BLOG

Clear Sky > **Blog** > Iranian Threat Agent Greenbug Impersonates Israeli High-Tech and Cyber Security Companies

Iranian Threat Agent Greenbug Impersonates Israeli High-Tech and Cyber Security Companies

By Clearsky October 24, 2017 Campaigns

Iranian Threat Agent **Greenbug** has been registering domains similar to those of Israeli High-Tech and Cyber Security Companies.

On 15 October 2017 a sample of **ISMdoor** was submitted to VirusTotal from Iraq. The sample name was WmiPrv.tmp (f5ef3b060fb476253f9a7638f82940d9) and it had the following PDB string:

*C:\Users\Void\Desktop\**v 10.0.194**\x64\Release\swchost.pdb*

Two domains were used for command and control:

thetareysecurityupdate[.]com
securepackupdater[.]com

By pivoting off the registration details and servers data of the two domains we discovered others registered by the threat agent. Eight contain the name of Israeli high-tech and cyber security companies and one of a Saudi Arabian testing & commissioning of major electrical equipment company.

We estimate that the domains were registered in order to be used when targeting these companies, organisations related to them, or unrelated third parties. However, we do not have any indication that the companies were actually targeted or otherwise impacted.

Below are the malicious domains and the companies who's names were used.

Malicious Domain	Impersonated company	Registration date
winsecupdater[.]com		11/6/2016
dnsupdater[.]com		12/4/2016
winscripts[.]net		3/4/2017
allsecpackupdater[.]com	Uncertain	4/8/2017
lbolbo[.]com		4/8/2017
securepackupdater[.]com	Uncertain	4/8/2017
thetaraysecurityupdate[.]com	**ThetaRay** (thetaray.com) – An Israeli cyber security and big data analytics company	4/8/2017
ymaaz[.]com	**YMAAZE** (ymaaze.com) – A Saudi Arabian testing & commissioning of major electrical equipment company	4/8/2017
oospoosp[.]com		8/9/2017
osposposp[.]com		8/9/2017
znazna[.]com		8/9/2017
mbsmbs[.]com		8/9/2017

Recent Posts

Iranian Threat Agent Greenbug Impersonates Israeli High-Tech and Cyber Security Companies

Recent ISMAgent Samples and Infrastructure by Iranian Threat Group GreenBug

The Economy Behind Phishing Websites Creation

Operation Wilted Tulip - Exposing a Cyber Espionage Apparatus

Recent Winnti Infrastructure and Samples

outbrainsecupdater[.]com	**Outbrain** (outbrain.com)– A major Israeli online advertising company	8/9/2017
securelogicupdater[.]com	**SecureLogic** (space-logic.com) – Likely an Israeli marketer of airport security systems by the same name. Other companies with the same name exist.	8/9/2017
benyaminsecupdater[.]com	Uncertain	8/9/2017
wixwixwix[.]com	**Wix** (wix.com) – A major Israeli cloud-based web development platform	8/9/2017
biocatchsecurity[.]com	**Biocatch** (biocatch.com) – an Israeli company developing technology for behavioral biometrics for fraud prevention and detection	10/14/2017
corticasecurity[.]com	**Cortica** (cortica.com) – an Israeli company developing Artificial Intelligence technology	10/14/2017
covertixsecurity[.]com	**Covertix** (covertix.com) – An Israeli data security company	10/14/2017
arbescurity[.]com	**Arbe Robotics** (arberobotics.com)– An Israeli company developing autonomous driving technology	10/14/2017

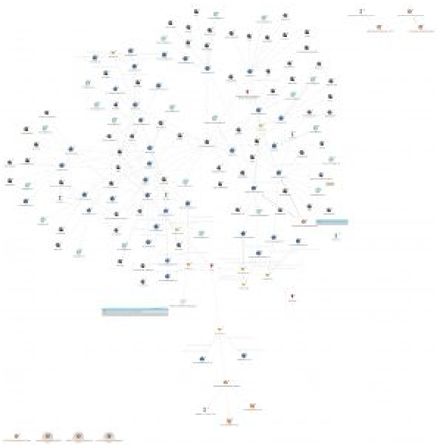
Indicators of compromise

Indicators of compromise are presented below and are available on PassiveTotal.

Domain	allsecpackupdater[.]com
Domain	znazna[.]com
Domain	arbescurity[.]com
Domain	benyaminsecupdater[.]com
Domain	biocatchsecurity[.]com
Domain	corticasecurity[.]com
Domain	covertixsecurity[.]com
Domain	dnsupdater[.]com
Domain	lbolbo[.]com
Domain	mbsmbs[.]com
Domain	ntpupdateserver[.]com
Domain	oospoosp[.]com

Domain	osposposp[.]com
Domain	outbrainsecupdater[.]com
Domain	securelogicupdater[.]com
Domain	securepackupdater[.]com
Domain	thetaraysecurityupdate[.]com
Domain	winscripts[.]net
Domain	winsecupdater[.]com
Domain	wixwixwix[.]com
Domain	ymaaz[.]com
Domain	benyaminsecupdater[.]com
Filename	WmiPrv.tmp
Hash	37d586727c1293d8a278b69d3f0c5c4b
Hash	82755bf7ad786d7bf8da00b6c19b6091
Hash	ad5120454218bb483e0b8467feb3a20f
Hash	e0175eecf8d31a6f32da076d22ecbdff
Hash	f5ef3b060fb476253f9a7638f82940d9
IP	151.80.113.150
IP	151.80.221.23
IP	217.182.244.254
IP	46.105.130.98
IP	5.39.31.91
IP	80.82.66.164
SSLCertificate	3b0b85ea32cab82eaf4249c04c05bdfce5b6074ca076fedf87dbea6b28fab99d

The Maltego graph below depicts the relationship among the indicators (click to enlarge):



Update 2017-10-25 – three hashes removed from IOC list

The following hashes were mistakenly included in the IOC list and have been removed, as they are unrelated to the campaign:
c594b52ec8922a1e980a2ea31b1d1157
179cb8839e9ee8e9e6665b0986bf7811
d30c4df6de21275ae69a4754fc2372ef

ClearSky

Ahead of the threat curve

13 Yosef Karo st., Tel Aviv, Israel
Phone: +972 3 624 0346

Email: info [at] clearskysec.com