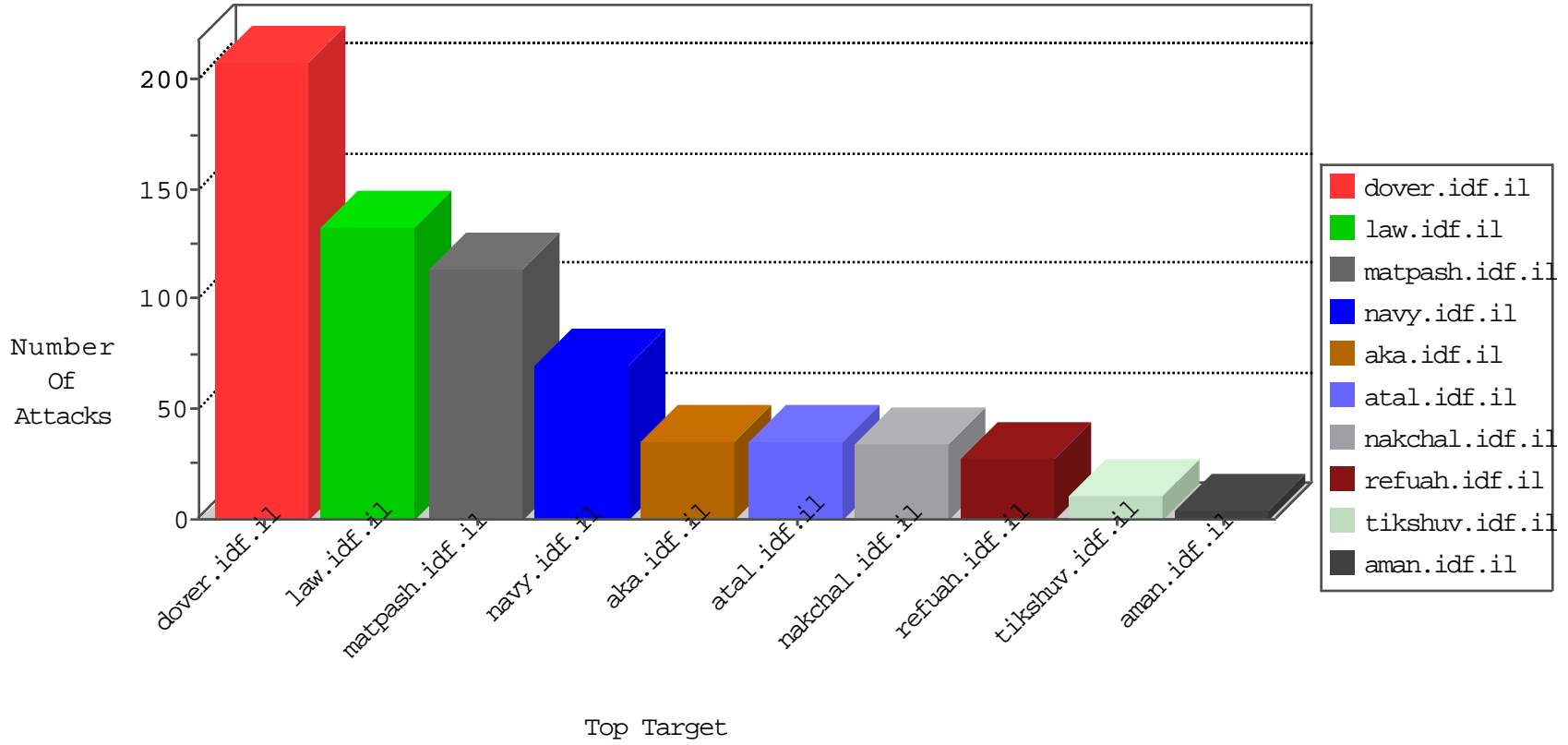


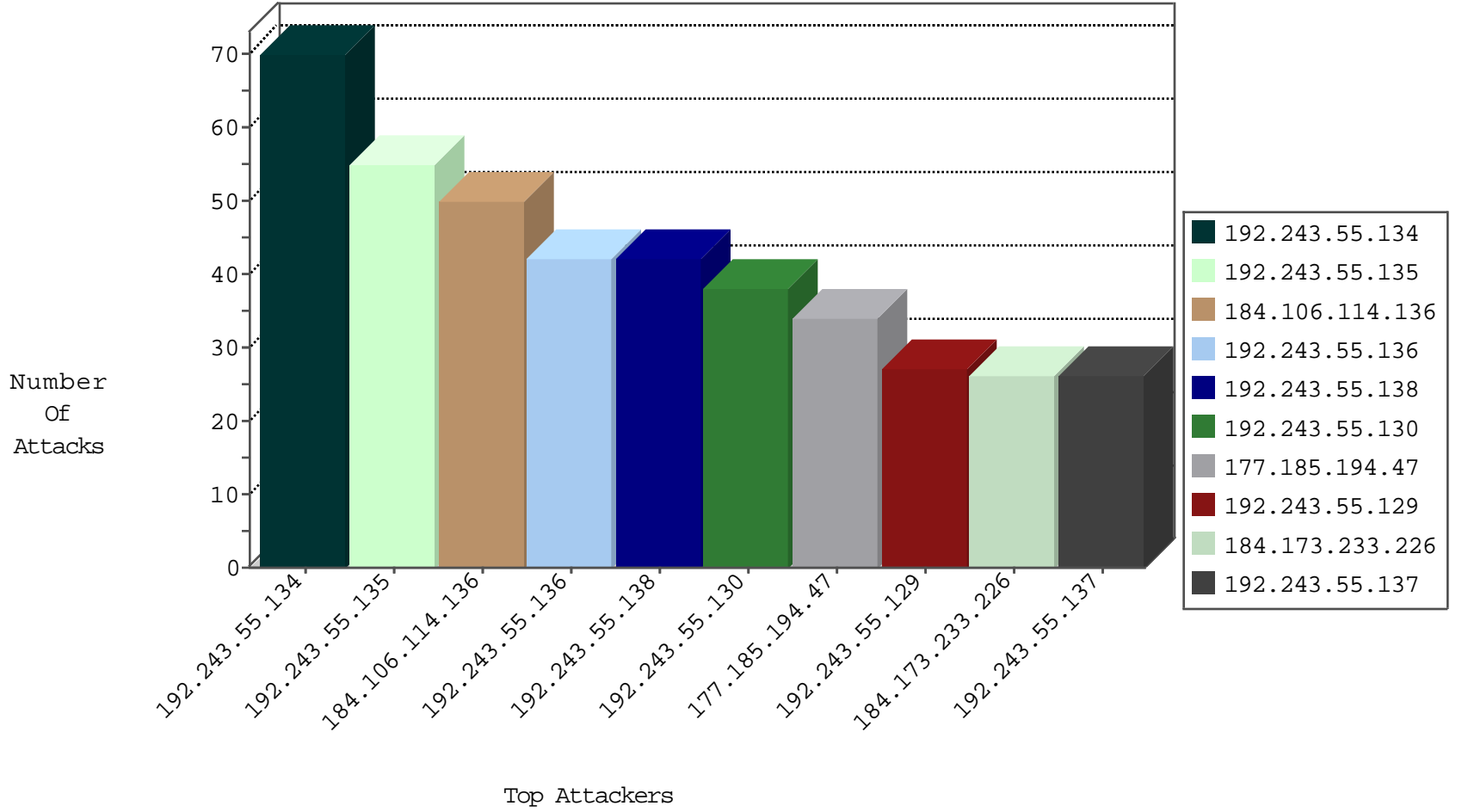
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.46.189	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
222.186.31.236	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
222.174.5.28	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
185.130.5.201		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.106.114.136	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	9
184.106.114.136	United States	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
177.185.194.47	Brazil	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
184.173.233.226	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
184.106.114.136	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
177.185.194.47	Brazil	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
177.185.194.47	Brazil	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
66.135.63.82	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
184.173.233.226	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
149.88.113.120	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
149.202.48.207	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	2
93.173.125.33	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
163.172.13.244	United Kingdom	147.237.77.176	matpash.idf.il	C1000106: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
87.71.7.15	Israel	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
184.106.114.136	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	26
177.185.194.47	147.237.76.31	Brazil	nakchal.idf.il	SQL Injection - Select From	18
184.173.233.226	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	14
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	11
66.135.63.82	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
190.140.220.170	147.237.8.28	Panama	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
146.148.116.152	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 3072	1
146.148.116.152	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -f -sS	1
115.28.218.77	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
71.6.165.200	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
146.148.116.152	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 2048	1
123.133.17.135	147.237.77.19	China	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
88.247.217.15	147.237.8.28	Turkey	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
71.6.165.200	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
59.45.79.117	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.210.226.9	France	147.237.77.233	atal.idf.il	drop	SAM rule	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
210.117.199.102	Korea, Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.134	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.136	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
210.117.199.102	Korea, Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.133	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.133	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.134	Dominica	147.237.77.176	matpash.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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.130	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
216.185.43.135	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.129	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence		monitor	4
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.136	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.130	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.134	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.73.145.90	Turkey	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	7
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 148.251.21.227	Block	3
80.246.133.45	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 80.246.133.45	Block	2
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
69.126.111.234	United States	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
208.70.28.119	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
128.232.110.28	United Kingdom	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
89.161.145.161	Poland	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
157.55.39.49	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
98.169.245.244	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
76.120.79.245	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
208.70.28.122	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
129.116.175.197	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
89.161.145.161	Poland	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/xmlrpc.php	Block	1
66.249.74.47	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 66.249.74.47	Block	1
203.127.96.250	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
98.169.245.244	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
80.246.133.45	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz/resources/images/innerpage/goback.gif	Block	1
37.187.114.171	France	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to /sap/hana/admin/	Block	1
208.115.113.82	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
148.251.21.227	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/hovot/templates/main.asp	Block	1
89.161.198.15	Poland	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
66.249.74.47	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
207.46.13.42	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
110.22.45.236	Australia	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/english	Block	1
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
220.255.146.34	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
89.161.198.15	Poland	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/xmlrpc.php	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8928-he/refuah.aspx	Block	1
207.46.13.193	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1
119.73.253.5	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1