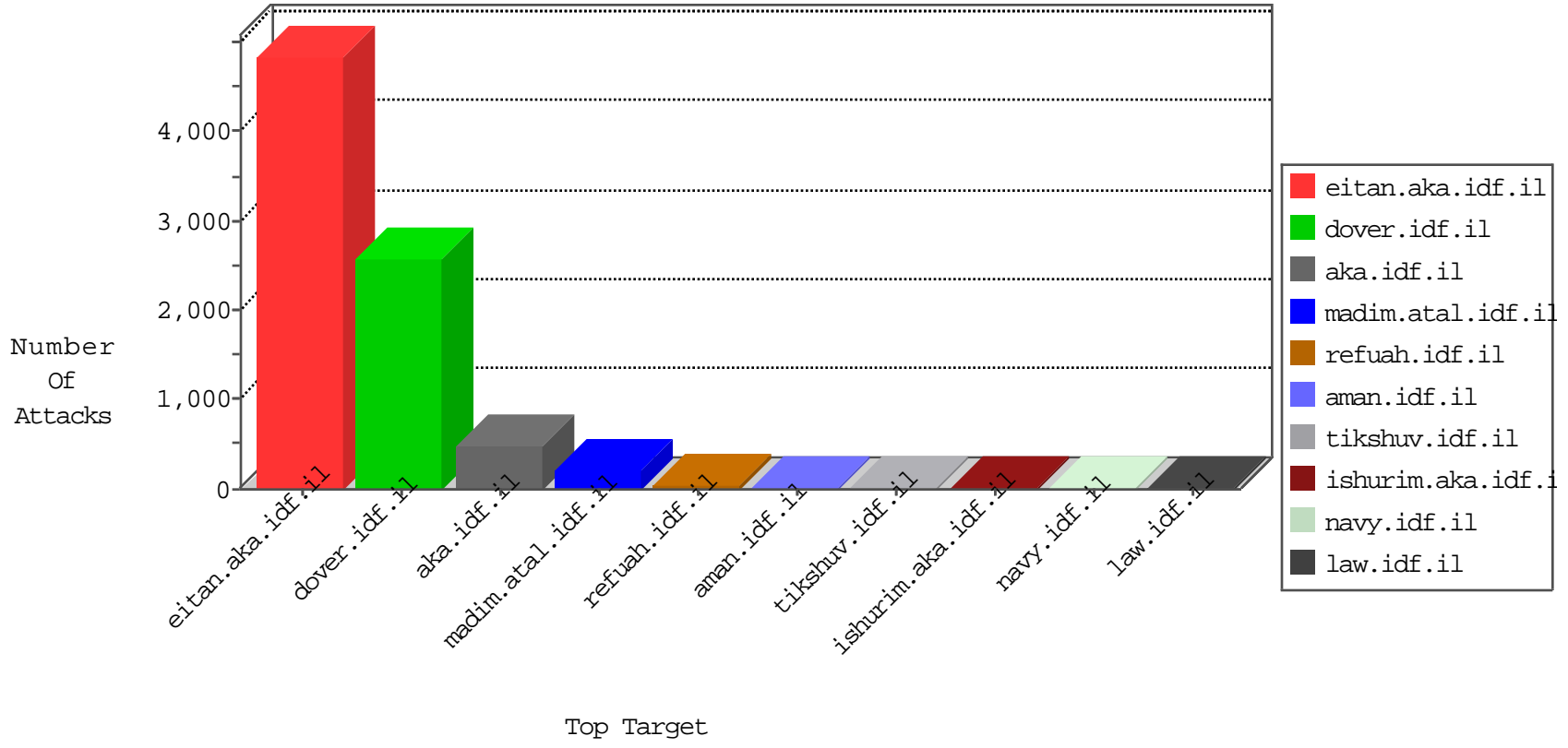


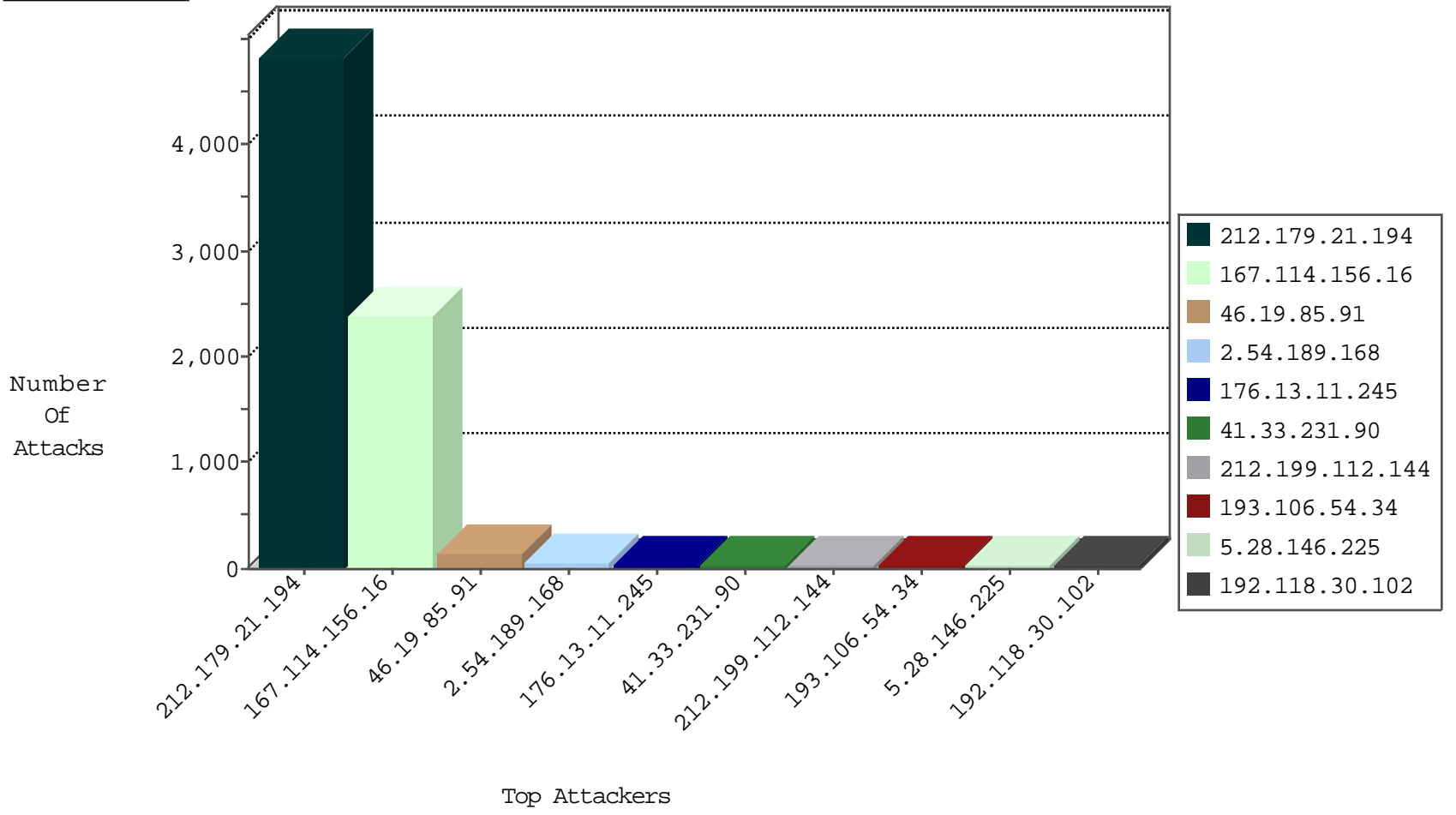
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3597
66.249.75.214	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	506
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	257
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
167.88.7.232	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-trafl	drop	1
167.88.7.252	United States	147.237.77.235	sviva.idf.il	block-sp-trafl	drop	1
118.193.23.46	China	147.237.76.34	yochalan.idf.il	Block_Ntp_All_Net	drop	1
198.48.92.104	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
167.88.7.240	United States	147.237.77.170	maarachot.idf.il	block-sp-trafl	drop	1
167.88.12.207	United States	147.237.0.34	tikshuv.idf.il	block-sp-trafl	drop	1
118.193.23.46	China	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
167.88.7.242	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-trafl	drop	1
167.88.7.229	United States	147.237.77.216	dover.idf.il	block-sp-trafl	drop	1
167.88.7.244	United States	147.237.76.42	refuah.idf.il	block-sp-trafl	drop	1

12-07-2015-16:04:07 to 12-07-2015-17:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.154	Italy	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.205	France	147.237.72.167	ishurim.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.52.137.9	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.78.82	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
217.132.23.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
210.117.121.60	147.237.0.15	Korea, Republic of	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
52.18.188.245	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.155	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
84.109.69.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.158	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
210.117.121.60	147.237.0.15	Korea, Republic of	kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.202.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.184.187	147.237.8.27	Israel	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
80.178.157.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.39	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	180
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
5.28.146.225	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
2.54.189.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
79.176.16.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.137.9	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
193.106.54.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.189.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
149.78.63.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
2.54.189.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
5.28.146.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
2.54.189.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
193.106.54.34	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
193.106.54.34	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
31.168.89.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
89.139.0.240	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.250.67.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.54.176	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.4.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.46.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.126.148.98	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.74	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.186.185.69	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
31.168.89.106	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.74	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.250.67.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.126.148.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
147.235.8.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.57	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
112.198.103.195	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.54.189.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
5.22.129.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.145.221.226	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.29.52.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.142.68.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
5.102.254.93	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.120.125.3		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
37.142.68.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
147.235.8.72	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.57	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
112.198.103.195	Philippines	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
77.126.148.118	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.52.192	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
77.126.148.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.111.128.254	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.189.168	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.21.194	Block	4649
46.19.85.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	99
46.19.85.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	40
176.13.11.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.54.24.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/\$\$\$&?&\$\$\$	Block	8
5.29.113.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.12.141.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.63.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.178.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.179.90.106	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
46.19.85.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.46.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
95.134.121.18	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	2
159.92.1.133	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	2
185.3.144.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.121.203.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	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
80.246.136.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.228.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to ww.aka.idf.il/sip_storage/files/7/	Block	1
31.168.208.53	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.28.36	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
128.232.110.29	United Kingdom	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.66.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/0/61310.jpg	Block	1
195.62.53.168	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /css/css	Block	1
87.69.190.81	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
46.19.86.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.68.72	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	Block	1
79.180.155.187	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/controls/atuda/Â	Block	1
5.29.120.26	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
149.88.149.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
50.154.173.107	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.108.46.162	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.120.126.48		147.237.72.156	aman.idf.il	Illegal Parameter Encoding ct100\$ct100\$cphMain\$CPHMainContent\$ct177s in www.aman.idf.il/modiin/questionnaires.aspx	None	1
79.177.38.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.148.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.147.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
140.247.218.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18485-he/dover.aspx	Block	1
66.249.66.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.86.222	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/size220x0/17672.jpg	Block	1
94.159.183.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.142.68.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.15.30	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.183.36.162	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1397-he/atal.aspx	Block	1