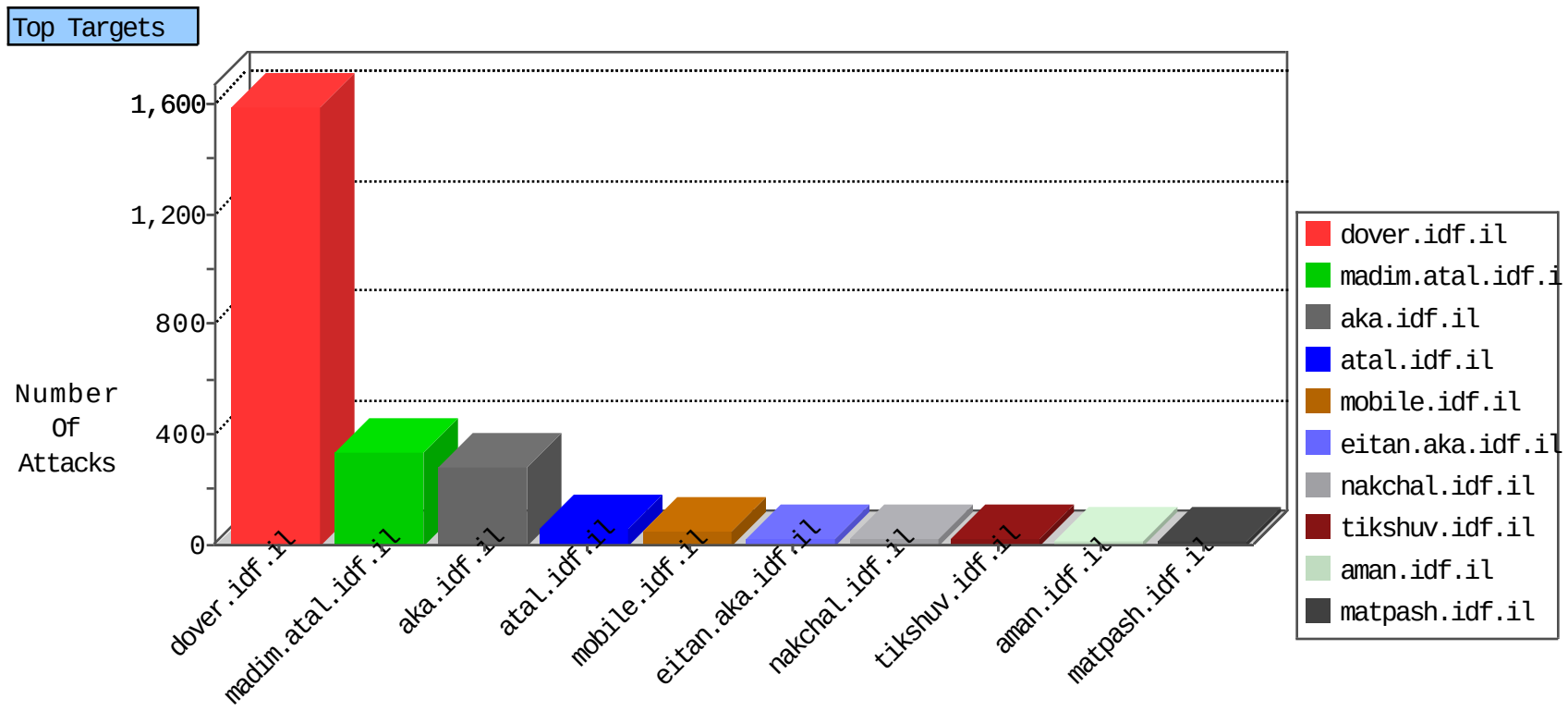
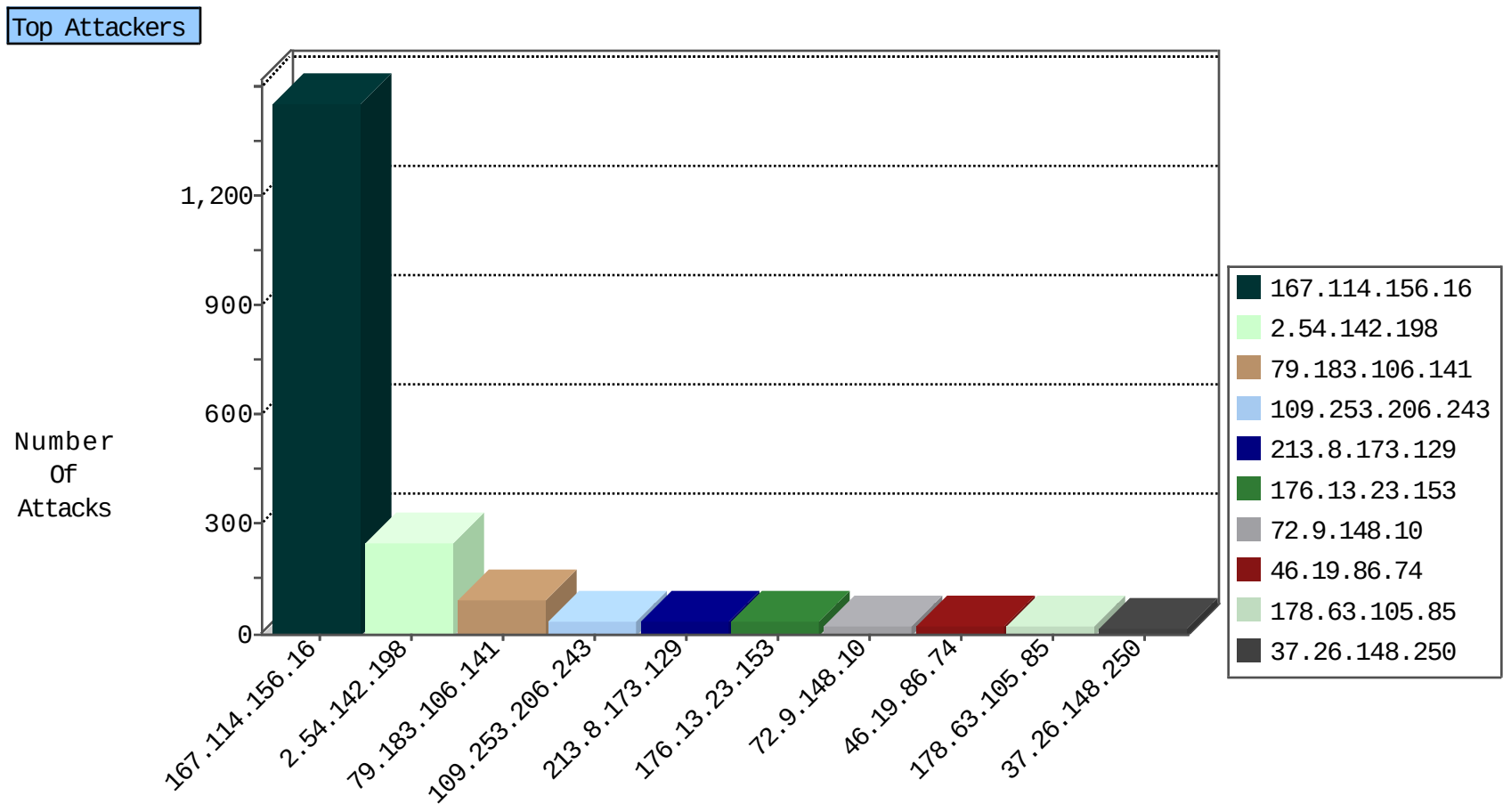
03-12-2016-23:04:03 to 03-13-2016-00:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-12-2016-23:04:03 to 03-13-2016-00:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3999
82.145.216.177	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
82.145.217.85	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
82.145.209.29	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	4
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
61.74.183.69	Korea, Republic of	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
46.105.160.158	France	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1

03-12-2016-23:04:03 to 03-13-2016-00:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.0.128	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
159.122.222.194	Netherlands	147.237.0.15	kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	4
159.122.222.194	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	4
184.19.86.115	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
89.138.95.54	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
109.64.188.218	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
176.228.68.96	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
188.165.15.27	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
159.122.222.194	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
159.122.222.194	Netherlands	147.237.0.15	kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

03-12-2016-23:04:03 to 03-13-2016-00:04:03

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
176.13.15.192	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
52.53.224.202	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
52.36.12.248	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
208.71.68.132	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -f -sS	1
202.71.25.29	147.237.76.196	India	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
192.3.9.122	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
159.122.222.194	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	1
109.235.254.181	147.237.76.201	Turkey	e.atal.idf.il	ET SCAN NMAP -sS window 2048	1
109.235.254.181	147.237.76.201	Turkey	e.atal.idf.il	ET SCAN NMAP -f -sS	1
52.53.224.202	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 4096	1
52.36.12.248	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
208.71.68.132	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
23.99.118.64	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
202.71.25.29	147.237.76.196	India	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
159.122.222.194	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	1
109.235.254.181	147.237.76.201	Turkey	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.77.233	Austria	atal.idf.il	ET SCAN NMAP -sS window 1024	1

03-12-2016-23:04:03 to 03-13-2016-00:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.8.173.129	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
46.19.86.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
37.26.148.250	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
109.67.62.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
77.125.153.129	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.183.106.141	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
79.183.106.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
79.183.106.141	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
79.183.106.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
79.183.106.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
79.183.106.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	12
109.253.157.252	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.8.155	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.183.106.141	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
164.138.117.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
185.32.179.246	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.154.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.122.158.235	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
95.91.213.12	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.15.192	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.0.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.15.192	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.177.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.254.8.69	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	6
79.183.182.235	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
46.19.85.34	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
79.183.106.141	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.i	drop	SAM rule	drop	4
46.19.85.34	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
84.109.50.139	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
95.91.212.197	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.22.135.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.177.131.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.245.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.217.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.17.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.34.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.116	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.118.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.10.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.242.21	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.182.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
94.159.152.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.29		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.144.64	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
2.54.142.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	253
109.253.206.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
176.13.23.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	34
79.178.212.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
31.44.136.55	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
37.26.147.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.148.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
157.55.39.193	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.122.158.235	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
217.69.133.242	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/doctor	Block	1
37.122.158.235	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/wp-admin/index.php	Block	1
176.13.8.2	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/wp-admin/index.php	Block	1
95.86.94.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/iturim/asp/displayallsoldiers.asp	Block	1
199.30.24.162	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
149.50.50.8	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
79.181.0.128	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
217.69.133.247	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/html/10.asp	Block	1
37.122.158.235	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-admin/index.php	Block	1
176.13.10.79	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
95.91.212.197	Germany	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/brothers/faq/default.asp	None	1
207.46.13.87	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/...	Block	1
156.174.186.207		147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.133.193	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
217.118.91.57	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
46.19.86.129	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/text.css	Block	1
176.13.10.79	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 176.13.10.79	Block	1
107.77.90.45	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1400-en/dover.aspx	Block	1
68.180.228.170	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation PageNum in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	1
207.241.229.223	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/opevent/opevent.aspx	Block	1
87.71.71.181	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
217.118.91.57	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
108.26.182.132	United States	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
68.180.230.152	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
213.8.173.129	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.8.2	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
89.138.114.170	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
5.22.135.116	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
180.76.15.8	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1