April Cyber Threat Intelligence report

2024-05-02 I **TLP:CLEAR** I CERT aDvens - CTI
Advens - 38 rue des Jeuneurs - 75002 Paris

Table of content

1. Executive summary

This month, the aDvens CERT presents three noteworthy vulnerabilities, in addition to those already published.

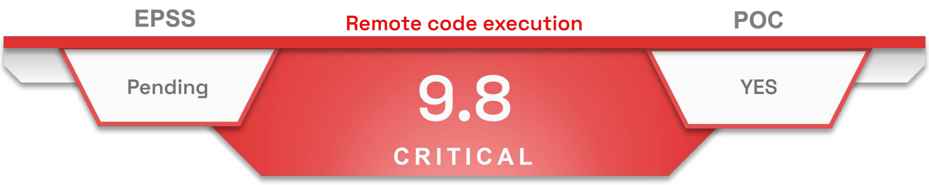
Through two articles, the CERT analysts discuss:

- The Trojan horse Mispadu used in campaigns targeting European countries.
- A study in cyberpsychology extrapolating techniques of mimicry and camouflage from the natural world to the cyber sphere.

2. Vulnerabilities

This month, aDvens' CERT highlights **three** vulnerabilities affecting commonly used technologies within companies.
They are sorted by severity (availability of proofs of concept, exploitation…). Applying their patches or workarounds is highly recommended.

2.1. GLPI - CVE-2024-31705


EPSS
Pending
Remote code execution
9.8
CRITICAL
POC
YES

A critical vulnerability was discovered in GLPI's plugin *Shell Commands* developed by Infotel. An insufficient validation of user-supplied input in this plugin allows an unauthenticated attacker, by sending a specially crafted request, to execute arbitrary code.

2.1.1. Type of vulnerability

- **CWE-78**: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

2.1.2. Risk

- Remote code execution

2.1.3. Severity (Base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.1.4. Impacted Products

- GLPI 10.x including the latest version

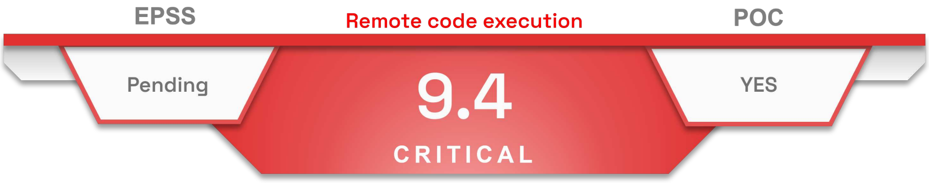
2.1.5. Recommendations

- Deactivate the Shell Commands plugin or apply mesures to restrict its access. GLPI has already removed it from its marketplace.

2.1.6. Proof of concept

A proof of concept is available in open source.

2.2. PHP - CVE-2024-1874



EPSS

Remote code execution

POC

Pending

9.4

CRITICAL

YES

On 9 april 2024, *Flatt Security Inc*'s security researcher RyotaK has disclosed multiple vulnerabilities in several programming languages on Windows. These languages contain argument parsing flaws when calling Windows' **CreateProcess()** function by running a batch file (.bat,.cmd,...).

This command injection vulnerability in the *$command* parameter of PHP's function **proc_open** allows an unauthenticated attacker, by sending specially crafted commands, to execute arbitrary code.

2.2.1. Type of vulnerability

- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

2.2.2. Risk

- Remote code execution

2.2.3. Severity (Base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	Low

2.2.4. Impacted Products

PHP:

- Versions 8.1.x prior to 8.1.28
- Versions 8.2.x prior to 8.2.18
- Versions 8.3.x prior to 8.3.6

2.2.5. Recommendations

- Update PHP to version 8.1.28, 8.2.18, 8.3.6 or later.

2.2.6. Proof of concept

A proof of concept is available in open source.

2.3. Cisco IMC - CVE-2024-20295

EPSS

Pending

Privilege escalation

8.8

IMPORTANT

POC

YES

An improper sanitisation of user input in Cisco IMC allows an authenticated attacker, by sending a specially crafted CLI command, to execute arbitrary code and obtain root privileges.

2.3.1. Type of vulnerability

- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

2.3.2. Risk

- Remote code execution
- Privilege escalation

2.3.3. Severity (Base score CVSS 3.1)

Attack vector	Local	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	Low	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.3.4. Impacted Products

Products running a vulnerable release of Cisco IMC in the default configuration:

- 5000 Series Enterprise Network Compute Systems (ENCS)
- Catalyst 8300 Series Edge uCPE
- UCS C-Series Rack Servers in standalone mode
- UCS E-Series Servers

Cisco appliances that are based on a preconfigured version of a Cisco UCS C-Series Server if they expose access to the Cisco IMC CLI:

- 5520 and 8540 Wireless Controllers
- Application Policy Infrastructure Controller (APIC) Servers
- Business Edition 6000 and 7000 Appliances
- Catalyst Center Appliances, formerly DNA Center (DNAC)
- Cisco Telemetry Broker Appliance
- Cloud Services Platform (CSP) 5000 Series
- Common Services Platform Collector (CSPC) Appliances
- Connected Mobile Experiences (CMX) Appliances
- Connected Safety and Security UCS Platform Series Servers
- Cyber Vision Center Appliances
- Expressway Series Appliances
- HyperFlex Edge Nodes
- HyperFlex Nodes in HyperFlex Datacenter without Fabric Interconnect (DC-NO-FI) deployment mode

- IEC6400 Edge Compute Appliances
- IOS XRv 9000 Appliances
- Meeting Server 1000 Appliances
- Nexus Dashboard Appliances
- Prime Infrastructure Appliances
- Prime Network Registrar Jumpstart Appliances
- Secure Email Gateways
- Secure Email and Web Manager
- Secure Endpoint Private Cloud Appliances
- Secure Firewall Management Center Appliances, formerly Firepower Management Center
- Secure Malware Analytics Appliances
- Secure Network Analytics Appliances
- Secure Network Server Appliances
- Secure Web Appliances
- Secure Workload Servers

2.3.5. Recommendations

- For Cisco 5000 Series ENCS and Cisco Catalyst 8300 Series Edge uCPE, upgrade Cisco Enterprise NFV Infrastructure Software (NFVIS) to version 4.14.1 or later. Cisco IMC is upgraded as part of the firmware auto-upgrade process.

- For other vulnerable products with default configuration, update Cisco IMC's version:
  - Cisco UCS C-Series M4 Rack Server: Update to version 4.1(2m) or later.
  - Cisco UCS C-Series M5 Rack Server: Update to version 4.1(3m), 4.2(3j), 4.2(3j) or later.
  - Cisco UCS C-Series M6 Rack Server: Update to version 4.2(3j), 4.3(2.240002) or later.
  - Cisco UCS C-Series M7 Rack Server: Update to version 4.3(2.240002) or later.
  - Cisco UCS E-Series M2 and M3: Update to version 3.2.15 or later.
  - Cisco UCS E-Series M6: Update to version 4.12.2 or later.

- For Cisco appliances that are based on a preconfigured version of a Cisco UCS C-Series Server, administrators can perform a direct upgrade of the Cisco IMC software to one of the fixed releases mentioned above. Exceptions are listed below:
  - Cisco Telemetry Broker Appliance: Update to version 4.3(2.240009) or later.
  - IEC6400 Edge Compute Appliances: Update to version 4.2(3j) or later.
  - Secure Email Gateways: Update to version 4.2(3j) or later.
  - Secure Email and Web Manager: Update to version 4.2(3j) or later.
  - Secure Endpoint Private Cloud Appliances: Update to version 4.3(2.240009) or later.
  - Secure Firewall Management Center Appliances: Update to version 4.3(2.240009) or later.
  - Secure Malware Analytics Appliances: Update to version 4.3(2.240009) or later.
  - Secure Network Analytics Appliances M4: Update to version 4.1(2m) or later.
  - Secure Network Analytics Appliances M5 and M6: Update to version 4.3(2.240009) or later.
  - Secure Network Server Appliances: Update to version 4.3(2.240009) or later.
  - Secure Web Appliances: Update to version 4.2(3j) or later.

- Additionnal information is available in Cisco's advisory.

2.3.6. Proof of concept

A proof of concept is available in open source.

3. Mispadu, the globalisation of South American malware

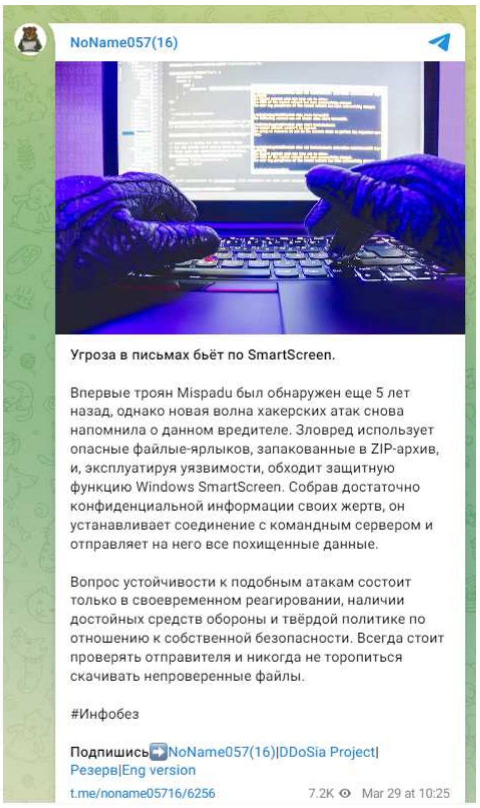
In a report published on 26 March 2024, the Morphisec Labs cybersecurity group reported a geographical expansion of Mispadu Trojan's activities. The Trojan was detected in three European countries during its last attack campaign in April 2023: Italy, Sweden and Poland.

3.1. Origins

The Mispadu banking Trojan was detected in 2019 by the ESET group. Created in Delphi, Mispadu runs on Windows systems. It is usually distributed via malicious executable files, often disguised as coupons or popular software. Once activated, Mispadu deploys various modules to steal credentials and manipulate banking transactions.

3.2. European campaign

In previous campaigns, Mispadu concentrated on Latin American countries, with a focus on Brazil and Mexico. In the April 2023 campaign, although Mexico remained the primary target, attacks against entities located in Italy, Poland and Sweden were detected. The sectors targeted included the financial and services sectors, as well as the automotive industry. This recent expansion into Europe reflects an evolution in the malware group's strategy to reach a wider audience. Following this campaign, the malware also attracted the interest of the pro-Russian Hacktivist group NoName057, which devoted a publication to it at the end of March 2024.



NoName057(16)

Угроза в письмах бьёт по SmartScreen.

Впервые троян Mispadu был обнаружен еще 5 лет назад, однако новая волна хакерских атак снова напомнила о данном вредителе. Зловред использует опасные файлые-ярлыков, запакованные в ZIP-архив, и, эксплуатируя уязвимости, обходит защитную функцию Windows SmartScreen. Собрав достаточно конфиденциальной информации своих жертв, он устанавливает соединение с командным сервером и отправляет на него все похищенные данные.

Вопрос устойчивости к подобным атакам состоит только в своевременном реагировании, наличии достойных средств обороны и твёрдой политике по отношению к собственной безопасности. Всегда стоит проверять отправителя и никогда не торопиться скачивать непроверенные файлы.

#Инфобез

Подпишись➡️NoName057(16)|DDoSia Project|
Резерв|Eng version

t.me/noname05716/6256 7.2K Mar 29 at 10:25

Figure 1. NoName057 publication

3.3. TTPs

The Mispadu malware works as follows: following a spear phishing e-mail, when victims attempt to "see the full bill", they are prompted to download a ZIP file triggering the infection process. This file usually contains a Visual Basic script (VBScript) which, once executed, downloads another VBScript. The latter loads and executes the Mispadu payload using a AutoIT script after being decrypted and injected into memory by a loader. This use of scripts is new compared to previous Mispadu campaigns. Furthermore, these attacks are characterised by the use of two distinct command and control servers: one to retrieve intermediate and final payloads, and the other to exfiltrate stolen credentials.

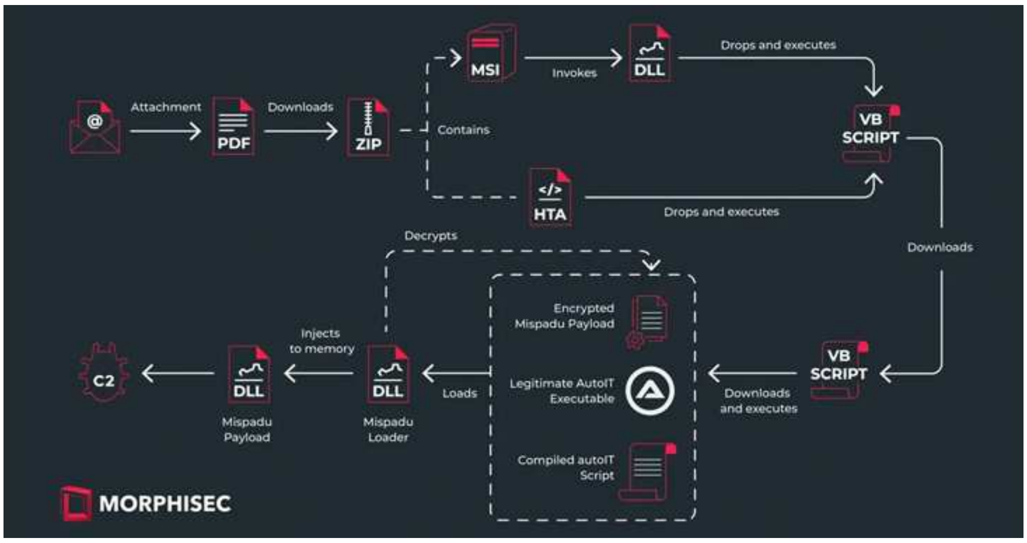
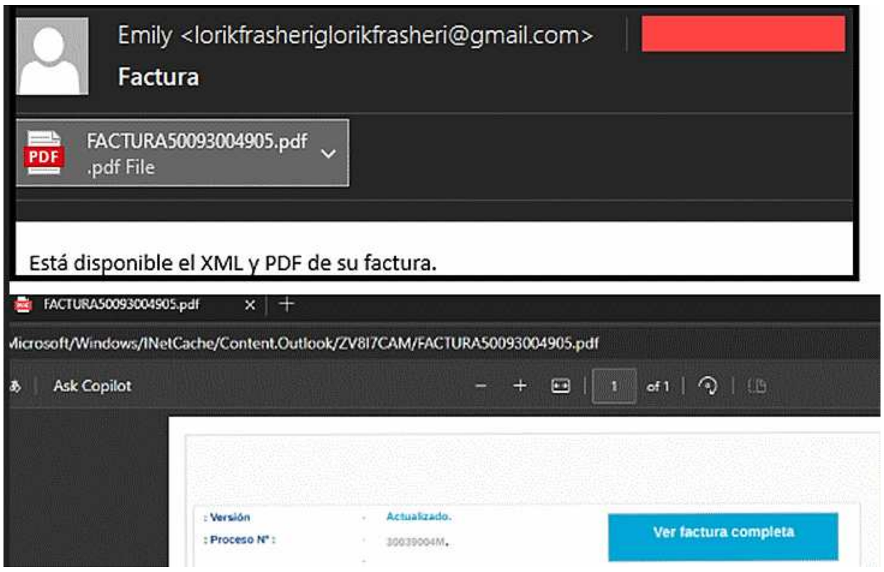


Figure 2. Kill Chain Mispadu – source : Morphisec

- Initial Access: Mispadu mainly uses spear phishing via fake invoice e-mails to reach its victims. It seems to have abandoned the malicious ads of its previous campaigns. In particular, Mispadu uses the CVE-2023-36025 vulnerability (CVSS 8.8) in Windows SmartScreen. This flaw allows threat actors to create Internet shortcut files or hyperlinks specifically designed to bypass SmartScreen warnings, exposing users to malicious binaries hosted on threat actor network shares.



Emily <lorikfrasheriglorikfrasheri@gmail.com> [redacted]
Factura

FACTURA50093004905.pdf
.pdf File

Está disponible el XML y PDF de su factura.

FACTURA50093004905.pdf

licrosoft/Windows/INetCache/Content.Outlook/ZV8I7CAM/FACTURA50093004905.pdf

: Versión Actualizado.
: Proceso N° : 30039004M.

Figure 3. Spear Phishing Mispadu – source : Morphisec

- Execution: The malware is executed via PowerShell scripts or malicious macros embedded in documents.
- Persistence: The malware modifies Windows registry entries or creates scheduled tasks that reactivate the malware every time the system is rebooted.
- Privilege escalation: Mispadu attempts to gain administrative rights to run its processes unhindered.
- Code injection: Mispadu is able to inject malicious code into legitimate processes to avoid detection.
- Evasion and defense: Mispadu uses DLL (Dynamic Link Library) injection to discreetly insert its malicious code into running processes. This technique enables it to hide its malicious activity behind legitimate processes, reducing the chances of detection by security software. For example, it can inject its code into processes such as *explorer.exe* or *svchost.exe*, which are essential to Windows and often excluded from detailed scans by antiviral software.

The malware also employs rootkit techniques to hide its files and registry keys, making it difficult to detect and remove. Mispadu can also disable Windows security settings and antivirus software via commands that modify group policies or registry entries that control security features. Finally, Mispadu uses polymorphism techniques to regularly change its executable code, making it difficult for traditional antivirus signatures to identify it. In addition, it employs methods to detect the execution environment and suspend its activities if it detects that it is running in a virtual machine or sandboxed environment.

- Information gathering: the malware is equipped with keylogging and clipboard monitoring features to collect credentials such as usernames and passwords, a tactic used to intercept information copied during financial transactions or other sensitive data exchanges. It also monitors web browsing activity, extracting data from forms and capturing cookies. Mispadu can intercept data in transit between the browser and web sites, enabling the theft of session data and other sensitive information.

3.4. Conclusion

Mispadu can have a significant impact on victims by stealing financial and personal information, compromising access to systems and enabling further intrusions. The reuse of this financial data to forge new, more elaborate spear phishing scenarios highlights the importance of this data for cybercriminal groups. To mitigate the risks associated with this malware, companies need to implement multi-layered security solutions, such as endpoint detection and response (EDR) systems, and regular security awareness training for employees.

4. Cyberpsychology : inspiration from biologicial mimicry and camouflage

This article proposes to **draw inspiration from biological mimicry and camouflage** to **imagine useful cybersecurity concepts**. Based on these concepts, **psychological tactics and strategies can be developed** to contribute to **cyberdefense** and **threat intelligence**.

This article is composed of 4 sections. The first is a description of mimicry and camouflage in biology. The second section explores mimicry, while the third is devoted to camouflage. Finally, the fourth section presents the psychological tactics and strategies that result from this reflective work.

4.1. The basics of mimicry and camouflage

4.1.1. An ultimate goal: survive

To survive in the natural environment, some organisms use **evolved resemblances** and **methods of disguise**.

These can be used by prey to psychologically deceive their predators, for example: the prey mimics the warning signals of a toxic organism to repel its predator (Batesian mimicry). Predators can exploit their prey's camouflage to disguise their appearance and blend in with their surroundings (Disruptive coloration).

Below is an infographic which conveys, in a simplified and non-exhaustive manner, some of well-known evolved resemblances and methods of disguise.

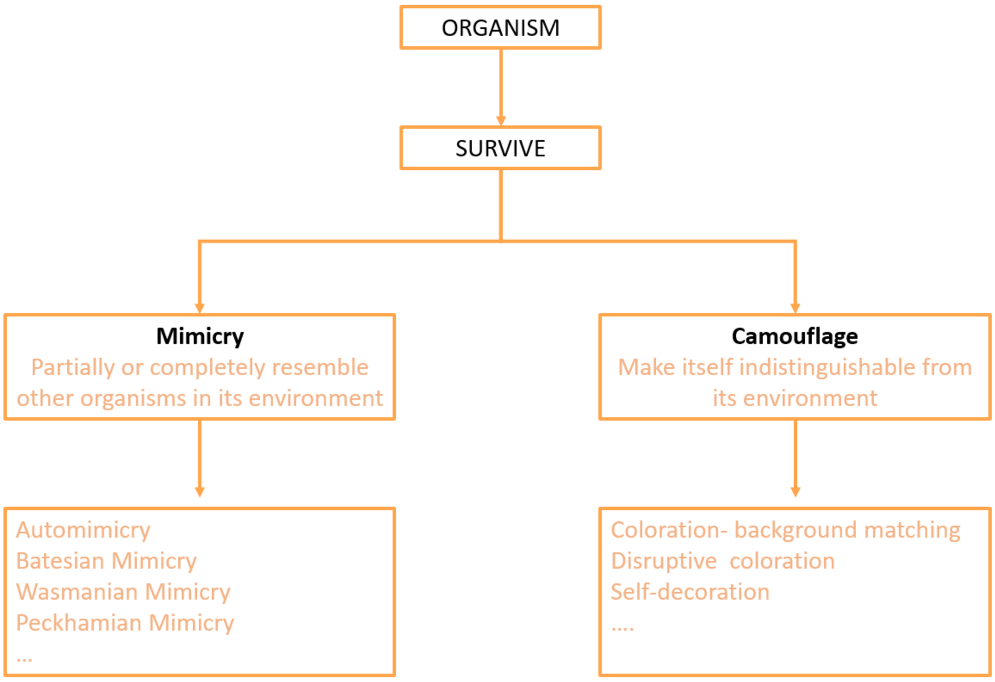

ORGANISM
SURVIVE
Mimicry
Partially or completely resemble other organisms in its environment
Camouflage
Make itself indistinguishable from its environment
Automimicry
Batesian Mimicry
Wasmanian Mimicry
Peckhamian Mimicry
…
Coloration- background matching
Disruptive coloration
Self-decoration
….

Figure 4. Mimicry and camouflage.

4.1.2. Understanding mimicry

Mimicry allows an organism to **partially or completely resemble other organisms in its environment**. The effort involves the **mimic organism** copying the morphology or behavior of another **model organism**. The one targeted by mimicry is the **dupe organism (receiver)**. It is possible that the model is also the one who is fooled by the mimic. Mimicry can be exploited in several ways: olfactory, tactile, acoustic, gustatory, behavioral and visual. Several categories of mimicry exist: automimicry, Batesian mimicry, Pekhamian mimicry, Wasmanian mimicry, Mullerian mimicry, etc.

In this article, two strategies are explored:

Automimicry

- Iphiclides podalirius - Butterfly "Le Flambé"
- Chelmon rostratus - Fish "Copperband butterfly"

Aggressive mimicry

- Hymenopus coronatus - The orchid mantis

4.1.3. Understanding camouflage

Camouflage allows an organism to **make itself indistinguishable from its environment**. The effort involves blending into the environment to be, for example, unrecognisable to predators, thereby contributing to the survival of the organism. There are many camouflage methods: coloration for background matching, disruptive coloration, self-decoration, etc.

In this article, two methods are explored:

Coloration for background matching

- Nezara viridula - Green stink bug

Disruptive coloration

- Leopardus Paradalis - Ocelot Leopard

4.2. Inspiration from natural mimicry

4.2.1. Automimicry: description and examples from nature

Among the different mimicry strategies, there is automimicry: the organism imitates a portion of its own body or that of another organism. One of the most famous phenomena is that of the ocellus, an eyespot that imitates an eye. This strategy can, for example, be used to **psychologically lure the predator** in order to: **waste time**, **provoke fear** or **divert an attack** to a less vital area.

Organism: Butterfly Iphiclides podalirius

Below is a photograph of a butterfly named "Le Flambé" (Iphiclides podalirius). At the bottom of its wings, towards the end of the abdomen, there is a blue ocellus surrounded by black inside an orange arch. This eyespot helps divert the predator's attack to attract it towards a non-vital area of the butterfly.

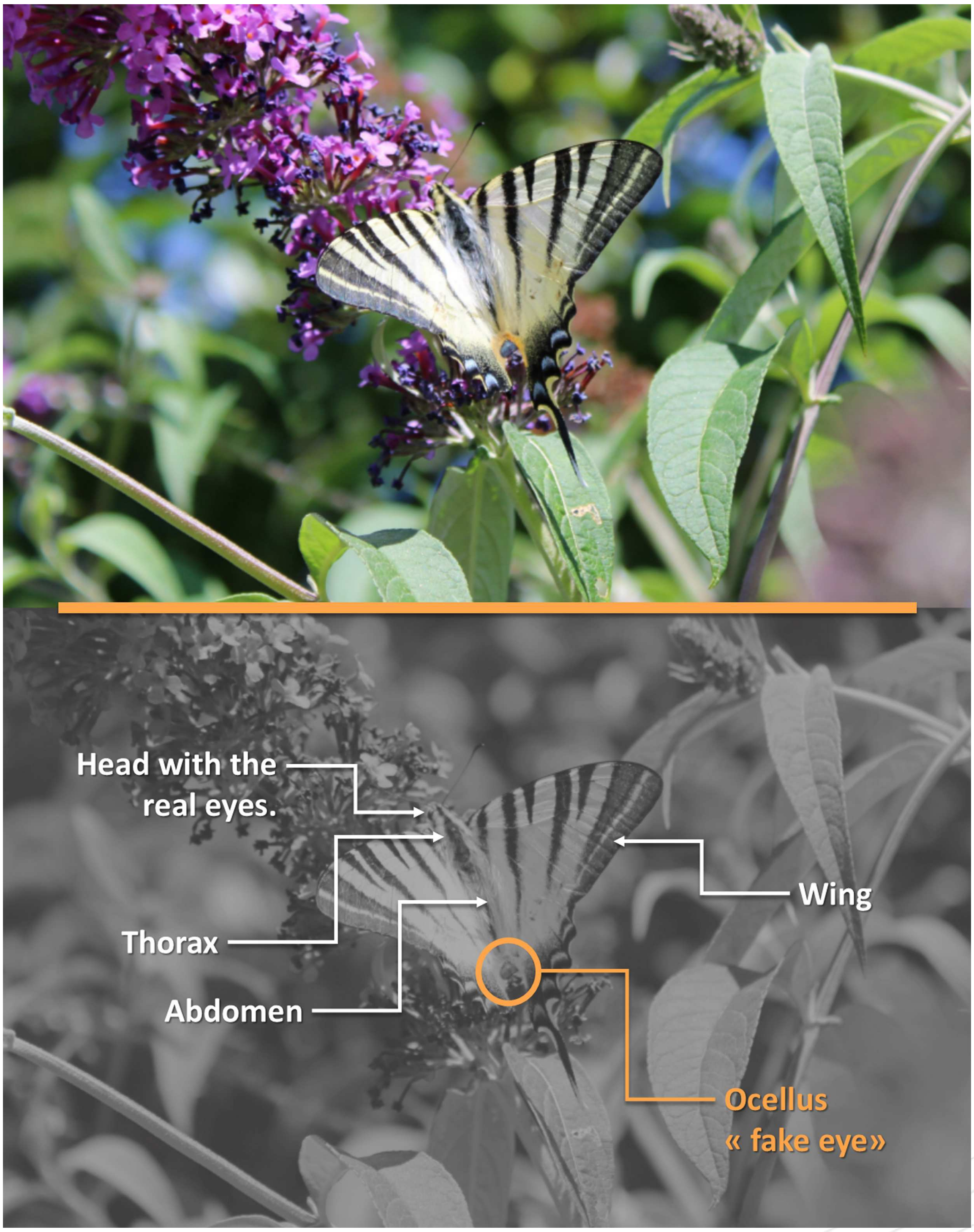


Figure 5. Butterfly: Iphiclides podalirius. Photographer: CTI Analyst. Garrigue of the Gard region, July 2021.

Organism: Fish Chelmon rostratus

Below is a photograph of a "Copper-banded Butterfly Fish" (Chelmon rostratus). This animal has an ocellus on its dorsal fin allowing it to escape from a predator. The real eyes are hidden by a yellow stripe while the "false eye" is highlighted by a strong contrast.

Like the butterfly "Le Flambé", this eyespot distracts the attacker and causes him to waste time during the offensive. This lost time gives the prey the opportunity to escape.

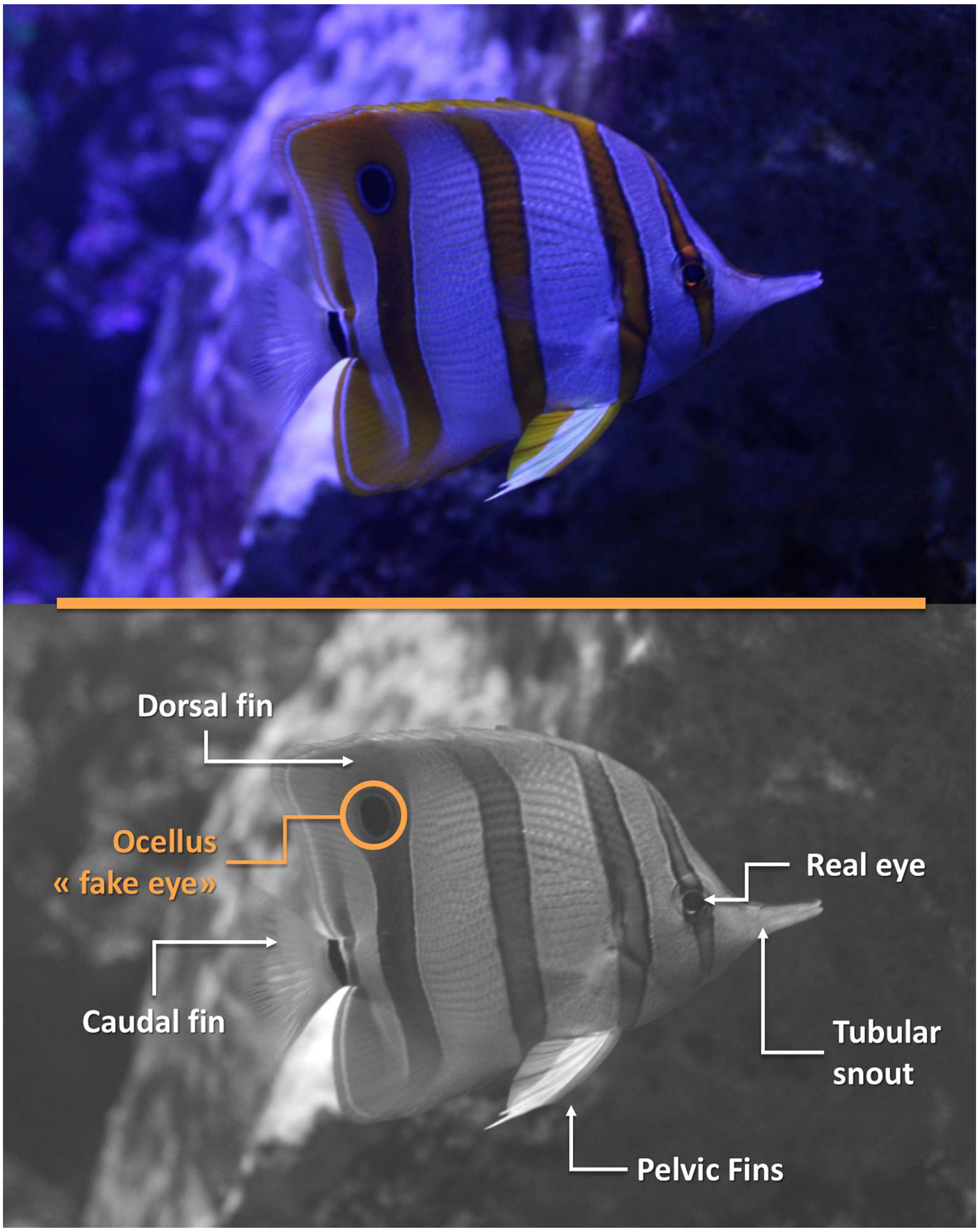


Figure 6. Fish: Chelmon rostratus. Photographer: CTI Analyst. Seaquarium of Grau du Roi, July 2022.

4.2.2. Automimicry: Cybersecurity application

The following are two examples of applications in cybersecurity.

Concept: divert the attacker towards a non-sensitive target

The goal of this first concept is to **divert the attacker's attention and effort**. To do this, the user creates an attractive folder (ocellus) with the title *Confidential*. In the attractive folder, a crafted file contains false information (fake credentials) to lure the attacker. The real sensitive file containing the usernames and passwords is hidden in another folder with an unattractive title.

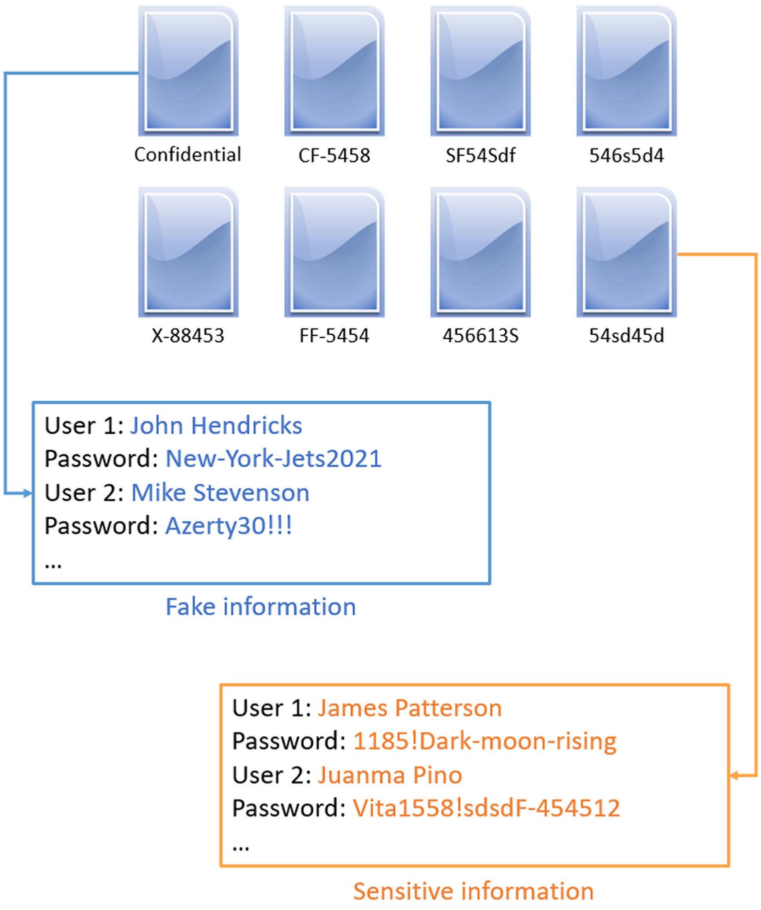


Figure 7. Scenario: divert the attacker.

Concept: divert and waste the attacker's time

If a case can be fabricated to lure the attacker in, to **divert their attention and effort**, then it is possible to complicate the context to also **waste their time**. In this imagined concept, several attractive folders and files are created. They are made up of false information, the quantity of which is significant. Like a disturbing background noise, this complication makes the environment difficult for the attacker to explore. The adversary's wasted time provides security with a time advantage in detecting, identifying, and responding to the threat.

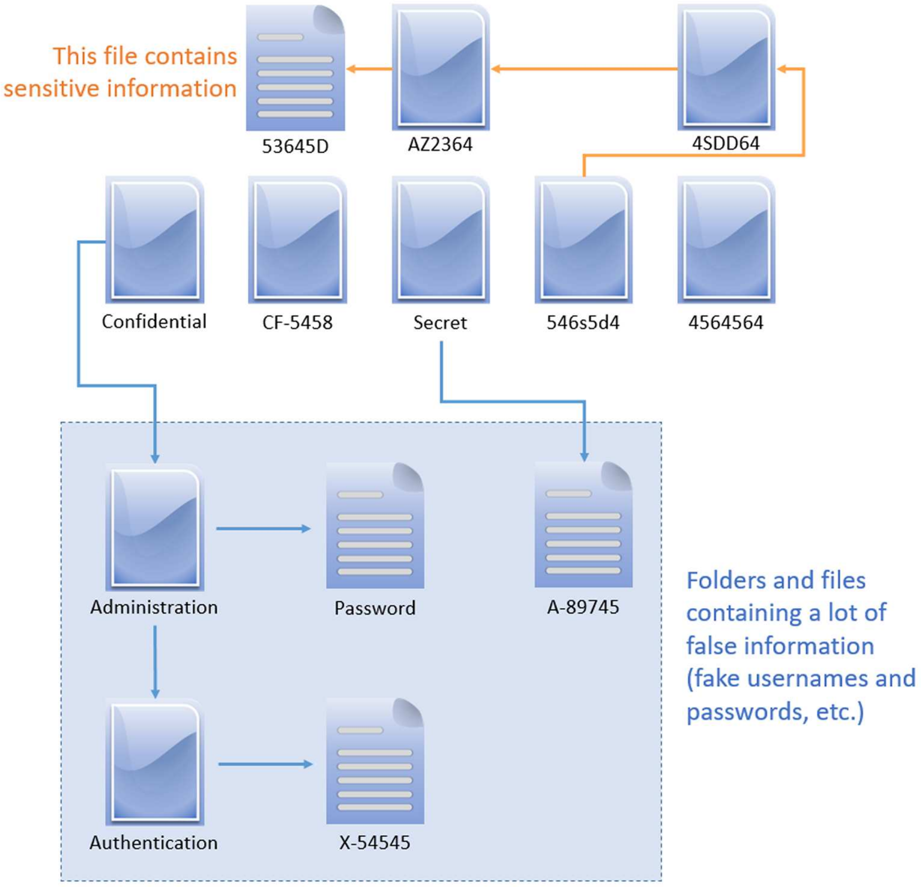

This file contains sensitive information
53645D
AZ2364
4SDD64
Confidential
CF-5458
Secret
546s5d4
4564564
Administration
Password
A-89745
Authentication
X-54545
Folders and files containing a lot of false information (fake usernames and passwords, etc.)

Figure 8. Scenario: distract the attacker and waste time.

4.2.3. Aggressive mimicry: description and natural example

Aggressive mimicry is used by certain predators to avoid being identified by their prey. Such predators can, for example, resemble a flower or dead leaf.

Organism: Hymenopus coronatus

Hymenopus coronatus is an orchid mantis, also known known as the flower mantis (resemblance and behavior). It is insectivorous and feeds on butterflies in particular. Hymenopus coronatus practices aggressive mimicry to lure its prey: they come to forage on the unsuspecting orchid mantis.

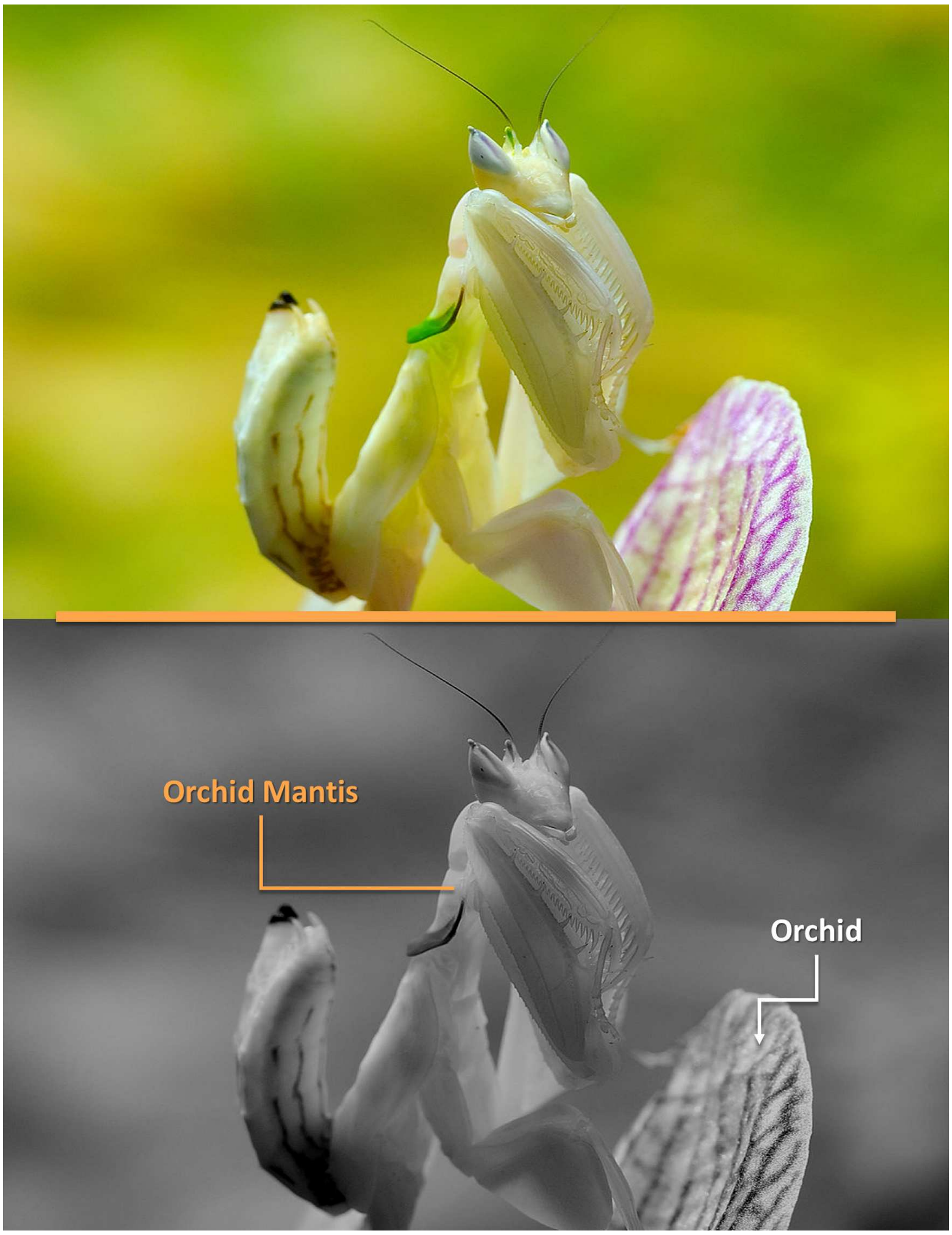


Figure 9. Hymenopus coronatus. Photographer: Luc Viatou. November 2008.

4.2.4. Aggressive mimicry: Cybersecurity application

Below are two examples of applications in cybersecurity.

Concept: disrupt the attacker's efforts and warn him

Several documents are crafted to contain false information as well as a hidden payload. In the event of intrusion and reconnaissance, these documents are strategically placed to attract the attacker's attention.

The document that contains the real sensitive information is encrypted and hidden among the crafted documents. If an exfiltration occurs, it is likely that the attacker will be duped into exfiltrating a crafted document that contains a payload.

When the exfiltrated document is consulted by the attacker on his system: the payload is activated and **triggers the self-deletion of the document**. Other actions are possible, for example: the payload displays **a warning message about the risks and sanctions of the crime carried out**. Its various possible actions also aim to **surprise the opponent** and **cause concern**.

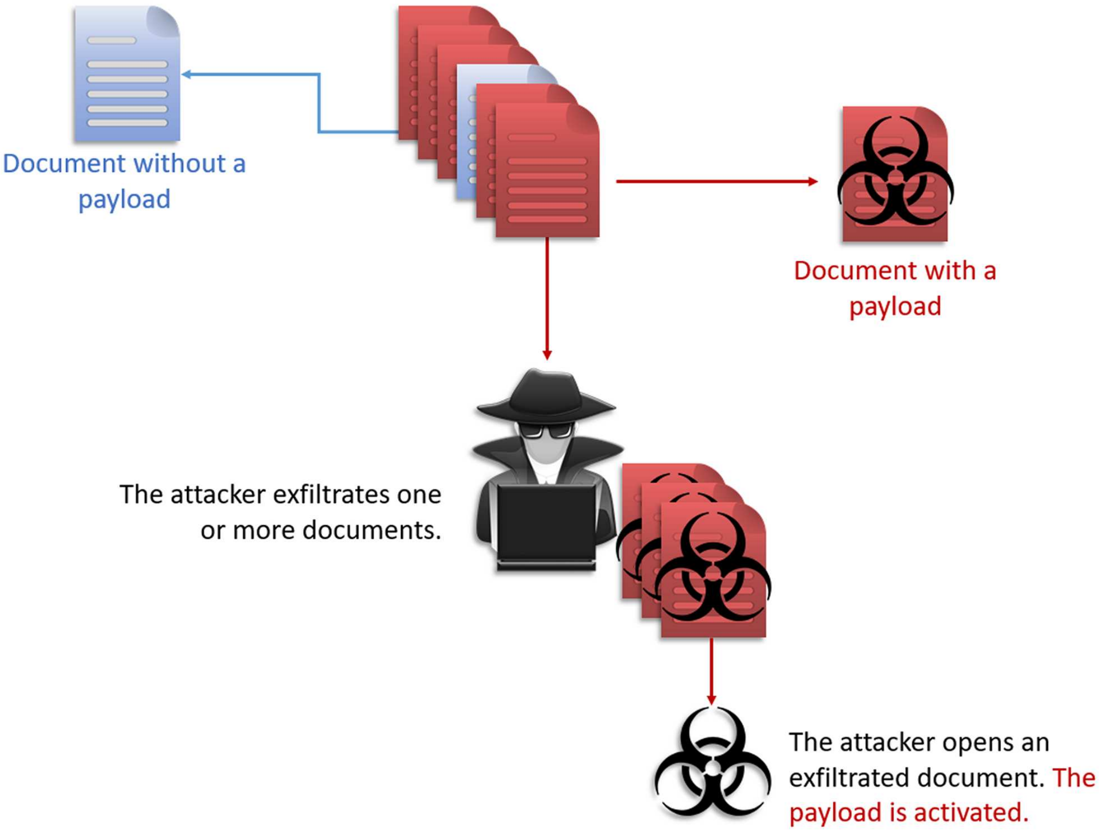

Document without a payload
Document with a payload
The attacker exfiltrates one or more documents.
The attacker opens an exfiltrated document. The payload is activated.

Figure 10. Crafted documents to disrupt the attacker's efforts.

Concept: collect information about the attacker

This second concept proposes that the activation of the payload triggers a discreet collection of information about the attacker (Host, IP address, user, etc.). These are uploaded to a CnC server controlled by security analysts. This concept contributes to the strategy of **threat intelligence**.

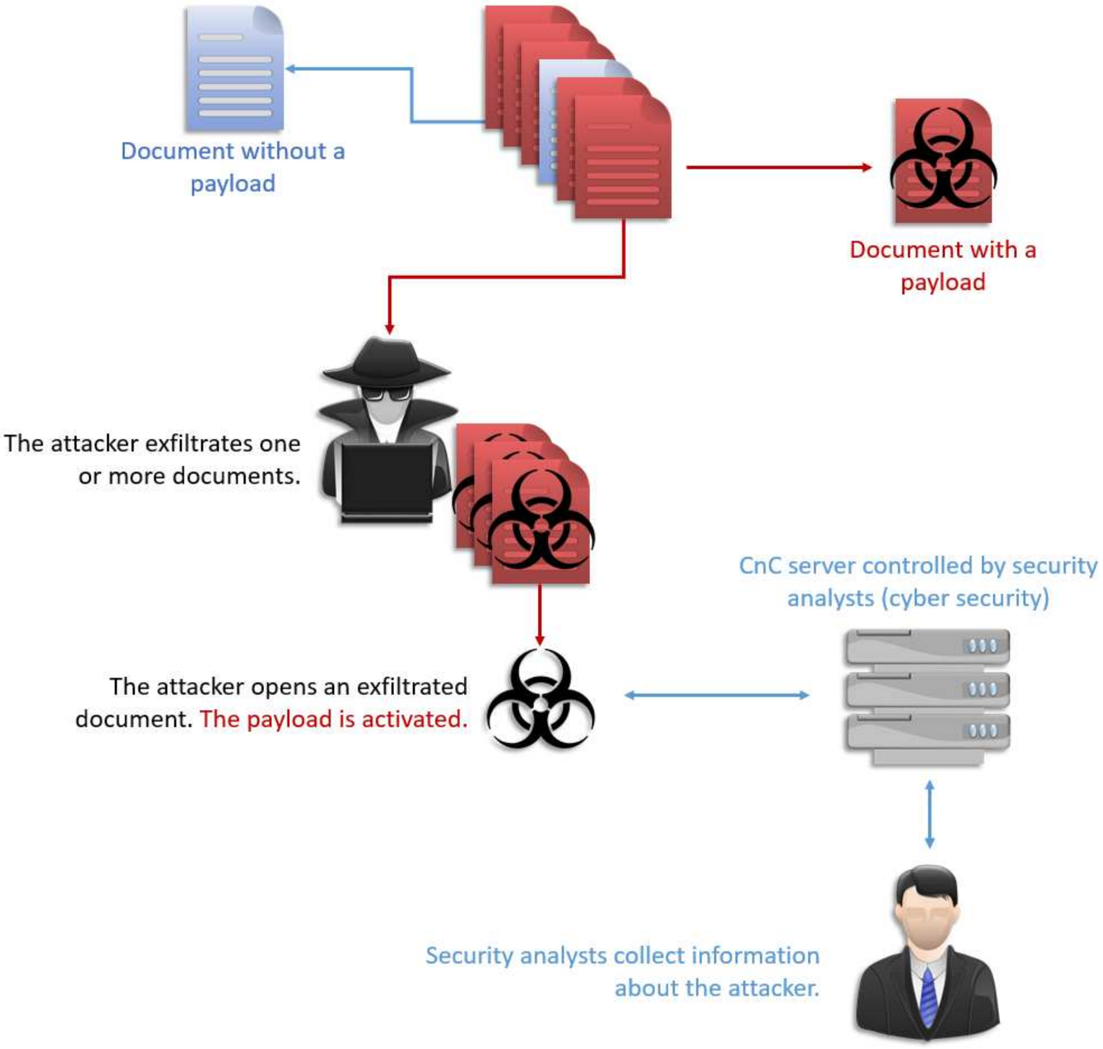

Document without a payload
Document with a payload
The attacker exfiltrates one or more documents.
CnC server controlled by security analysts (cyber security)
The attacker opens an exfiltrated document. The payload is activated.
Security analysts collect information about the attacker.

Figure 11. Crafted documents to collect information about the attacker.

4.3. Inspiration from camouflage

4.3.1. Coloration: description and example from nature

A very common method of camouflage in the natural environment is coloration. It consists in an organism having a color which matches the one of its background environment. The coloration method can, for example, be used to **psychologically lure the predator**: **deception through hiding** and to **waste time** (the predator must look for details).

Organism: Nezara viridula

Below is a photograph of a "green stink bug" larva Nezara viridula. Although still in the larval stage (summer), the green coloring is beginning to cover several parts of the body.

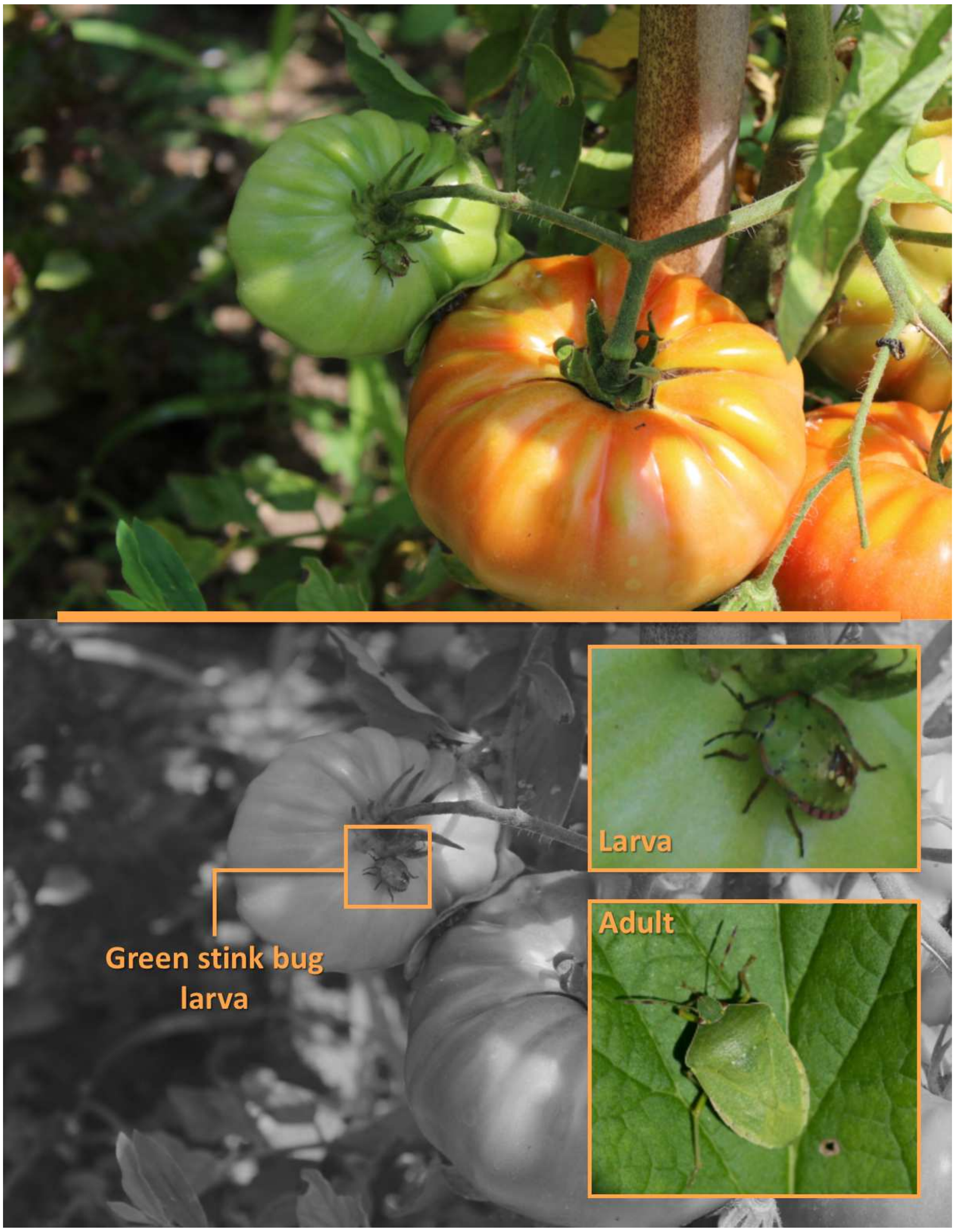


Figure 12. Bug Nezara viridula. Photographer: CTI Analyst. Garrigue of the Gard region. Tomato field. July 2021. Adult bedbug: pixabay Fablegros photography.

4.3.2. Coloration: Cybersecurity application

The following is an example of application in cybersecurity.

Concept: hiding information from the attacker

The goal of this concept is to **deceive by hiding** and **waste time** for the attacker. For this, many pages containing false information are created in a Word document. Sensitive information is written, in white on a white background, on a page inserted randomly between the others. In this concept of obfuscation, the visibility of sensitive information merges with the background (*Backgound matching*).

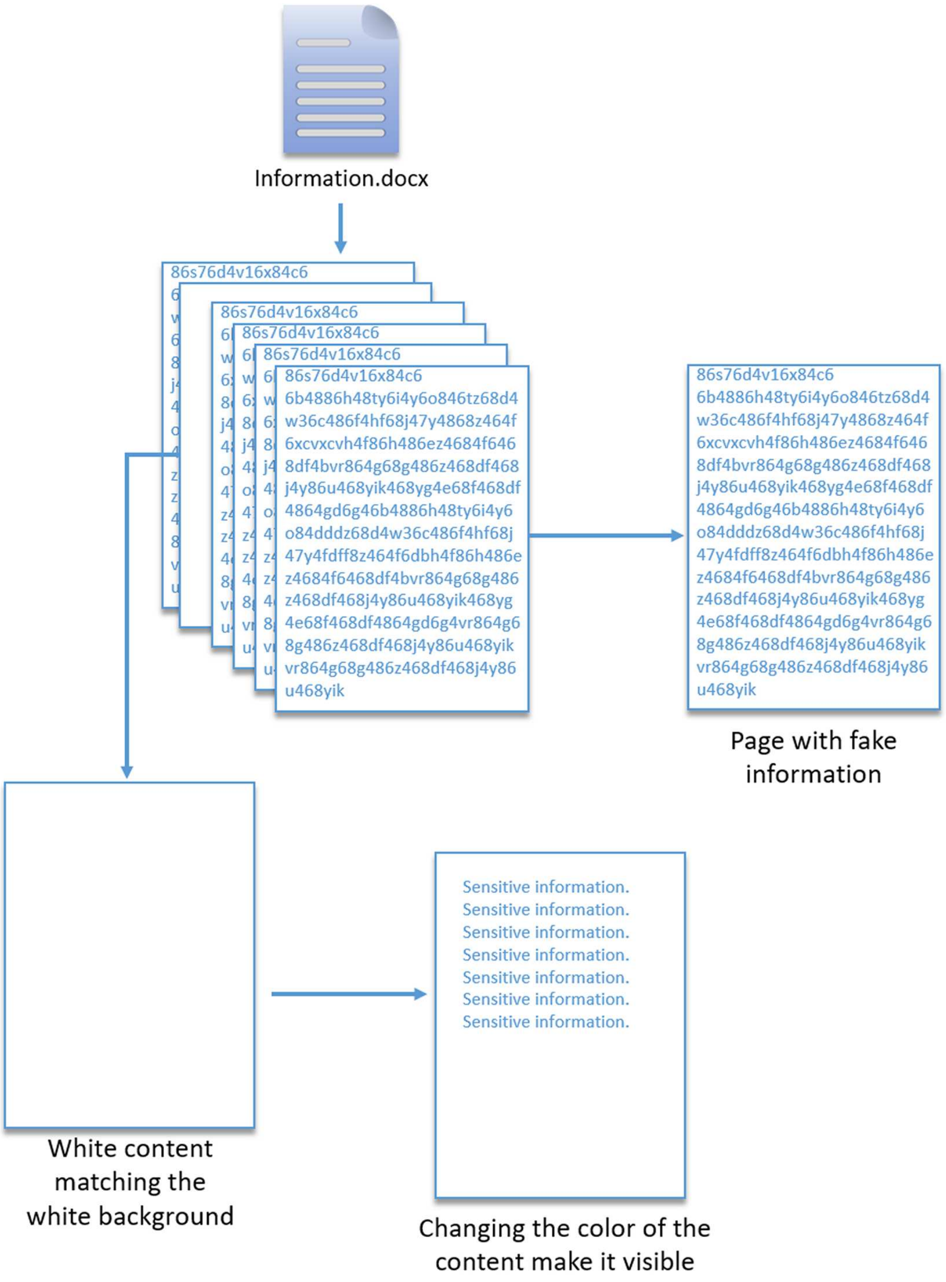

Information.docx
86s76d4v16x84c6
6b4886h48ty6i4y6o846tz68d4
w36c486f4hf68j47y4868z464f
6xcvxcvh4f86h486ez4684f646
8df4bvr864g68g486z468df468
j4y86u468yik468yg4e68f468df
4864gd6g46b4886h48ty6i4y6
o84dddz68d4w36c486f4hf68j
47y4fdff8z464f6dbh4f86h486e
z4684f6468df4bvr864g68g486
z468df468j4y86u468yik468yg
4e68f468df4864gd6g4vr864g6
8g486z468df468j4y86u468yik
vr864g68g486z468df468j4y86
u468yik
Page with fake information
White content matching the white background
Sensitive information.
Sensitive information.
Sensitive information.
Sensitive information.
Sensitive information.
Sensitive information.
Sensitive information.
Changing the color of the content make it visible

Figure 13. Sensitive information is hidden via a background matching coloration.

4.3.3. Disruptive coloration: description and example from biology

Disruptive coloration is an optical camouflage that allows an organism to hide itself in the environment. This type of camouflage can be characterised by rosettes (rounded patterns). The patterns break up the overall silhouette of the animal to reduce its detectability. It is therefore very difficult, for example, for prey to identify a leopard in grassy vegetation.

Organism: Leopardus Paradalis

Below is a photograph of a leopard Leopardus Paradalis. This wild cat lives in South America and Central America. The coat of the ocelot corresponds to an optical camouflage: **disruptive coloration**. This is made up of rosettes (rounded patterns).

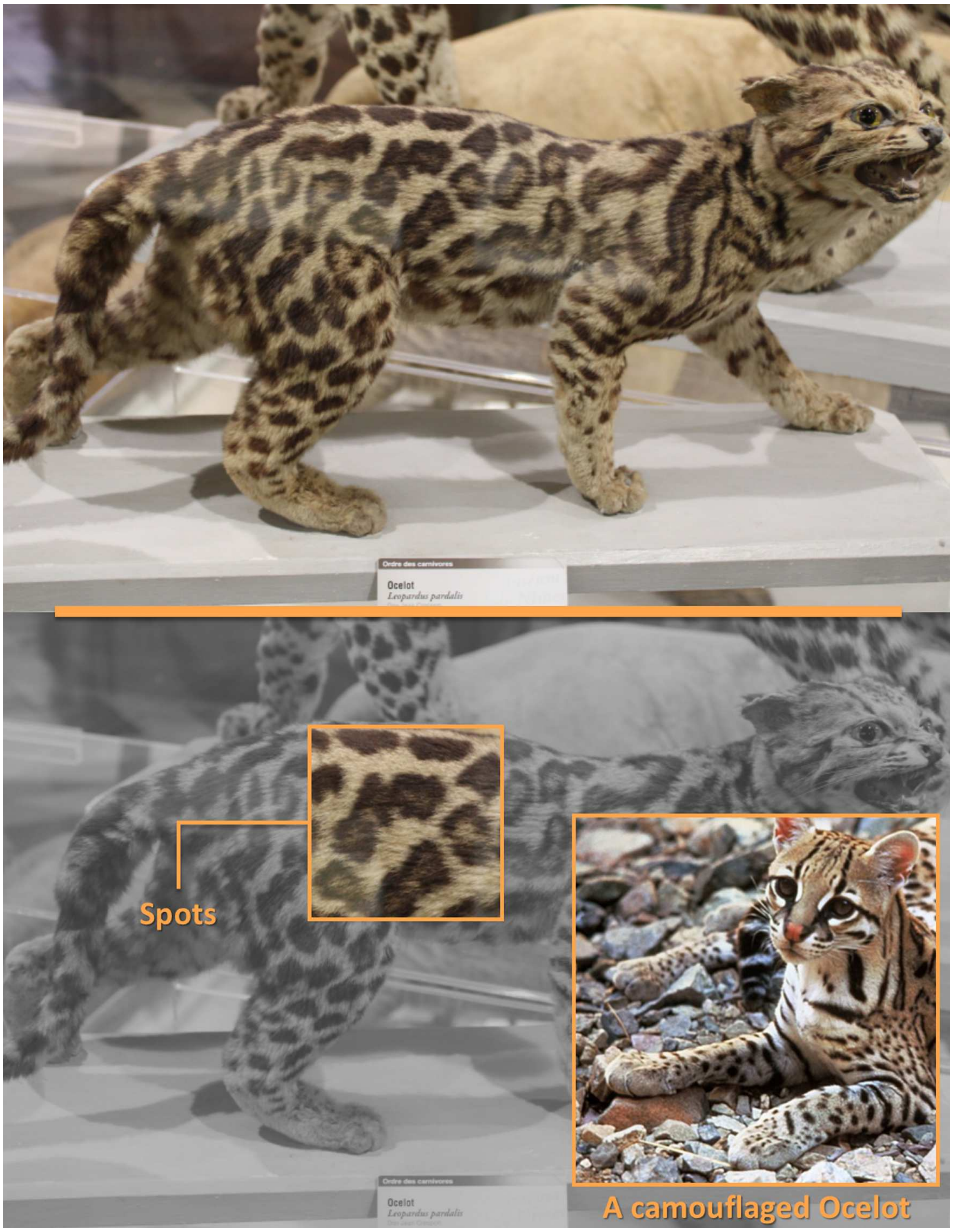


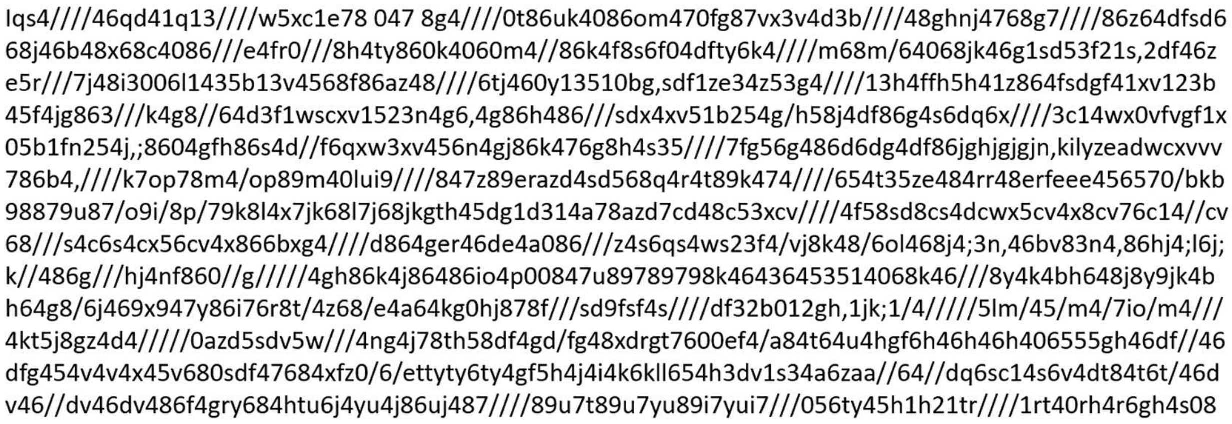
Figure 14. Leopardus Paradalis. Photographer: CTI Analyst. Nîmes's Museum of Natural History and Prehistory. July 2021. Ocelot camouflaged on the ground: U.S. Fish and Wildlife Service photograph - Wikipedia - Public domain.

4.3.4. Disruptive coloration: Cybersecurity application

Below is an example of an application in cybersecurity.

Concept: hiding information from the attacker (text version)

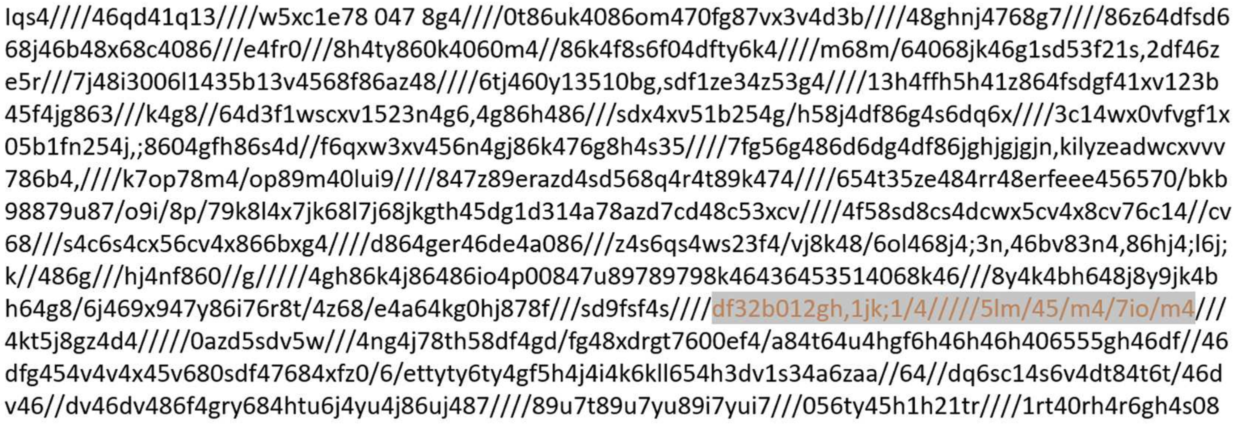
Identifying sensitive code in the content below can be extremely difficult for an attacker. First, the attacker may **experience the effect of camouflage and not discern the potential presence of sensitive code**. Secondly, any attempts to discern sensitive code **can be extremely time consuming**.



```
Iqs4////46qd41q13////w5xc1e78 047 8g4////0t86uk4086om470fg87vx3v4d3b////48ghnj4768g7////86z64dfsd6
68j46b48x68c4086///e4fr0///8h4ty860k4060m4//86k4f8s6f04dfty6k4////m68m/64068jk46g1sd53f21s,2df46z
e5r///7j48i3006l1435b13v4568f86az48////6tj460y13510bg,sdf1ze34z53g4////13h4ffh5h41z864fsdgf41xv123b
45f4jg863///k4g8//64d3f1wscxv1523n4g6,4g86h486///sdx4xv51b254g/h58j4df86g4s6dq6x////3c14wx0vfvgf1x
05b1fn254j,;8604gfh86s4d//f6qxw3xv456n4gj86k476g8h4s35////7fg56g486d6dg4df86jghjgjgjn,kilyzeadwcxvvv
786b4,////k7op78m4/op89m40lui9////847z89erazd4sd568q4r4t89k474////654t35ze484rr48erfeee456570/bkb
98879u87/o9i/8p/79k8l4x7jk68l7j68jkgth45dg1d314a78azd7cd48c53xcv////4f58sd8cs4dcwx5cv4x8cv76c14//cv
68///s4c6s4cx56cv4x866bxg4////d864ger46de4a086///z4s6qs4ws23f4/vj8k48/6ol468j4;3n,46bv83n4,86hj4;l6j;
k//486g///hj4nf860//g/////4gh86k4j86486io4p00847u89789798k46436453514068k46///8y4k4bh648j8y9jk4b
h64g8/6j469x947y86i76r8t/4z68/e4a64kg0hj878f///sd9fsf4s////df32b012gh,1jk;1/4/////5lm/45/m4/7io/m4///
4kt5j8gz4d4/////0azd5sdv5w///4ng4j78th58df4gd/fg48xdrgt7600ef4/a84t64u4hgf6h46h46h406555gh46df//46
dfg454v4v4x45v680sdf47684xfz0/6/ettyty6ty4gf5h4j4i4k6kll654h3dv1s34a6zaa//64//dq6sc14s6v4dt84t6t/46d
v46//dv46dv486f4gry684htu6j4yu4j86uj487////89u7t89u7yu89i7yui7///056ty45h1h21tr////1rt40rh4r6gh4s08
```

Figure 15. Code hidden in content.

In this concept of obfuscation, the sensitive code **df32b012gh,1jk;145lm45m47iom4** is hidden by taking inspiration from the leopard's coat. The typographic character **/** is added randomly in the sensitive code: **df32b012gh,1jk;1/4/////5lm/45/m4/7io/m4**. Added, the **/** character acts like a rosette (disruptive coloration): it breaks the "silhouette" of the sensitive code and causes it to be confused with all the rest of the content. Only a user who has knowledge of this code can easily identify it.



```
Iqs4////46qd41q13////w5xc1e78 047 8g4////0t86uk4086om470fg87vx3v4d3b////48ghnj4768g7////86z64dfsd6
68j46b48x68c4086///e4fr0///8h4ty860k4060m4//86k4f8s6f04dfty6k4////m68m/64068jk46g1sd53f21s,2df46z
e5r///7j48i3006l1435b13v4568f86az48////6tj460y13510bg,sdf1ze34z53g4////13h4ffh5h41z864fsdgf41xv123b
45f4jg863///k4g8//64d3f1wscxv1523n4g6,4g86h486///sdx4xv51b254g/h58j4df86g4s6dq6x////3c14wx0vfvgf1x
05b1fn254j,;8604gfh86s4d//f6qxw3xv456n4gj86k476g8h4s35////7fg56g486d6dg4df86jghjgjgjn,kilyzeadwcxvvv
786b4,////k7op78m4/op89m40lui9////847z89erazd4sd568q4r4t89k474////654t35ze484rr48erfeee456570/bkb
98879u87/o9i/8p/79k8l4x7jk68l7j68jkgth45dg1d314a78azd7cd48c53xcv////4f58sd8cs4dcwx5cv4x8cv76c14//cv
68///s4c6s4cx56cv4x866bxg4////d864ger46de4a086///z4s6qs4ws23f4/vj8k48/6ol468j4;3n,46bv83n4,86hj4;l6j;
k//486g///hj4nf860//g/////4gh86k4j86486io4p00847u89789798k46436453514068k46///8y4k4bh648j8y9jk4b
h64g8/6j469x947y86i76r8t/4z68/e4a64kg0hj878f///sd9fsf4s////df32b012gh,1jk;1/4/////5lm/45/m4/7io/m4///
4kt5j8gz4d4/////0azd5sdv5w///4ng4j78th58df4gd/fg48xdrgt7600ef4/a84t64u4hgf6h46h46h406555gh46df//46
dfg454v4v4x45v680sdf47684xfz0/6/ettyty6ty4gf5h4j4i4k6kll654h3dv1s34a6zaa//64//dq6sc14s6v4dt84t6t/46d
v46//dv46dv486f4gry684htu6j4yu4j86uj487////89u7t89u7yu89i7yui7///056ty45h1h21tr////1rt40rh4r6gh4s08
```

Figure 16. Code hidden in content.

Concept: hiding information from the attacker (graphic version)

The idea is identical to the previous concept, but the technique is different. A password is hidden in the picture below. Each letter of the password has a coloration that matches its background. Additionally, the letters are scattered in such a way as to break the "silouhette" of the password.

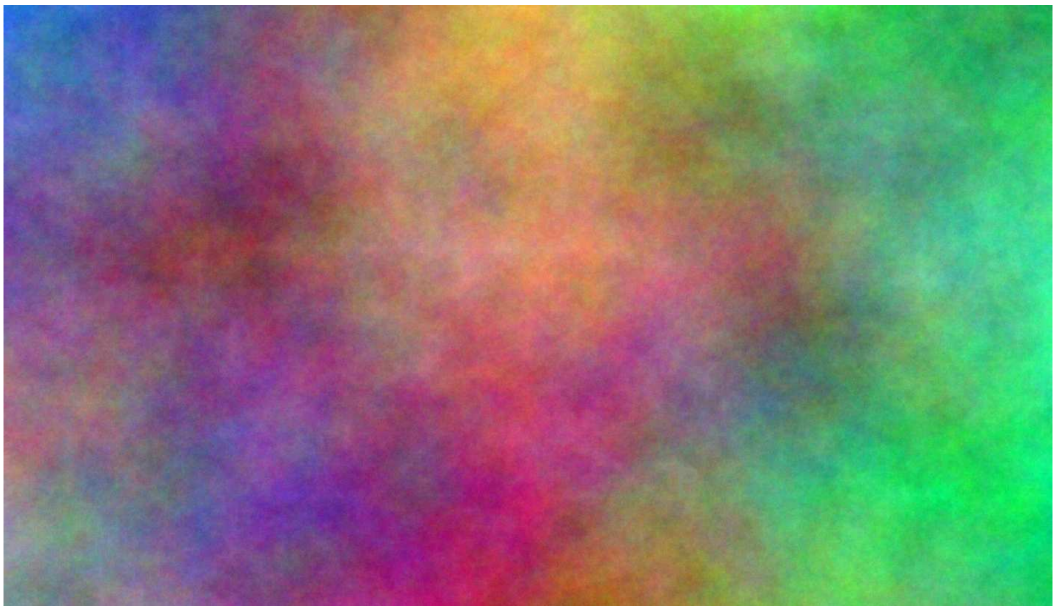


Figure 17. Password hidden in a picture.

By performing a contour search with a drawing software, the letters are revealed:

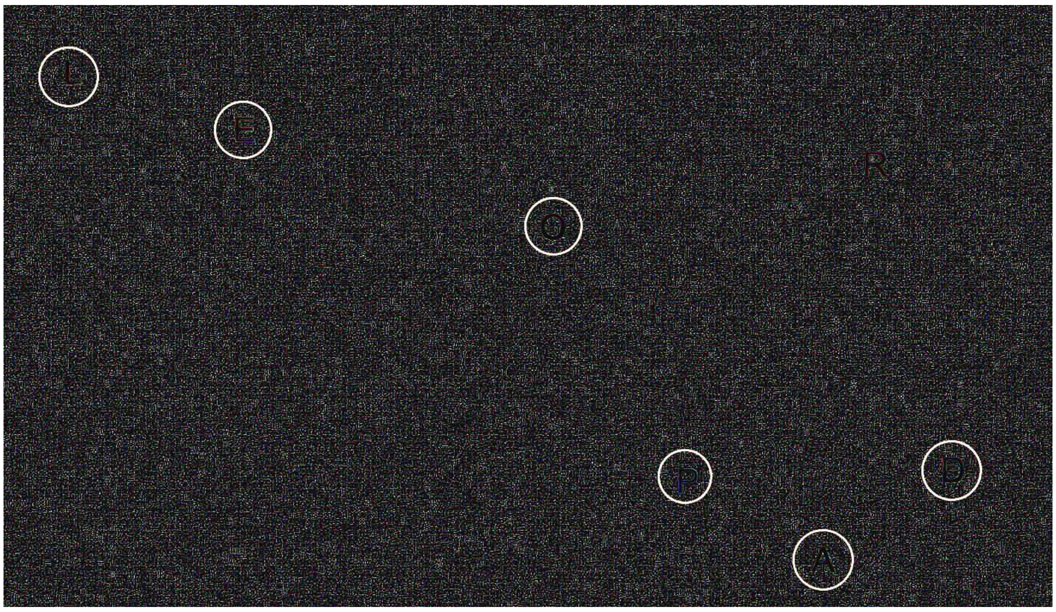


Figure 18. Password revealed in the picture.

The password is **LEOPARD**:

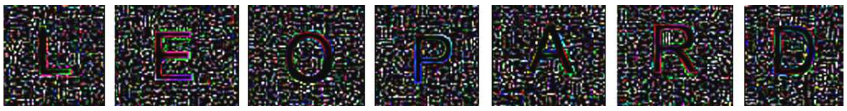


Figure 19. Reassembled password.

4.4. Cyberpsychology

The previous sections demonstrated how to develop useful cybersecurity concepts by drawing inspiration from biological mimicry and camouflage. From this reflection, interesting psychological tactics arise.

4.4.1. Psychological tactics

This section presents a (non-exhaustive) list of the tactics identified previously.

- Divert/distract attention
- Redirect offensive efforts
- Cause stress
- Cause frustration and anger
- Discourage the completion of the offensive
- Deceive by hiding
- Confuse
- Surprise/shock
- Warn the attacker that the offensive will have consequences (sanctions provided for by the Penal Code. Impose the superiority of the law)
- Warn the attacker that the offensive is futile (impose defensive superiority)
- Cause worry

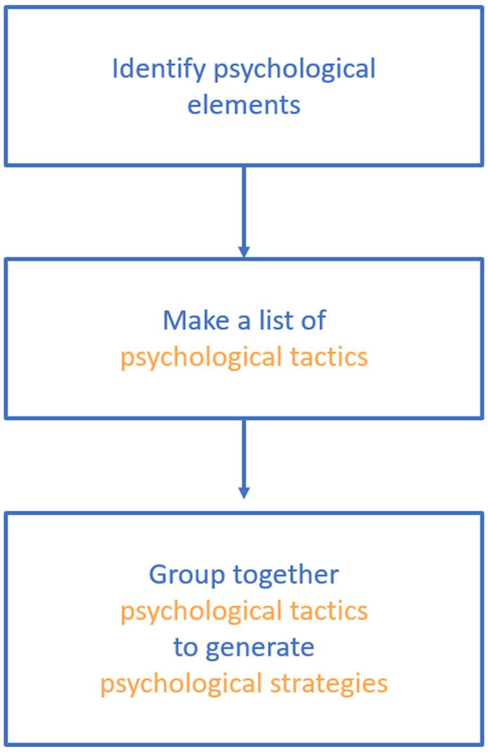

Identify psychological elements
Make a list of psychological tactics
Group together psychological tactics to generate psychological strategies

Figure 20. From inspiration to strategy.

4.4.2. Psychological strategies

Psychological tactics can be grouped, for example, into two **psychological strategies**: **Demoralise** and **Study**. These are combined with the main areas of cyber security effort: **cyberdefense** and **threat intelligence**.

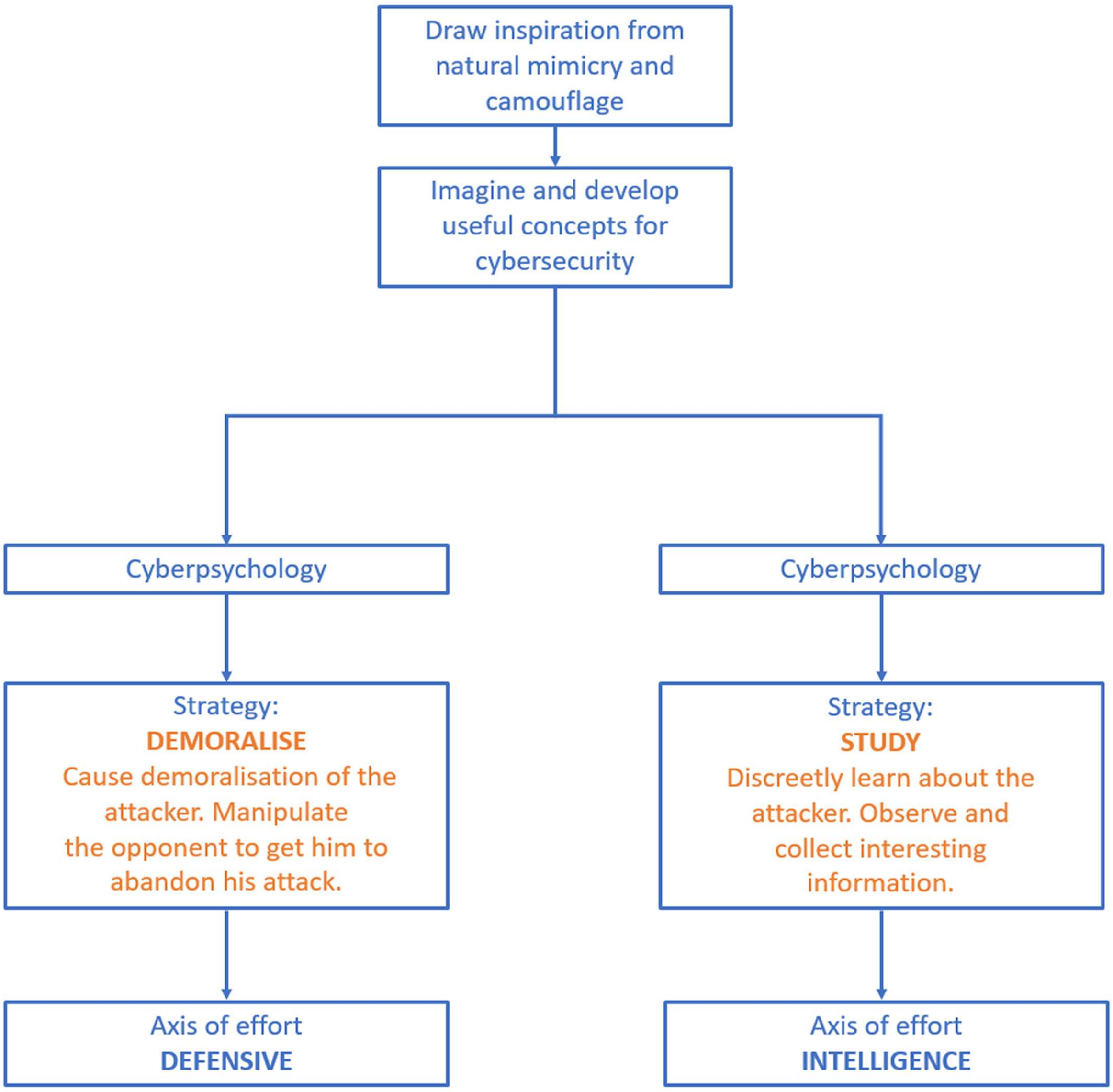

Draw inspiration from natural mimicry and camouflage
Imagine and develop useful concepts for cybersecurity
Cyberpsychology
Cyberpsychology
Strategy:
DEMORALISE
Cause demoralisation of the attacker. Manipulate the opponent to get him to abandon his attack.
Strategy:
STUDY
Discreetly learn about the attacker. Observe and collect interesting information.
Axis of effort
DEFENSIVE
Axis of effort
INTELLIGENCE

Figure 21. From inspiration to strategy.

4.5. Observe, imagine and conceptualise

4.5.1. A step-by-step guide

Below is step-by-step guide to practice and develop your own concepts. The recommended steps are as follows:

- Step 0 - **Curiosity and exploration**. What is happening in nature? (take photographs)
- Step 1 - **Observing the photograph**. Is there an organism?
- Step 2 - **Organism identification**. What organsim is it?
- Step 3 - **Method identification**. What does the organism do to hide in its environment?
- Step 4 - **Imagination and conceptualisation**. What use could this method have in cybersecurity?
- Step 5 - **Cyberpsychology**. Are there any psychological elements useful for cybersecurity?

4.5.2. Training

Below is a photograph to practice with, simply follow steps 1 to 5:

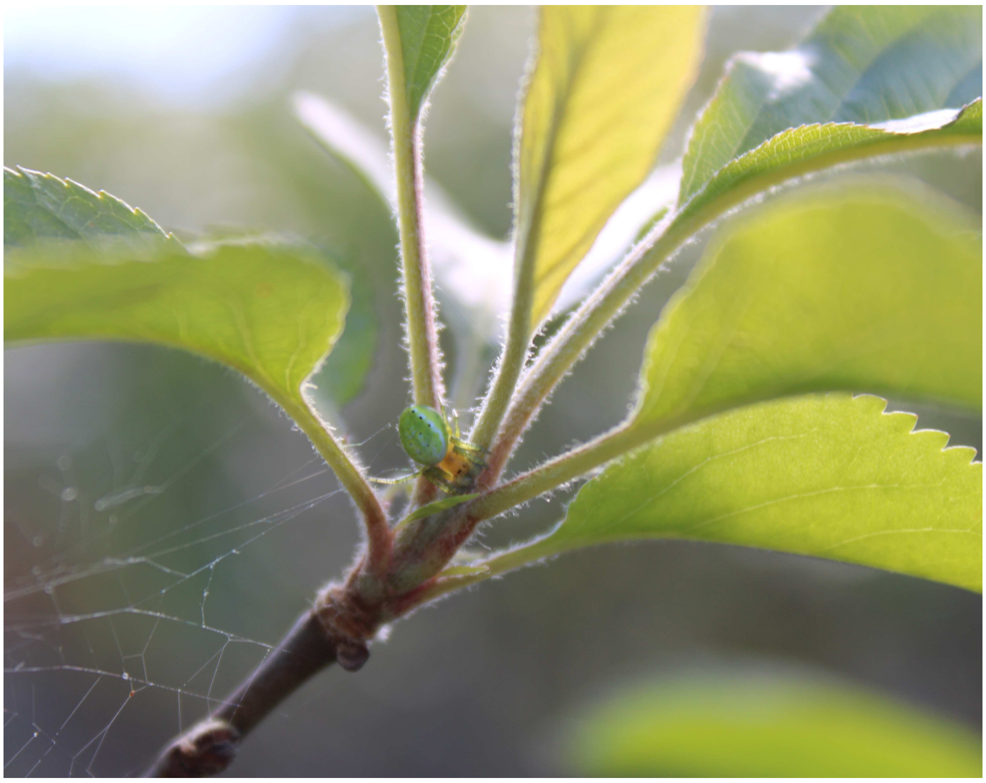


Figure 22. Observation, imagination and conceptualisation. Photographer: CTI Analyst. Garrigue of the Gard region. April 2024.

4.6. Conclusion

Biological mimicry and camouflage represent an endless source of inspiration. Exploring and understanding these natural phenomena allows analysts to imagine and develop concepts useful for cybersecurity.

It is at the core of this effort of reflection that potential psychological tactics are illustrated. Together, these tactics can be strategically coordinated: **demoralise** attackers and **study** them.

These **psychological strategies** enrich the main areas of cybersecurity effort, which are **cyberdefense** and **threat intelligence**.

5. Sources

CVE

- https://www.cve.org/CVERecord?id=CVE-2024-31705
- https://www.cve.org/CVERecord?id=CVE-2024-1874
- https://www.cve.org/CVERecord?id=CVE-2024-20295
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-mUx4c5AJ

MISPADU

- https://thehackernews.com/2024/04/mispadu-trojan-targets-europe-thousands.html
- https://blog.morphisec.com/mispadu-infiltration-beyond-latam
- https://thehackernews.com/2024/02/new-mispadu-banking-trojan-exploiting.html

Cyberpsychology: Inspiration from natural mimicry and camouflage

- https://www.aquaportail.com/dictionnaire/definition/2761/mimetisme
- https://sciences-nature.fr/biodiversite/interactions-biologiques/camouflage-et-mimetisme/
- https://fr.wikipedia.org/wiki/Camouflage
- https://inpn.mnhn.fr/espece/cd_nom/54475
- https://lejardindesoiseaux.fr/autres/les-ocelles-des-papillons/
- https://nomadica.jimdofree.com/poissons/poissons-papillons/chelmon-rostratus/
- https://fr.wikipedia.org/wiki/Ocelot
- https://fr.wikipedia.org/wiki/Coloration_disruptive
- https://www.britannica.com/science/disruptive-coloration
- https://www.researchgate.net/figure/An-example-of-disruptive-colouration-juvenile-ocelot-Leopardus-pardalis-in_fig1_308698072
- https://fr.wikipedia.org/wiki/D%C3%A9ception_(militaire)
- https://en.wikipedia.org/wiki/Flower_mantis
- https://en.wikipedia.org/wiki/Hymenopus_coronatus
- https://pixabay.com/fr/photos/nezara-viridula-punaise-verte-3651970/