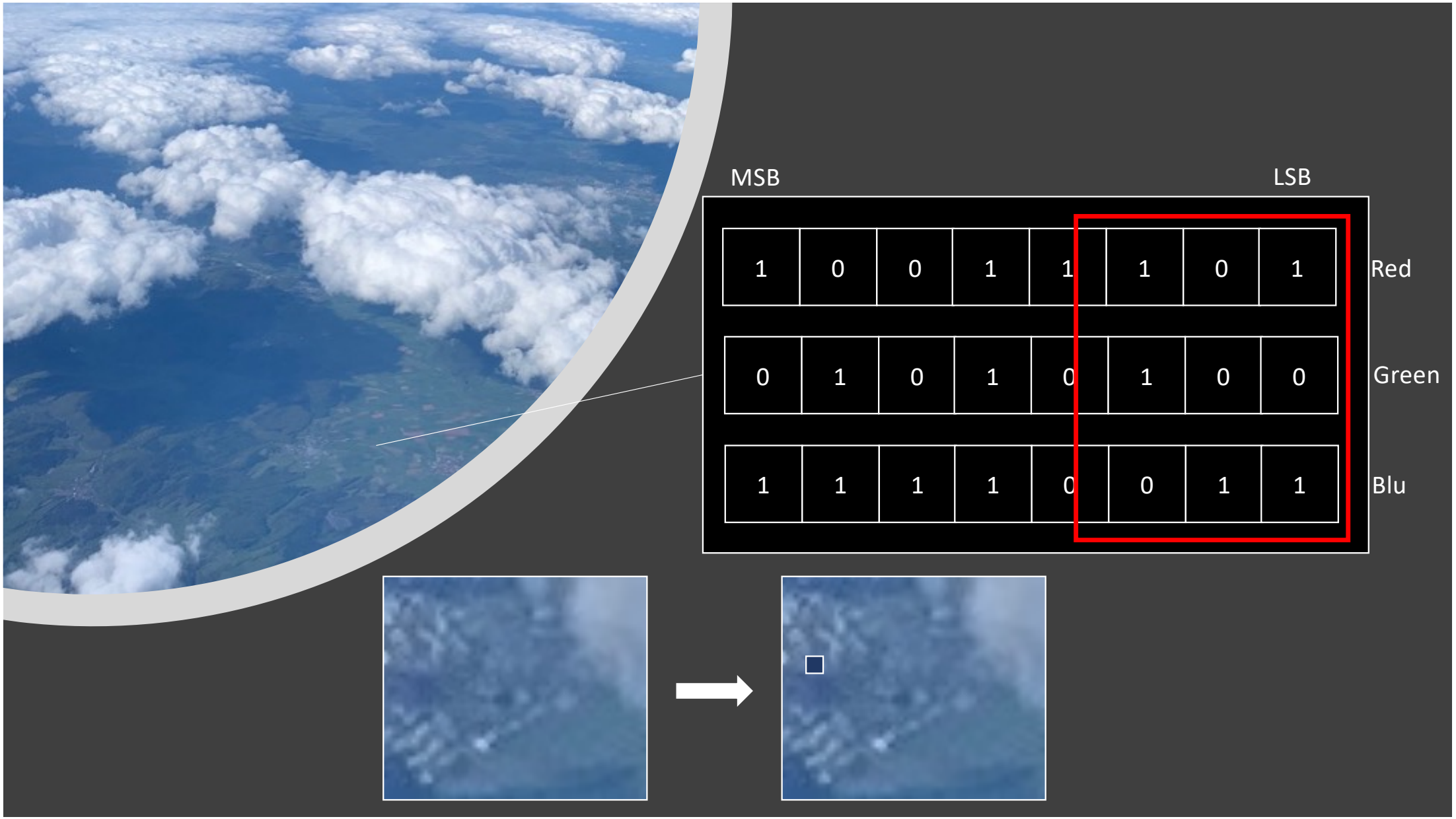
- **Mimicry** allows to obfuscate some attributes by adopting the characteristics of another living organism.
- As a result, the prey **hides** information about its own identity by impersonating something that it is not.

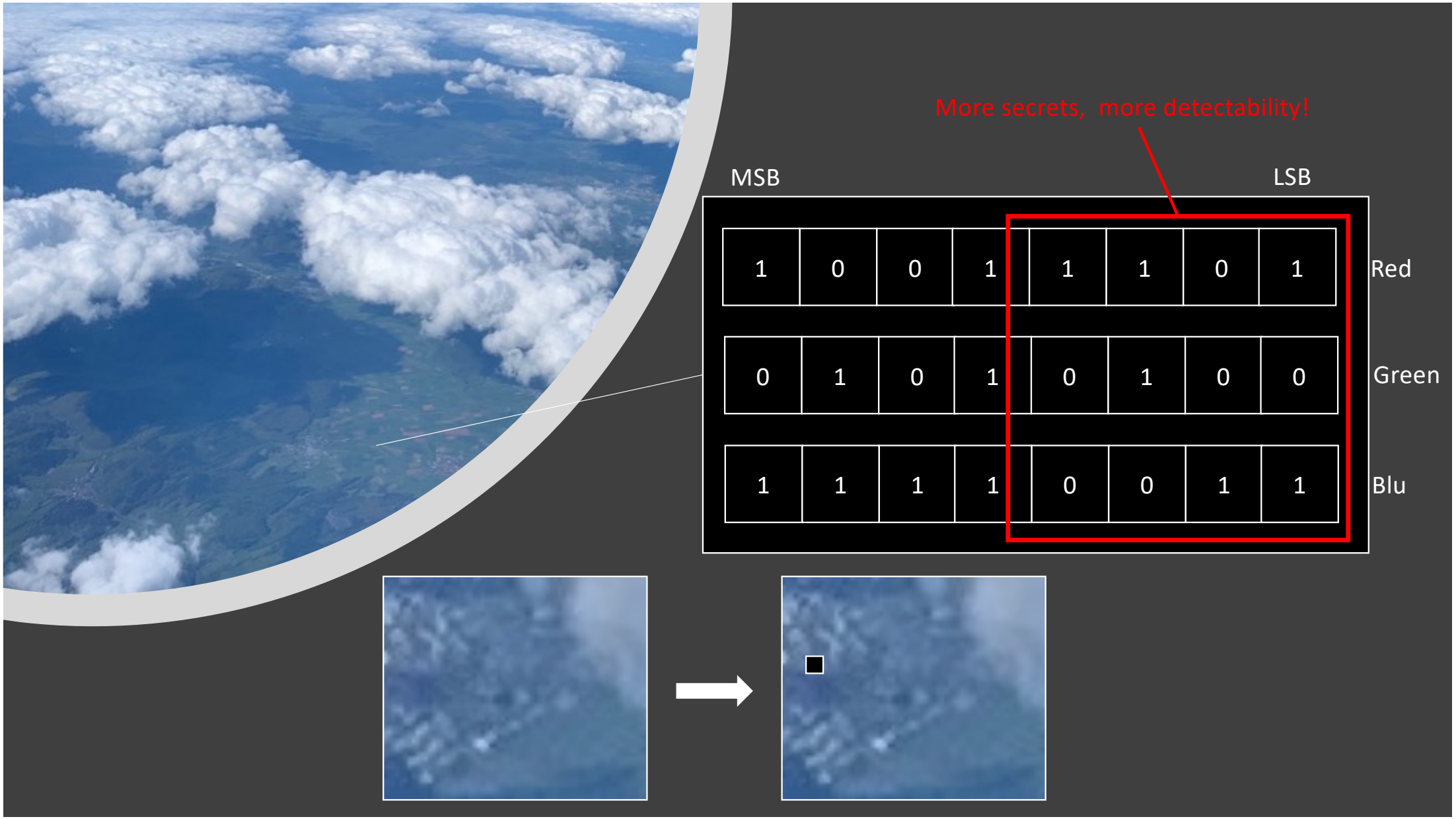
Information Hiding in Digital Media

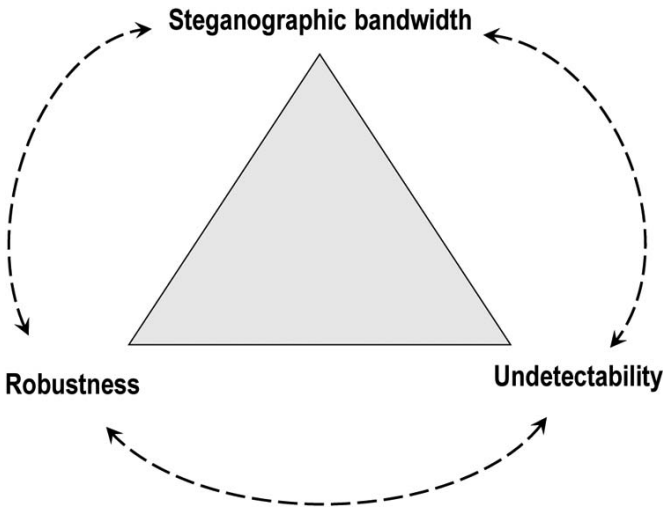
- Least Significant Bit (LSB) steganography is the simplest method for hiding data in digital media.


MSB
LSB
1 0 0 1 1 1 0 1
Red
0 1 0 1 0 1 0 0
Green
1 1 1 1 0 0 1 1
Blu
Hide Secret Here


MSB
LSB
1 0 0 1 1 1 0 1
Red
0 1 0 1 0 1 0 0
Green
1 1 1 1 0 0 1 1
Blu


MSB
LSB
1 0 0 1 1 1 0 1
Red
0 1 0 1 0 1 0 0
Green
1 1 1 1 0 0 1 1
Blu


More secrets, more detectability!
MSB
LSB
1 0 0 1 1 1 0 1
Red
0 1 0 1 0 1 0 0
Green
1 1 1 1 0 0 1 1
Blu



The “Magic Triangle”

- **Bandwidth**: the amount of secret data that can be sent per time unit when using a particular method.
- **Undetectability**: the inability to detect secret data within a certain carrier.
- **Robustness:** the amount of alteration a carrier containing the covert data can withstand before the secret message is destroyed.

W. Mazurczyk, L. Caviglione, "Steganography in Modern Smartphones and Mitigation Techniques", *IEEE Communications Surveys & Tutorials*, Vol. 17, No. 1, pp. 334-357, 2015

Why are we here?

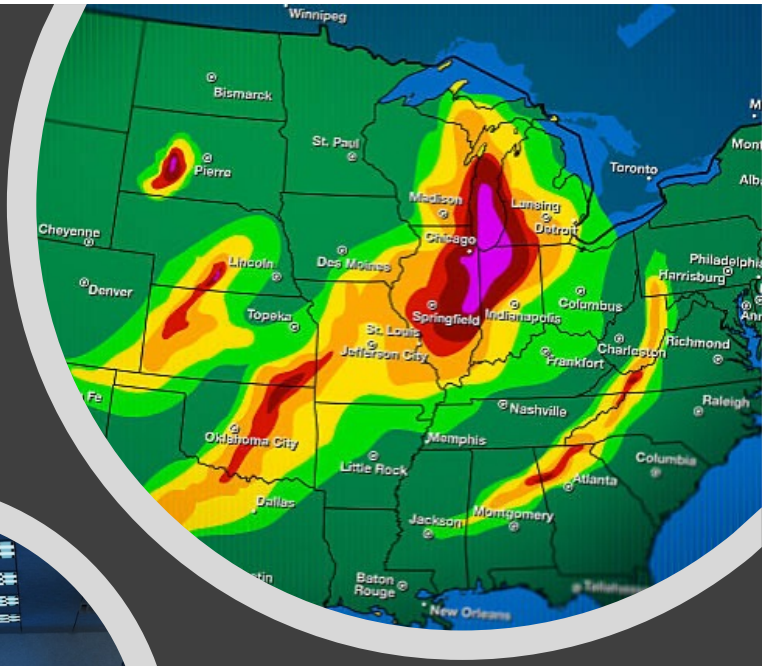
- The practice of hiding data has been used through the years for:
  - military and intelligence purposes;
  - tracking the diffusion of the knowledge;
  - industrial espionage;
  - covering the sources in investigative journalism;
  - preventing censorships and avoid regimes;
  - copyright management;
  - detecting alterations in digital contents;
  - information and network traffic tracing;
  - meta-datation;
  - malware and advanced persistent threats;
  - …

Why are we here?

- The practice of hiding data has been used through the years for:
  - military and intelligence purposes;
  - **tracking the diffusion of the knowledge;**
  - industrial espionage;
  - covering the sources in investigative journalism;
  - preventing censorships and avoid regimes;
  - **copyright management;**
  - **detecting alterations in digital contents**;
  - information and network traffic tracing;
  - meta-datation;
  - **malware and advanced persistent threats;**
  - …

Why are we here?

- Information Hiding is based on the following **facts**:
  - opportunity makes the thief;
  - needle in the haystack;
  - the more the burden, the more the cloaking capability;
  - social engineering and importance of applications.
- Then, the **security** of advanced, heterogenous and data-intensive applications needs a partial rethink, due to:
  - the diffusion of the “as-a-Service” paradigm;
  - industrial/economical competition;
  - artificial intelligence everywhere;
  - pervasiveness and volumes of data.
- **Increase the awareness on the topic!**



Part One
Hiding Data for Offending

Some Facts About Modern Malware

- Exponential growth of malicious software.
- Despite the effort of many security experts and researchers:
  - countermeasures are progressively showing limitations;
  - only a fraction of threats is detected;
  - malware increasingly operates **undisturbed** for **longer timeframes.**

Malware	Discovered	Present since...
Stuxnet	06.2010	2007
Duqu	04.2011	2008
Flame	05.2012	2007
The Mask	2013	2007
Regin	2014	2003

Some Facts About Modern Malware

- Exponential growth of malicious software.
- Despite the effort of many security experts and researchers:
  - countermeasures are progressively showing limitations;
  - only a fraction of threats is detected;
  - malware increasingly operates **undisturbed** for **longer timeframes.**
- How can malware developers avoid detection for long periods?

Giving an answer is **not** simple!

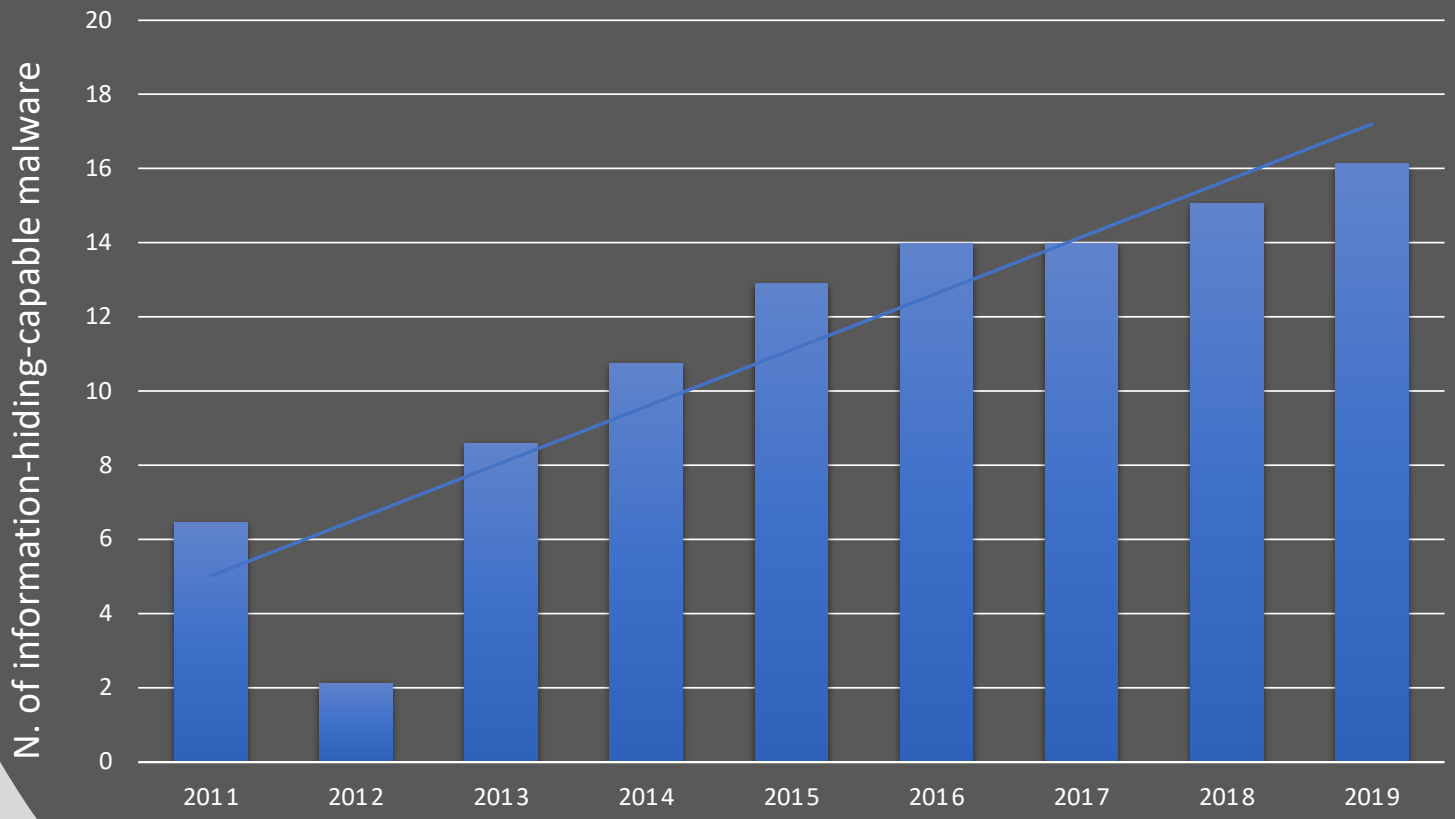
Some Facts About Modern Malware

- Some possible reasons are:
  - Modular design for customization (e.g., Regin, Flamer, Weevil);
  - Multistage loading (e.g., Regin, Stuxnet, Duqu);
  - Cybercrime-as-a-Service models and Remote Access Trojans (e.g., Gh0st Rat);
  - **Information Hiding** techniques and **steganography** (e.g., Platinum APT).

Main Attack Purposes

- Information Hiding techniques have been **increasingly observed** in malicious software, for instance to:
  - elude detection;
  - covertly spread an infection or orchestrate attacks;
  - exfiltrate sensitive data;
  - bypass sandboxing mechanisms;
  - implement covert channels;
  - …

A Constant Trend



Data collected by members of Criminal Use of Information Hiding initiative (CUING): cuing.org and cuing.eu

A Constant Trend

The impact of information-hiding-capable malware is heavily underestimated: security experts often do not correctly recognize and classify the used techniques

Data collected by members of Criminal Use of Information Hiding initiative (CUING): cuing.org and cuing.eu

The Root of the Trend

- Probably, Trojan.Downbot (circa 2006, Operation Shady RAT)
- The trojan created a back door and:
  - downloaded files appearing as real HTML pages or JPEG images;
  - hidden data contained commands for remote servers.

The Root of the Trend

- Probably, Trojan.Downbot (circa 2006, Operation Shady RAT)
- The trojan created a back door and:
  - downloaded files appearing as real HTML pages or JPEG images;
  - hidden data contained commands for remote servers.
- Three attack stages:
  - Stage 1: phishing!

The Root of the Trend

- Probably, Trojan.Downbot (circa 2006, Operation Shady RAT)
- The trojan created a back door and:
  - downloaded files appearing as real HTML pages or JPEG images;
  - hidden data contained commands for remote servers.
- Three attack stages:
  - Stage 1: phishing!
  - Stage 2: the trojan attempts to retrieve data from remote sources;

www.comto[SANITIZED].com/wak/mansher0.gif
www.kay[SANITIZED].net/images/btn_topsec.jpg
www.swim[SANITIZED].net/images/sleepyboo.jpg
www.comto[SANITIZED].com/Tech/Lesson15.htm

The Root of the Trend

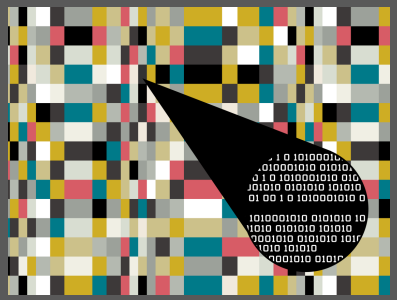
- Probably, Trojan.Downbot (circa 2006, Operation Shady RAT)
- The trojan created a back door and:
  - downloaded files appearing as real HTML pages or JPEG images;
  - hidden data contained commands for remote servers.
- Three attack stages:
  - Stage 1: phishing!
  - Stage 2: the trojan attempts to retrieve data from remote sources;

```
<!-- {685DEC108DA731F1} -->
<!-- {685DEC108DA73CF1} -->
<!-- {eqNBb-Ou07WM} -->
<!-- {eqNBb-Ou07iM} -->
<!-- {eqNBb-Ou01OMOO++} -->
<!-- {eqNBb-Ou11O+} -->
<!-- {eqNBb-Ou2Ra+} -->
<!-- {uGu~iWA1,Q(iNyn'/} -->
<!-- {ujQ~iY,UnQ[!,hboZWg} -->
<!-- {ujQ~iY,UnQ[!,hmoZWg} -->
<!-- {ujQ~iY,UnQ[!,hvoZWg} -->
```

Commands hidden in HTML comments
(encrypted + base64 encoded)

The Root of the Trend

- Probably, Trojan.Downbot (circa 2006, Operation Shady RAT)
- The trojan created a back door and:
  - downloaded files appearing as real HTML pages or JPEG images;
  - hidden data contained commands for remote servers.
- Three attack stages:
  - Stage 1: phishing!
  - Stage 2: the trojan attempts to retrieve data from remote sources;



Commands hidden in images via steganographic techniques

The Root of the Trend

- Probably, Trojan.Downbot (circa 2006, Operation Shady RAT)
- The trojan created a back door and:
  - downloaded files appearing as real HTML pages or JPEG images;
  - hidden data contained commands for remote servers.
- Three attack stages:
  - Stage 1: phishing!
  - Stage 2: the trojan attempts to retrieve data from remote sources;
  - Stage 3: the trojan connects to a host and sets up a remote shell waiting for commands.

Stegomalware

- Many researchers are starting to identify this class of threats as:
  - **Stegomalware**: steganographic malware;
  - "borrowed" from works on mobile security and covert social botnets.
- A possible (common) definition:
  - **Stegomalware is a malware using some form of steganography to remain undetected.**
- Personally, I found it:
  - a bit ambiguous (Information Hiding vs steganography);
  - it is not only about detection (e.g., "colluding applications") so it narrows the scope too much.

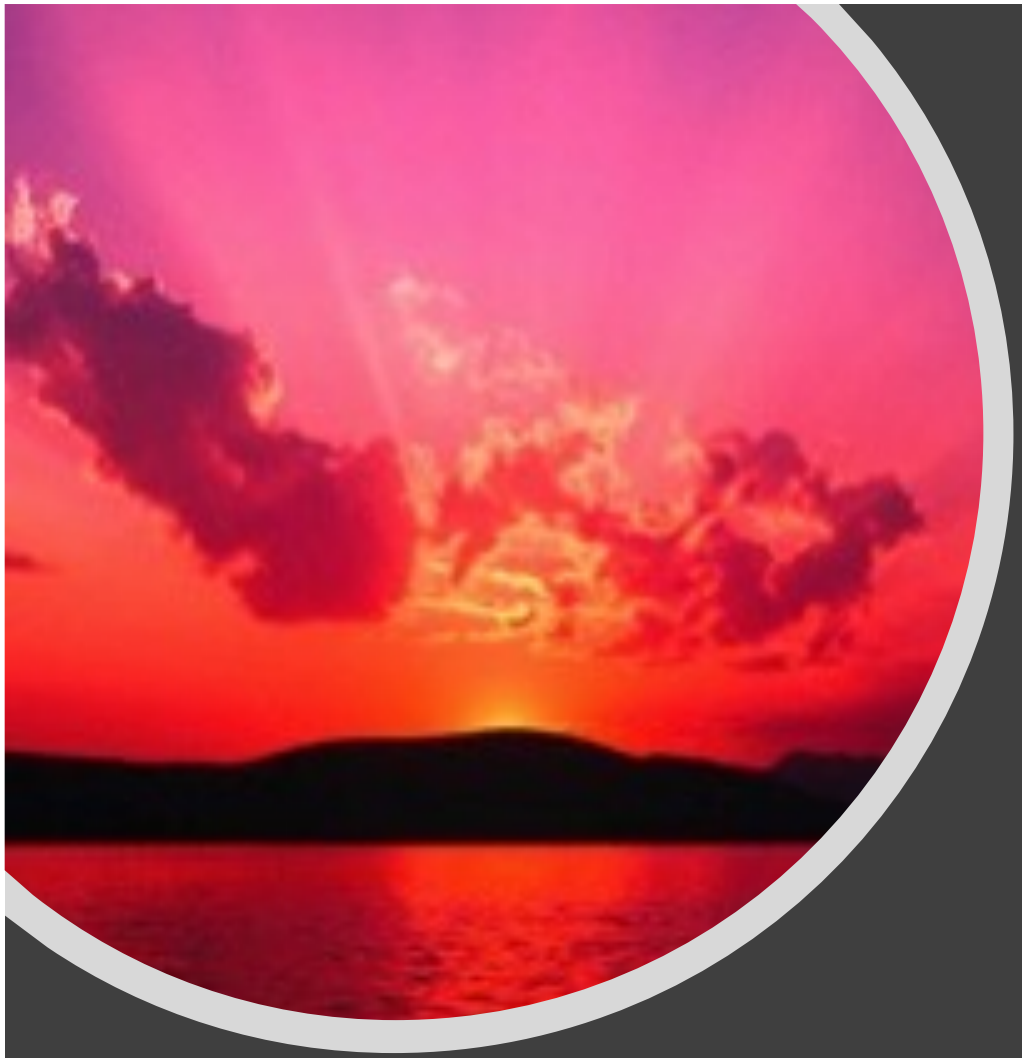
G. Suarez-Tangil, J. Tapiador, P. Peris-Lopez, "Stegomalware: Playing Hide and Seek with Malicious Components in Smartphone Apps", 10th International Conference on Information Security and Cryptology, pp. 496–515, 2014.

S. Nagaraja, A. Houmansadr, P. Piyawongwisal, V. Singh, P. Agarwal, B. Nikita, "Stegobot: A Covert Social Network Botnet", Information Hiding - 13th International Conference, pp. 299 – 313, 2011.

Stegomalware

- Attacks observed in the wild tend to hide data in a limited number of places.
- Three main groups:
  - **Group 1**: malware hiding information by modulating the status of shared hardware/software resources (8%);
  - **Group 2**: malware injecting secret data into network traffic (32%);
  - **Group 3**: malware embedding secret data by modifying a digital file structure or by using digital media steganography (60%).

W. Mazurczyk, L. Caviglione, “Information Hiding as a Challenge for Malware Detection”, IEEE Security & Privacy, Vol. 13, No. 2, pp. 89-93, Mar.-Apr. 2015.

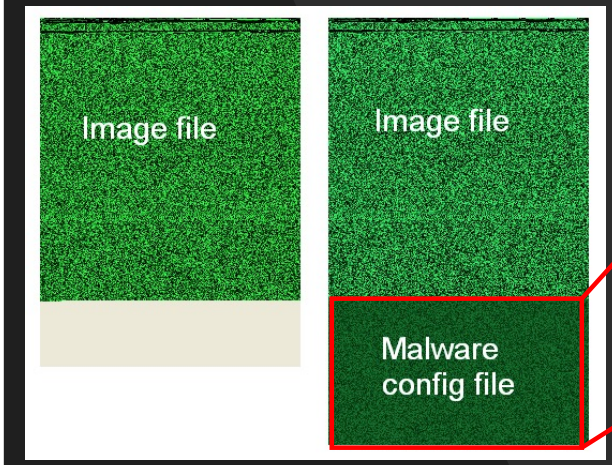


Example: ZeusVM

- Discovered in 2014, it is an evolution of the Zeus/Zbot malware.
- A variant has been also used in the Hammertoss APT isolated in 2015.
- Attack phases:
  - the malware downloads an innocent JPG from a C&C server;
  - the image perfectly works but a configuration file is appended;

Source: https://blog.malwarebytes.com/threat-analysis/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/

Example: ZeusVM

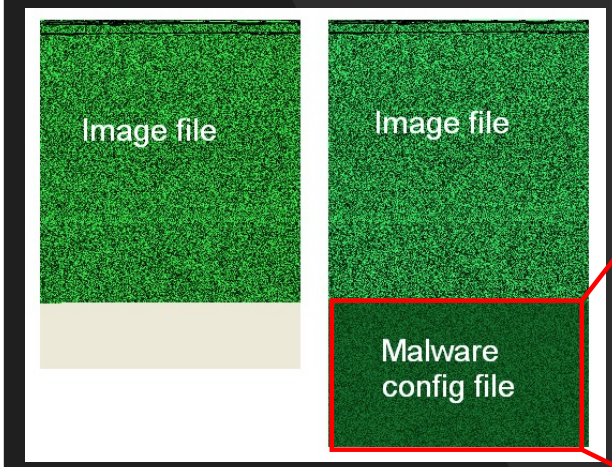



```
8A F4 AE 1D D8 FA 43 FF FE 3F 10 00 00 F8 B7 4F 9B 2C 90 00  ......C..?.....O.,..
00 75 5A 71 42 48 42 2F 6F 57 43 71 73 30 49 45 44 68 4D 54  .uZqBHB/oWCqs0IEDhMT
30 35 32 66 59 52 4C 37 72 58 78 53 42 71 45 49 65 71 76 6F  052fYRL7rXxSBqEIeqvo
6B 64 31 6B 30 48 41 75 61 56 67 71 66 71 47 2B 6E 2B 54 47  kd1k0HAuaVgqfqG+n+TG
61 56 46 61 76 48 6F 36 35 69 55 4A 34 73 6F 4C 34 6C 58 7A  aVFavHo65iUJ4soL4lXz
36 54 63 78 4E 72 62 64 6A 55 59 39 61 73 49 2B 6A 56 52 49  6TcxNrbdjUY9asI+jVRI
58 62 33 2F 73 48 34 4A 4C 6F 51 74 67 69 63 30 38 34 74 79  Xb3/sH4JLoQtgic084ty
69 46 38 35 57 6B 30 6A 4C 41 72 41 66 46 70 6A 52 67 39 79  iF85Wk0jLArAfFpjRg9y
```

Data is encoded in base64 and encrypted with a mix of RC4 and XOR

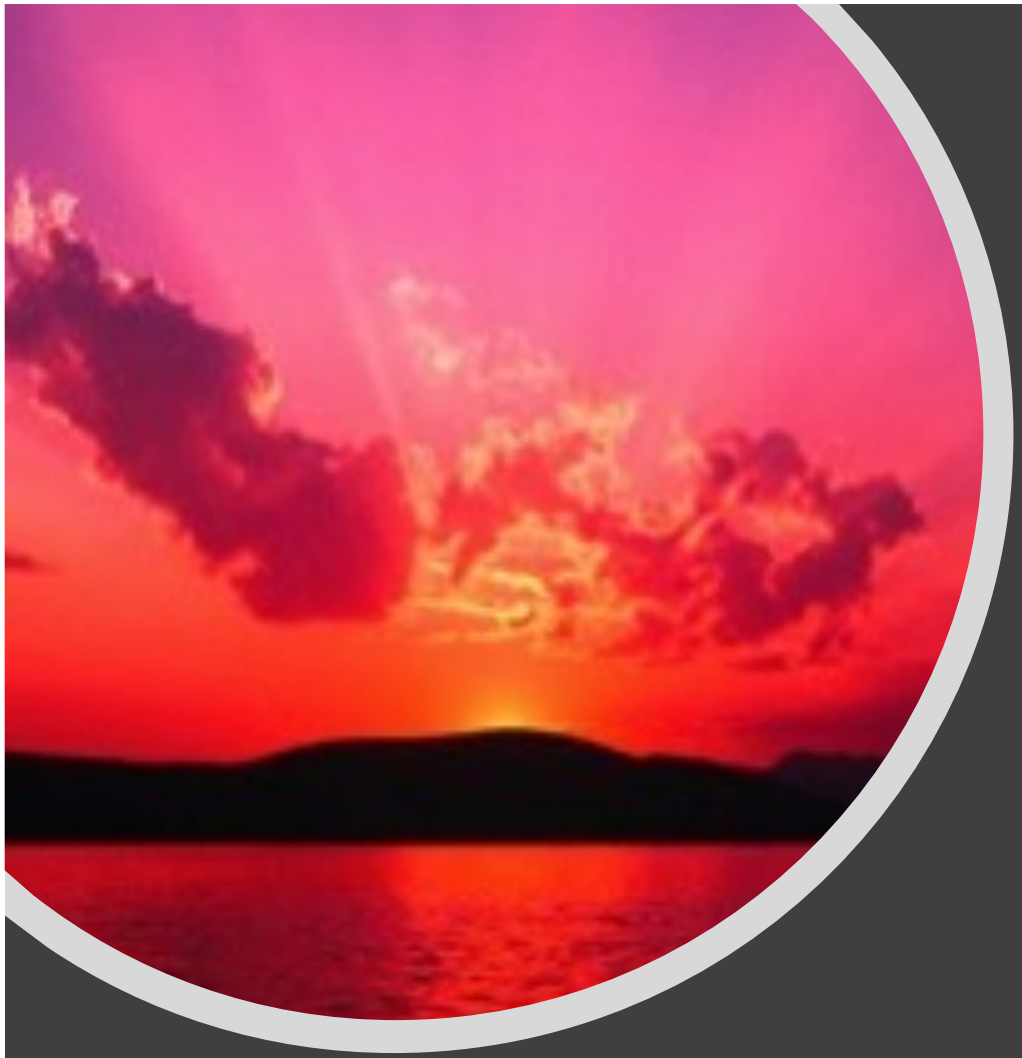
Source: https://blog.malwarebytes.com/threat-analysis/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/

Example: ZeusVM



ueberSicht/anzeige*dMhttps://kunde.comdirect.de/itx/kontouebersicht/anzeige*d=https://kunde.comdirect.de/itx/ueberweisung*d=https://kunde.comdirect.de/itx/ueberweisung*d@https://kunde.comdirect.de/ip/pt/login*dPhttps://ssl2.haspa.de/OnlineFiliale/banking/authenticate/login*dFhttps://ssl2.haspa.de/OnlineFiliale/banking/services*d;https://www.moneybookers.com/app/login.pl*d@*www.online.fnb.co.za/banking/main.isp*dR*netbank.nedsecure.co.za/Browser/Brands/Nedbank/Logon/Logon.aspx*dP*netbank.nedsecure.co.za/Browser/Brands/Nedbank/Logon/Logon.bank*d8*encrypt.standardbank.co.za/ibsa/signonmenu.do*dJ*encrypt.standardbank.co.za/ibsa/accounts/getbalances.do*d*adib.ae*d*hdfcbank.com*d
*onlinesbi.com*d&*bancocredicoop.coop*d&*santanderrio.com.ar*d
*raiffeisen.at*d*sparkasse.at*d!*bankaustria.at*d*bawagpsc.com*d"*bradesco.com.br*d,*bradesconetempresa.com.br*d*bci.cl*d
*bancochile.cl*d!*bancoestado.cl*d*santander.cl*d*bcinova.cl*d#*bancosantiago.cl*d*db.com*d*ing-diba.de*d*bv-bank.de*d*sparda.de*d"*bancopopular.es*d$*gruposantander.es*d*lacaixa.es*d*bbva*d
*bankinter.com*d*caja3.es*d*cajamar.es*d&*novagaliciabanco.es*d"*bancogallego.es*d*bankia.es*d*unicaja.es*d*ingdirect.es*d*ruralvia.com*d*liberbank.es*d'*adeslassegurcaixa.es*d!*bourso rama.com*d$*credit-du-nord.fr*d#*lloydsbank.co.uk*d!*barclays.co.uk*d!*isideonline.it*d*tecmarket.it*d
*bpergroup.net*d*cedacri.it*d$*businesswaybnl.it*d*bnl.it*d*mps.it*d%*intesasanpaolo.com*d*cgebo.it*d*quercia.com*d*credem.it*d*nbk.com.kw*d
*kfhonline.com*d*bancomer.com*d*rabobank*d*ing.nl*d#*banknetpower.net*d$*almubasher.com.sa*d"*bankalbilad.com*d'*cardinalcommerce.com*d#*alahlionline.com*d*samba.com*d'*geojitbnpparibas.com*d!*fednetbank.com*d*swedbank.se*d!*wellsfargo.com*d*regions.com*d*tdbank.com*d*fnb.co.za*d*absa.co.za*d"*nedsecure.co.za*d)*ruralvia.com/isum/Main*d*targobank.de*dF*commerzbanking.de/P-Portal*/XML/IFILPortal/pgf.html*dF*banking.sparda.de/wps/myportal/spardamodern-banking*dF*banking.sparda.de/wps/myportal/spardamodern-banking*d*lacaixa.es**ND&Q'

Source: https://blog.malwarebytes.com/threat-analysis/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/



Example: ZeusVM

- Discovered in 2014, it is an evolution of the Zeus/Zbot malware.
- A variant has been also used in the Hammertoss APT isolated in 2015.
- Attack phases:
  - the malware downloads an innocent JPG from a C&C server;
  - the image perfectly works but a configuration file is appended;
  - trojan activates when traffic towards financial institutions provided in the configuration file is sensed;
  - it steals user credentials by acting in a MitM fashion.

Source: https://blog.malwarebytes.com/threat-analysis/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/

Example: Invoke-PSImage

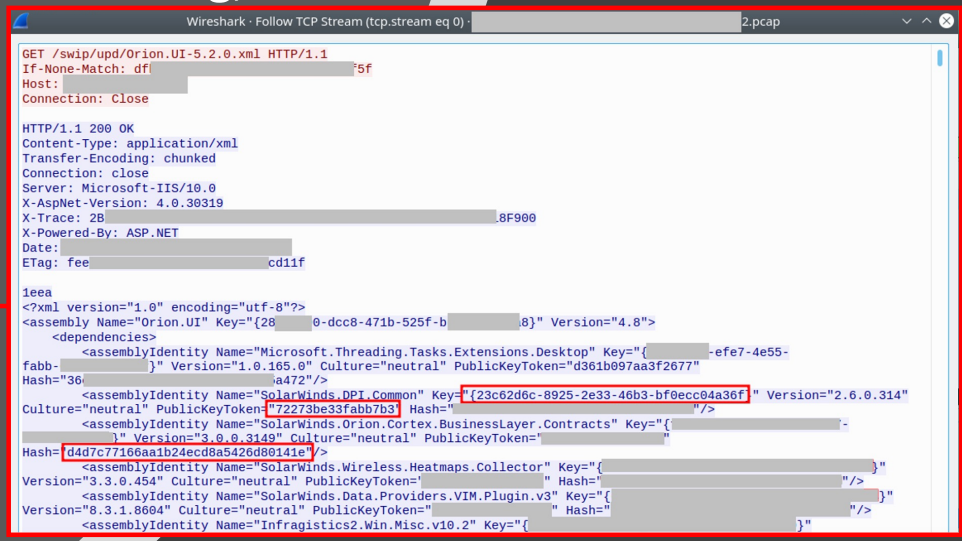
- Invoke-PSImage is a tool for encoding a PowerShell Script in pixels of a PNG image.
- It uses LSB steganography.
- Invoke-PSImage has been released in Dec. 2017 and it has been used for a malware campaign just 1 week later.
- Phases observed in the Ursnif/INPS campaign:
  - infected Excel is used to launch a malicious VB macro;
  - the macro downloads an image containing a PowerShell script;
  - the script is extracted and launched to retrieve the Ursnif loader.

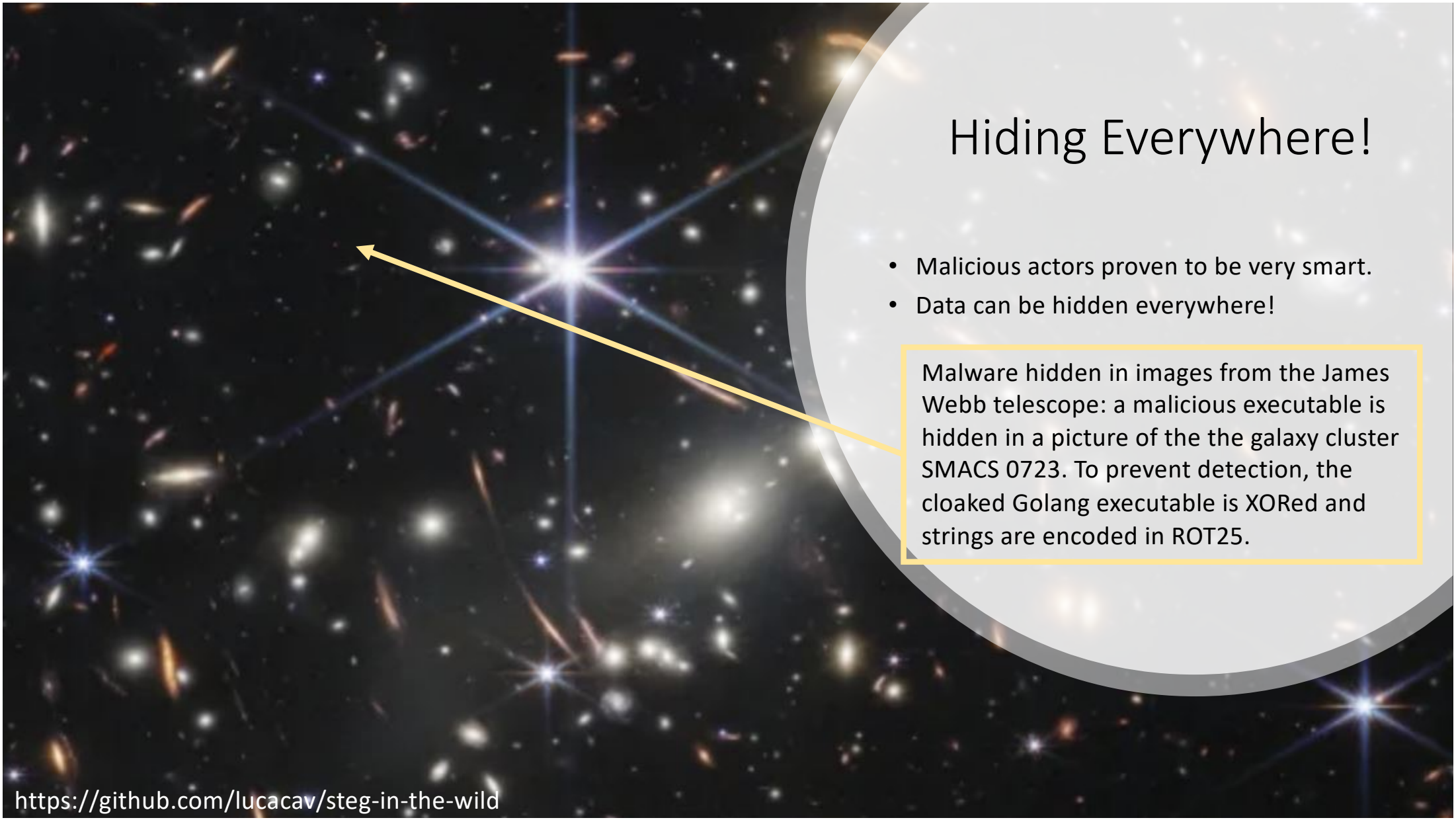
Invoke-PSImage: https://github.com/peewpw/Invoke-PSImage

Example: Sunburst

- Sunburst is a trojanized version of the Orion plugin (Solarwind).
- It targets HTTP traffic.
- Attack Phases:
  - various checks to understand if an analysis tool is running;
  - … (including, opening a backdoor);
  - creates a hidden C&C channel in HTTP.

Sunburst uses HTTP GET or POST requests. The server hides data within HTTP response bodies mimicking benign XML/.NET files. Hidden data is spread across many IDs and strings and extracted via the *\{[0-9a-f-]{36}\}"|"[0-9a-f]{32}"|"[0-9a-f]{16}* regexep.





Hiding Everywhere!

- Malicious actors proven to be very smart.
- Data can be hidden everywhere!

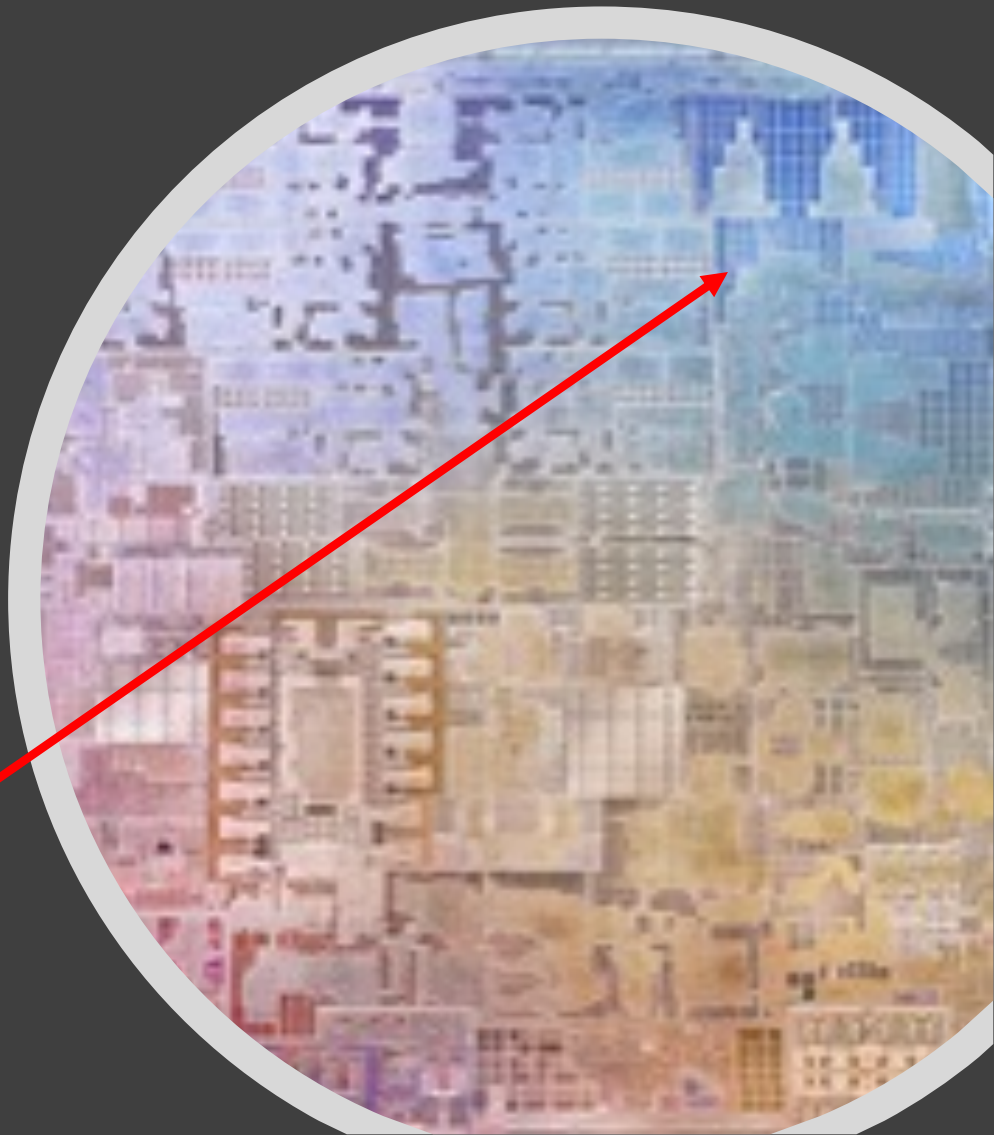
Malware hidden in images from the James Webb telescope: a malicious executable is hidden in a picture of the the galaxy cluster SMACS 0723. To prevent detection, the cloaked Golang executable is XORed and strings are encoded in ROT25.

https://github.com/lucacav/steg-in-the-wild

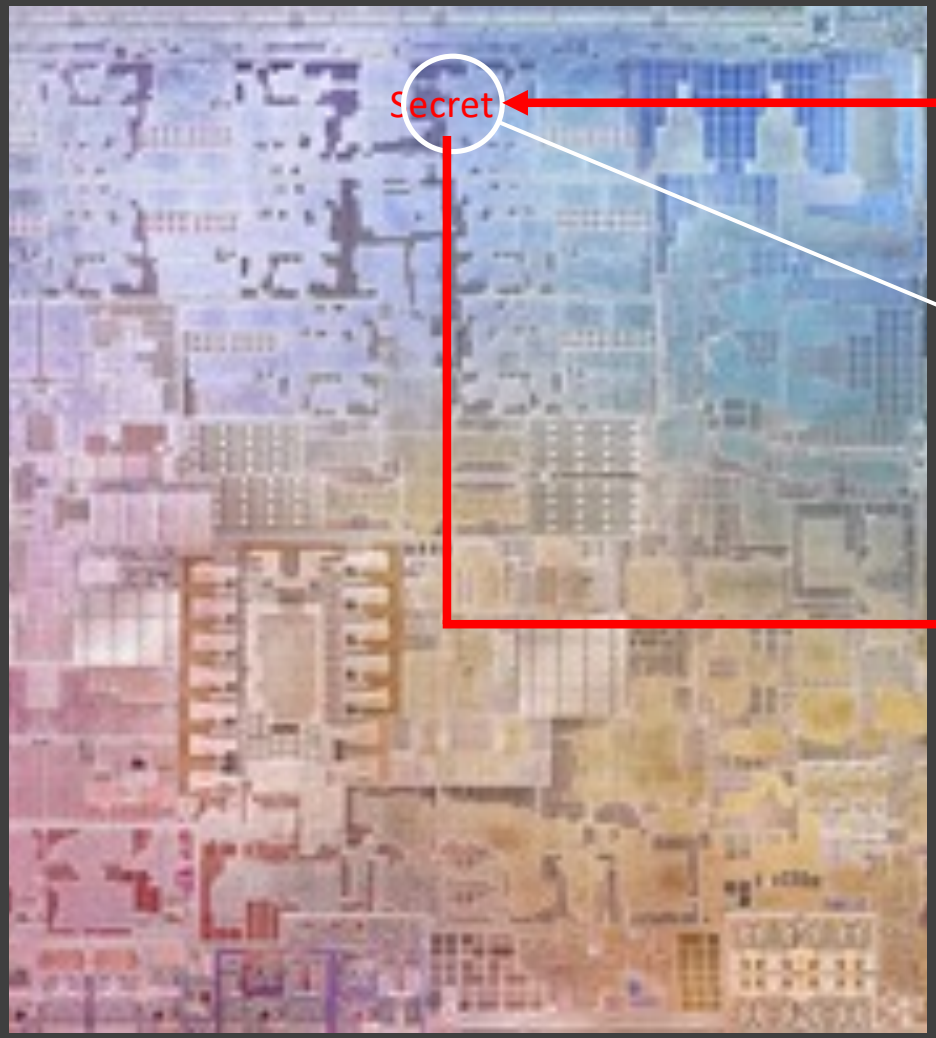
Hiding Everywhere!

M1ssing Register Access Controls Leak EL0 State
(CVE-2021-30747)
https://m1racles.com

Probably more for privacy leaking and moderately dangerous, but it is a covert-channel-based exploit.



EL0 (Exception Level) User Applications



1

ARM System Register: its original purpose is unknown, but probably not to be made accessible to EL0 intentionally.

2

Part Two
Hiding Data for Defending

Why Watermarking?

- Watermarking is a popular application of data hiding.
- A **watermark** can be used for:
  - Copyright protection;
  - Fingerprinting and tracking;
  - Integrity;
  - Metadata-tion.
- It can be applied to a variety of digital artifacts, e.g.:
  - Digital media (audio and video);
  - Pictures;
  - Maps/Medical data;
  - 3D meshes;
  - Network traffic;
  - …

Digital

Digital/Analog

Analog/Digital

Digital

Digital/Analog

Analog/Digital

Why Watermarking?

- The main idea is to hide data in contents to:
  - Track their use (diffusion);
  - Recognize tampering and manipulations;
  - Enforce copyright;
  - …

Digital

Digital/Analog

Analog/Digital

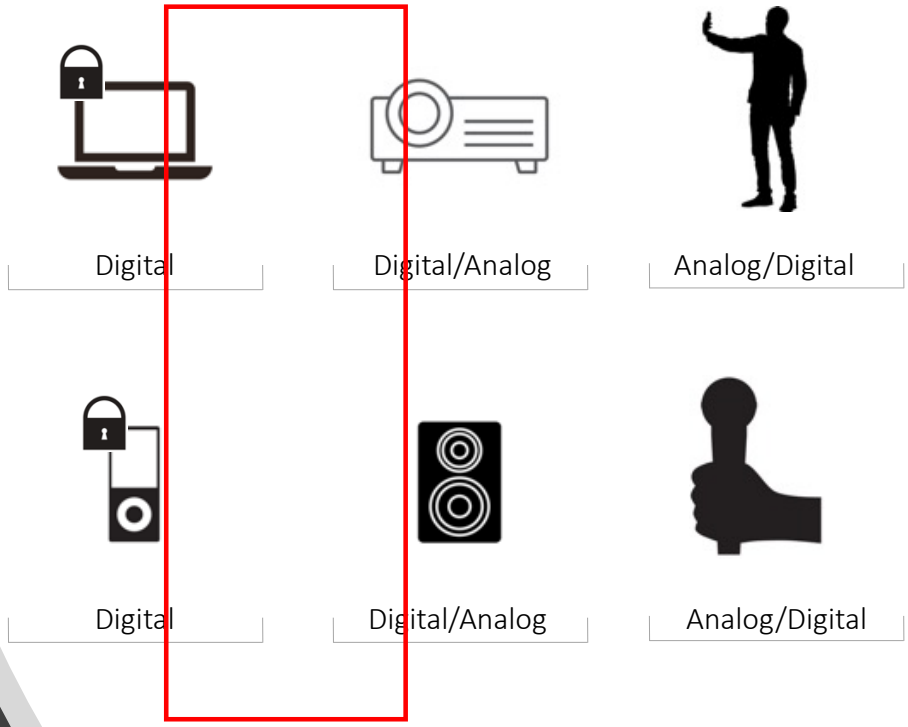
Digital

Digital/Analog

Analog/Digital

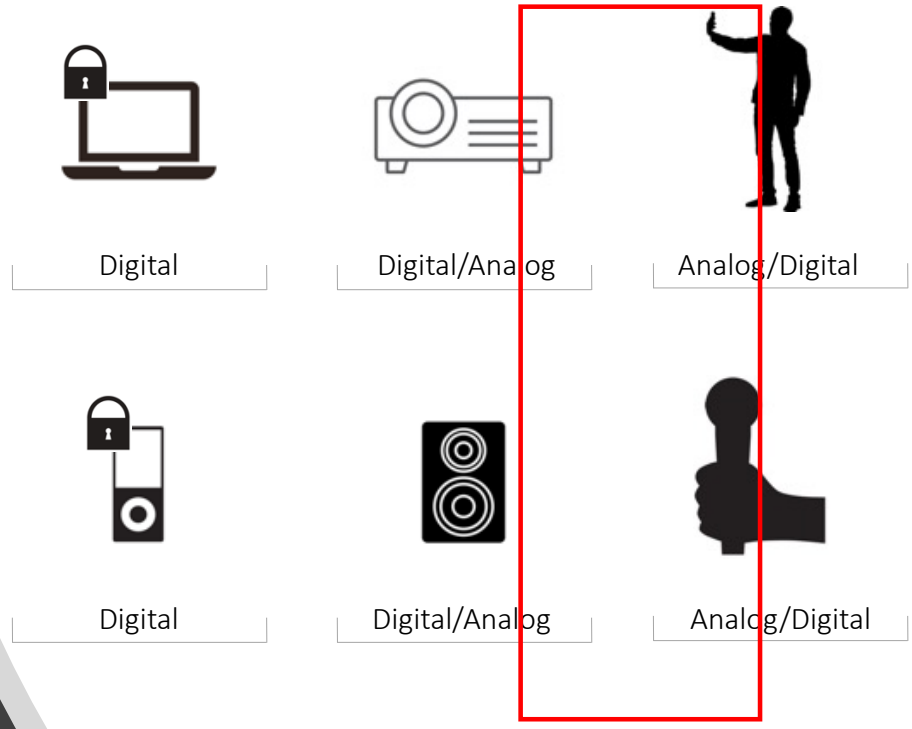
Why Watermarking?

- The main idea is to hide data in contents to:
  - Track their use (diffusion);
  - Recognize tampering and manipulations;
  - Enforce copyright;
  - …
- Main applications:
  - Digital Right Management (DRM) in media and digital contents;



Why Watermarking?

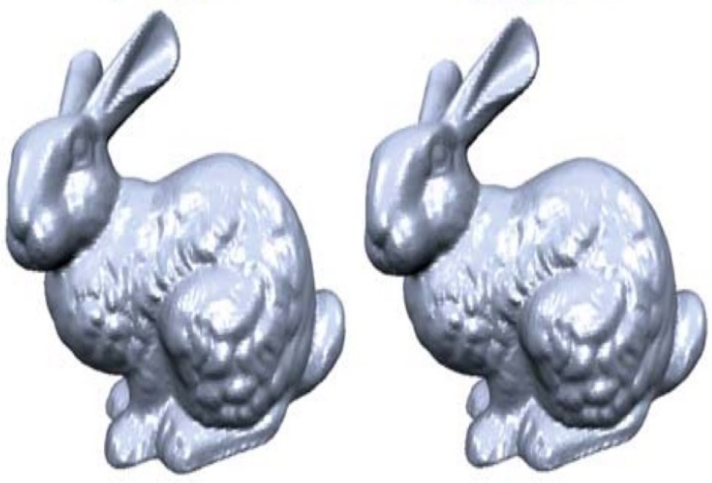
- The main idea is to hide data in contents to:
  - Track their use (diffusion);
  - Recognize tampering and manipulations;
  - Enforce copyright;
  - …
- Main applications:
  - Digital Right Management (DRM) in media and digital contents;
  - Elimination of the “Analog Hole”.



Example

“Screener” – Copyright and Tracking

Example



3D Mesh – Copyright and 3D printing management

Source: J. Wu, L. Kobbelt, “Efficient spectral watermarking of large meshes with orthogonal basis functions”, Visual Computing.

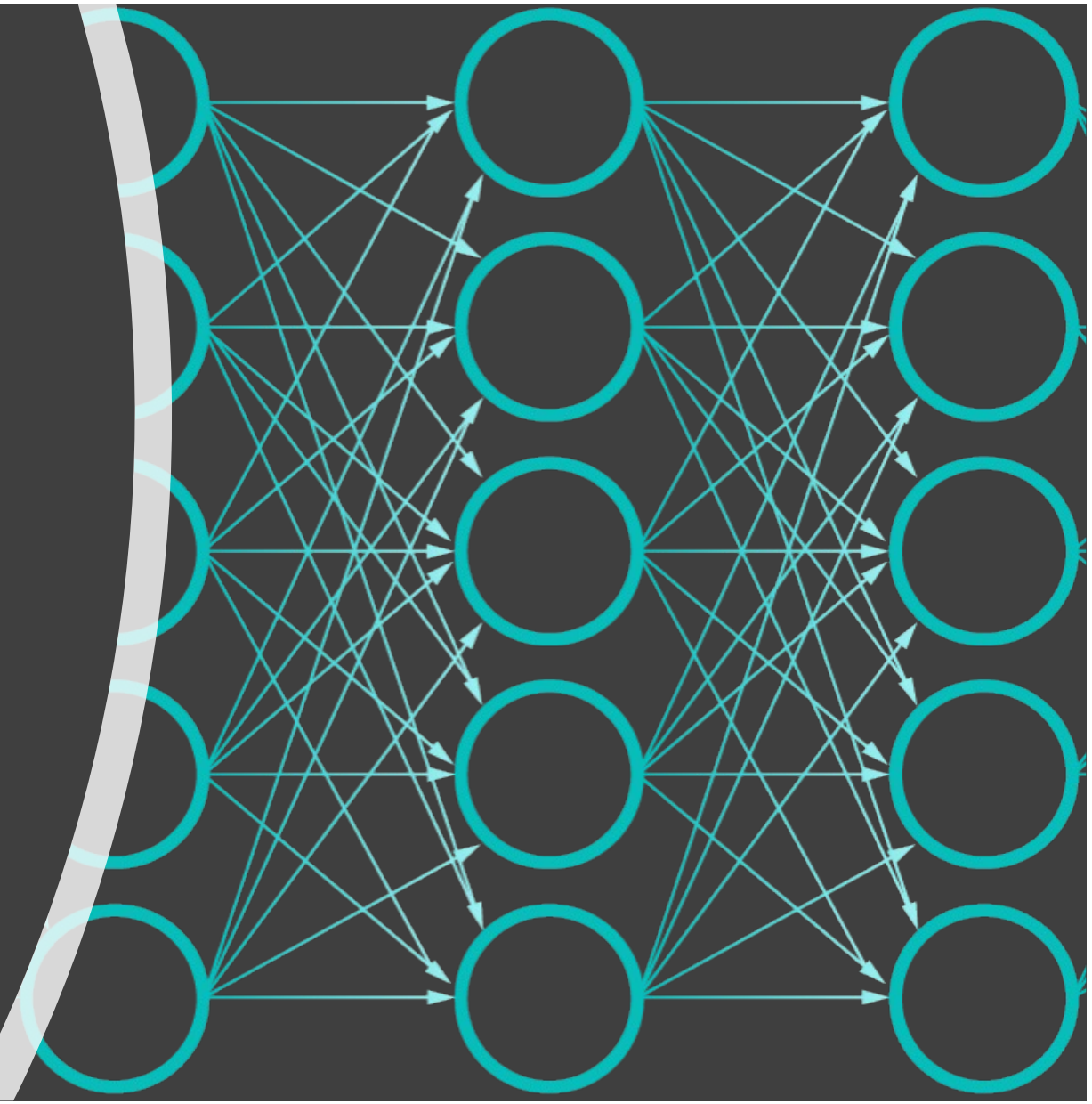
Types of watermarks

- Alas, there is **not** a **comprehensive** watermarking scheme.
- In general, there are **two** types of watermarking techniques:
  - **robust**: detectable after a wide range of attacks, it is mainly used for copyright and tracking;
  - **fragile**: typically used for authentication and localization of modifications made to the original digital media.
- Other possible types are:
  - **perceptible:** detectable by human senses and typically used to display copyright notices and to identify public documents;
  - **imperceptible:** not visible by human senses;
  - **non-invertible**: preventing the possibility of removing the watermark, recovering the original document, and applying new data.

Attack Example: Cropping

AI Watermarking

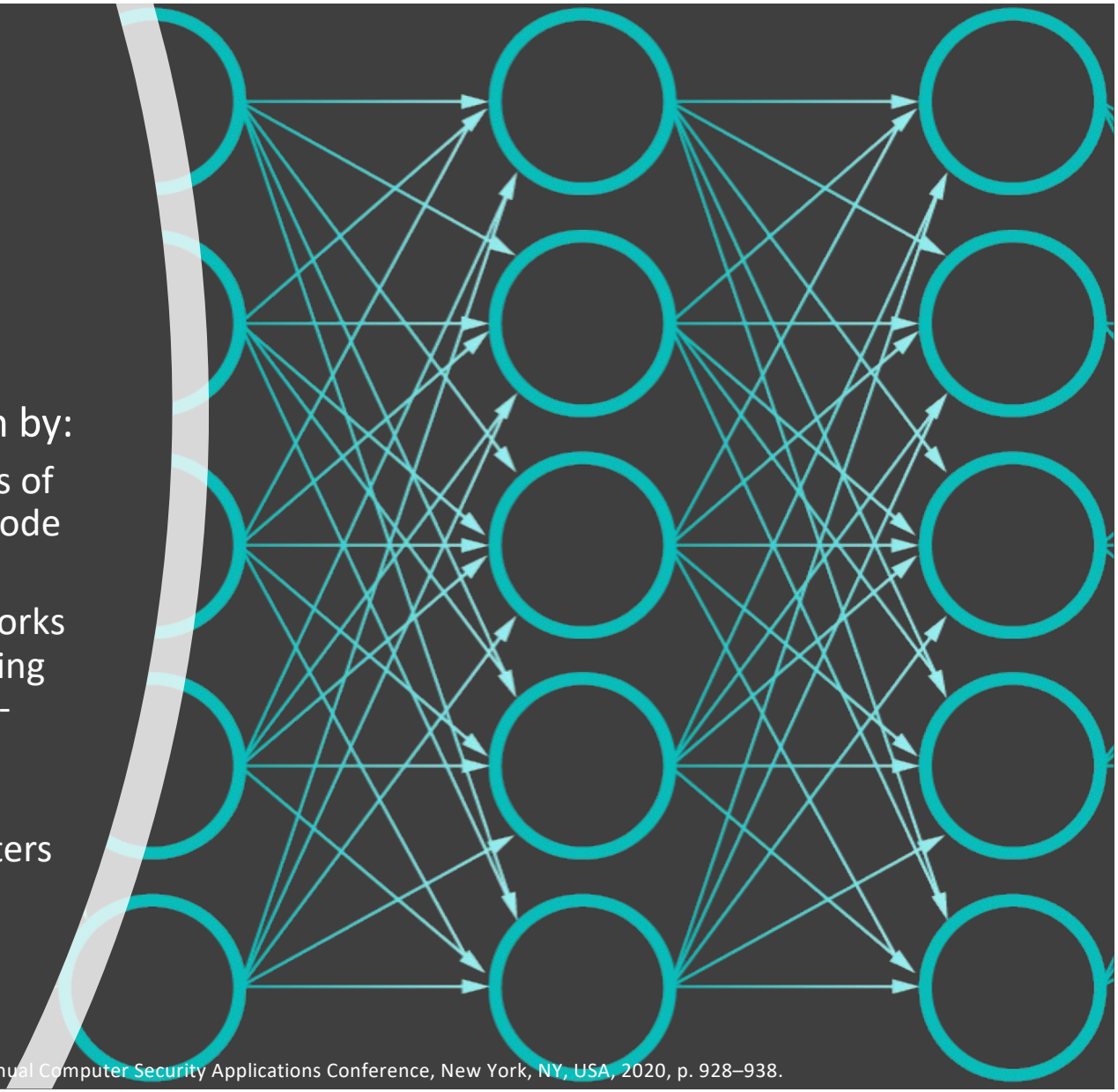
- In 2021, the industry of machine learning had a value of 15.5 billions of USD.
- Some important drivers:
  - AI-as-a-Service and ML-as-a-Service;
  - IP protection;
  - tracking unfair usages;
  - protection against new attacks.
- Typical defensive approaches are in computer/network security.
- Information Hiding could play a role!



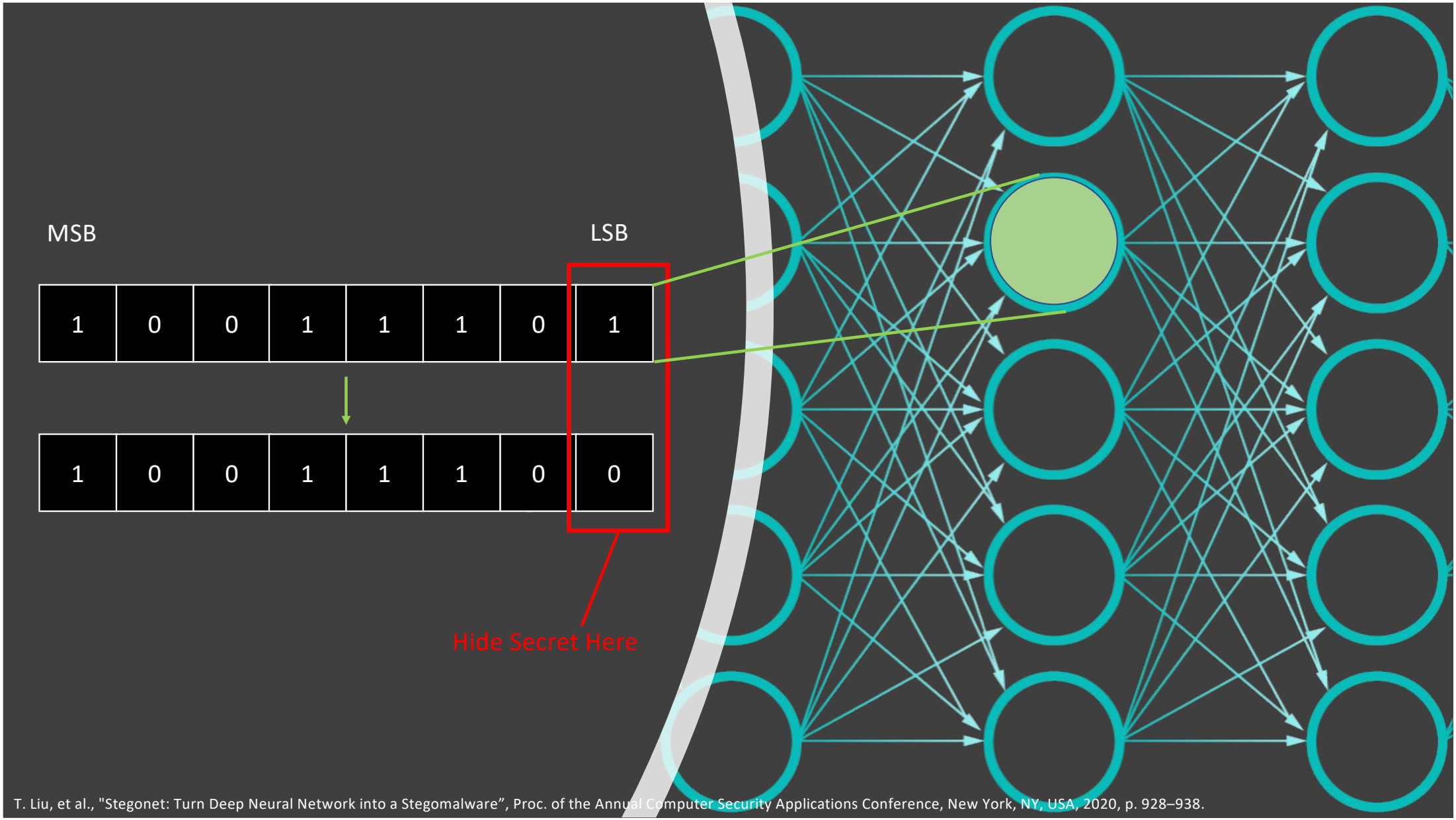
https://blogs.sap.com/2021/11/08/protect-your-machine-learning-models-with-watermarking/

AI Watermarking

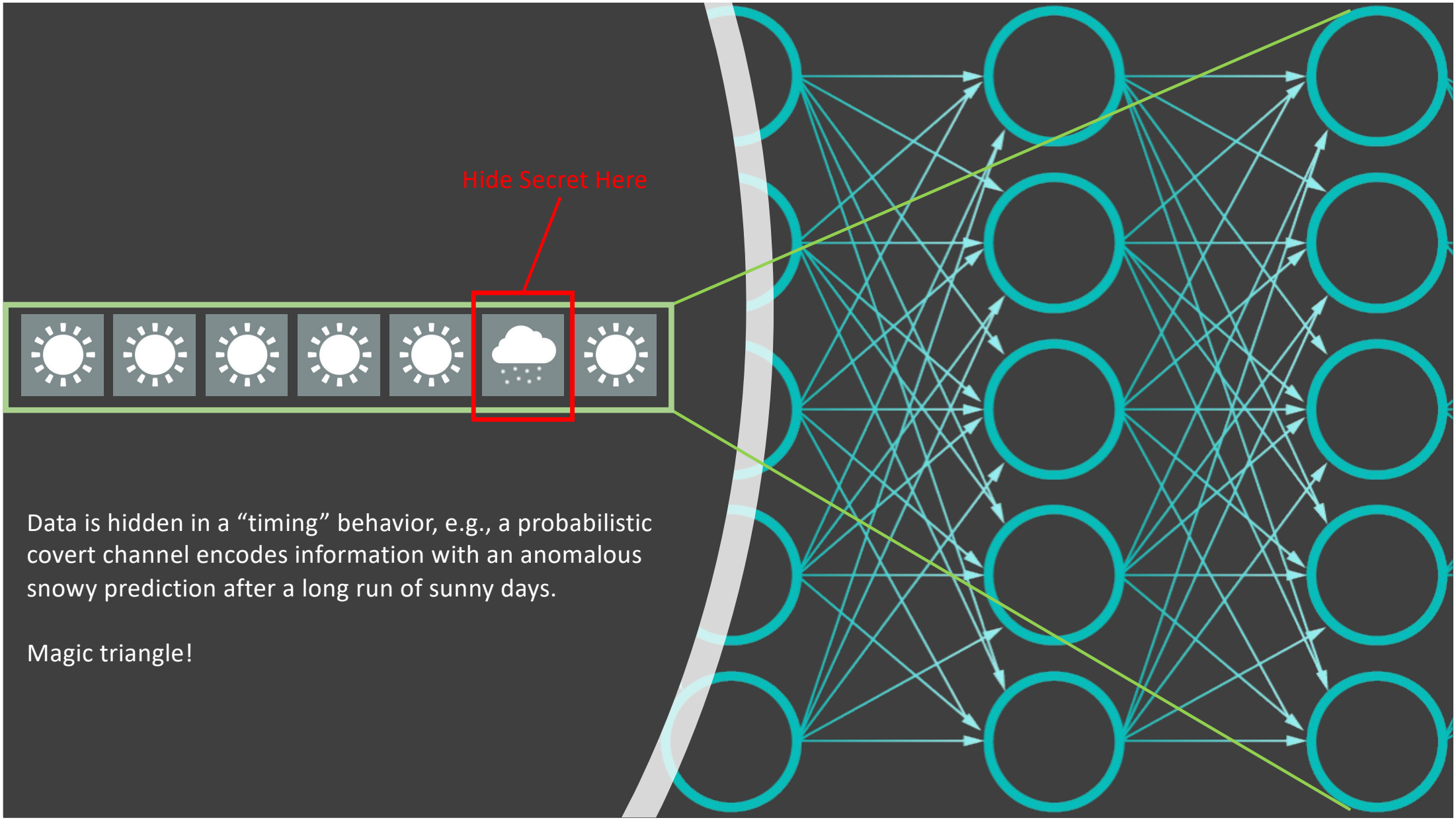
- To track a model, a payload can be hidden by:
  - classical **LSB approaches** (i.e., the last bits of each model parameter are altered to encode arbitrary data);
  - exploiting **resilience** of deep neural networks and introduce internal errors by overwriting the model with secret data and do not re-train the resulting “broken neurons”;
  - **mapping** techniques, i.e., arbitrary information is placed by altering parameters with same or closest values.



T. Liu, et al., "Stegonet: Turn Deep Neural Network into a Stegomalware”, Proc. of the Annual Computer Security Applications Conference, New York, NY, USA, 2020, p. 928–938.



T. Liu, et al., "Stegonet: Turn Deep Neural Network into a Stegomalware", Proc. of the Annual Computer Security Applications Conference, New York, NY, USA, 2020, p. 928–938.



Data is hidden in a “timing” behavior, e.g., a probabilistic covert channel encodes information with an anomalous snowy prediction after a long run of sunny days.

Magic triangle!

Software Obfuscation

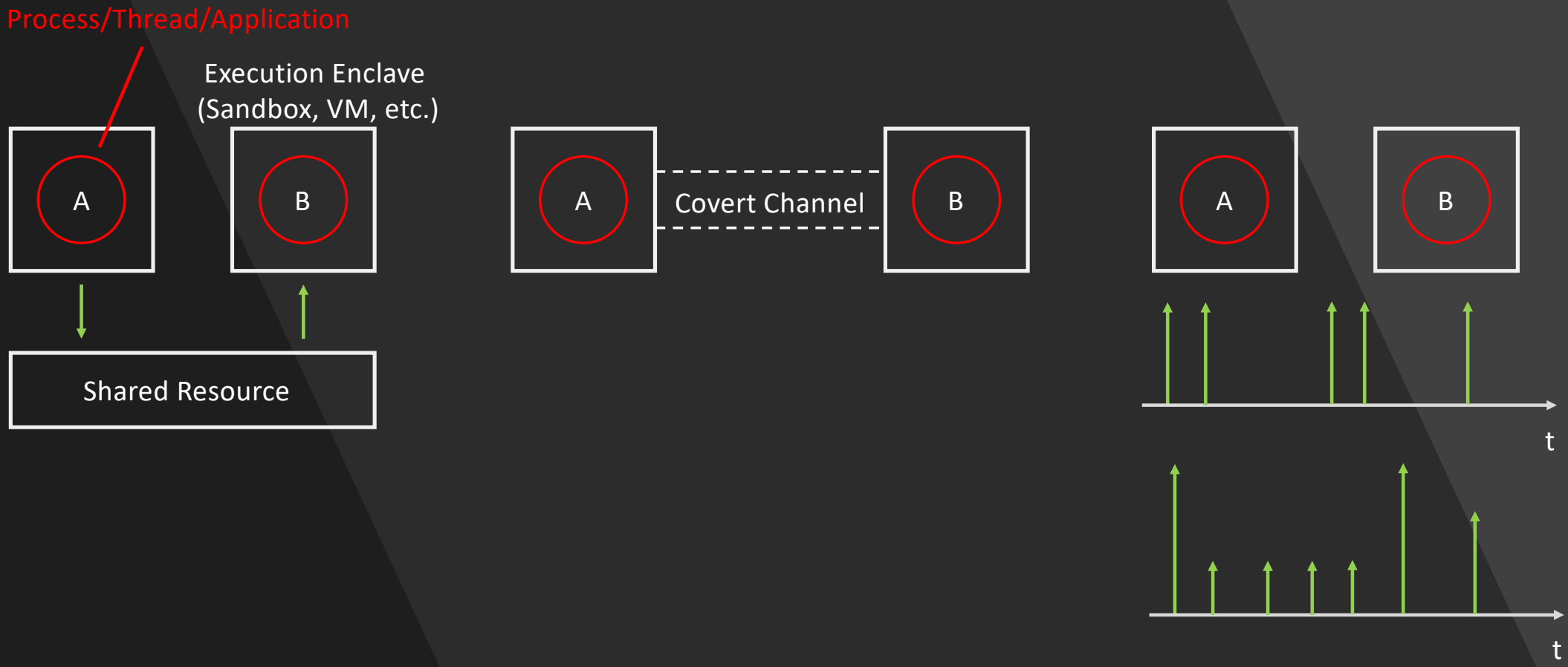
```
void P() {
    int a = b;
}
```

- Software protection, e.g., to make reverse engineering attempts harder, usually exploits **code obfuscation**.
- Information Hiding can be a valuable tool, too.
- The “colluding applications” scheme can be used to implement timing or probabilistic channels for obfuscating the code as well as for enforcing specific execution behaviors.

```
void P() {
    int i,a = 0;
    for(i=0;i<b;i++) {
        a++;
    }
}
```

J. Stephens, et al., "Probabilistic Obfuscation Through Covert Channels", *European Symposium on Security and Privacy,* 2018, pp. 243-257

Software Obfuscation



Takeaway Message N.1

Information Hiding is a double-edged sword: fear it or use it.

Takeaway Message N.2

There is not a unique hiding strategy and there is not a general defensive methodology.

Takeaway Message N.3

Scientific computing and manipulation of large-scale data are appealing for attackers and have many societal implications (e.g., climate change). Do not underestimate your attractiveness.

Conclusions

- Information Hiding is a double-edged sword that can be used for:
  - **attack**, for instance to conceal malicious payloads or create covert channels;
  - **defense**, for instance to watermark or protect AI models or software.
- The embedding process, attacks, applications, and countermeasures are tightly-coupled with the specific tasks:
  - no one-size-fits-all mechanisms!
- Hiding data can be done (almost) against **any media** or **digital object** and in an **unbounded** numbers of **scenarios**.

Thank You!
Questions?

Twitter: @lucacaviglione

email: luca.caviglione@cnr.it

The Canary Trap!

Why Watermarking?

- The main idea is to hide data in contents to:
  - Track their use (diffusion);
  - Recognize tampering and manipulations;
  - Enforce copyright;
  - …
- Main applications:
  - Digital Right Management (DRM) in media and digital contents;
  - Elimination of the “Analog Hole”.