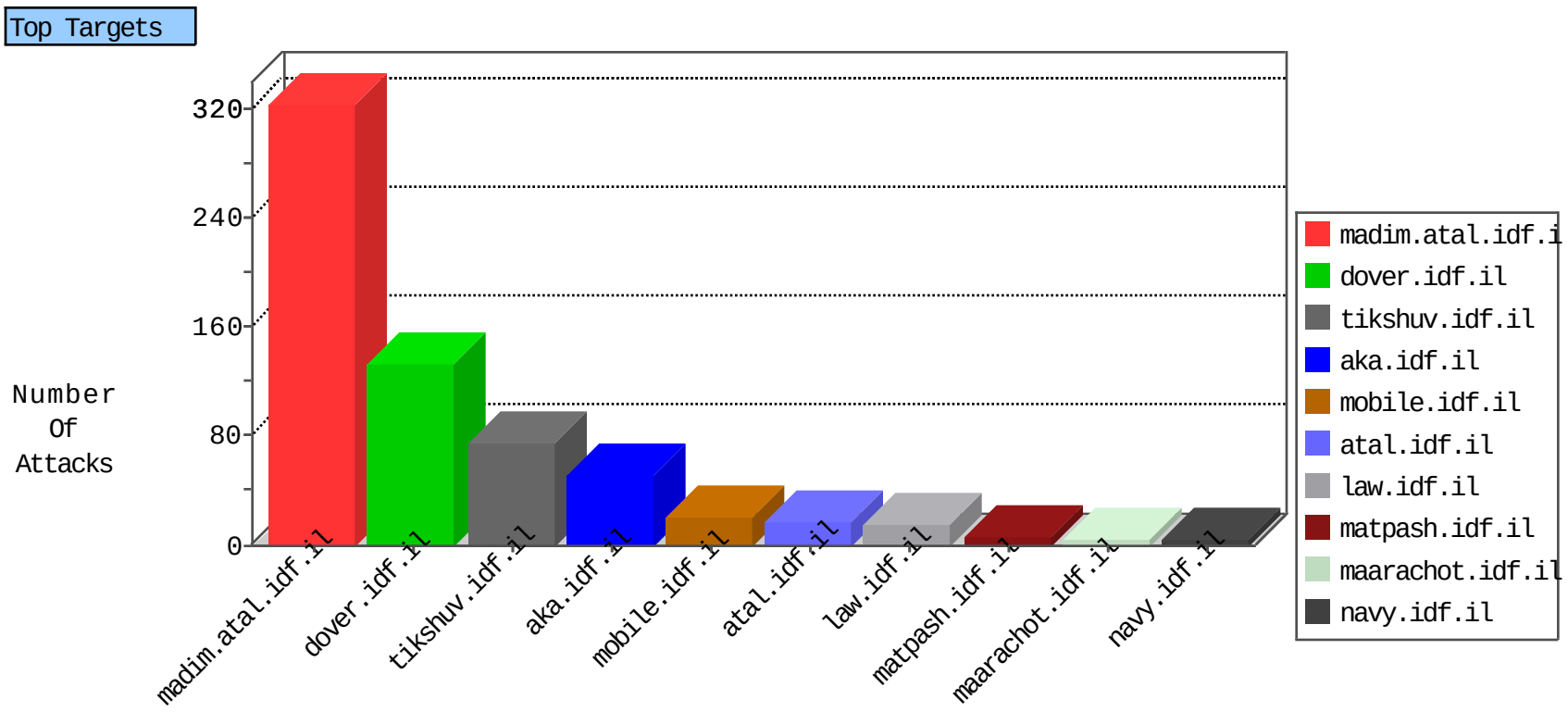
01-28-2016-06:04:00 to 01-28-2016-07:04:00

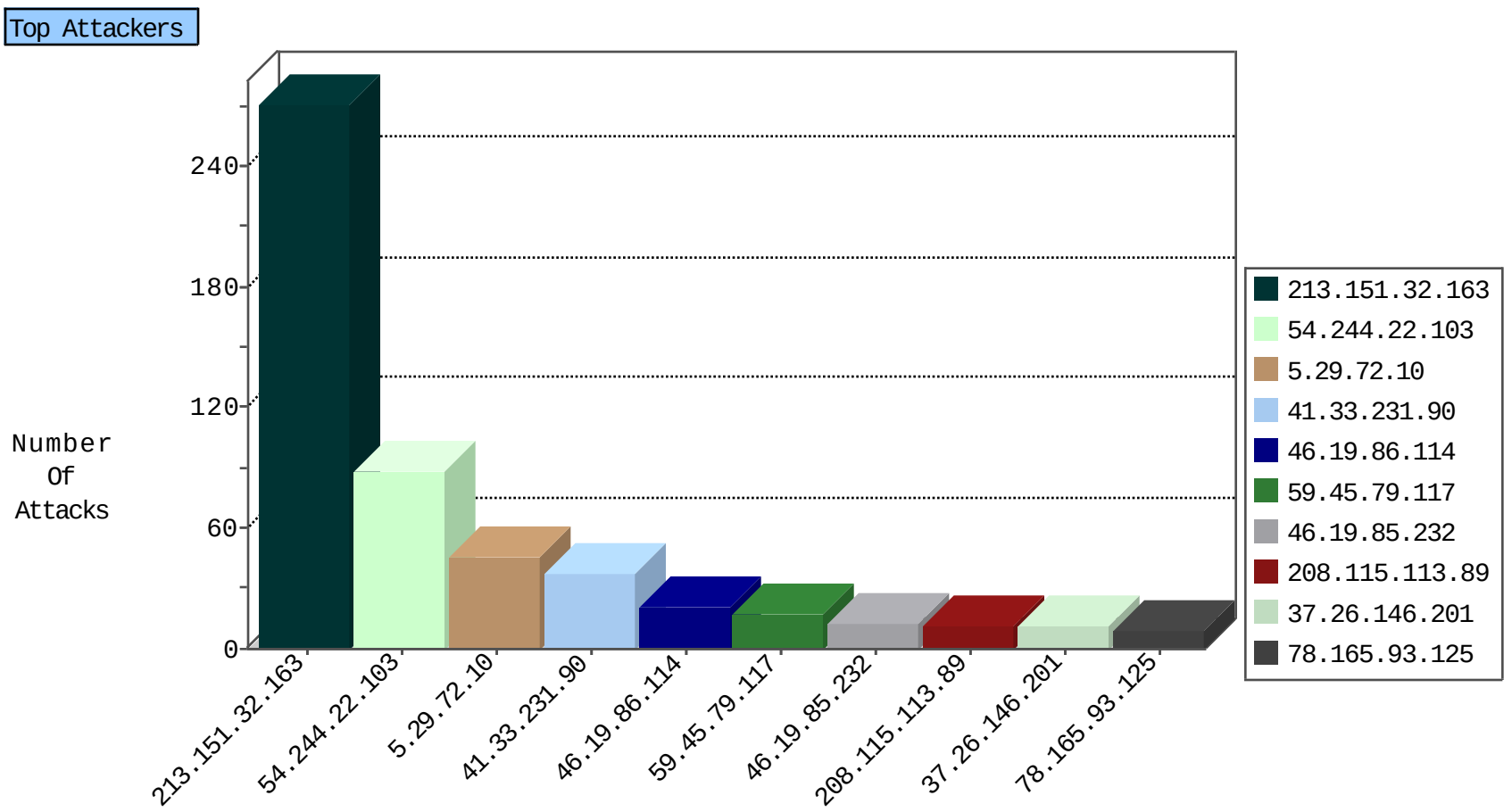
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-28-2016-06:04:00 to 01-28-2016-07:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.117.37.140	Russian Federation	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
176.117.37.140	Russian Federation	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
167.114.92.57	Canada	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
176.117.37.140	Russian Federation	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

01-28-2016-06:04:00 to 01-28-2016-07:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
78.165.93.125	Turkey	147.237.77.74	law.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

01-28-2016-06:04:00 to 01-28-2016-07:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
61.149.161.186	147.237.76.147	China	chinuch.aka.idf.il	GPL SCAN nmap TCP	2
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
66.240.213.93	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.237	147.237.77.74		law.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.237	147.237.77.74		law.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
115.214.66.59	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
66.240.213.93	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.237	147.237.77.74		law.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
115.214.66.59	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
115.214.66.59	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
96.35.144.107	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1

01-28-2016-06:04:00 to 01-28-2016-07:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	74
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.86.114	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	14
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
177.228.216.34	Mexico	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
37.26.146.201	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
66.249.64.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
171.99.171.73	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.3.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.206	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.147.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.201.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.30.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.35.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	2
66.249.78.199	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
180.234.217.154	Bangladesh	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
83.169.10.185	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.29.158.85	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.52.160.56	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
54.219.106.162	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.247.200	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.107	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.248	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.139.102	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
108.31.54.136	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
31.168.126.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
77.126.16.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
184.105.247.212	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.9.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
81.169.237.146	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
216.218.206.107	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.29.110.184	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.221	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.115	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
146.185.239.102	Russian Federation	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

01-28-2016-06:04:00 to 01-28-2016-07:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 213.151.32.163	Block	149
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	122
5.29.72.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
192.116.159.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
78.165.93.125	Turkey	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 78.165.93.125	Block	3
78.165.93.125	Turkey	147.237.77.74	law.idf.il	PHP Attempt	Block	2
77.126.16.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.17.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
94.159.146.224	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
68.180.230.240	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/109335.pdf×¦×‘×?-×″×″×¦×œ×″	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
64.79.85.205	United States	147.237.77.170	maarachot.idf.il	URL is Above Root Directory maarachot.idf.il/../	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
94.159.146.224	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
2.54.153.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.95.145	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
78.165.93.125	Turkey	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
65.132.59.34	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
105.155.188.9	Morocco	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
78.165.93.125	Turkey	147.237.77.74	law.idf.il	Admin Blocking	Block	1
79.179.110.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.181	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
105.155.188.9	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
78.165.93.125	Turkey	147.237.77.74	law.idf.il	Multiple Admin Blocking from 78.165.93.125	Block	1
184.105.247.195	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
80.246.136.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.211.137.195	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1

01-28-2016-06:04:00 to 01-28-2016-07:04:00