

A person wearing a dark hoodie is centered in the foreground, looking directly at the camera. Behind them are several computer monitors displaying various data, including binary code (0s and 1s), network diagrams, and security-related icons like padlocks and shields. The overall color scheme is dark with blue and red highlights. At the bottom of the image, there is a horizontal bar with a blue section on the left and a red section on the right.

AI w rękach Blue Team'u

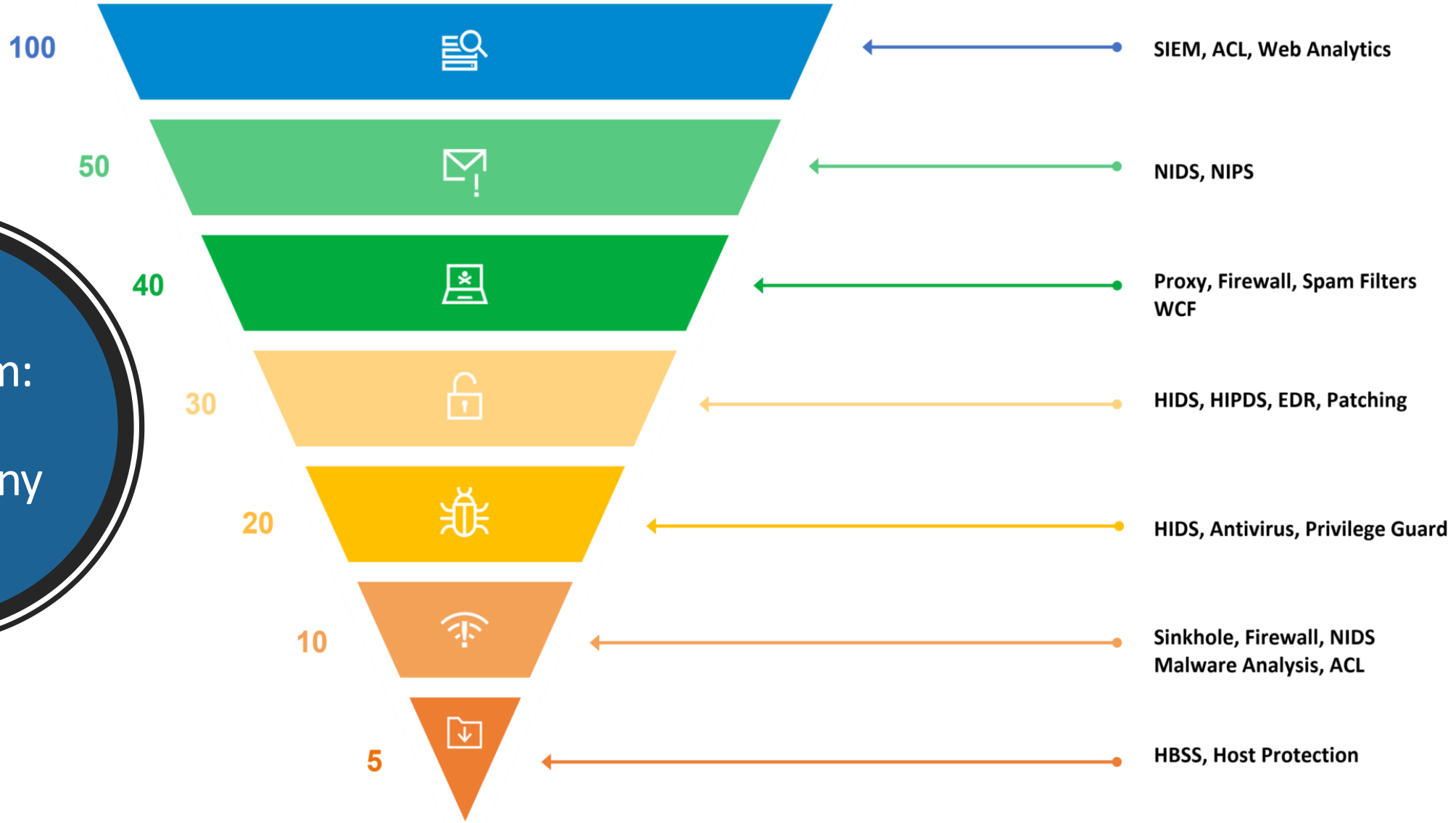
# Joanna Wziętek-Ładosz



- Mgr inż. informatyk
- Obecnie **Senior Security Engineer** w Tenable
- Ponad **15 lat doświadczenia** w cyberbezpieczeństwie
- Roczny certyfikowany program podyplomowy na *Massachusetts Institute of Technology* z cyberbezpieczeństwa
- Członkini ISSA Polska, ISSA International, **Polskiego Towarzystwa Informatycznego (PTI)** i Sekcji AWSI
- Autorka podcastów Polskiego Radia **“Cyberbezpieczni”** a obecnie podcastu **„Cyberbezpieczeństwo po ludzku”**
- W social mediach **„@Pani od cyber”**

<https://www.linkedin.com/in/joanna-wziatek/>

Blue Team:  
zespół  
defensywny

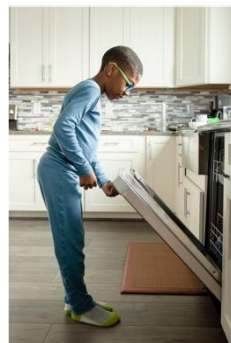


# Metody uczenia maszynowego w cyberbezpieczeństwie



## SUPERVISED MACHINE LEARNING (nadzorowane)

- wykrywanie złośliwego oprogramowania,
- wykrywanie spamu,
- wykrywanie anomalii,
- risk scoring in cybersecurity



## UNSUPERVISED MACHINE LEARNING (nienadzorowane)

- wykrywanie anomalii,
- Ataki zero-day oparte na IoT,
- klasyfikacja podmiotów



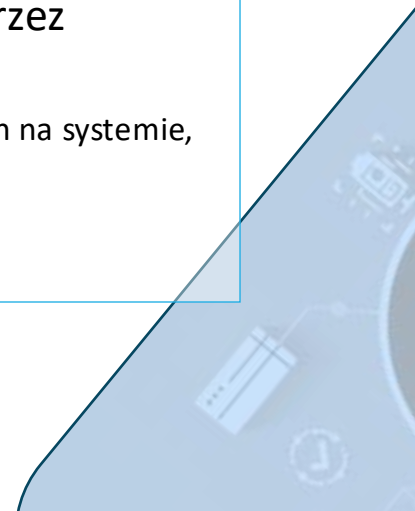
## SEMI-SUPERVISED LEARNING (półnadzorowane)

- Wykrywanie włamań do sieci
- ataki DDoS,
- Ataki złośliwego oprogramowania



## REINFORCEMENT LEARNING (przez wzmacnianie)

- przeprowadzanie testów penetracyjnych na systemie,
- ocena ryzyka
- Nietypowe zachowanie



# Typy algorytmów i ich wykorzystanie

## REGRESSION

- wykrywanie oszustw,
- identyfikacja złośliwego oprogramowania,
- wykrywanie ataków,

## PROBABILISTIC

- wykrywanie włamań,
- wykrywanie złośliwego oprogramowania,
- filtrowanie spamu

## DISTANCE BASED LEARNING

- wykrywanie złośliwego oprogramowania,
- anomalie w ruchu sieciowym,
- wykrywanie nadużyć,
- klasyfikacja DNS

## DECISION TREES

- wykrywanie i kategoryzacja złośliwego oprogramowania,
- wykrywanie włamań,
- rozpoznawanie spamu,
- ocena luk w zabezpieczeniach

## Support Vector Machines (SVM)

- wykrywanie włamań,
- wykrywanie złośliwego oprogramowania,
- naruszenie bezpieczeństwa(ataki)
- identyfikacja i wykrywanie oszustw,
- spam

Jak AI pomaga  
tworzyć narzędzia do  
cyberobrony?



# Reverse engineering

odtajnione i udostępnione  
opinii publicznej w 2019 r.

# LLM do pomocy !

```
#####
# Script Configuration
#####
MODEL = "gpt-3.5-turbo" # Choose which large language model we query -- gpt-4 and claude-v1.2 also supported
TEMPERATURE = 0.19 # Set higher for more adventurous comments, lower for more conservative
TIMEOUT = 600 # How many seconds should we wait for a response from OpenAI?
MAXTOKENS = 512 # The maximum number of tokens to request from OpenAI
C3POSAY = True # True if you want the cute C-3PO ASCII art, False otherwise
LANGUAGE = "English" # This can also be used as a style parameter.
EXTRA = "" # Extra text appended to the prompt.
LOGLEVEL = INFO # Adjust for more or less line noise in the console.
COMMENTWIDTH = 80 # How wide the comment, inside the little speech balloon, should be.
G3POASCII = r"""
    /~\
    |oo )
    _\=/_
   /      \
  //|. \ \
 || \  / ||
 || \ / ||
 # \_ / #
  | | |
  | | |
  [] []
  | | |
  /_ \_ \_ \
#####
```

- [G-3PO: A Protocol Droid for Ghidra](#)

- G-3PO narzędzie, do kontynuowania pracy dekompiłatora Ghidry, dodając kolejną warstwę automatyzacji do procesu inżynierii wstecznej.
- G-3PO przesyła zdekompilowany kod C funkcji do modelu językowego (obecnie obsługuje modele zarówno z OpenAI, jak i Anthropic) i żąda wyjaśnienia, co robi funkcja, wraz z sugestiami dotyczącymi opisowych nazw zmiennych.
- G-3PO może następnie automatycznie dodać te nazwy i komentarze do listy dekompilacji Ghidra



File Edit Analysis Graph Navigation Search Select Tools Window Help

Listing: fw\_1@43face00

4520a9bc	01 30 50 e0	subs	r3,src,dest
4520a9c0	03 00 52 21	cmpcs	size,r3
4520a9c4	b9 8a e4 9a	bis	copyData
4520a9c8	03 00 52 e3	cmp	size,#0x3
4520a9cc	02 00 80 e0	add	src,src,size
4520a9d0	02 10 81 e0	add	dest,dest,size
4520a9d4	25 00 00 9a	bis	LAB_4520aa70
4520a9d8	03 00 10 e3	tst	src,#0x3

LAB\_4520a9dc

4520a9dc	01 30 71 15	ldrbne	r3,[dest,#-0x1]!
4520a9e0	01 20 42 12	subne	size,size,#0x1
4520a9e4	01 30 60 15	strbne	r3,[src,#-0x1]!
4520a9e8	03 00 10 e3	tst	src,#0x3
4520a9ec	fa ff ff 1a	bne	LAB_4520a9dc
4520a9f0	03 30 11 e2	ands	r3,dest,#0x3
4520a9f4	41 cc 02 0a	beq	LAB_452bdb00
4520a9f8	04 20 52 e2	subs	size,size,#0x4
4520a9fc	1b 00 00 3a	bcc	LAB_4520aa70
4520aa00	03 c0 31 e7	ldr	r12,[dest,-r3]!
4520aa04	02 00 53 e3	cmp	r3,#0x2
4520aa08	08 00 00 3a	bcc	LAB_4520aa30
4520aa0c	0f 00 00 8a	bhi	LAB_4520aa50

LAB\_4520aa10

4520aa10	0c 38 a0 e1	mov	r3,r12, lsl #0x10
4520aa14	04 c0 31 e5	ldr	r12,[dest,#-0x4]!
4520aa18	04 20 52 e2	subs	size,size,#0x4
4520aa1c	2c 38 83 e1	orr	r3,r3,r12, lsr #0x10
4520aa20	04 30 20 e5	str	r3,[src,#-0x4]!
4520aa24	f9 ff ff 2a	bcs	LAB_4520aa10
4520aa28	02 10 81 e2	add	dest,dest,#0x2
4520aa2c	0f 00 00 ea	b	LAB_4520aa70

LAB\_4520aa30

4520aa30	0c 3c a0 e1	mov	r3,r12, lsl #0x18
4520aa34	04 c0 31 e5	ldr	r12,[dest,#-0x4]!
4520aa38	04 20 52 e2	subs	size,size,#0x4
4520aa3c	2c 3c 83 e1	orr	r3,r3,r12, lsr #0x18

Program Tree

- fw\_1
  - ram

Symbol Tree

- Imports
- Exports
- Functions
- Labels
- Classes
- Namespaces

Filter:

Data Type Mana...

Data Types

- BuiltinTypes
- fw\_1 (1 of 0)
- generic\_clib

Console - Scripting

```
performance."}, u'finish_reason': u'stop'}}], u'object': u'chat.completion'}
INFO:root:Added comment to function: FUN_4520a9bc
INFO:root:Renaming variables...
currentAddress: 4520a9bc
g3po.py> Finished!
```

4520a9bc custom\_memmove subs r3,r0,r1

File Edit Navigation Search Select Help

Decompile: custom\_memmove - (fw\_1@43face00)

```
1
2
3 /* /-----
4 |AI generated comment, take with a grain of salt:
5 |
6 | The function FUN_4520a9bc appears to be a custom implementation of the
7 | memmove function, which copies a block of memory from one location to another,
8 | handling overlapping regions correctly.
9 | Let's start by renaming the variables and the function itself:
10 | ...
11 | $param_1 -> $src
12 | $param_2 -> $dest
13 | $param_3 -> $size
14 | $FUN_4520a9bc :: $custom_memmove
15 | ...
16 | Now let's go through the code step by step:
17 | 1. The function calculates the difference between the source and destination
18 | pointers, and checks if the source and destination pointers are equal or if the
19 | size is equal to the difference. If either of these conditions is true, the
20 | function returns the destination pointer without doing anything.
21 | 2. If the source pointer is greater than the destination pointer, the
22 | function copies the memory block in reverse order, starting from the end of the
23 | block. This is done to handle overlapping regions correctly.
24 | 3. If the source pointer is less than the destination pointer, the function
25 | copies the memory block in the forward direction, starting from the beginning of
26 | the block.
27 | 4. The function handles different alignment cases by copying data in chunks
28 | of different sizes (1 byte, 2 bytes, 4 bytes, or 8 bytes) depending on the
29 | alignment of the source and destination pointers.
30 | 5. After copying the memory block, the function returns the destination
31 | pointer.
32 | There are no obvious security vulnerabilities in this code. However, it is
33 | worth noting that this custom implementation may not be as efficient as the
34 | standard memmove function provided by the C library, and it may not handle all
35 | edge cases correctly. It is generally recommended to use the standard library
36 | functions when possible, as they are well-tested and optimized for performance.
37 | Model: gpt-4, Temperature: 0.05
38 |-----
39
40
41
42
43
44
45
46
47
48
49
50
```

~/\ /  
|oo |  
-|=|  
//|.\|\  
|| \ / ||  
# \ / #  
|||  
|||

# An AI assistant for the GNU Debugger (GDB)

- **Asystent GDB:** narzędzie, które używa modelu językowego do analizowania informacji debugowania i odpowiadania na pytania dotyczące stanu środowiska uruchomieniowego lub kodu zestawu.
- **Narzędzie interaktywne:** Narzędzie odbiera informacje o rejestrach, wartościach stosu, śladzie wstecznym, zestawie i dekompilowanym kodzie oraz umożliwia użytkownikowi zadawanie zapytań do modelu.
- **Analiza luk w zabezpieczeniach:** narzędzie prowadzi użytkownika przez analizowanie luk w zabezpieczeniach lub innych zachowań środowiska uruchomieniowego w programie docelowym. Może również zadawać pytania uzupełniające w celu wyjaśnienia lub korekty.
- **Zmniejszenie złożoności debugowania:** narzędzie zamienia GDB w interfejs konwersacyjny, w którym użytkownicy mogą dyskutować o tym, co robi kod na każdym kroku, zamiast rozszyfrowywać surowe dane debugowania.

```
idra, code"
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
EAX 0xffffcc10 ← 0x1
EBX 0x804c000 ( _GLOBAL_OFFSET_TABLE_ ) → 0x804bf14 ( _DYNAMIC ) ← 0x1
ECX 0xffffcc10 ← 0x1
EDX 0xffffcc30 → 0xf7f83000 ( _GLOBAL_OFFSET_TABLE_ ) ← 0x229dac
EDI 0xf7ffcb80 ( _rtld_global_ro ) ← 0x0
ESI 0xffffccc4 → 0xffffce9e ← '/home/lucca/scratch/pwnable/bin/stacksmash.unsafe32'
EBP 0xffffcbf8 → 0xf7ff020 ( _rtld_global ) → 0xf7ffda40 ← 0x0
ESP 0xffffcbe0 → 0xffffcc20 → 0xf7f83000 ( _GLOBAL_OFFSET_TABLE_ ) ← 0x229dac
EIP 0x80491a8 (main+34) ← 0x408b1f7f

-2 "stack"
00:0000 esp 0xffffcbe0 → 0xffffcc20 → 0xf7f83000 ( _GLOBAL_OFFSET_TABLE_ ) ← 0x229dac
01:0004 0xffffcbe4 → 0xf7be66c → 0xf7ffdba9 → 0xf7be780 → 0xf7ffda40 ← ...
02:0008 0xffffcbe8 → 0xf7fbeb10 → 0xf7d73cc6 ← 'GLIBC_PRIVATE'
03:000c 0xffffcbec ← 0x1
04:0010 0xffffcbf0 → 0xffffcc10 ← 0x1
05:0014 0xffffcbf4 → 0xf7f83000 ( _GLOBAL_OFFSET_TABLE_ ) ← 0x229dac
06:0018 ebp 0xffffcbf8 → 0xf7ff020 ( _rtld_global ) → 0xf7ffda40 ← 0x0
07:001c 0xffffcbfc → 0xf7d7a519 ( __libc_start_call_main+121 ) ← add esp, 0x10

-5 "disasm"
0x80491a5
ax], 1
▶ 0x80491a8
0x80491aa
tr [eax + 4]
0x80491ad
tr [eax]
0x80491af
0x80491b2
0x80491b3
0x1ff8]
0x80491b9
0x80491ba
0x80491bf
0x80491c2
Python 3.10.6
GCC 11.3.0]
Type 'copyrig
more informat
IPython 7.30.6
hon. Type '?'
In [1]:

db* 1:zsh-
```

# BurpGPT

- Narzędzie BurpGPT, będące rozszerzeniem dla Burp Suite, pozwala badaczom wykorzystać GPT do analizy żądań i odpowiedzi HTTP.
- Działa poprzez wykorzystanie funkcji proxy Burp do przechwytywania ruchu HTTP i analizy go za pomocą API OpenAI w celu identyfikacji ryzyk i potencjalnych rozwiązań problemów.
- Może być używane do odkrywania punktów iniekcji, błędnych konfiguracji i więcej.
- Podczas rozwijania tego rozszerzenia przetestowano kilka scenariuszy z życia realnego i stwierdzono, że GPT3.5 i GPT4 skutecznie identyfikują podatności na Cross-Site Scripting (XSS) i błędnie skonfigurowane nagłówki HTTP bez potrzeby dodatkowego dostrojenia.

ChatGPT Answer:

The HTTP request and response depict a series of interactions between a client and a web server hosting a simple forum page (Forum v0.001) with the functionality to submit and display messages. The client first sends a GET request for the forum page, followed by requests for a stylesheet (s.css) and a favicon (favicon.ico). The stylesheet is returned with a 304 Not Modified, indicating that the requested file has not changed. The favicon returns a 404 Not Found, as the server cannot locate the requested file. The client then submits a POST request with the message data, and the server returns a 200 OK with the updated forum page, displaying the submitted message.

1. Risk: Cross-site scripting (XSS) attacks. Fix: Sanitize user inputs and escape outputs to prevent malicious scripts from being embedded in messages.
2. Risk: Insecure HTTP connection. Fix: Implement HTTPS to encrypt data transmitted between the server and the client.
3. Risk: Exposed server version (nginx). Fix: Adjust the web server configuration to hide version information in the response header.
4. Risk: Outdated or unused resources (s.css file). Fix: Keep resources up to date, remove unused resources, and adjust caching settings as needed.
5. Risk: Favicon not found (404). Fix: Add a favicon file to the server and adjust the reference in the HTML code if necessary.
6. Risk: Unprotected form submission. Fix: Implement CSRF tokens or other anti-CSRF mechanisms to protect form data from cross-site request forgery attacks.
7. Risk: No server-side input validation for the form. Fix: Implement input validation on the server-side to check for data correctness, length and format, and prevent processing of malicious data.

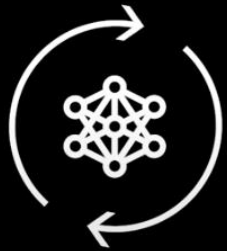


Jak działają narzędzie  
korzystające z AI (ML)?

NVIDIA



# NVIDIA Anti-spear phishing



Generative-AI



NVIDIA Morpheus



Exposure Signals

Inventory

Assets

Vulnerability Management 1%

Identity Exposure 97%

Web Application Scanning <1%

Cloud Security <1%

OT Security 1%

Number Of Assets 92.4k

New Assets In Last 7 Days 103

Updated Assets in last 7 days 8.7k

FIND > Assets Search by typing a valid query

Query [ ] [ ] [ ] [ ] [ ] Score Score (Beta)

TENABLE ONE

Name	Source	Asset Type	AE	Assets	Score	Score (Beta)	Last Updated	See Details	
<input type="checkbox"/> qapvs-centos7-2-2		Device		992		6k	21 listopada 2024	<a href="#">See Details &gt;</a>	
<input type="checkbox"/> rhel8.dc.demo.io		Device		985		650	42	21 listopada 2024	<a href="#">See Details &gt;</a>
<input type="checkbox"/> Herman Crumback		Person		973		6	12	20 listopada 2024	<a href="#">See Details &gt;</a>
<input type="checkbox"/> Danial Gordey		Person		973		8	12	20 listopada 2024	<a href="#">See Details &gt;</a>
<input type="checkbox"/> Doug Busken		Person		973		11	13	21 listopada 2024	<a href="#">See Details &gt;</a>
<input type="checkbox"/> Chester Bolding		Person		973		11	13	21 listopada 2024	<a href="#">See Details &gt;</a>
<input type="checkbox"/> Rachael Stibitz		Person		973		11	13	21 listopada 2024	<a href="#">See Details &gt;</a>
<input type="checkbox"/> Columbus Freville		Person		973		11	13	21 listopada 2024	<a href="#">See Details &gt;</a>
<input type="checkbox"/> Jeannette Brace		Person		973		11	13	21 listopada 2024	<a href="#">See Details &gt;</a>
<input type="checkbox"/> Queenie Bellemare		Person		973		11	13	21 listopada 2024	<a href="#">See Details &gt;</a>
<input type="checkbox"/> Tamara Eppling		Person		973		11	13	21 listopada 2024	<a href="#">See Details &gt;</a>

DEVICE

# qapvs-centos7-2-2

Source: [Tenable Vulnerability Management](#) | [Hide Summary](#) ^



### About this asset

The asset qapvs-centos7-2-2 is a general-purpose device running Linux Kernel 4.8. It has a high relative exposure (AES: 992) and is considered critical for the business (ACR: 10). This asset is not internet-facing and has not been authenticated since February 2024. It has several critical and high-risk vulnerabilities, including CVE-2019-5736, CVE-2016-5195, CVE-2021-4034, CVE-2023-4863, CVE-2016-0728, CVE-2017-1000112, CVE-2017-5375, CVE-2021-3156, CVE-2017-7308, and CVE-2021-22555. These vulnerabilities expose the asset and the network to various risks, including unauthorized access, privilege escalation, service interruption, data breach, and tampering.

### Weaknesses

This asset is vulnerable to several critical risks and vulnerabilities, including: 1. **CVE-2019-5736**: This vulnerability allows attackers to overwrite the host runc binary and obtain host root access by executing a command as root within a container. It has a VPR score of 10.0 and is considered HIGH risk. 2. **CVE-2016-5195**: This vulnerability allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping. It has a VPR score of 9.8 and is considered HIGH risk. 3. **CVE-2021-4034**: This vulnerability allows unprivileged users to gain administrative rights on the target machine by crafting environment variables to induce pexec to execute arbitrary code. It has a VPR score of 9.8 and is considered HIGH risk. 4. **CVE-2023-4863**: This vulnerability allows a remote attacker to perform an out-of-bounds memory write via a crafted HTML page. It has a VPR score of 9.8 and is considered HIGH risk. 5. **CVE-2016-0728**: This vulnerability allows local users to gain privileges or cause a denial of service via crafted keyctl commands. It has a VPR score of 9.7 and is considered HIGH risk. 6. **CVE-2017-1000112**: This vulnerability allows for a bypass of ASLR and DEP protections leading to potential memory corruption attacks. It has a VPR score of 9.7 and is considered HIGH risk. 7. **CVE-2017-5375**: This vulnerability allows for a bypass of ASLR and DEP protections leading to potential memory corruption attacks. It has a VPR score of 9.7 and is considered CRITICAL risk. 8. **CVE-2021-3156**: This vulnerability allows privilege escalation to root via "sudoedit -s" and a command-line argument that ends with a single backslash character. It has a VPR score of 9.7 and is considered HIGH risk. 9. **CVE-2017-7308**: This vulnerability allows local users to cause a denial of service or gain privileges via crafted system calls. It has a VPR score of 9.7 and is considered HIGH risk. 10. **CVE-2021-22555**: This vulnerability allows an attacker to gain privileges or cause a DoS (via heap memory corruption) through user name space. It has a VPR score of 9.7 and is considered HIGH risk.

- Data Breach and Tampering
- Privilege Escalation
- Service Interruption
- Unauthorized Access and Control



Asset Exposure Score

992/1000

Asset Criticality Rating

10/10 User Overridden

Weaknesses Identified

2575

Key Properties

Asset Class	Device
Asset Type	Compute and Application Server
Asset Functionality	UNDEFINED
Last Observed At	20 lis 2024 at 14:27

- Properties
- Attack Paths
- Weaknesses
- Tags
- Exposure Cards
- Exposure Signals**
- Relationships
- Users
- Device Accounts



tenableone | Inventory

Exposure Signals

Inventory

Add Exposure Signal

Tenable 30/30

AD Devices not scanned by Tenable Vulnerability Management

Violations Exposure Mgmt. Trends (Last 7 days)

55.7K 0.02%

Accounts Using a Breached Password to Connect to Hosts

Violations Exposure Mgmt. Trends (Last 7 days)

1 0%

Active Directory Domain Admin Group used on Internet-Exposed Hosts with...

Violations Exposure Mgmt. Trends (Last 7 days)

0 0%

Active Directory Domain Controller with Microsoft Vulnerabilities including "Acti...

Violations Exposure Mgmt. Trends (Last 7 days)

11 0%

Active Directory Domain Controllers being Administered by Non-Administrative...

noPacWorkstation

See Asset Details

Exposure Signals Summary Gen AI

Tenable is considering the asset "noPacWorkstation" to be part of the exposure insight "Accounts Using a Breached Password to Connect to Hosts" because: it is an Account that was last observed on November 21st, 2024 UTC and has been flagged with the detection code "C-PASSWORD-HASHES-ANALYSIS:R-BREACHED-PASSWORD". This indicates that the account is using a password that has been compromised in a previous data breach. The account has three weaknesses, including "Use of a Breached Password", "Use of a Weak Password", and "Password stored using reversible encryption". This means that the account's password is likely to be easily guessed or compromised, making it vulnerable to attack. The account was created on July 19th, 2024 UTC.

Key Properties (3)

Last Observed At Nov 21, 2024 8:30AM

Created Date Jul 19, 2024 3:40PM

Asset Class

Weaknesses (3)

Search

Use of a Breached Password

Use of a Weak Password

Password stored using reversible encryption

Account Details

November 21 3:28A

What is it

Associated Assets

Relationship

See results

Impacted Assets

Search

Name

noPacWorkstat

Account to Hosts

Archive

Generated by AI

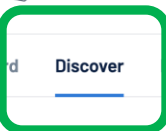
hosts. These accounts may be vulnerable to attack, as they are using

HASHES-ANALYSIS:R-BREACHED-PASSWORD WITH

device

nopacworkstation

See Details



← Back to Attack Paths

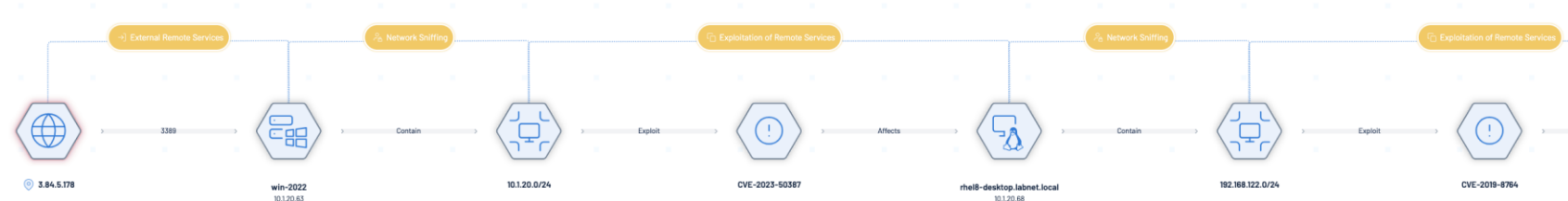
- Attacker gains credentials of Administrator by dumping LSASS memory from ARCHIE
- External asset 54.163.3.197 reaches to Azure user Daryl Buszka by exploiting Windows vulnerability C...
- External asset 54.163.3.197 reaches to Azure user Marion Bircheat by exploiting Windows vulnerabil...
- External asset 54.163.3.197 reaches to Azure user Carter Kerbow by exploiting Windows vulnerability ...
- External asset 54.163.3.197 reaches to Azure user Epsie Jessing by exploiting Windows vulnerability ...
- External asset 54.163.3.197 reaches to Azure user Mallie Afonin by exploiting Windows vulnerability ...
- External asset 54.163.3.197 reaches to Azure user Zola Spiering by exploiting Windows vulnerability ...
- External asset 54.163.3.197 reaches to Azure user Hans Hawbecker by exploiting Windows vulnerability...
- External asset 54.163.3.197 reaches to

### 3.84.5.178 exploits three vulnerabilities to reach qapvs-centos7-2-2 AI

View Findings (7)

An attacker starts the attack from 3.84.5.178 and gains access to the internal network by exploiting a vulnerability in win-2022, win-2022 is a Windows server. The attacker then exploits CVE-2023-50387, CVE-2019-8764 and CVE-2016-1962 to gain access to qapvs-centos7-2-2. The attacker uses network sniffing to find new targets in the network. This attack path is a good example of how an attacker can use multiple vulnerabilities to gain access to a target system.

- Related Products, Assets, and Findings**
- Tenable Vulnerability Management (19506, 24272, 64582, 89763, 143288, 190971)



Exposed Asset Critical Asset

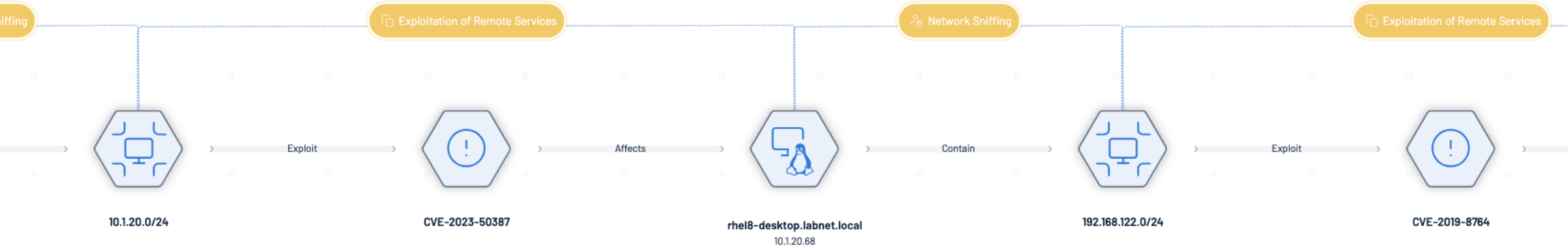
AI Assistant | Zoom | Refresh | See in APA

3.84.5.178 exploits three vulnerabilities to reach qapvs-centos7-2-2

AI Critical



See in APA



AI Assistant | | |



AI

Hey there! 🚀 Ask me anything about the **attack path**.

Nov 21, 2024



User

możesz mi po polsku wyjaśnić dlaczego ten port 3389 jest niebezpieczny ?

Nov 21, 2024

Port 3389 jest używany przez **Remote Desktop Protocol (RDP)**, który pozwala na zdalne sterowanie komputerem. Choć RDP jest przydatnym narzędziem, może być również niebezpieczny, ponieważ:

- **Ataki brute force:** Hakerzy mogą próbować odgadnąć hasło do konta RDP, używając zautomatyzowanych narzędzi, które testują tysiące kombinacji.
- **Exploity:** W przeszłości odkryto luki w zabezpieczeniach RDP, które umożliwiały hakerom przejęcie kontroli nad komputerem bez znajomości hasła.
- **Brak uwierzytelniania wieloskładnikowego:** Domyślnie RDP nie wymaga uwierzytelniania wieloskładnikowego (MFA), co ułatwia hakerom dostęp do komputera po kradzieży hasła.
- **Nieszyfrowany ruch:** Domyślnie ruch RDP nie jest szyfrowany, co oznacza, że hakerzy mogą podsłuchiwać komunikację i wykraść dane, takie jak hasła.

W tym konkretnym przypadku, połączenie z zewnątrz (ExternalAsset) do komputera z systemem Windows Server (B) przez port 3389 sugeruje, że RDP jest narażony na ataki z Internetu. To stwarza poważne zagrożenie bezpieczeństwa, ponieważ hakerzy mogą wykorzystać luki w zabezpieczeniach RDP do przejęcia kontroli nad serwerem.



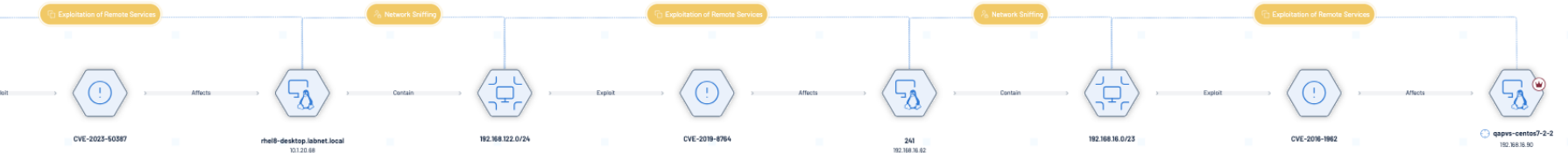
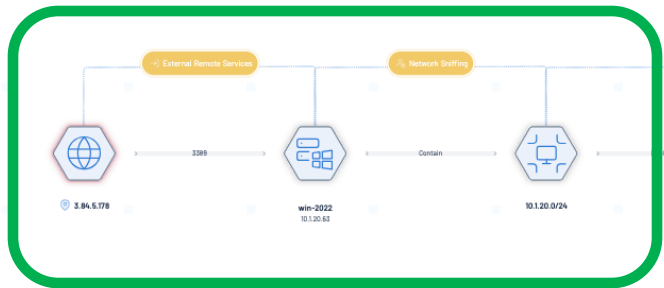
AI

#### Zalecenia:

- **Zamknij port 3389 na firewallu**, jeśli nie jest używany.
- **Używaj silnych haseł** do kont RDP i **włącz uwierzytelnianie wieloskładnikowe (MFA)**.
- **Regularnie aktualizuj system operacyjny i oprogramowanie**, aby upewnić się, że korzystasz z najnowszych poprawek bezpieczeństwa.
- **Rozważ użycie VPN** do szyfrowania ruchu RDP.

Nov 21, 2024





→ External Remote Services

🕸 Network Sniffing



📍 3.84.5.178

3389



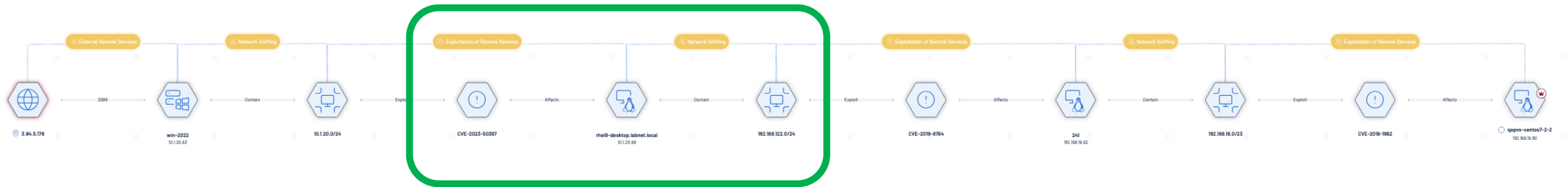
win-2022  
10.1.20.63

Contain



10.1.20.0/24

Exploit



Exploitation of Remote Services

Network Sniffing

Exploit



CVE-2023-50387

Affects



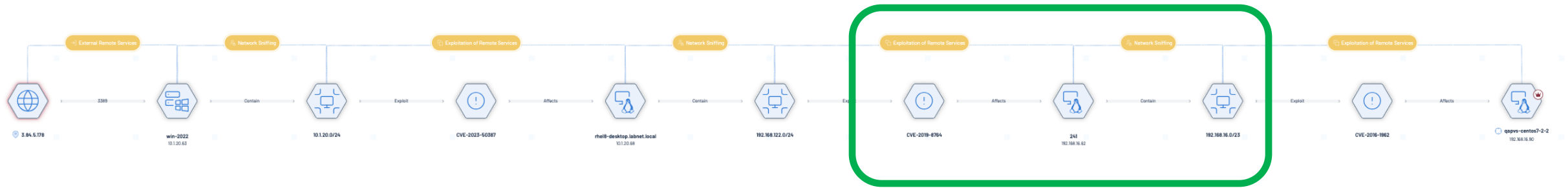
rhel8-desktop.labnet.local  
10.1.20.68

Contain



192.168.122.0/24

Exploit



Exploitation of Remote Services

Network Sniffing

Exploit



CVE-2019-8764

Affects



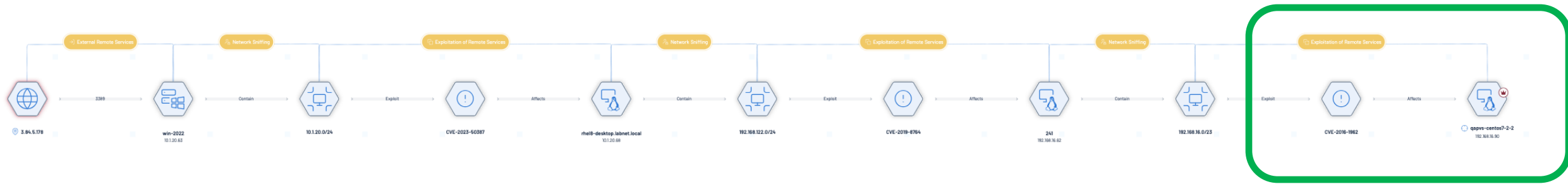
241  
192.168.16.62

Contain



192.168.16.0/23

Exploit



## Exploitation of Remote Services

Exploit



**CVE-2016-1962**

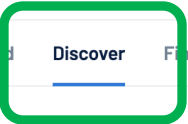
Affects



**qapvs-centos7-2-2**

192.168.16.90





### Query builder

[Back to queries](#)

Standard queries

#### Blast Radius



Search

Please add parameters first

Standard  Blast Radius  Asset Exposure

Source



#### Target

Asset type  Specific asset

AllAssets



+ Add a Target

# Top Attack Paths

Choose your filter... Apply

- Target ACR > 8
- Vulnerability Management
- Identity Exposure
- Web Application Scanning
- OT Security
- Cloud Security
- Attack Surface Management

0 Selected | [Export Selected \(0\)](#) | [Export All](#)

Page 1 of 2364 | 1 to 25 of 59079

<input type="checkbox"/>	View Graph	Name	Path Priority Rating	Nodes	Actions
<input type="checkbox"/>	<a href="#">New</a>	Attacker gains credentials of Administrator by dumping LSASS memory from ...	AI Critical	🌐 > 🏠	⋮
<input checked="" type="checkbox"/>	<a href="#">New</a>	External asset 54.163.3.197 reaches to Azure user Daryl Buszka by exploiting W...	AI Critical	🌐 > 🏠 > 🛠️ ...	⋮
<b>Attack Summary by AI</b>					
An attacker starts from an external asset 54.163.3.197 and gains initial access into Windows workstation water-plant-01 using external remote services. The attacker then sniffs the network traffic and discovers the subnet 192.168.15.0/24 and the vulnerability CVE-2023-50387 which exists in the domain controller SE-DC1. The attacker exploits the vulnerability and compromises the domain controller. The attacker then gains access to a service ADSync which is running on the domain controller. The attacker uses the service to gain access to the Azure tenant Tenable Cloud Security Customer 2. Finally, the attacker gains access to the Azure user Daryl Buszka by using the cloud account technique.					
<input type="checkbox"/>	<a href="#">New</a>	External asset 54.163.3.197 reaches to Azure user Marion Bircheat by exploitin...	AI Critical	🌐 > 🏠 > 🛠️ ...	⋮
<input type="checkbox"/>	<a href="#">New</a>	External asset 54.163.3.197 reaches to Azure user Carter Kerbow by exploiting ...	AI Critical	🌐 > 🏠 > 🛠️ ...	⋮
<input type="checkbox"/>	<a href="#">New</a>	External asset 54.163.3.197 reaches to Azure user Fnsie Jessing by exploiting ...	AI Critical	🌐 > 🏠 > 🛠️ ...	⋮

- Target ACR > 8
- Vulnerability Management
- Identity Exposure
- Web Application Scanning
- OT Security
- Cloud Security
- Attack Surface Management

0 Selected | [Export Selected \(0\)](#) | [Export All](#)

			View Graph	Name	Path	Priority Rating	Nodes	Actions
>	<input type="checkbox"/>	New		Attacker gains credentials of Administrator by dumping LSASS memory from ...	AI	Critical	>	
^	<input type="checkbox"/>	New		External asset 54.163.3.197 reaches to Azure user Daryl Buszka by exploiting W...	AI	Critical	>  >  ...	
<b>Attack Summary by AI</b>								
An attacker starts from an external asset 54.163.3.197 and gains initial access into Windows workstation water-plant-01 using external remote services. The attacker then sniffs the network traffic and discovers the subnet 192.168.15.0/24 and the vulnerability CVE-2023-50387 which exists in the domain controller SE-DC1. The attacker exploits the vulnerability and compromises the domain controller. The attacker then gains access to a service ADSync which is running on the domain controller. The attacker uses the service to gain access to the Azure tenant Tenable Cloud Security Customer 2. Finally, the attacker gains access to the Azure user Daryl Buszka by using the cloud account technique.								
>	<input type="checkbox"/>	New		External asset 54.163.3.197 reaches to Azure user Marion Bircheat by exploitin...	AI	Critical	>  >  ...	
>	<input type="checkbox"/>	New		External asset 54.163.3.197 reaches to Azure user Carter Kerbow by exploiting ...	AI	Critical	>  >  ...	
>	<input type="checkbox"/>	New		External asset 54.163.3.197 reaches to Azure user Ensie, Jessing by exploiting ...	AI	Critical	>  >  ...	

# Blast Radius

Search

Please add parameters first

Standard  Blast Radius  Asset Exposure

Source



Target

Asset type  Specific asset

AllAssets 1

Add a Target

Choose your filter...

Target ACR > 8

Vulnerability Management

Identity Exposure

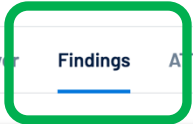
Web Application Scanning

OT Security

Attack Surface Management

0 Selected | [Export Selected \(0\)](#) [Export All](#)

<input type="checkbox"/>	<a href="#">View Graph</a>	Name	Path	Priority	Rating
<input type="checkbox"/>		Attacker gains credentials of Administrator by dumping LSASS memory from ...	AI	Critical	
<input checked="" type="checkbox"/>		External asset 54.163.3.197 reaches to Azure user Daryl Buszka by exploiting W...	AI	Critical	
<b>Attack Summary by AI</b> An attacker starts from an external asset 54.163.3.197 and gains initial access into Windows workstation water-plant-01 using external remote services. The attacker then sn... the vulnerability CVE-2023-50387 which exists in the domain controller SE-DC1. The attacker exploits the vulnerability and compromises the domain controller. The attacker... domain controller. The attacker uses the service to gain access to the Azure tenant Tenable Cloud Security Customer 2. Finally, the attacker gains access to the Azure user D...					
<input type="checkbox"/>		External asset 54.163.3.197 reaches to Azure user Marion Bircheat by exploitin...	AI	Critical	
<input type="checkbox"/>		External asset 54.163.3.197 reaches to Azure user Carter Kerbow by exploiting ...	AI	Critical	
<input type="checkbox"/>		External asset 54.163.3.197 reaches to Azure user Fnsie , lessing by exploiting ...	AI	Critical	



**Open Findings**

**13035**

- 0 Critical
- 9 High
- 3 Medium
- 13K Low

**Archived Findings**

**101937**

- 0 Critical
- 32 High
- 53 Medium
- 101.9K Low

**Total Findings**

**114972**

- 0 Critical
- 41 High
- 56 Medium
- 114.9K Low

Choose your filter... [Apply] [Filter Icon]

0 Selected | [Export Selected (0)] [Export All] << > Page 1 of 522 >> 1 to 25 of 13035

<input type="checkbox"/>	View Path	Priority	MITRE ATT&CK Id	Technique	Source	Target	Status	Actions
<input type="checkbox"/>		High	T1040 <a href="#">↗</a>	Network Sniffing	<ul style="list-style-type: none"> <li>Linux Computers 10</li> <li>Windows Servers 24</li> <li>Windows Workstations 2</li> </ul>	192.168.15.0/24	To Do	
<input type="checkbox"/>		High	T1210 <a href="#">↗</a>	Exploitation of Remote Services	<ul style="list-style-type: none"> <li>192.168.15.0/24</li> <li>Windows Servers 27</li> <li>Windows Workstations 38</li> </ul>	se-dc1.demo.io	To Do	
<input type="checkbox"/>		High	T1133 <a href="#">↗</a>	External Remote Services	54.163.3.197	water-plant-...	To Do	
<input type="checkbox"/>		High	T1210 <a href="#">↗</a>	Exploitation of Remote Services	<ul style="list-style-type: none"> <li>192.168.15.0/24</li> <li>Windows Servers 6</li> <li>Windows Workstations 24</li> </ul>	se-dc1.demo.io	To Do	
<input type="checkbox"/>		High	T1558 <a href="#">↗</a>	AS-REP Roasting	LABNET\domai...	LABNET\spalp...	To Do	

0 Selected | [Export Selected \(0\)](#) [Export All](#)



<input type="checkbox"/>	View Path	Priority	MITRE ATT&CK Id	Technique	Source	Target
<input type="checkbox"/>		● High	T1040 <a href="#">↗</a>	Network Sniffing	Linux Computers 10 Windows Servers 24 Windows Workstations 2	192.168.15.0/24
<input type="checkbox"/>		● High	T1210 <a href="#">↗</a>	Exploitation of Remote Services	192.168.15.0/24 Windows Servers 27 Windows Workstations 38	se-dc1.demo.io
<input type="checkbox"/>		● High	T1133 <a href="#">↗</a>	External Remote Services	54.163.3.197	water-plant-...
<input type="checkbox"/>		● High	T1210 <a href="#">↗</a>	Exploitation of Remote Services	192.168.15.0/24 Windows Servers 6	se-dc1.demo.io

MITRE ATT&CK Heatmap

- Enterprise
- PRE
- Windows
- MacOS
- Linux
- Cloud
- Network
- Containers
- ICS

Show All Techniques  | Critical High Medium Low Not leading to Critical Asset

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Active Scanning	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle
Gather Victim Host Information	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force
Gather Victim Identity Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution	Account Manipulation	BITS Jobs	Credentials from Password Stores
Gather Victim Network Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Initialization Script...	Boot or Logon Autostart Execution	Build Image on Host	Exploitation for Credential Access
Gather Victim Org Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Script...	Debugger Evasion	Forced Authentication
Phishing for Information	Establish Accounts	Phishing	Inter-Process Communication	Compromise Host Software Binary	Create or Modify System Process	Deobfuscate/Decode Files or Inform...	Forge Web Credentials
Search Closed Sources	Obtain Capabilities	Replication Through Removable Media	Native API	Create Account	Domain or Tenant Policy Modificatio...	Deploy Container	Input Capture

## Case Details

[Overview](#) / [Threat Analysis Center Dashboard](#) / [Cases](#) / [Case Details](#)

#3-394005

High

Investigating

Owner

Brett VanWagoner

Created date

Aug 11, 2024, 11:09:28 PM

Assigned date

Aug 12, 2024, 3:31:59 PM

(EC2AMAZ-FQCB9QB on Windows) - WIN-PROT-VDL-MALWAR... [✎](#)

Overview

Detections

Notebook

History

Respond

 Information

Case type

Origin


Detection  
count

XDR

12

 MITRE Tactic(s)

No MITRE data found.

 Initial detection

Name	WIN-PROT-VDL-MALWARE-ATK-GETINBOX-A
Severity	High
Type	Threat
Source	 Sophos Endpoint
First detected	Aug 11, 2024, 11:08:50 PM
Created	Aug 11, 2024, 11:08:50 PM

 SummaryUse Sophos AI to analyze case  
detections

SOPHOS XDR

 Sophos Assistant Summary

### Summary

Multiple malware detection events were observed on a Windows Server 2019 Datacenter system (EC2AMAZ-FQCB9QB, IP: 10.0.1.217). Detected malware includes Mal/Generic-S, Mal/Generic-R, Troj/Squib-A, and ATK/GetInbox-A. The detections involved various files including RtlCreateUserThread.exe, calc.dll, test.sct, and Get-Inbox.ps1. All detected files were cleaned up by the antivirus software.

#### Observed MITRE Techniques

UNKNOWN

#### Impacted Hosts

EC2AMAZ-FQCB9QB (IP: 10.0.1.217)

#### Artifacts

- Artifact 1:

- Purpose: Mal/Generic-S - This detection family indicates a generic malware threat.

- Parent path: C:\AtomicRedTeam\atomics\T1055\bin\x64\

- Cleanup status: True

# Case Details

Overview / Threat Analysis Center Dashboard / Cases / Case Details

#3-189702 Critical New

WIN-PROT-BEHAVIORAL-MALWARE-EXEC-12B-T1059-001

Owner  
Brett VanWagoner

Created date  
Sep 22, 2023, 4:08:20 PM

Assigned date  
Aug 12, 2024, 4:44:55 PM

Last updated  
Aug 12, 2024, 4:44:55 PM

- Overview
- Detections
- Notebook
- History
- Respond

### Information

Case type

Origin XDR

Detection count 20

### MITRE Tactic(s)

No MITRE data found.

### Initial detection

Name WIN-PROT-BEHAVIORAL-MALWARE-EXEC-12B-T1059-001

Severity High

Type Threat

Source Sophos

First detected Sep 13, 2023, 11:03:30 PM

Created Sep 13, 2023, 11:03:30 PM

### Summary

### Command Line

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Command "IEX ([Text.Encoding]::UNICODE.GetString([Convert]::FromBase64String((gp HKCU:\Software\Microsoft\Windows\CurrentVersion\Debug).Debug)))"
```

**Sophos AI Analysis**

**Intent**  
The intent of the command is to execute a PowerShell script that is stored in the Windows Registry in an obfuscated Base64 encoded format.

**Outcome**  
If the command runs successfully, it will decode and execute the PowerShell script stored in the registry key HKCU:\Software\Microsoft\Windows\CurrentVersion\Debug. The exact outcome depends on the content of the script stored in the registry.

### Impacted Entities Beta

Show filters



## Command Line



```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Command "IEX ([Text.Encoding]::UNICODE.GetString([Convert]::FromBase64String((gp HKCU:Software\Microsoft\Windows\CurrentVersion Debug).Debug)))"
```

### Sophos AI Analysis ✕


#### Intent

The intent of the command is to execute a PowerShell script that is stored in the Windows Registry in an obfuscated Base64 encoded format.

#### Outcome

If the command runs successfully, it will decode and execute the PowerShell script stored in the registry key HKCU:Software\Microsoft\Windows\CurrentVersion\Debug. The exact outcome depends on the content of the script stored in the registry.


## Impacted Entities Beta


 Show filters



## Threat Analysis Center

### DETECT


 Dashboard

 Cases

 Detections

### INVESTIGATE


 Search

 Live Discover

 Threat Graph

### SETTINGS

 Integrations >

 Preferences

## Search

TAC > Natural Language Query

Help ▾ Annabelle Mercer ▾

Sophos Inc. • Super Admin

Detections ▾

Enter a natural language question to search the Sophos data lake

Last hour ▾

Search

✦ Suggestions:

Processes running from a temp directory, limit to 10

Display all High and Critical severity detections that have occurred in the last 24 hours

Active users last 24 hours

How many Critical severity detections have occurred in the last 7 days? Which endpoints are involved?



Charlotte AI is a generative AI security analyst that uses the world's highest-fidelity security data and is continuously improved by CrowdStrike's industry-leading threat hunters, managed detection and response operators, and incident response experts.

+ What are the indicators for Bitwise Spider?

▶ Send

# CrowdStrike

## Example prompts

Which threat actors target my industry?

What tactics does Silent Chollima use?

Hunt my environment for signs of Silent Chollima

What is my exposure to CVE-2023-34362?

Show me TeamViewer installations

Which hosts tried to connect to 194.59.164.67?

## Capabilities

Help users of all skill levels elevate their ability to stop breaches. Reduce complexity with easy to understand, plain language prompts that simplify your use of the platform. Get intuitive summaries of adversary activity in your environment, investigate and hunt with nothing but a prompt, and even trigger response actions.

## Privacy

Our generative AI was purpose-built for privacy, accuracy and safety. Charlotte AI actively redacts sensitive data and obtains only factual, traceable data to minimize AI hallucinations. Charlotte AI also advises users of the risks of any recommended actions and leverages built-in role-based access controls (RBAC) to prevent unauthorized user access.

---

## Example prompts

Which threat actors target my industry?

What tactics does Silent Chollima use?

Hunt my environment for signs of Silent Chollima

What is my exposure to CVE-2023-34362?

Show me TeamViewer installations

Which hosts tried to connect to 194.59.164.67?

---

## Capabilities

Help users of all skill levels elevate their ability to stop breaches. Reduce complexity with easy to understand, plain language prompts that simplify your use of the platform. Get intuitive summaries of adversary activity in your environment, investigate and hunt with nothing but a prompt, and even trigger response actions.

# What are the indicators for Bitwise Spider?

## Actors



Seen in your environment



11



2



4



**Actors**

BITWISE SPIDER

[See more about BITWISE SPIDER](#)



Last active  
**Jan 2024**

Status  
**Active**

Origin  
**Unknown**

Intel reports  
**399**

Target industries  
**44**

Target countries  
**103**

Actor type  
**eCrime**

Motivation  
**Criminal**

Community identifiers  
**LockBit, LockBitSupp**

## Indicators



Indicator	Type	Malware f...	Related a...	Kill chain	Created at	Updated at
lockbitsup4yez1	domain	LockBitRanso...	bitwise-spider	C2,ActionOn...	Feb. 1, 2022 1...	Feb. 6, 2024 2...
278c1492a06...	hash_md5	LockBitRanso...	bitwise-spider	ActionOnObj...	Nov. 27, 2023 ...	Feb. 1, 2024 1...

es\_notable ID: 200 HIGH TLPRED

Threat - Vectra AI - Conrad-hp suspected to be compromise

View Summary Analyst

Activity Workbook Guidance Timeline Artifacts Evidence Files Approvals Reports ACTION PLAYBOOK

Recent Activity

- admin Aug 26th at 11:32 pm
  - Vectra Ransomware Respons...
- Vectra Demo Aug 31st at 1:16 pm
  - Vectra Ransomware Respons...
- Vectra Demo Aug 31st at 3:31 pm
  - Vectra Ransomware Respons...
  - Create\_Jira\_Ticket
  - Get\_C2\_Detection
  - Add\_C2\_Detection\_info\_into\_Jira\_Ticket
  - Hunt\_C2\_IP\_Address
  - Add\_Hunting\_result\_in\_Jira\_Ticket
  - Approve\_blocking\_of\_an\_active\_threat
  - Block\_IP\_at\_Perimeter
  - Quarantine\_Host
  - Update\_Jira\_Ticket\_for\_CS
  - Update\_Jira\_Ticket\_for\_FW
- Vectra Demo 2 minutes ago
  - Vectra Ransomware Respons...
  - Create\_Jira\_Ticket



# Vectra SOAR

Widgets Notes MANAGE WIDGETS

**CROWDSTRIKE**

quarantine device conrad-hp [demolab cs]

DEVICE ID	PATH
ec63ebc68d09475796ceb3db80a24d19	/devices/entities/devices/v1

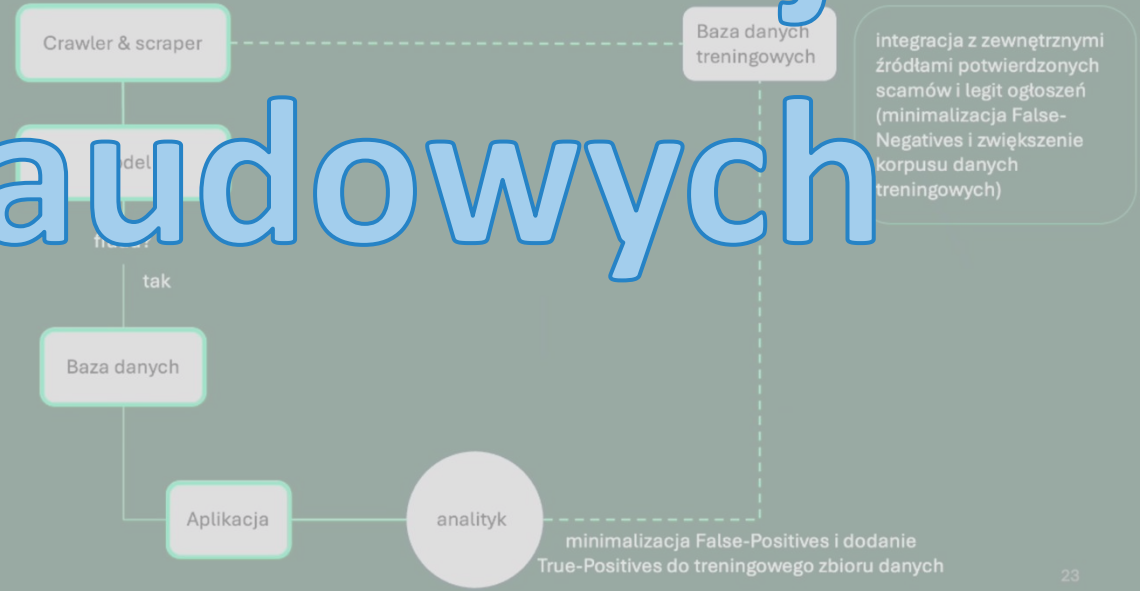
## zadanie

Mechanizm webscrappingu ofert pracy i ofert handlowych na popularnych serwisach ogłoszeniowych: olx.pl, sprzedajmy.pl, ogłaszamy24.pl

W oparciu o modele statystyczne lub modele AI stworzenie algorytmów pozwalających na analizę wyników, pozwalającą na ocenę charakteru ogłoszenia

# UKNF LLM do detekcji ogłoszeń fraudowych

Zadanie porównania



Supervision\_Hack 2023





## Chcę więcej !

- <https://github.com/tenable/awesome-llm-cybersecurity-tools>
- [Machine Learning \(ML\) in Cybersecurity: Use Cases – CrowdStrike](#)
- [Deep Learning Threat Protection: Powered by AI | Sophos](#)
- [Real-Life Examples of Machine Learning in Cybersecurity - SOCRadar® Cyber Intelligence Inc.](#)
- [System predicts 85 percent of cyber-attacks using input from human experts | MIT News | Massachusetts Institute of Technology](#)





Zapraszamy do dyskusji