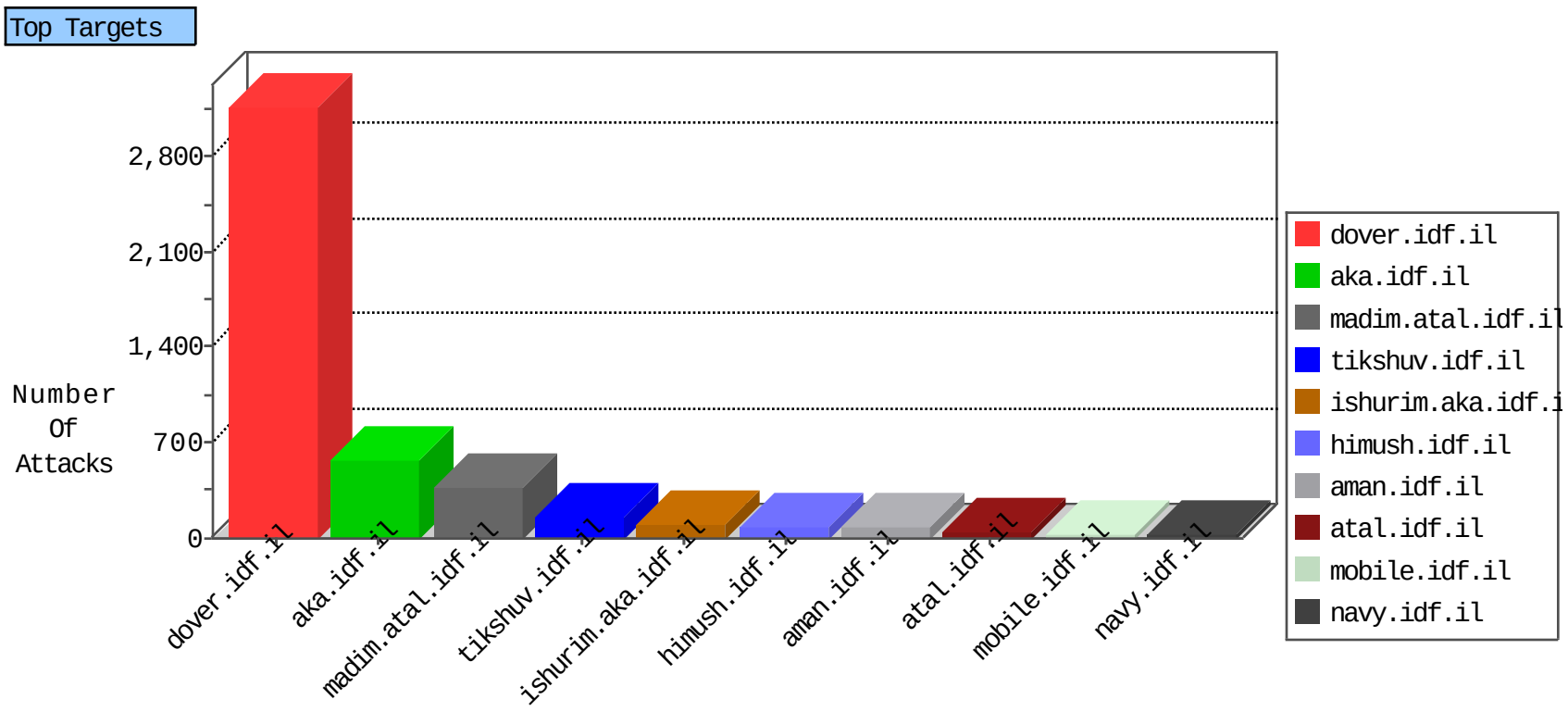
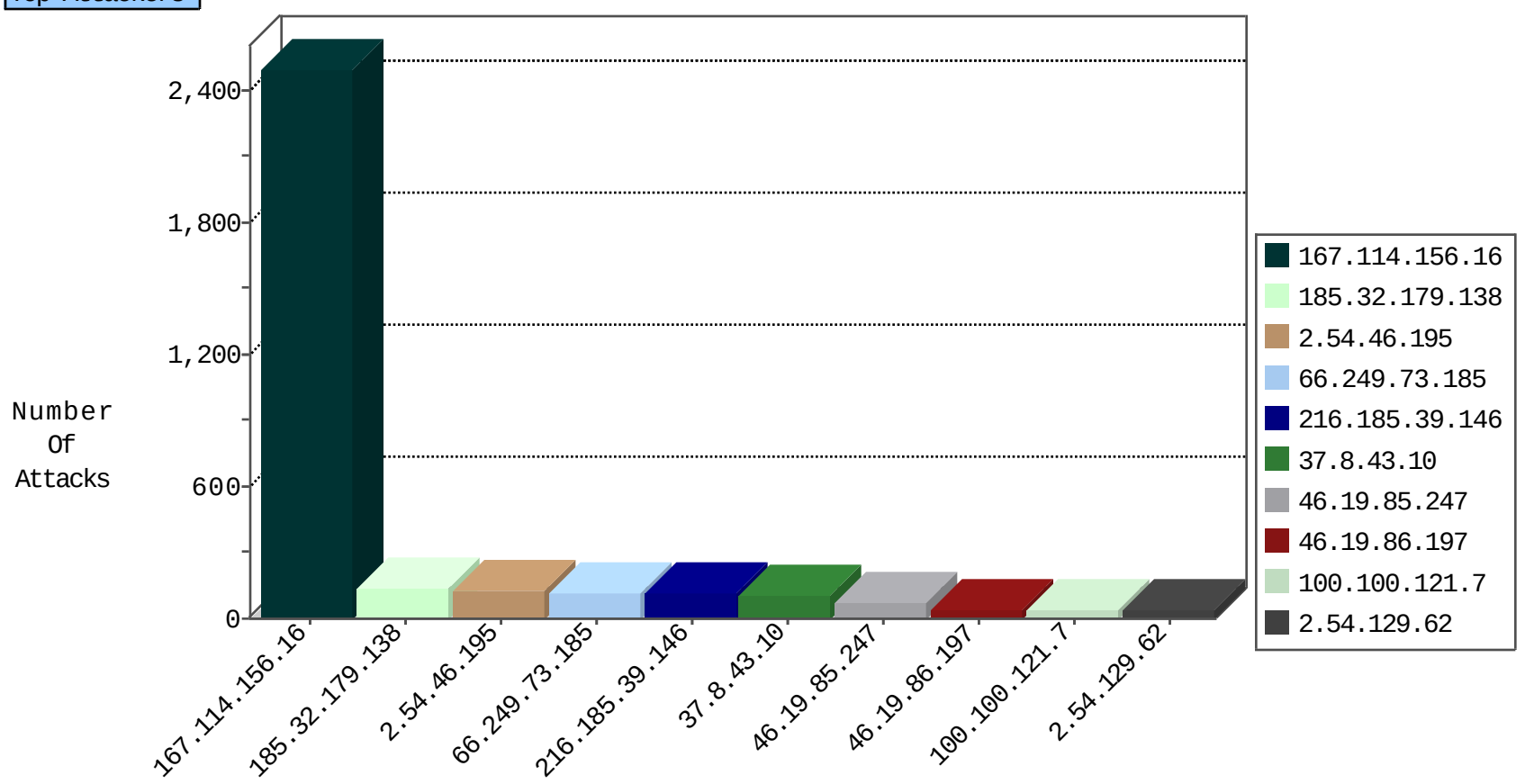
11-25-2015-17:04:07 to 11-25-2015-18:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-25-2015-17:04:07 to 11-25-2015-18:04:07

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	3413
66.249.66.40	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	282
82.145.209.136	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	11
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	11
212.179.64.162	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
149.78.2.63	Israel	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	3
5.22.134.109	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
93.174.93.151	Netherlands	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
178.217.186.86	Poland	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
101.36.72.249	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1

11-25-2015-17:04:07 to 11-25-2015-18:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.187	Israel	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	2
37.8.43.10	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

11-25-2015-17:04:07 to 11-25-2015-18:04:07

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
37.8.43.10	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SERVER-WEBAPP admin.php access	4
37.8.43.10	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SERVER-WEBAPP login.htm access	3
46.151.55.35	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
213.57.197.155	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.120.75.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.80.155.223	147.237.77.170	United States	maarachot.idf.il	Tehila - Perl LWP with fake user agent	1
188.120.148.140	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.6.71.154	147.237.77.227	Poland	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
119.73.228.130	147.237.8.27	Singapore	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
87.69.231.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.170.142	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.151.55.35	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
213.55.105.93	147.237.77.216	Ethiopia	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.76.147	Cote D'Ivoire	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
37.8.43.10	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SERVER-WEBAPP adminlogin access	1
192.115.83.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.92.219	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.149.219	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.56.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.68	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.246.137.208	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-25-2015-17:04:07 to 11-25-2015-18:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	114
216.185.39.146	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	110
46.19.86.197	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	43
100.100.121.7		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	38
46.19.86.65	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
12.181.197.100	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
213.55.105.118	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
100.100.31.73		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
100.100.44.241		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.85.247	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
46.19.85.247	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
100.100.87.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
100.100.41.51		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
46.19.85.247	Israel	147.237.76.30	himush.idf.il	SYN Attack		reject	16
2.54.129.62	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
100.100.41.51		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
100.100.110.77		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
100.100.76.149		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
79.182.202.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
100.100.65.16		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.73.201	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.182.202.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.2.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.65.37.227	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
46.19.86.193	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
79.176.183.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
100.100.87.76		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
77.126.32.69	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.247	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.129.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.129.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
157.55.39.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
100.100.81.83		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.54.42.65	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
100.100.70.92		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.98	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
109.65.55.56	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
100.100.111.40		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.52.54.29	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.52.56.68	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.54.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.64.75	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.56.68	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.189.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.250.217.197	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6

11-25-2015-17:04:07 to 11-25-2015-18:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
2.54.46.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
185.32.179.138	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.179.138	Block	64
2.54.46.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
37.8.43.10	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.8.43.10	Block	40
37.8.43.10	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 37.8.43.10	Block	38
46.19.85.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
109.66.128.206	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.66.128.206	Block	26
109.64.16.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
176.13.14.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
37.8.43.10	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	PHP Attempt	Block	14
85.65.60.30	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.60.30	Block	8
2.54.26.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.122	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.19.85.122	None	5
149.78.139.230	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
109.67.206.200	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/ufi/reaction/	Block	4
192.118.11.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.229.55.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.111.198.55	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
2.54.162.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.141.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.169.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.142.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.228.142.29	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
5.22.129.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
2.54.2.139	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.10.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.128.206	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
79.179.56.165	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
176.13.20.193	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
85.65.60.30	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
207.46.13.49	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.49	Block	2
109.66.128.206	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
80.246.137.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.250.68.120	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
79.176.15.158	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$btnSend.x in www.refua.atal.idf.il/926-he/refuah.aspx	Block	2
46.19.85.61	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
5.29.178.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
84.229.27.239	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
212.143.169.119	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.143	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1361-10624-he/dover.aspx	Block	1
46.19.85.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.166.22.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
37.142.96.137	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1

11-25-2015-17:04:07 to 11-25-2015-18:04:07