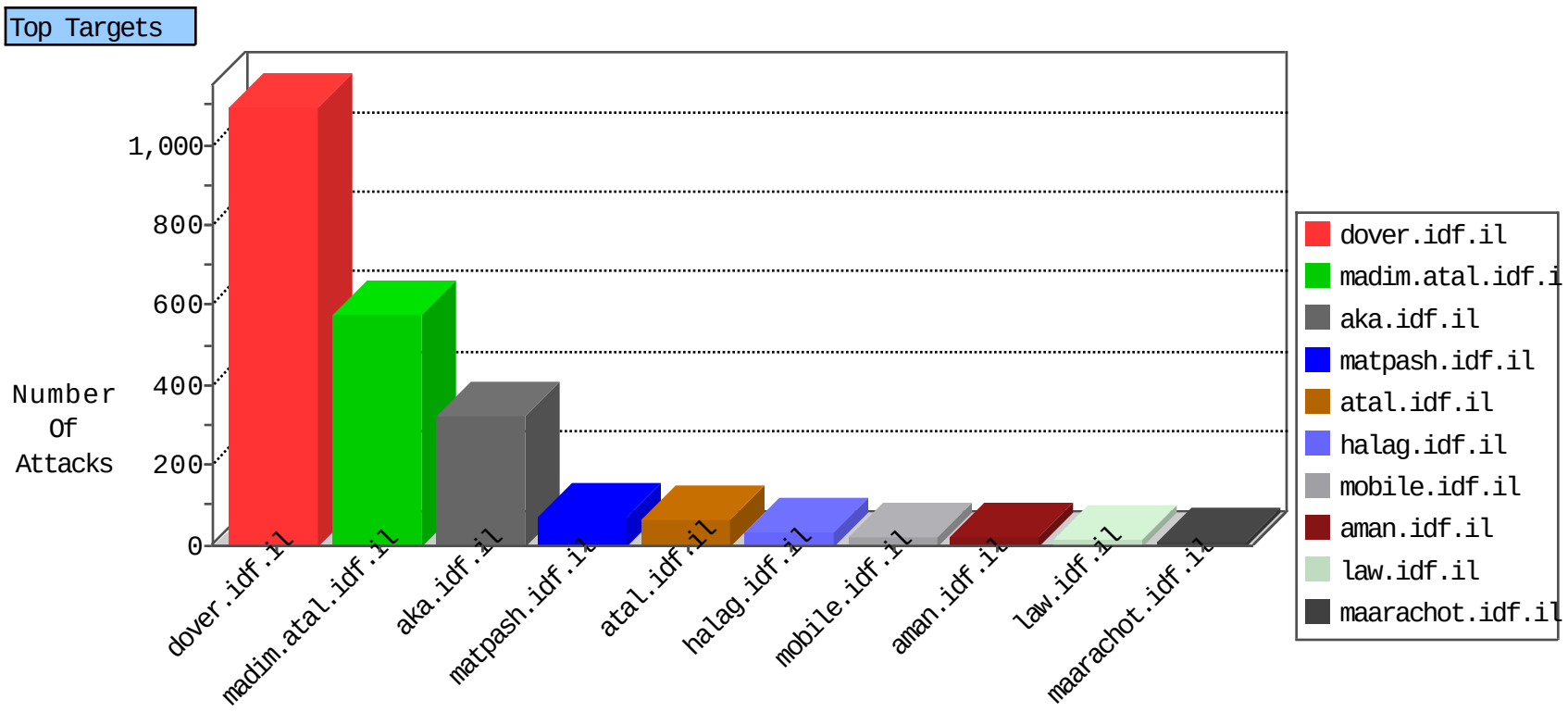
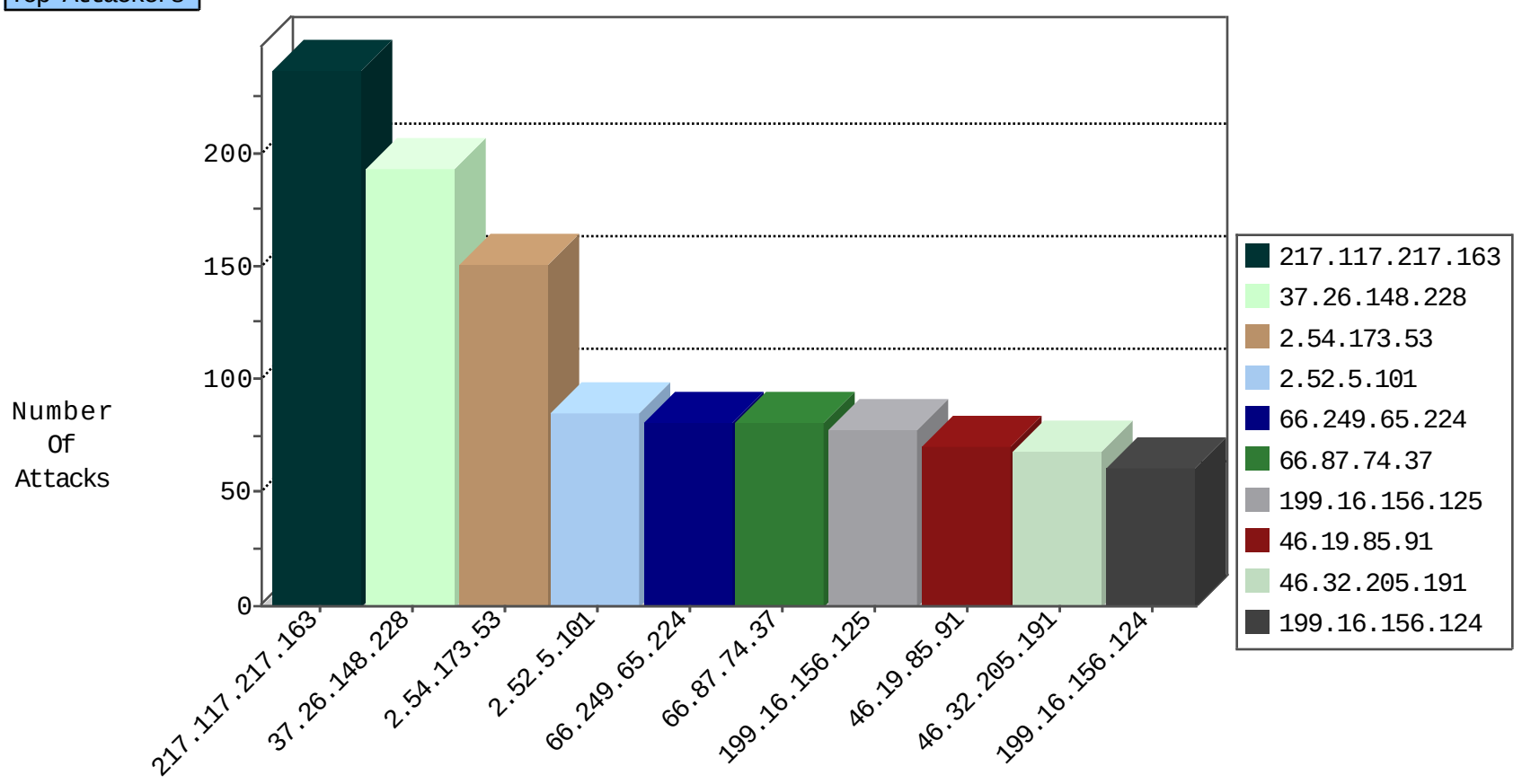
11-21-2015-12:04:00 to 11-21-2015-13:04:00

IDF Under Attack
Daily Report

Top Targets



Top Attackers



11-21-2015-12:04:00 to 11-21-2015-13:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.64	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
109.64.20.128	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
70.94.195.150	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	2
109.64.28.114	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
85.130.227.13	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
59.45.74.90	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
94.41.248.234	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
1.82.191.175	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
176.228.168.12	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.177.126	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
185.3.146.206	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-21-2015-12:04:00 to 11-21-2015-13:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
117.169.6.60	China	147.237.77.170	maarachot.idf.il	8479: HTTP: Suspicious HTTP Request	Block	2
185.106.94.2		147.237.72.156	aman.idf.il	0543: HTTP: php.cgi Access	Block	1

11-21-2015-12:04:00 to 11-21-2015-13:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.67.73	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
74.117.209.136	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.178	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
84.22.155.242	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

11-21-2015-12:04:00 to 11-21-2015-13:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
217.117.217.163	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	233
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
46.32.205.191	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
199.16.156.125	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	60
66.87.74.37	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	54
199.16.156.126	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	42
199.16.156.124	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	38
85.27.200.33	Denmark	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
46.19.85.91	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
46.19.85.91	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
100.100.81.217		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	28
100.100.51.7		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
66.87.74.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
62.128.48.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
100.100.51.7		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
178.63.165.187	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
73.136.149.83	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
100.100.54.11		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
199.16.156.125	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
69.175.127.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
213.57.140.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
31.168.201.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
50.116.28.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.54.179.152	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
199.16.156.126	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
199.16.156.124	United States	147.237.77.216	dover.idf.il	drop		drop	9
199.16.156.124	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
77.127.152.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.149.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.65.191.247	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
198.58.96.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.246.133.66	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
80.246.133.66	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
207.46.13.123	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
91.12.72.5	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
64.19.78.242	United States	147.237.76.44	e.refuah.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	7
40.77.167.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.36.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.177.43.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.186.49.73	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.119.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
149.78.254.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	143
2.54.173.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
2.52.5.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
46.19.85.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
176.13.20.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
37.26.148.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	50
2.54.173.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	47
2.52.5.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
176.12.150.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.13.16.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
208.115.113.89	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.229.1.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.106.94.2		147.237.72.156	aman.idf.il	Multiple URL worm attacks from 185.106.94.2	Block	3
149.88.125.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.126.86.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
86.67.9.88	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
46.117.207.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.88.109.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
117.169.6.60	China	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	2
176.106.226.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.153.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9364-he/refuah.aspx	Block	1
213.57.56.30	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/7/110517.pdf"	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-20127-he/kkkkkkk=bc69e9b3kkkkkkk_bc69e9b3	Block	1
157.55.39.75	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-14886-en/dover.aspx	Block	1
77.126.86.99	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.67.31	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
109.67.155.33	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.131	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
80.246.136.243	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
176.13.13.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.70.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	1
216.218.206.68	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8821-he/refuah.aspx	Block	1
46.19.85.91	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
183.79.222.36	Japan	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
87.68.246.193	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
79.181.22.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.229	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim/fund/Ã£â€”Ã¢â‚¬Ëœ Ã£â€”Ã?Ã£â€”Ã¢Â§Ã£â€”Ã¥Â¾Ã£â€”Ã¢â‚¬Ã?	Block	1
66.249.67.54	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1275-he/atal.aspx	Block	1
109.67.155.33	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/pages/fan_status.php	Block	1
107.150.43.203	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /	Block	1
46.117.207.54	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie _pk_ref.322.9cd2: Expected ["","",1447922376,"https://www.google.co.il/"], Observed ["","",1448100543,"https://www.google.co.il/"]	None	1