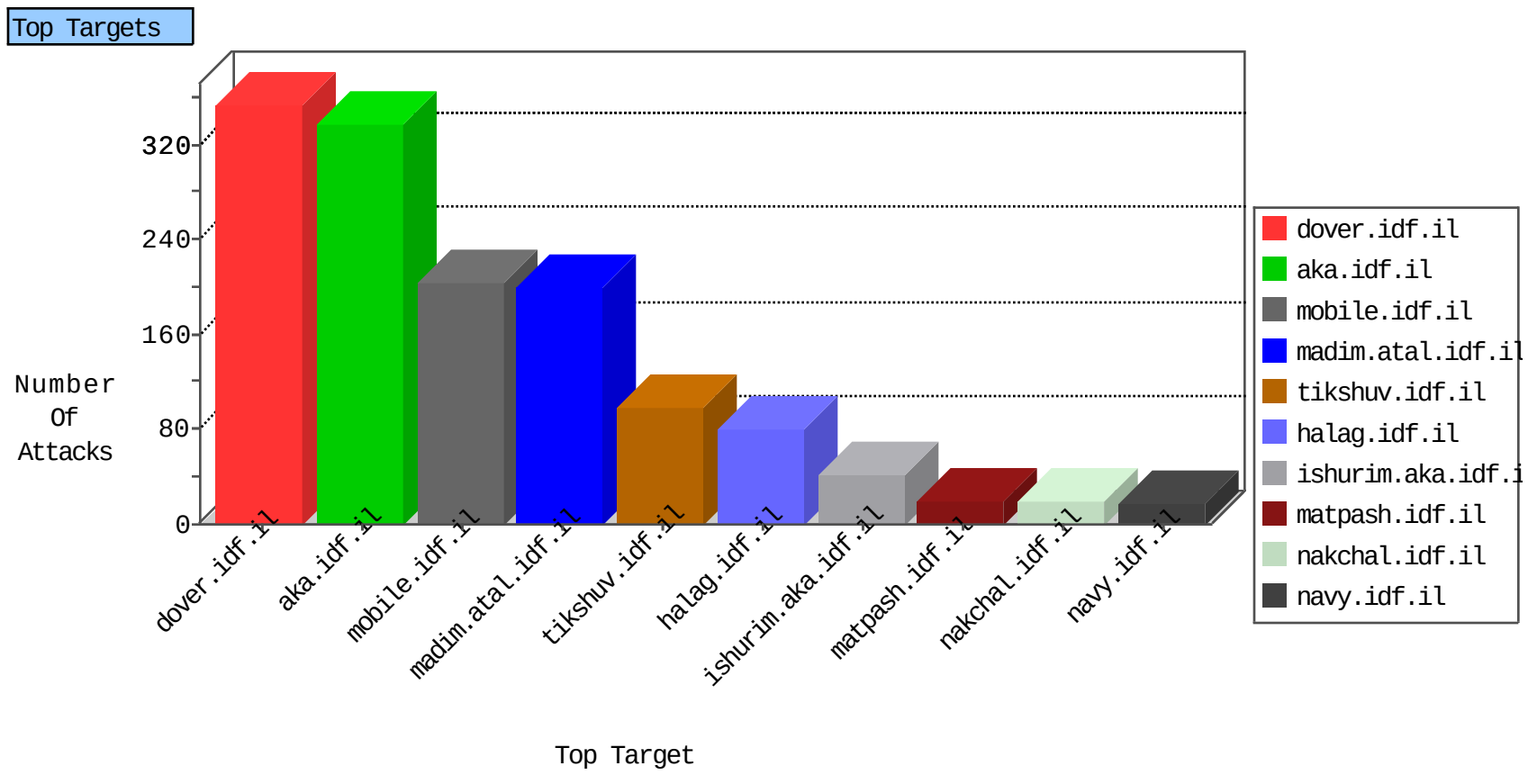
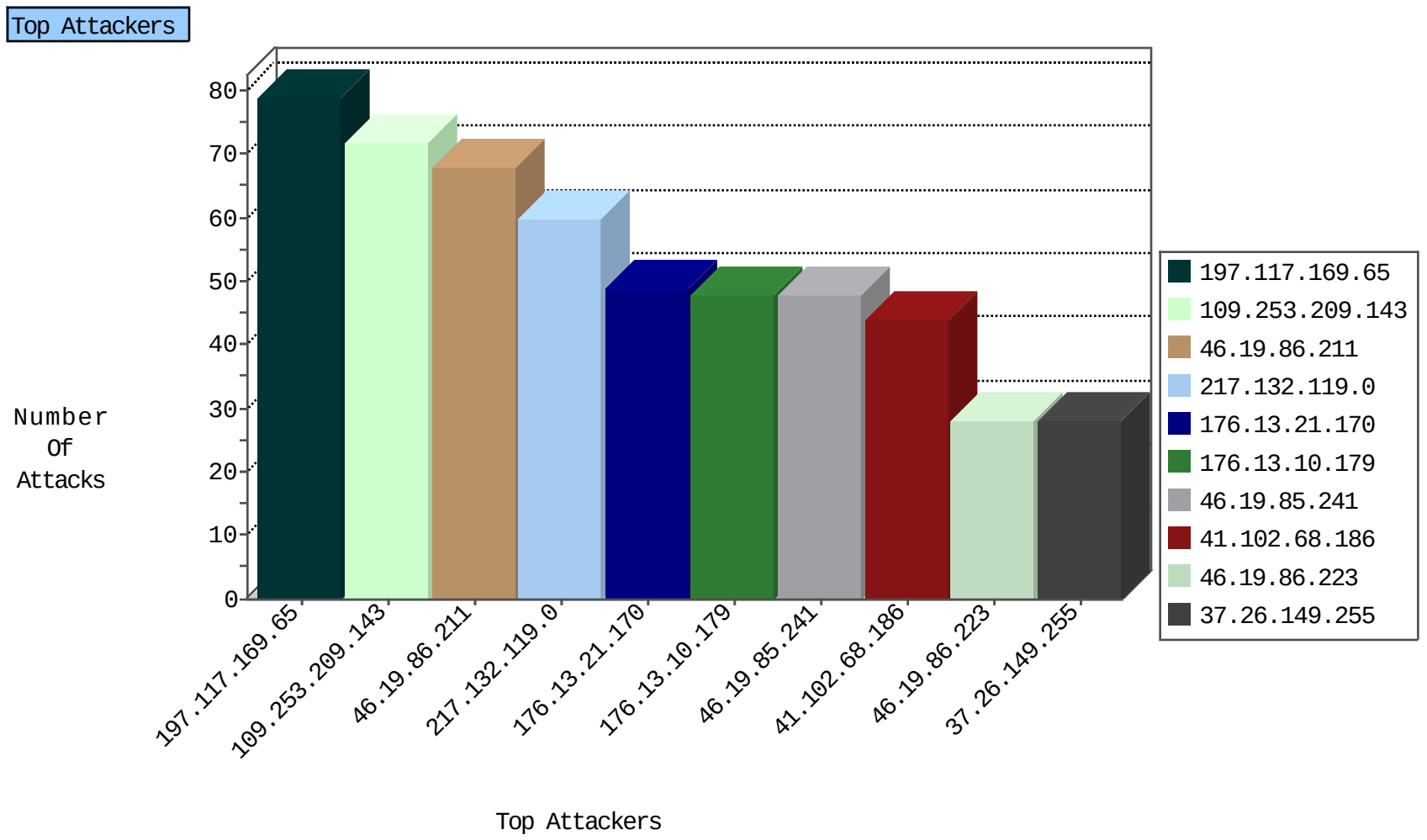
02-28-2016-14:04:06 to 02-28-2016-15:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-28-2016-14:04:06 to 02-28-2016-15:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.117.169.65	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	81
41.102.68.186	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	44
149.88.106.86	Israel	147.237.72.166	aka.idf.il	Anomaly-TCP-shortheader	dest-reset	3
149.88.106.86	Israel	147.237.72.166	aka.idf.il	Anomaly-TCP-SYN-FIN	dest-reset	2
134.147.203.115	Germany	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	2
146.185.239.100	Russian Federation	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
179.208.148.68	Brazil	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
74.82.47.17	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
199.115.117.12	United States	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	1
179.208.148.68	Brazil	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
114.33.82.30	Taiwan	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.33	Switzerland	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1

02-28-2016-14:04:06 to 02-28-2016-15:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.188.158.91	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
217.194.206.30	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
5.29.84.165	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
5.29.10.243	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.183.68.77	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.228.226.218	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
2.52.45.165	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.177.115.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
192.114.38.139	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.64.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.64.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

02-28-2016-14:04:06 to 02-28-2016-15:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
93.172.231.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
82.80.198.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.116.193.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.102.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.2.76	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.243.70	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.201.15	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
93.113.125.11	147.237.77.121	Romania	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
91.231.192.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.224.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.72.217		e.idf.il	ET SCAN NMAP -sS window 1024	1
192.117.2.168	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.48.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.114.176.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
68.180.228.112	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
164.39.11.198	147.237.8.45	United Kingdom	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.128.219	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.183.112	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.243.162	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.113.125.11	147.237.72.217	Romania	e.idf.il	ET SCAN NMAP -sS window 1024	1
84.229.148.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-28-2016-14:04:06 to 02-28-2016-15:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
217.132.119.0	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	52
46.19.85.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
176.13.21.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
46.19.86.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
37.26.149.255	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
37.26.148.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
82.81.47.15	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
46.19.85.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
62.219.137.44	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.253.150.165	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
109.253.201.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.210.131.50	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
197.117.169.65	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
109.253.150.165	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.81.238	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
79.179.55.196	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.209	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	8
66.249.81.238	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
217.132.119.0	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
79.179.55.196	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.52.157.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.81.241	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.179.230.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.81.241	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
132.64.215.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.81.241	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
132.66.199.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.157.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.69.38	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.122.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
79.182.176.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
66.249.81.235	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.179.69	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.114.111.17	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.248	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
185.33.169.66	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
204.12.251.37	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.150.161.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.116.13.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.150.161.210	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.52.4.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.40	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.144.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.177.191	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
192.114.91.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.53.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.209.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
46.19.86.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
176.13.10.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
66.249.79.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	14
66.249.66.69	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.69	Block	13
176.13.21.170	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
109.253.214.14	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	9
138.134.102.15	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 138.134.102.15	Block	7
66.249.81.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
37.26.149.255	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.210.131.50	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
80.246.139.184	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	4
46.19.86.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
37.26.147.179	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
2.54.32.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.118.114.75	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	3
109.253.209.143	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	3
2.54.143.175	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.8.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.214.14	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.52.5.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.64.202	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il/main/giyus/general.aspx	Block	3
109.253.201.111	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.148.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
138.134.102.15	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/2/size338x0/1802.jpg	Block	2
176.13.6.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.199.153	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	2
66.249.64.212	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il/main/giyus/general.aspx	Block	2
213.151.55.75	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 213.151.55.75	Block	2
66.249.69.38	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.69.38	Block	2
66.249.69.46	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.69.46	Block	1
109.253.216.117	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.54.18.134	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
94.188.158.91	Israel	147.237.0.34	tikshuv.idf.il	Parameter Type Violation FolderId in www.tikshuv.idf.il/modules/forums/forum.aspx	Block	1
66.249.64.202	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/tizmoret/gallery/	Block	1
213.8.204.38	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	1
79.181.63.13	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/112899.pdf	Block	1
46.117.131.181	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
199.207.253.96	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.183	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
66.249.64.233	United States	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
37.26.146.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.76.112.15	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/113525.pdf&sa=u&ved=0ahukewiv0jo5u5rlahwfhxokhtw3cuoqfggxmac&usg=afqjcnfmfdforv0thmmvoocpv3gi8up0pq	Block	1
82.81.47.15	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.177.166.232	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.86.72	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.46	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1

02-28-2016-14:04:06 to 02-28-2016-15:04:06