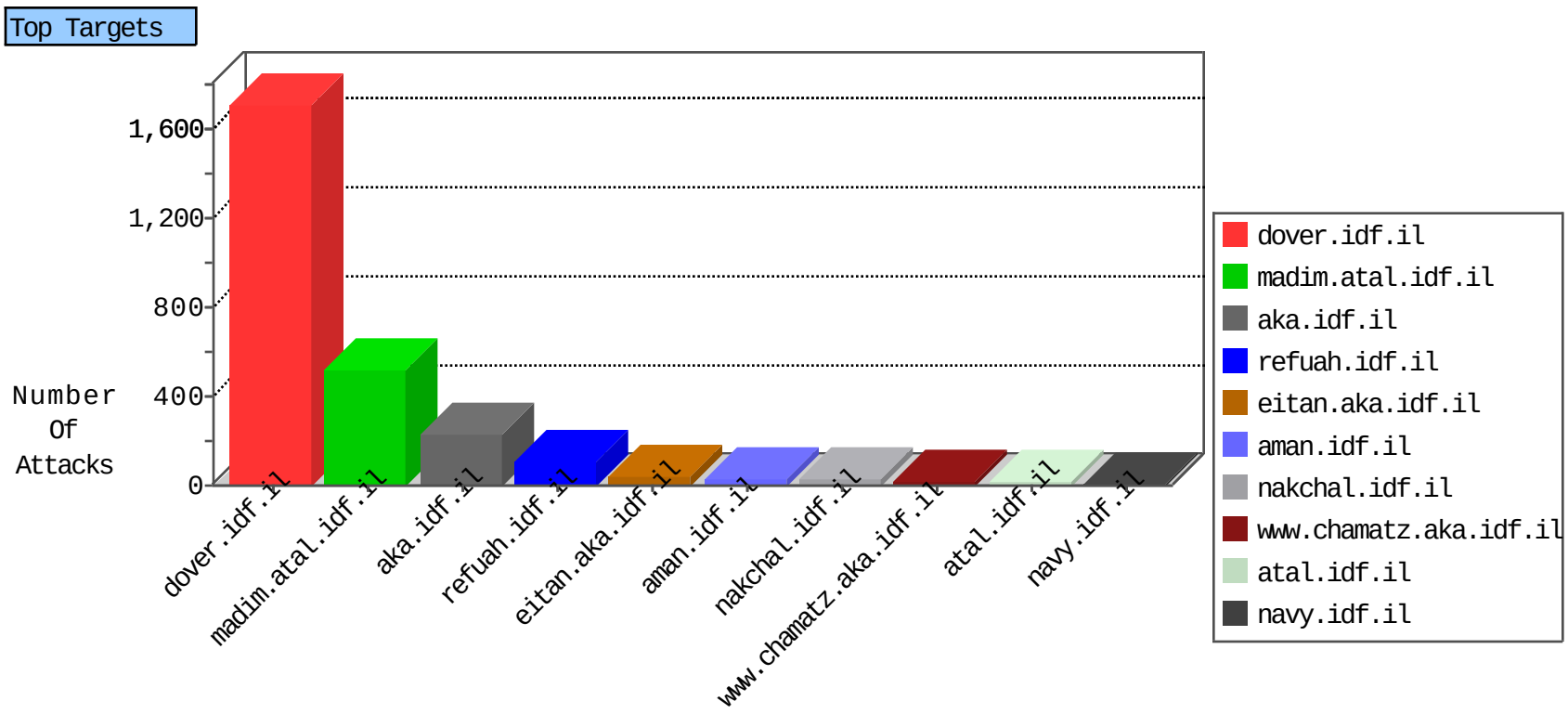
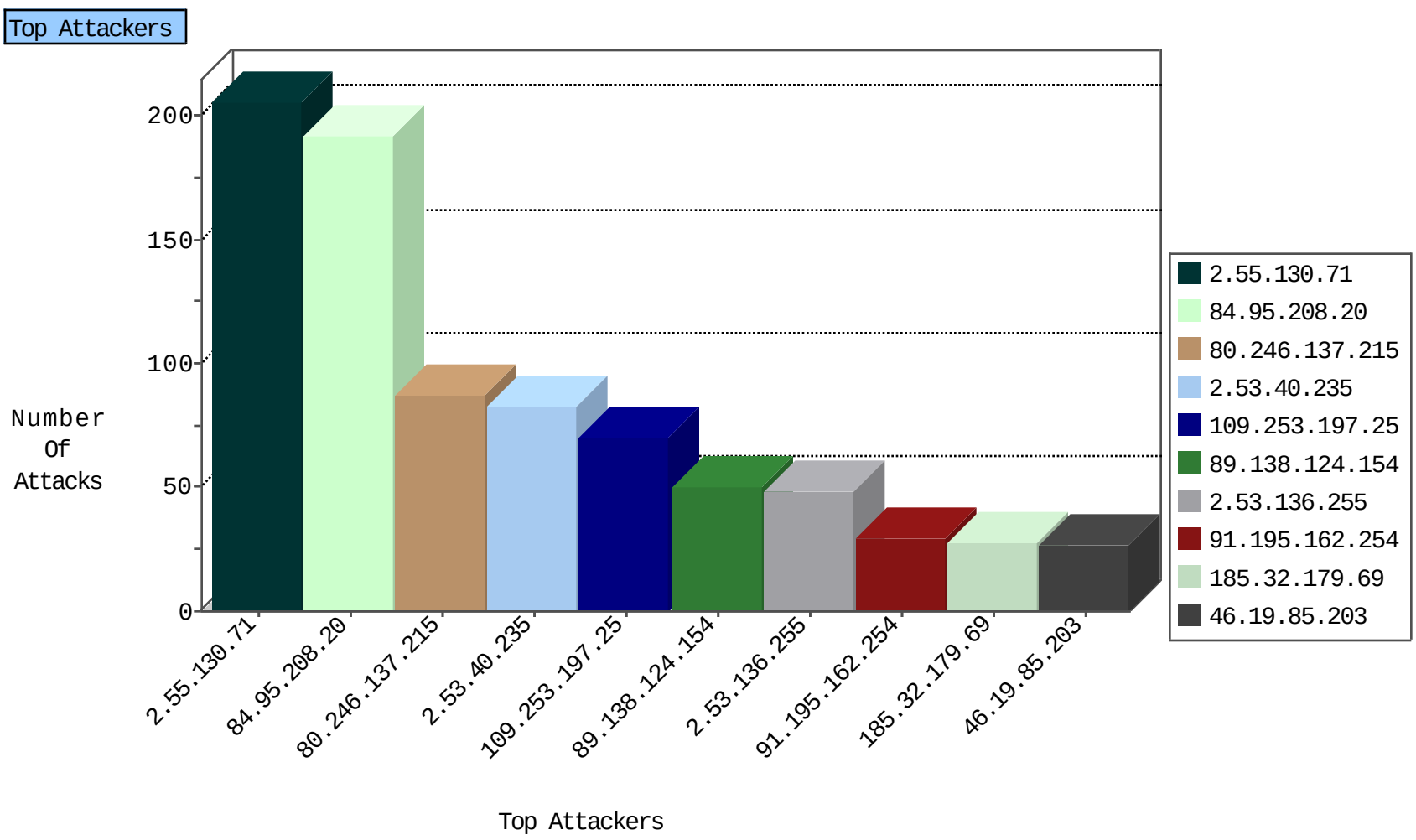
09-26-2016-11:04:06 to 09-26-2016-12:04:06

IDF Under Attack Daily Report





09-26-2016-11:04:06 to 09-26-2016-12:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
2.53.140.230	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
79.180.122.72	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
5.29.171.20	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
77.127.73.83	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
77.139.26.28	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
141.226.217.239	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
104.238.145.167	United States	147.237.76.176	test.ncore.idf.i	Black List	drop	1
109.253.220.112	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
185.32.179.105	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
134.134.139.76	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.235.116.236	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-26-2016-11:04:06 to 09-26-2016-12:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.48.155	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.255.48.155	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
195.154.255.20	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
195.154.255.20	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
2.53.172.253	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-26-2016-11:04:06 to 09-26-2016-12:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
211.149.244.79	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
31.24.228.20	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
185.32.179.213	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
141.226.217.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.240.250.154	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
82.81.209.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.223.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
54.175.4.38	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.250.82	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	1
213.151.35.213	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.24.228.20	147.237.77.205	United Kingdom	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
185.129.148.230	147.237.77.235	Latvia	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.146.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.23.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
121.46.106.39	147.237.72.14	India	dover.idf.il(old)	ET DROP Spamhaus DROP Listed Traffic Inbound	1
85.250.231.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.124.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.218.200.137	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.81.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-26-2016-11:04:06 to 09-26-2016-12:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
91.195.162.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
46.19.86.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
109.253.143.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
141.226.217.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
84.109.194.208	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.19.85.110	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	13
109.253.132.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.251	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.106	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.80.219.164	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.220.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
89.138.124.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
89.138.124.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
89.138.124.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
176.13.22.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.236.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.253.137.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.15.72	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.177.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
185.32.179.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
89.138.124.154	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
89.138.124.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.170.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.28.178.189	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.13.230.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
62.0.212.201	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
2.53.133.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
62.0.251.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
109.226.28.148	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
87.69.89.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.3.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
62.90.202.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.55.178.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.55.137.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.127.31.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.66.116.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.178.106	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.212.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

09-26-2016-11:04:06 to 09-26-2016-12:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.130.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	205
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	90
80.246.137.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
2.53.40.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
109.253.197.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	52
2.53.136.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	11
62.219.238.54	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	8
109.253.198.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	5
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
81.218.34.242	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
37.26.148.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.115	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
79.178.48.109	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	3
46.19.86.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.34.242	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
46.121.115.171	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.121.115.171	Block	2
109.253.197.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	2
2.55.175.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.53.131.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.201.124	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.76.87	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8763-he/refuah.aspx	Block	1
189.218.218.94	Mexico	147.237.0.19	madim.atal.idf.il	Redundant HTTP Headers Content-Type	Block	1
84.108.87.238	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/wp-login.php	Block	1
217.132.63.220	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
187.160.97.180	Mexico	147.237.0.15	kosher-kravi.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Illegal Byte Code Character in Method N•fº±b™E:Ít•!·[[#20]]Æ•¯hÜá$¦…p6Kï"—î?[[#25]]D[[#29]]áää••'½'È Ãˆ-•'³[[#16]]	Block	1
201.173.160.130	Mexico	147.237.77.74	law.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
194.90.99.193	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/images/1.he/titlecap.png	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in URL	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover	Block	1
187.252.229.206	Mexico	147.237.76.42	refuah.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
2.24.14.15	United Kingdom	147.237.76.42	refuah.idf.il	Distributed NULL Character in Method	Block	1
109.67.202.232	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
46.19.86.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
180.76.15.157	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/list5.htm	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/send_but.png	Block	1
201.172.63.173	Mexico	147.237.77.235	sviva.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
2.55.135.95	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Multiple Illegal Byte Code Character in URL from 169.229.3.91	Block	1
2.53.43.241	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1

09-26-2016-11:04:06 to 09-26-2016-12:04:06