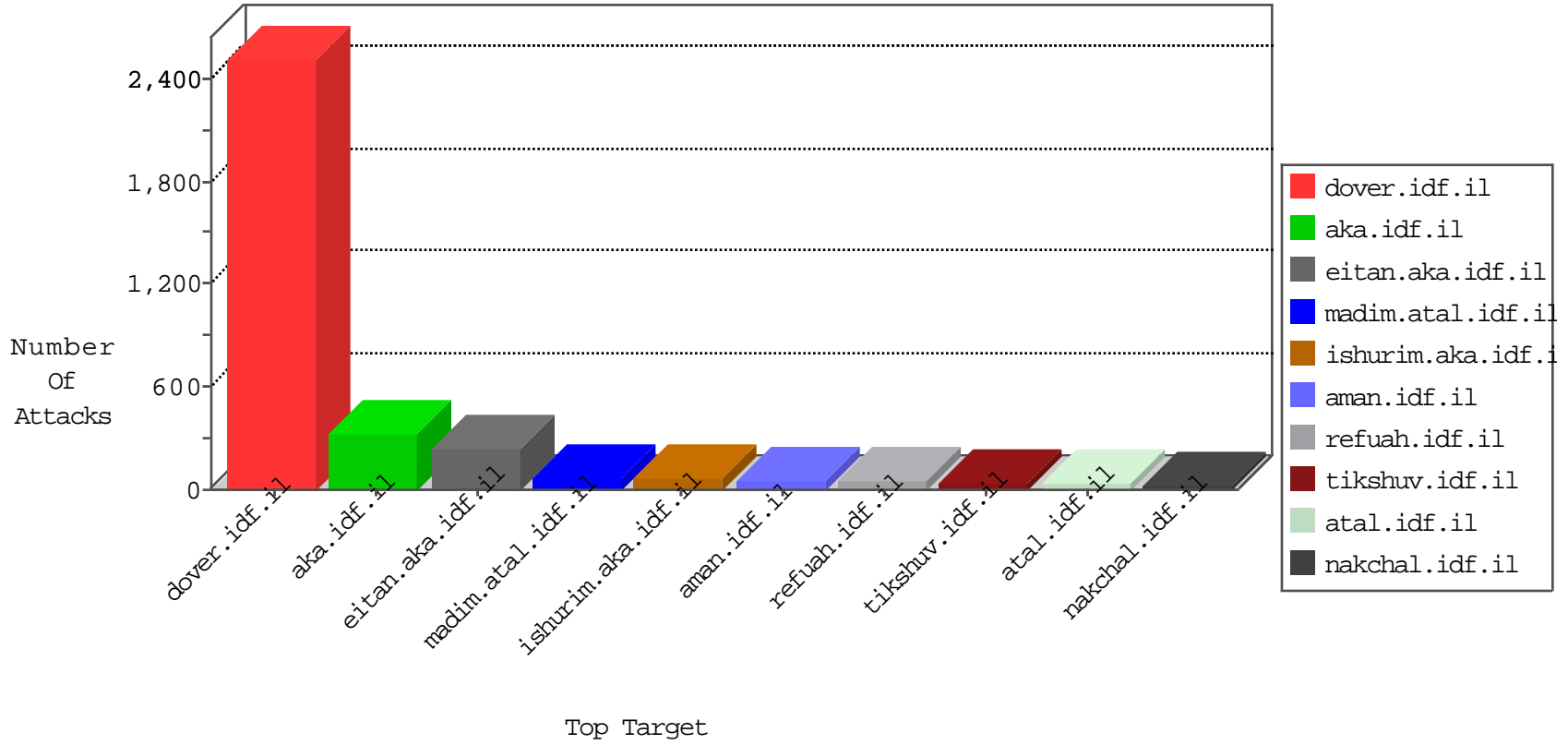


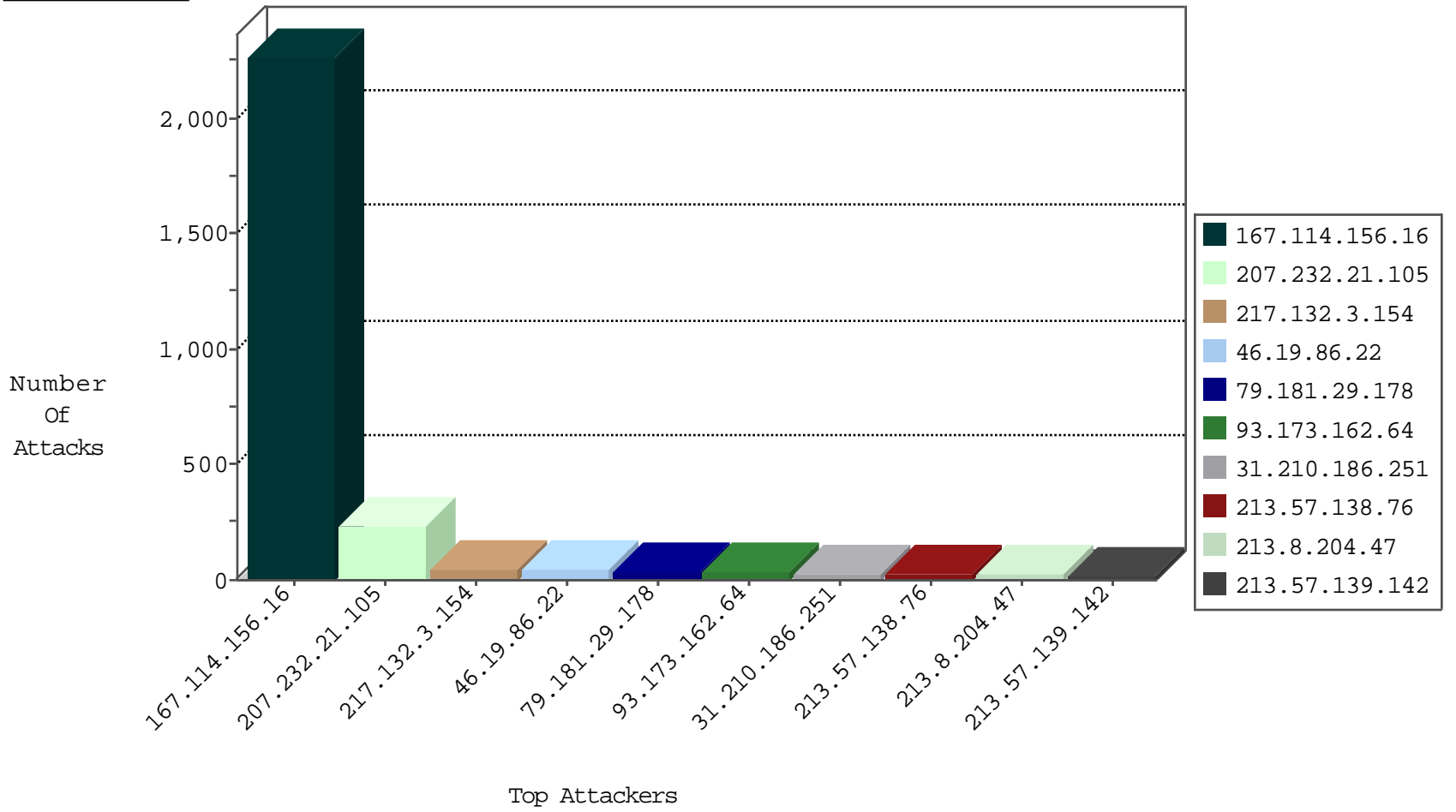
IDF Under Attack Daily Report



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	3649
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	28
109.65.204.207	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.183.56.19	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
109.66.56.35	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	6
79.183.56.19	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
109.66.56.35	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
94.228.214.44	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
158.69.214.116	United States	147.237.77.176	matpash.idf.il	C1000106: HTTP: majestic bot	Block	1
188.165.15.87	France	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	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	8
77.125.126.140	147.237.72.156	Israel	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
66.249.78.82	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
173.160.184.241	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
142.54.163.74	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 3072	1
124.195.223.142	147.237.76.201	Maldives	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.77.79.38	147.237.72.217	China	e.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
124.195.223.142	147.237.76.31	Maldives	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.116.147	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
124.195.223.142	147.237.0.33	Maldives	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.116.147	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
85.30.51.119	147.237.0.35	Sweden	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
199.101.186.202	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
199.101.186.202	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -f -sS	1
173.160.184.241	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
149.78.97.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
142.54.163.74	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
124.195.223.142	147.237.76.148	Maldives	ggcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.116.147	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
124.195.223.142	147.237.0.34	Maldives	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.116.147	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
124.195.223.142	147.237.0.19	Maldives	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
207.46.140.7	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.202	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
46.234.109.121	147.237.0.16	Czech Republic	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.22	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	41
207.232.21.105	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
213.8.204.47	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
213.57.139.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
31.210.186.251	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
213.57.138.76	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
41.202.219.68	Cameroon	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
213.57.138.76	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
79.179.19.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
31.210.186.251	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack		reject	10
87.68.245.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
87.68.71.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.181.29.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
84.228.235.32	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
5.28.158.84	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
93.173.162.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
80.246.136.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
79.181.29.178	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.181.29.178	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
80.246.136.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
79.182.64.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.210.186.251	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
5.144.57.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.16.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.146.167	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.120.125.56		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.64.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.235.32	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.66.109.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.173.162.64	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
85.65.2.91	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
108.60.138.226	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.59.113	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.181.29.178	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
79.181.29.178	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
5.144.57.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.65.2.91	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
93.173.162.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
84.109.20.180	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
93.173.162.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.109.233.130	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.232.21.105	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 207.232.21.105	Block	197
217.132.3.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
79.178.19.72	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.178.19.72	Block	4
77.127.182.148	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.127.182.148	Block	3
37.26.146.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
173.13.253.73	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authentication-service.asmx/getauthuser	Block	2
79.177.128.113	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	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
84.111.139.163	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
213.57.178.104	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
46.19.85.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	2
46.19.86.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.177.128.113	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	2
2.54.4.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.229.39.165	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/maln/sacnar	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yoman/yoman.asp	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1631-he/refuah.aspx	Block	1
119.130.98.0	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/usercontrols/headerupper/	Block	1
80.246.136.156	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 80.246.136.156 (Unknown SSL Session)	None	1
213.57.208.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.128.113	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
52.32.245.167	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	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
77.237.154.221	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized Method HEAD for /	Block	1
176.13.20.102	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.144.57.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.11.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
84.94.189.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
141.212.122.129	United States	147.237.77.235	sviva.idf.il	Distributed Malformed URL	Block	1
109.66.149.56	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
79.180.28.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.174.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
52.91.175.197	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
37.142.68.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.215.198.135	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
195.62.53.168	Russian Federation	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /css/css	Block	1
66.249.78.15	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/163-4314-en/patzar.aspx5	Block	1
173.13.253.73	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
2.54.6.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.60.23	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
66.249.66.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
136.243.61.196	Germany	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/shared/usercontrols/headerupper/	Block	1
80.246.136.156	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
213.57.228.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.227.93	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
52.32.245.167	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1