

A white outline icon of a folder with a tab on the left side.

BRIEF

Russia-Ukraine Conflict: Cyber Updates on APT Activity

ZEROFOX INTELLIGENCE

B-2022-03-08a

Classification: TLP Amber

Criticality: High

Intelligence Requirements: Malware, Deep Dark Web & Criminal
Underground

March 8, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 11:00 AM (EST) on March 8, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Russia-Ukraine Conflict: Cyber Updates on APT Activity

Executive Summary

The Gamaredon Group is one of the most active, existing advanced persistent threats (APT) targeting Ukraine and has been pursuing access to organizations in Ukraine or entities related to Ukrainian affairs since at least 2014. Given its pro-Russian activities, ZeroFox anticipates additional malicious cyber activities against targets in Ukraine and the West, as geopolitical tensions continue to be unresolved. Since February 1, 2022, ZeroFox has observed over 470 Indicators of Compromise (IOCs) associated with the group's infrastructure. This is an extremely aggressive APT group with little or no reduction in its activity.

Details

This threat actor group has historically focused its offensive cyberattacks against Ukrainian government officials and organizations. In 2021, Ukraine disclosed Gamaredon's ties to Russia's Federal Security Service (FSB).¹ In the Russia-Ukraine conflict, the Ukrainian government has alleged that Gamaredon's main objectives include controlling critical infrastructure; stealing and collecting intelligence and classified information for geopolitical gains; conducting "operations of information and psychological influence"; and blocking access to information systems.² The Gamaredon Group frequently leverages spear-phishing emails to deliver common remote access tools (RATs), including UltraVNC and Remote Manipulator System (RMS). ZeroFox observed the use of the Pteranodon backdoor with over 230 IOCs between February and March 2022. The trojan is often used for espionage-related operations, as it can collect data by taking screenshots of the victim's desktop. This threat also can be used to deploy additional malware on the infected host by utilizing its backdoor feature. The group primarily makes use of compromised domains, dynamic DNS providers, Russian and Ukrainian country code top-level domains (ccTLDs), and Russian hosting providers to distribute its custom-built malware. The group has also

¹

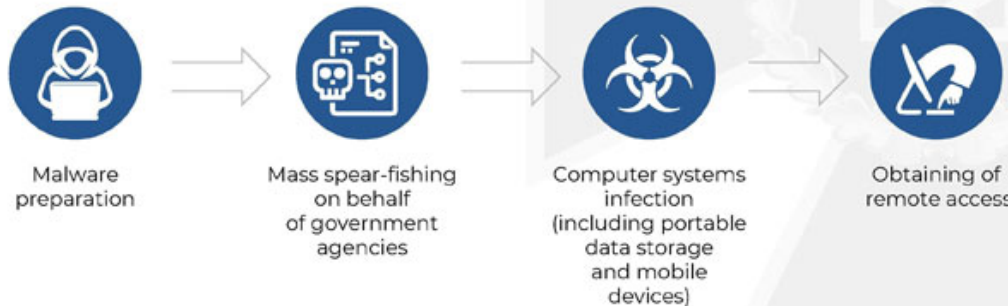
<https://ssu.gov.ua/en/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy>

² <https://www.cyberscoop.com/ukraine-russian-hackers-armageddon-videos-gamaredon/>



been found to recycle its used domains by consistently rotating them across new infrastructure, which is a unique tactic among threat actors.³

Penetration by the hacker group was carried out by mass distribution of malicious software, **which was disguised as official electronic correspondence of the authorities of Ukraine**



Gamaredon attack mechanism, as captured by the Security Service of Ukraine in 2021

Source: <https://thehackernews.com/2021/11/ukraine-identifies-russian-fsb-officers.html>

Analyst Commentary

Gamaredon has long been associated with pro-Russian activities, however, security researchers are split in their classification of the group as an APT. Gamaredon's information-gathering activities are often classified as a second-tier APT; the group's main objective is to gather information to share with its smembers, who will eventually use that data to perform the end goal. Gamaredon's TTPs are in line with cybercriminal groups' activities; the group uses off-the-shelf tools and a large number of domains across its campaigns, which are tactics not typically associated with APT groups. While the group has previously demonstrated its global reach, it nonetheless continuously pursues Ukrainian targets. Ukrainian government sources have blamed the group for more than 5,000 cyberattacks on Ukrainian state entities and critical infrastructure that attempted to "infect" more than 1,500 government computer systems to date.⁴ In February 2022, cybersecurity researchers reported that Gamaredon had attempted to compromise an undisclosed Western government entity operating in Ukraine through a January phishing campaign. The threat actors leveraged a Ukrainian job search and employment platform to upload a malware downloader masquerading as a candidate's resume in response to a job advertisement that was posted by the targeted organization.

³ <https://thehackernews.com/2022/02/russian-gamaredon-hackers-targeted.html>

⁴

<https://www.washingtonpost.com/politics/2021/11/05/cyber-bipartisanship-may-fracture-over-regulations/>



Recommendations

The best defense against this persistent threat group is a security posture focused on prevention. ZeroFox recommends that organizations implement the following:

- Search network and endpoint logs for any evidence of the IOCs associated with this threat group.
- Monitor and log network, workstation, and server activity and alert on all suspicious events.
- Strong perimeter defenses, such as firewalls and antivirus, are a key part of preventing APT malware from being installed on computer systems.
- Create and maintain a regular patch cycle policy, allowing the necessary time for testing and gradual rollout of the most critical systems.
- Create, maintain, and exercise a basic cyber incident response plan and an associated communications plan that includes response and notification procedures.



Appendix A

IOCs Observed Between February and March 2022

DOMAINS:

accordan[.]ru
adleer[.]ru
alibetar[.]ru
aligatou[.]ru
alseid[.]ru
anits[.]ru
berezini[.]ru
bikestr[.]ru
bikortas[.]ru
bolotran[.]ru
buffalor[.]ru
calendas[.]ru
corintar[.]ru
cryptonas[.]ru
dambart[.]ru
danirat[.]ru
deep-six[.]gortomalo[.]ru
diletras[.]ru
distorhan[.]ru
domasq[.]ru
doriga[.]ru
doscotra[.]ru
drumtar[.]ru
dushnilo[.]ru
eidoloni[.]ru
engardos[.]ru
ericsoni[.]ru
faroinh[.]ru
filikato[.]ru
filopar[.]ru
firasoska[.]ru
fortitat[.]ru
fortuskan[.]ru



fukakumog[.]ru
gaderu[.]ru
gartisop[.]ru
genkai[.]ru
giboltar[.]ru
giltorad[.]ru
giroed[.]ru
glotrast[.]ru
golitrap[.]ru
golitus[.]ru
goloser[.]ru
gongorat[.]ru
goruda[.]ru
goshita[.]ru
gotpnib[.]ru
haguret[.]ru
hikorta[.]ru
hikorto[.]ru
hilotrapa[.]ru
hilotras[.]ru
hiskolan[.]ru
historyna[.]ru
hokoldar[.]ru
holorotop[.]ru
holotras[.]ru
holpantra[.]ru
hostarama[.]ru
hotilar[.]ru
hotornas[.]ru
hustorta[.]ru
ibigao[.]ru
idaite[.]ru
ienaike[.]ru
ishinde[.]ru
jenipot[.]ru
jistarka[.]ru
jokrista[.]ru
jolopar[.]ru
jortiska[.]ru



jupirest[.]ru
karamono[.]ru
kassanfo[.]ru
keiwakaw[.]ru
kibou[.]ru
koete[.]ru
kofukaku[.]ru
kolopart[.]ru
koloparto[.]ru
kolotara[.]ru
koltorist[.]ru
korgant[.]ru
koutora[.]ru
kovalsko[.]ru
kukarat[.]ru
legasto[.]ru
leonot[.]ru
lestori[.]ru
libasti[.]ru
machiwo[.]ru
mafdis[.]ru
marisut[.]ru
mavzolit[.]ru
mihardo[.]ru
milopoda[.]ru
milotor[.]ru
mirabits[.]ru
mirtokla[.]ru
miyago[.]ru
molortasa[.]ru
moonilar[.]ru
motteiru[.]ru
mtageri[.]ru
nakona[.]ru
nalitoras[.]ru
nastorlam[.]ru
nbator[.]ru
nintara[.]ru
noiiano[.]ru



nokitrav[.]ru
nokratis[.]ru
nolortasto[.]ru
nostikarta[.]ru
nukegaran[.]ru
omona[.]ru
optivan[.]ru
padiska[.]ru
pokolas[.]ru
polonti[.]ru
portalahr[.]ru
postoral[.]ru
potrahid[.]ru
potrosiha[.]ru
powerton[.]ru
printinap[.]ru
raidata[.]ru
retarus[.]ru
richia[.]ru
ringali[.]ru
riontos[.]ru
sadotra[.]ru
saihate[.]ru
samayoi[.]ru
sarium[.]ru
scorpiones[.]ru
seigaiso[.]ru
seitoshi[.]ru
selotra[.]ru
sertopar[.]ru
shaparto[.]ru
sikolra[.]ru
simfopar[.]ru
skriptan[.]ru
somebodar[.]ru
soredake[.]ru
tagdesam[.]ru
taramiet[.]ru
terminar[.]ru



tirotar[.]ru
titolora[.]ru
tofordat[.]ru
torohota[.]ru
tsukiru[.]ru
tsuzuketa[.]ru
turikar[.]ru
uchkuduko[.]ru
uharun[.]ru
usherfat[.]ru
utemomac[.]ru
vartogal[.]ru
verusa[.]ru
vidarri[.]ru
videotri[.]ru
vivaldar[.]ru
vodagi[.]ru
vostilo[.]ru
wakatteru[.]ru
xantoma[.]ru
zeinar[.]ru
zerotask[.]ru
znakort[.]ru
Zygost[.]ru

HASHES:

002e1b63a76a7125772cbf2ffd69e80d4d6491d72376ff04dafeb8c3cdc43831
029005b595c5b9f3c7ddb49883b325f8f0bf5d13b18010a38d04b15f227d2052
043d696c2199d61ee0a09be93e387498c6a53188c3e3ec20acfeccc9c9aeb251
07698f9b727daec99c446525aca889fc086e3cf6e3c307afdd72adff0113ceb0
0869881422aa20a93eb4567794d9c8bac175dcbb02e4e3f5591a81266ca94102
0911c20a123b21c077a12b43914ff2f8a1bccf5a983d0561004cf86a27b5154a
0afce2247ffb53783259b7dc5a0afe04d918767c991db2da906277898fd80be5
0e00837d95eac249c831e1bae314ea9aa1ac3a60e3fc018eb81f6e14e822b6c5
0e5b4e578788760701630a810d1920d510015367bf90c1eab4373d0c48a921d9
0fb55f55ffca9927472f7ada8fdd9d84bc57108860be0f1c737d5111d3020b5a
1164ba0688458c44b2063894100ecdc52221eb85b82a5044c55043e7918d4a19
15099fc6aea1961164954033b397d773ebf4b3ef7a5567feb064329be6236a01
182ec5f3859a78ce0c42995ecf63a0e412ff189b02b57a20057d2886a9098d88



1d8a5b468c90eeb8d6787a2578e840c1f1ff275819fa2dd54d8072304b315178
23725c0994c065d9221fa3d6a91eb0693410dd2585c835c935db04b812b1486f
23d417cd0d3dc0517adb49b10ef11d53e173ae7b427dbb6a7ddf45180056c029
2407793f8bd2b4f3b9b14c4227b6110e48bb0b5388d181cf9eaa9585f4d595b1
280a55919e502ecb66082107374e5b71a534338a8a7c02680cc4f1f84a204d59
283937afa83ac2bfc38f8bb3478704ae65f372b52809def5782a697d1dbf4fd3
28c5629b18b097015ef8c256a8a7f2019ddc1a362a92a0379dd5d0c98b0e33d3
2cf0408ed2819bbdb36b2fd113c64339ceee893dce971e723de3d01a3e3dadbb
2ef4275e4ca83f726839c7de922d8d60c3d1df292275f2a0afb252ef109aed42
304de8f4548cb616c97fcc841132a704f449c5dae709e7d1fb25810e7136cb46
32df8c49d6f89722c6aca8943883cfff3cdf34074e87ff48f7c96da5d732c02b
352b5ec506823ffc008e7b71b2968a282ea6ac08cf372ac23cc87d957ecbd889
367117e3acf6317b4cec64e514d461f9e761146aca0cb6eed9ef5a1fb35b63cc
3974f0b347dd42c5bd9d695a965f2fdd5a03b232702cb1162aad11307b68b6d7
3aac1c049eb628e1c289d3fc3a209f9262ed4cef862a3e2157bd6f3b02cc4698
3b6445cf6f8e9e70cb0fff35d723fec8203375d67cbd67c9a672cddc02a7ff99
3bab73a7ba6b84d9c070bb7f71daab5b40fcb6ee0387b67be51e978a47c25439
3dca96ef38d4b8d1dbb4afed43a22ace93cc3a0a105120d4cf637e6dafe129e9
3e1d17efe857c935869fc28ce94c3528f7f5232fceb40442a7c3c388e3d69be
3e273cec5fd77784c72f90018f11e0690387c9fde93defca16a971c8396f64df
3fede347c45eccd0967431b7496672d43b057a3a3e42dc2922421cb7f2457d43
42f8223ba588d510e2f2a00ca6500ba1b71684509f10695a156069876600ccdc
490365b7579861fdef91aff3d83a1972657a35505b193f363b934faa7955132c
4b7aecb006b8d3543265fc051e9b435bc0a8bb2698d5351604263e52a0af4a7c
4e9c8ef5e6391a9b4a705803dc8f2daaa72e3a448abd00fad36d34fe36f53887
5339f3468fa4bbb6b10073289b6cfe18b28b1db9c9d5e72c810e0435b1668e9f
535f533b1008a55c89cab7f4d4163e609d0d6e5b512002022d2634e74e84edf9
5440415c4a1702084a7c49b7024d0c75b9528b71d1faa4c744e95435dad6b533
5c8e7b35e40fc6613a8ec304f36c9ea1986a51c65a0389445f90778e94fa15ed
6126072bac10935b539660b9879097889c52070816ecb3042f54c1d563bac6e0
61e67302a85ff98eabc589572dbf3bf6e1012207d399b9f2b6b38527833e9198
63f3112aca7c36772caf6c6482e4faece639035818be8f236e5f3f7b84ac420c
652d9bc90cc1833f667508c7f794237a0945c875c61370e54c73073ba27e7c85
6705f4b9ffabbf9f4a9b112286f194a05fe593e6076c5fcf9296624042823265
695fabf0d0f0750b3d53de361383038030752d07b5fc8d1ba6eb8b3e1e7964fa
6d4b97e74abf499fa983b73a1e6957eadb2ec6a83e206fff1ab863448e4262c6
72086e3e2992e60f2fdd35049653478db397cad5b81c59789ce0aae0590ce78b
72b7609e0871eb7418d64e38cb40d74dda17356c96572fcd524f8bd22274af4a
74cb6c1c644972298471bff286c310e48f6b35c88b5908dbddfa163c85debdee



798cd714cf9e352c1e9de3d48971a366b09eeffb3513950fd64737d882c25a38
7c7c8548b7657c34e2b654919edbe848d460ab93630021e8e9743f8204cb0c76
849c372906c0f9815832e8178a829b5196150bc402a0aa081e5621f336508292
8762522851f33de2707725cd7a89879c0b0afb32bd34e2ac4443e4cbf285640
884c15502dbd6fe6dd4fca322904a38bce117ab6ed102ab2da84dfb4064c3e44
8a8c1a292eeb404407a9fe90430663a6d17767e49d52107b60bc229c090a0ae9
8a9f45e819513fd02aa0521aea3a0d85490c91523227b130d7ff08d12b8820ae
8d27a625c033baf16a0c8cc1b32e5ab3720525d87b1f63e328e32bf60b03740a
8ed03b1d544444b42385e79cd17c796fefae71d140b146d0757a3960d8ba3cba
93f3ff62452444c6c93f708ec9c110cfb0c630f462ea63db9abbe96a6053acb1
96b9a11f2b4f8051083643da6bdc9e3952a91ad3f882cde2e4a8910726ffc09c
96ce576f383584e0a62225a91bb50fc7fd8efa068443c4785373c86f51d2e3eb
986905caada61f2ea4aebd5664ed71cc9109a3886b998d91433216f30dc6b0e7
9a9d8cd54ee439d781ba9499ac1d4a878007c995f59f72ccaad4a7a6c3793938
9d085a26813cd1aa43e12d9b90aeb24df6269db92b965f61d93a8018d6b8a0cf
a01e12988448a5b26d1d1adecc2dda539b5842f6a7044f8803a52c8bb714cdb0
a123c8bc9bb6a7254764aa69928d2fec6784493eb5904683636b369507124710
a60df90504735f4e424ec0842e328181d7e93ac9ecd8193e892584871643bec7
a67e5d562e754426e061c74b04af19d8f59a9bfe5134d5bb6ed4d429d022840a
a6867e9086a8f713a962238204a3266185de2cc3c662fba8d79f0e9b22ce8dd6
ac4ea751ca1382550efb2d3f4df9242f4541836b0e82deb49847f763afdf20ca
af67c332c95d045f4847b06e70ed590d492ecf0e59da0244d117b02bb04cfc5a
afcbaae700e1779d3e0abe52bf0f085945fc9b6935f7105706b1ab4a823f565f
b27372960d28d3f36c93988a0b6df9d3f8211b2a252cd375e179bb8a9b54559b
b3d68268bd4bb14b6d412cef2b12ae4f2a385c36600676c1a9988cf1e9256877
b6ff96193514aa11b6fc0e5d58e7dcdccedfa373ee4858a2da582e4eceae86c5
b7a814deba56c6905c72d744d02398d46b34e9d1d7d02b5a501b1bddaf566407
b92dcbacbaaf0a05c805d31762cd4e45c912ba940c57b982939d79731cf97217
b9dd1e5ec018090b404dd7550d4423ff38ee1f016a5ab214f128544f5b399759
ba96cfe58a5c8f4636b0a0668a9d9127eee3ed80c96db48d3a63ae9c6ce97b2d
bae9895ad4e392990a09b1b8a01e424a7ad3769e538ac693919d1b99989f0cb3
bb1c8ad9f422a39ce6329e93dc060438
c05f4c5a6bb940e94782e07cf276fc103a6acca365ba28e7b4db09b5bbc01e58
c5248a00ccee03a159fff2e30709c3b23fb47faa811959d3249bc347f7e34a80
c6236e293e6dc2ec419d24e81d810dc16a7dc162d8e5fc19e5c44b44f4819a18
c66ce9f228c9065a90b22bd71363a81d1a8f1d26eb5fe3815046eb42b72c0d5f
c6e092316f61d2fc9c84299dd224a6e419e74c98c51a44023f8f72530ac28fdc
c77fb3d3053958ea3aa4419e2bf4d0caf14f6c74047216e789628d095cc9e733
cb0d151d930b17f6376c18aa15fd976eac53d6f07d065fc27c40b466e3bc49aa



cb4963fb3a85766278426ebf4a00ae5c5d7576f21b35cfa0df1f9529073015a9
cbe1dbd167bccbf61ee8608092a767ce3fbfb5fe5f6e959848d9a8d9091402fb
ccd5f196de54ac8ba5d5c3612f8807091f6c23dd501fa64161a161849f65f2a2
ce02bba7857842bee8eb490ae2971926c9e0412dbd1efc5a2c173fc7f59bd1d2
d2d3a5b67e275e7805f3216cb8d59cb8cfbd39798115ca504c5ad865a4fe52fb
d60a4dfc2c48fd80957ee77ab0ec4221f67e3f92551c9c245292f56dbaf9912e
d7eb0d9cb1709f8e32827bc8d7ba93aa8b6cf55ac43917caeb08b76ba3d7e3c1
d93551a9fa3ad9bdbb0f10dd447046e03a29bbb36245ac4245b80d982a78a930
d9ca10667cbffcbf1caa8b9020a93cfd
dddd77f42bfb365f36762ad4db4a741e
df70346afd410d3ba26eeeb0194fc7e6d427bfafef9a34b9efd49936ca9e273b
e3e98ec10a1ae7ce3c37cd6d4e79d12d9bbdelac382809d17917786253cd7265
e3eb6e9bc8321adb844e30606ed275a4
e4d309735f5326a193844772fc65b186fd673436efab7c6fed9eb7e3d01b6f19
e56254b6b78f0bdc82cddff15c49f5b56ffef9aa105f1aae435504d1cdfef3310
eb1724d14397de8f9dca4720dada0195ebb99d72427703cabcb47b174a3bfea2
ee818a51cc890bf80e81523a051c82293d6c57acf47f8ddccd667d12fc88cb45
f08c54c4d8a470f96a0acf6aefeb95c49a8704a473d6105a921a18917e1747fa
f211e0eb49990edbb5de2bcf2f573ea6a0b6f3549e772fd16bf7cc214d924824
f8dcd730cd06b18dc109473b7dac83c4f74f5c0c864cecc80bbf9e8bae974d8e
fd204f552fcc0fc8d63650302742c2d9e32175eb9675f5e57eeb2012816519d5

IP ADDRESSES:

104.238.189.186
109.200.159.45
124.15.125.1
151.248.116.243
176.118.164.124
176.57.208.203
178.20.44.214
185.193.143.11
185.20.226.9
185.251.91.137
185.46.10.28
185.46.10.73
188.225.42.206
188.225.43.174
188.225.44.181
188.225.44.76



193.164.150.111
194.58.121.94
194.67.109.14
194.67.109.76
194.67.110.89
194.67.116.180
194.67.86.240
194.67.90.15
217.69.0.35
217.69.4.51
31.31.203.17
31.40.251.171
37.140.199.20
37.140.199.224
5.63.158.233
80.78.245.223
80.78.251.191
83.166.247.110
87.249.49.103
89.108.115.241
89.108.76.226
89.108.78.126
89.108.78.128
92.242.62.181
92.242.62.254
92.255.76.169
94.228.120.181
94.250.251.39



Appendix B

Traffic-Light Protocol for Information Dissemination

Color	When Should It Be Used?	How May It Be Shared?
RED	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
AMBER	Sources may use the TLP: AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization and only as widely as necessary to act on that information.
GREEN	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.
WHITE	Sources may use TLP: WHITE when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.	TLP: WHITE information may be distributed without restriction, subject to copyright controls.