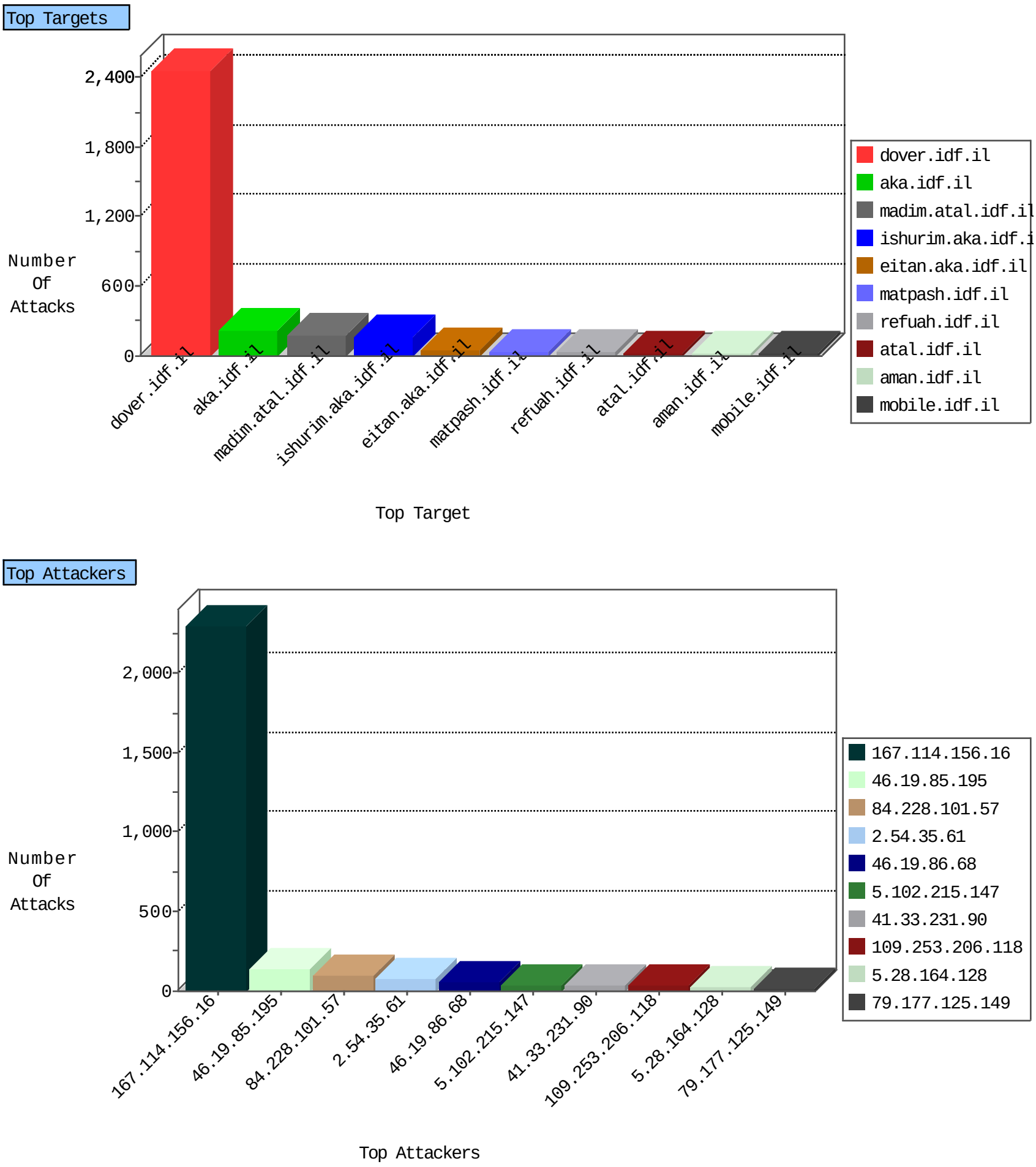
12-19-2015-16:04:07 to 12-19-2015-17:04:07

IDF Under Attack
Daily Report



12-19-2015-16:04:07 to 12-19-2015-17:04:07

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	3259
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	964
46.19.85.195	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	475
38.229.1.13	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
208.67.1.66	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

12-19-2015-16:04:07 to 12-19-2015-17:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

12-19-2015-16:04:07 to 12-19-2015-17:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.28.164.128	147.237.72.167	Israel	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	24
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
77.127.254.243	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.55	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
79.178.189.96	147.237.76.147	Israel	chinuch.aka.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
5.39.222.253	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.91	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.91	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.38	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
173.193.252.211	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
90.189.151.244	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.39.222.253	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.91	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.91	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
173.193.252.211	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

12-19-2015-16:04:07 to 12-19-2015-17:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.68	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	58
84.228.101.57	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
2.54.35.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	30
207.244.77.4	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	20
2.54.35.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	15
2.54.35.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
2.54.35.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
84.228.101.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
46.120.137.220	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
79.177.125.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
37.26.148.164	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.57.128.92	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
213.57.128.92	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
207.244.82.187	United States	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
2.54.12.112	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.136.108	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.102.215.147	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.131.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.64.133	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
94.230.86.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.56	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
213.244.118.251	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
166.171.184.128	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.181.107.130	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
77.125.100.61	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
5.102.254.15	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.56	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
213.244.119.251	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.127.221.64	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
149.88.202.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.136.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.12.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
77.127.253.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.15.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.68.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.180.48.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.125.149	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
109.66.132.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.93.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.204.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.52.163.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.68.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.67.145.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.254	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-19-2015-16:04:07 to 12-19-2015-17:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
109.253.206.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
5.102.215.147	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 5.102.215.147	Block	33
176.13.9.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
94.159.139.143	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
5.29.89.93	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
2.54.175.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.183.132.201	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.228.101.57	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Abnormally Long Request	Block	2
84.228.101.57	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Illegal HTTP Version	Block	2
37.142.68.36	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
37.142.68.36	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	2
84.228.101.57	Israel	147.237.72.167	ishurim.aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
46.120.212.219	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.186.39.220	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyus	Block	1
80.246.136.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.93.91.84	Germany	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/404.aspx	Block	1
84.228.101.57	Israel	147.237.72.167	ishurim.aka.idf.il	NULL Character in Header Name at Ã”Ã?9Ã±[[#26]]w`Â–Ãº[6[[#0]](•gÂ¹EÂ†Ã¨Ã€Ã›Â®Â¹HÃµÂ™q,Â-3Âµ[[#4]]Ã¢[[#8]]Ã•Â²Â»[[#19]]9Â?3Â¦fÂ,Ã«Â™FÂŽnÃˆ[[#29]]Ãœ[[#19]]Ã…Ã”Â¼q[[#3]];Ã½Â‘5JwÃ¯Ãž[[#24]]YÃ¯ÃœÃª	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
213.57.157.172	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
149.78.62.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.101.57	Israel	147.237.72.167	ishurim.aka.idf.il	Illegal Parameter Encoding kÃœ.,× â€?×“[[#4]]ÃŠ×••Ã¹[[#14]]Â±eÖ°YÖ·Ö»ER×™Wâ€?×³×€[[#19]][[#12]]×¥fÂŸ^"Â±Ã»$bnâ€¡[[#15]]ÕµE×‘â€¦×šÃžT×¦×±Â¢Â?~ ÃœË†[[#0]]W0â,¬â,¬qmz×¦~[[#11]]$Ö¾Zq/Â¸Â³Â«r×§[[#11]]"×—Ö¿Â¼Â ×ª[[#26]]×¡t×™*ÃšÃ?AÂžÂ¼Â§Ã?Â»×?p2×–×¡×¥04b	None	1
46.19.86.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.228.101.57	Israel	147.237.72.167	ishurim.aka.idf.il	Abnormally Long Header Line request header name	Block	1
40.77.167.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16775-en/dover.aspx-title=chief	Block	1
84.228.101.57	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many Headers per Request - 28 Headers	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/tfasim.aspx	Block	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
2.54.33.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.101.57	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Method from 84.228.101.57	Block	1
84.228.101.57	Israel	147.237.72.167	ishurim.aka.idf.il	Illegal Byte Code Character in Method [[#25]][[#5]]Ã¹ÃœÂ¸Â±!aTÃ¦Â³ÃŸÂ¼Ã^Â‘gÂšG[[#28]][[#22]]ÃœÃµ[[#6]]ÂŒSÃ¼FÃ‘Ã¾ÃŠÂ¬Âœp9mÂµÂ®Â¾Â²A[UÂ?	Block	1
46.121.67.215	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/gyus	Block	1
109.201.154.213	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
85.250.158.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.94.207.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.175.13.138	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
84.228.101.57	Israel	147.237.72.167	ishurim.aka.idf.il	NULL Character in Method Â‰[[#15]]Ij[[#2]]Â®Ã‡vÃ…s^[[#0]]EÂ¥.;)Â®	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-12522-he/dover.aspx	Block	1
157.55.39.214	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.228.101.57	Israel	147.237.72.167	ishurim.aka.idf.il	Illegal URL Path Encoding xÂ?Âž×´>[[#20]]1â€”{Â?â€ž×¤ÂŸnÂ¦eâ,¬Ã¼Â½nÖ¸â€°×?â€ ×ªÖ³45×—×•Ö¼&1Â¢Â©â€°[[#22]]sÂ?[[#7]]Ö½pnâ€¦>/â€”!×¢â€žlÖ¶×”"×²ÂŒ!â€˜xi×—%[[#4]]nk;Â»Ö¹y17[[#14]]Â·×³Â³p×¨â€œzÃ¼[[#28]]r%Â¼ÃŸr×¥×ªÃŸÂ½dr×”Â?6Â¡-gâ€¡ÃšÂ®[[#8]][[#16]]xâ€˜â€š]inÃœâ€?k\l[[#11]]fjÂž×³q	Block	1
46.19.86.169	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
79.183.165.249	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
46.19.85.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-19-2015-16:04:07 to 12-19-2015-17:04:07