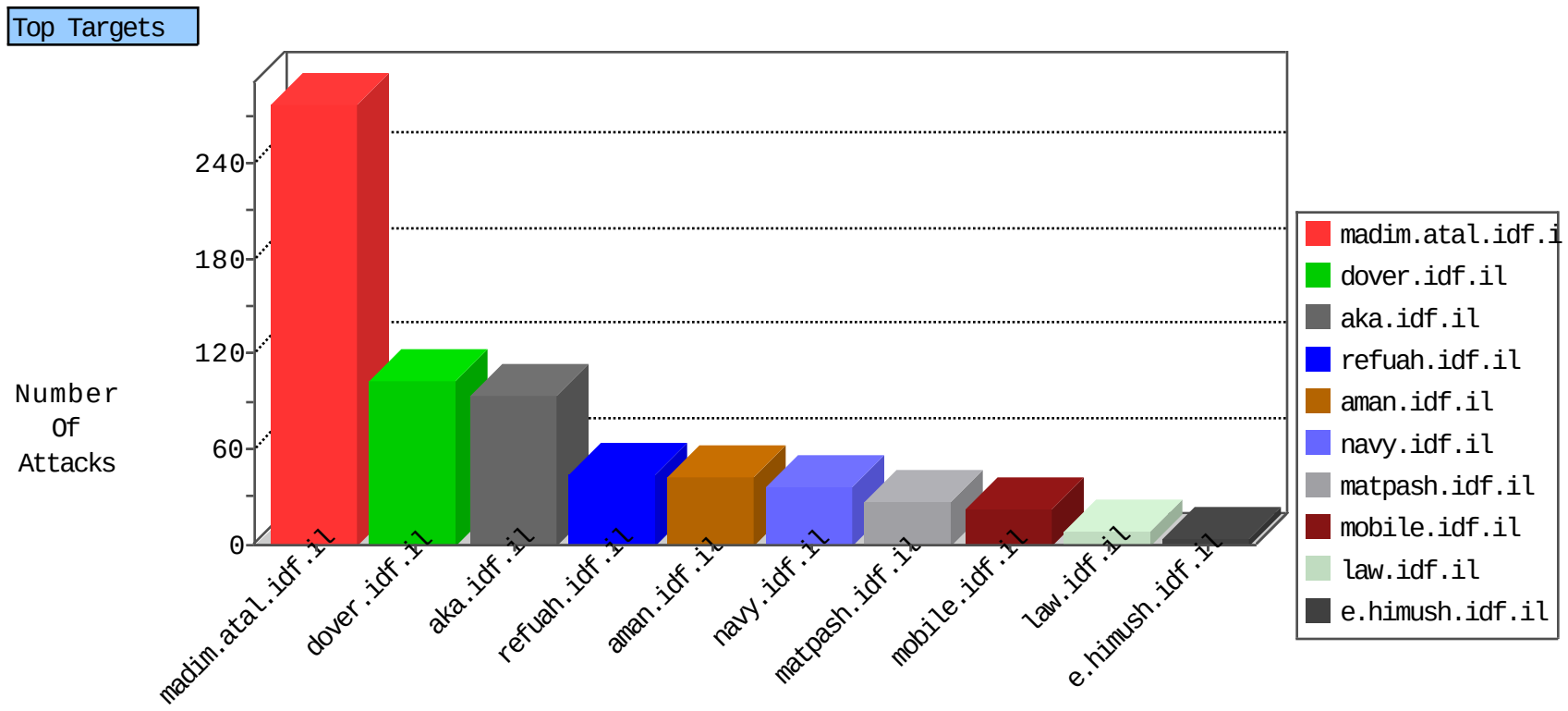
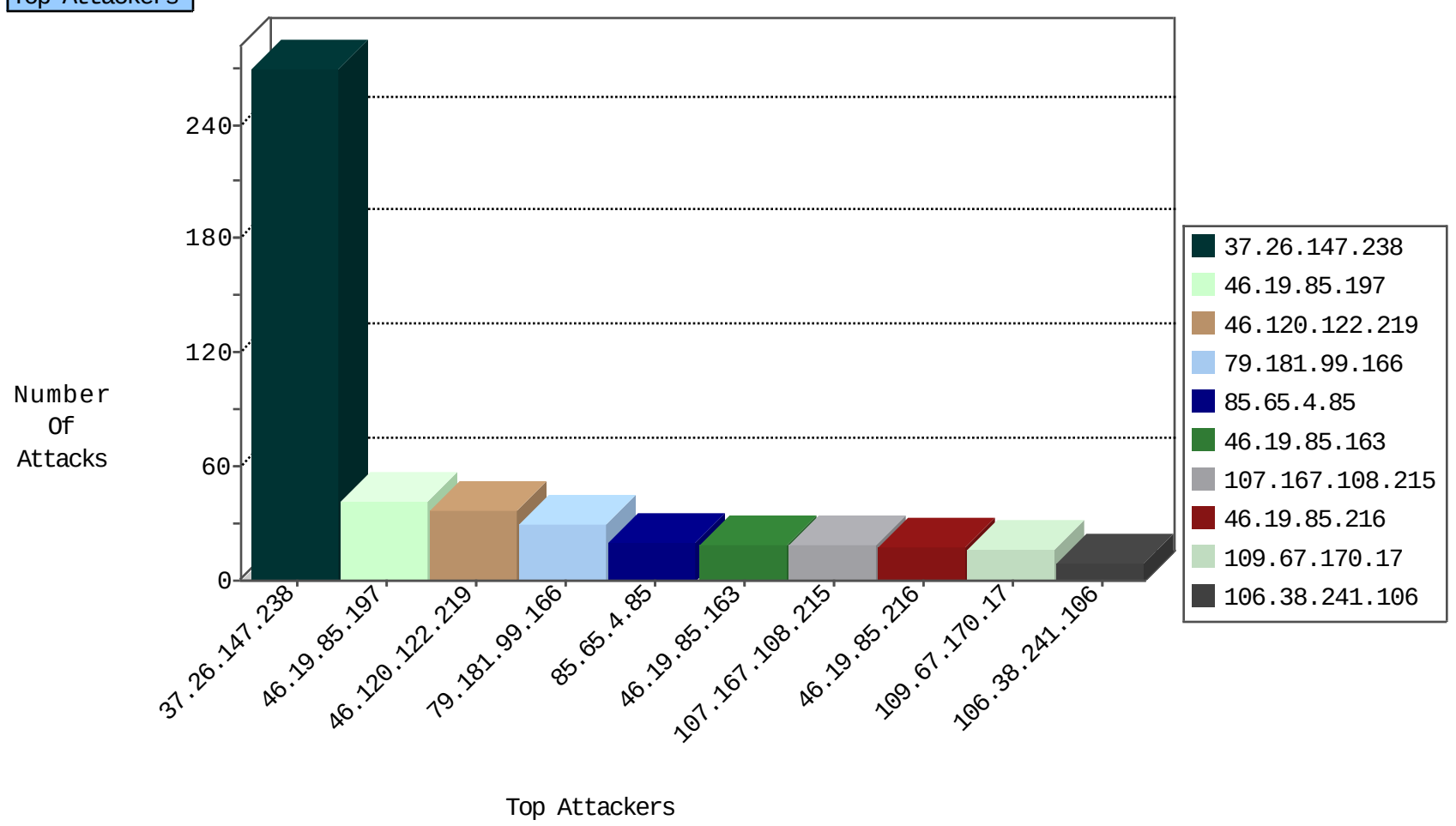
09-30-2016-21:04:07 to 09-30-2016-22:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-30-2016-21:04:07 to 09-30-2016-22:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.139.79	Israel	147.237.72.166	aka.idf.il	Black List	drop	5
95.211.189.18	Netherlands	147.237.76.31	nakchal.idf.il	Black List	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.76.202	e.halag.idf.il	Black List	drop	1
117.201.51.153	India	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

09-30-2016-21:04:07 to 09-30-2016-22:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	3
51.254.141.30	France	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.106	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-30-2016-21:04:07 to 09-30-2016-22:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.76.42	Israel	refuah.idf.il	Xenu Link Sleuth User Agent	31
66.219.211.107	147.237.76.197	United States	e.himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	3
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
106.120.209.149	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 2048	1
46.172.91.21	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	1
218.205.151.198	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 2048	1
183.129.160.229	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
106.120.209.149	147.237.77.74	China	law.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.65	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.147.238	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
218.205.151.198	147.237.77.74	China	law.idf.il	ET SCAN NMAP -f -sS	1
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1

09-30-2016-21:04:07 to 09-30-2016-22:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.65.4.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
107.167.108.215	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
46.19.85.163	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	17
46.19.85.197	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.197	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.216	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.216	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	8
109.67.170.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
79.181.99.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.86.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
109.67.170.17	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.64.128.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
79.181.99.166	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
46.120.122.219	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
193.43.246.250	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
77.138.27.112	France	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.53.28.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
5.22.134.169	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.71	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.2.43	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
109.67.170.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
77.138.27.112	France	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
217.24.254.114	Albania	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
2.223.242.153	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.26	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
79.181.145.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.237.138.202	Czech Republic	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
80.246.137.252	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.72	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
109.65.192.78	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
84.109.231.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
141.226.218.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.57.253.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.72	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.244.28	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.147.238	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence		alert	2
77.126.59.117	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
89.139.162.119	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
2.53.49.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
82.166.244.82	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
176.13.244.67	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
37.26.147.238	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence		monitor	2
46.19.85.10	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

09-30-2016-21:04:07 to 09-30-2016-22:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	264
37.26.149.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
37.26.147.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.97.173	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/5/1705.pdf	Block	3
79.179.132.189	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
85.65.134.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniot.aspx	Block	1
213.57.52.217	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
109.65.150.165	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
157.55.39.145	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in aka.idf.il/main/giyus/	None	1
96.230.95.159	United States	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/lies.stm<hr></blockquote>	Block	1
77.138.243.23	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
192.243.55.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
96.230.95.159	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method i[[#0]][[#0]][[#0]]BôYÀÛÀm[[#18]]™k‰b=œ[[#19]][[#15]]í[[#27]]S•Ã[[#3]][[#5]][[#6]]¶Á[[#11]]MwÌl"¾[[#20]]TAÎ.ZLÌ[[#5]]É!*k›M”>ºã[[#26]]úÙøÚ{ô;h½örP‡[[#20]]Y,ùÊoõÎ4œ^¾Hßø.Þr¼[[#4]]ÖÙ1ãg{H[•}()	Block	1
66.249.65.60	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8847-he/refuah.aspx	Block	1
120.27.37.74	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
198.20.69.74	United States	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/robots.txt	Block	1
96.230.95.159	United States	147.237.77.216	dover.idf.il	NULL Character in Method i[[#0]][[#0]][[#0]]BôYÀÛÀm[[#18]]™k‰b=œ[[#19]][[#15]]í[[#27]]S•Ã[[#3]][[#5]][[#6]]¶Á[[#11]]MwÌl"¾[[#20]]TAÎ.ZLÌ[[#5]]É!*k›M”>ºã[[#26]]úÙøÚ{ô;h½örP‡[[#20]]Y,ùÊoõÎ4œ^¾Hßø.Þr¼[[#4]]ÖÙ1ãg{H[•}()	Block	1
66.249.73.133	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19369-he/idfgdover.aspx	Block	1
120.27.37.74	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
81.4.129.178	Cyprus	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.120.122.219	Israel	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/894-he/refuah.aspx	Block	1
204.79.180.159	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
96.230.95.159	United States	147.237.77.216	dover.idf.il	Unknown HTTP Request Method i[[#0]][[#0]][[#0]]BôYÀÛÀm[[#18]]™k‰b=œ[[#19]][[#15]]í[[#27]]S•Ã[[#3]][[#5]][[#6]]¶Á[[#11]]MwÌl"¾[[#20]]TAÎ.ZLÌ[[#5]]É!*k›M”>ºã[[#26]]úÙøÚ{ô;h½örP‡[[#20]]Y,ùÊoõÎ4œ^¾Hßø.Þr¼[[#4]]ÖÙ1ãg{H[•}() in URL	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
2.53.27.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
125.77.28.26	China	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to 147.237.76.147/	Block	1

09-30-2016-21:04:07 to 09-30-2016-22:04:07