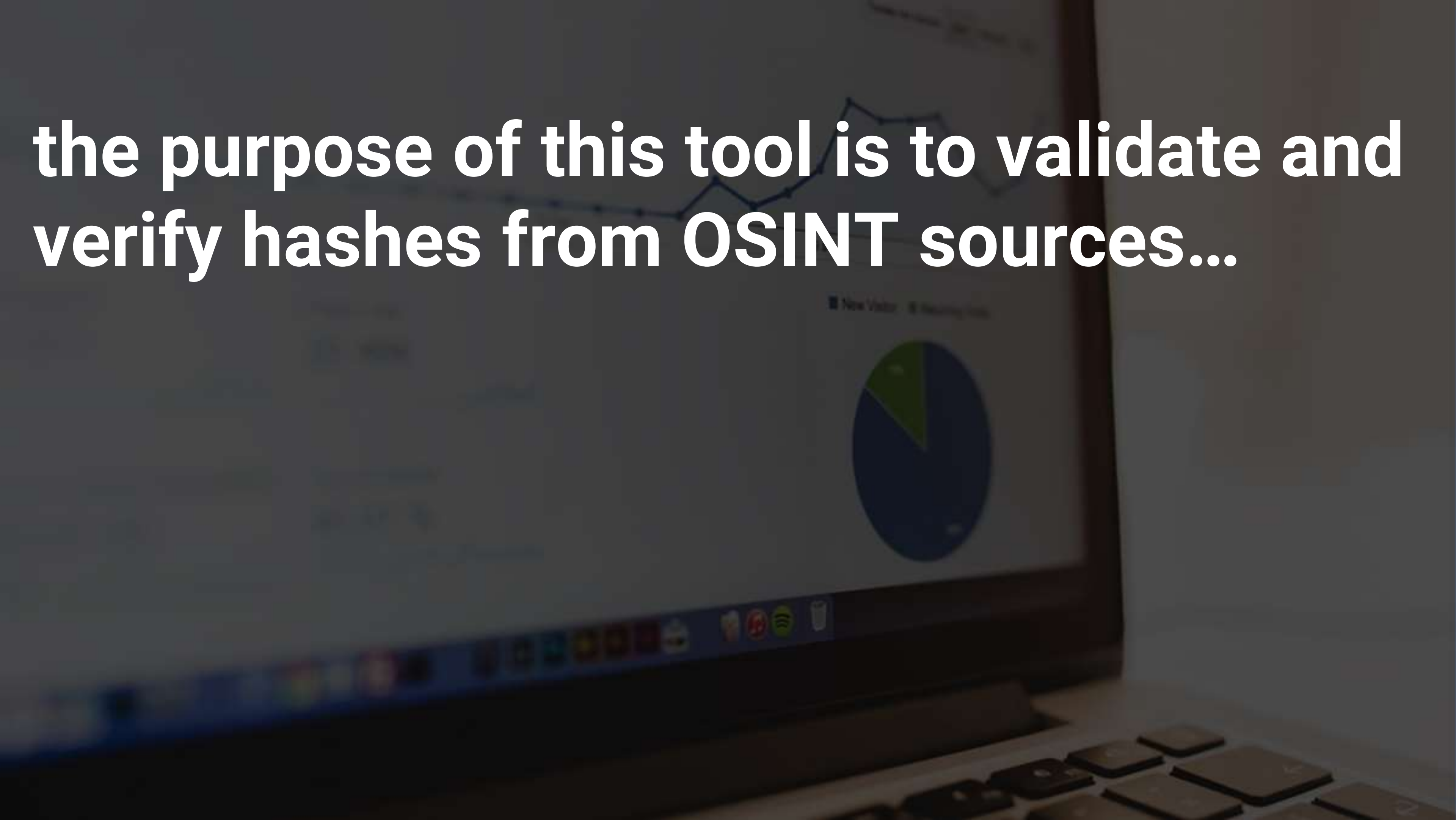
</Hash Check!

Verification & Validation Tools for Hashes

Hybrid Warfare

- On February 23rd, 2022, a destructive campaign using **HermeticWiper** targeted multiple Ukrainian organizations.
- On February 24th, 2022, a second destructive attack against a Ukrainian governmental network started, using a wiper we have named **IsaacWiper**.



the purpose of this tool is to validate and verify hashes from OSINT sources…

Indicators of Compromise (IoCs)

Indicators of compromise (IoCs) are the clues, artifact, and pieces of forensic data found on the network or operating system of an organization that indicate a potential intrusion or malicious activity in the organization’s infrastructure.

IoCs are not intelligence, although they do act as a good source of information regarding the threats that serve as data points in the intelligence process.

Security professionals need to perform continuous monitoring of IoCs to effectively and efficiently detect and respond to evolving cyber threats.

Categories of indicators of Compromise (IoCs)

Email Indicators

Are used to send malicious data to target organization or individual.

Examples include the sender’s email address, email subject, and attachments or link.

Network Indicators

Are useful for command and control, malware, malware delivery, identifying the operating system, and other task.

Examples include URLs, domain names, and IP addresses.

Host-Based Indicators

Are found by performing an analysis of the infected system within the organizational network.

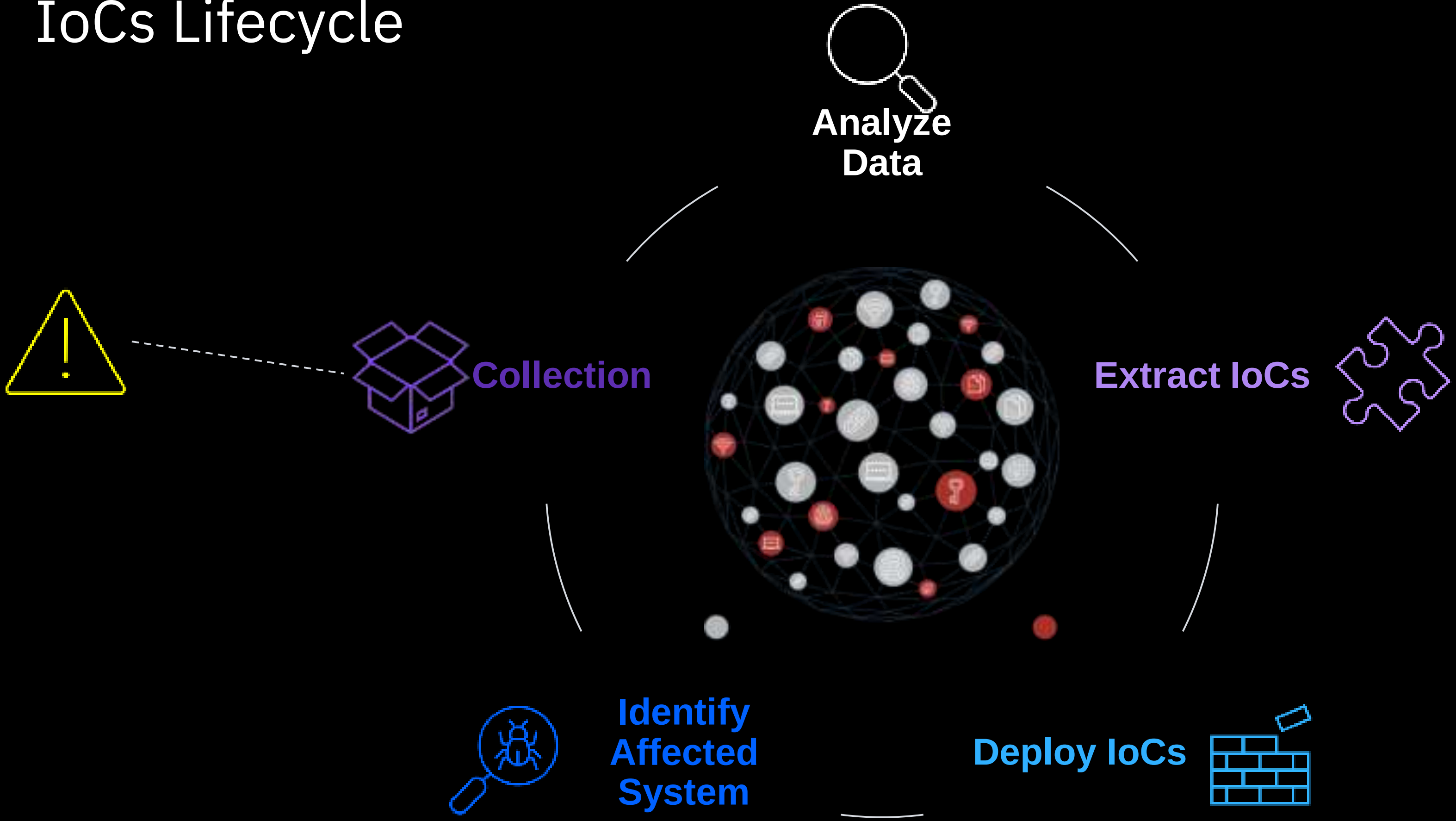
Examples include filenames, file hashes, registry keys, DLLs, and mutex.

Behavioral Indicators

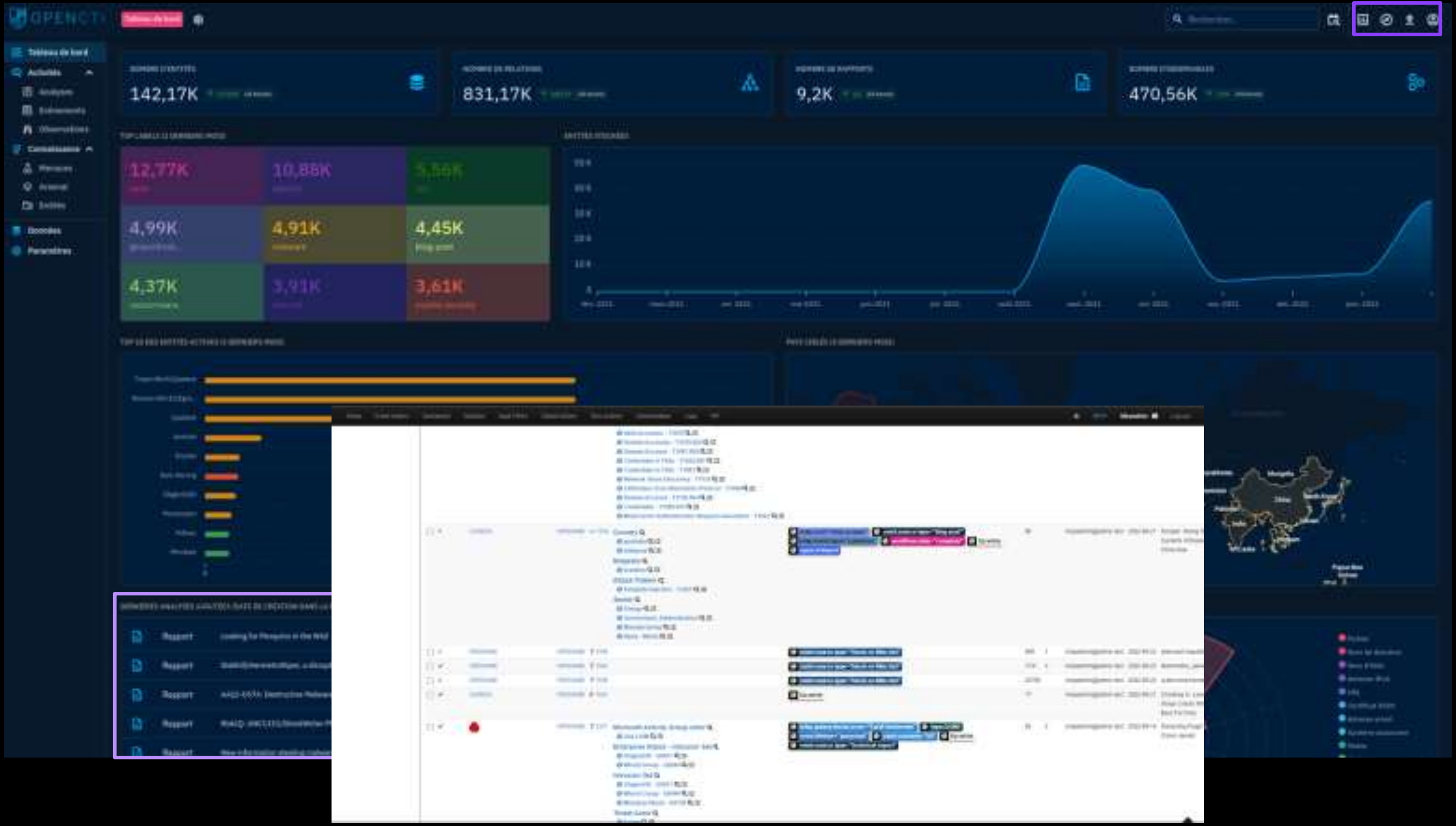
Are used to identify specific behavior related to malicious activities.

Examples of behavioral indicators include document executing PowerShell script, and remote command execution.

IoCs Lifecycle

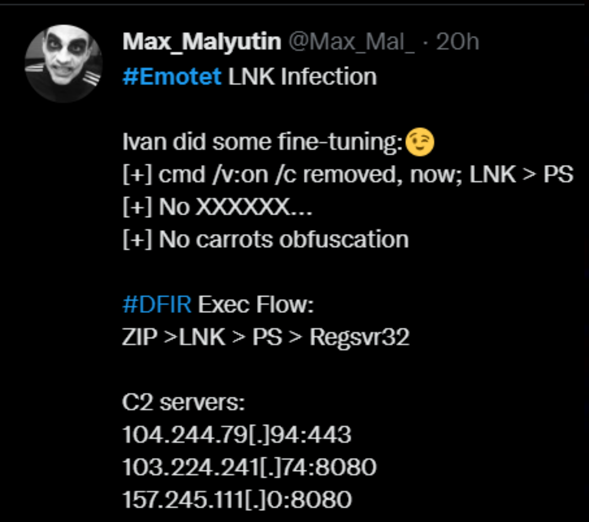


1. Collection - *Sources*



Threat Intelligence Platform

1. Collection - *Sources*



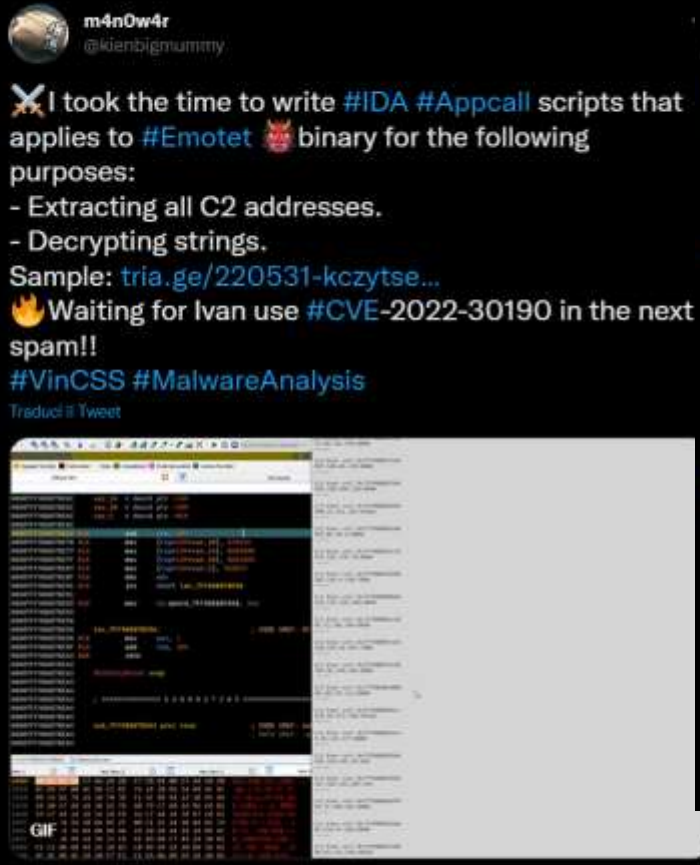
Max_Malyutin @Max_Mal_ · 20h

#Emotet LNK Infection

Ivan did some fine-tuning:😉
[+] cmd /v:on /c removed, now; LNK > PS
[+] No XXXXXX...
[+] No carrots obfuscation

#DFIR Exec Flow:
ZIP >LNK > PS > Regsvr32

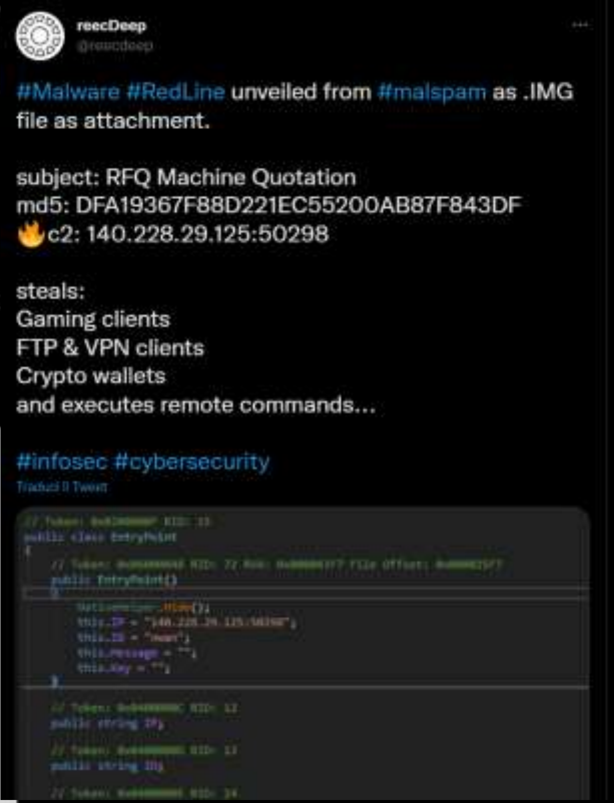
C2 servers:
104.244.79[.]94:443
103.224.241[.]74:8080
157.245.111[.]0:8080



m4n0w4r
@kienbigmummy

⚔️I took the time to write #IDA #Appcall scripts that applies to #Emotet 👹 binary for the following purposes:
- Extracting all C2 addresses.
- Decrypting strings.
Sample: tria.ge/220531-kczytse...
🔥Waiting for Ivan use #CVE-2022-30190 in the next spam!!
#VinCSS #MalwareAnalysis

Traduci il Tweet



reecDeep
@reecdeep

#Malware #RedLine unveiled from #malspam as .IMG file as attachment.

subject: RFQ Machine Quotation
md5: DFA19367F88D221EC55200AB87F843DF
🔥c2: 140.228.29.125:50298

steals:
Gaming clients
FTP & VPN clients
Crypto wallets
and executes remote commands...

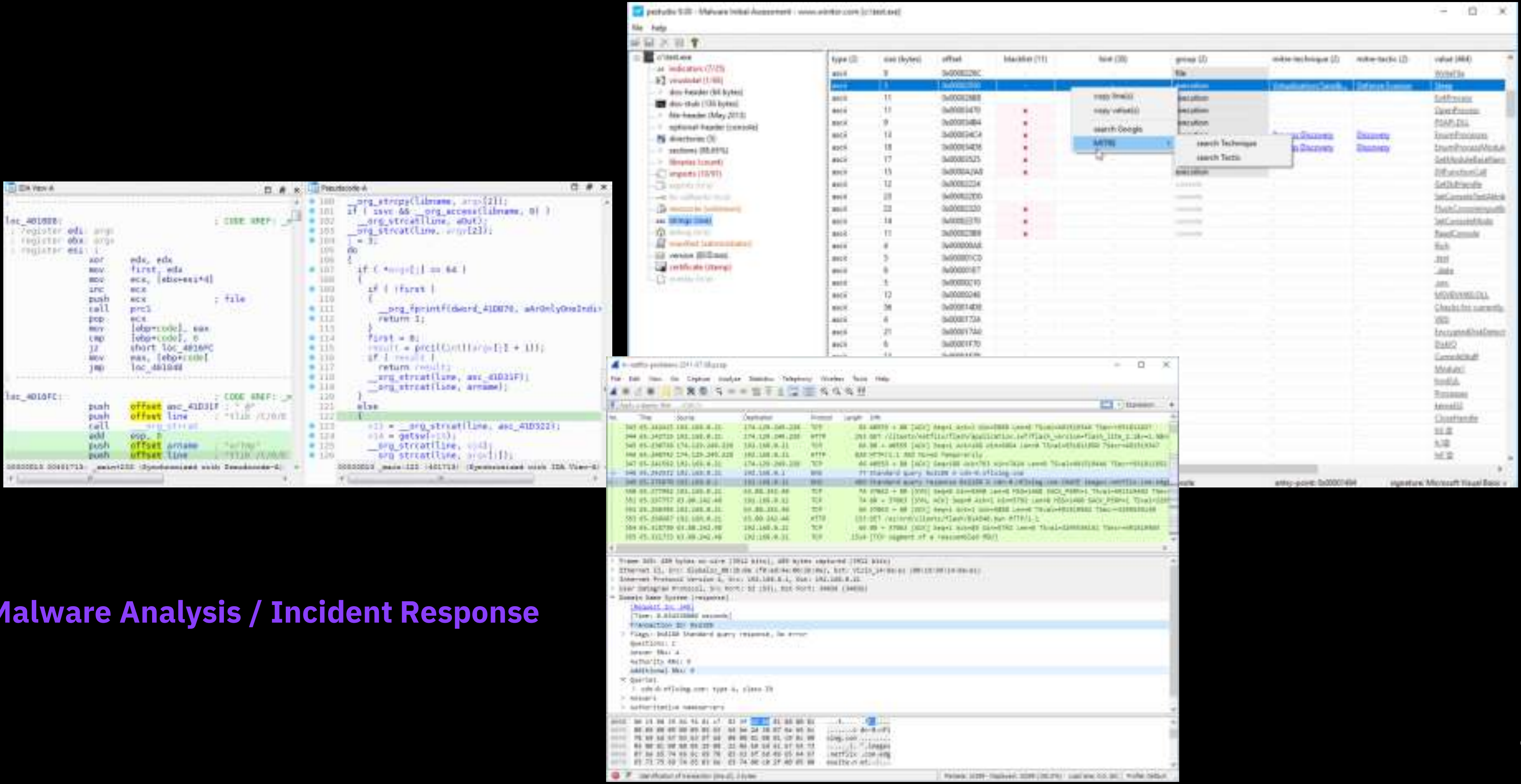
#infosec #cybersecurity

Traduci il Tweet

```
// Token: [illegible] RID: [illegible]
public class EntryPoint
{
    // Token: [illegible] RID: [illegible] RVA: [illegible] File Offset: [illegible]
    public EntryPoint()
    {
        [illegible]();
        this.IP = "140.228.29.125:50298";
        this.ID = "[illegible]";
        this.Message = "";
        this.Key = "";
    }

    // Token: [illegible] RID: 12
    public string IP;

    // Token: [illegible] RID: 13
    public string ID;

    // Token: [illegible] RID: 14
```

SOCMINT Analysis

1. Collection - *Sources*

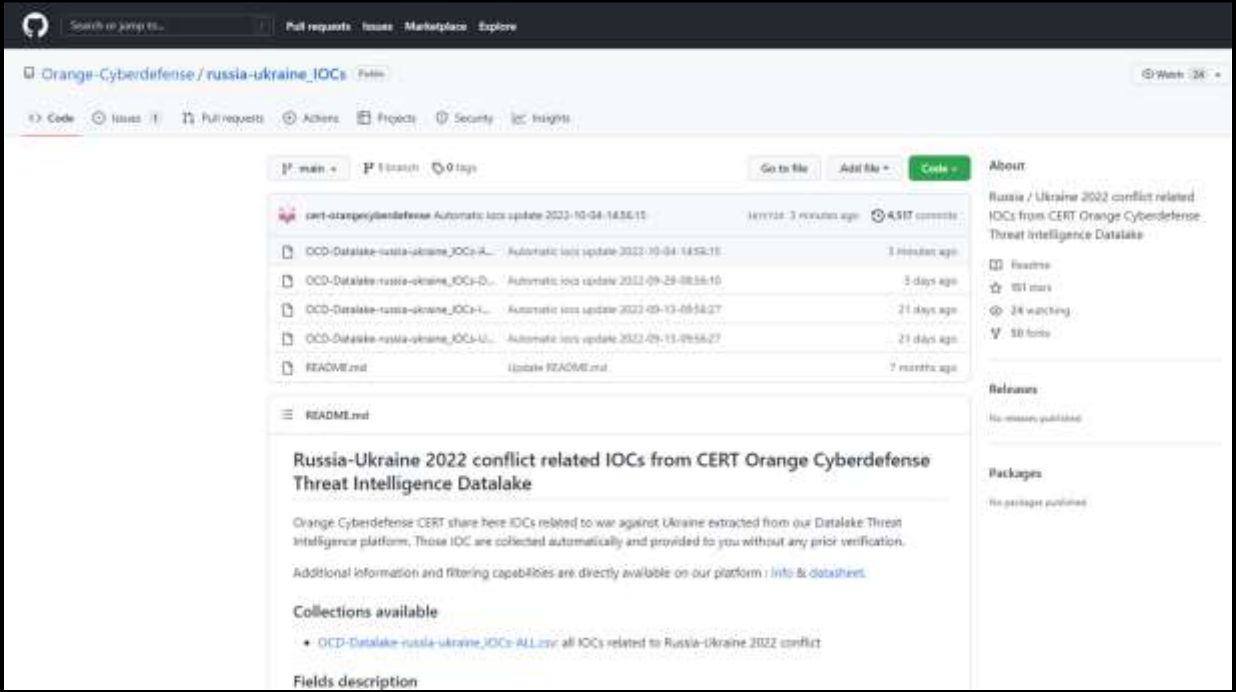


```
loc_401088:                             ; CODE XREF: _m
; register edi: argv
; register ebx: argv
; register esi: i
                xor     edx, edx
                mov     first, edx
                mov     ecx, [ebx+esi*4]
                inc     ecx
                push    ecx             ; file
                call    prc1
                pop     ecx
                mov     [ebp+code], eax
                cmp     [ebp+code], 0
                jz      short loc_4010FC
                mov     eax, [ebp+code]
                jmp     loc_401048
; ---------------------------------------------------------------

loc_4010FC:                             ; CODE XREF: _m
                push    offset asc_41D31F ; " #"
                push    offset line     ; "tlib /C/0/E
                call    _org_strcat
                add     esp, 8
                push    offset arname   ; "arfnp"
                push    offset line     ; "tlib /C/0/E
```

```
  _org_strcpy(libname, argv[2]);
  if ( isvc && _org_access(libname, 0) )
    _org_strcat(line, aOut);
  _org_strcat(line, argv[2]);
  i = 3;
  do
  {
    if ( *argv[i] == 64 )
    {
      if ( !first )
      {
        _org_fprintf(dword_41D870, aArOnlyOneIndi
        return 1;
      }
      first = 0;
      result = prc1((int)(argv[i] + 1));
      if ( result )
        return result;
      _org_strcat(line, asc_41D31F);
      _org_strcat(line, arname);
    }
    else
    {
      v13 = _org_strcat(line, asc_41D322);
      v14 = getswl(v13);
      _org_strcat(line, v14);
      _org_strcat(line, argv[i]);
```

Malware Analysis / Incident Response

1. Collection - *Sources*



Search or jump to...
Pull requests Issues Marketplace Explore

Orange-Cyberdefense / russia-ukraine_IOCs Public

Code Issues 1 Pull requests Actions Projects Security Insights
main 1 branch 0 tags
Go to file Add file Code

cert-orangecyberdefense Automatic iocs update 2022-10-04-14:56:15 · 3 minutes ago · 4,517 commits

OCD-Datalake-russia-ukraine_IOCs-A... Automatic iocs update 2022-10-04-14:56:15 3 minutes ago
OCD-Datalake-russia-ukraine_IOCs-D... Automatic iocs update 2022-09-29-08:56:10 5 days ago
OCD-Datalake-russia-ukraine_IOCs-I... Automatic iocs update 2022-09-13-09:56:27 21 days ago
OCD-Datalake-russia-ukraine_IOCs-U... Automatic iocs update 2022-09-13-09:56:27 21 days ago
README.md Update README.md 7 months ago

README.md

Russia-Ukraine 2022 conflict related IOCs from CERT Orange Cyberdefense Threat Intelligence Datalake

Orange Cyberdefense CERT share here IOCs related to war against Ukraine extracted from our Datalake Threat Intelligence platform. Those IOC are collected automatically and provided to you without any prior verification.

Additional information and filtering capabilities are directly available on our platform : info & datasheet.

Collections available

- OCD-Datalake-russia-ukraine_IOCs-ALL.csv: all IOCs related to Russia-Ukraine 2022 conflict

Fields description

About

Russia / Ukraine 2022 conflict related IOCs from CERT Orange Cyberdefense Threat Intelligence Datalake

Readme
151 stars
24 watching
50 forks

Releases

No releases published

Packages

No packages published

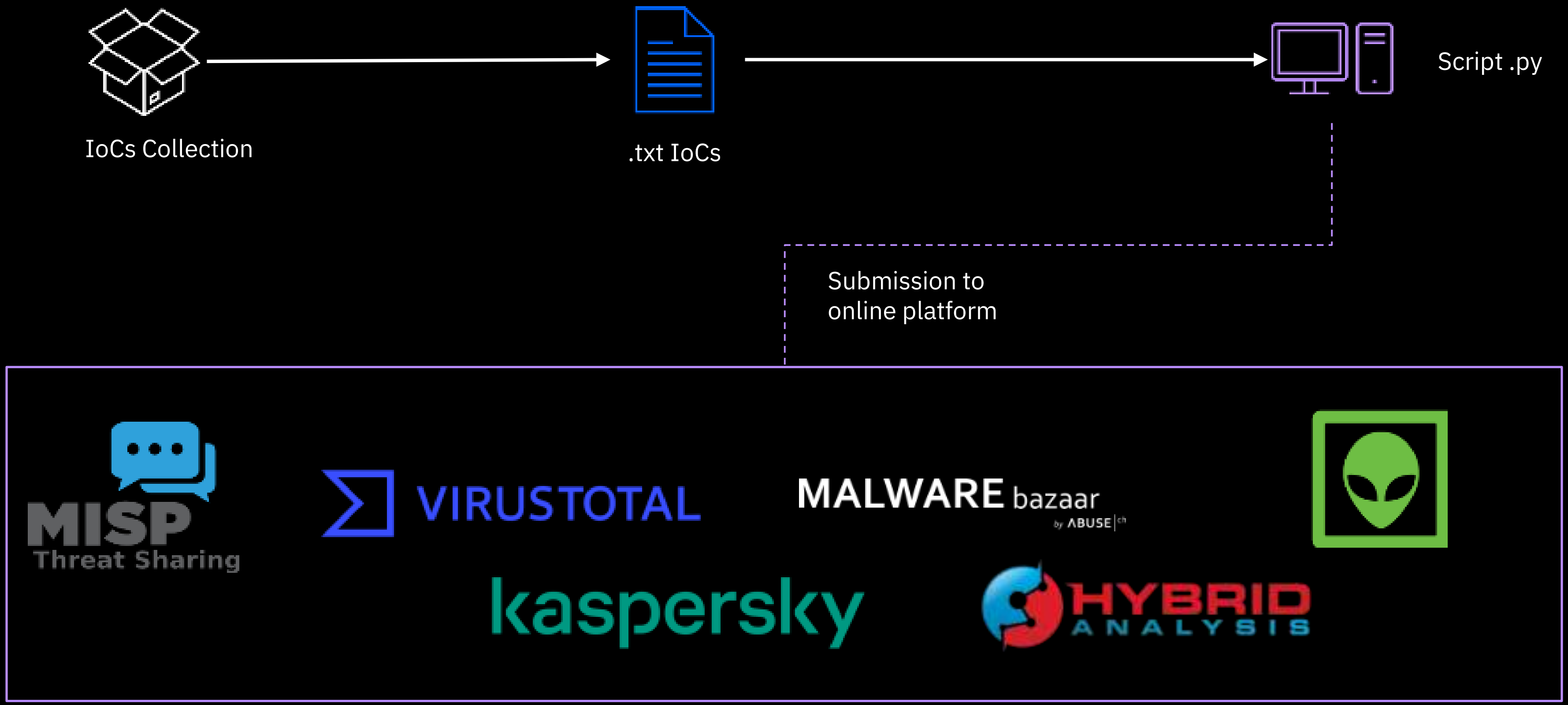
curated-intel/**Log4Shell-IOCs**

A collection of intelligence about Log4Shell and its exploitation activity.

7 Contributors · 0 Issues · 168 Stars · 36 Forks

Repository

2. Analyze Data



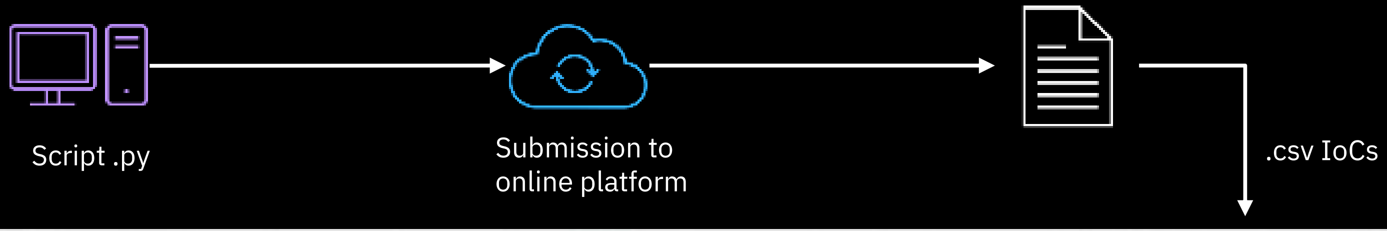
IoCs Collection

.txt IoCs

Script .py

Submission to online platform

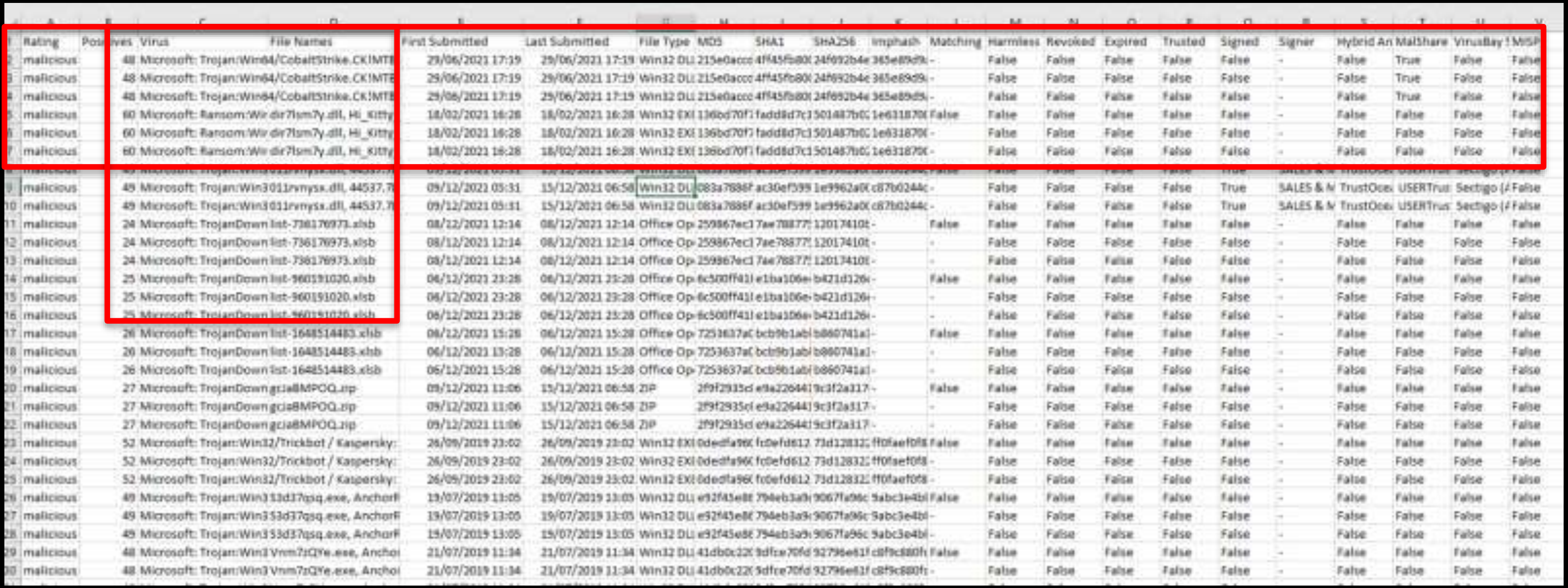
2. Analyze Data



Script .py

Submission to
online platform

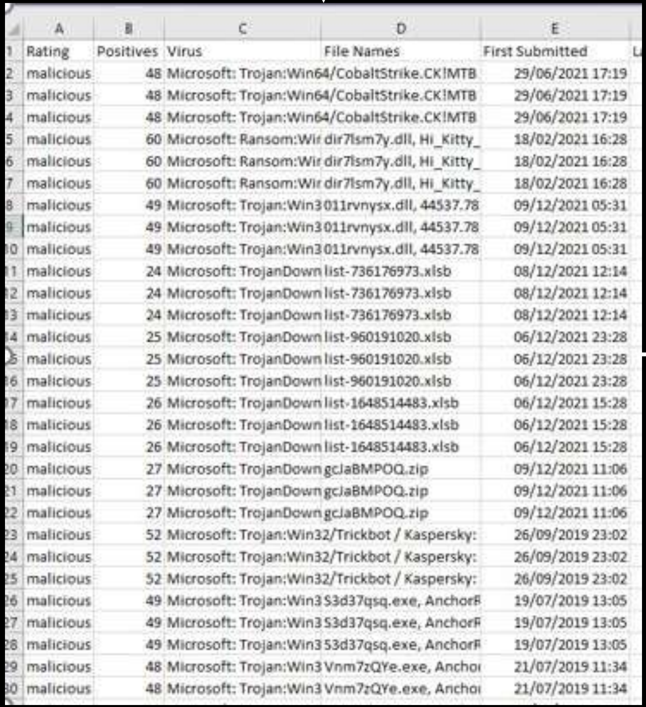
.csv IoCs



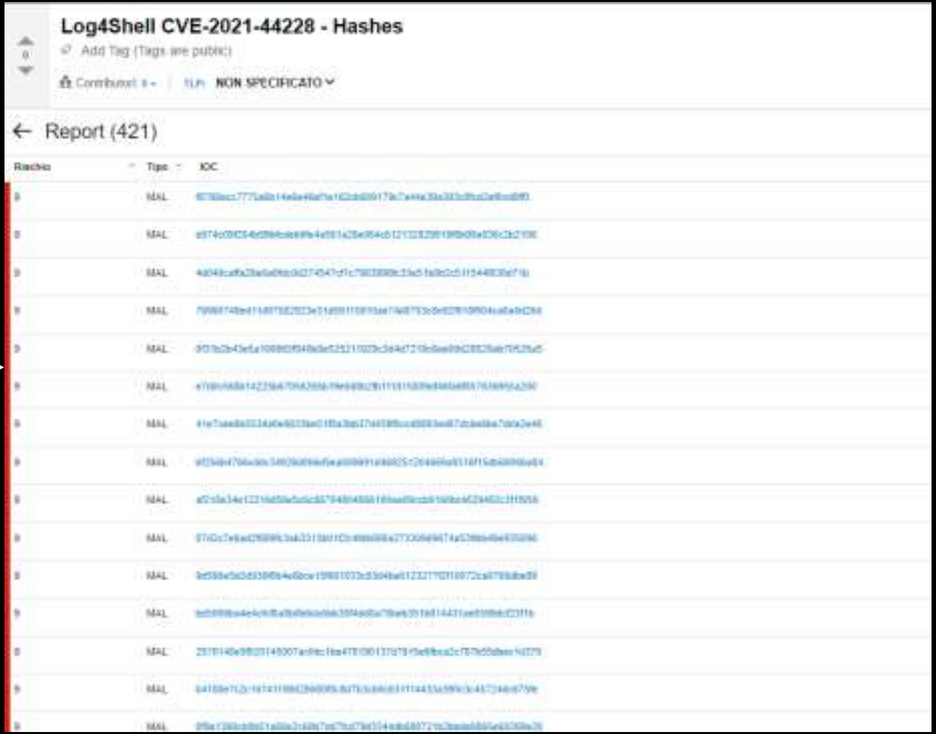
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
1	Rating	Positives	Virus	File Names	First Submitted	Last Submitted	File Type	MD5	SHA1	SHA256	imphash	Matching	Harmless	Revoked	Expired	Trusted	Signed	Signer	Hybrid An	MalShare	VirusBay !	MISP
2	malicious	48	Microsoft: Trojan:Win64/CobaltStrike.CK!MTE		29/06/2021 17:19	29/06/2021 17:19	Win32 DL	215e0accc	4ff45fb80(	24f692b4e	365e89d9	-	False	False	False	False	False	-	False	True	False	False
3	malicious	48	Microsoft: Trojan:Win64/CobaltStrike.CK!MTE		29/06/2021 17:19	29/06/2021 17:19	Win32 DL	215e0accc	4ff45fb80(	24f692b4e	365e89d9	-	False	False	False	False	False	-	False	True	False	False
4	malicious	48	Microsoft: Trojan:Win64/CobaltStrike.CK!MTE		29/06/2021 17:19	29/06/2021 17:19	Win32 DL	215e0accc	4ff45fb80(	24f692b4e	365e89d9	-	False	False	False	False	False	-	False	True	False	False
5	malicious	60	Microsoft: Ransom:Wir	dir7lsm7y.dll, Hi_Kitty	18/02/2021 16:28	18/02/2021 16:28	Win32 EX	136bd70f1	fadd8d7c1	501487b0	1e631870(	False	False	False	False	False	False	-	False	False	False	False
6	malicious	60	Microsoft: Ransom:Wir	dir7lsm7y.dll, Hi_Kitty	18/02/2021 16:28	18/02/2021 16:28	Win32 EX	136bd70f1	fadd8d7c1	501487b0	1e631870(	-	False	False	False	False	False	-	False	False	False	False
7	malicious	60	Microsoft: Ransom:Wir	dir7lsm7y.dll, Hi_Kitty	18/02/2021 16:28	18/02/2021 16:28	Win32 EX	136bd70f1	fadd8d7c1	501487b0	1e631870(	-	False	False	False	False	False	-	False	False	False	False
8	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	False	[illegible]	[illegible]	[illegible]	[illegible]	True	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
9	malicious	49	Microsoft: Trojan:Win3	011rvnysx.dll, 44537.7	09/12/2021 05:31	15/12/2021 06:58	Win32 DL	083a7886f	ac30ef599	1e9962a0(	c87b0244c	-	False	False	False	False	True	SALES & M	TrustOce	USERTrus	Sectigo (/	False
10	malicious	49	Microsoft: Trojan:Win3	011rvnysx.dll, 44537.7	09/12/2021 05:31	15/12/2021 06:58	Win32 DL	083a7886f	ac30ef599	1e9962a0(	c87b0244c	-	False	False	False	False	True	SALES & M	TrustOce	USERTrus	Sectigo (/	False
11	malicious	24	Microsoft: TrojanDown	list-736176973.xlsb	08/12/2021 12:14	08/12/2021 12:14	Office Op	259867ec1	7ae78877	12017410t	-	False	False	False	False	False	False	-	False	False	False	False
12	malicious	24	Microsoft: TrojanDown	list-736176973.xlsb	08/12/2021 12:14	08/12/2021 12:14	Office Op	259867ec1	7ae78877	12017410t	-	-	False	False	False	False	False	-	False	False	False	False
13	malicious	24	Microsoft: TrojanDown	list-736176973.xlsb	08/12/2021 12:14	08/12/2021 12:14	Office Op	259867ec1	7ae78877	12017410t	-	-	False	False	False	False	False	-	False	False	False	False
14	malicious	25	Microsoft: TrojanDown	list-960191020.xlsb	06/12/2021 23:28	06/12/2021 23:28	Office Op	6c500ff41	e1ba106e	b421d126	-	False	False	False	False	False	False	-	False	False	False	False
15	malicious	25	Microsoft: TrojanDown	list-960191020.xlsb	06/12/2021 23:28	06/12/2021 23:28	Office Op	6c500ff41	e1ba106e	b421d126	-	-	False	False	False	False	False	-	False	False	False	False
16	malicious	25	Microsoft: TrojanDown	list-960191020.xlsb	06/12/2021 23:28	06/12/2021 23:28	Office Op	6c500ff41	e1ba106e	b421d126	-	-	False	False	False	False	False	-	False	False	False	False
17	malicious	26	Microsoft: TrojanDown	list-1648514483.xlsb	06/12/2021 15:28	06/12/2021 15:28	Office Op	7253637a(	bcb9b1ab	b860741a1	-	False	False	False	False	False	False	-	False	False	False	False
18	malicious	26	Microsoft: TrojanDown	list-1648514483.xlsb	06/12/2021 15:28	06/12/2021 15:28	Office Op	7253637a(	bcb9b1ab	b860741a1	-	-	False	False	False	False	False	-	False	False	False	False
19	malicious	26	Microsoft: TrojanDown	list-1648514483.xlsb	06/12/2021 15:28	06/12/2021 15:28	Office Op	7253637a(	bcb9b1ab	b860741a1	-	-	False	False	False	False	False	-	False	False	False	False
20	malicious	27	Microsoft: TrojanDown	gcia8MPOQ.zip	09/12/2021 11:06	15/12/2021 06:58	ZIP	2f9f2935c	e9a226441	9c3f2a317	-	False	False	False	False	False	False	-	False	False	False	False
21	malicious	27	Microsoft: TrojanDown	gcia8MPOQ.zip	09/12/2021 11:06	15/12/2021 06:58	ZIP	2f9f2935c	e9a226441	9c3f2a317	-	-	False	False	False	False	False	-	False	False	False	False
22	malicious	27	Microsoft: TrojanDown	gcia8MPOQ.zip	09/12/2021 11:06	15/12/2021 06:58	ZIP	2f9f2935c	e9a226441	9c3f2a317	-	-	False	False	False	False	False	-	False	False	False	False
23	malicious	52	Microsoft: Trojan:Win32/Trickbot / Kaspersky:		26/09/2019 23:02	26/09/2019 23:02	Win32 EX	0dedfa96(	fc0efd612	73d12832	ff0faef0f8	False	False	False	False	False	False	-	False	False	False	False
24	malicious	52	Microsoft: Trojan:Win32/Trickbot / Kaspersky:		26/09/2019 23:02	26/09/2019 23:02	Win32 EX	0dedfa96(	fc0efd612	73d12832	ff0faef0f8	-	False	False	False	False	False	-	False	False	False	False
25	malicious	52	Microsoft: Trojan:Win32/Trickbot / Kaspersky:		26/09/2019 23:02	26/09/2019 23:02	Win32 EX	0dedfa96(	fc0efd612	73d12832	ff0faef0f8	-	False	False	False	False	False	-	False	False	False	False
26	malicious	49	Microsoft: Trojan:Win3	53d37qsq.exe, AnchorF	19/07/2019 13:05	19/07/2019 13:05	Win32 DL	e92f45e8	794eb3a9	9067fa96c	9abc3e4bl	False	False	False	False	False	False	-	False	False	False	False
27	malicious	49	Microsoft: Trojan:Win3	53d37qsq.exe, AnchorF	19/07/2019 13:05	19/07/2019 13:05	Win32 DL	e92f45e8	794eb3a9	9067fa96c	9abc3e4bl	-	False	False	False	False	False	-	False	False	False	False
28	malicious	49	Microsoft: Trojan:Win3	53d37qsq.exe, AnchorF	19/07/2019 13:05	19/07/2019 13:05	Win32 DL	e92f45e8	794eb3a9	9067fa96c	9abc3e4bl	-	False	False	False	False	False	-	False	False	False	False
29	malicious	48	Microsoft: Trojan:Win3	Vnm7zQYe.exe, Anchoi	21/07/2019 11:34	21/07/2019 11:34	Win32 DL	41db0c22(	9dfce70fd	92796e61f	c8f9c880f	False	False	False	False	False	False	-	False	False	False	False
30	malicious	48	Microsoft: Trojan:Win3	Vnm7zQYe.exe, Anchoi	21/07/2019 11:34	21/07/2019 11:34	Win32 DL	41db0c22(	9dfce70fd	92796e61f	c8f9c880f	-	False	False	False	False	False	-	False	False	False	False

3. Extract IoCs

Analyzed IoCs



	A	B	C	D	E
1	Rating	Positives	Virus	File Names	First Submitted
2	malicious	48	Microsoft: Trojan:Win64/CobaltStrike.CK!MTB		29/06/2021 17:19
3	malicious	48	Microsoft: Trojan:Win64/CobaltStrike.CK!MTB		29/06/2021 17:19
4	malicious	48	Microsoft: Trojan:Win64/CobaltStrike.CK!MTB		29/06/2021 17:19
5	malicious	60	Microsoft: Ransom:Wi	dir7lsm7y.dll, Hi_Kitty_	18/02/2021 16:28
6	malicious	60	Microsoft: Ransom:Wi	dir7lsm7y.dll, Hi_Kitty_	18/02/2021 16:28
7	malicious	60	Microsoft: Ransom:Wi	dir7lsm7y.dll, Hi_Kitty_	18/02/2021 16:28
8	malicious	49	Microsoft: Trojan:Win3	011rvnysx.dll, 44537.78	09/12/2021 05:31
9	malicious	49	Microsoft: Trojan:Win3	011rvnysx.dll, 44537.78	09/12/2021 05:31
10	malicious	49	Microsoft: Trojan:Win3	011rvnysx.dll, 44537.78	09/12/2021 05:31
11	malicious	24	Microsoft: TrojanDown	list-736176973.xlsb	08/12/2021 12:14
12	malicious	24	Microsoft: TrojanDown	list-736176973.xlsb	08/12/2021 12:14
13	malicious	24	Microsoft: TrojanDown	list-736176973.xlsb	08/12/2021 12:14
14	malicious	25	Microsoft: TrojanDown	list-960191020.xlsb	06/12/2021 23:28
15	malicious	25	Microsoft: TrojanDown	list-960191020.xlsb	06/12/2021 23:28
16	malicious	25	Microsoft: TrojanDown	list-960191020.xlsb	06/12/2021 23:28
17	malicious	26	Microsoft: TrojanDown	list-1648514483.xlsb	06/12/2021 15:28
18	malicious	26	Microsoft: TrojanDown	list-1648514483.xlsb	06/12/2021 15:28
19	malicious	26	Microsoft: TrojanDown	list-1648514483.xlsb	06/12/2021 15:28
20	malicious	27	Microsoft: TrojanDown	gclaBMPOQ.zip	09/12/2021 11:06
21	malicious	27	Microsoft: TrojanDown	gclaBMPOQ.zip	09/12/2021 11:06
22	malicious	27	Microsoft: TrojanDown	gclaBMPOQ.zip	09/12/2021 11:06
23	malicious	52	Microsoft: Trojan:Win32/Trickbot / Kaspersky:		26/09/2019 23:02
24	malicious	52	Microsoft: Trojan:Win32/Trickbot / Kaspersky:		26/09/2019 23:02
25	malicious	52	Microsoft: Trojan:Win32/Trickbot / Kaspersky:		26/09/2019 23:02
26	malicious	49	Microsoft: Trojan:Win3	S3d37qsq.exe, AnchorF	19/07/2019 13:05
27	malicious	49	Microsoft: Trojan:Win3	S3d37qsq.exe, AnchorF	19/07/2019 13:05
28	malicious	49	Microsoft: Trojan:Win3	S3d37qsq.exe, AnchorF	19/07/2019 13:05
29	malicious	48	Microsoft: Trojan:Win3	Vnm7zQYe.exe, Ancho	21/07/2019 11:34
30	malicious	48	Microsoft: Trojan:Win3	Vnm7zQYe.exe, Ancho	21/07/2019 11:34



Log4Shell CVE-2021-44228 - Hashes

Add Tag (Tags are public)

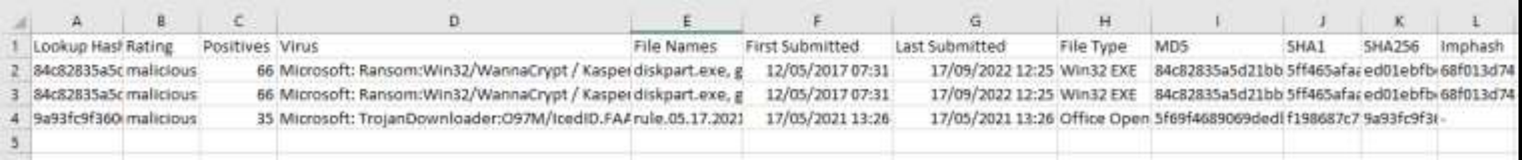
Contributori 8 ▾ | TLP: NON SPECIFICATO ▾

← Report (421)

Rischio	Tipo	IOC
[illegible]	MAL	[illegible]
[illegible]	MAL	[illegible]
[illegible]	MAL	[illegible]
[illegible]	MAL	[illegible]
[illegible]	MAL	[illegible]
[illegible]	MAL	[illegible]
[illegible]	MAL	[illegible]
[illegible]	MAL	[illegible]
[illegible]	MAL	[illegible]
[illegible]	MAL	[illegible]
[illegible]	MAL	[illegible]
[illegible]	MAL	[illegible]
[illegible]	MAL	[illegible]
[illegible]	MAL	[illegible]
[illegible]	MAL	[illegible]

4. Implement IOCs

Hashes results



	A	B	C	D	E	F	G	H	I	J	K	L
1	Lookup Hasl	Rating	Positives	Virus	File Names	First Submitted	Last Submitted	File Type	MD5	SHA1	SHA256	Imphash
2	84c82835a5c	malicious	66	Microsoft: Ransom:Win32/WannaCrypt / Kasper	diskpart.exe, g	12/05/2017 07:31	17/09/2022 12:25	Win32 EXE	84c82835a5d21bb	5ff465afa	ed01ebfb	68f013d74
3	84c82835a5c	malicious	66	Microsoft: Ransom:Win32/WannaCrypt / Kasper	diskpart.exe, g	12/05/2017 07:31	17/09/2022 12:25	Win32 EXE	84c82835a5d21bb	5ff465afa	ed01ebfb	68f013d74
4	9a93fc9f360	malicious	35	Microsoft: TrojanDownloader:O97M/IcedID.FA	rule.05.17.2021	17/05/2021 13:26	17/05/2021 13:26	Office Open	5f69f4689069dedl	f198687c7	9a93fc9f3	-
5												

Import in Cyber Security Solution

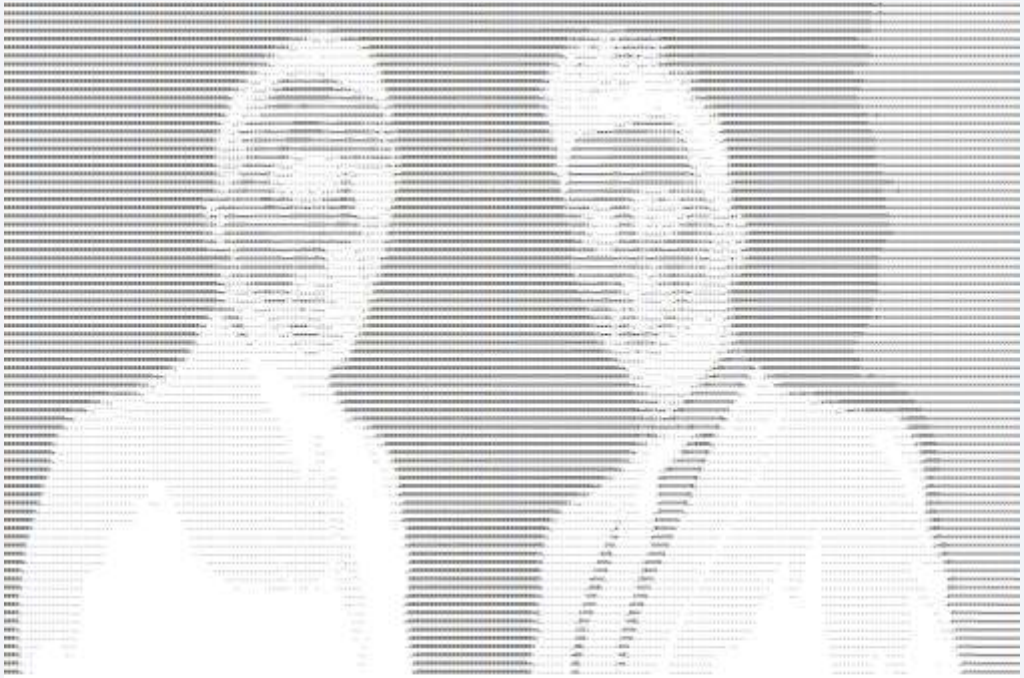
Create IDS rules on Suricata and import them

SURICATA

Create a custom rule on Wazuh Manager

WAZUH

Thanks to All!



Vincenzo Di Lello

Pietro Melillo

melillopietro.github.io