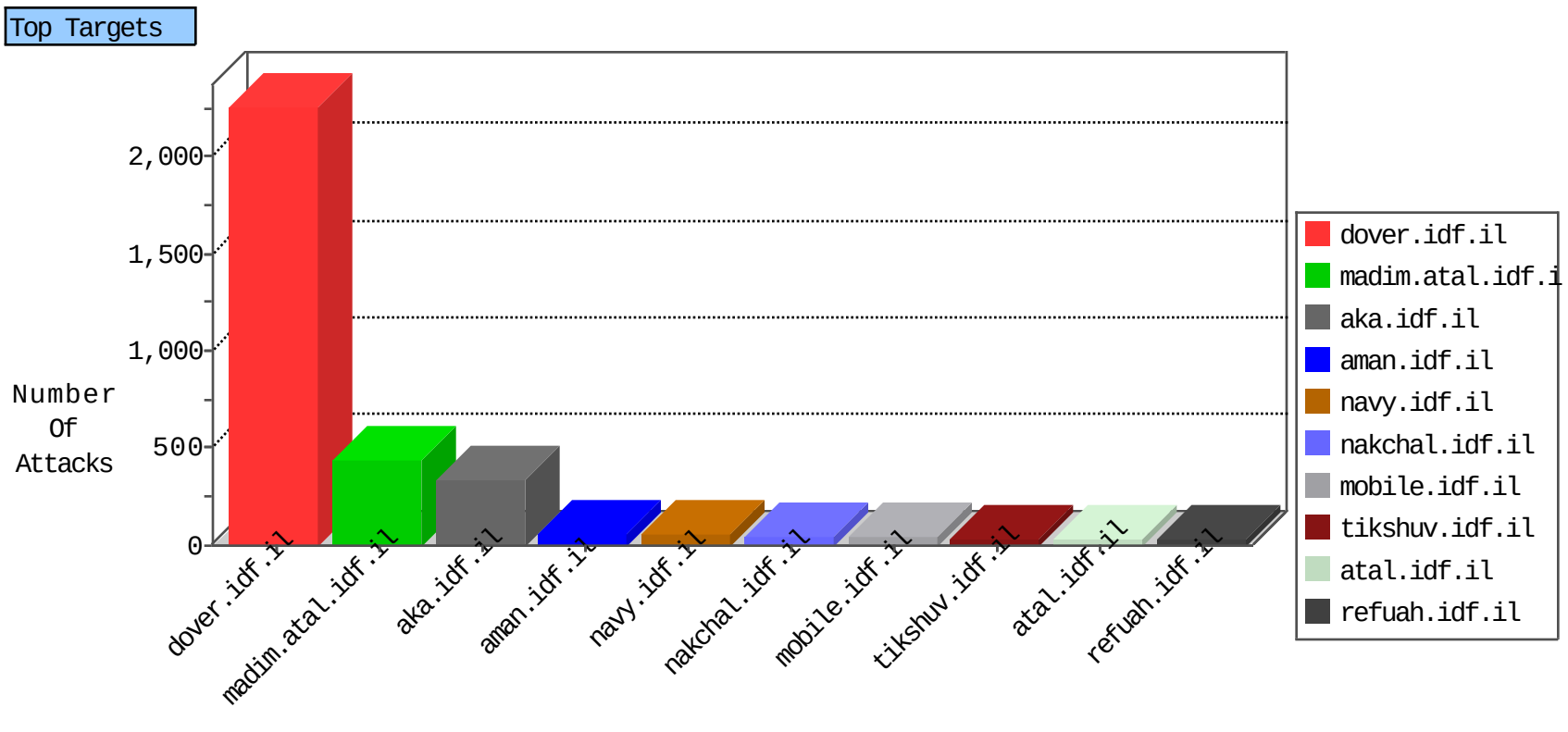
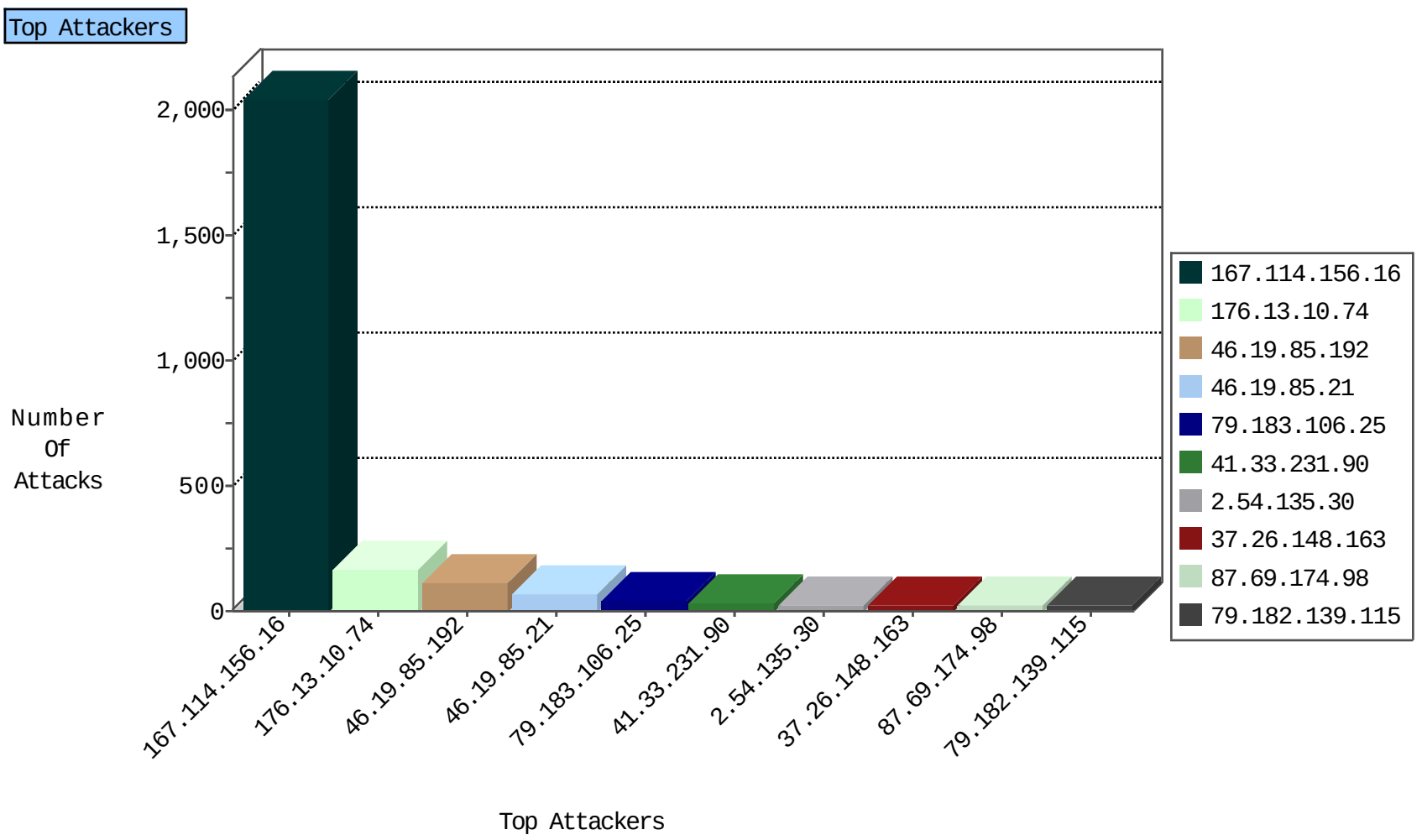
01-13-2016-21:04:00 to 01-13-2016-22:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-13-2016-21:04:00 to 01-13-2016-22:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3014
79.177.11.229	Israel	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	6
185.56.28.67	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

01-13-2016-21:04:00 to 01-13-2016-22:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.202.54.50	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

01-13-2016-21:04:00 to 01-13-2016-22:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.82.64.68	147.237.0.15	Netherlands	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
45.32.36.233	147.237.76.201		e.atal.idf.il	ET SCAN Potential SSH Scan	1
45.32.36.233	147.237.8.14		e.orchot.idf.il	ET SCAN Potential SSH Scan	1
217.132.14.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.7	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
109.67.210.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.238.129.186	147.237.76.177		ncore.idf.il	ET SCAN NMAP -sS window 2048	1
97.32.139.79	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.104.148	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.32.36.233	147.237.76.148		gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
14.168.113.202	147.237.77.212	Vietnam	e.dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
176.51.158.7	147.237.0.33	Russian Federation	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
114.112.90.54	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
104.238.129.186	147.237.76.177		ncore.idf.il	ET SCAN NMAP -sS window 4096	1
104.238.129.186	147.237.76.177		ncore.idf.il	ET SCAN NMAP -f -sS	1

01-13-2016-21:04:00 to 01-13-2016-22:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
2.54.135.30	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
217.132.45.23	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
79.182.139.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
193.43.245.250	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	14
84.228.119.24	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
46.19.85.88	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
2.54.187.67	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
193.43.246.250	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	11
37.26.146.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
79.181.182.78	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
79.181.99.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.147.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
79.179.155.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.174	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
79.179.155.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
212.235.23.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
84.95.45.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.69.34	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.50.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.110.203	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
79.179.96.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.90.89.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.150.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.148.77	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.18.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.170.52	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
23.101.61.176	Ireland	147.237.76.86	navy.idf.il	drop	SAM rule	drop	5
188.120.148.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.88	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
31.210.188.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.228	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
85.65.59.46	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.147.240	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
5.29.238.54	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.228	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
172.56.38.58	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
217.194.193.53	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
68.180.229.168	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
37.26.147.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.199.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.235.23.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.202.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-13-2016-21:04:00 to 01-13-2016-22:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.10.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	130
46.19.85.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
46.19.85.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
79.183.106.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
176.13.10.74	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.10.74	Block	34
46.19.85.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	24
37.26.148.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
46.19.86.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
62.219.154.93	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
79.182.104.148	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.182.104.148	Block	6
79.182.139.115	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.182.139.115	Block	5
17.138.57.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	4
62.90.100.121	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	4
79.183.23.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.65.59.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.192.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.69.149.239	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
87.68.244.156	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.68.244.156	Block	3
176.13.10.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3
79.182.104.148	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/sachar/	Block	2
46.116.76.127	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
95.86.83.231	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.161.129	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	2
87.68.19.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.182.57.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
17.138.57.83	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.57.83	Block	2
188.143.232.19	Russian Federation	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 188.143.232.19	Block	2
2.54.47.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.65.25	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/3/109993.pdf	Block	1
87.69.174.98	Israel	147.237.72.156	aman.idf.il	NULL Character in Method VÃ¼Â±CÃ˜sÂ“Â†	Block	1
83.130.115.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
2.54.10.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.156	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/family	Block	1
46.121.133.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files	Block	1
87.69.174.98	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Header Line from 87.69.174.98	Block	1
79.177.2.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.201.152.3	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.86.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.69.174.98	Israel	147.237.72.156	aman.idf.il	Abnormally Long Request method	Block	1
41.141.12.170	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.141.12.170	Block	1
85.64.16.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.204.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
94.159.178.24	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
87.69.174.98	Israel	147.237.72.156	aman.idf.il	Multiple Malformed URL from 87.69.174.98	Block	1
2.54.148.77	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
62.176.112.77	Bulgaria	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

01-13-2016-21:04:00 to 01-13-2016-22:04:00