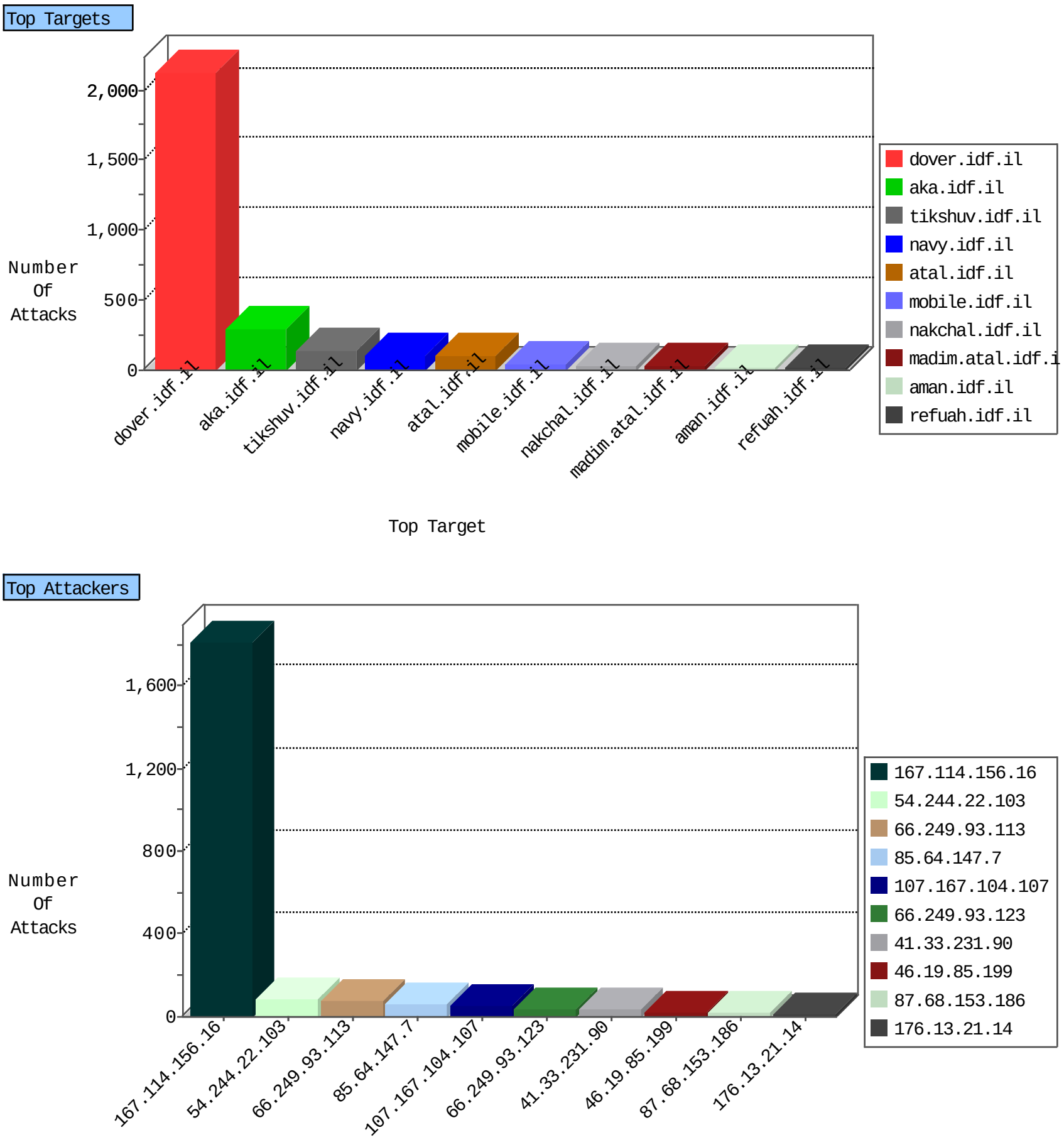
01-14-2016-17:04:01 to 01-14-2016-18:04:01

IDF Under Attack Daily Report



01-14-2016-17:04:01 to 01-14-2016-18:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	19970
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3485
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.10	China	147.237.76.196	e.sviva.idf.il	JLM_Purple_Con_Limit_Http	drop	3
192.118.132.185	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.10	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Http	drop	1
151.80.109.172	Italy	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
74.143.58.3	United States	147.237.76.44	e.refuah.idf.i	Block_Udp_All_Nets	drop	1

01-14-2016-17:04:01 to 01-14-2016-18:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.36.87	United Kingdom	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

01-14-2016-17:04:01 to 01-14-2016-18:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.113	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	76
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.93.123	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.160	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.127	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.73.214	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
151.76.255.8	147.237.77.216	Italy	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.253.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.251.56.171	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.76.198	Canada	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
84.228.250.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
216.178.244.30	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
80.246.136.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.55.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.93.187.23	147.237.76.196		e.sviva.idf.il	ET SCAN Potential SSH Scan	1
185.93.187.23	147.237.76.86		navy.idf.il	ET SCAN Potential SSH Scan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.142.7	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.39.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.76.198	Canada	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
2.52.13.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.63.7	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
220.130.235.173	147.237.76.38	Taiwan	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
81.218.122.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
216.178.244.30	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
79.179.10.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.93.187.23	147.237.76.198		e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
185.93.187.23	147.237.76.148		gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
185.93.187.23	147.237.0.33		idf.il	ET SCAN Potential SSH Scan	1

01-14-2016-17:04:01 to 01-14-2016-18:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	70
107.167.104.107	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	52
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
176.13.21.14	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	13
87.68.153.186	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
37.142.64.65	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.86.41	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.45	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
157.55.39.196	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
94.230.86.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.183.86	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.6.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.15.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.68.153.186	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
79.178.6.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.174.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.129.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.147.238	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.98	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.161.229	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.93.127	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
84.111.7.5	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.29	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.202.203	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
23.101.61.176	Ireland	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
37.17.224.62	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.88	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.13.46	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.202.203	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.88	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.46.39.20	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4

01-14-2016-17:04:01 to 01-14-2016-18:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.147.7	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 85.64.147.7	Block	61
2.52.10.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
187.156.138.240	Mexico	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 187.156.138.240	Block	6
62.219.154.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
125.46.26.253	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-admin/admin-ajax.php	Block	2
109.253.157.215	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
109.64.32.75	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.64.32.75	Block	2
46.19.85.35	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
176.13.13.228	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
125.46.26.253	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
89.138.116.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.120.28.83	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
37.187.129.166	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
176.13.21.50	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
80.246.133.226	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
5.22.129.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
125.46.26.253	China	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 125.46.26.253	Block	1
62.210.84.121	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.228.176.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.120.126.36		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
79.179.199.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.146.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.54.49.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.141.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
93.232.255.235	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.121.209.91	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
38.81.65.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
183.79.221.223	Japan	147.237.76.200	eitan.aka.idf.il	Unknown Parameter l in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
82.80.166.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.126.253.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.28.163.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.210.84.121	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.210.84.121	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.85.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.168	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.181.184.125	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
37.26.149.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
2.54.133.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
46.166.137.213	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
213.8.245.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/63904.ppt	Block	1
95.86.97.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1

01-14-2016-17:04:01 to 01-14-2016-18:04:01