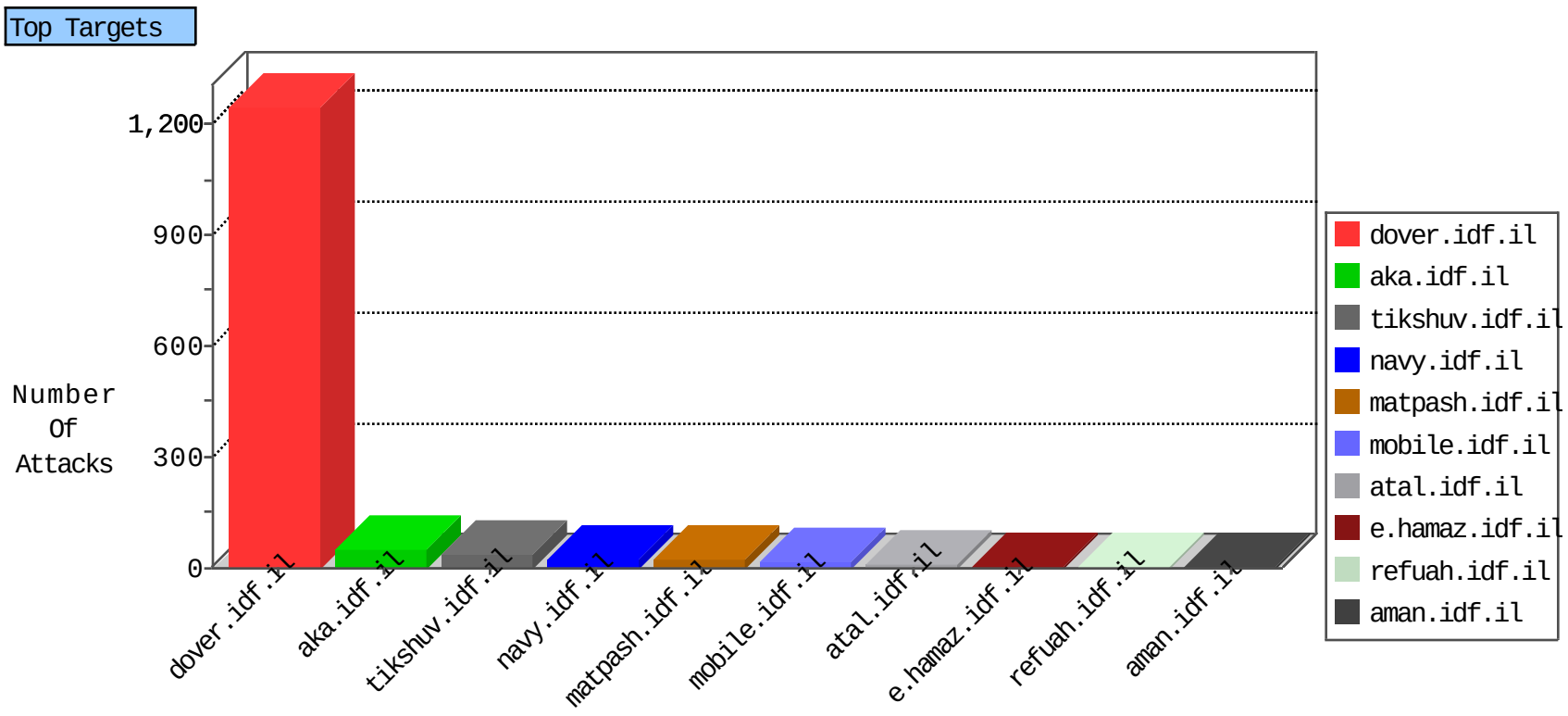
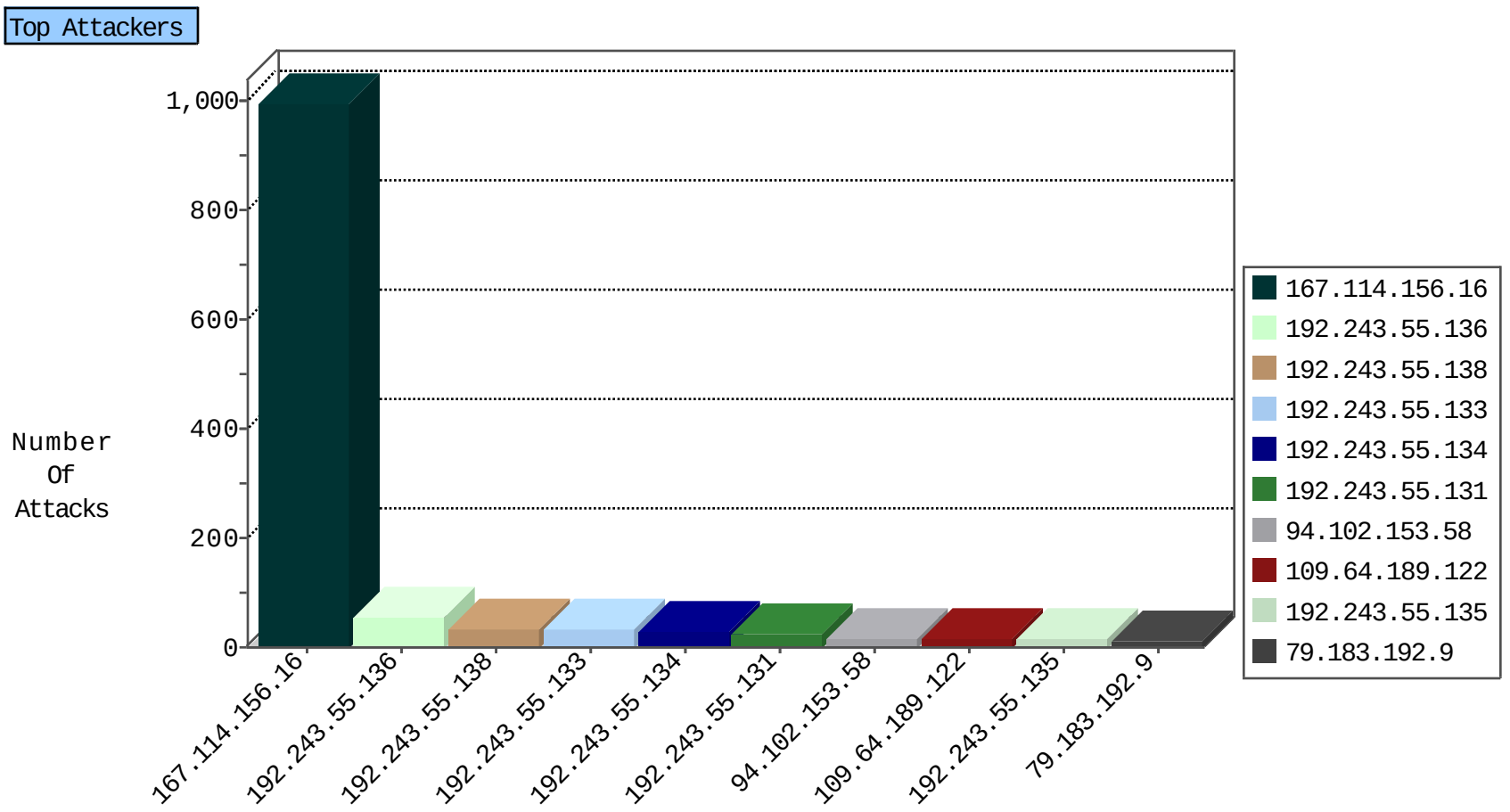
03-12-2016-08:04:06 to 03-12-2016-09:04:06

IDF Under Attack Daily Report





03-12-2016-08:04:06 to 03-12-2016-09:04:06

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	3038
134.147.203.115	Germany	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	2
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
69.25.27.115	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
162.248.100.195	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.206	Netherlands	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
162.248.100.195	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
118.104.245.161	Japan	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1
58.97.74.88	Thailand	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1

03-12-2016-08:04:06 to 03-12-2016-09:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.192.9	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
89.139.244.147	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
184.173.233.226	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
94.102.153.58	United Kingdom	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
203.171.33.38	New Zealand	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
5.102.206.148	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
209.15.196.171	Canada	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
108.59.8.80	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
213.8.204.20	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
87.68.59.23	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
134.249.53.96	Ukraine	147.237.77.176	matpash.idf.il	C1000016: HTTP: administrator in URI	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-12-2016-08:04:06 to 03-12-2016-09:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.102.153.58	147.237.77.176	United Kingdom	matpash.idf.il	SQL Injection - Select From	12
184.173.233.226	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
209.15.196.171	147.237.76.86	Canada	navy.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
203.171.33.38	147.237.76.86	New Zealand	navy.idf.il	SQL Injection - Select From	4
185.72.179.221	147.237.77.170		maarachot.idf.il	ET SCAN Potential SSH Scan	1
117.247.188.5	147.237.77.19	India	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.48.194	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.72.166	Austria	aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
93.113.125.12	147.237.0.19	Romania	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.244.49.137	147.237.76.199	Hong Kong	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
40.74.124.12	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.221	147.237.77.227		e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.72.217		e.idf.il	ET SCAN Potential SSH Scan	1
139.217.27.204	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
93.113.125.12	147.237.8.14	Romania	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
61.244.49.137	147.237.77.234	Hong Kong	halag.idf.il	ET SCAN NMAP -sS window 1024	1
61.244.49.137	147.237.76.198	Hong Kong	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.76.202	Sweden	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1

03-12-2016-08:04:06 to 03-12-2016-09:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
109.64.189.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
99.93.104.54	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
2.54.29.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
104.232.181.118		147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	5
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
203.171.33.38	New Zealand	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
40.77.167.9	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.70.98.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.55.9.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.44.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.19.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
87.71.93.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
93.158.152.77	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.1.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.218.177	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
93.158.152.201	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
220.240.108.14	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
157.55.39.134	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.135	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	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

03-12-2016-08:04:06 to 03-12-2016-09:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
160.16.234.227	Japan	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 160.16.234.227	Block	5
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
40.77.167.21	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/rights/asp/home.asp/info.asp	Block	2
40.77.167.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/contactus.aspx	Block	1
213.21.33.24	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/default.aspx'	Block	1
134.249.53.96	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
192.30.231.229	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20296-he/dover.aspx	Block	1
88.2.225.36	Spain	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
64.19.78.242	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
213.21.33.24	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter amp;catid in www.aka.idf.il/rights/asp/info.asp	None	1
157.55.39.134	United States	147.237.72.166	aka.idf.il	Unknown Parameter innercatid in aka.idf.il/giyus/qanda/	None	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1391-12626-e n/dover.aspx	Block	1
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17060-en/dover.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
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/3480.jpg	Block	1
157.55.39.183	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/rights/asp/home.asp/info.asp	Block	1
74.82.47.4	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
37.26.146.132	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
197.132.47.95	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
95.54.174.143	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/story.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/71547.pdf	Block	1
79.179.217.156	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb14567119 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
199.30.25.54	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
134.249.53.96	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
184.105.247.195	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
84.108.207.146	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1

03-12-2016-08:04:06 to 03-12-2016-09:04:06