# FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

**25 JUL 2017**

Alert Number

**ML-000084-DM**

**WE NEED YOUR HELP!**

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately**.

Email:

**cywatch@ic.fbi.gov**

Phone:

**1-855-292-3937**

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP:AMBER**: Recipients may only share **TLP:AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

## IP Addresses and Domains Used by Likely Iran-Based Cyber Actors to Attack Victims Worldwide

**Summary**

The FBI assesses a group of malicious cyber actors—likely located in Iran—use Virtual Private Server infrastructure hosted in the United States to compromise government, corporate, and academic computer networks based in the Middle East, Europe and the United States. This infrastructure is used in conjunction with identified malicious domains to support a broad cyber campaign which likely includes the use of e-mail spear phishing, social engineering, and malicious Web sites ("watering hole attack"). These cyber actors almost certainly have been involved in this activity since at least early-2015.

Through a combination of FBI and private sector analysis, it is likely the actors involved with this activity are located in Iran. At least some victim information from this cyber activity transits US-based infrastructure to IP addresses located in Iran. At least one identified malicious domain was registered by a presumed Iranian national connected to a physical address in Tehran, Iran. The majority of the victims were located in Middle Eastern countries known to be traditional adversaries of the Iranian regime.

**Technical Details**

Attached to this FLASH is a list of 87 IP addresses and 136 domain names associated with this cyber activity. Activity related to these IPs and domains detected on a network should be considered an indication of compromise requiring mitigation.

**Recommended Mitigations**

Precautionary measures to mitigate this activity are:

- Prepare an incident response plan to be rapidly implemented in case of a cyber intrusion.
- Patch all systems for critical vulnerabilities, prioritizing timely patching of Internet-connected servers and software that processes Internet data such as Web browsers, browser plugins, and document readers.
- Scrutinize links contained in e-mails, and do not open attachments included in unsolicited e-mails.
- Implement application whitelisting to block execution of malware, or at least block execution of files from TEMP directories where most malware attempts to execute from.

**Reporting Notice**

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@ic.fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@ic.fbi.gov or (202) 324-3691.

# FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

**Administrative Note**

This product is marked **TLP:AMBER**. Recipients may only share **TLP:AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

# FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

## Your Feedback on the Value of this Product Is Critical

**Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:**
https://www.ic3.gov/PIFSurvey

***Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.***

104.200.128.126
104.200.128.161
104.200.128.173
104.200.128.183
104.200.128.184
104.200.128.185
104.200.128.187
104.200.128.195
104.200.128.196
104.200.128.198
104.200.128.205
104.200.128.206
104.200.128.208
104.200.128.209
104.200.128.48
104.200.128.58
104.200.128.64
104.200.128.71
107.181.160.138
107.181.160.178
107.181.160.179
107.181.160.194
107.181.160.195
107.181.161.141
107.181.174.21
107.181.174.232
107.181.174.241
141.105.70.235
141.105.70.236
141.105.70.237
141.105.70.238
141.105.70.239
141.105.70.240
141.105.70.241
141.105.70.242
141.105.70.243
141.105.70.244
141.105.70.245
141.105.70.246
141.105.70.247
141.105.70.248
141.105.70.249
141.105.70.250
144.168.45.126
146.0.73.107
146.0.73.108
146.0.73.109

146.0.73.110
146.0.73.111
146.0.73.112
146.0.73.113
146.0.73.114
173.244.173.10
173.244.173.11
173.244.173.12
173.244.173.13
173.244.173.14
206.221.181.253
209.51.199.112
209.51.199.113
209.51.199.114
209.51.199.115
209.51.199.116
209.51.199.117
209.51.199.118
31.192.105.15
31.192.105.16
31.192.105.17
38.130.75.20
66.55.152.164
68.232.180.122
91.218.247.157
91.218.247.158
91.218.247.160
91.218.247.161
91.218.247.162
91.218.247.165
91.218.247.166
91.218.247.167
91.218.247.168
91.218.247.169
91.218.247.170
91.218.247.173
91.218.247.180
91.218.247.181
91.218.247.182
91.218.247.183

cloud-analyzer.com
1e100.tech
1m100.tech
ads-youtube.net
ads-youtube.online
ads-youtube.tech
akamai.press
akamaitechnology.com
akamaitechnology.tech
alkamaihd.com
alkamaihd.net
azurewebsites.tech
banat48.org
big-windowss.com
britishnews.press
broadcast-microsoft.tech
cachevideo.com
cachevideo.online
cachevideo.xyz
chromeupdates.online
chromium.online
cissco.net
clalit.press
cloudflare.news
cloudflare.site
cloudflare-analyse.com
cloudflare-analyse.xyz
cloudflare-statics.com
cloudmicrosoft.net
cortana-search.com
digicert.online
digicert.space
digicert.xyz
dnsserv.host
elasticbeanstalk.tech
fbcdn.bid
fbexternal-a.press
fbexternal-a.pw
fb-nameserver.com
fbstatic-a.space
fbstatic-a.xyz
fbstatic-akamaihd.com
fb-statics.com
fb-statics.info
fdgdsg.xyz
f-tqn.com
githubapp.online

githubapp.tech
githubusecontent.tech
gmailtagmanager.com
google-api-analyse.com
google-api-update.com
hamedia.xyz
hotseller.info
intel-api.com
intelchip.org
ipresolver.org
javaupdator.com
jguery.net
jguery.online
js.jguery.online
kernel4windows.in
labs-cloudfront.com
mcafee-analyzer.com
mcafeemonitoring.com
mcafee-monitoring.com
microsoft-ds.com
microsoft-security.host
microsoftserver.org
microsoft-tool.com
micro-windows.in
mpmicrosoft.com
mssqlupdate.com
mswordupdate15.com
mswordupdate16.com
mswordupdate17.com
myservers.site
mywindows24.in
nameserver.win
nasr.xyz
newsfeeds-microsoft.press
nsserver.host
officeapps-live.com
officeapps-live.net
officeapps-live.org
onlinewebcam.press
outlook360.net
outlook360.org
owa-microsoft.online
patch7-windows.com
patch8-windows.com
patchthiswindows.com
qoldenlines.net
sdlc-esd-oracle.online

sharepoint-microsoft.co
sphotos-b.bid
sphotos-b.pw
ssl-gstatic.net
ssl-gstatic.online
static.news
symcd.site
symcd.xyz
tehila.co
tehila.global
tehila.info
tehila.press
trendmicro.tech
twiter-statics.com
twiter-statics.info
un-webmail.com
updatedrivers.org
walla.press
win-api.com
windefender.org
windowkernel.com
windowkernel14.com
windows-10patch.in
windows24-kernel.in
windows-api.com
windows-drive20.com
windows-india.in
windowskernel.com
windowskernel.in
windows-kernel.in
windowskernel.net
windowskernel14.com
windowslayer.in
windowssup.in
windowsupup.com
winfeedback.net
win-update.com
winupdate64.com
winupdate64.net
winupdate64.org
winupdate64.us
win-updates.com