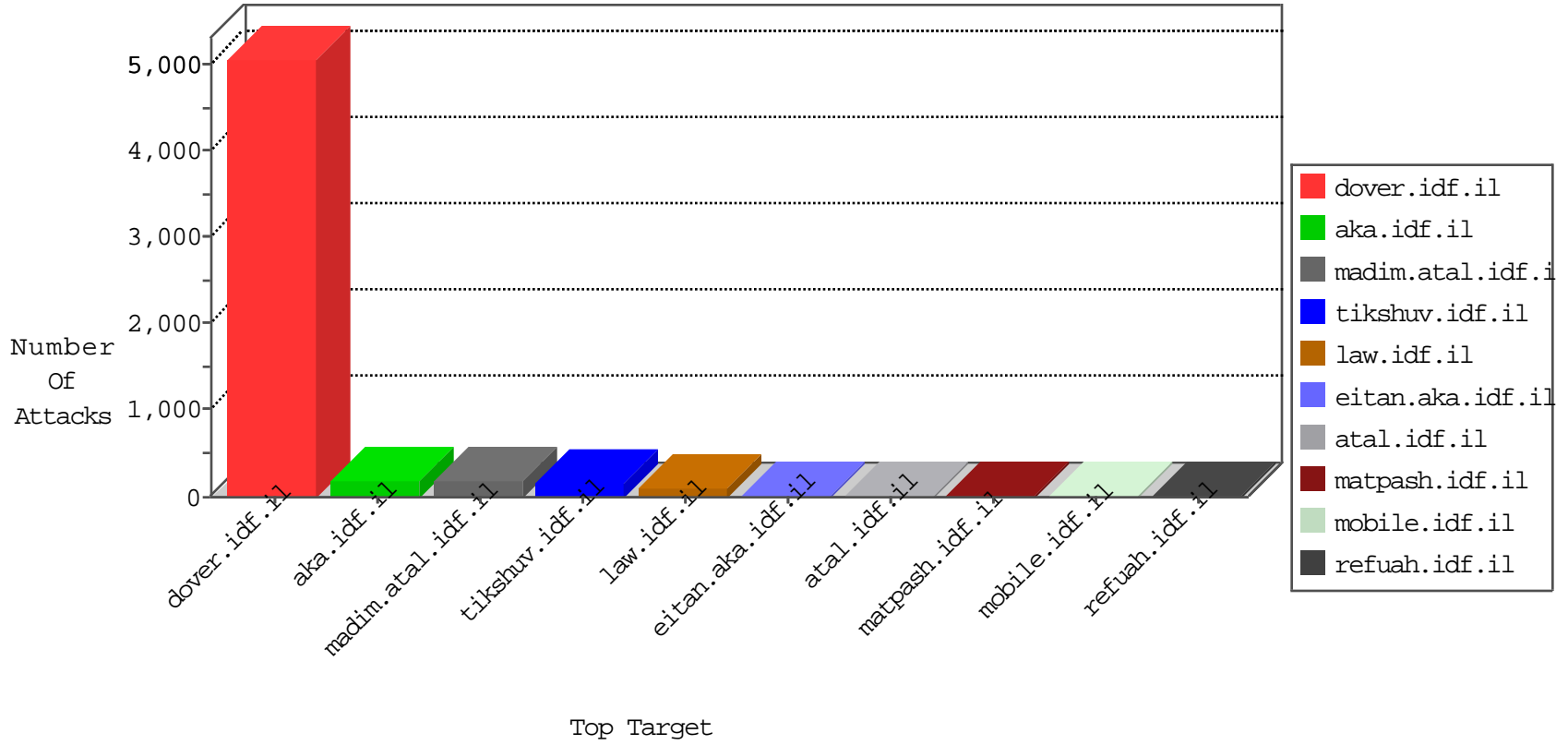


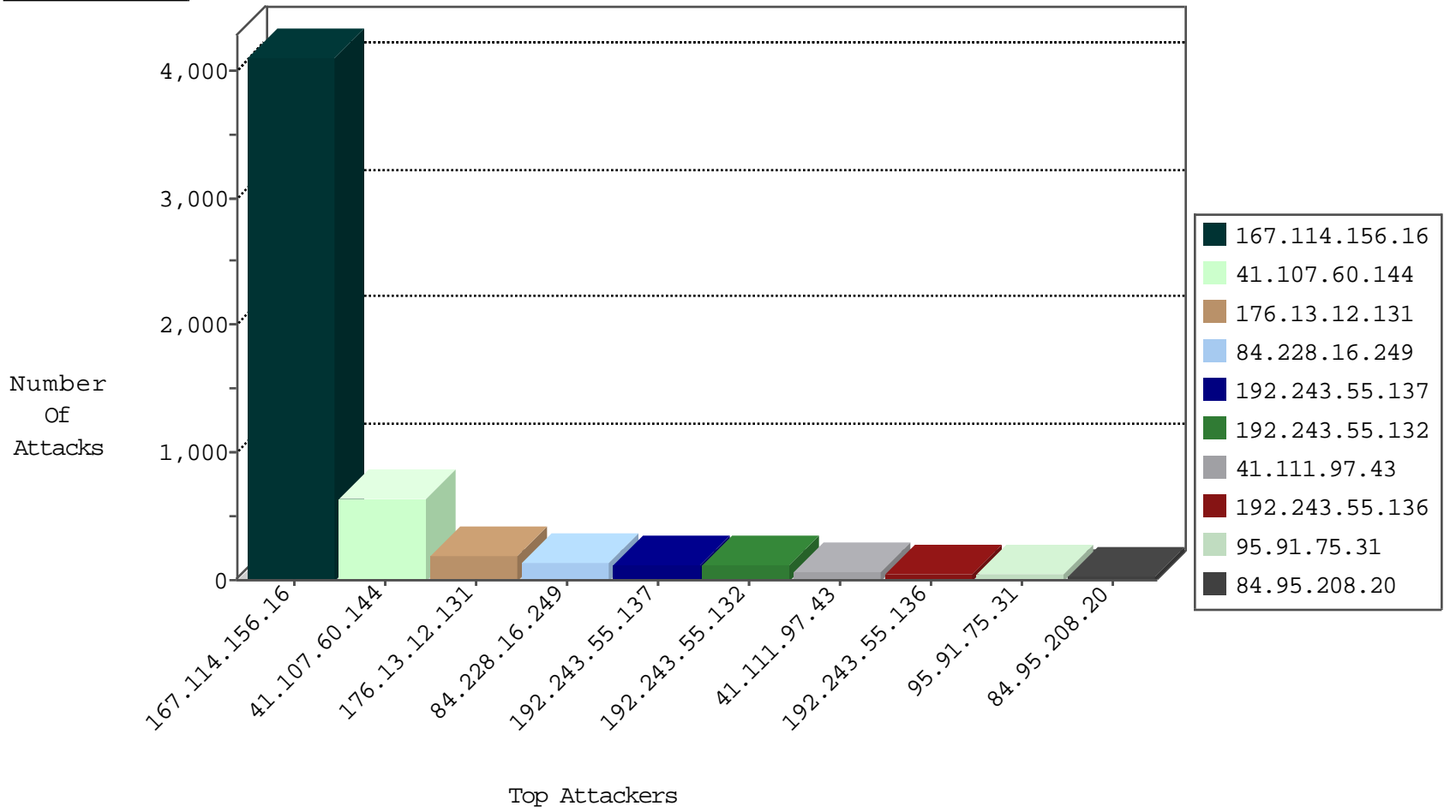
IDF Under Attack Daily Report



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	Block_Ip_Web_In	drop	4085
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	521
176.13.12.131	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	251
41.111.97.43	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	67
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
41.111.97.43	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
95.91.75.31	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
176.31.60.249	France	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
115.86.116.32	Korea, Republic of	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
221.215.106.66	China	147.237.0.16	my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.228.16.249	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
95.91.75.31	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	12
95.91.75.31	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	9
95.91.75.31	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	7
95.91.75.31	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	6
95.91.75.31	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Block	3
51.255.51.68	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
199.30.25.127	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
176.9.131.69	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
95.91.75.31	Germany	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
185.106.92.47	Russian Federation	147.237.76.31	nakchal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
185.106.92.47	Russian Federation	147.237.76.31	nakchal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1

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
185.106.92.47	147.237.76.31	Russian Federation	nakchal.idf.il	ET WEB_SERVER Muieblackcat scanner	1
147.75.194.107	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
90.63.167.235	147.237.0.33	France	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.40.122.194	147.237.76.200	Romania	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
50.46.145.142	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
40.84.149.32	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
186.210.91.216	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.140.23	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
124.105.17.67	147.237.8.28	Philippines	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.248.167.152	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.8.27	Netherlands	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
40.84.149.32	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.228.16.249	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	107
192.243.55.137	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
192.243.55.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.137	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
41.107.60.144	Algeria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
46.121.211.156	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
93.172.4.114	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
79.178.28.149	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.132	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
108.40.117.111	United States	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.76.127.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.137	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.132	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
105.192.246.239	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.16.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.137	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.137	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.65.224.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.132	United States	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
192.243.55.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
66.102.9.89	United States	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.132	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
37.187.200.36	France	147.237.76.44	e.refuah.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	4
67.50.128.28	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
107.167.102.176	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
93.172.4.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.136	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.132	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.12.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	161
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	11
213.57.91.199	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized HTTP Method	Block	8
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
192.243.55.132	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	6
79.179.18.64	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	5
2.55.188.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.91.199	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/sip_storage/files/0/	Block	3
199.30.25.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.25.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.14.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.102.7.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
192.243.55.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	3
79.179.18.64	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.179.18.64	Block	3
199.30.25.146	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.25.156	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.155	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.2.174	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
199.30.24.161	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
199.30.25.177	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.205	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.148	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.25.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.229	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.232	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.25.5	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
62.210.116.228	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
79.182.216.51	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 79.182.216.51 (Open Mode)	None	1
199.30.25.37	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.153.33.145	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
192.243.55.132	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
14.192.211.166	Malaysia	147.237.77.74	law.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
62.210.116.228	France	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
46.121.62.81	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
54.153.33.145	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
192.243.55.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
14.192.211.166	Malaysia	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
46.121.209.103	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
62.210.116.228	France	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
130.185.155.82	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
24.142.27.209	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1