



Partnership for  
Cyber Security  
Innovation

WEBINAR

# Automated Threat Actor Profiling

🕒 25 MAY 2021, 10:00 CET

HOST

REINDER WOLTHUIS

SPEAKERS



**Richard Kerkdijk**  
TNO



**Lalit Bhakuni**  
ABN AMRO



**Nicole Gervasoni**  
TNO

# Contents

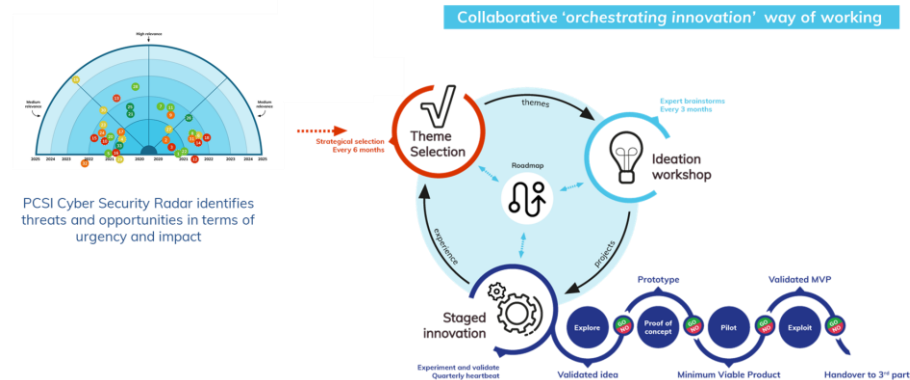
- Introduction to PCSI
- The challenge
- State of the art
- Attributes and taxonomies
- Implementation
- Demonstration
- Take aways
- Q&A

# In this webinar you'll learn more about...

## 1. Threat Actor profiling



## 2. The PCSI programme



# Practical stuff

- Attendees are muted
- If you have questions or remarks, please use the chat; the chat will be moderated
  - Questions will either be addressed directly or in the discussion section at the end of the presentation

# Introduction

# The need for cyber security innovation

“the cybersecurity community is still far from striking the balance between defenders and attackers.”

[...]

“the increased defence levels and expenses cannot successfully reduce levels of cyberthreat exposure.”

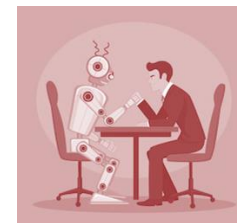
ENISA's Threat Landscape Report, 2017



Increasingly complex and dynamic ICT



Increasing number and complexity of attacks



Attacks get more automated, response is human-centered



Shortage of skilled cybersecurity staff

# Collaborative innovation

Isolated protection

Leaves gaps



lack of innovation | isolated efforts

Shared innovation

Creates bonds



focus on innovation | joint effort

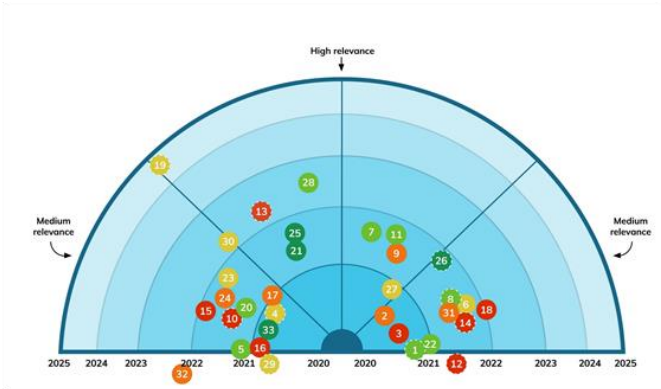
” Alone we are smart. Together we are brilliant.

- Steven W. Anderson

# PCSI: Orchestrating innovation

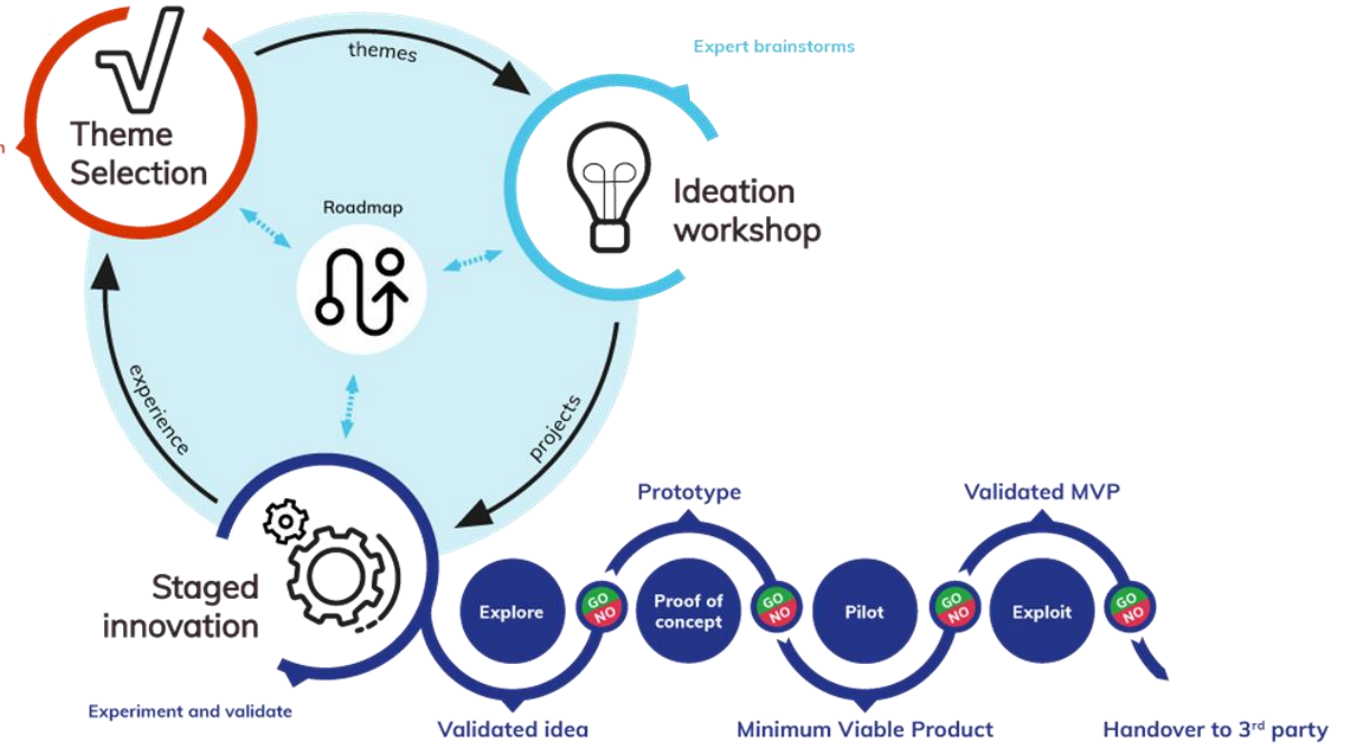
## Collaborative 'orchestrating innovation' way of working

Heartbeat of 4 months



PCSI Cyber Security Radar identifies threats and opportunities in terms of urgency and impact

Strategical selection





# Sample projects

## Crystal ball DDoS detection

- Investigate whether new DDoS attacks can be predicted before they have an actual impact
- Analyse public and private data using AI techniques, to give out a warning (like a tsunami warning) before the attack actually hits



## Security journey

- Investigating whether the 'customer journey methodology' can be used to reduce human induced security incidents
- We use data-driven AI tooling to identify internal processes, define the right steps for each role involved, and determine how to make employees security aware

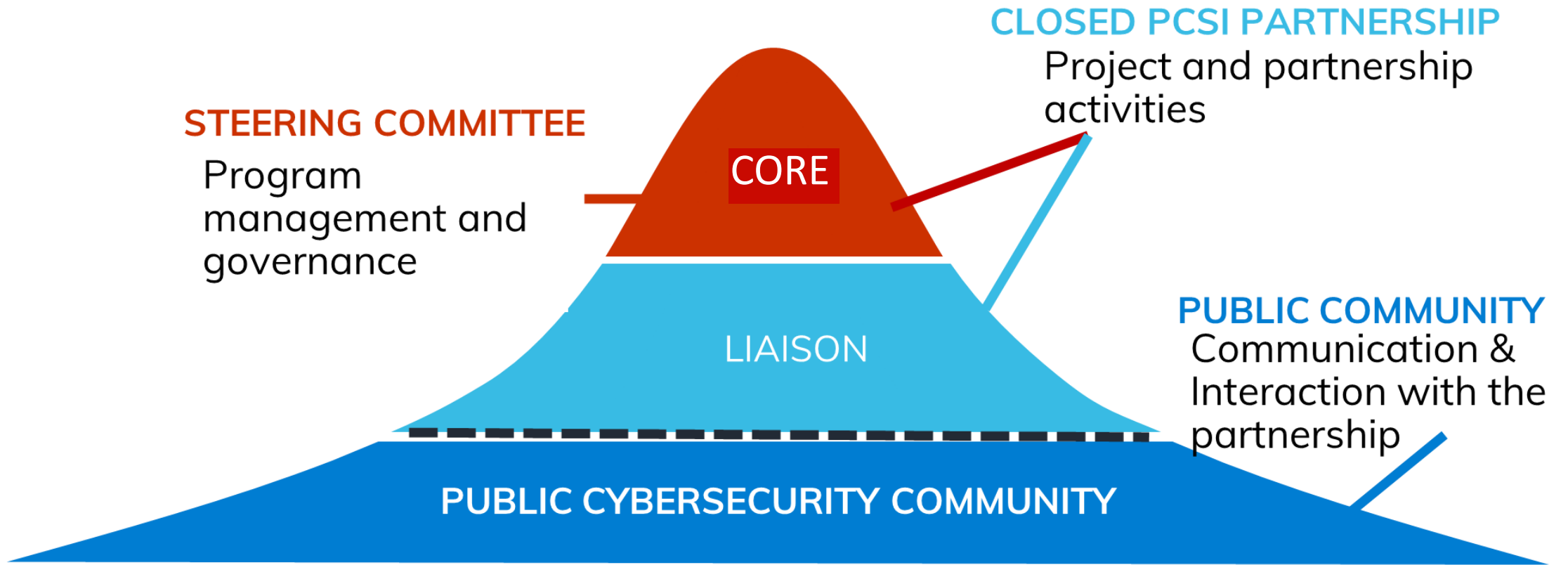


## Collaborative fleet

- Set up 'honey pots' with the specific purpose of tempting attackers to target it, so we can monitor their behavior
- We combine information from a large number of honey pots, resulting in strategic insights that would not be possible for individual organisations



# PCSI Partner model



"To increase the resilience level of Dutch society and participating organisations against tomorrow's cyber threats and vulnerabilities"

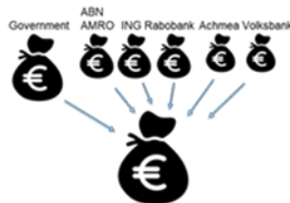
# PCSI predecessor



Shared working

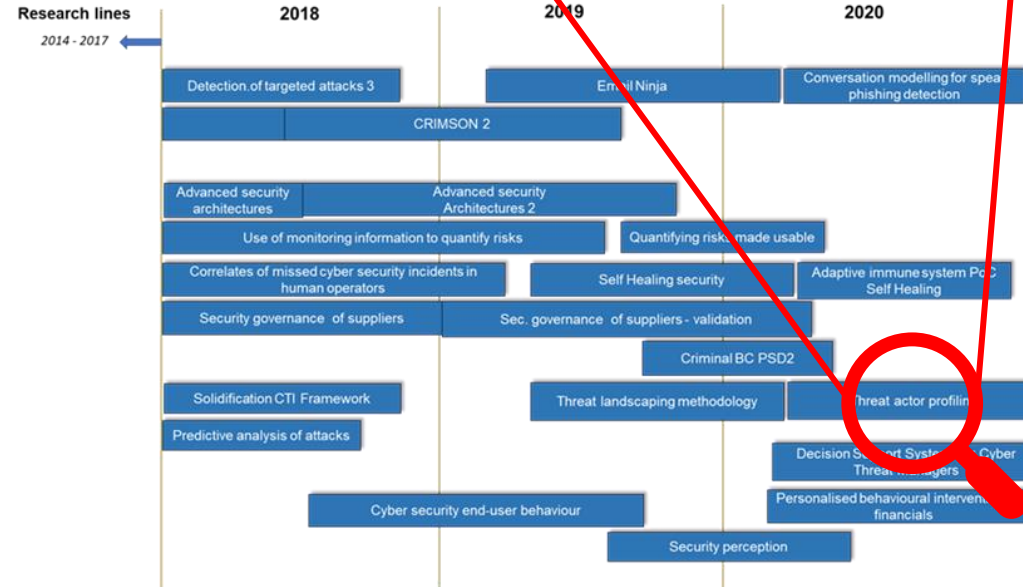


Sharing data



Shared funding

## Threat actor profiling



Direct application of results by partners and increase resilience society by publications, presentations, spin-offs etc.

Shared Research Program cyber security 2014 - 2020 (2020 onwards: PCSI)  
Yearly 1 million euro to innovate on cyber security



<https://www.tno.nl/srpcybersecurity>

# Today's presenters



**Richard Kerkdijk**  
TNO



**Lalit Bhakuni**  
ABN AMRO



**Nicole Gervasoni**  
TNO

[www.pcsi.nl](http://www.pcsi.nl) 

follow us 

# Collecting and processing threat information



to operational security systems (e.g. SIEM, IDS, EDR)

*ingest, enrich, correlate, visualize, export, share...*

threat intel platform



eclectic iq ANOMALI mnemonic OPENCTI MISP Threat Sharing

structured sources

**STIX**  
(machine readable)

unstructured sources

HTML PDF @  
(natural language)



(not exhaustive)

Threat information

- Threat actor names, aliases and affiliations
- Threat actor objectives and known targets
- Historic and ongoing attacker campaigns
- Tools, techniques and procedures (TTP/ MO)
- Indicators of Compromise (IoCs)

# Challenges in processing narrative intel

## Challenges

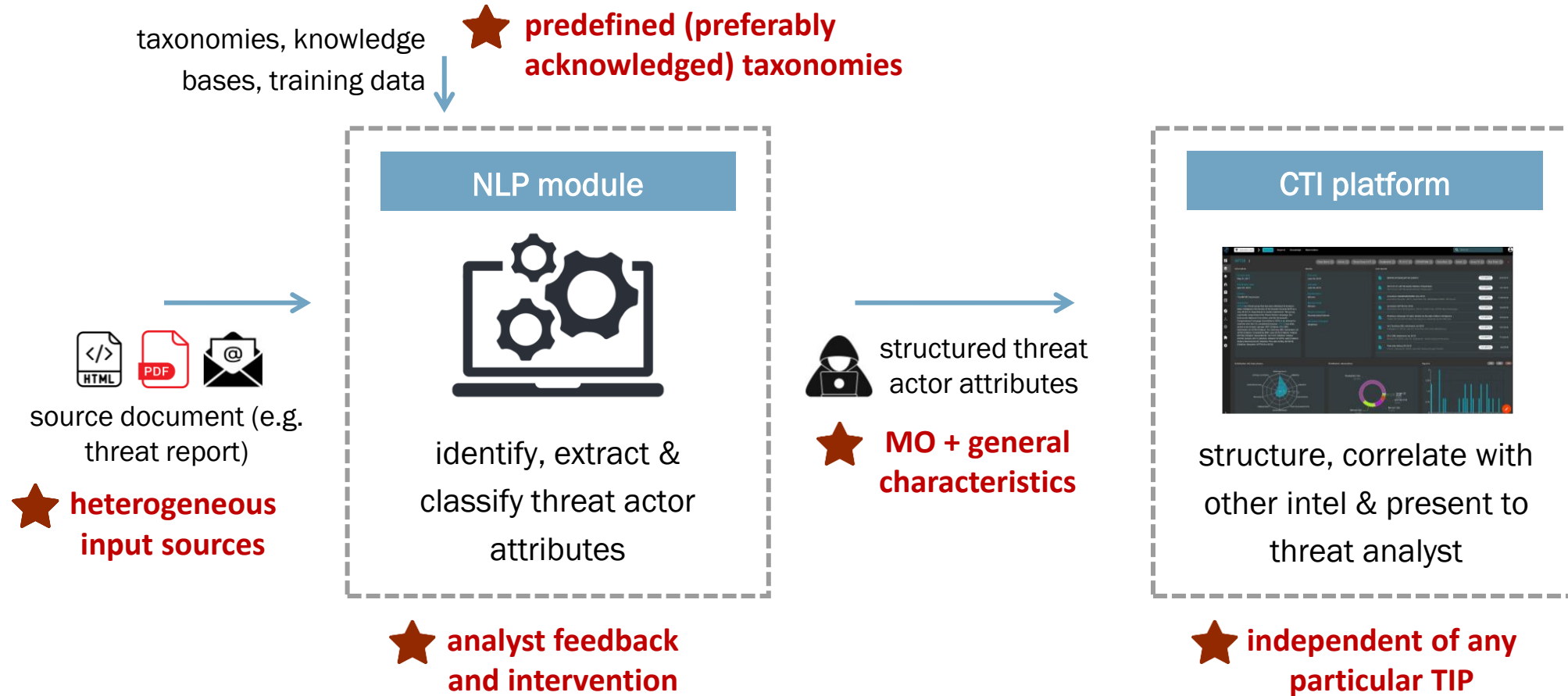
- **Limited time to read and analyze** - Uncountable impressive research reports/blogs by researchers in an unstructured format
- **No industry standard for actor naming convention** - Multiple naming conventions for same threat actor group(s)
- **Analytical capability** – Carving right Tactics, techniques and procedures (TTPs) is not necessarily trivial

## Key Attributes of an **Actionable Insight**



Image Source - Forbes

# Envisaged setup and key requirements



The background features a perspective view of a grid of squares. The grid lines are thin and light blue. Several squares within the grid are filled with a solid, vibrant blue color. The overall color palette is a gradient of light blues and teals, creating a clean, modern, and technical aesthetic.

STATE OF THE ART



# CTR to TT

How to classify unstructured CTR data into ATT&CK Tactics and Techniques?

## Cyber Threat Reports

- Unstructured text
- Several formats: pdf, html, doc

## ATT&CK frameworks classification

- Tactics represent the “why” of an ATT&CK technique or sub-technique  
Tactics are treated as “tags” within ATT&CK where a technique or sub-technique is associated or tagged with one or more tactic categories.
- Several techniques represent “how” an adversary achieves a tactical objective by performing an action.
- Several sub-techniques, describing more specific means by which adversaries achieve tactical goals at a lower level than techniques.

# Natural Language Processing

- Problem: It is difficult to retrieve relevant information from unstructured data.
- NLP is an AI technique that tackles this problem by combining techniques of statistics with machine learning.

# State of the art solutions

TRAM - Threat Report ATT&CK® Mapping

rcATT - reports classification by adversarial tactics and techniques

## Common features

- Train set from ATT&CK database
- Python libraries (scikit + nltk)
- Final human decision on the output
- Every new CTR the algorithm can be retrained

# Tram

By MITRE

CTR webpage → pdf table (on techniques)

## Approach

Multi class logistic regression

## Results

Unknown

The screenshot displays the MITRE ATT&CK Mapper (TRAM) interface. At the top, there's a navigation bar with 'Home', 'About', and 'ATT&CK'. Below it, a progress bar shows the report status: 'NEEDS REVIEW', 'ANALYST REVIEWING', and 'COMPLETE'. The main title is 'Ocean Lotus', with an 'Export PDF' button. The content area contains several paragraphs of text, some highlighted in yellow. The right sidebar shows 'Techniques Found' with a table for 'Exploitation for Client Execution (m)' and buttons for 'Accept' and 'Reject'. Below that, it lists 'Confirmed Techniques' and an 'Add Missing Technique' button. The footer includes the MITRE logo, copyright information, and social media links.

Threat Report ATT&CK Mapper (TRAM)

Home About ATT&CK

Enter New Report

NEEDS REVIEW ANALYST REVIEWING COMPLETE

## Ocean Lotus

Export PDF

ESET researchers detail the latest tricks and techniques OceanLotus uses to deliver its backdoor while staying under the radar This article will first describe how the OceanLotus group (also known as APT32 and APT-C-00) recently used one of the publicly available exploits for CVE-2017-11882, a memory corruption vulnerability present in Microsoft Office software, and how OceanLotus malware achieves persistence on compromised systems without leaving any traces.

Then the article describes how, since the beginning of 2019, the group has been leveraging self-extracting archives to run code. Context Following OceanLotus' activities is taking a tour in the world of deception.

This group is known to lure victims by forging appealing documents to entice potential victims into executing the group's backdoor, and keeps coming up with new ideas to diversify its toolset.

The techniques employed for the decoys range from files with so-called double extensions, self-extracting archives and macro-enabled documents, to reusing known exploits.

On top of that, they are very active and relentlessly continue to raid their favourite victims, South East Asian countries. Summing up the Equation Editor exploit In mid-2018, OceanLotus carried out a campaign using documents abusing the weakness exposed by the CVE-2017-11882 vulnerability.

Techniques Found

Exploitation for Client Execution (m)	Accept	Reject
---------------------------------------	--------	--------

Confirmed Techniques

Add Missing Technique

MITRE

Copyright © 2019-2020, The MITRE Corporation.

MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.

Privacy Policy Terms of Use

@MITREattack

Contact

# rcATT

Text reports → STIX file

## Approach

- TF-IDF weighted bag-of-words + binary Linear SVC
- Post-processing techniques

rcATT is a python tool to predict ATT&CK tactics and techniques from cyber threat reports. Paste your report in the text area so it can be predicted. Tactics and techniques displayed in a darker colored background are predicted as included in the report. The percentage displayed next to the name of the tactic/technique is the likelihood of this tactic/technique of being in the report. If the tactic/technique is indicated as not being in the report, despite the displayed likelihood, it is due to the post-processing in our model. If you disagree with the prediction, you can correct these results and save them to the training set to improve it.

Predict

Woburn, MA – May 7, 2018 – Kaspersky Lab researchers have discovered a new variant of the SynAck ransomware Trojan using the Doppelgänger technique to bypass anti-virus security by hiding in legitimate processes. This is the first time the Doppelgänger technique has been seen in ransomware in the wild. The developers behind SynAck also implement other tricks to evade detection and analysis, obfuscating all malware code prior to sample compilation and exiting if signs suggest it is being launched in a sandbox.

The SynAck ransomware has been known since fall 2017, and in December, it was observed targeting mainly English-speaking users with remote desktop protocol (RDP) brute-force attacks followed by the manual download and installation of malware. The new variant uncovered by Kaspersky Lab researchers implements a far more sophisticated approach, using the Process Doppelgänger technique to evade detection.

Reported in December 2017, Process Doppelgänger involves a fileless code injection that takes advantage of a built-in Windows function and an undocumented implementation of the Windows process loader. By manipulating how Windows handles file transactions, attackers can pass off malicious actions as harmless, legitimate processes, even if they are using known malicious code. Doppelgänger leaves no traceable evidence behind, making this type of intrusion extremely difficult to detect. This is the first time ransomware has been observed using this technique in-the-wild.

Other noteworthy features of the new variant of SynAck include:

The Trojan obfuscates its executable code prior to compilation, rather than packing it like most other ransomware, making it harder for researchers to reverse engineer and analyze the malicious code.

It also obscures the links to the necessary API function, and stores hashes to strings rather than the actual strings.

Upon installation, the Trojan reviews the directory its executable is started from, and if it spots an attempt to launch it from an 'incorrect' directory – such as a potential automated sandbox – it exits.

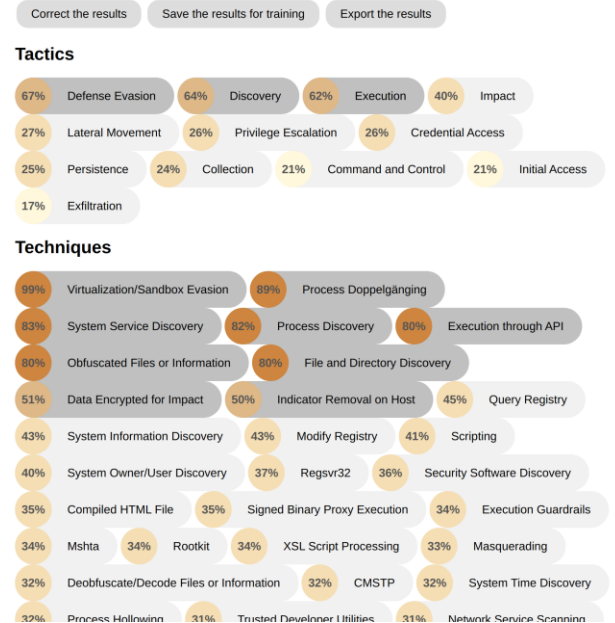
The malware also exits without execution if the victim PC has a keyboard set to Cyrillic script.

Before encrypting files on a victim device, SynAck checks the hashes of all running processes and services against its own hard coded list. If it finds a match, it tries to kill the process. Processes blocked in this way include virtual machines, office applications, script interpreters, database applications, backup systems, gaming applications and more - possibly to make it easier to seize valuable files which might otherwise be tied up into the running processes.

Researchers believe attacks using this new variant of SynAck are highly targeted. To date, they have observed a limited number of attacks in the U.S., Kuwait, Germany and Iran, with ransom demands of \$3,000.

"The race between attackers and defenders in cyberspace is a never-ending one. The ability of the Process Doppelgänger technique to sneak malware past the latest security measures represents a significant threat; one that has, not surprisingly, quickly been seized upon by attackers," said Anton Ivanov, lead malware analyst, Kaspersky Lab. "Our research shows how the relatively low profile, targeted ransomware SynAck used the technique to upgrade its stealth and infection capability. Fortunately, the detection logic for this ransomware was implemented before it appeared in the wild."

Kaspersky Lab detects this variant of the SynAck ransomware as:



## Results

Possible macro-averaged  $F_{0.5}=80\%$  on tactics prediction and  $F_{0.5}>27.5\%$  on techniques prediction

$$F_{0.5}(y_t, y_p) = 1.25 \cdot \frac{Pr(y_t, y_p) \cdot Re(y_t, y_p)}{(0.25 \cdot Pr(y_t, y_p)) + Re(y_t, y_p)}$$

The background features a perspective view of a grid of squares, with some squares highlighted in a light blue color. On the left side, there are several overlapping, semi-transparent blue rectangular frames, creating a sense of depth and structure. The overall color palette is dominated by various shades of blue and cyan, with a slight gradient from top to bottom.

# ATTRIBUTES AND TAXONOMIES

# Attributes and Taxonomies

**ATT&CK**<sup>®</sup> ⇒ Tactics and techniques taxonomy

 **ThaiCERT**  
Thailand Computer Emergency Response Team  
a member of ETDA ⇒ Actor name and motivation

# Tactics and techniques



	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 34 techniques	Credential Access 14 techniques	Discovery 23 techniques	Lateral Movement 9 techniques	Collection 16 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Drive-by Compromise	Command and Scripting Interpreter (6)	Account Manipulation (3)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Clipboard Data	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Data from Cloud Storage Object	Data Encoding (2)	Data Manipulation (3)	Data Manipulation (3)
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Create or Modify System Process (4)	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Remote Services (6)	Data from Information Repositories (2)	Data Obfuscation (3)	Defacement (2)	Defacement (2)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Event Triggered Execution (15)	Execution Guardrails	Man-in-the-Middle (1)	Domain Trust Discovery	Replication Through Removable Media	Data from Local System	Dynamic Resolution (3)	Disk Wipe (2)	Disk Wipe (2)
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (2)	File and Directory Discovery	Software Deployment Tools	Data from Network Shared Drive	Encrypted Channel (2)	Endpoint Denial of Service (4)	Endpoint Denial of Service (4)
Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	Group Policy Modification	File and Directory Permissions Modification (2)	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Removable Media	Fallback Channels	Firmware Corruption	Firmware Corruption
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (10)	Hijack Execution Flow (10)	Group Policy Modification	OS Credential Dumping (8)	Network Service Scanning	Use Alternate Authentication Material (4)	Data from Staged (2)	Ingress Tool Transfer	Inhibit System Recovery	Inhibit System Recovery
	Windows Management Instrumentation	Hijack Execution Flow (10)	Process Injection (11)	Process Injection (11)	Hide Artifacts (4)	Steal Application Access Token	Network Share Discovery		Email Collection (3)	Multi-Stage Channels	Network Denial of Service (2)	Network Denial of Service (2)
		Implant Container Image	Scheduled Task/Job (5)	Scheduled Task/Job (5)	Hijack Execution Flow (10)	Steal or Forge Kerberos Tickets (3)	Network Sniffing		Input Capture (4)	Non-Application Layer Protocol	Resource Hijacking	Resource Hijacking
		Office Application Startup (6)	Valid Accounts (4)	Valid Accounts (4)	Indicator Removal on Host (6)	Steal Web Session Cookie	Password Policy Discovery		Man in the Browser	Non-Standard Port	Service Stop	Service Stop
		Pre-OS Boot (3)			Indirect Command Execution	Two-Factor Authentication Interception	Peripheral Device Discovery		Man-in-the-Middle (1)	Protocol Tunneling	System Shutdown/Reboot	System Shutdown/Reboot
		Scheduled Task/Job (5)			Masquerading (6)	Unsecured Credentials (6)	Process Discovery		Screen Capture	Remote Access Software		
		Server Software Component (3)			Modify Authentication Process (2)		Query Registry		Video Capture	Traffic Signaling (1)		
		Traffic Signaling (1)			Modify Registry		Remote System Discovery			Web Service (3)		
		Valid Accounts (4)			Obfuscated Files or Information (5)		Software Discovery (1)					
					Pre-OS Boot (3)		System Information Discovery					
					Process Injection (11)		System Network Configuration Discovery					
					Revert Cloud Instance		System Network Connections Discovery					
					Rogue Domain Controller		System Owner/User Discovery					
					Rootkit		System Service Discovery					
					Signed Binary Execution (10)		System Time Discovery					
					Signed Script Proxy Execution (1)							
					Subvert Trust Controls (4)							
					Template Injection							
					Traffic Signaling (1)							
					Trusted Developer Utilities Proxy Execution (1)							
					Unused/Unsupported Cloud Regions							
					Use Alternate Authentication Material (4)							
					Valid Accounts (4)							
					Virtualization/Sandbox							



# Actor name and motivation



## Motivation

- Information theft and espionage
- Financial crime
- Financial gain
- Sabotage and destruction

### ⇒ APT group: APT 29, Cozy Bear, The Dukes

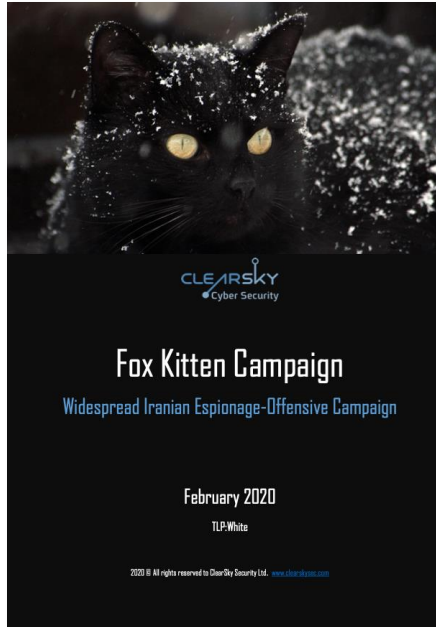
Names	APT 29 ( <i>Mandiant</i> ) Cozy Bear ( <i>CrowdStrike</i> ) The Dukes ( <i>F-Secure</i> ) Group 100 ( <i>Talos</i> ) Yttrium ( <i>Microsoft</i> ) Iron Hemlock ( <i>SecureWorks</i> ) Minidionis ( <i>Palo Alto</i> ) CloudLook ( <i>Kaspersky</i> ) ATK 7 ( <i>Thales</i> ) ITG11 ( <i>IBM</i> ) Grizzly Steppe ( <i>US Government</i> ) together with <i>Sofacy, APT 28, Fancy Bear, Sednit</i>
Country	 Russia
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2008
Description	<p>(<i>F-Secure</i>) The Dukes are a well-resourced, highly dedicated and organized cyberespionage group that we believe has been working for the Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making.</p> <p>The Dukes primarily target Western governments and related organizations, such as government ministries and agencies, political think tanks, and governmental subcontractors. Their targets have also included the governments of members of the Commonwealth of Independent States; Asian, African, and Middle Eastern governments; organizations associated with Chechen extremism; and Russian speakers engaged in the illicit trade of controlled substances and drugs.</p> <p>The Dukes are known to employ a vast arsenal of malware toolsets, which we identify as MiniDuke, CosmicDuke, OnionDuke, CozyDuke, CloudDuke, SeaDuke, HammerDuke, PinchDuke, and GeminiDuke. In recent years, the Dukes have engaged in apparently biannual large-scale spear-phishing campaigns against hundreds or even thousands of recipients associated with governmental institutions and affiliated organizations.</p>

The background features a perspective view of a grid of squares. The grid lines are thin and light blue. Several squares within the grid are filled with a solid, medium blue color. The overall color palette is a gradient from light blue on the left to a pale yellow-green on the right. The word 'IMPLEMENTATION' is centered horizontally and vertically in a dark blue, sans-serif font.

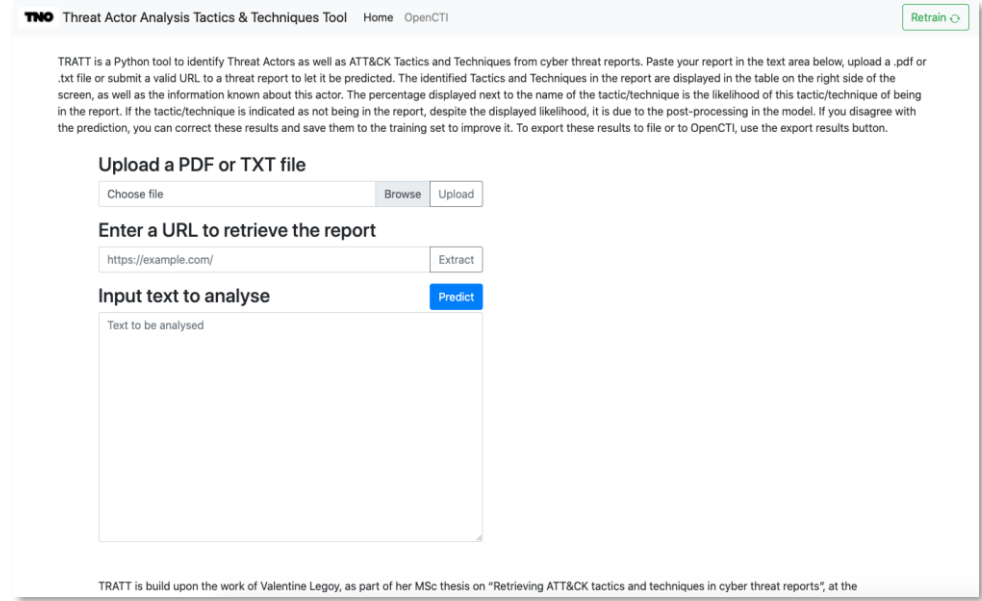
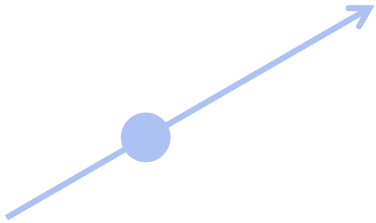
# IMPLEMENTATION

# Final analyst flow

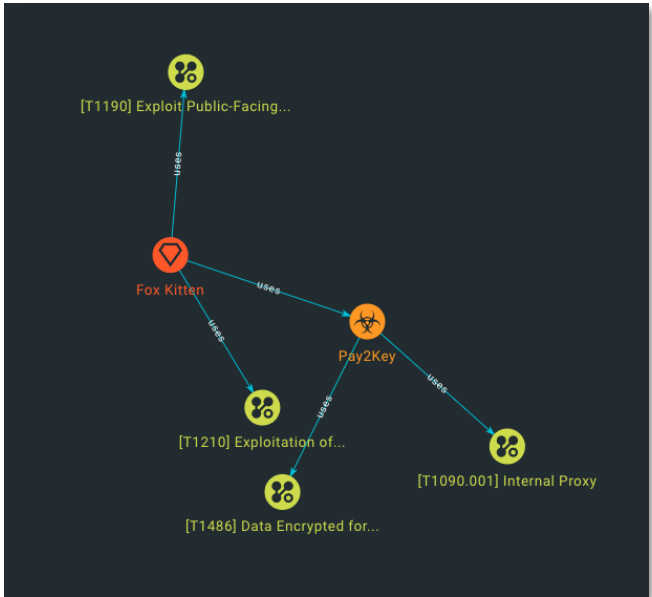
It's **ATRAPP**



Threat report



ATRAPP: Automated Threat Report ATT&CK maPPer



OpenCTI

# OpenCTI

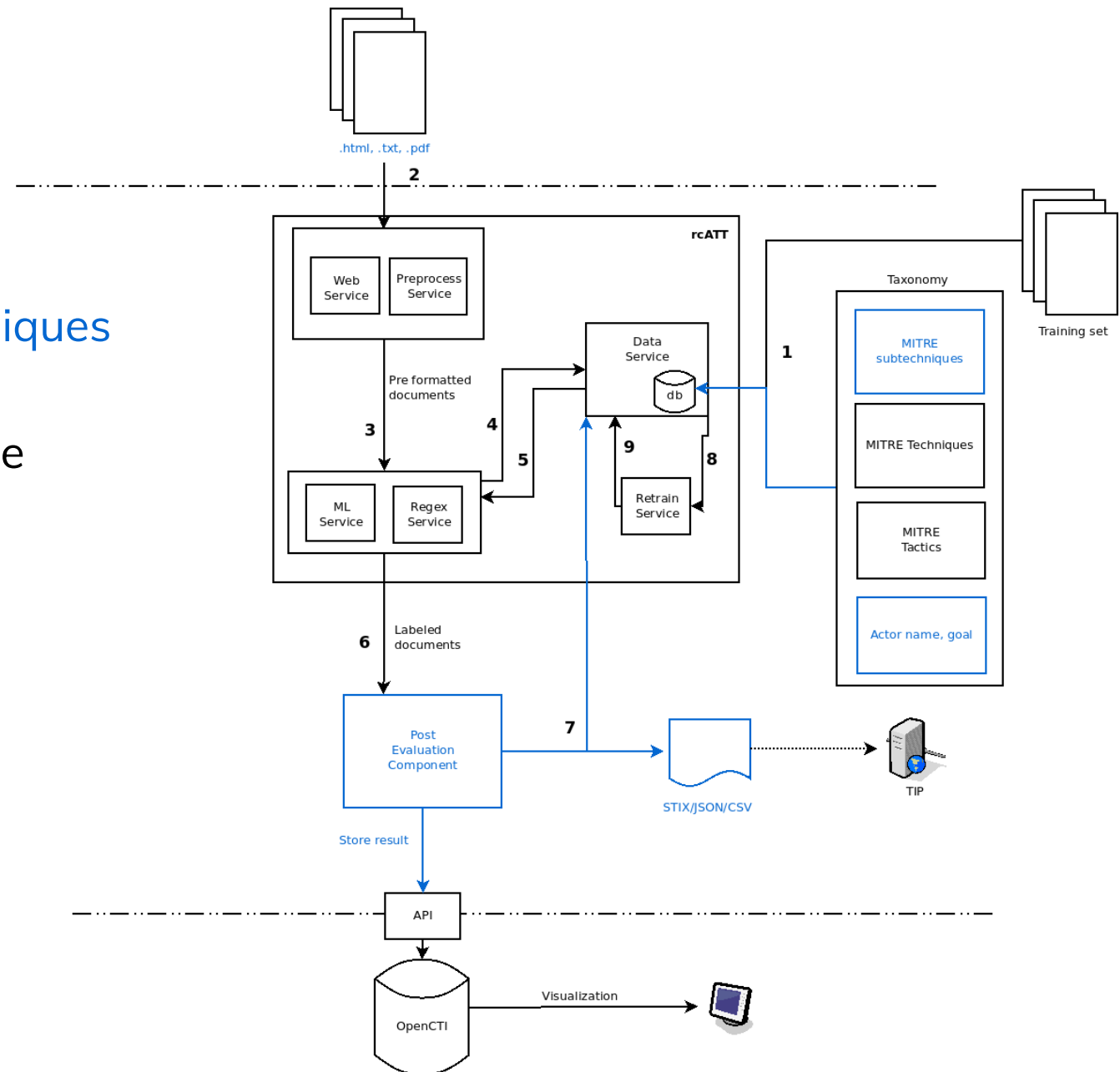
We chose to adopt OpenCTI as our data enrichment platform due to its intuitiveness and to increasing interest that it is gaining from our financial partners.

The screenshot displays the OpenCTI interface for the APT28 intrusion set. The top navigation bar includes 'Intrusion sets', 'Overview', 'Knowledge', 'Reports', 'Indicators', 'Files', and 'History'. The main content area is divided into three sections: 'INFORMATION', 'DETAILS', and 'LAST REPORTS ABOUT THE ENTITY'. The 'INFORMATION' section shows the creation date (May 31, 2017), modification date (October 11, 2019), and author (THE MITRE CORPORATION). The 'DETAILS' section provides a description of APT28 as a threat group attributed to Russia's Main Intelligence Directorate, along with metadata like 'First seen' and 'Last seen' dates. The 'LAST REPORTS ABOUT THE ENTITY' section lists several reports, including 'Phishing attacks from APT28 in 2019' and 'US firm says Russia hacked company at heart of Trump impeachment'. A sidebar on the left contains navigation icons, and a bottom section shows a note about a new campaign by Samuel Hassine.

The screenshot displays the OpenCTI interface for the APT28 intrusion set, focusing on the 'Knowledge' section. The top navigation bar is similar to the previous screenshot. The main content area shows a list of knowledge items related to APT28, such as 'establish-&-maintain-infrastructure', 'T1328 - Buy domain name', 'build-capabilities', 'T1346 - Obtain/re-use payloads', 'initial-access', 'T1192 - Spearphishing Link', 'T1193 - Spearphishing Attachment', 'T1199 - Trusted Relationship', 'execution', 'T1059 - Command-Line Interface', and 'T1085 - Rundll32'. Each item includes a brief description and a 'Copyright' status. A sidebar on the right provides an overview of the knowledge graph, including sections for 'Overview', 'Attribution', 'Victimology', 'Campaigns', 'Incidents', 'Malwares', 'Techniques', 'Tools', and 'Vulnerabilities'. A search bar is visible at the top of the knowledge list.

# Implementation

- 1 Feed initial training set + subtechniques and actors info
- 2 - 3 extract text from [html](#), [pdf](#), [docx](#) file
- 4 - 5 techniques, [subtechniques](#), [groups](#) prediction through ML + regex algorithms
- 6 feed TRAM labelled output to PEC
- 7 store new labelled report in db
- 8 - 9 use new report to retrain model



# Changelog

What has been done?

## FUNCTIONALITIES

ATRAPP now offers a lot more functionalities to the user. We made it possible to easily interact with the application to get the most out of it and integrated it with OpenCTI.

- › Dockerized application
- › URL submission possible
- › Change identified actor
- › Easily change incorrect results
- › Smooth integration with OpenCTI

## TEXT PROCESSING

We examined the possibility to identify ATT&CK sub techniques and made it possible in the future. We added actor name extraction functionalities.

- › Actor name, motivation and country of origin are extracted
- › Submit .pdf or .txt files
- › Output is now a STIX2 bundle
- › Share data to OpenCTI

## USER INTERFACE

A complete overhaul of the design of the application has been finished. A clean user interface with recognizable buttons and text make it easy for the user to navigate.

- › Brand new UI
- › Actor country flags added
- › Feedback on clicks and status
- › Required input fields prevent errors

The background features a 3D grid of squares, some light blue and some white, receding into the distance. On the left side, there is a blue wireframe box that appears to be a container or a frame. The overall color palette is dominated by various shades of blue and cyan, with a slight gradient from light blue on the left to a slightly darker blue on the right.

DEMO

The background features a perspective view of a grid of squares. The grid lines are thin and light blue. Several squares within the grid are filled with a solid, medium blue color. The overall color palette is a gradient of light blues and greens, creating a clean, modern, and technical aesthetic.

TAKE  
AWAYS



# Some take aways



- It is feasible to **automatically extract essential adversary attributes** from narrative threat reports and feed these into a threat intelligence platform in a common, structured form
- The demonstrated setup seems **promising as a support tool for CTI practitioners** that automates much of the bulk processing and lets them focus their effort on selected reports of interest
- To realise the full potential of the envisaged support solution, its **accuracy will need to be improved** through more (and better) training data and processing of analyst feedback (corrections) in operational use



We intend to make the solution available as **open source** and welcome your contribution to its further development!  
*(webinar registrants will be informed when software is released)*

Partnership for Cyber Security Innovation is a collaboration of



ING 



ABN·AMRO

TNO

achmea 

de volksbank

[www.pcsi.nl](http://www.pcsi.nl) 

follow us 

Partnership for Cyber Security Innovation is a collaboration of



ING 



ABN·AMRO

TNO

achmea 

de volksbank

[www.pcsi.nl](http://www.pcsi.nl) 

follow us 