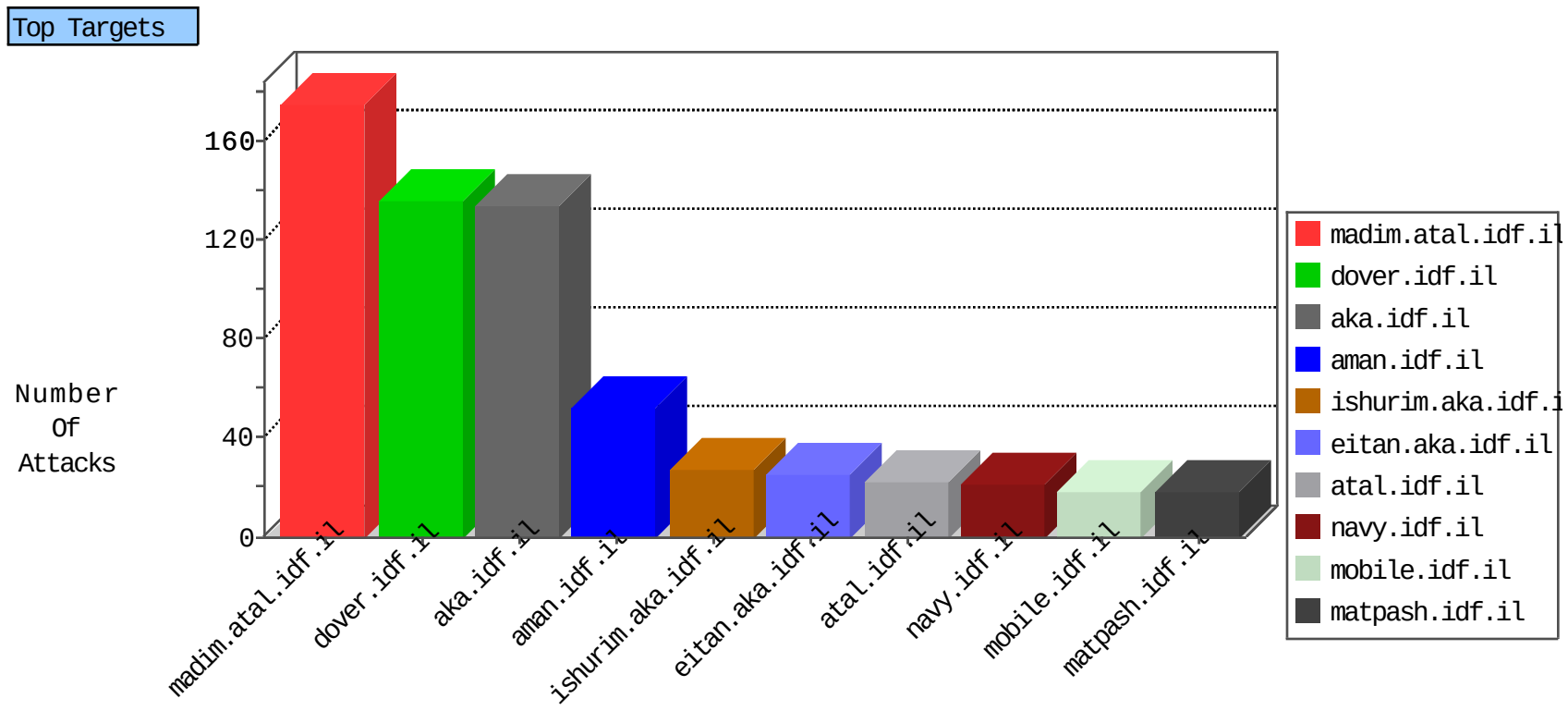
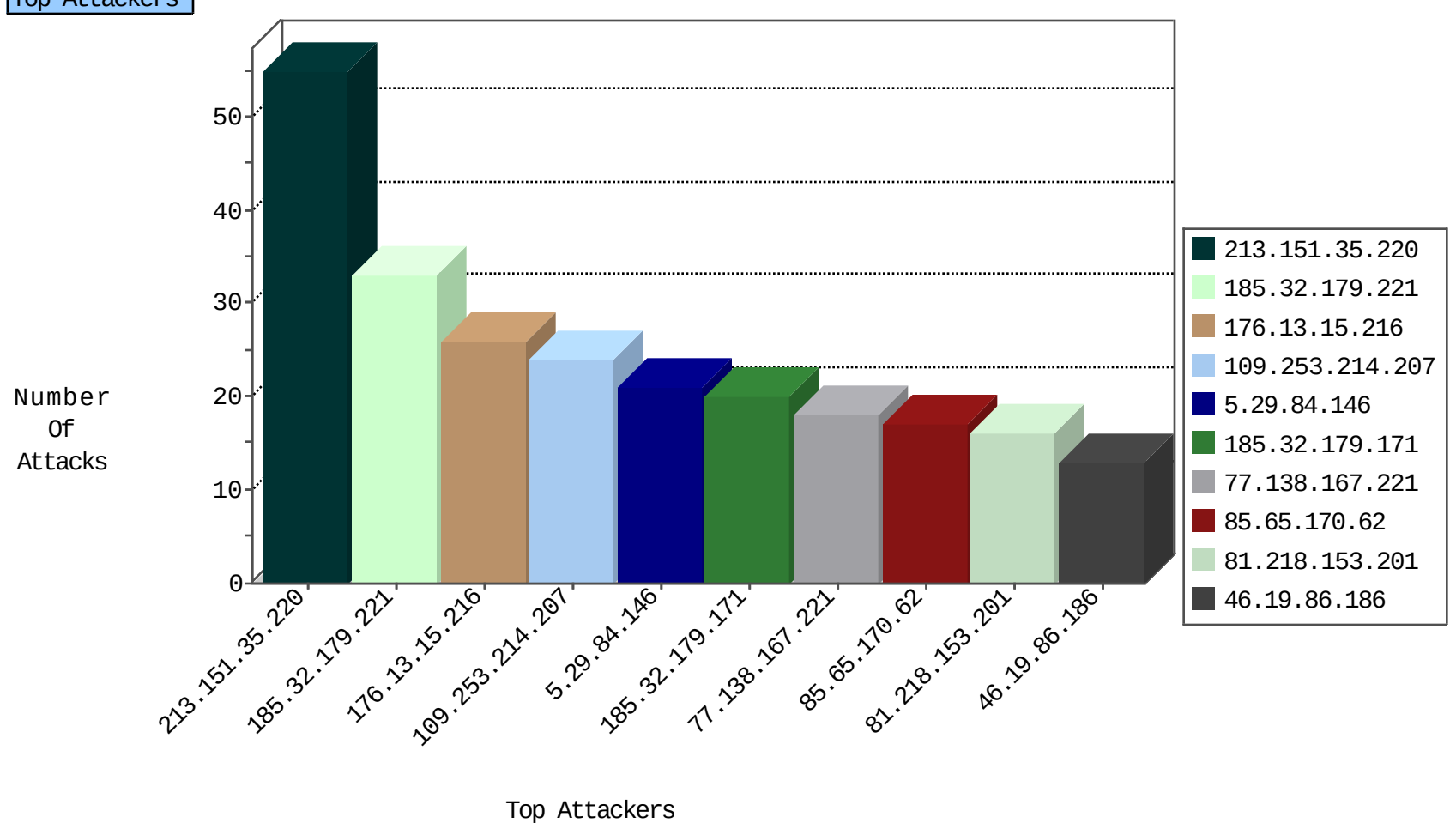
09-19-2016-20:04:05 to 09-19-2016-21:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-19-2016-20:04:05 to 09-19-2016-21:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.105.139	Israel	147.237.77.233	atal.idf.il	Black List	drop	6
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
195.62.53.168	Russian Federation	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
165.242.90.129	Japan	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1

09-19-2016-20:04:05 to 09-19-2016-21:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

09-19-2016-20:04:05 to 09-19-2016-21:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.135	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	2
46.19.85.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.33.116.208	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
200.98.129.133	147.237.76.31	Brazil	nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.32.179.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.60.153.178	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
106.120.118.2	147.237.72.166	China	aka.idf.il	GPL SCAN nmap TCP	1
66.249.93.139	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	1
46.120.61.23	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.4.85.112	147.237.0.200	Germany	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.146.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.121.115.189	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
200.98.129.133	147.237.0.200	Brazil	m4u.idf.il	ET SCAN Potential SSH Scan	1
129.194.184.66	147.237.76.42	Switzerland	refuah.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.0.15	Russian Federation	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
69.162.69.222	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1

09-19-2016-20:04:05 to 09-19-2016-21:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.218.153.201	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
79.180.181.34	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.32.179.221	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
185.32.179.221	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
185.32.179.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
87.69.180.230	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
109.253.147.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
176.13.11.23	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	9
79.178.177.223	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.26.148.138	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.86.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
212.235.16.21	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
185.32.179.171	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
37.26.148.185	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.66.173.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.35.247	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
84.229.43.14	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
31.154.81.9	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
176.13.229.204	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.143.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.138.112	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.186	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.86.60	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
73.1.125.243	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.86.186	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
2.53.2.251	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
178.39.218.11	Switzerland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
73.1.125.243	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.253.158.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.66.19.85	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
82.81.16.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.205.124.207	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.32.179.171	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.32.179.171	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	2
77.138.177.161	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.54.220.176	Ukraine	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
84.109.236.130	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.253.147.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
185.3.147.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.80	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.22.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.66.62.230	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
5.29.182.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
37.54.220.176	Ukraine	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
141.226.232.16	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

09-19-2016-20:04:05 to 09-19-2016-21:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.151.35.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
176.13.15.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
109.253.214.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
5.29.84.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
85.65.170.62	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	17
46.19.85.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
77.138.167.221	France	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	10
77.138.167.221	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.167.221	Block	8
46.19.85.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
185.32.179.171	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
37.26.148.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
46.120.255.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.70.242.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.108.24.213	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	2
77.138.29.153	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/megurim/	Block	2
77.139.236.27	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunsummary.aspx	Block	2
66.249.93.156	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
192.116.81.41	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
64.41.200.101	United States	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.101 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
213.151.61.29	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/brothers/news/	Block	1
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
176.13.1.242	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
80.246.139.96	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	1
66.249.93.157	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
194.187.170.130	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il./robots.txt	Block	1
64.41.200.101	United States	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.101 (Unsupported Cipher)	None	1
106.186.113.132	Japan	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteyerua/	Block	1
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method &l=he&f=1133&d=21240 in URL	Block	1
82.81.63.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.149.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.228.159	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1035-he/cogat.aspx	Block	1
195.62.53.168	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to gmail.com/engine/log.txt	Block	1
64.41.200.101	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
106.186.113.132	Japan	147.237.77.233	atal.idf.il	NULL Character in Method	Block	1
46.19.85.46	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
77.139.184.54	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
46.19.86.94	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
176.13.229.204	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.54.220.176	Ukraine	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/5/2635.jpg	Block	1
207.46.13.165	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
64.41.200.101	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	1
109.66.62.230	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
2.53.57.153	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	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
40.77.167.55	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
77.138.117.58	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/drushim	Block	1

09-19-2016-20:04:05 to 09-19-2016-21:04:05