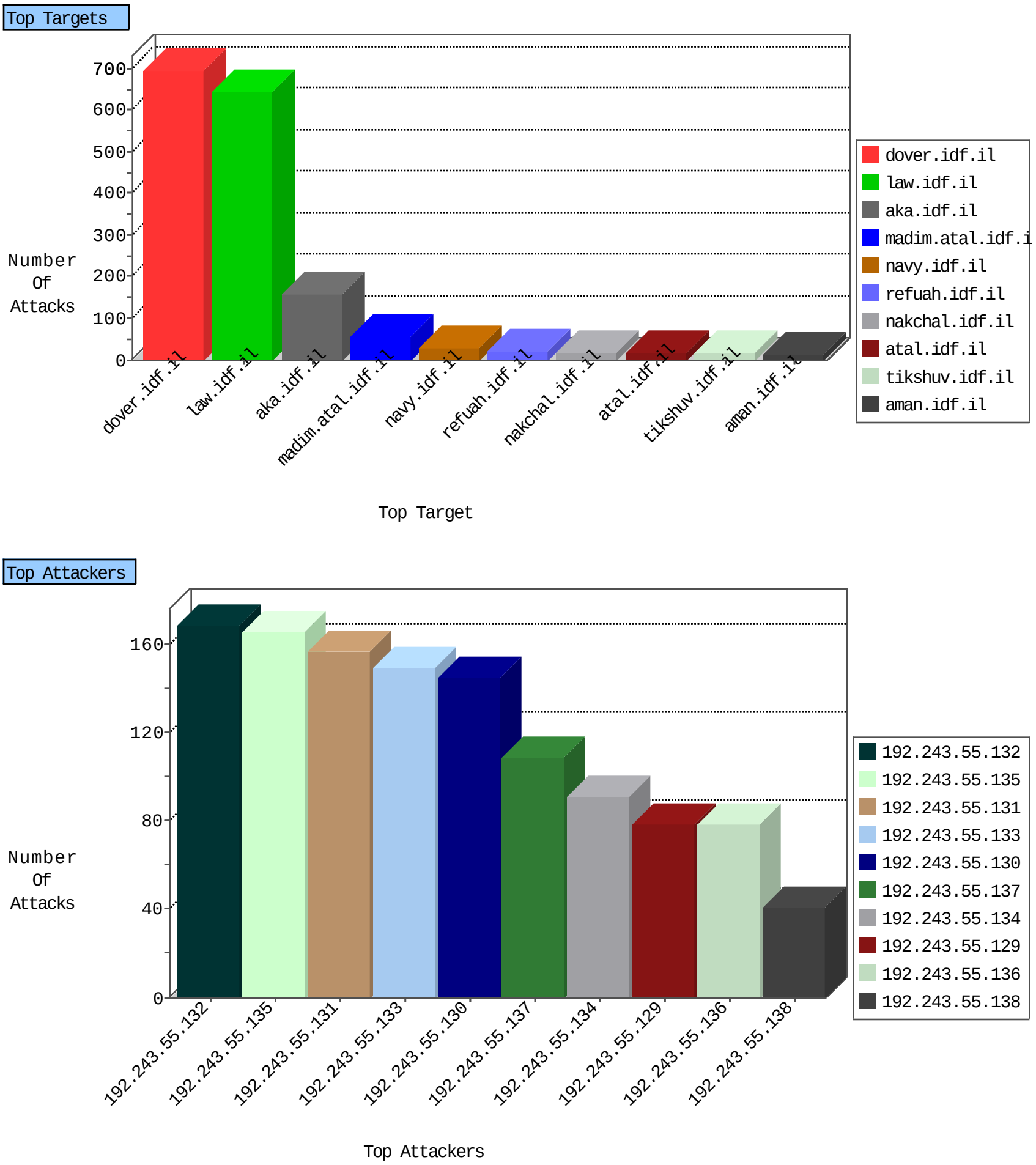
04-12-2016-08:04:07 to 04-12-2016-09:04:07

IDF Under Attack Daily Report



04-12-2016-08:04:07 to 04-12-2016-09:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.197.110	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	157
79.177.137.251	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	131
85.64.120.27	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	24
192.243.55.133	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
194.9.252.237	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.243.55.130	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
2.53.8.255	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
79.178.181.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
2.53.49.23	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.243.55.135	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
24.217.142.219	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-12-2016-08:04:07 to 04-12-2016-09:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	6
212.117.143.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
80.246.133.227	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
212.235.98.139	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
192.118.12.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-12-2016-08:04:07 to 04-12-2016-09:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.178.78.138	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
1.34.35.15	147.237.0.35	Taiwan	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
208.100.26.228	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.72.166	Latvia	aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
149.78.248.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.59.33.61	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 2048	1
109.253.206.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.50.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.11.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.48.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.72.156	Latvia	aman.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.140.23	147.237.8.46	United Kingdom	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
122.3.156.75	147.237.0.16	Philippines	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.59.33.61	147.237.0.33	China	idf.il	ET SCAN NMAP -f -sS	1
80.82.78.38	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

04-12-2016-08:04:07 to 04-12-2016-09:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	36
192.243.55.132	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	32
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	26
192.243.55.135	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	26
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	24
192.243.55.131	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	23
192.243.55.133	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	22
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
192.243.55.130	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
192.243.55.132	United States	147.237.77.216	dover.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
192.243.55.130	United States	147.237.77.216	dover.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
192.243.55.135	United States	147.237.77.216	dover.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
192.243.55.137	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
192.243.55.135	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
192.243.55.132	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.133	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
195.200.205.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.131	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	15
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.131	United States	147.237.77.216	dover.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
192.243.55.131	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	13
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.130	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.132	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
87.70.23.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.130	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
192.243.55.129	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.130	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.131	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
192.243.55.137	United States	147.237.77.216	dover.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
212.143.142.56	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
192.243.55.137	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.135	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10

04-12-2016-08:04:07 to 04-12-2016-09:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.14.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
37.26.149.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
46.19.86.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
79.177.118.81	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	8
79.177.118.81	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.177.118.81	Block	7
80.178.157.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.15.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.24.204	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.195	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.66	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	2
2.53.163.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
199.30.25.12	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.253	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
80.178.157.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
65.55.210.98	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.12.68	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.25.144	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
65.55.210.100	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.25.147	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.16.170	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.158	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
130.185.155.82	Sweden	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
46.19.85.190	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.183.50.113	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
192.243.55.135	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	1
149.78.219.88	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
130.185.155.82	Sweden	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/master/vendorscript	Block	1
192.243.55.135	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/titlecap.png	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
79.177.118.81	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	1
66.249.64.4	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/navmenu/	Block	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/1/561.doc.	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2110-he/cogat.aspx	Block	1
195.200.205.2	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
157.55.39.54	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/src="http:/www.youtube.com/v/0mwqtc ld1fe	Block	1
108.227.98.31	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
23.106.239.232	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/shared/usercontrols/headerupper/	Block	1
79.180.183.29	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/schar	Block	1
192.243.55.132	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	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
46.116.52.123	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
149.50.85.17	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl17 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
68.180.230.155	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in www.eitan.aka.idf.il/1103-he/eitan.aspx	None	1

04-12-2016-08:04:07 to 04-12-2016-09:04:07