Pulse Report:
Insikt Group Discovers Global Credential Harvesting Campaign Using FiercePhish Open Source Framework

Recorded Future's Insikt Group discovered a wide-reaching phishing campaign utilizing the FiercePhish open source offensive phishing framework. The campaign, which is hosted on Russian domain infrastructure but does not target users in Russia, is globally harvesting credentials from a variety of organizations in the public and private sectors. This campaign, coordinated using asherintartrading[.]com, has been active since at least December 2019 and has cycled through over 30 DigitalOcean IP addresses, sometimes in a matter of hours. The fast changes in infrastructure indicate that the threat actor is proficient in evading security defenses and blocking tactics.

Analysis of a screenshot of asherintartrading[.]com was taken on the day the domain was first created on December 27, 2019, and shows the domain was configured as a FiercePhish management portal.

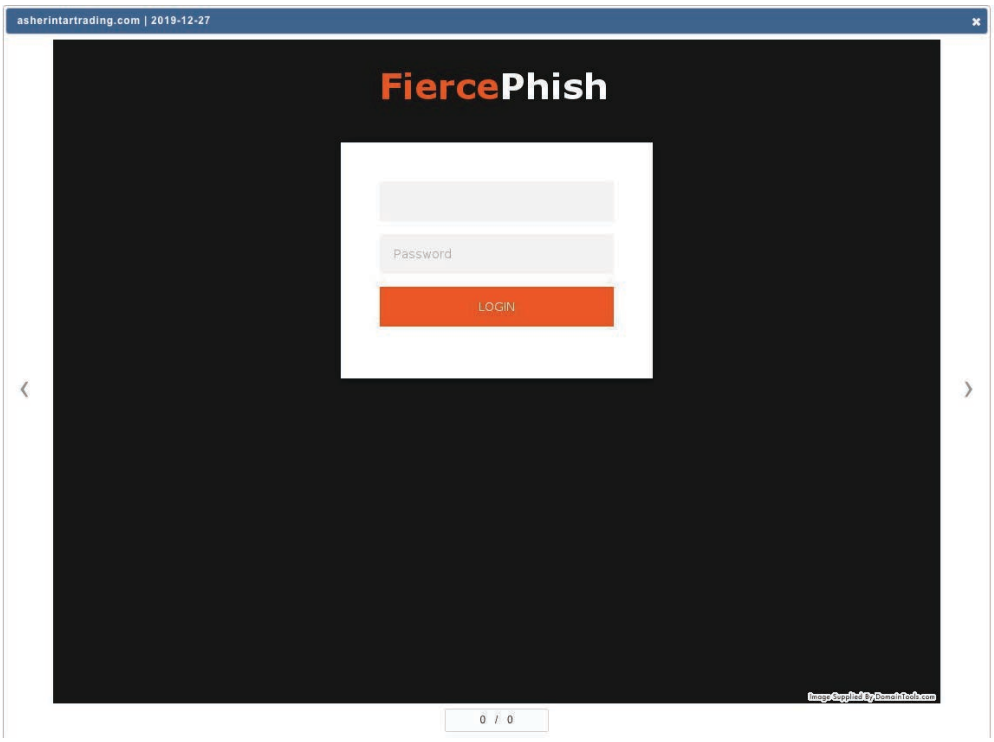


Image source: DomainTools

FiercePhish, created by Chris King, is an open source phishing framework designed to manage phishing engagements and is popular with ethical and non-ethical hackers. King's social media bio states that he is a Red Team Manager and Lead at Mandiant, as well as an open source developer. . Use of the FiercePhish framework in this campaign highlights the continued prevalence of offensive security tools being used for malicious purposes.

Infrastructure Analysis

Between August 28 and September 3, 2020, Insikt Group identified the malicious domain, asherintartrading[.]com, and began to track historical threat data related to the domain, including a copy of a phishing message sent by "root@asherintartrading[.]com" to an email account affiliated to a foreign diplomatic office in Uganda on July 15, 2020. SMTP headers show the email was sent via mail.asherintartrading[.]com and the email body was formatted in HTML.

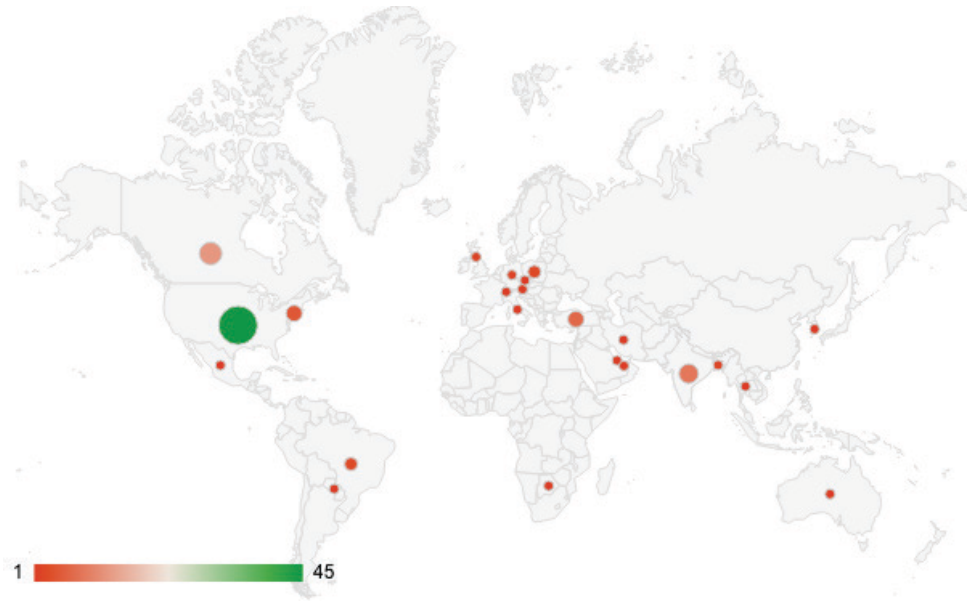
```
Protocol:       hXXps:
Hostname:       levidom[.]ru
Path name:      /zxcv/
Arguments:
        procardid = 9539856
        userid    = [[-Email-]]
        source    = 3Dgmail
        ust       = 3D1594249668042000=
        usg       = 3DAFQjCNFy16NCB-qy7QJHZ86vhApggpqfdQ
```

The email was designed to harvest email credentials by duping the target to re-enter their login details on a tailored spoofed Gmail login page hosted on https://filminglocationwanted[.]ru. The campaign included two other .ru URL's coded into the message: v88779.ht-test[.]ru, and levidom[.]ru (image below), the latter of which is a second credential harvesting link that also prompts the victim to enter their details when attempting to "unsubscribe" from the message.

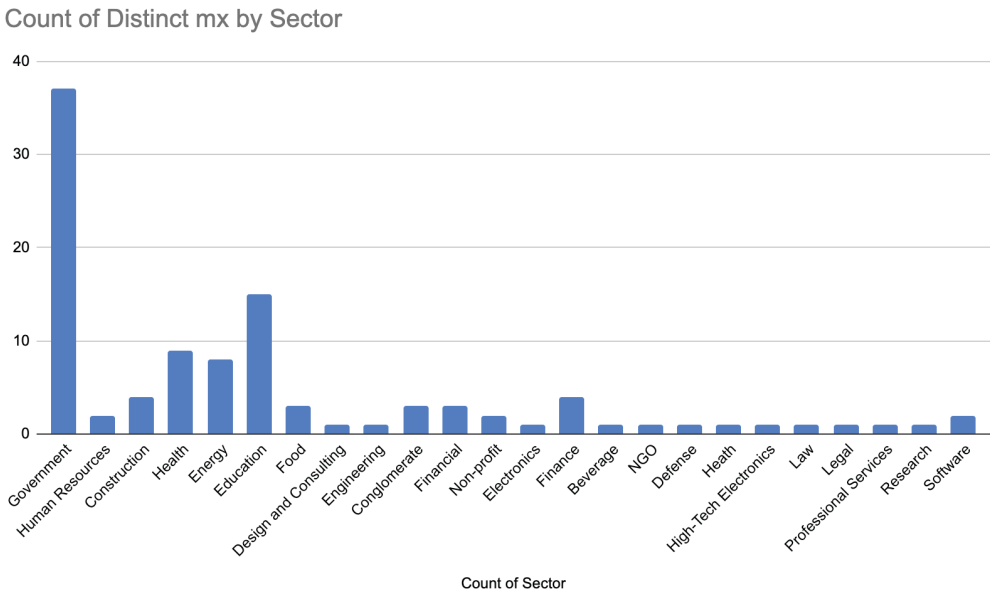
Insikt researchers identified over 200 similarly constructed domains and URLs (see Appendix A), some of which were already tagged as phishing or spyware-related in VirusTotal. These domains and URLs are highly likely engaged in malicious credential harvesting phishing activity related to the "asherintartrading" campaign.

Target Analysis

Recorded Future network telemetry shows that the "asherintartrading" infrastructure was used extensively for phishing activity, with a high volume of SMTP traffic. Our data reveals that almost two thirds of all companies' and organizations' mail servers that received phishing emails from the "asherintrading" campaign were within the government, education, finance, heath, and energy sectors, with organizations in the U.S, Canada, India, and Turkey making up the largest portion of targeted countries.



Breaking this down further, both local municipalities and federal level government organizations, primarily in the U.S. and Canada, were targeted as well as global intergovernmental organizations.



Government organizations in the UK, Turkey, Qatar, Republic of Korea, India, UAE, and Australia were also targeted. Further analysis also reveals that the vast majority of phishing emails were sent to the government sector. Recorded Future data does not confirm that the target organizations were successfully compromised. However, the presence of some of these indicators in VirusTotal may indicate that some organizations are aware of and defending against this campaign.

Defense and Action

Given the wide scale of this phishing campaign, Recorded Future recommends customers configure their network defenses to alert and block on the domains, URLs, and IPs listed below. We also strongly recommend network defenders to check enterprise email logs, SMTP headers, message ids and similar datasets for messages sent from any email address tied to the domain “asherintartrading[.]com.”

Appendix A (Indicators)

asherintartrading[.]com
mail.asherintartrading[.]com
22hotmail[.]ru
9girls[.]ru
addosports[.]ru
agenziapieropanwit[.]ru
airiseurope[.]ru
alexpwru[.]ru
allinsgrp[.]ru
allisonpyep[.]ru
americangrowthfund[.]ru
apmeukwcowuk[.]ru
asianmoviesfree[.]ru
auqzzx[.]ru
autojanwcz[.]ru
backupmdwnet[.]ru
baolekangwcn[.]ru
berndseneconste[.]ru
biologikawco[.]ru
blogagewde[.]ru
bloomhospital[.]ru
bolsasymofei[.]ru
bucktickets winfo[.]ru
callpointe[.]ru
capequilog[.]ru
clubaddisoed[.]ru
colombiavozwnet[.]ru
computersiteswnet[.]ru
confized[.]ru
crediteure[.]ru
cvjmebraunschweigwde[.]ru
dentseawaywie[.]ru
dicasfree[.]ru
digitalemikan[.]ru
earlyfordv8worg[.]ru
ebctwit[.]ru
energybulbswcowuk[.]ru
evideocardwinfo[.]ru
fashionflamenco[.]ru
filminglocationwanted[.]ru

fudonetwnet[.]ru
gokpopede[.]ru
healthhypnotherapy[.]ru
healthwyzeworg[.]ru
horshamyoga[.]ru
hotelsebastianswnl[.]ru
huangqiukui[.]ru
identitydesigned[.]ru
indiasinvite[.]ru
internhere[.]ru
intertruckwnl[.]ru
ivanmclean[.]ru
iwantthatfreestuff[.]ru
jajceportal[.]ru
jeepfore[.]ru
jksparklerfe[.]ru
jwookede[.]ru
kalamenoorwir[.]ru
karaoketextywcz[.]ru
kk3gwnet[.]ru
l0calnet[.]ru
liliannaborowska[.]ru
lipperleaders[.]ru
livenetworknewse[.]ru
lovelysubswit[.]ru
lshstream[.]ru
mastertargetwru[.]ru
minecraftqce[.]ru
mooieserverwnl[.]ru
motifyachting[.]ru
mshpworg[.]ru
mssoftwru[.]ru
multiestorageesystems[.]ru
mwzip[.]ru
myadultblogswtk[.]ru
newhealthyou[.]ru
nobiswal[.]ru
nomadrail[.]ru
ns01winfo[.]ru
nzyx[.]ru
omcwrued[.]ru
pdftowordenet[.]ru

pkucceeds[.]ru
ppphq[.]ru
quanyong79wcn[.]ru
quasimojomedia[.]ru
quertonwbe[.]ru
randorffwdk[.]ru
reneweastarkansas[.]ru
reperirewcowkr[.]ru
reporo[.]ru
revosnd[.]ru
richardtr[.]ru
safety63wru[.]ru
sbdanbury[.]ru
seacoastcareers[.]ru
seekandfind[.]ru
smartkeeda[.]ru
socialmartwru[.]ru
teachmyasswinfo[.]ru
thorntonroadcdjrnews[.]ru
torrentzwst[.]ru
trwgged[.]ru
tsksvwru[.]ru
uckoe[.]ru
ucozphpwru[.]ru
usahaedong[.]ru
verticaliowmx[.]ru
viktoria84wru[.]ru
vkwme3ewq[.]ru
voicestar[.]ru
wyomingoutdoorce[.]ru
yaoslwru[.]ru
yorkshireepine[.]ru
zickzickzick[.]ru
zyxelwpl[.]ru
142throckmortontheatre[.]ru
22hotmail[.]ru
abogadosmadrid[.]ru
aktarmawfr[.]ru
auqzzx[.]ru
autojanwcz[.]ru
bartoncccwedu[.]ru
bloomhospital[.]ru

computersiteswnet[.]ru
confized[.]ru
dentseawaywie[.]ru
eeodzywkiwpl[.]ru
elmundodetehuacan[.]ru
filminglocationwanted[.]ru
flirtswinwua[.]ru
gloryfloweinte[.]ru
healthwyzeworg[.]ru
jajceportal[.]ru
jksparklerfe[.]ru
kk3gwnet[.]ru
koeziowco[.]ru
levidom[.]ru
livenetworknewse[.]ru
mail.22hotmail[.]ru
mail.allisonpyep[.]ru
mail.americangrowthfund[.]ru
mail.auqzzx[.]ru
mail.autojanwcz[.]ru
mail.backupmdwnet[.]ru
mail.berndseneconste[.]ru
mail.biologikawco[.]ru
mail.bloomhospital[.]ru
mail.bucktickets winfo[.]ru
mail.confized[.]ru
mail.crediteure[.]ru
mail.dentseawaywie[.]ru
mail.dicasfree[.]ru
mail.digitalemikan[.]ru
mail.energybulbswcowuk[.]ru
mail.fudonetwnet[.]ru
mail.healthhypnotherapy[.]ru
mail.horshamyoga[.]ru
mail.huangqiukui[.]ru
mail.intertruckwnl[.]ru
mail.jajceportal[.]ru
mail.jeepfore[.]ru
mail.jksparklerfe[.]ru
mail.jwookede[.]ru
mail.kalamenoorwir[.]ru
mail.kk3gwnet[.]ru

mail.l0calnet[.]ru
mail.lipperleaders[.]ru
mail.livenetworknewse[.]ru
mail.lovelysubswit[.]ru
mail.lshstream[.]ru
mail.minecraftqce[.]ru
mail.mshpworg[.]ru
mail.multiestorageesystems[.]ru
mail.myadultblogswtk[.]ru
mail.nobiswal[.]ru
mail.nomadrail[.]ru
mail.ns01winfo[.]ru
mail.nzyx[.]ru
mail.pdftowordenet[.]ru
mail.ppphq[.]ru
mail.quanyong79wcn[.]ru
mail.quasimojomedia[.]ru
mail.quertonwbe[.]ru
mail.randorffwdk[.]ru
mail.revosnd[.]ru
mail.safety63wru[.]ru
mail.seacoastcareers[.]ru
mail.socialmartwru[.]ru
mail.ucozphpwru[.]ru
mail.viktoria84wru[.]ru
mail.vkwme3ewq[.]ru
mail.wyomingoutdoorce[.]ru
mail.yaoslwru[.]ru
mail.zickzickzick[.]ru
marsupiworg[.]ru
mssoftwru[.]ru
mtfwebwch[.]ru
nicklally[.]ru
nomadrail[.]ru
nzyx[.]ru
ppphq[.]ru
quasimojomedia[.]ru
randorffwdk[.]ru
revosnd[.]ru
texasninja[.]ru
torrentzwst[.]ru
uckoe[.]ru

www.22hotmail[.]ru
www.allisonpyep[.]ru
www.americangrowthfund[.]ru
www.auqzzx[.]ru
www.autojanwcz[.]ru
www.backupmdwnet[.]ru
www.berndseneconste[.]ru
www.biologikawco[.]ru
www.bloomhospital[.]ru
www.buckticketswinfo[.]ru
www.confized[.]ru
www.crediteure[.]ru
www.dentseawaywie[.]ru
www.dicasfree[.]ru
www.digitalemikan[.]ru
www.energybulbswcowuk[.]ru
www.fudonetwnet[.]ru
www.healthhypnotherapy[.]ru
www.horshamyoga[.]ru
www.huangqiukui[.]ru
www.intertruckwnl[.]ru
www.jajceportal[.]ru
www.jeepfore[.]ru
www.jksparklerfe[.]ru
www.jwookede[.]ru
www.kalamenoorwir[.]ru
www.kk3gwnet[.]ru
www.l0calnet[.]ru
www.lipperleaders[.]ru
www.livenetworknewse[.]ru
www.lovelysubswit[.]ru
www.lshstream[.]ru
www.minecraftqce[.]ru
www.mshpworg[.]ru
www.multiestorageesystems[.]ru
www.myadultblogswtk[.]ru
www.nobiswal[.]ru
www.nomadrail[.]ru
www.ns01winfo[.]ru
www.nzyx[.]ru
www.pdftowordenet[.]ru
www.ppphq[.]ru

www.quanyong79wcn[.]ru
www.quasimojomedia[.]ru
www.quertonwbe[.]ru
www.randorffwdk[.]ru
www.revosnd[.]ru
www.safety63wru[.]ru
www.seacoastcareers[.]ru
www.socialmartwru[.]ru
www.ucozphpwru[.]ru
www.viktoria84wru[.]ru
www.vkwme3ewq[.]ru
www.wyomingoutdoorce[.]ru
www.yaoslwru[.]ru
www.zickzickzick[.]ru

hXXp://apmeukwcowuk[.]ru/xzaq?award=17786
hXXp://apmeukwcowuk[.]ru/xzaq/?award=17786
hXXp://backupmdwnet[.]ru/qwer?award=17786&userid=
hXXp://clubaddisoed[.]ru/okmn/?award=17786
hXXp://colombiavozwnet[.]ru/fdsa/?award=17786
hXXp://cvjmebraunschweigwde[.]ru/erty?award=17786
hXXp://cvjmebraunschweigwde[.]ru/ytre/?award=17786
hXXp://dentseawaywie[.]ru/fdsa/?award=17786
hXXp://earlyfordv8worg[.]ru/sdcx?award=17786
hXXp://filminglocationwanted[.]ru/sdcx/?award=17786
hXXp://healthwyzeworg[.]ru/fdsa/?award=17786
hXXp://identitydesigned[.]ru/ghji?award=17786
hXXp://identitydesigned[.]ru/ghji/?award=17786
hXXp://ivanmclean[.]ru/erty?award=17786
hXXp://ivanmclean[.]ru/erty/?award=17786
hXXp://mshpworg[.]ru/qwsa/?award=17786
hXXp://mssoftwru[.]ru/asdf/?award=17786
hXXp://mssoftwru[.]ru/fdsa?award=17786
hXXp://mssoftwru[.]ru/fdsa/?award=17786
hXXp://mwzip[.]ru/asdf?award=17786
hXXp://pkucceeds[.]ru/asxz?award=17786
hXXp://pkucceeds[.]ru/asxz/?award=17786
hXXps://22hotmail[.]ru/xcvb/?award=17786
hXXps://9trestwru.xyz/sdfg/?award=17786
hXXps://actinglikeachef[.]ru/qwer/?award=17786
hXXps://addosports[.]ru/ijhg/?award=17786
hXXps://agenziapieropanwit[.]ru/fcxz/?award=17786

hXXps://alexpwru[.]ru/cxsw/?award=17786
hXXps://allinsgrp[.]ru/erty/?award=17786
hXXps://allinsgrp[.]ru/erty/?award=17786&pc=1
hXXps://americangrowthfund[.]ru/fgbv/?award=17786
hXXps://americangrowthfund[.]ru/vbgf/?award=17786
hXXps://apmeukwcowuk[.]ru/xzaq/?award=17786
hXXps://arcatatrane[.]ru/zxcv/?award=17786
hXXps://auqzzx[.]ru/asdf/?award=17786
hXXps://backupmdwnet[.]ru/qwer/?award=17786&userid=
hXXps://biologikawco[.]ru/xcvb/?award=17786
hXXps://blogagewde[.]ru/qazx/?award=17786
hXXps://blogagewde[.]ru/xzaq/?award=17786
hXXps://bolsasymofei[.]ru/vcxz/?award=17786
hXXps://caaeksworg[.]ru/xcds/?award=17786
hXXps://callpointe[.]ru/asdf/?award=17786
hXXps://capequilog[.]ru/sdfvc/?award=17786
hXXps://clubaddisoed[.]ru/okmn/?award=17786
hXXps://colombiavozwnet[.]ru/asdf/?award=17786
hXXps://colombiavozwnet[.]ru/fdsa/?award=17786
hXXps://computersiteswnet[.]ru/bvcx/?award\=17786&userid\=
hXXps://computersiteswnet[.]ru/bvcx/?award=17786&userid=
hXXps://computersiteswnet[.]ru/bvcx/?award=17786&userid=%250%25
hXXps://computersiteswnet[.]ru/xcvb/?award=17786&userid=
hXXps://confized[.]ru/asdf/?award=17786
hXXps://cvjmebraunschweigwde[.]ru/erty/?award=17786
hXXps://cvjmebraunschweigwde[.]ru/ytre/?award=17786
hXXps://dentseawaywie[.]ru/asdf/?award=17786
hXXps://dentseawaywie[.]ru/fdsa/?award=17786
hXXps://dunhamwqcwca[.]ru/vcxz/?award=17786
hXXps://earlyfordv8worg[.]ru/sdcx/?award=17786
hXXps://ebctwit[.]ru/ytre/?award=17786
hXXps://eeodzywkiwpl[.]ru/tyui/?award=17786
hXXps://environmenrf[.]ru/zxcf/?award=17786
hXXps://evideocardwinfo[.]ru/asdf/?award=17786
hXXps://fapearchive[.]ru/weds/?award=17786&userid=
hXXps://filminglocationwanted[.]ru/sdcx/?award=17786
hXXps://fudonetwnet[.]ru/fgbv/?award=17786
hXXps://gokpopede[.]ru/ghji/?award=17786
hXXps://granitecitygranite[.]ru/weds/?award=17786&userid=
hXXps://guaguazc[.]ru/zxcf/?award=17786
hXXps://healthhypnotherapy[.]ru/qazx/?award=17786
hXXps://healthhypnotherapy[.]ru/xzaq/?award=17786

hXXps://healthhypnotherapy[.]ru/xzaq/?award=17786&
hXXps://healthwyzeworg[.]ru/fdsa/?award=17786
hXXps://hotelsebastianswnl[.]ru/zxcf/?award=17786
hXXps://huangqiukui[.]ru/fgtr/?award=17786
hXXps://identitydesigned[.]ru/ghji?award=17786
hXXps://identitydesigned[.]ru/ghji/?award=17786
hXXps://identitydesigned[.]ru/ghji/?award=17786|
hXXps://imongwme[.]ru/tyui/?award=17786
hXXps://indiasinvite[.]ru/ijhg/?award=17786
hXXps://internhere[.]ru/erty/?award=17786
hXXps://intertruckwnl[.]ru/asxz/?award=17786
hXXps://ivanmclean[.]ru/erty?award=17786
hXXps://ivanmclean[.]ru/erty/?award=17786
hXXps://ivanmclean[.]ru/ytre?award=17786
hXXps://ivanmclean[.]ru/ytre/?award=17786
hXXps://iwantthatfreestuff[.]ru/erty/?award=17786
hXXps://jeepfore[.]ru/asxz/?award=17786
hXXps://jeepfore[.]ru/zxsa/?award=17786
hXXps://jingyigroup[.]ru/zxsa/?award=17786
hXXps://jksparklerfe[.]ru/rtgf/?award=17786
hXXps://kalamenoorwir[.]ru/edcv/?award=17786
hXXps://karaoketextywcz[.]ru/erty?award=17786
hXXps://liliannaborowska[.]ru/vbgf/?award=17786
hXXps://lipperleaders[.]ru/zxcf/?award=17786
hXXps://livenetworknewse[.]ru/ghnb/?award=17786
hXXps://marisacastelli[.]ru/cxsw/?award=17786&c=E
hXXps://mastertargetwru[.]ru/xzaq/?award=17786
hXXps://mooieserverwnl[.]ru/asxz/?award=17786
hXXps://mordiawnet[.]ru/sdew/?award=17786&userid=
hXXps://motifyachting[.]ru/rewq/?award=17786
hXXps://mssoftwru[.]ru/asdf/?award=17786
hXXps://mssoftwru[.]ru/fdsa/?award=17786
hXXps://multiestorageesystems[.]ru/rtgf/?award=17786&userid=
hXXps://mwzip[.]ru/asdf/?award=17786
hXXps://myadultblogswtk[.]ru/rtgf/?award\=17786
hXXps://myadultblogswtk[.]ru/rtgf/?award=17786
hXXps://newhealthyou[.]ru/xcft/?award=17786
hXXps://ns01winfo[.]ru/zxcf/?award=17786
hXXps://omcwrued[.]ru/eszx/?award=17786
hXXps://pdftowordenet[.]ru/zxsa/?award=17786
hXXps://pkucceeds[.]ru/asxz/?award=17786
hXXps://ppphq[.]ru/fcxz/?award=17786

hXXps://ptlwrued[.]ru/sdfvc/?award=17786
hXXps://randorffwdk[.]ru/rewq/?award=17786&amp
hXXps://redporky[.]ru/ghji/?award=17786
hXXps://reperirewcowkr[.]ru/aswq/?award=17786
hXXps://reporo[.]ru/qwer/?award=17786
hXXps://richardtr[.]ru/xzaq/?award=17786
hXXps://rmpincwnet[.]ru/fdsa/?award=17786
hXXps://sbdanbury[.]ru/zxcf?award=17786
hXXps://sbdanbury[.]ru/zxcf/?award=17786
hXXps://seekandfind[.]ru/asxz/?award=17786
hXXps://smartkeeda[.]ru/fgbv/?award=17786
hXXps://socialmartwru[.]ru/qazx/?award=17786
hXXps://teachmyasswinfo[.]ru/qazx/?award=17786
hXXps://teachmyasswinfo[.]ru/xzaq/?award=17786
hXXps://thorntonroadcdjrnews[.]ru/qazx/?award=17786
hXXps://toolesite[.]ru/asxz/?award=17786
hXXps://trwgged[.]ru/edcv/?award=17786
hXXps://tsksvwru[.]ru/cxsw/?award=17786
hXXps://uckoe[.]ru/xcds/?award=17786
hXXps://usahaedong[.]ru/uhbv/?award=17786
hXXps://verticaliowmx[.]ru/tfcx/?award=17786
hXXps://viaductwse[.]ru/xcvb/?award=17786
hXXps://viktoria84wru[.]ru/zxcf/?award=17786
hXXps://voicestar[.]ru/sdew/?award=17786
hXXps://webforditaswhu[.]ru/xcds/?award=17786
hXXps://webforditaswhu[.]ru/xcds/?award=17786|
hXXps://wjfbhtvfktdcdxwwws[.]ru/asdf/?award=17786
hXXps://wyomingoutdoorce[.]ru/asxz/?award=17786
hXXps://yorkshireepine[.]ru/qazx/?award=17786

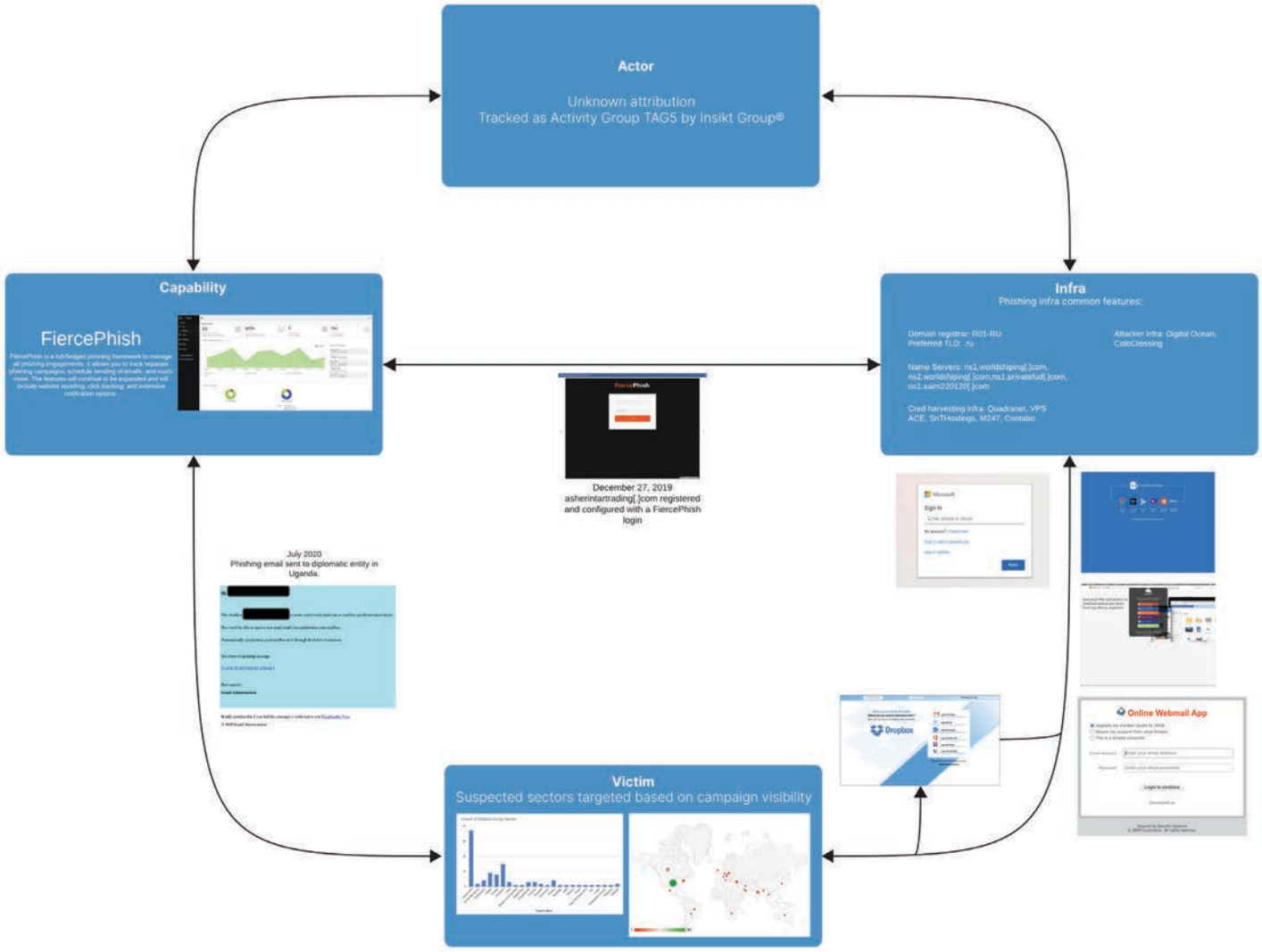
159.65.158[.]125
192.3.136[.]23
173.249.8[.]134
167.71.67[.]7
134.122.121[.]233
138.68.232[.]220
206.189.230[.]118
198.211.110[.]75
206.189.136[.]17
161.35.70[.]47
178.128.210[.]218
198.199.66[.]84

46.101.253[.]160
134.122.65[.]94
139.59.89[.]63
157.245.187[.]92
64.227.23[.]156
204.48.16[.]104
104.131.69[.]139
159.89.120[.]227
159.203.46[.]154
159.203.28[.]116
68.183.205[.]161
138.197.158[.]51
159.203.30[.]155
159.89.126[.]42
138.197.157[.]161
138.197.173[.]86
134.122.44[.]30
138.197.141[.]73
68.183.194[.]91
138.197.167[.]69
134.122.44[.]140
134.122.36[.]50
138.197.167[.]32
103.153.182[.]14
103.153.182[.]2
104.129.25[.]20
172.94.68[.]175
173.212.207[.]202
192.227.132[.]198
92.227.132[.]201
92.223.79[.]254
198.23.194[.]185
165.22.42[.]131
104.248.225[.]10

Appendix B (YARA rules)

```
rule SUSP_Asherintartrading_FiercePhish_campaign {

        meta:
    author = "Insikt Group, Recorded Future"
    description = "Detecting phishing email content used in asherintartrading campaign throughout 2020"
    hash1 = "bfb0bb8d8ff2802519e55ceef583dcb9eceaab6420dc341127215980656d5408"
    date = "2020-10-22"

        strings:

                $eml_1 = "has some undelivered mails due to mailbox synchronization failure.</p></td></tr>" fullword ascii
                $eml_2 = "<p>You won't be able to receive new mails until you synchronize your mailbox.</p></td></tr>" fullword
ascii
                $eml_3 = "<p>Automatically synchronize your mailbox now through the below instruction.</p></td></tr>" fullword
ascii
    $eml_4 = "You have (4) pending message.</font></span>" fullword ascii
                $eml_5 = "<p>Kindly unsubscribe if you feel this message is irrelevant to you <a href=3D" fullword ascii

        condition:
                4 of them

}
```

Appendix C



About Recorded Future

Recorded Future delivers security intelligence to amplify the effectiveness of security and IT teams by informing decisions in real time with contextual, actionable intelligence. By analyzing data from open, dark, and proprietary sources, Recorded Future offers a singular, integration-ready view of threat information, risks to digital brand, vulnerabilities, third-party risk, geopolitical risk, and more.