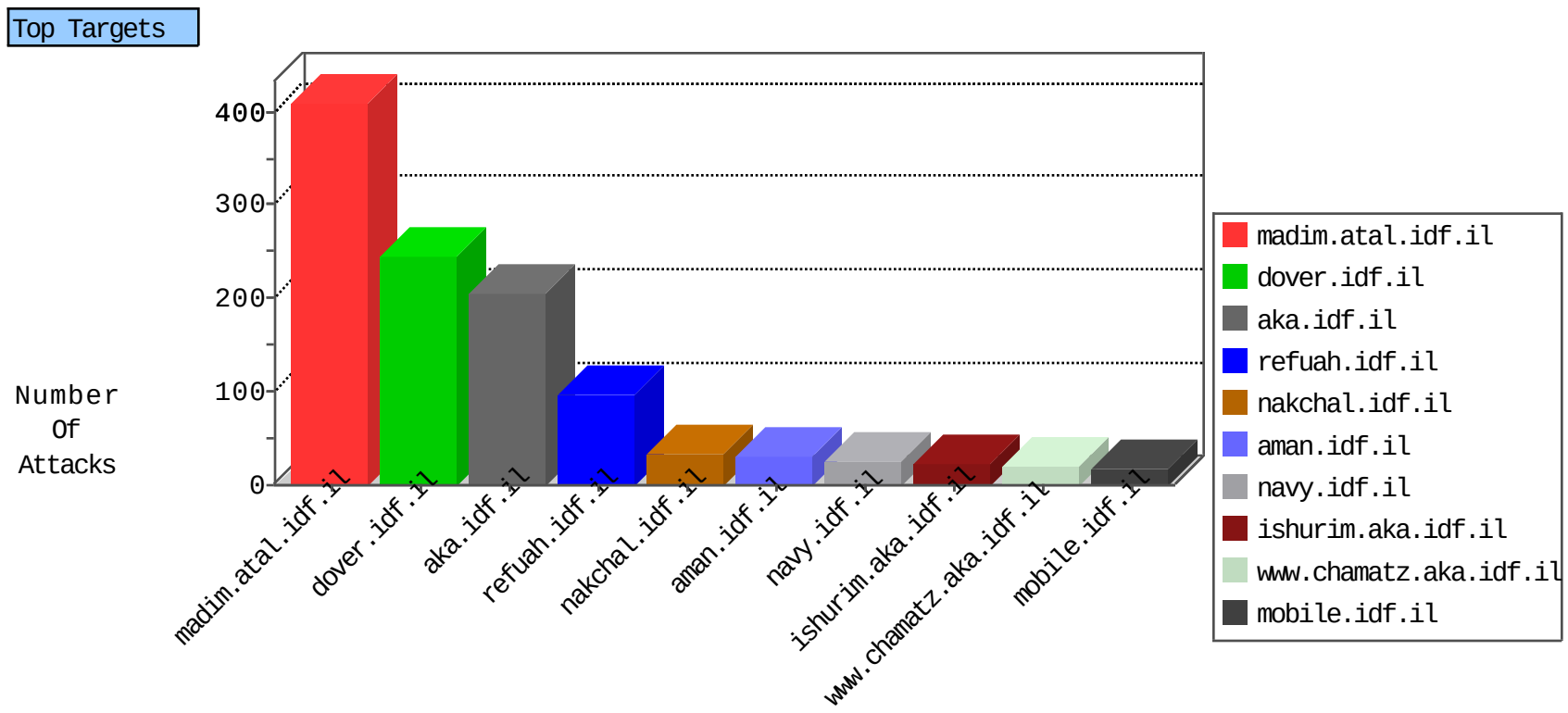
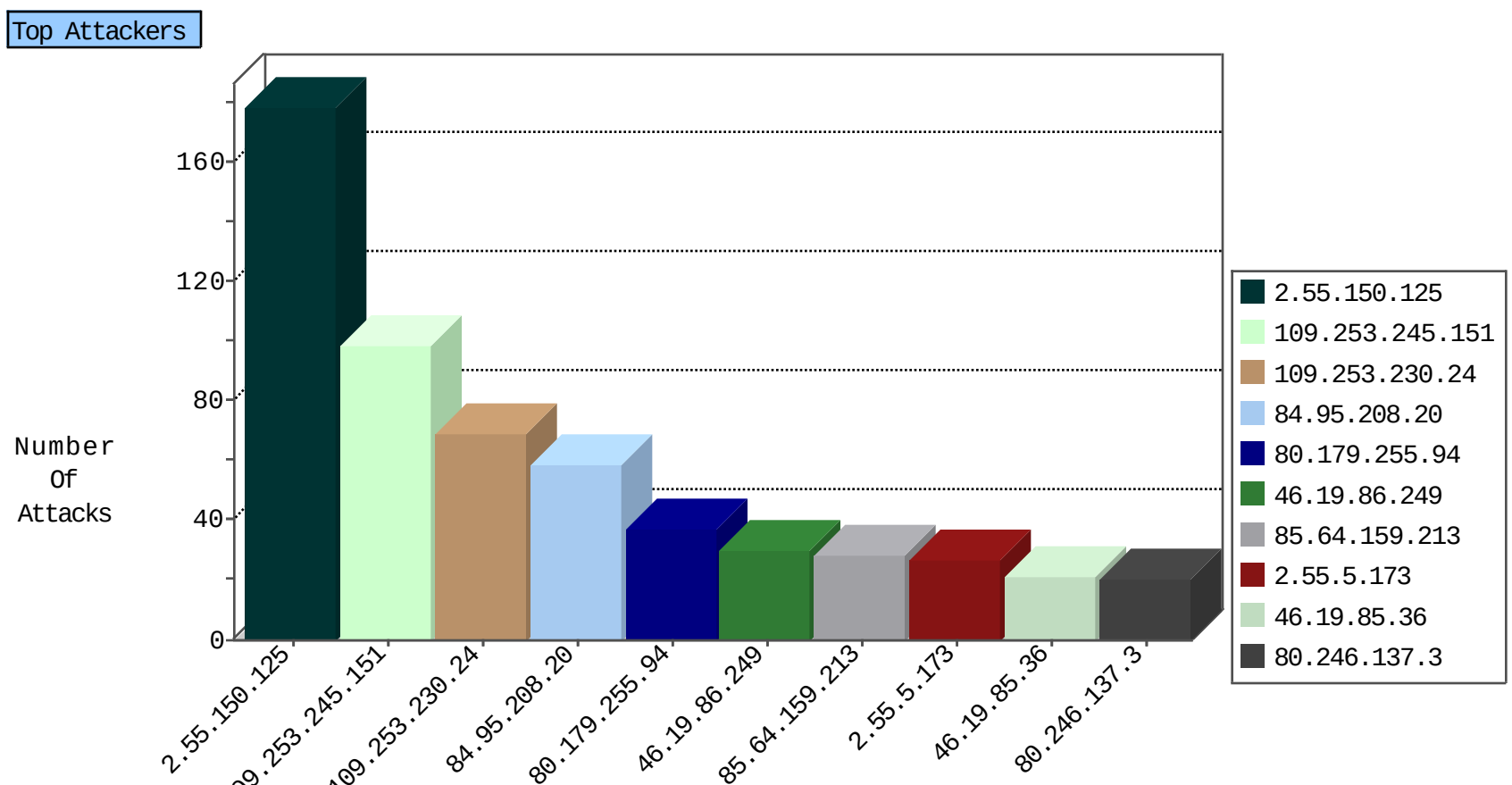
09-20-2016-10:04:02 to 09-20-2016-11:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-20-2016-10:04:02 to 09-20-2016-11:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.141.184	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
2.53.41.148	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.53.42.224	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
195.62.53.168	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	2
204.42.253.130	United States	147.237.76.177	ncore.idf.il	Black List	drop	2
173.208.197.205	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
82.166.140.117	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
173.208.150.115	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
128.208.4.198	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
63.141.242.195	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
208.110.84.68	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
173.208.197.206	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
87.69.248.198	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
198.204.224.237	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	1
173.208.197.202	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
69.30.193.250	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	1
182.58.54.210	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
173.208.197.205	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
69.30.226.218	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
165.242.90.128	Japan	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
63.141.231.196	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	1

09-20-2016-10:04:02 to 09-20-2016-11:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.206	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	10
199.58.86.206	United States	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
105.98.143.91	Algeria	147.237.77.176	matpash.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

09-20-2016-10:04:02 to 09-20-2016-11:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
105.98.143.91	147.237.77.176	Algeria	matpash.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	4
213.57.87.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
195.154.184.122	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
66.249.76.106	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
213.57.193.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
54.70.0.115	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.124.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.44.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.154.174	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.156.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.139.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.114.97.11	147.237.77.226	Portugal	www.chamatz.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
84.111.111.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
65.156.199.242	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.208.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
138.59.200.75	147.237.76.34	Brazil	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
109.60.153.178	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
89.138.98.148	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.61.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.96.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-20-2016-10:04:02 to 09-20-2016-11:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.179.255.94	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
85.64.159.213	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
62.0.212.169	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
62.0.225.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
80.246.137.3	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
176.13.224.14	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
2.55.5.173	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
46.19.85.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.55.5.173	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.36	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
81.218.206.12	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	8
31.210.188.88	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
62.0.205.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
62.0.230.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.13.162	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
100.92.140.205		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.36	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.144.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.39.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
95.35.180.94	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
84.95.37.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.148.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.47.217	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
84.95.37.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
199.203.8.2	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.39.229	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
176.13.246.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
5.29.38.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.14.147	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
80.246.137.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.189	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.14.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.189	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
62.0.230.1	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	4
188.120.154.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.36	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
176.13.14.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
37.26.146.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.198.247	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
81.218.66.107	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
2.53.148.36	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.5.173	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
62.0.222.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
2.53.4.204	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3

09-20-2016-10:04:02 to 09-20-2016-11:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.150.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	179
109.253.245.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	99
109.253.230.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	32
46.19.86.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
109.253.242.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
46.19.86.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
192.116.177.194	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
46.19.86.169	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	4
37.26.147.243	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
37.26.148.196	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	3
46.19.86.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.59.186	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
2.53.149.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
176.13.246.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
79.181.151.67	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/u1t4pvovmkk	Block	1
176.106.46.74	Palestinian Territory, Occupied	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/71954-en/maarachot.aspx	Block	1
185.132.156.3	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
80.179.255.94	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
195.62.53.168	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to gmail.com/engine/log.txt	Block	1
181.215.118.89	United States	147.237.76.147	chinuch.aka.idf.il	Distributed PHP Attempt	Block	1
109.253.218.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.159.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/70002.doc	Block	1
185.132.156.3	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
37.26.148.233	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.226	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/templates/homepage/	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/homepage/piwik.php	Block	1
81.97.235.193	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
212.143.104.25	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	1
181.215.118.89	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/blog/wp-login.php	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
185.159.37.6		147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/hnap1/	Block	1
40.77.167.3	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
176.13.0.200	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
85.64.159.213	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
212.143.104.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
185.16.107.42	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/	Block	1
66.102.9.3	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
5.22.134.204	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.229.223	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1

09-20-2016-10:04:02 to 09-20-2016-11:04:02