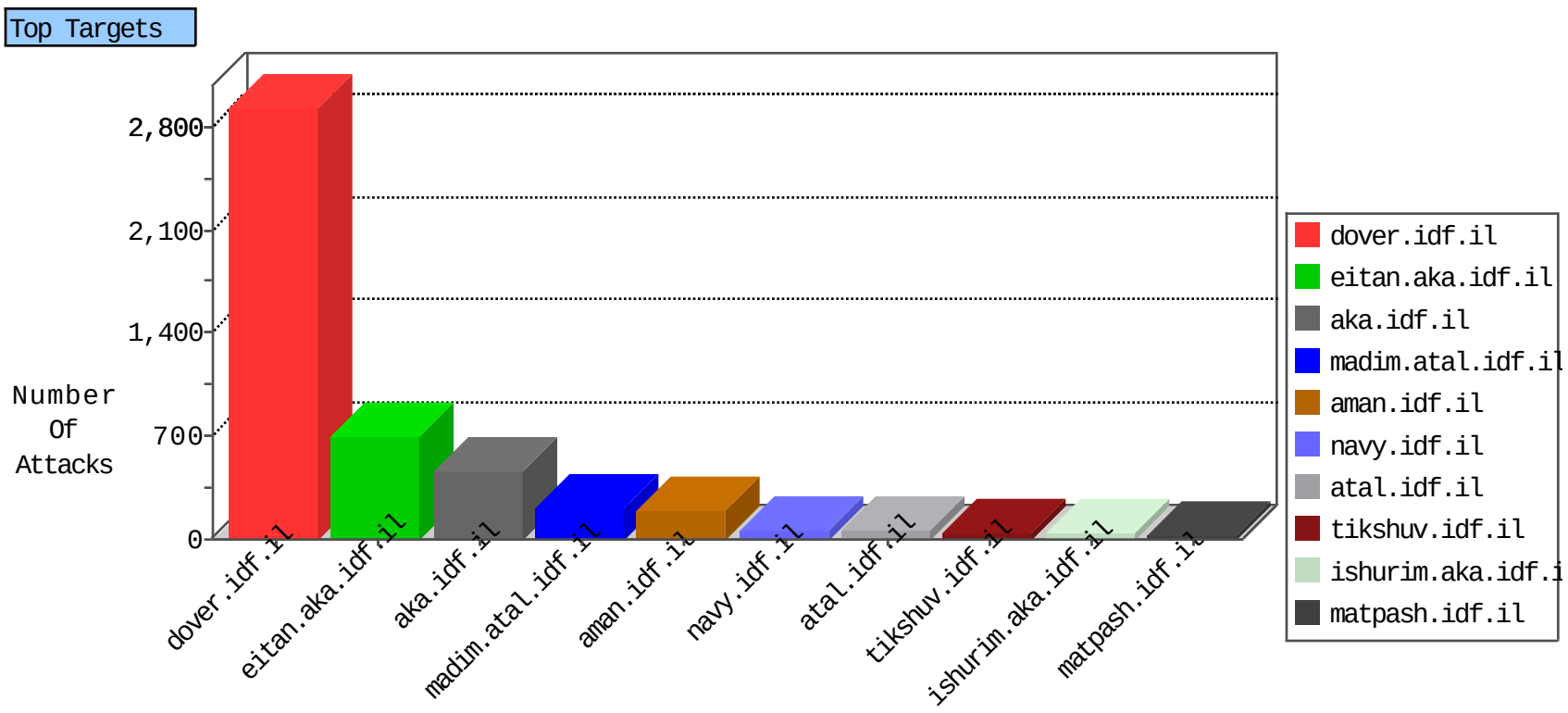
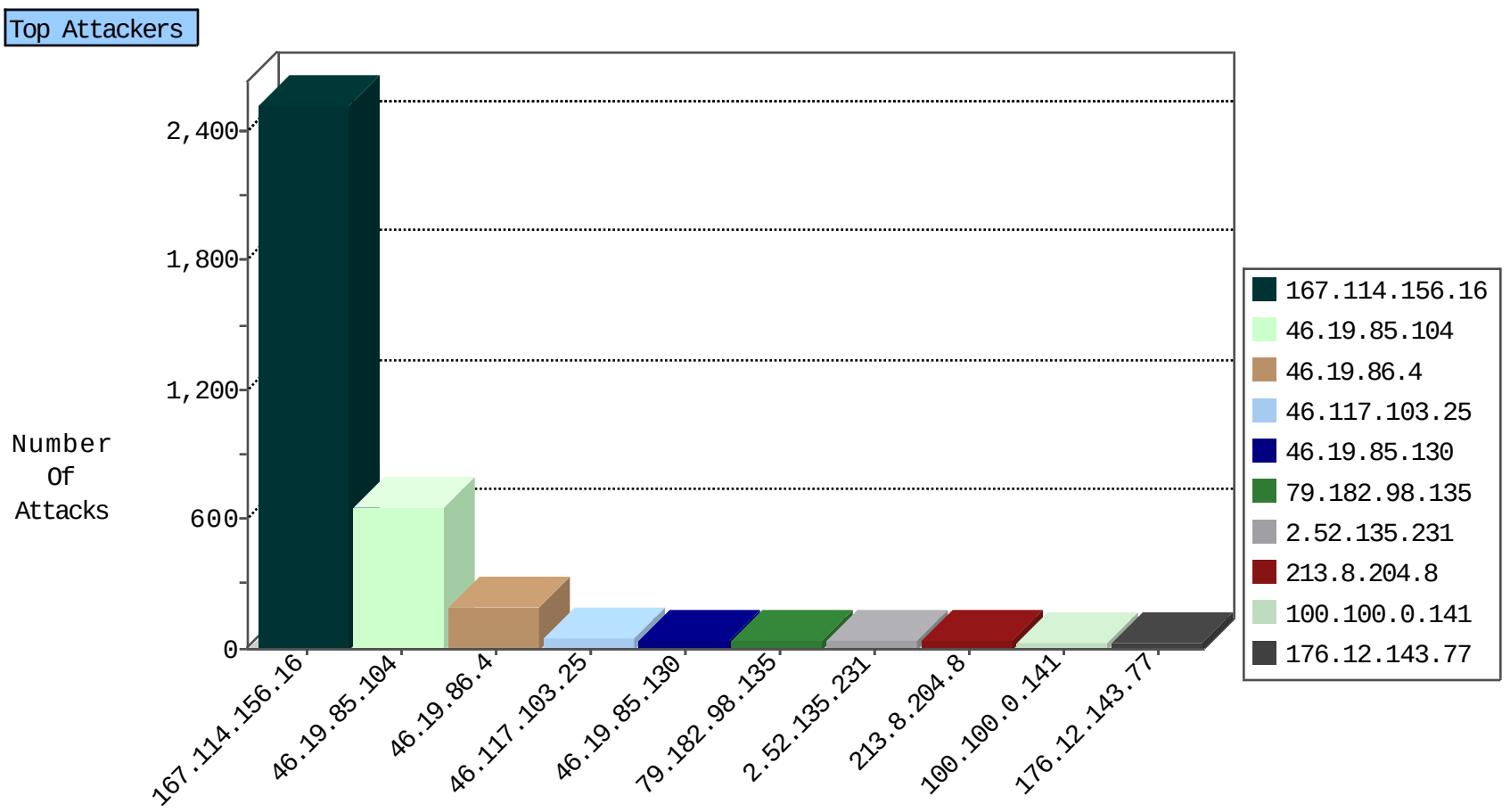
12-01-2015-20:04:00 to 12-01-2015-21:04:00

IDF Under Attack
Daily Report





12-01-2015-20:04:00 to 12-01-2015-21:04:00

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	3426
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	11
37.26.148.208	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
84.109.130.231	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
112.198.79.54	Philippines	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
146.185.239.100	Russian Federation	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1

12-01-2015-20:04:00 to 12-01-2015-21:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
195.154.188.28	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.188.224	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.211.20	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

12-01-2015-20:04:00 to 12-01-2015-21:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.28	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
195.154.211.20	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	2
195.154.211.20	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
195.154.188.28	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
31.6.71.154	147.237.77.216	Poland	dover.idf.il	ET SCAN NMAP -sS window 1024	2
195.154.211.20	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	2
195.154.211.20	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS) .asp Filename Extension Parsing File Upload Security Bypass Attempt (asp)	2
195.154.188.28	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP phptest.php access	2
195.154.188.28	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	2
209.126.116.147	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.13.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
51.254.46.129	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.76.176	United States	test.ncore.idf.il	ET DROP Dshield Block Listed Source	1
159.147.148.28	147.237.76.196	Spain	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.125.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
131.109.15.2	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
2.54.18.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.212.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.154.188.224	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	1
85.65.71.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.154.188.224	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS) .asp Filename Extension Parsing File Upload Security Bypass Attempt (asp)	1
84.229.38.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.154.188.188	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	1
79.177.214.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.154.188.28	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	1
71.177.22.76	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 3072	1
209.126.116.147	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
66.66.18.81	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
207.219.231.226	147.237.76.198	Canada	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
176.13.3.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.154.211.20	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP phptest.php access	1
131.109.15.2	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
128.199.255.85	147.237.77.74	Singapore	law.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
109.67.25.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.154.188.224	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	1
85.64.88.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.154.188.188	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP phptest.php access	1
79.180.182.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.50.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.1.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-01-2015-20:04:00 to 12-01-2015-21:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.104	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	567
46.19.85.130	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	42
79.182.98.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
213.8.204.8	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
100.100.0.141		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
100.100.111.80		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
2.52.135.231	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
188.139.253.108	Syrian Arab Republic	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
100.100.120.6		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
206.190.141.92	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
176.12.143.77	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
176.13.3.105	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	16
176.12.143.77	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
100.100.105.73		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.54.151.62	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
66.249.75.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.102.254.128	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.160.244.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.174.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
213.57.137.3	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.66	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
113.161.87.116	Vietnam	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
185.3.146.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.19.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.14.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
94.230.86.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.206.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.229.82.224	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.176.105.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.177.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.180.217.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
173.252.89.52	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
84.229.82.224	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.176.203.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
173.252.89.57	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.225	Israel	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6

12-01-2015-20:04:00 to 12-01-2015-21:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	114
46.19.85.104	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	84
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.4	Block	79
46.117.103.25	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
2.54.151.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.86.4	Block	4
79.180.177.18	Israel	147.237.0.16	my-kosher-kravi.idf.il	Parameter Type Violation Master$ContentPlaceHolder1$password in my-kosher-kravi.idf.il/templates/login/login.aspx	Block	3
79.182.53.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
103.11.55.116	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
46.200.25.194	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	3
103.11.55.116	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
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
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.117.83.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.182.111.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.94.92.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
77.237.154.221	Czech Republic	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /	Block	1
207.232.28.184	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 207.232.28.184	Block	1
46.19.85.161	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method abe.1425463069.3.1442566652.1442566652. in URL	Block	1
37.26.146.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.69.229.180	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20752-he/idfgdover.aspx	Block	1
176.240.79.29	Turkey	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
5.22.131.114	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
84.108.32.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
59.152.106.34	Bangladesh	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
149.78.163.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.123	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
109.65.155.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
103.11.55.116	Australia	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.66.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf/console/search_resources.aspx	Block	1
176.12.138.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.102.206.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.111.180.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.8.199	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.183.13.219	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
46.121.91.29	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
123.152.143.110	China	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
79.176.1.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
37.26.147.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.69.229.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.22.131.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.108.118.76	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
59.152.106.34	Bangladesh	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
149.88.2.146	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1

12-01-2015-20:04:00 to 12-01-2015-21:04:00