Resurgo
Cyber Threat Alert Summaries

Hi All,

On July 25th, 2017 the FBI released a Flash Bulletin to alert the public about IP Addresses and Domains likely used by Iran-based Cyber Actors. Be aware that many of the domains listed below look legitimate and can easily be mistaken for the real domains.

Here is the listing of domains:

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

Resurgo
Cyber Threat Alert Summaries

js.jguery.online	nasr.xyz	ssl-gstatic.online	windows24-kernel.in
kernel4windows.in	newsfeeds-microsoft.press	static.news	windows-api.com
labs-cloudfront.com	nsserver.host	symcd.site	windows-drive20.com
mcafee-analyzer.com	officeapps-live.com	symcd.xyz	windows-india.in
mcafeemonitoring.com	officeapps-live.net	tehila.co	windowskernel.com
mcafee-monitoring.com	officeapps-live.org	tehila.global	windowskernel.in
microsoft-ds.com	onlinewebcam.press	tehila.info	windows-kernel.in
microsoft-security.host	outlook360.net	tehila.press	windowskernel.net
microsoftserver.org	outlook360.org	trendmicro.tech	windowskernel14.com
microsoft-tool.com	owa-microsoft.online	twiter-statics.com	windowslayer.in
micro-windows.in	patch7-windows.com	twiter-statics.info	windowssup.in
mpmicrosoft.com	patch8-windows.com	un-webmail.com	windowsupup.com
mssqlupdate.com	patchthiswindows.com	updatedrivers.org	winfeedback.net
mswordupdate15.com	qoldenlines.net	walla.press	win-update.com
mswordupdate16.com	sdlc-esd-oracle.online	win-api.com	winupdate64.com
mswordupdate17.com	sharepoint-microsoft.co	windefender.org	winupdate64.net
myservers.site	sphotos-b.bid	windowkernel.com	winupdate64.org
mywindows24.in	sphotos-b.pw	windowkernel14.com	winupdate64.us
nameserver.win	ssl-gstatic.net	windows-10patch.in	win-updates.com

Resurgo
Cyber Threat Alert Summaries

For a listing of IPs, contact me at ryan.ito@resurgo.net.

Notice
These flagged IPs and domains are not a definitive black list, but a recommendation and advisement provided by the FBI. It is up to the recipients of this information to decide how, when and where to use the information contained in these summaries.