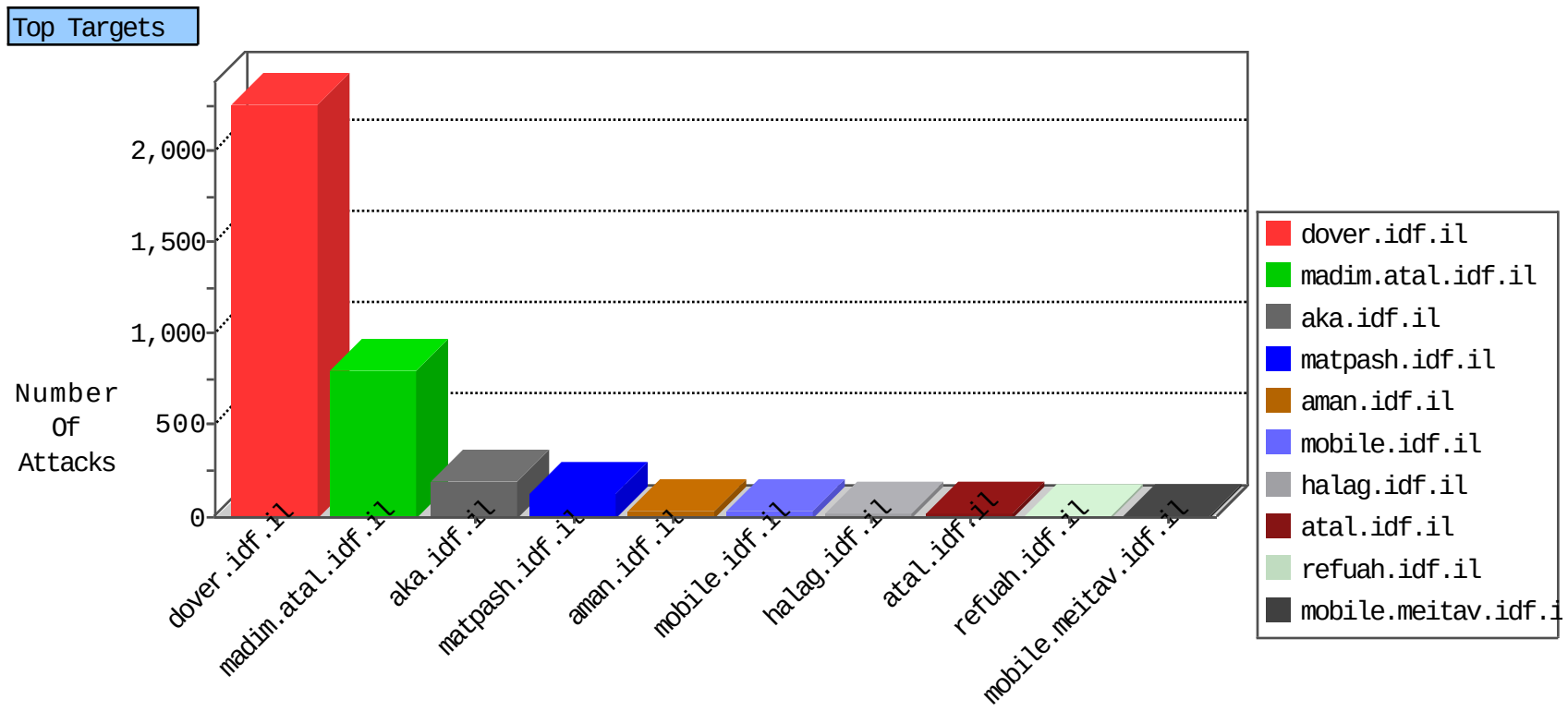
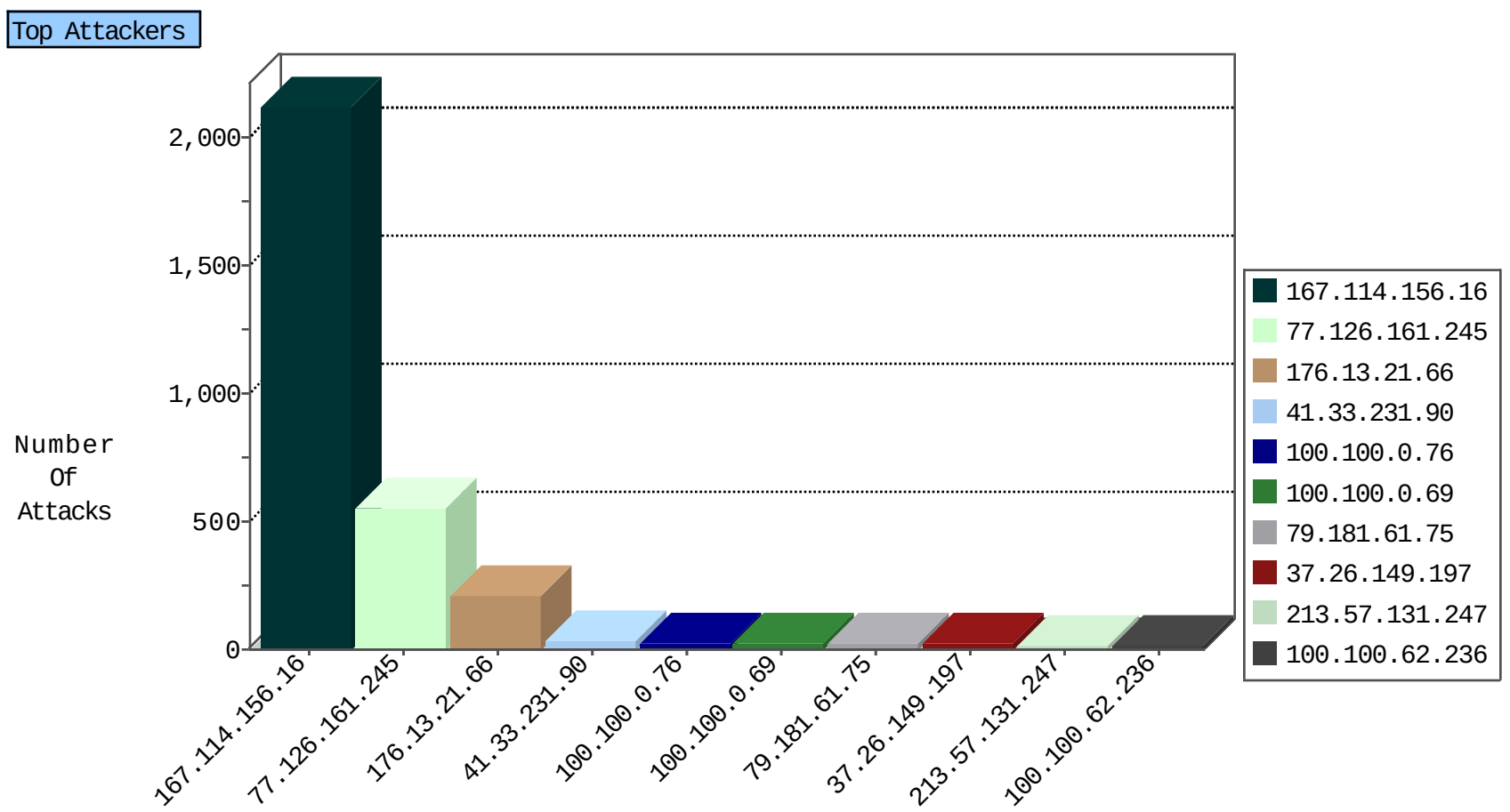
11-28-2015-10:04:07 to 11-28-2015-11:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-28-2015-10:04:07 to 11-28-2015-11:04:07

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	3244
66.249.66.33	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	186
61.182.170.38	China	147.237.76.147	chinuch.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
66.240.236.119	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
196.184.16.94		147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
66.249.66.39	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1

11-28-2015-10:04:07 to 11-28-2015-11:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-28-2015-10:04:07 to 11-28-2015-11:04:07

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
66.249.73.193	147.237.77.216	United States	dover.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
113.240.250.155	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.182.170.38	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
58.218.177.171	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
31.6.71.154	147.237.72.166	Poland	aka.idf.il	ET SCAN NMAP -sS window 1024	1
121.27.100.184	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
119.254.103.15	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
119.254.103.15	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
119.254.103.15	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
79.180.55.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
61.182.170.38	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
40.76.57.67	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
23.227.196.29	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
119.254.103.15	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
119.254.103.15	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
119.254.103.15	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

11-28-2015-10:04:07 to 11-28-2015-11:04:07

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.il	drop	SAM rule	drop	36
100.100.0.76		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
100.100.0.69		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
37.26.149.197	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
100.100.62.236		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
176.13.21.66	Israel	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	13
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.86.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
100.100.117.81		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
77.126.252.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.73.201	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.131.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
40.77.167.76	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.146.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.106.183	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.83.155	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.131.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.83.158	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
66.249.83.161	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.7.59	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
213.57.177.56	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
176.13.7.59	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
31.210.186.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.131.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
157.55.39.208	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.57.177.56	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
188.120.148.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.177.181.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.147.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.56.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.177.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
186.202.127.238	Brazil	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
79.176.20.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.85	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
188.120.148.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.177.164.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.218	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

11-28-2015-10:04:07 to 11-28-2015-11:04:07

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
77.126.90.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.190.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

11-28-2015-10:04:07 to 11-28-2015-11:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.126.161.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	343
77.126.161.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	168
176.13.21.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
176.13.21.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	66
77.126.161.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	42
79.181.61.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
111.67.19.116	Australia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
91.185.213.137	Slovenia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
54.174.197.117	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
173.254.55.58	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
200.98.197.90	Brazil	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
50.87.161.155	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
182.160.163.148	Australia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
198.20.241.76	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
176.106.227.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
194.100.58.154	Finland	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
185.120.126.60		147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 185.120.126.60	None	3
37.9.169.3	Slovakia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
217.199.164.217	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
37.187.29.115	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
2.54.176.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
41.78.6.166	South Africa	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
209.175.158.221	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
64.34.157.120	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
176.31.90.37	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
173.254.55.137	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
37.187.29.115	France	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 37.187.29.115	Block	2
217.199.164.217	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
209.175.158.221	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 209.175.158.221	Block	2
64.34.157.120	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 64.34.157.120	Block	2
200.98.197.90	Brazil	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 200.98.197.90	Block	2
173.254.55.137	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
111.67.19.116	Australia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
54.174.197.117	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
85.65.12.111	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/kapatz/	Block	2
198.20.241.76	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 198.20.241.76	Block	2
173.254.55.58	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
2.54.38.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.13.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
50.87.161.155	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
182.160.163.148	Australia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
85.65.205.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.13.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.228.24.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
77.125.96.181	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
192.117.13.162	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.14.131.109	Romania	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
216.218.206.66	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
66.249.67.133	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1

11-28-2015-10:04:07 to 11-28-2015-11:04:07