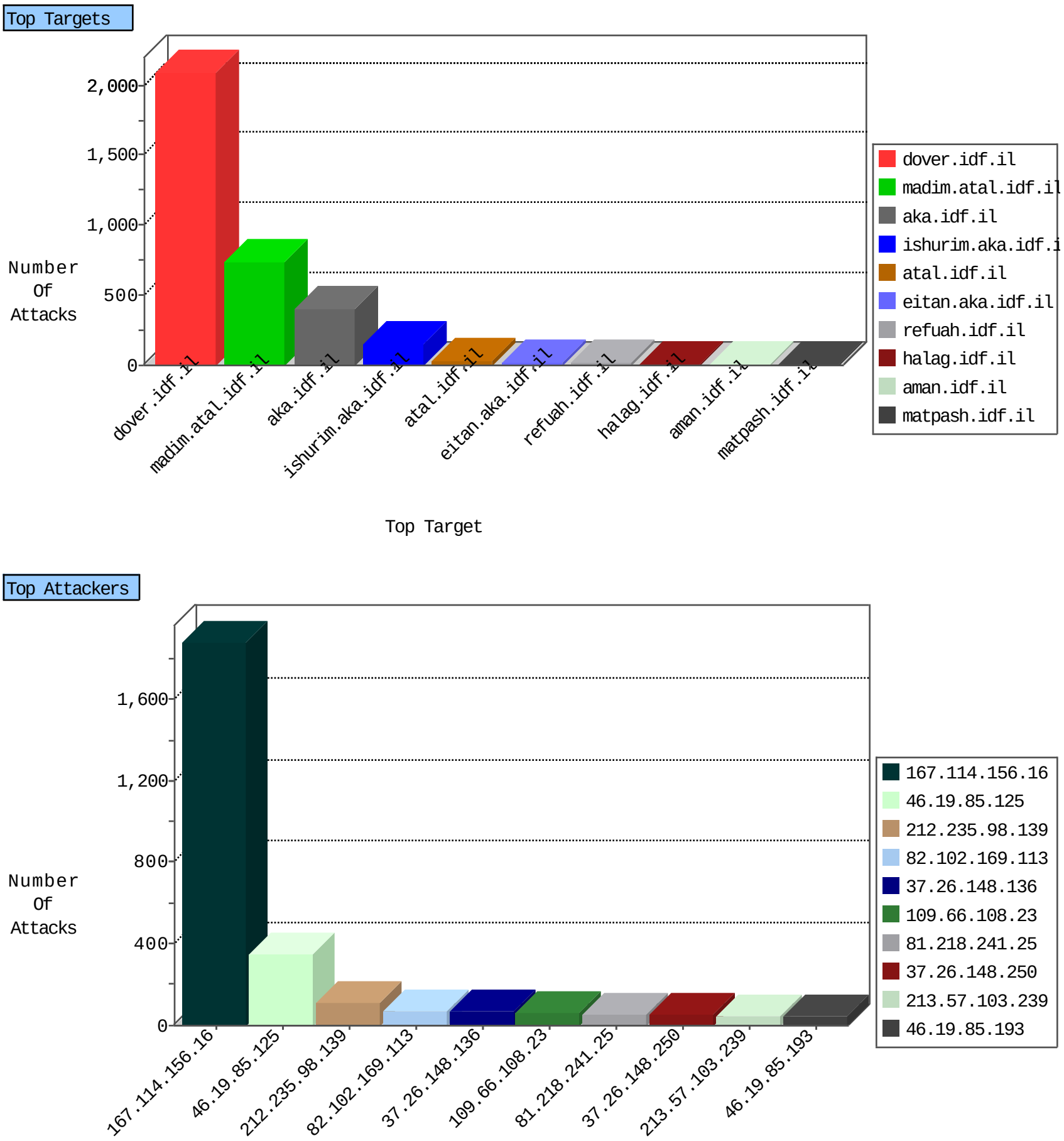
12-06-2015-08:04:04 to 12-06-2015-09:04:04

IDF Under Attack Daily Report



12-06-2015-08:04:04 to 12-06-2015-09:04:04

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	3412
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	285
190.43.170.200	Peru	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.2	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

12-06-2015-08:04:04 to 12-06-2015-09:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.25.148.67	Germany	147.237.77.176	matpash.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

12-06-2015-08:04:04 to 12-06-2015-09:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.126.116.147	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.176.124	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
77.125.13.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
174.114.17.137	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
119.73.228.130	147.237.76.31	Singapore	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.85.200	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
119.73.228.130	147.237.76.31	Singapore	nakchal.idf.il	ET SCAN NMAP -f -sS	1
98.119.105.221	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
93.174.89.82	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
217.194.193.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.174.89.82	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
209.236.124.188	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
82.166.240.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
203.197.205.118	147.237.77.170	India	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
82.80.173.50	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.90.128.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.201	China	e.atal.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
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
119.73.228.130	147.237.76.31	Singapore	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
31.168.13.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.219.238.10	147.237.76.38		e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
93.174.89.82	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.204.14	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-06-2015-08:04:04 to 12-06-2015-09:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	110
213.57.103.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
46.19.86.78	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	36
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	24
37.26.149.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.74	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
84.228.86.180	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
192.116.105.90	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
213.57.130.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
213.57.130.251	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	13
213.57.130.251	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
5.47.80.117	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
199.30.25.15	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.86.245	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.22.6	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
5.47.80.117	Turkey	147.237.77.216	dover.idf.il	SYN Attack		reject	7
5.47.80.117	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.86.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.1.134	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.200.163	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
176.13.22.6	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.136.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.132.70	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
62.219.139.237	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	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.248.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.116.232.175	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.245	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.94.205.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.19.85.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
50.174.107.222	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.67.160.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.36.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.152.51	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	3
207.232.35.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.97.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.74	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.188	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
79.182.145.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-06-2015-08:04:04 to 12-06-2015-09:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.125	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.125	Block	191
46.19.85.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	108
37.26.148.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
109.66.108.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
37.26.148.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
46.19.85.125	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.85.125	Block	50
46.19.85.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
176.12.145.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
46.19.85.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
46.19.85.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
2.52.157.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
37.26.147.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.13.19.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
93.173.18.226	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
37.26.147.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.75.76.169	Czech Republic	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.75.76.169	Block	3
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	2
37.26.147.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
192.116.105.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.12.142.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
210.187.200.215	Malaysia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
80.246.140.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	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
210.187.200.215	Malaysia	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 210.187.200.215	Block	2
46.166.190.167	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
210.187.200.215	Malaysia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
81.218.165.246	Israel	147.237.72.166	aka.idf.il	Extremely Long Parameter in www.aka.idf.il b16DXmdedOiDXmdepINec15TXlteZ158g16LXqNeaINeR16nXk9eUICfXqi7XkydkZAIZDw8WAh8EBXvXm9eq15XXkdeqINeU15D	Block	1
197.36.49.84	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
37.26.147.154	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.148.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.202.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.199.244.112	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/110291.pdf	Block	1
2.54.17.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.181.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
208.98.226.97	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
84.94.205.140	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 84.94.205.140	Block	1
80.246.138.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.3.144.160	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
77.75.76.169	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/28/	Block	1
5.29.40.9	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
176.12.141.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.132.70	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1275-he/atal.aspx	Block	1
66.249.66.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
210.187.200.215	Malaysia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 210.187.200.215	Block	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/size220x0/11591.jpg	Block	1
81.218.165.246	Israel	147.237.72.166	aka.idf.il	Unknown Parameter b16DXmdedOiDXmdepINec15TXlteZ158g16LXqNeaINeR16nXk9eUICfXqi7XkydkZAIZDw8WAh8EBXvXm9eq15XXkdeqINeU15DXqteoINeR15Ug157XkNeV15fXodeg15nXnSDXlNeX15XXnteo15nXnSDXlNee16HXldeb16DXmdedOiDXmdepINec15TXlteZ158g16LXqNeaINeR16nXk9eUICfXmdep15XXkSDXqi7XkydkZAIbDw8WAh8EBX/Xm9eq15XXkdeqINeU15DXqteoINeR15Ug157XkNeV15fXodeg15nXnSDXlNeX15XXnteo15nXnSDXlNee16HXldeb16DXmdedOiDXmdepINec15HXl9eV16gg16LXqNeaINeX15XXp9eZINeR16nXk9eUICfXmdep15XXkScuZGQCHQ8PFgQfAgUHXGR7NSw3fR8EBY0B15vXqteV15HXqiDXlNeQ16rXqCDXkdeVI	None	1
46.19.85.125	Israel	147.237.0.19	madim.atal.idf.i	Too Many 403: Response Code per Session	Block	1
79.180.3.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

12-06-2015-08:04:04 to 12-06-2015-09:04:04