Appendix: Iran IOCs

Hashes	Description
5798aefb07e12a942672a60c2be101dc26b01485616713e8be1f68b321747f2f	Notestuk/TURNEDUP
a67461a0c14fc1528ad83b9bd874f53b7616cfed99656442fb4d9cdd7d09e449	AutoIt backdoor
f2943f5e45befa52fb12748ca7171d30096e1d4fc3c365561497c618341299d5	Gpppassword
87e2cf4aa266212aa8cf1b1c98ae905c7bac40a6fc21b8e821ffe88cf9234586	LaZagne
709df1bbd0a5b15e8f205b2854204e8caf63f78203e3b595e0e66c918ec23951	LaZagne
a23c182349f17398076360b2cb72e81e5e23589351d3a6af59a27e1d552e1ec0	Quasar RAT
0b3610524ff6f67c59281dbf4a24a6e8753b965c15742c8a98c11ad9171e783d	Quasar RAT
d5262f1bc42d7d5d0ebedadd8ab90a88d562c7a90ff9b0aed1b3992ec073e2b0	Quasar RAT
ae1d75a5f87421953372e79c081e4b0a929f65841ed5ea0d380b6289e4a6b565	Remcos
e999fdd6a0f5f8d1ca08cf2aef47f5ddc0ee75879c6f2c1ee23bc31fb0f26c70	Remcos
018360b869d8080cf5bcca1a09eb8251558378eb6479d8d89b8c80a8e2fa328c	Remcos
367e78852134ef488ecf6862e71f70a3b10653e642bda3df00dd012c4e130330	Remcos
ea5295868a6aef6aac9e117ef128e9de107817cc69e75f0b20648940724880f3	Remcos
6401abe9b6e90411dc48ffc863c40c9d9b073590a8014fe1b0e6c2ecab2f7e18	SniffPass
bf9c589de55f7496ff14187b1b5e068bd104396c23418a18954db61450d21bab	DarkComet
af41e9e058e0a5656f457ad4425a299481916b6cf5e443091c7a6b15ea5b3db3	DarkComet
c7a2559f0e134cafbfc27781acc51217127a7739c67c40135be44f23b3f9d77b	AutoIt FTP tool
99c1228d15e9a7693d67c4cb173eaec61bdb3e3efdd41ee38b941e733c7104f8	.NET FTP tool
94526e2d1aca581121bd79a699a3bf5e4d91a4f285c8ef5ab2ab6e9e44783997	PowerShell downloader (registry.ps1)
dedfbc8acf1c7b49fb30af35eda5e23d3f7a202585a5efe82ea7c2a785a95f40	POSHC2 backdoor
a1029d20f595ff92746fd9d1d351a215cdffbdd7f0b19ba1859f1c211fddc060	ZeroCleare
08dc0073537b588d40deda1f31893c52	ZeroCleare
be2b88f3074bdbc7e990d472a1a6c71edfb950f1	ZeroCleare
2fc39463b6db44873c9c07724ac28b63cdd72f5863a4a7064883e3afdd141f8d	ZeroCleare
cc99395963de6da81dac96929a8e234c8415714a	ZeroCleare
33f98b613b331b49e272512274669844	ZeroCleare
44100c73c6e2529c591a10cd3668691d92dc0241152ec82a72c6e63da299d3a2	ZeroCleare
7f70d8ae6a8eea7657b4726d08fb0c8a62040f0bfdfc8a5d68a054a3e3780652	ZeroCleare
3a7ab2fbeaca7eb724549608119f78d36bc8cee59fd3e1c391d87df10f871997	ZeroCleare
f07b0c79a8c88a5760847226af277cf34ab5508394a58820db4db5a8d0340fc7	ZeroCleare
36a4e35abf2217887e97041e3e0b17483aa4d2c1aee6feadd48ef448bf1b9e6c	ZeroCleare
cf3a7d4285d65bf8688215407bce1b51d7c6b22497f09021f0fce31cbeb78986	ZeroCleare

IP Addresses	Domains
8.26.21.120	mynetwork.ddns.net
162.250.145.234	mynetwork.ddns.net
91.235.142.76	mywinnetwork.ddns.net
8.26.21.120	[REDACTED].ddns.net
8.26.21.119	hyperservice.ddns.ne
8.26.21.120	[REDACTED].ddns.net
95.211.191.117	update-sec.com
5.187.21.70	microsoftupdated.com
217.13.103.46	securityupdated.com
8.26.21.120	[REDACTED].ddns.net
5.187.21.71	backupnet.ddns.net
91.230.121.143	backupnet.ddns.net
8.26.21.119	[REDACTED].ddns.net
8.26.21.117	srvhost.servehttp.com
37.48.105.178	servhost.hopto.org
8.26.21.117	srvhost.servehttp.com
5.187.21.70	microsoftupdated.com
64.251.19.214	mynetwork.ddns.net
64.251.19.217	[REDACTED].servehttp.com
64.251.19.214	[REDACTED].ddns.net
64.251.19.214	mynetwork.ddns.net
64.251.19.214	[REDACTED].sytes.net
64.251.19.217	[REDACTED].myftp.org
64.251.19.216	srvhost.servehttp.com
64.251.19.217	[REDACTED].myftp.org
64.251.19.217	[REDACTED].myftp.org
64.251.19.215	[REDACTED].myftp.org
64.251.19.217	[REDACTED].myftp.org
64.251.19.216	[REDACTED].myftp.org
64.251.19.232	mynetwork.ddns.net
64.251.19.214	[REDACTED].ddns.net
162.250.145.204	mynetwork.ddns.net
188.165.4.81	svcexplores.com
64.251.19.231	mynetwork.ddns.net
64.251.19.231	[REDACTED].ddns.net
64.251.19.232	[REDACTED].ddns.net
64.251.19.216	[REDACTED].myftp.biz
91.230.121.143	remote-server.ddns.net
162.250.145.222	[REDACTED].ddns.net
64.251.19.216	[REDACTED].redirectme.net

8.26.21.222	mynetwork.ddns.net
8.26.21.223	[REDACTED].ddns.net
217.147.168.44	remserver.ddns.net
195.20.52.172	mynetwork.cf
8.26.21.221	mynetwork.ddns.net
8.26.21.220	[REDACTED].ddns.net
8.26.21.221	[REDACTED].ddns.net
91.230.121.144	remserver.ddns.net
89.34.237.118	mywinnetwork.ddns.net
192.119.15.35	mynetwork.ddns.net
5.79.127.177	mypsh.ddns.net
192.119.15.35	[REDACTED].ddns.net
192.119.15.35	[REDACTED].ddns.net
192.119.15.35	[REDACTED].ddns.net
192.119.15.36	[REDACTED].ddns.net
192.119.15.37	mynetwork.ddns.net
192.119.15.38	[REDACTED].ddns.net
192.119.15.39	remote-server.ddns.net
192.119.15.40	[REDACTED].ddns.net
192.119.15.41	mynetwork.cf
192.119.15.42	[REDACTED].ddns.net

Filename / Domain / IP Address	MD5 Hash or Description
CVE-2017-11882 exploit document	A0E6933F4E0497269620F44A083B2ED4
b.txt	9267D057C065EA7448ACA1511C6F29C7
v.txt/v.vbs	B2D13A336A3EB7BD27612BE7D4E334DF
dUpdateCheckers.base	4A7290A279E6F2329EDD0615178A11FF
hUpdateCheckers.base	841CE6475F271F86D0B5188E4F8BC6DB
cUpdateCheckers.bat	52CA9A7424B3CC34099AD218623A0979
dUpdateCheckers.ps1	BBDE33F5709CB1452AB941C08ACC775E
hUpdateCheckers.ps1	247B2A9FCBA6E9EC29ED818948939702
GoogleUpdateschecker.vbs	C87B0B711F60132235D7440ADD0360B0
hxxp://mumbai-m[.]site	POWRUNER C2
hxxp://dns-update[.]club	Malware Staging Server
CVE-2017-0199 exploit document	63D66D99E46FB93676A4F475A65566D8
94.23.172.164:80	Malware Staging Server
dupdatechecker.doc	D85818E82A6E64CA185EDFDDBA2D1B76

94.23.172.164:80	Malware Staging Server
dupdatechecker.doc	D85818E82A6E64CA185EDFDDBA2D1B76
dupdatechecker.exe	C9F16F0BE8C77F0170B9B6CE876ED7FB
proxycheker[.]pro	C2
46.105.221.247	Has resolved mumbai-m[.]site & hpserver[.]online
148.251.55.110	Has resolved mumbai-m[.]site and dns-update[.]club
185.15.247.147	Has resolved dns-update[.]club
145.239.33.100	Has resolved dns-update[.]club
82.102.14.219	Has resolved ns2.dns-update[.]club & hpserver[.]online & anyportals[.]com
v7-hpserver.online.hta	E6AC6F18256C4DDE5BF06A9191562F82
dUpdateCheckers.base	3C63BFF9EC0A340E0727E5683466F435
hUpdateCheckers.base	EEB0FF0D8841C2EBE643FE328B6D9EF5
cUpdateCheckers.bat	FB464C365B94B03826E67EABE4BF9165
dUpdateCheckers.ps1	635ED85BFCAAB7208A8B5C730D3D0A8C
hUpdateCheckers.ps1	13B338C47C52DE3ED0B68E1CB7876AD2
googleupdateschecker.vbs	DBFEA6154D4F9D7209C1875B2D5D70D5
hpserver[.]online	C2
v7-anyportals.hta	EAF3448808481FB1FDBB675BC5EA24DE
dUpdateCheckers.base	42449DD79EA7D2B5B6482B6F0D493498
hUpdateCheckers.base	A3FCB4D23C3153DD42AC124B112F1BAE
dUpdateCheckers.ps1	EE1C482C41738AAA5964730DCBAB5DFF
hUpdateCheckers.ps1	E516C3A3247AF2F2323291A670086A8F
anyportals[.]com	C2

ABOUT INTSIGHTS

IntSights is revolutionizing cybersecurity operations with the industry's only all-in-one external threat protection platform designed to neutralize cyberattacks outside the wire. Our unique cyber reconnaissance capabilities enable continuous monitoring of an enterprise's external digital profile across the clear, deep, and dark web to identify emerging threats and orchestrate proactive response. Tailored threat intelligence that seamlessly integrates with security infrastructure for dynamic defense has made IntSights one of the fastest-growing cybersecurity companies in the world. IntSights has offices in Amsterdam, Boston, Dallas, New York, Singapore, Tel Aviv, and Tokyo. To learn more, visit: intsights.com or connect with us on LinkedIn, Twitter, and Facebook.

To see the IntSights External Threat Protection Suite of solutions in action, **schedule a demo today.**