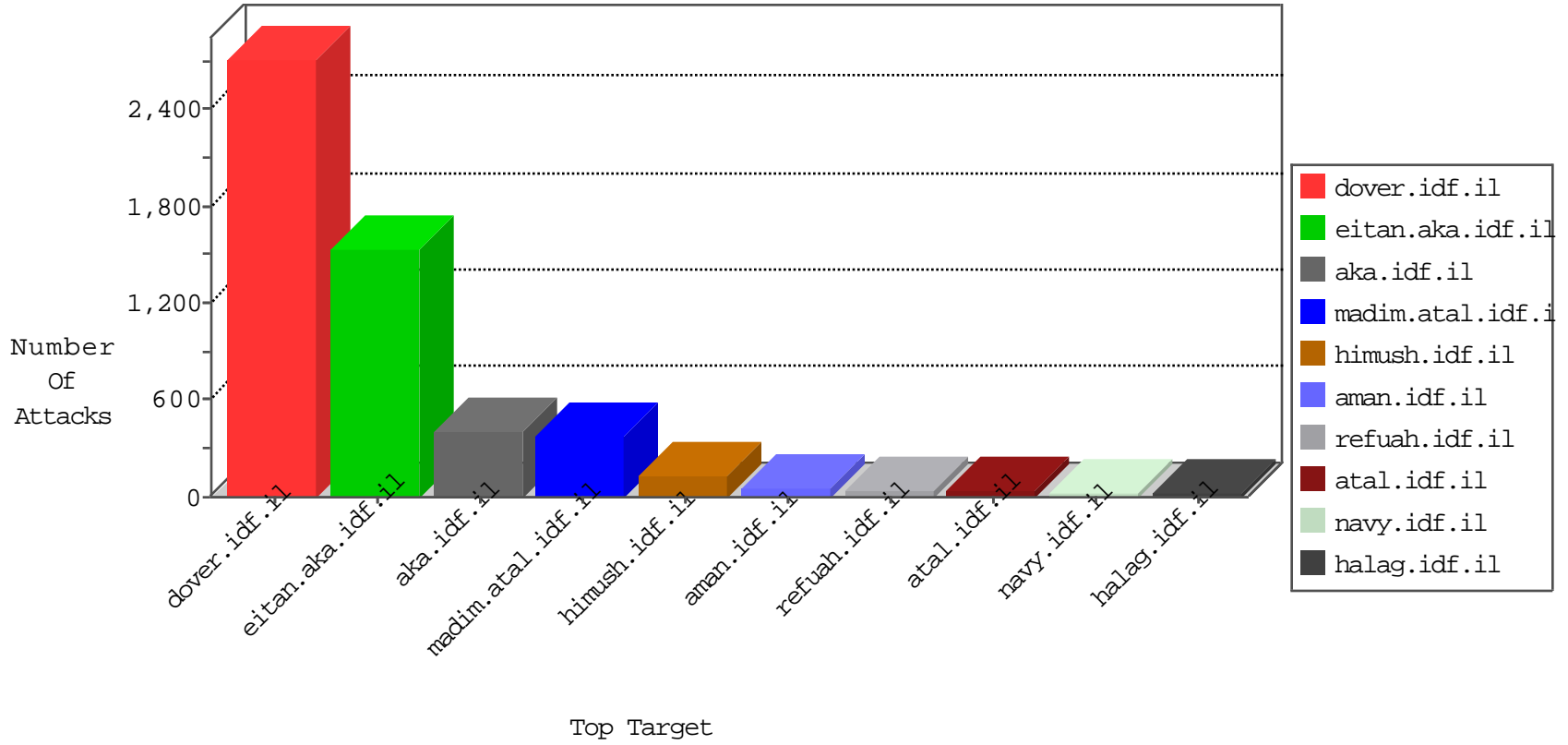


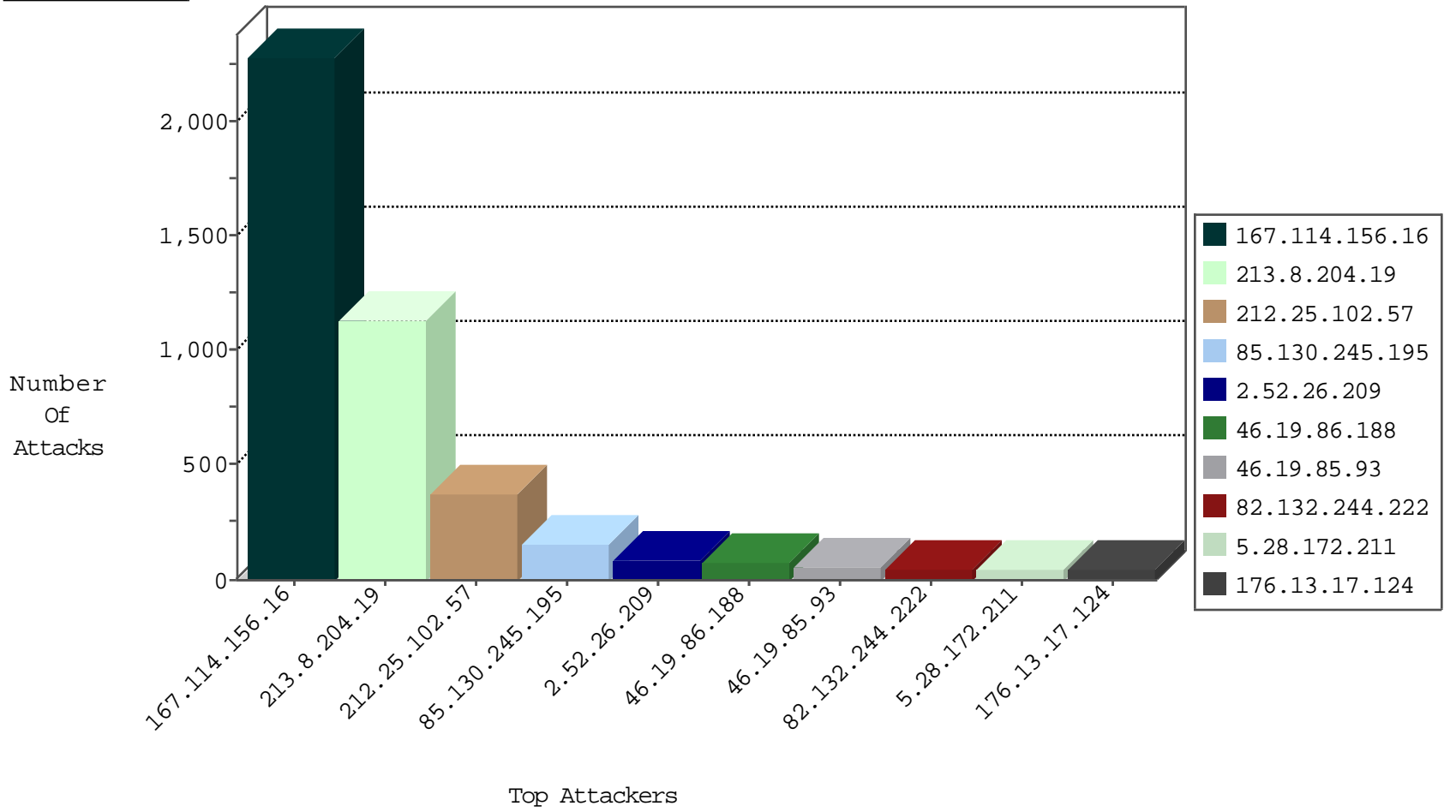
IDF Under Attack Daily Report



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	3060
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
45.32.246.5		147.237.76.201	e.atal.idf.il	Invalid TCP Flags	drop	8
66.249.64.233	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
45.32.246.5		147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	2
71.6.216.43	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.46	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

12-09-2015-12:04:00 to 12-09-2015-13:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.12.70.34	United States	147.237.77.74	law.idf.il	21609: HTTP: pChart Directory Traversal Vulnerability	Block	1
106.38.241.144	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

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	3
84.109.124.28	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.76.42	United States	refuah.idf.il	ET DROP Dshield Block Listed Source	1
80.246.137.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.8.28	Sweden	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 3072	1
137.226.113.7	147.237.72.156	Germany	aman.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	1
45.32.246.5	147.237.72.166		aka.idf.il	ET SCAN NMAP -sS window 1024	1
121.141.225.10	147.237.76.86	Korea, Republic of	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
117.31.224.80	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
115.159.3.147	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
98.119.105.221	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
84.228.21.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.49.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
83.130.117.150	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.200	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
188.226.206.204	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.255.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.66.231.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
121.141.225.10	147.237.0.35	Korea, Republic of	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
117.31.224.80	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
109.67.202.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.8.204.19	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
85.130.245.195	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	45
85.130.245.195	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	44
85.130.245.195	Israel	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	40
5.28.172.211	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	37
79.176.211.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
107.167.108.53	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
80.178.13.85	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
2.52.26.209	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
2.52.26.209	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
66.249.79.6	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
2.52.26.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
2.52.26.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
2.52.26.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	16
79.176.184.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
82.132.244.222	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
82.132.244.222	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
93.173.50.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.76	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
80.246.133.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.28.157.134	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
93.173.50.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
5.28.157.134	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.19.85.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.183.114.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.90	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
80.246.138.160	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.163.164	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
81.218.241.26	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
5.28.172.211	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	8
62.219.110.87	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
82.132.244.222	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
41.206.148.7	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
82.132.244.222	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
82.132.244.222	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
62.0.100.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.161.135	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.26.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.179.21.194	Israel	147.237.77.227	e.hamaz.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.161.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.58.80.11	Netherlands	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	6
62.0.210.1	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
77.125.161.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.78.110.8	Sudan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.204.19	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	845
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	368
213.8.204.19	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 213.8.204.19	Block	144
46.19.86.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
46.19.85.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
176.13.17.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
80.246.139.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
80.246.138.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
46.116.223.180	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (403) in Session from 46.116.223.180	Block	22
213.8.204.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.204.51	Block	22
185.32.179.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
185.32.179.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
80.246.137.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
185.32.179.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
176.13.23.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
213.8.204.33	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
80.246.137.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.246.137.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.12.136.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
80.246.136.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.154.4.36	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	3
80.246.137.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.227.119.27	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/gyus/main/defaulten.asp	Block	3
80.246.136.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.79.25	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
109.186.1.253	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyus/	Block	2
176.13.21.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.64.112.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.111.6.81	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 84.111.6.81	Block	2
80.246.137.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.138.56.78	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.138.56.78	Block	2
79.177.180.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
81.218.37.2	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.37.2	Block	2
80.246.137.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.143.3.44	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
62.219.115.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.175.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.108.158.173	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
79.183.183.79	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct109 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
185.120.125.10		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.13.102.109	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.139.8.180	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
79.178.96.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.20.218	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/popups/markivsachar.aspx	None	1
137.226.113.7	Germany	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1
84.108.67.67	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.8.204.19	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/rules.abe	Block	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