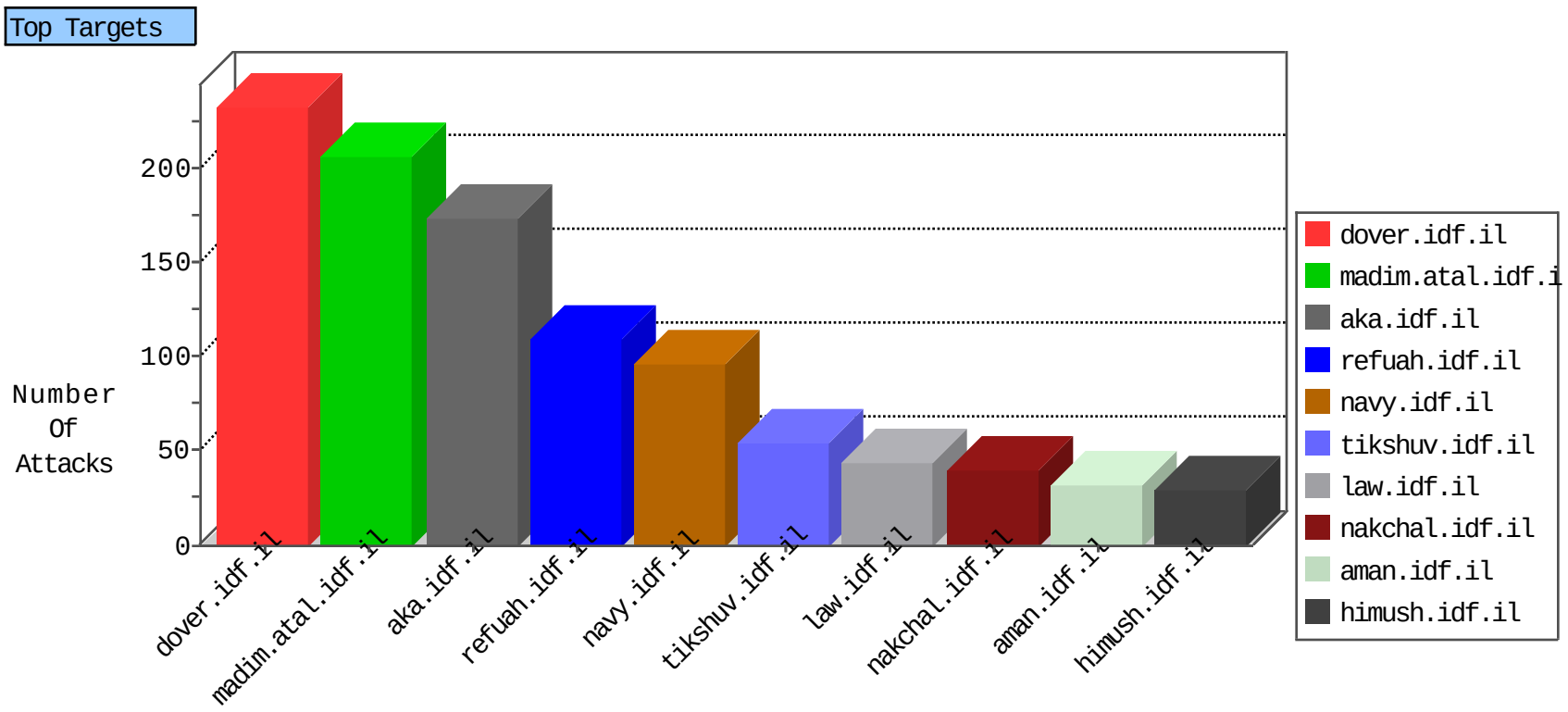
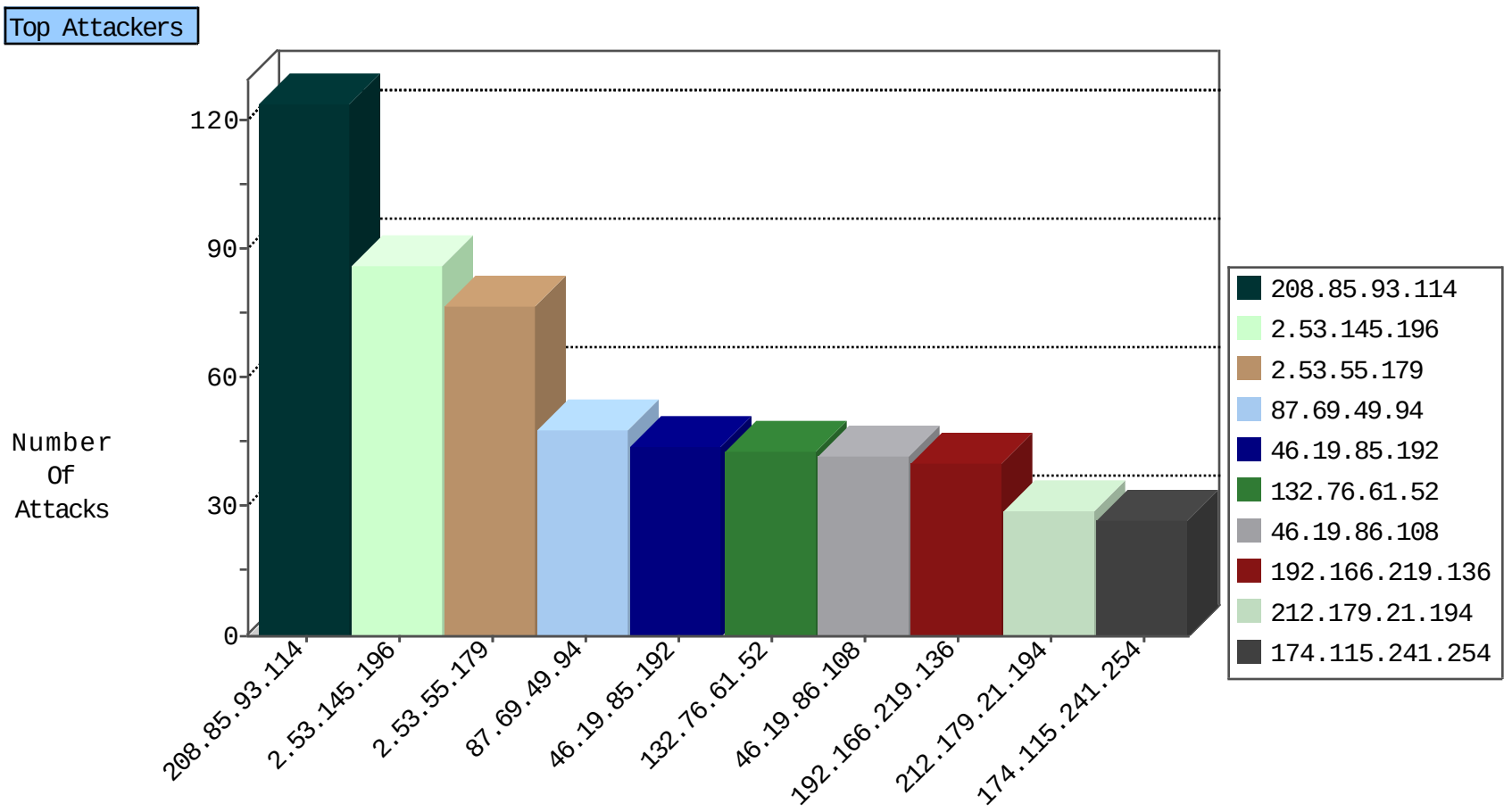
09-08-2016-08:04:02 to 09-08-2016-09:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-08-2016-08:04:02 to 09-08-2016-09:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
132.76.61.52	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
209.126.136.2	United States	147.237.76.30	himush.idf.il	Black List	drop	1

09-08-2016-08:04:02 to 09-08-2016-09:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.166.219.136	Poland	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	26
192.166.219.136	Poland	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	7
192.166.219.136	Poland	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	7

09-08-2016-08:04:02 to 09-08-2016-09:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.210.38.242	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
62.210.113.216	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
163.172.129.15	147.237.8.45	United Kingdom	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
109.123.101.31	147.237.77.74	United Kingdom	law.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.137.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.26.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.9.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
207.232.28.59	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.252.173.4	147.237.77.216	Germany	dover.idf.il	GPL SCAN nmap TCP	1
91.201.236.50	147.237.8.24	Ukraine	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.136.119	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1

09-08-2016-08:04:02 to 09-08-2016-09:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.108	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
132.76.61.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
46.19.85.192	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
87.69.49.94	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	24
87.69.49.94	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
176.13.244.5	Israel	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
174.115.241.254	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
79.179.99.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
208.85.93.114	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
208.85.93.114	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
208.85.93.114	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
208.85.93.114	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
208.85.93.114	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
208.85.93.114	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
208.85.93.114	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
208.85.93.114	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
109.253.241.127	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
62.90.21.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
185.101.16.202	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.192	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
109.253.230.159	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
81.218.101.66	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
2.53.178.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.192	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.136	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.35	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.91	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.135	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
132.76.61.52	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
37.26.148.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.135	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.91	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.99.222	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.204	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.204	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.193	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
37.247.36.88	Netherlands	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
46.19.85.35	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.44	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.94.2.246	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.157.101	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
176.65.17.119	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.69.36.120	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
68.180.230.47	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

09-08-2016-08:04:02 to 09-08-2016-09:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.145.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
2.53.55.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
80.246.137.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
212.179.21.194	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	16
176.13.235.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.148.175	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.26.148.175	Block	5
79.180.185.70	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	5
37.26.146.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
79.180.185.70	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.180.185.70	Block	4
37.26.148.175	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1750	Block	3
159.122.159.28	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 159.122.159.28	Block	2
77.139.46.233	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	2
176.13.242.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.139.122.192	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
77.139.138.32	France	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/login.aspx	Block	2
37.26.149.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.180.114.10	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	2
85.65.19.161	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
189.218.187.120	Mexico	147.237.76.30	himush.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
187.160.46.176	Mexico	147.237.77.216	dover.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
75.156.49.249	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/matash/login/	Block	1
180.97.106.37	China	147.237.77.170	maarachot.idf.il	Distributed NULL Character in Method	Block	1
212.179.21.194	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	1
189.219.230.101	Mexico	147.237.76.86	navy.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
189.218.99.8	Mexico	147.237.0.15	kosher-kravi.idf.il	Redundant HTTP Headers from 189.218.99.8	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/71542.pdf	Block	1
180.97.106.161	China	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Method	Block	1
180.97.106.37	China	147.237.0.19	madim.atal.idf.il	Distributed NULL Character in Method	Block	1
201.173.98.177	Mexico	147.237.72.166	aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
85.65.19.161	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatusDay in www.aka.idf.il/main/sachar/payslips.aspx	None	1
189.218.187.120	Mexico	147.237.76.31	nakchal.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
187.252.73.152	Mexico	147.237.76.42	refuah.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
77.139.46.233	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.46.233	Block	1
180.97.106.37	China	147.237.77.235	sviva.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
195.160.242.40	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
189.218.99.8	Mexico	147.237.0.17	m.my-kosher-kravi.idf.il	Redundant HTTP Headers Content-Type	Block	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
180.97.106.161	China	147.237.77.233	atal.idf.il	NULL Character in Method	Block	1
180.97.106.37	China	147.237.76.30	himush.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
201.175.76.182	Mexico	147.237.76.39	mobile.meitav.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
85.65.233.40	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
189.218.253.174	Mexico	147.237.72.167	ishurim.aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
189.218.20.47	Mexico	147.237.77.233	atal.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
180.97.106.37	China	147.237.77.235	sviva.idf.il	Distributed NULL Character in Method	Block	1
201.166.203.159	Mexico	147.237.72.156	aman.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
79.180.185.70	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	1
189.218.99.8	Mexico	147.237.0.19	madim.atal.idf.il	Redundant HTTP Headers Content-Type	Block	1
66.249.66.179	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
180.97.106.162	China	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
180.97.106.37	China	147.237.76.30	himush.idf.il	Distributed NULL Character in Method	Block	1

09-08-2016-08:04:02 to 09-08-2016-09:04:02