Taking Action Against Hackers in Iran

about.fb.com/news/2021/07/taking-action-against-hackers-in-iran/

April 7, 2022

Facebook threat intelligence analysts and security experts work to find and stop a wide range of threats including cyber espionage campaigns, influence operations and hacking of our platform by nation-state actors and other groups. As part of these efforts, our teams routinely disrupt adversary operations by disabling them, notifying users if they should take steps to protect their accounts, sharing our findings publicly and continuing to improve the security of our products.

Today, we're sharing actions we took against a group of hackers in Iran to disrupt their ability to use their infrastructure to abuse our platform, distribute malware and conduct espionage operations across the internet, targeting primarily the United States. This group is known in the security industry as Tortoiseshell, whose activity was previously reported to mainly focus on the information technology industry in the Middle East. In an apparent expansion of malicious activity to other regions and industries, our investigation found them targeting military personnel and companies in the defense and aerospace industries primarily in the US, and to a lesser extent in the UK and Europe. This group used various malicious tactics to identify its targets and infect their devices with malware to enable espionage.

This activity had the hallmarks of a well-resourced and persistent operation, while relying on relatively strong operational security measures to hide who's behind it. Our platform was one of the elements of the much broader cross-platform cyber espionage operation, and the group’s activity on Facebook manifested primarily in social engineering and driving people off-platform (e.g. email, messaging and collaboration services and websites), rather than directly sharing the malware itself.

We identified the following tactics, techniques and procedures (TTPs) used by this threat actor across the internet:

Social engineering: In running its highly targeted campaign, Tortoiseshell deployed sophisticated fake online personas to contact its targets, build trust and trick them into clicking on malicious links. These fictitious personas had profiles across multiple social media platforms to make them appear more credible. These accounts often posed as recruiters and employees of defense and aerospace companies from the countries their targets were in. Other personas claimed to work in hospitality, medicine, journalism, NGOs and airlines. They leveraged various collaboration and messaging platforms to move conversations off-platform and send malware to their targets. Our investigation found that this group invested significant time into their social engineering efforts across the internet, in some cases engaging with their targets for months.

Phishing and credential theft: This group created a set of tailored domains designed to attract particular targets within the aerospace and defense industries. Among them were fake recruiting websites for particular defense companies. They also set up online infrastructure that spoofed a legitimate US Department of Labor job search site. As part of their phishing campaigns, they spoofed domains of major email providers and mimicked URL-shortening services, likely to conceal the final destination of these links. These domains appeared to have been used for stealing login credentials to the victims’ online accounts (e.g. corporate and personal email, collaboration tools, social media). They also appeared to be used to profile their targets’ digital systems to obtain information about people’s devices, networks they connected to and the software they installed to ultimately deliver target-tailored malware.

Malware: This group used custom malware tools we believe to be unique to their operations, including full-featured remote-access trojans, device and network reconnaissance tools and keystroke loggers. Among these tools, they continued to develop and modify their malware for Windows known as Syskit, which they’ve used for years. They also shared links to malicious Microsoft Excel spreadsheets, which enabled malware to perform various system commands to profile the victim’s machine in a manner very similar to the Liderc reconnaissance tool identified by researchers at Cisco. One previously unreported variant of the malicious tool was embedded in a Microsoft Excel document and was capable of writing the output (i.e. result of the system reconnaissance) to a hidden area of the spreadsheet, which presumably required an attacker to social engineer the target to trick them into saving and returning the file.

Outsourcing malware development: We’ve observed this group use several distinct malware families. Our investigation and malware analysis found that a portion of their malware was developed by Mahak Rayan Afraz (MRA), an IT company in Tehran with ties to the Islamic Revolutionary Guard Corps (IRGC). Some of the current and former MRA executives have links to companies sanctioned by the US government.

We shared our findings and threat indicators with industry peers so they too can detect and mitigate this activity. To disrupt this operation, we blocked malicious domains from being shared on our platform, took down the group’s accounts and notified people who we believe were targeted by this threat actor.

Threat Indicators

Domains:

```
1st-smtp2go[.]email
2nd-smtp2go[.]email
3rd-smtp2go[.]email
4th-smtp2go[.]email
accounts[.]cam
activesessions[.]me
adobes[.]software
alhds[.]net
apppure[.]cf
bahri[.]site
bbcnews[.]email
bitly[.]cam
biturl[.]cx
brdcst[.]email
careeronestop[.]site
cc-security-inc[.]email
ccsecurity-mail-inc[.]email
ccsecurity-mail-inc[.]services
citymyworkday[.]com
cityofberkeley[.]support
cnbcnews[.]email
cnnnews[.]global
codejquery-ui[.]com
com-account-challenge[.]email
com-signin-v2[.]email
comlogin[.]online
comlogin[.]services
copyleft[.]today
crisiswatchsupport[.]shop
datacatch[.]xyz
dayzim[.]org
dh135[.]world
dollrealdoll[.]com
dollrealdoll[.]online
entrust[.]work
erictrumpfundation[.]com
facebookservices[.]gq
fblogin[.]me
fileblade[.]ga
findcareersatusbofa[.]com
fiservcareers[.]com
goodreads[.]rest
googl[.]club
gropinggo[.]com
hex6mak5z98nubb9vpd6t36cydkncfci9im872qx6hjci2egx8irq3qyt9pj[.]online
hike[.]studio
hiremilitaryheroes[.]com
hosted-microsoft[.]com
iemail[.]today
incognito[.]today
infoga[.]cam
iqtel[.]org
irtreporter[.]com
itiee[.]life
itieee[.]life
```

```
jessicamcgill[.]life
jqueryui-code[.]com
jumhuria[.]com
kartick[.]net
kaspersky[.]team
linkgen[.]me
linksbit[.]com
linq[.]ink
liveleak[.]cam
liveuamap[.]live
lockheedmartinjobs[.]us
loginaccount[.]email
logonexchangeonline[.]com
logonmicrosoftonline[.]com
lskjirn[.]life
mail2go[.]live
mail2go[.]online
mail2u[.]live
mailaccountlive[.]email
mailaccountlive[.]support
mailpublisher[.]live
mails[.]center
metacafe[.]live
micorsoftonilne[.]com
micorsoftonline[.]website
micorsoftonline[.]xyz
microsoftoffice[.]systems
microsoftonilne[.]cloud
mispace[.]cam
msol[.]live
msonline[.]live
mssecurityaccount[.]online
mydomainxyz[.]xyz
news-smtp2go[.]email
newsl[.]ink
noreplay[.]email
novafile[.]tk
onpointcorp[.]co
outlook-services[.]com
outlookservices[.]live
outlookservices[.]me
outube[.]live
pic-shareonline[.]com
pixlr[.]live
pixlr[.]myftp[.]org
post-jquery[.]com
prefiles[.]ml
publicsgroupe[.]net
pwutc[.]live
rali[.]live
recruitme[.]international
robotics[.]land
sabic[.]work
sandsngo[.]com
saudivisions2030[.]org
```

```
securityaccountreply[.]com
seery[.]online
sendblaster[.]org
sender[.]gb[.]net
shareae[.]cf
shlink[.]run
shlnk[.]run
short-l[.]link
shortli[.]live
shrt[.]rip
shur[.]live
shurl[.]site
site1[.]life
smtp-2go[.]com
smtp2go[.]best
smtp2go[.]club
smtp2go[.]email
smtp2go[.]fun
smtp2go[.]icu
smtp2go[.]live
smtp2go[.]me
smtp2go[.]pw
smtp2go[.]site
smtp2go[.]space
smtp2go[.]website
smtper[.]center
smtptogo[.]pw
soc-usa[.]email
soundcloud[.]fun
soundcloud[.]live
spreadme[.]international
src-ymlang[.]link
support-securitymail[.]email
support-ymail-team[.]online
surl[.]ist
surl[.]live
sxk8xrjtaikv3dxl7hgghw3vptvxpzzxeynrcltu4k3yeecjq3[.]online
systembackend[.]site
techmahindra[.]support
teleweb[.]world
tetra[.]email
thegardian[.]ml
thegaurdian[.]live
thomsonsreuters[.]email
thomsonsreuters[.]eu
thomsonsreuters[.]link
thomsonsreuters[.]net
tinil[.]ink
tinly[.]me
tinylink[.]pro
tinyurl[.]gold
tiwpan[.]xyz
tox[.]cheap
treasury[.]email
treporter[.]com
```

```
trumphotel[.]net
trumpnationallosangeles[.]email
trumporganization[.]world
trumporganizations[.]com
tv-youtube[.]com
uploaderfile[.]cf
usdailypost[.]com
usdailypost[.]net
usdp[.]news
vps[.]limited
watch-youtube[.]com
wikileaks[.]email
workshopplatform[.]network
xn--rumphotels-vcc[.]com
xn--twitte-u9a[.]com
xyzsitexyz[.]xyz
ymail-account[.]support
ymail-security-support[.]email
ymail-security[.]support
ymailaccounts[.]us
ymailsupport[.]info
zain[.]network
```