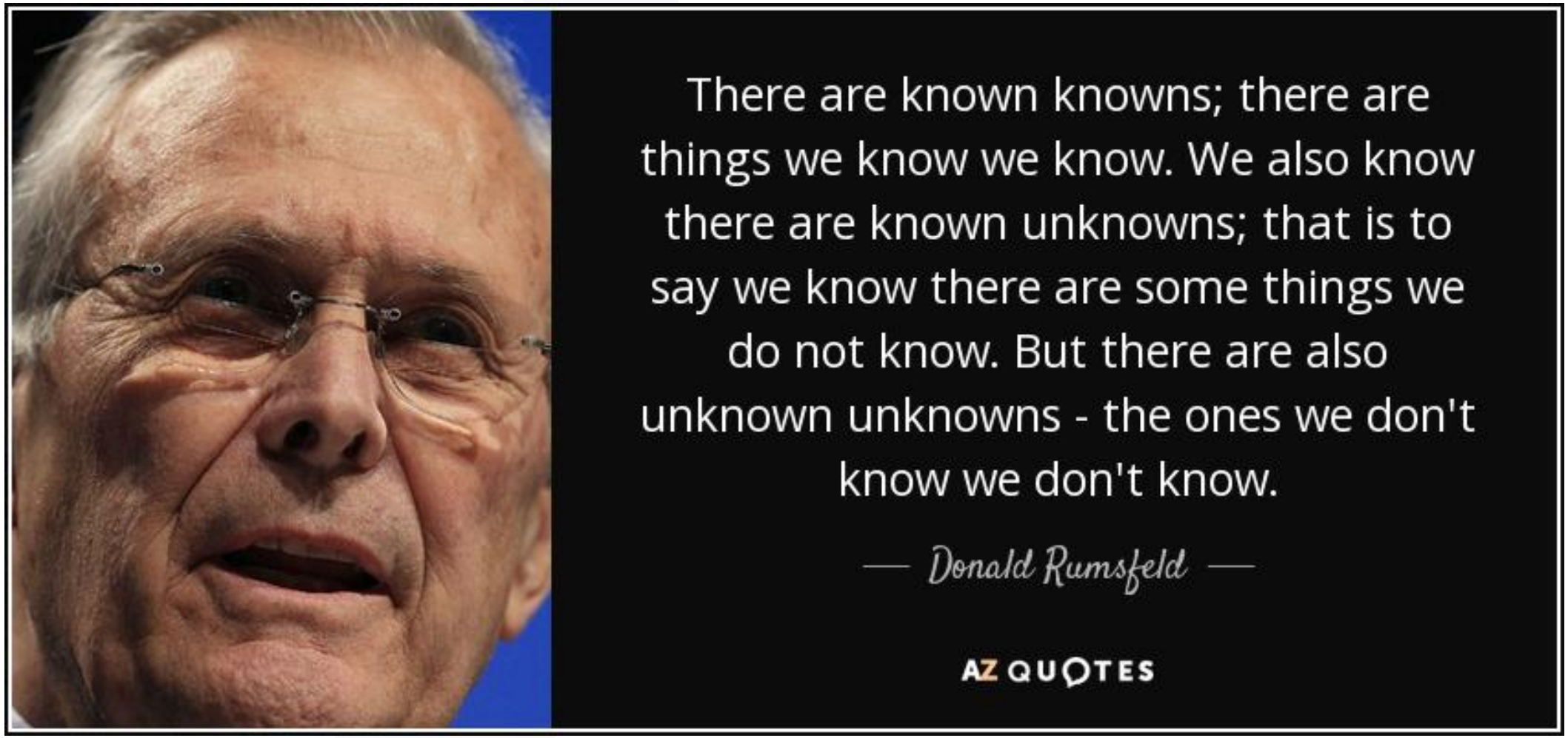
Smartes Cyber-Risikomanagement mit Threat Intelligence

Stephan Halbmeier
Product Specialist | Outpost24

Outpost24


There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns - the ones we don't know we don't know.
— Donald Rumsfeld —
AZ QUOTES

DIE SUCHE NACH DER NADEL IM HEUHAUFEN

Known Knowns

You have all possible details about an event

Known Unknows

You know that an event will happen but you don‘t know when or its magintude

Unknown Kowns

A third party has all details about an event that happened but you don‘t

Unknown Unknowns

An event where no one had an idea this could happen

Outpost24

CREDENTIALS

[redacted].com

← Back to list →

Mark as incident | Mark as favorite | Mark as unread | Delete threat ✓ | Comments · 0

RATING	★★★☆☆	CREDENTIAL TYPE	Botnet
USERNAME	[redacted]	CLASSIFICATION	UNCLASSIFIED
PASSWORD	[redacted]	IS EMAIL	−
BOTNET TYPE	RACCOONSTEALER	UPDATED AT	25/8/2023 18:24h
AFFECTED URL	https://login[redacted]/ad...	REPORTED AT	4/7/2023 11:45h
LABELS	Botnet Credentials, Clear Password, First Data Load, [redacted], POC Corp_BotCred	BREACHED AT	13/6/2023 00:51h

Report Email

Outpost24

DARK_WEB

[redacted]

← Back to list →

Mark as incident | Mark as favorite | Mark as unread | Delete threat ✓ | Follow up | Comments · 0

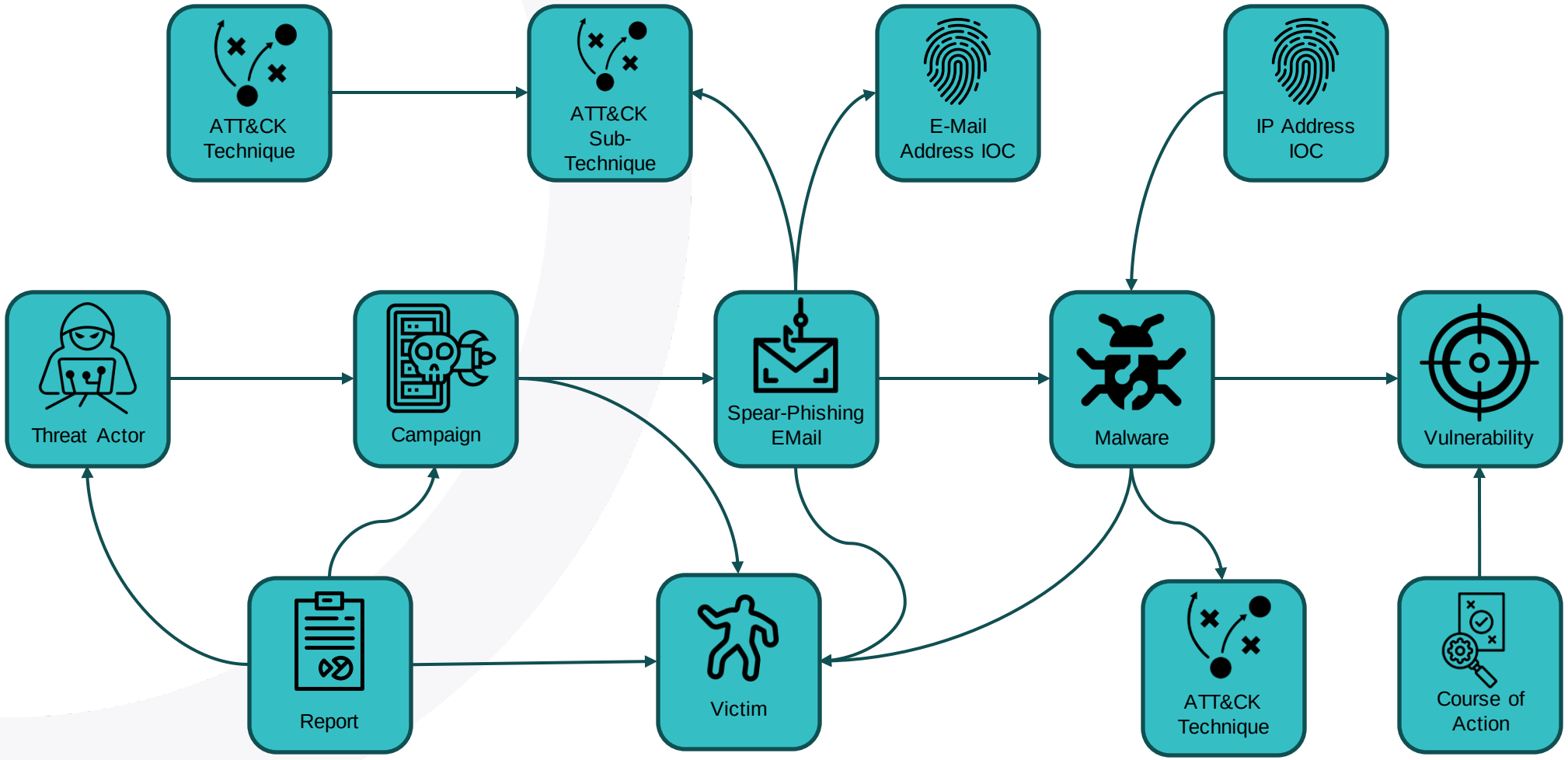
RATING	★★★★☆	**SEARCH WORDS**	[redacted]
URL	https://genesis.m...?id=[redacted]	**CONTENT TYPE**	text/html; charset=utf-8
COUNTRY	NL	**DOMAIN TYPE**	Other
LANGUAGE	English	**REPORTED AT**	25/8/2023 18:30h
LABELS	DeepWebSearch, POC Corp, POC Corp_Domain, POC Custom_Port, POC Login_4Sale, POC URL_List, [redacted], TARGETED ATTACK	**UPDATED AT**	25/8/2023 18:30h
RELEVANCE	INFORMATIVE		
ORIGIN	DeepWebSearch		

Report Email

oginsLoginData edgeno2022-08-30 17:22:222022-08-31 06:57:25[redacted]https://[redacted]/"Login": Available After Purchase"Password": Available After Purchase Saved LoginsLo
LoginsLoginData edgeno2022-08-30 17:22:222022-08-31 06:57:25

Outpost24

STRUCTURED INTELLIGENCE - ATT&CK MIT STIX



Outpost24

TOOLS

RedLine

Export ▾ Back to li

FIRST SEEN	18/02/2020	TARGETED PLATFORMS	Windows
LAST SEEN	15/09/2022	VERSION	-
TLP			

Description | Malware(+100k) | Threat Actors(9) | Campaigns(0) | CVE(0) | Signatures(9)

Description ▾

RedLine is an extremely popular stealer written in C# and discovered in March 2020.

Initially, it implemented SOAP (Simple Object Access Protocol) over HTTP for its communications with the C&C. However, more recent samples implement SOAP data over Net.TCP Port Sharing Protocol instead. This update makes it more difficult to identify and understand communication data being exchanged between a victim and the malware's C2 servers.

Being a stealer, its main goal is to export all sorts of personal information, such as credentials, cryptocurrency wallets, and financial data, and upload it to the malware's c2 infrastructure. On many occasions, RedLine payload is delivered along with a cryptocurrency miner to be deployed on the victim's machine, especially in those campaigns that had gamers as the preferred target, since they are often related to powerful GPUs, which makes them the perfect type of machine for cryptomining.

It has been associated with a wide variety of distribution methods, with phishing campaigns as the most prominent one. Threat actors have been seen using current worldwide lures such as COVID-19. Precisely in a phishing campaign related to this theme, a new variant of RedLine was observed in January 2022.

In October 2021, Google's Threat Analysis Group announced that RedLine had been used in phishing attacks against YouTube creators to obtain credentials and browser cookies to hijack their accounts in pass-the-cookie attacks. Once compromised their channels were sold on underground forums or used in cryptocurrency scam schemes.

From mid-2021 onwards, YouTube has also been used as a distribution method for RedLine, among other stealing families, in a process that could be resumed as follows. Firstly, the threat actor compromises a Google/YouTube account. Once compromised, the threat actor creates different channels or directly publishes videos on them. In the description of the uploaded videos, mostly ones that advertise cheats and cracks and provide instructions on hacking popular games and software, threat actors usually include a malicious link related to the theme of the video that will end with the distribution of RedLine.

By September 2022, Securelist researchers observed an improvement in the use of YouTube as a method of propagation, after seeing RedLine self-distributing itself through it. On this occasion, the link included in the description of the videos downloaded a self-extracting RAR archive that contained among the RedLine payload and the miner, a third executable in charge of running some batch files. These batch files, in turn, run three other malicious files responsible for the RAR's self-distribution. The first one is a password stealer whose function is to extract cookies from browsers and store them in a separate file without sending the stolen data anywhere. It is through cookies that the bundle gains access to the infected user's YouTube account, where it uploads the video. The second one is a regular loader whose purpose is to download videos from a GitHub repository for uploading to YouTube, as well as files with the description text and links to the malicious archive. Finally, the third executable uploads the video previously downloaded to YouTube. When the video is successfully uploaded to YouTube, a message is sent to Discord with a link to the uploaded video.

OUTPOST24 CYBER THREAT INTELLIGENCE ÜBERSICHT

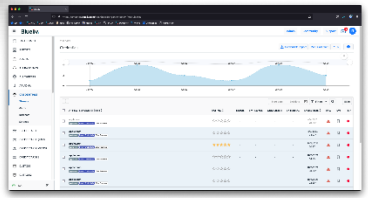
INFORMATION GATHERING

- Internet
- Deep Web
- Dark Web
- Proprietary intelligence
- Labs Team
- Blueliv Community
- Experts
- Organizations
- Malware sharing
- Third Parties
- Partners
- Public sources
- Web Crawlers
- Malware Reversal
- Sinkholing
- Honeypots

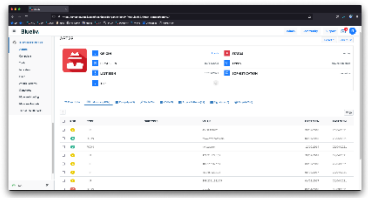
2 PROCESSING

- Enriched data
- Threat Actor Expertise
- Machine Learning

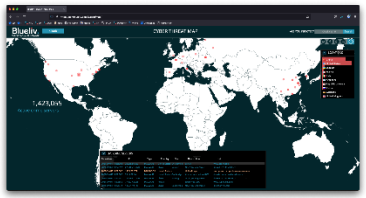
3 INFORMATION DELIVERY + REMEDIATION



Threat Compass



Threat Context



MRTI Data Feed

Outpost24

Vielen Dank für Ihre Aufmerksamkeit

Für weitere Fragen zum Thema: https://outpost24.com/de/contact

Produkt-Demo: https://outpost24.com/products/cyber-threat-intelligence#demo

E-Mail: stephan.halbmeier@outpost24.com

LinkedIn: https://www.linkedin.com/in/stephanhalbmeier

Outpost24