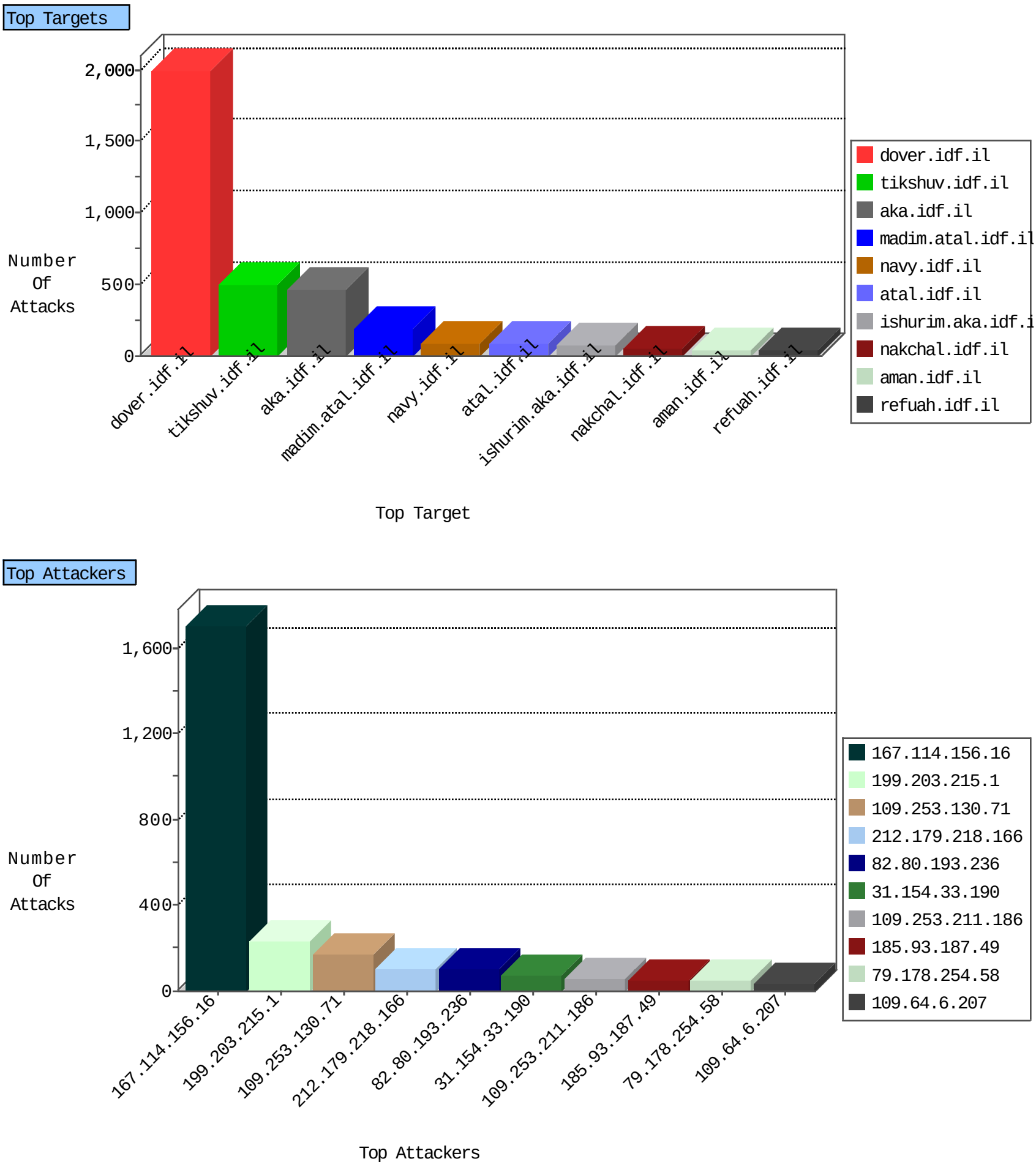
01-11-2016-15:04:05 to 01-11-2016-16:04:05

IDF Under Attack Daily Report



01-11-2016-15:04:05 to 01-11-2016-16:04:05

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	3045
177.142.176.143	Brazil	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
177.142.176.143	Brazil	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
163.44.149.213	Japan	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
208.67.1.158	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

01-11-2016-15:04:05 to 01-11-2016-16:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.144.59.103	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-11-2016-15:04:05 to 01-11-2016-16:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
149.78.229.88	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.129.69	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	1
85.130.179.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.49.16	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.151.53.196	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
36.72.228.72	147.237.77.216	Indonesia	dover.idf.il	ET SCAN NMAP -sS window 1024	1
185.27.105.147	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.129.69	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	1
94.102.48.195	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.138.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.62	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
46.120.78.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.218.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-11-2016-15:04:05 to 01-11-2016-16:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.154.33.190	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	71
109.64.6.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
212.179.218.166	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
212.179.218.166	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	27
46.19.86.30	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.23	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	24
212.179.218.166	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	22
79.178.254.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
79.178.254.58	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
46.120.78.235	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
37.26.146.254	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.221	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
2.52.130.247	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
213.244.88.90	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
2.54.139.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
121.54.32.165	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
121.210.9.93	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
192.117.173.158	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
212.179.218.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.179.218.166	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.121	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
197.252.1.150	Sudan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.121	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
31.168.147.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.166.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.118	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.50.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.254.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.120.78.235	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.130.247	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.147.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.235.55.70	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
37.26.149.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
94.230.85.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.179.218.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.52.130.247	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.110	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
197.252.1.150	Sudan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.49.145	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.235.55.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.104	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
94.230.86.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.242.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.253.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.130.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.104	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.203.215.1	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	226
109.253.130.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
82.80.193.236	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	98
109.253.130.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	58
109.253.211.186	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
84.111.1.236	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
79.182.6.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
176.13.0.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.111.233.17	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.111.233.17	Block	4
46.19.85.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.93.187.49		147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 185.93.187.49	Block	3
185.93.187.49		147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 185.93.187.49	Block	3
185.93.187.49		147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 185.93.187.49	Block	3
185.93.187.49		147.237.0.15	kosher-kravi.idf.i	PHP Attempt	Block	2
84.228.199.27	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.228.199.27	Block	2
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	2
185.93.187.49		147.237.77.170	maarachot.idf.il	Multiple Admin Blocking from 185.93.187.49	Block	2
185.93.187.49		147.237.0.34	tikshuv.idf.il	Multiple Admin Blocking from 185.93.187.49	Block	2
185.93.187.49		147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 185.93.187.49	Block	2
185.93.187.49		147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.93.187.49	Block	2
185.93.187.49		147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 185.93.187.49	Block	2
185.93.187.49		147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.93.187.49	Block	2
2.54.187.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.93.187.49		147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 185.93.187.49	Block	2
62.90.210.199	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1119-he/nakhal.aspx	Block	2
212.235.77.150	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homas	Block	2
185.93.187.49		147.237.77.233	atal.idf.il	PHP Attempt	Block	2
185.93.187.49		147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 185.93.187.49	Block	2
185.93.187.49		147.237.72.166	aka.idf.il	PHP Attempt	Block	2
46.117.21.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
185.93.187.49		147.237.0.15	kosher-kravi.idf.i	Multiple Admin Blocking from 185.93.187.49	Block	2
185.93.187.49		147.237.77.170	maarachot.idf.il	PHP Attempt	Block	2
82.166.58.100	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 82.166.58.100	Block	2
185.93.187.49		147.237.76.31	nakchal.idf.il	PHP Attempt	Block	2
185.93.187.49		147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	2
185.93.187.49		147.237.76.86	navy.idf.il	PHP Attempt	Block	2
77.75.76.163	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/30/	Block	1
184.105.139.68	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
85.65.50.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.114.105.254	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.93.187.49		147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp-login.php	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/main/stm	Block	1
141.212.122.81	United States	147.237.0.19	madim.atal.idf.il	Distributed Malformed URL	Block	1
2.54.171.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.111.28.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.137.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.93.187.49		147.237.76.31	nakchal.idf.il	Admin Blocking	Block	1
46.117.21.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.226.21.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.199.57.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1

01-11-2016-15:04:05 to 01-11-2016-16:04:05