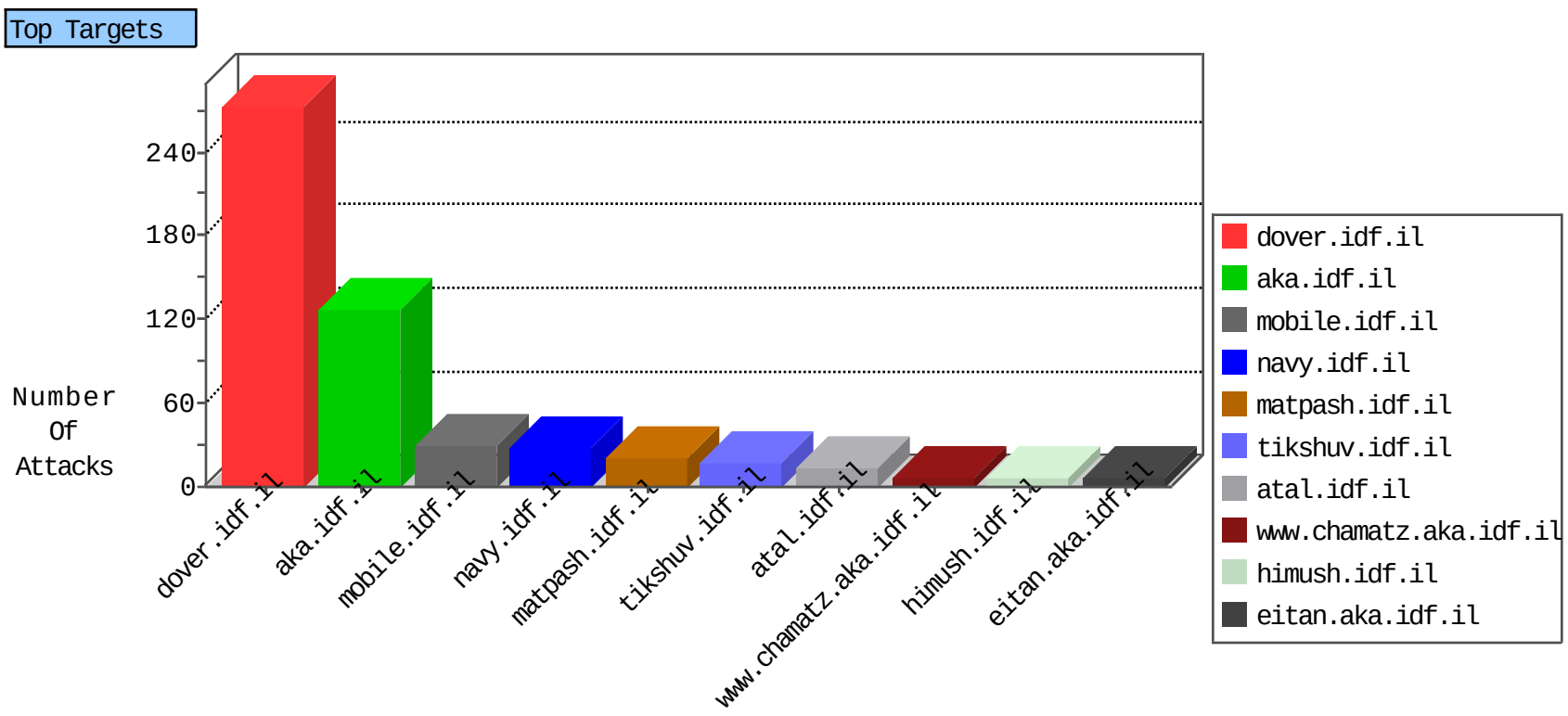
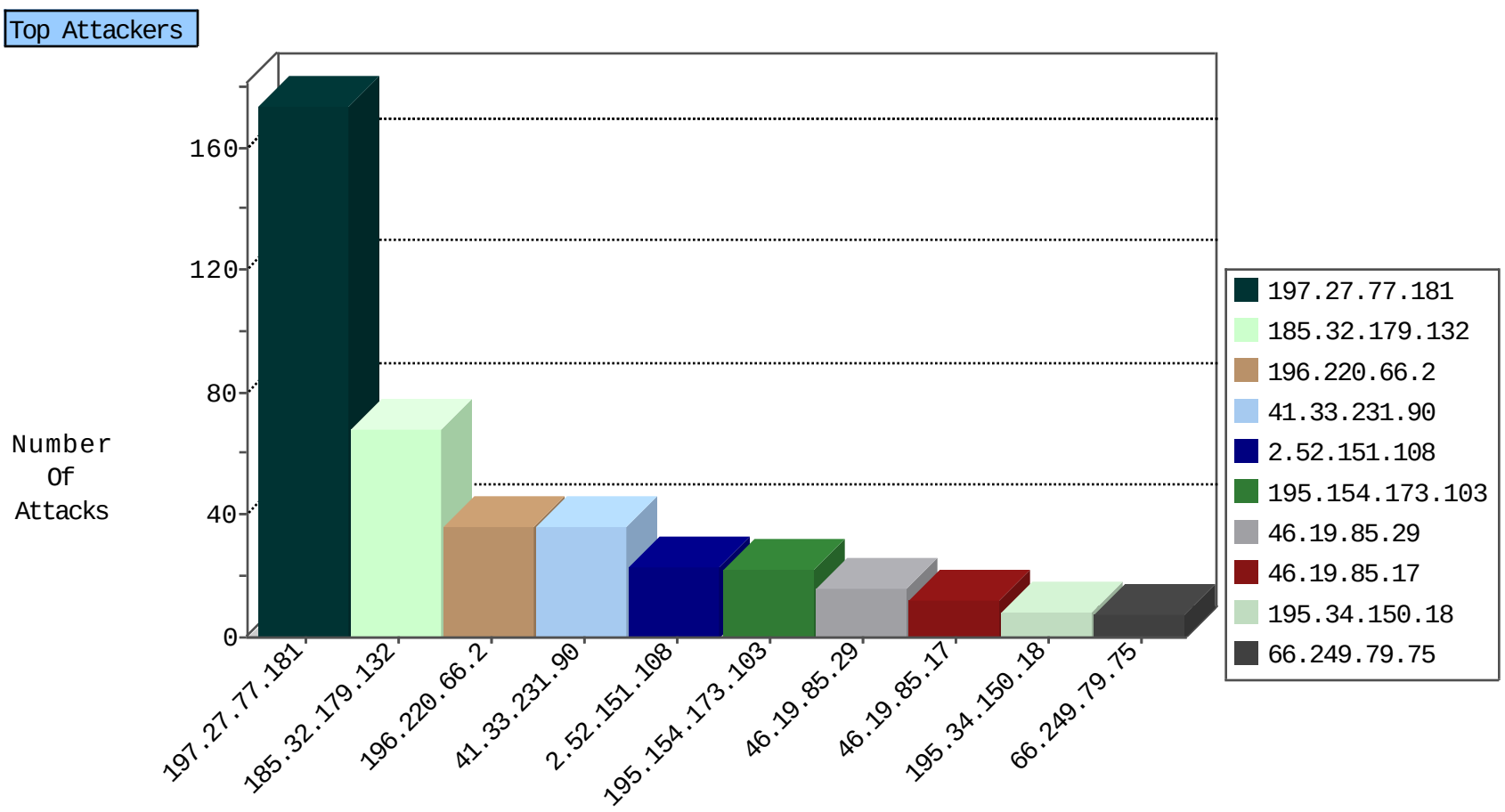
02-28-2016-05:04:01 to 02-28-2016-06:04:01

IDF Under Attack Daily Report





02-28-2016-05:04:01 to 02-28-2016-06:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	2
184.105.139.104	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.76	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
124.127.145.214	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.92	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.33	Switzerland	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
71.6.135.131	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.112	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.80	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.100	United States	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.58	United States	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.124	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
184.105.139.80	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.100	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
124.127.145.214	China	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.84	United States	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
146.185.239.100	Russian Federation	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

02-28-2016-05:04:01 to 02-28-2016-06:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.130	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.64.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

02-28-2016-05:04:01 to 02-28-2016-06:04:01

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
59.45.79.117	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
223.95.76.194	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
218.108.22.46	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
198.180.198.185	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
195.216.176.244	147.237.0.200	Latvia	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
121.18.74.98	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
88.247.57.34	147.237.8.28	Turkey	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
223.95.76.194	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
218.108.22.46	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
195.216.176.244	147.237.8.28	Latvia	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
93.113.125.11	147.237.77.61	Romania	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1

02-28-2016-05:04:01 to 02-28-2016-06:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
2.52.151.108	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
185.32.179.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
185.32.179.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
195.154.173.103	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
185.32.179.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	19
196.220.66.2	Nigeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
196.220.66.2	Nigeria	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	10
197.27.77.181	Tunisia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
197.27.77.181	Tunisia	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.46.39.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
37.46.39.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
196.220.66.2	Nigeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
196.220.66.2	Nigeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
196.220.66.2	Nigeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
207.46.13.133	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.29	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.253.133.28	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.45.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.172.2.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
185.32.179.132	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
66.249.69.38	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.9.122.203	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
176.13.19.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
195.154.173.103	France	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
46.19.85.29	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
94.230.86.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.29	Israel	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.11	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
139.162.40.248	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.64.23.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.32.179.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
66.240.192.138	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.79	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
78.46.97.213	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.247	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.233	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.46.41.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
123.125.71.85	China	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1

02-28-2016-05:04:01 to 02-28-2016-06:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.27.77.181	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.27.77.181	Block	93
197.27.77.181	Tunisia	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 197.27.77.181	Block	23
197.27.77.181	Tunisia	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 197.27.77.181	Block	14
197.27.77.181	Tunisia	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 197.27.77.181	Block	8
66.249.79.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	7
197.27.77.181	Tunisia	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 197.27.77.181	Block	7
46.116.13.16	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	6
46.19.86.180	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	5
197.27.77.181	Tunisia	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 197.27.77.181	Block	4
37.26.149.231	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
85.250.124.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
197.27.77.181	Tunisia	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 197.27.77.181	Block	3
149.88.163.57	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 149.88.163.57	Block	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
46.19.86.72	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	2
84.228.97.112	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
197.27.77.181	Tunisia	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 197.27.77.181	Block	1
46.117.58.73	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
197.27.77.181	Tunisia	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 197.27.77.181	Block	1
149.88.163.57	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1540	Block	1
77.75.79.36	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
203.133.171.71	Korea, Republic of	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
40.77.167.72	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
197.27.77.181	Tunisia	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/default'.aspx	Block	1
87.70.48.237	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.249.64.239	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1244-he/atal.aspx	Block	1
197.27.77.181	Tunisia	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 197.27.77.181	Block	1
175.96.193.9	Taiwan	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.94.33.30	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/trajector/	Block	1
87.70.48.237	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
196.220.66.2	Nigeria	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.94.63.157	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
91.215.137.151	Russian Federation	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/1093-7939-en/eitan.aspx	None	1
66.249.79.119	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19178-he/dover.aspx	Block	1
2.52.151.108	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1

02-28-2016-05:04:01 to 02-28-2016-06:04:01