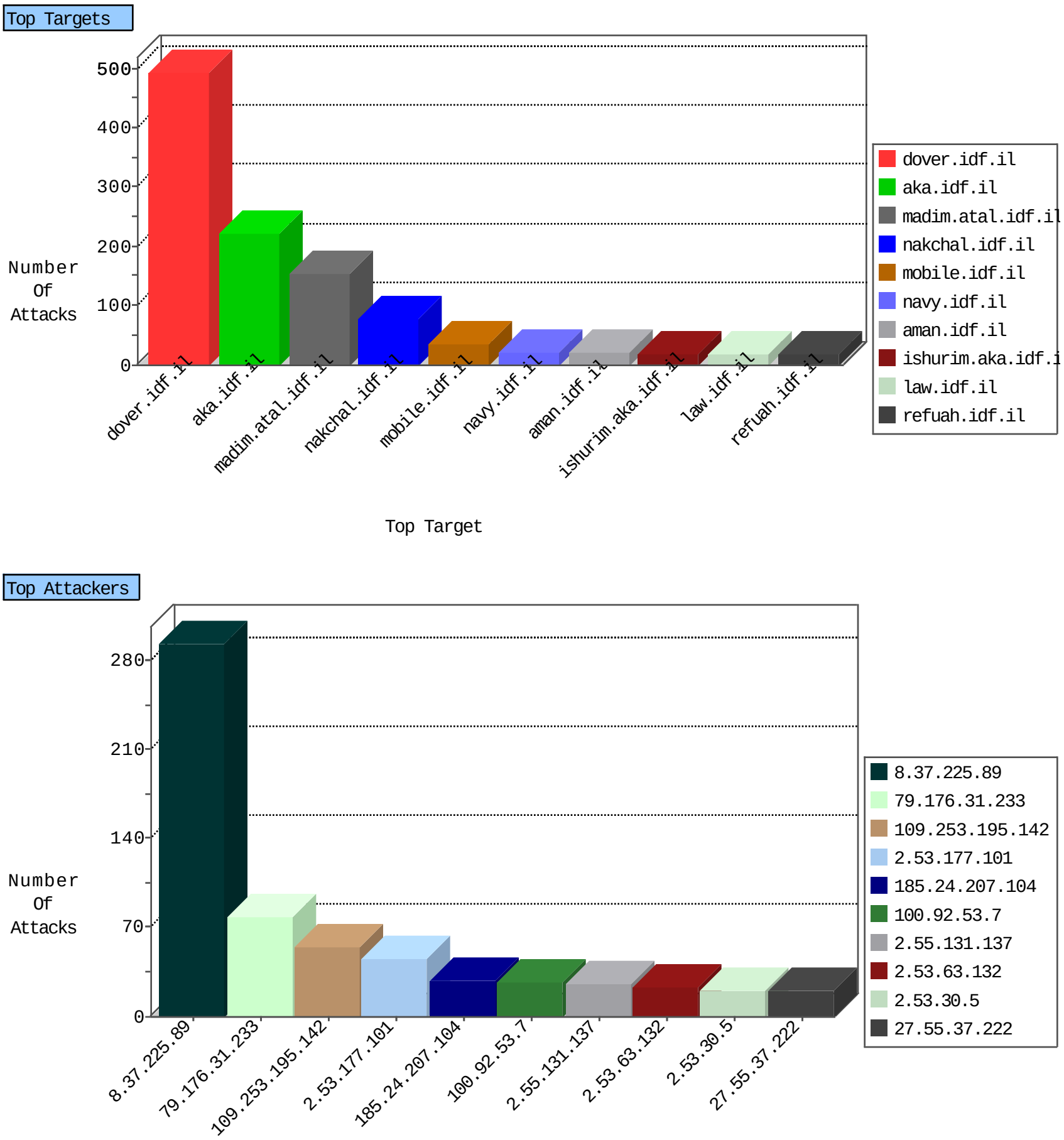
09-21-2016-17:04:05 to 09-21-2016-18:04:05

IDF Under Attack Daily Report



09-21-2016-17:04:05 to 09-21-2016-18:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.226.136	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	40
46.19.85.138	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.53.161.101	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
8.37.225.89	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
123.59.59.52	China	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
68.180.231.57	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
147.236.238.55	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
24.99.45.58	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1

09-21-2016-17:04:05 to 09-21-2016-18:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
193.111.140.153	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
213.239.205.207	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-21-2016-17:04:05 to 09-21-2016-18:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
77.125.94.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.60.153.178	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
46.121.60.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.56.151	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.154.19.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.50	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.50	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
87.69.62.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.149.231.57	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
81.28.96.74	147.237.0.15	France	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
185.32.179.19	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.231.210	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.228.194.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.31.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.24.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
47.88.4.204	147.237.72.156	Canada	aman.idf.il	ET SCAN NMAP -sS window 1024	1
95.86.115.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.56.151	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.50	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
89.138.174.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.174.125.53	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
81.218.131.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.120.126.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.42	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.76.15.159	147.237.72.166	China	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.234.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
110.5.109.236	147.237.0.19	Indonesia	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1

09-21-2016-17:04:05 to 09-21-2016-18:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.225.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	275
79.176.31.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	77
100.92.53.7		147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	21
27.55.37.222	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
207.241.226.144	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	16
2.55.131.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
185.24.207.104	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
2.55.131.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.53.177.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.19.85.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.85.148	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
8.37.225.89	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
2.53.63.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
185.24.207.104	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
176.13.234.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.193	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.92.53.7		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.125.45.210	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.53.177.108	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.253.139.58	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
187.33.38.114	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
2.53.44.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
77.125.7.225	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
185.24.207.104	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.85.201	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.148	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.24.207.104	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	4
2.53.172.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.180	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.138.135.254	France	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
8.37.225.89	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
176.13.237.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.246.139.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
62.0.197.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.207.207	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	3
195.182.96.4	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.63.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
2.55.131.137	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.53.63.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
87.69.160.52	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.63.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.55.140.0	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
80.246.139.23	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.53.63.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
187.33.38.114	Brazil	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.63.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.69.43.221	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

09-21-2016-17:04:05 to 09-21-2016-18:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.195.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
2.53.177.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	46
2.53.30.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
77.126.33.85	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 77.126.33.85	Block	15
80.246.137.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
194.90.198.10	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	9
194.90.198.10	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 194.90.198.10	Block	8
2.53.30.5	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	6
77.139.139.243	France	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	5
2.55.52.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
194.90.198.10	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	3
46.19.85.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.209.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.250.160.243	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
5.102.195.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.140.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.138.79.19	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
169.229.3.91	United States	147.237.77.234	halag.idf.il	Abnormally Long Header Line request header name	Block	1
46.19.85.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.19.86.180	Israel	147.237.0.34	tikshuv.idf.il	Malformed URL	Block	1
180.76.15.163	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list.htm	Block	1
109.253.156.172	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
66.102.9.26	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Header Name	Block	1
46.19.85.112	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
85.250.160.243	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	1
46.19.86.180	Israel	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method es.186.dfb3=* in URL	Block	1
192.116.199.98	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/113484.pdf	Block	1
2.55.183.231	Israel	147.237.77.234	halag.idf.il	Parameter Type Violation search in www.logistics.atal.idf.il/1213-he/halag.aspx	Block	1
77.139.139.243	France	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/	Block	1
66.249.64.128	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Malformed URL	Block	1
89.138.174.170	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
62.219.137.5	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
192.157.252.155	United States	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
204.12.255.130	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.64.185	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/brothers/gallery/showpicture.asp	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Unknown HTTP Request Method &b";Q8 in URL	Block	1
109.64.43.101	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
77.126.33.85	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1134-he/navy.asp	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
192.157.252.155	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/blog/wp-login.php	Block	1
157.55.39.218	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
37.26.147.209	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.109.38.47	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
204.12.255.130	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/7/307.pdf/wp-login.php	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1

09-21-2016-17:04:05 to 09-21-2016-18:04:05