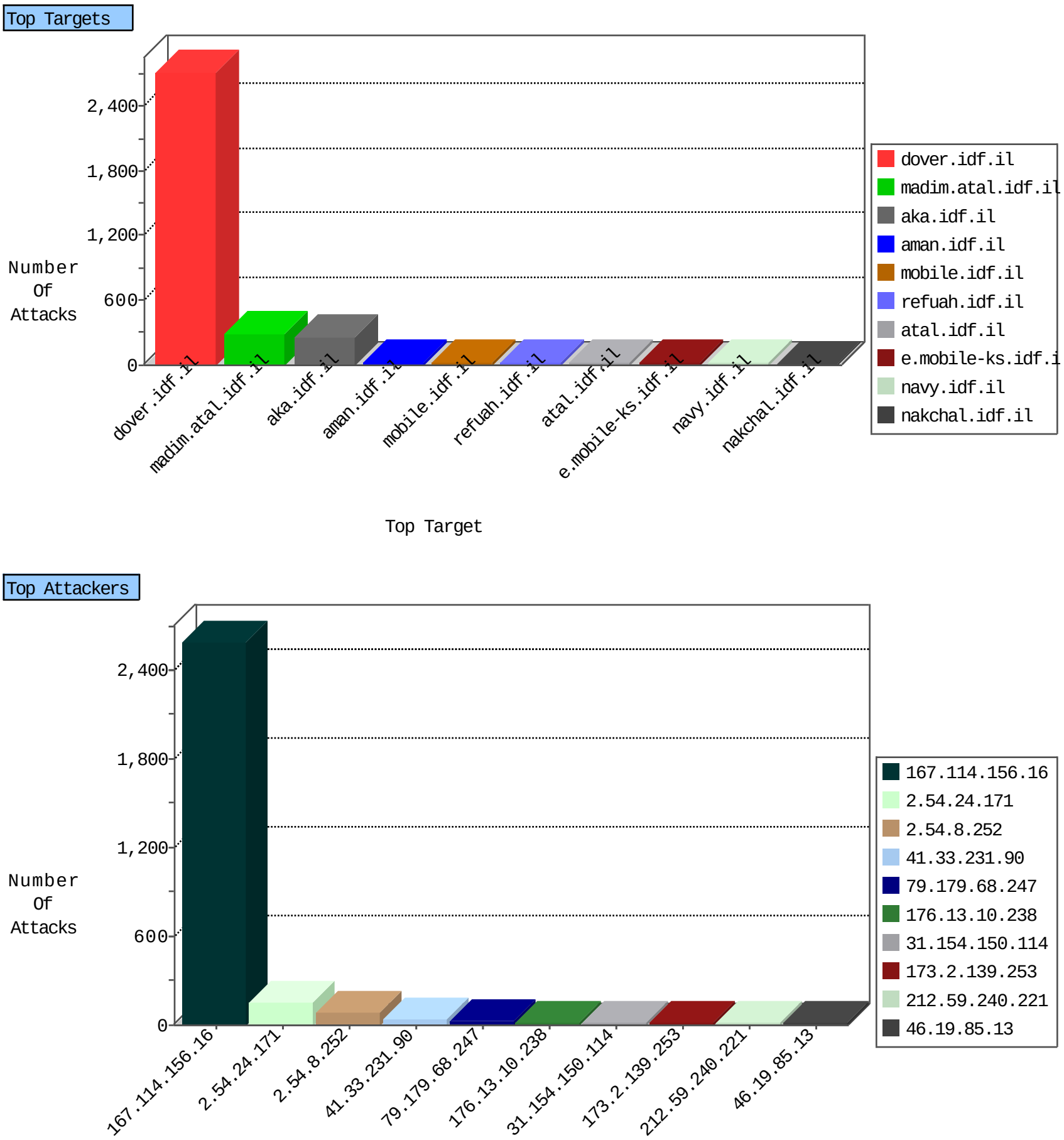
12-12-2015-20:04:03 to 12-12-2015-21:04:03

IDF Under Attack Daily Report



12-12-2015-20:04:03 to 12-12-2015-21:04:03

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	3357
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	304
146.185.57.7	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
52.53.222.9	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1

12-12-2015-20:04:03 to 12-12-2015-21:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
58.248.103.2	China	147.237.77.170	maarachot.idf.il	13764: HTTP: China Chopper Malware Communication Attempt	Block	2

12-12-2015-20:04:03 to 12-12-2015-21:04:03

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
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.186	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
79.179.126.29	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
218.108.132.58	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.108.132.58	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
50.252.197.194	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 4096	1
199.191.56.188	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
5.39.222.253	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
113.164.7.249	147.237.8.50	Vietnam	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
113.164.7.249	147.237.8.28	Vietnam	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
113.164.7.249	147.237.8.14	Vietnam	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
94.102.60.89	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
218.108.132.58	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.51.147.34	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
199.191.56.188	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
50.252.197.194	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
199.191.56.188	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -f -sS	1
5.39.222.253	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
124.107.167.132	147.237.76.30	Philippines	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.164.7.249	147.237.8.45	Vietnam	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
113.164.7.249	147.237.8.24	Vietnam	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
113.106.129.219	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1

12-12-2015-20:04:03 to 12-12-2015-21:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
176.13.10.238	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
212.59.240.221	Poland	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	18
5.28.165.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.127.61.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
173.2.139.253	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
173.2.139.253	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	8
2.54.8.252	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
31.154.152.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.120	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
31.154.152.224	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
213.57.128.138	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.120.125.6		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.110.111.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.150.114	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.225.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.208	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
40.77.167.89	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.166.253	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
87.68.61.78	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
207.46.13.48	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	4
31.154.150.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
5.102.254.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.13	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.65.18.148	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.15	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
46.120.36.83	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.22.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.148.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.27.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.32.179.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.150.114	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
79.183.35.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.182.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.147	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.176.168.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.178	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
77.127.221.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.173.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.68.81.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.178	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
185.120.126.115		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.206.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-12-2015-20:04:03 to 12-12-2015-21:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.24.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
2.54.8.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
2.54.24.171	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.24.171	Block	65
46.19.86.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
84.109.152.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
77.126.61.86	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.126.61.86	Block	5
2.54.24.171	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.24.171	Block	5
109.67.69.34	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/1088-he/meretz.aspx	Block	4
46.19.85.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.10.238	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
213.57.34.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.138.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.46.39.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.186.95.68	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
79.176.214.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.94.96	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.94.96	Block	2
79.179.68.247	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.179.68.247	Block	2
79.179.112.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
109.65.108.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.179.68.247	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 79.179.68.247	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
79.179.68.247	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
79.179.68.247	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 79.179.68.247	Block	2
213.57.211.70	Israel	147.237.0.17	m.my-kosher-kravi .idf.il	Distributed Illegal Parameter Encoding	None	2
79.179.68.247	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 79.179.68.247	Block	2
79.179.68.247	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 79.179.68.247	Block	2
89.139.51.39	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	2
58.248.103.2	China	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	2
79.179.68.247	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 79.179.68.247	Block	2
79.179.68.247	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 79.179.68.247	Block	2
79.179.68.247	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 79.179.68.247	Block	2
58.248.103.2	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 58.248.103.2	Block	2
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
79.179.68.247	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at +Â–[[#25]]ÂŽhJHÂ–nÂ'[[#1]]ÃŽÃž [[#0]]Â„Â¯Â›qÃ³Â-^ÂƒÂœÂ„Ã¿• Ã£{4Ã€yÂ„Â'	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19027-he/dover.aspx	Block	1
167.114.229.248	Canada	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	1
5.29.179.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.68.247	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8823-he/refuah.aspx	Block	1
79.179.68.247	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 79.179.68.247	Block	1
79.179.68.247	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
45.35.71.181		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
87.69.219.76	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
2.54.132.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.94.161.14	Israel	147.237.0.17	m.my-kosher-kravi .idf.il	Double URL Encoding - parameter: ReturnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	1
79.177.3.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
188.143.232.13	Russian Federation	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 188.143.232.13	Block	1
79.179.68.247	Israel	147.237.72.166	aka.idf.il	NULL Character in Method b4Ã„EÃ—:PÂ´Ã¬$sOÂ™Â•ZlÃ?VÃƒ [[#21]]6Ã…Ã•Â¹w@Ã…[[#5]]2EÃ?[[#0]]pÂ§Ã±vÂ·^W[[#23]];Ã´Â°Â˜ Ã«A![[#4]]([[#3]]\<bÂžÃ˜Ã¡Â·[[#1]]Ã?@Ã·Ã¤Â©Â•Â'u.jÂšÃ– #Ã±Â?Ã»Go{.Ã¯Â«Â¬aÂ,ÂŸÃ˜lÂ”/GÂªÃ´[[#30]]AÃ–[[#8]]Ã©9'8Â¥GÂ” *[[#19]]Â±Ã‡Ã…Ã£•Â“y$Â½[[#31]]/-•Â®Â°g[[#5]]Ã¾Ã›Â¥	Block	1
66.249.66.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1

12-12-2015-20:04:03 to 12-12-2015-21:04:03