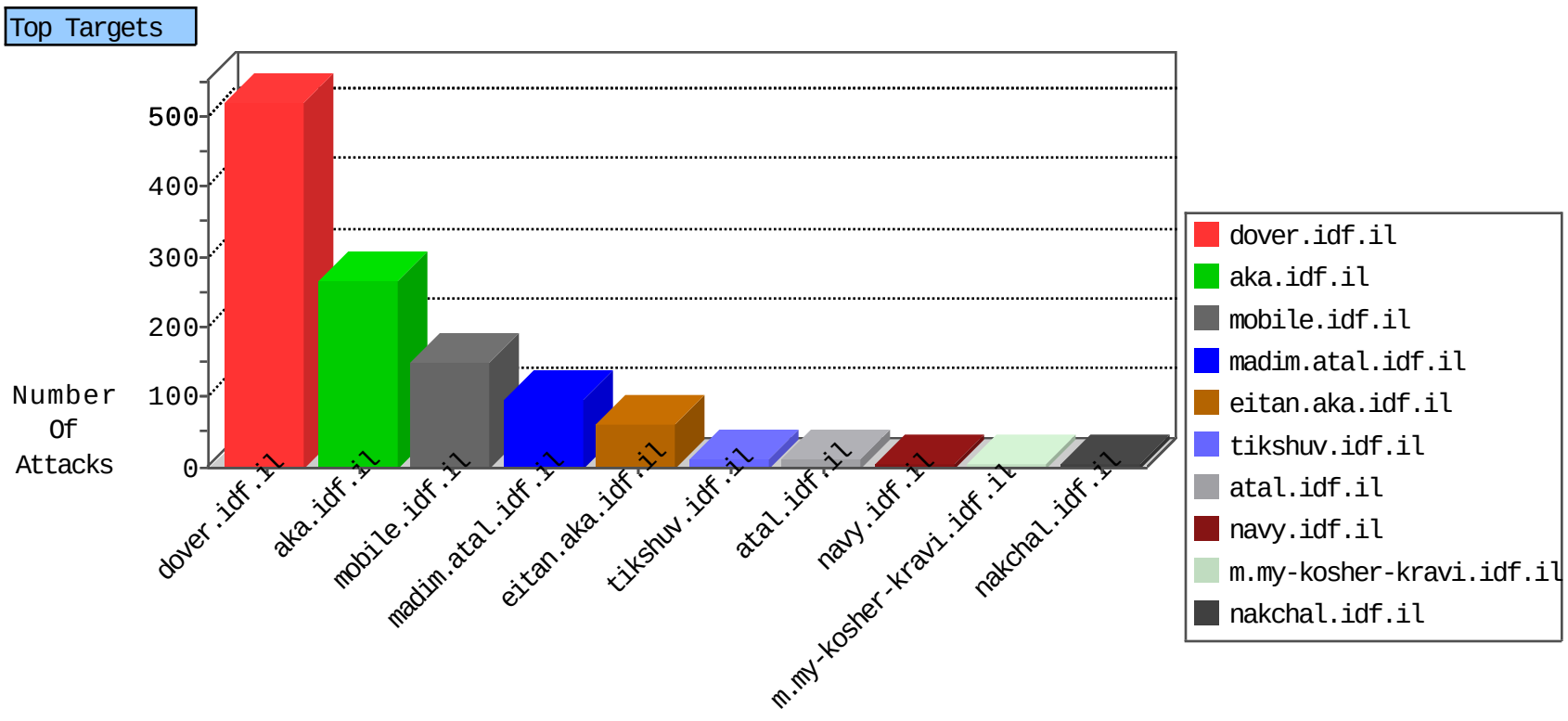
02-29-2016-01:09:48 to 02-29-2016-02:09:48

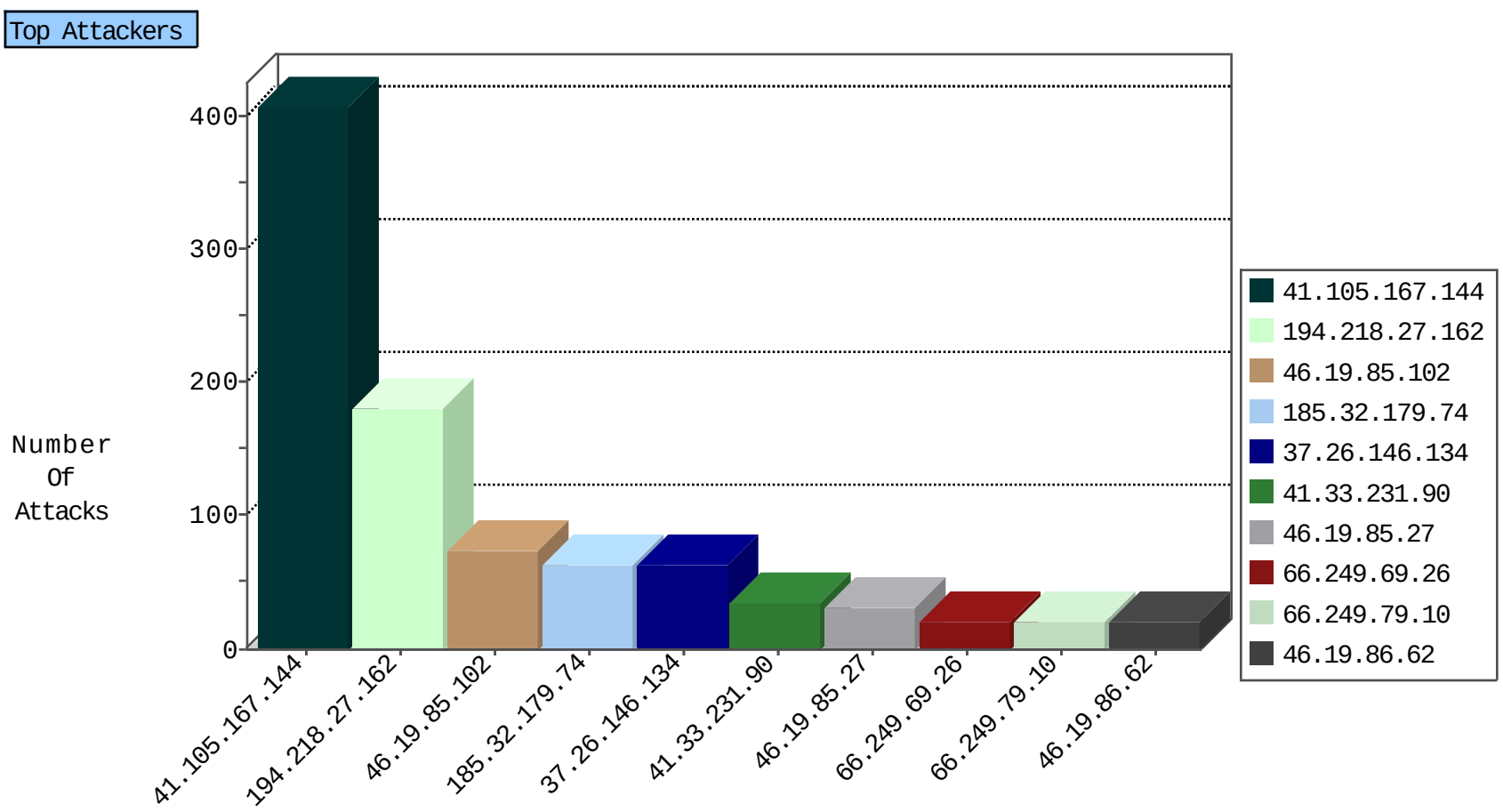
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-29-2016-01:09:48 to 02-29-2016-02:09:48

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.105.167.144	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	405
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
179.43.144.33	Switzerland	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
23.239.64.15	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
23.239.64.15	United States	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	1
23.239.64.15	United States	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
179.43.144.33	Switzerland	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.201		147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
23.239.64.15	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1

02-29-2016-01:09:48 to 02-29-2016-02:09:48

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.154.169.200	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
136.243.5.215	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	7
106.120.173.124	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
79.183.54.193	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
136.243.5.215	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	3
41.105.167.144	Algeria	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2
51.255.65.41	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.46	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.4	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.70	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.9	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.88	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.37	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

02-29-2016-01:09:48 to 02-29-2016-02:09:48

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
66.249.64.153	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
132.74.95.21	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
94.102.48.193	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
72.68.135.103	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
201.235.215.254	147.237.77.19	Argentina	law-forum.idf.il	ET SCAN NMAP -f -sS	1
185.130.5.249	147.237.72.217		e.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.249	147.237.8.28		e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
180.150.177.188	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.8.24		e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
201.235.215.254	147.237.77.19	Argentina	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
71.41.114.210	147.237.0.35	United States	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
195.216.176.244	147.237.76.34	Latvia	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
50.77.145.78	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.249	147.237.77.205		prisha.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.249	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.249	147.237.8.27		e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
164.39.11.198	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 4096	1

02-29-2016-01:09:48 to 02-29-2016-02:09:48

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
37.26.146.134	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
185.32.179.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
46.19.85.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
107.150.24.106	United States	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
104.132.1.98	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.62	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.230	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.209	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.213.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
104.177.186.182	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
156.192.2.80		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	5
46.19.86.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
66.249.79.10	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.177.61.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.224.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.104.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.132.2.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.158.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.54.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.8.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.45.78	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.129.230	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
79.181.146.104	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.46.39.243	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
97.32.132.193	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
157.55.39.58	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
67.183.66.106	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.52.129.230	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.170	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
138.36.0.3		147.237.76.44	e.refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
138.36.0.3		147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.62.53.168	Russian Federation	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.46.38.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.54.244.75	Netherlands	147.237.72.14	dover.idf.il(old	drop	First packet isn't SYN	drop	1
93.174.93.218	Netherlands	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.78	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.88.142.63	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
138.36.0.3		147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.21.5	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
138.36.0.3		147.237.8.14	e.orchot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.171	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
138.36.0.3		147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	20
185.32.179.74	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	12
185.32.179.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.62	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
46.19.85.27	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
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
66.249.66.15	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.66.15	Block	2
40.77.167.86	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
66.249.78.80	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
46.19.86.209	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.79.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;resized in www.aka.idf.il/edim/yoman/enlarge.asp	None	1
66.249.79.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/yohalan/main/main.asp	None	1
172.56.38.2	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.18	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.66.18	Block	1
66.249.79.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/giyus/kadatzhelp/	None	1
66.249.78.87	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
95.24.56.182	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.79.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;sOrderBy in www.aka.idf.il/iturim/asp/wars.asp	None	1
66.249.79.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;doc in www.aka.idf.il/yohalan/main/main.asp	None	1
66.249.66.39	United States	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
81.223.254.34	Austria	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /robots.txt	Block	1
66.249.79.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;innerCatID in www.aka.idf.il/giyus/qanda/	None	1
66.249.78.94	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
52.48.17.30	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
95.24.56.182	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.79.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;sideScroll in www.aka.idf.il/giyus/general/	None	1
66.249.79.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/brothers/faq/default.asp	None	1
66.249.69.26	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.64.134.25	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gws_rd in www.aka.idf.il/	None	1
46.19.86.11	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.79.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;pageNum in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
66.249.79.10	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.79.10	Block	1
66.249.64.165	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
141.212.122.64	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /x	Block	1
66.249.79.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;sidescroll in www.aka.idf.il/giyus/kadatz/	None	1
66.249.79.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/brothers/gallery/	None	1
203.133.170.168	Korea, Republic of	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.64.134.25	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gws_rd in www.aka.idf.il/main/home/default.aspx	None	1
66.249.79.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;pagenum in www.aka.idf.il/giyus/forum/asp/showforum.asp	None	1
66.249.79.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/lomdim/tochen/	None	1
157.55.39.58	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/sachar/klali.aspx	None	1
66.249.79.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter catlD in www.aka.idf.il/yohalan/main/main.asp	None	1
66.249.79.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/giyus/forms/	None	1
87.70.45.78	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1