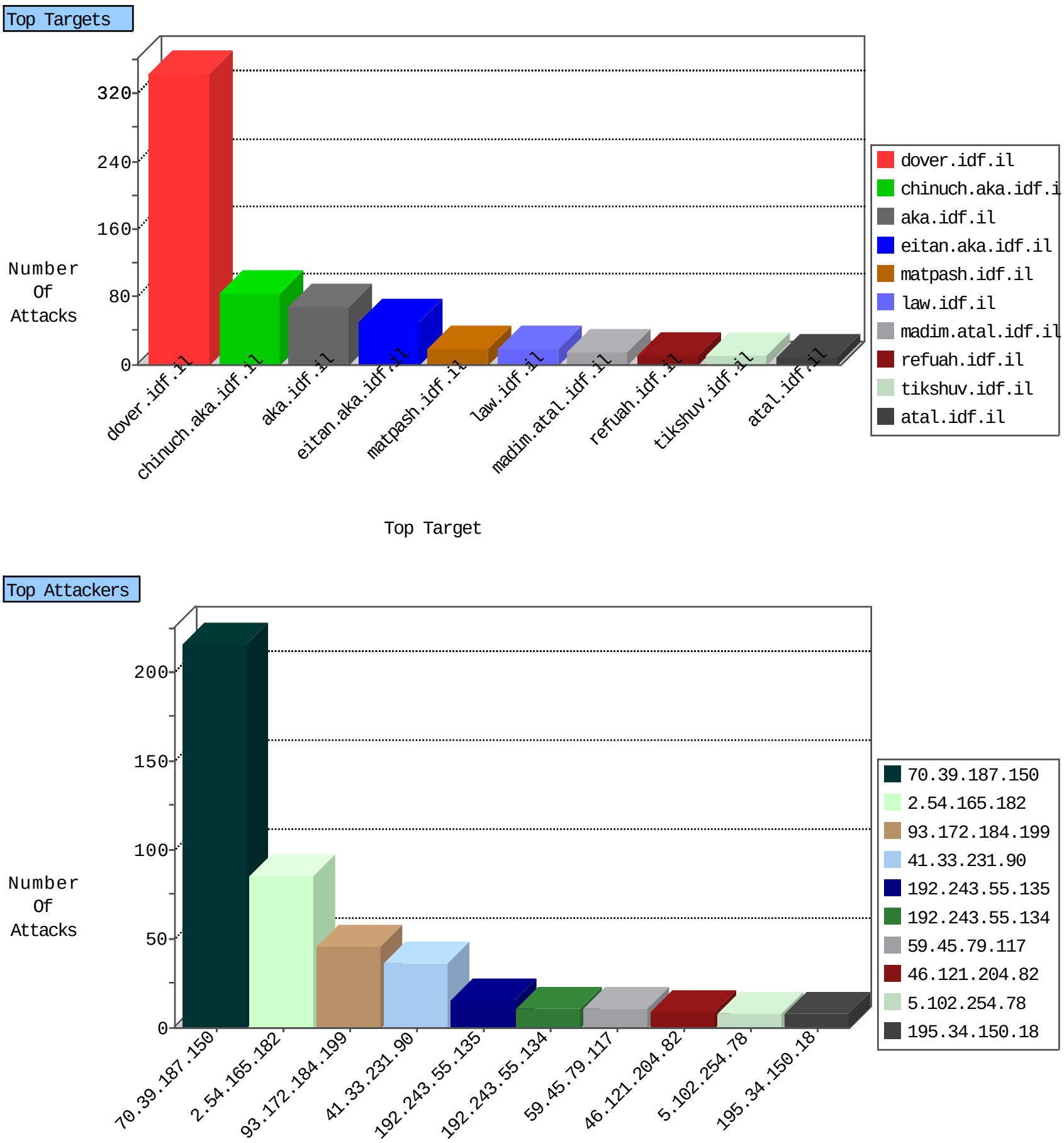
02-19-2016-08:04:02 to 02-19-2016-09:04:02

IDF Under Attack Daily Report



02-19-2016-08:04:02 to 02-19-2016-09:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
185.130.5.224		147.237.76.44	e.refuah.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
59.33.23.109	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
109.201.152.234	Netherlands	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

02-19-2016-08:04:02 to 02-19-2016-09:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.130.33	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
136.243.152.18	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	2
79.177.204.97	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1

02-19-2016-08:04:02 to 02-19-2016-09:04:02

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
80.246.133.102	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
27.221.10.194	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.105	147.237.77.19	Russian Federation	law-forum.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.105	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
45.55.236.147	147.237.8.45		e.eitan.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
190.29.102.18	147.237.8.28	Colombia	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.105	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.105	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.77.226	China	www.chamatz.aka.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

02-19-2016-08:04:02 to 02-19-2016-09:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
70.39.187.150	Satellite Provider	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	119
70.39.187.150	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	97
2.54.165.182	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
93.172.184.199	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.121.204.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.102.254.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
149.88.67.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
62.0.197.197	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.76	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
89.138.108.191	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.96.128.60	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
188.120.154.57	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.133.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.188.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.114.163.168	Israel	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
37.26.146.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.6.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.84	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
80.246.133.102	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
176.13.20.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
84.108.61.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.243.55.136	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
80.246.133.102	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.20.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.142.68.10	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.110	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
148.251.21.227	Germany	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence		monitor	2
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
94.230.86.184	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.146.222	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.108.61.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
188.120.148.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
79.177.183.10	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	1
184.105.139.74	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
65.25.190.154	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.36.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.121.57.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.15.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.188.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.149	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.164	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
86.62.117.180	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
66.249.79.104	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
185.89.217.231		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
128.232.110.28	United Kingdom	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
46.146.130.126	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
210.51.55.3	China	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/console	Block	1
88.27.116.214	Spain	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
74.82.47.4	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
2.54.165.182	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
185.89.217.233		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
148.251.21.227	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 148.251.21.227	Block	1
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
220.134.189.104	Taiwan	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
49.237.199.129	Thailand	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$3 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
178.215.80.72	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
77.75.78.171	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/31/	Block	1
195.138.85.250	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/sendtofriend.aspx?&amp	Block	1
148.251.21.227	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/undefined/	Block	1
80.246.136.177	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$1 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
220.134.189.104	Taiwan	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/xmlrpc.php	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2412.jpg	Block	1
178.215.80.72	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
95.86.84.98	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19149-he/dover	Block	1
77.125.88.69	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/926-he/refuah.aspx	Block	1
207.46.13.84	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
148.251.21.227	Germany	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 148.251.21.227	Block	1
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
220.255.148.17	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
178.255.87.242	United Kingdom	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/robots.txt	Block	1
104.128.144.131	Canada	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
79.179.57.4	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1

02-19-2016-08:04:02 to 02-19-2016-09:04:02