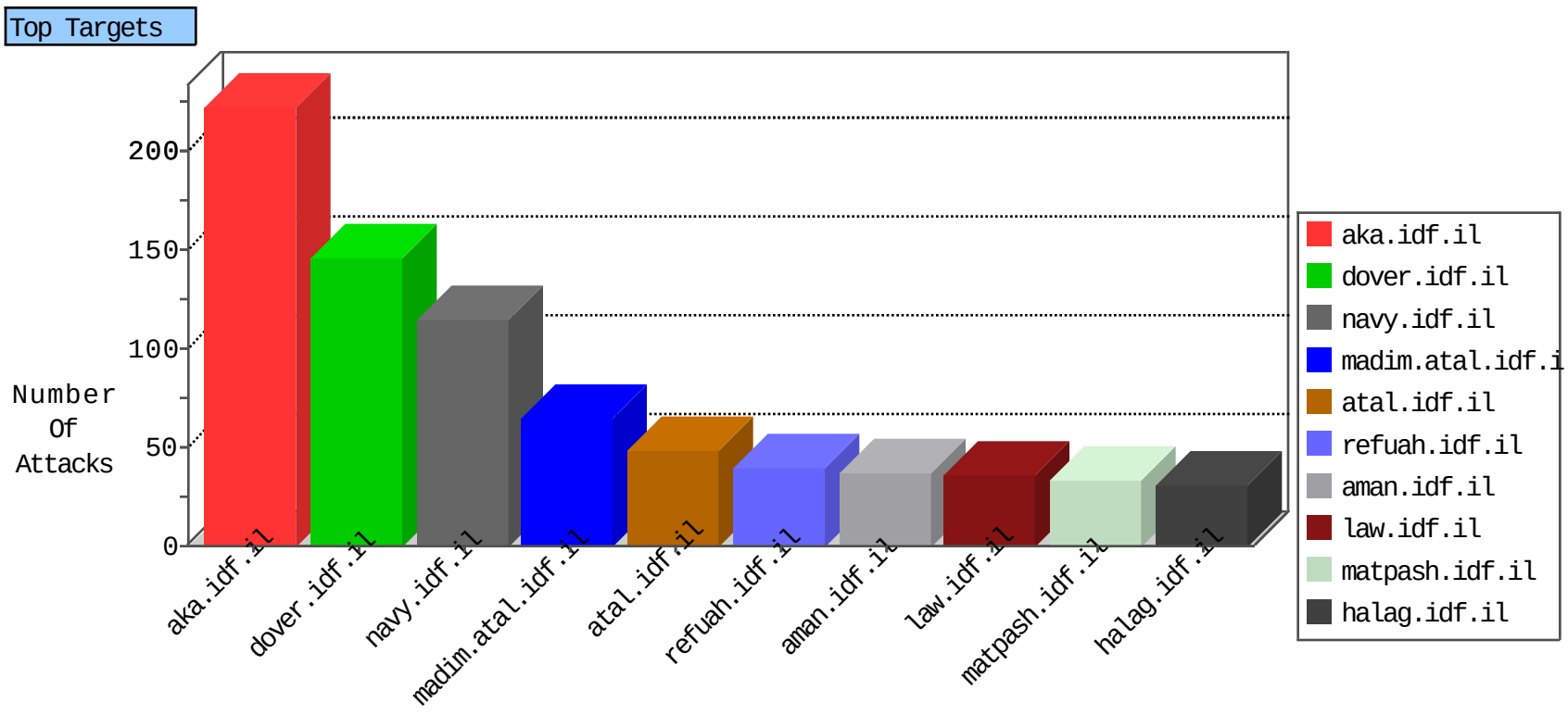
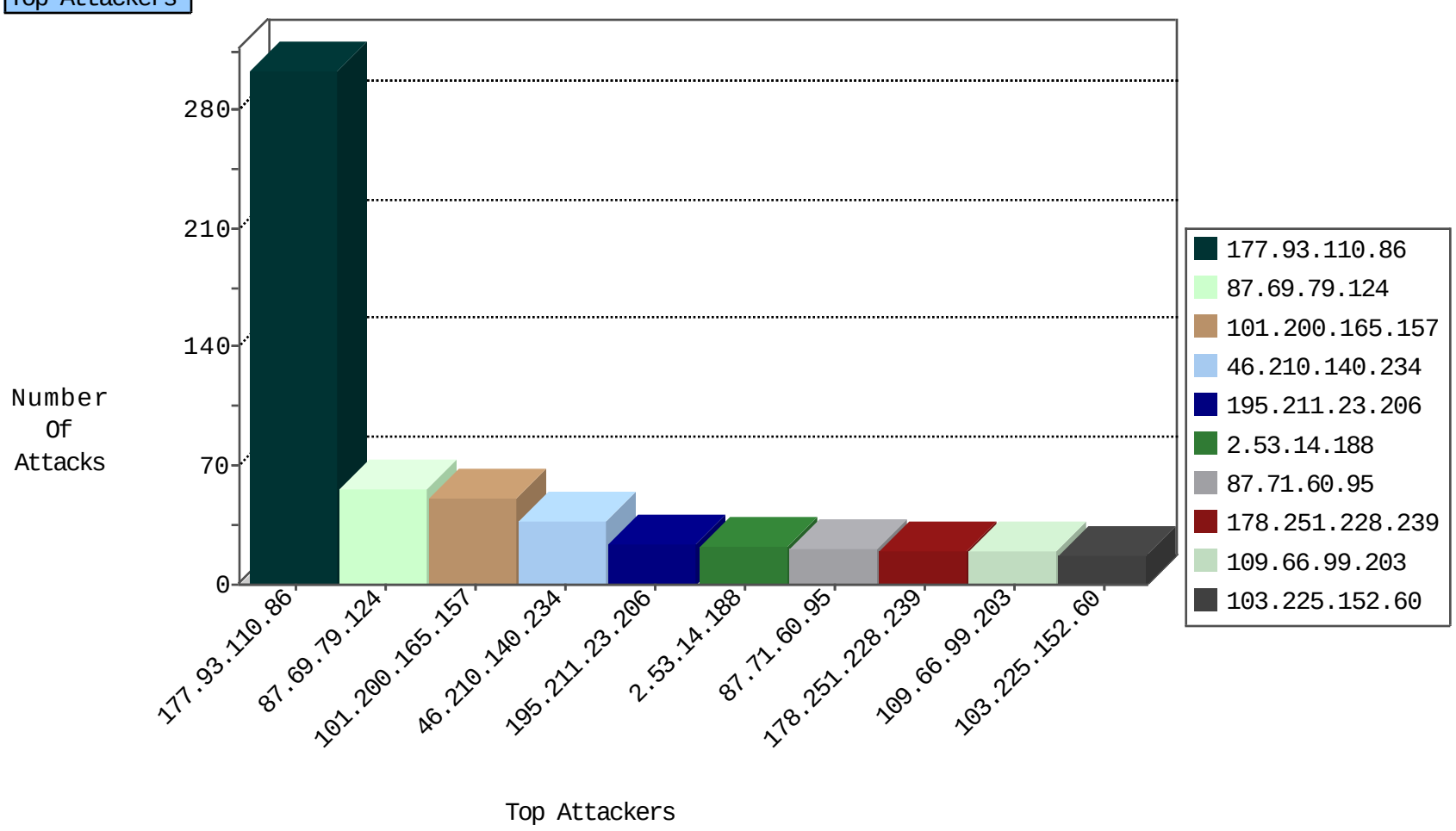
09-09-2016-20:04:02 to 09-09-2016-21:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-09-2016-20:04:02 to 09-09-2016-21:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.145.189	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
185.81.158.121	France	147.237.76.176	test.ncore.idf.i	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.202	e.halag.idf.il	Black List	drop	1
98.139.135.129	United States	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1
98.139.135.129	United States	147.237.77.121	e.navy.idf.il	Invalid TCP Flags	drop	1

09-09-2016-20:04:02 to 09-09-2016-21:04:02

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	17
195.154.187.115	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
195.154.187.115	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
188.163.109.21	Ukraine	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Permit	1

09-09-2016-20:04:02 to 09-09-2016-21:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
45.79.71.122	147.237.72.166	United States	aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
195.88.208.193	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN NMAP -sS window 1024	1
116.12.175.233	147.237.77.226	Singapore	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.195	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.41.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.187	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
216.81.230.167	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
161.10.9.69	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
116.12.175.233	147.237.77.226	Singapore	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
93.174.91.29	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.111.175	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

09-09-2016-20:04:02 to 09-09-2016-21:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
87.69.79.124	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
87.69.79.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
195.211.23.206	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	24
2.53.14.188	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
87.71.60.95	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
177.93.110.86	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
101.200.165.157	China	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	17
177.93.110.86	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
101.200.165.157	China	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	16
177.93.110.86	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
177.93.110.86	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
177.93.110.86	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
101.200.165.157	China	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
177.93.110.86	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
177.93.110.86	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
177.93.110.86	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
109.253.216.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
177.93.110.86	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
177.93.110.86	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
188.120.154.65	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
77.139.247.124	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
177.93.110.86	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
177.93.110.86	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
177.93.110.86	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
177.93.110.86	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
177.93.110.86	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
46.19.86.106	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
177.93.110.86	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
177.93.110.86	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
177.93.110.86	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
177.93.110.86	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
177.93.110.86	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
177.93.110.86	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
177.93.110.86	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
46.19.85.128	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.66.99.203	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
2.53.53.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
87.69.79.124	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
86.177.75.33	United Kingdom	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.99.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
204.88.159.118	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.216	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
110.171.37.147	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.142.86.109	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.216	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
86.104.178.206	Romania	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
185.3.147.204	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.99.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
82.101.247.28	Netherlands	147.237.77.216	dover.idf.il	drop		drop	5

09-09-2016-20:04:02 to 09-09-2016-21:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.210.140.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
79.177.133.198	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	3
84.111.102.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.221.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
207.46.13.57	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
109.253.216.176	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 109.253.216.176	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/piwik.php	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/3/71573.pdf	Block	1
2.53.1.162	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
188.120.154.65	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
86.104.178.206	Romania	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
79.178.15.172	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.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
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/3156.jpg	Block	1
2.55.14.12	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
188.163.109.21	Ukraine	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
87.71.60.95	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
82.166.240.200	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
157.55.39.224	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/www.tikshuv.idf.il	Block	1
66.249.76.83	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/3126.jpg	Block	1
5.228.18.157	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
188.163.109.21	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
89.237.65.166	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
176.13.251.60	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
84.108.27.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.66.5	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
188.163.109.21	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin.php	Block	1
109.65.117.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
66.249.66.29	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
176.67.58.193	Palestinian Territory, Occupied	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/favicon.ico	Block	1

09-09-2016-20:04:02 to 09-09-2016-21:04:02