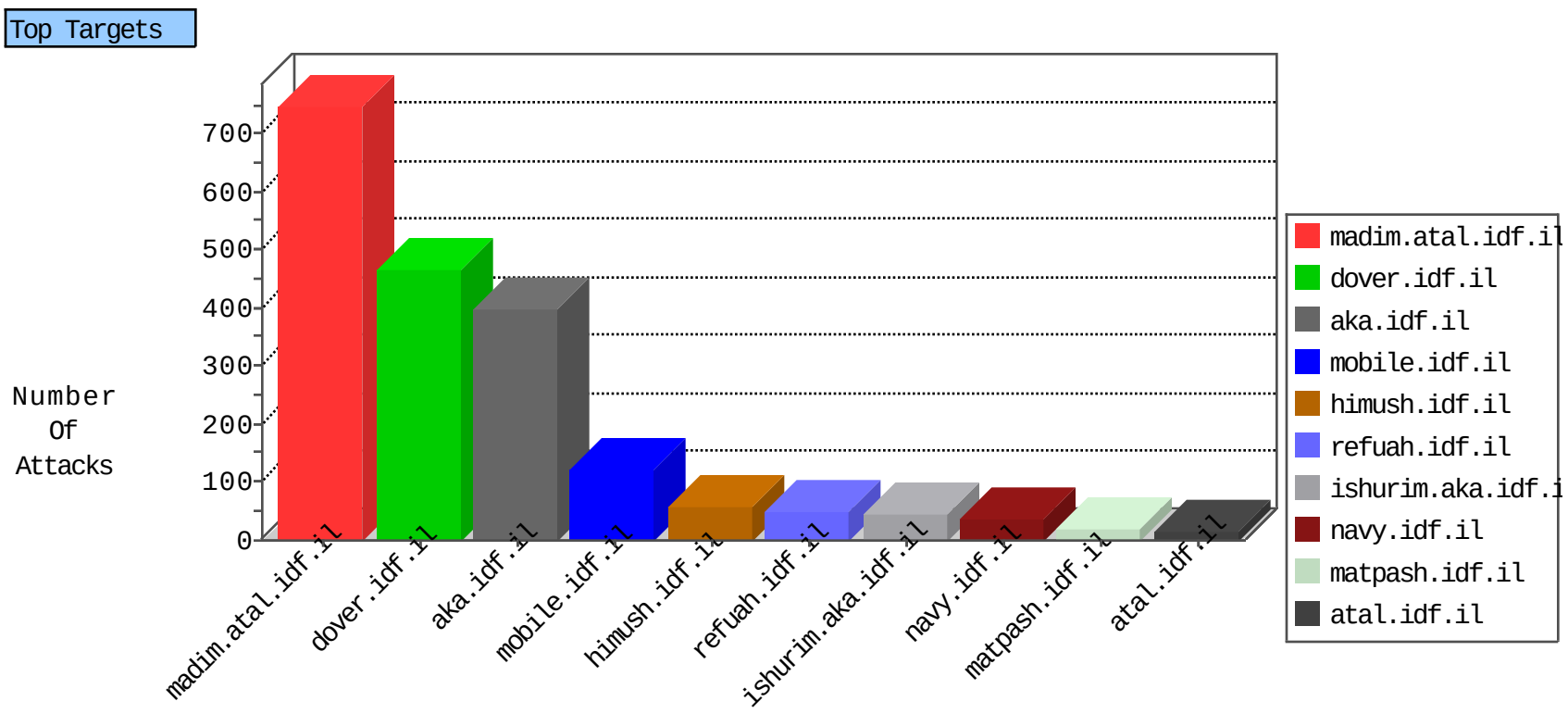
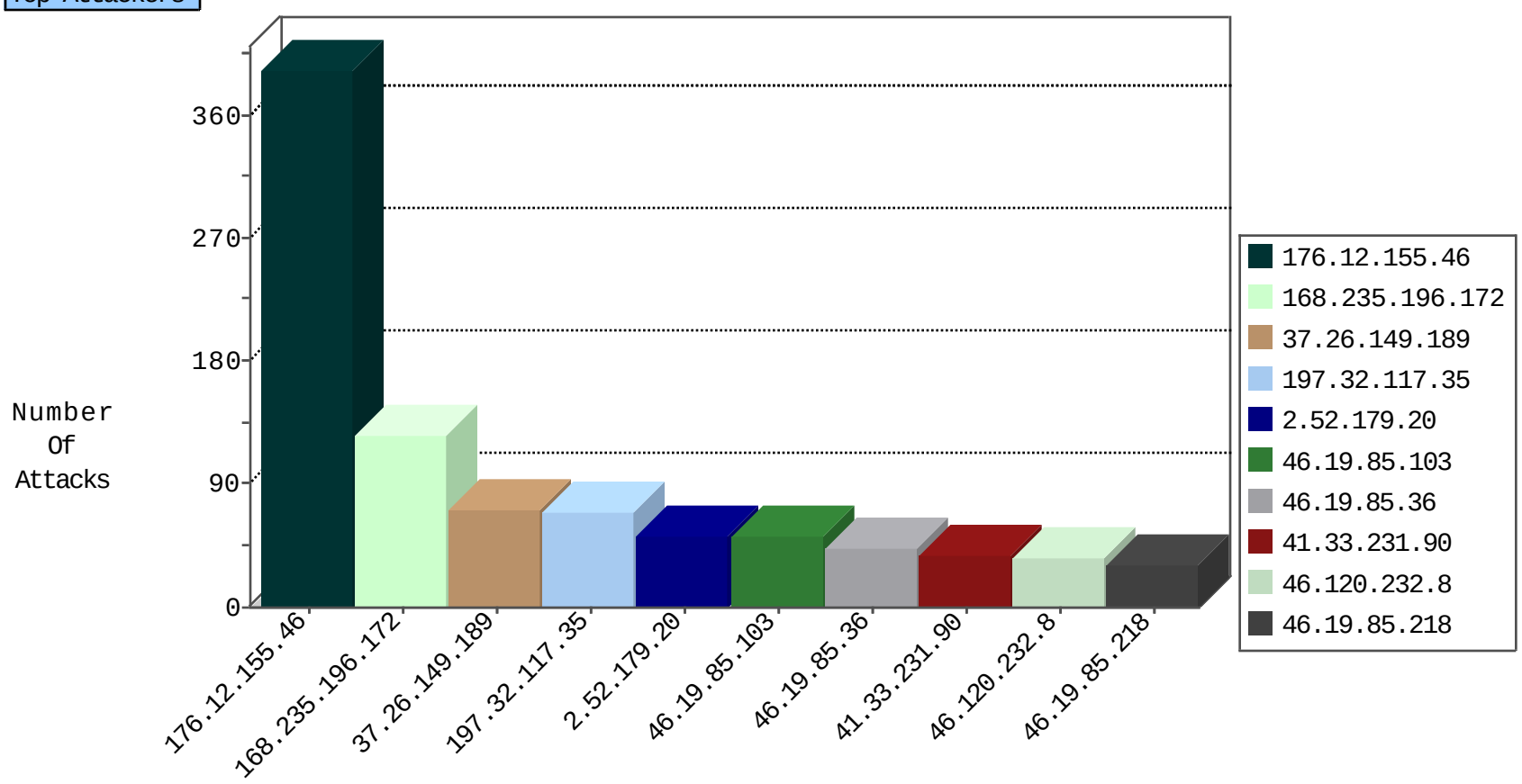
02-02-2016-10:04:09 to 02-02-2016-11:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-02-2016-10:04:09 to 02-02-2016-11:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
168.235.196.172	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2

02-02-2016-10:04:09 to 02-02-2016-11:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-02-2016-10:04:09 to 02-02-2016-11:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
192.115.67.2	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	5
54.157.215.29	147.237.77.176	United States	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.116.16.175	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.122.211.1	147.237.76.199	United Kingdom	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
132.64.53.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.122.211.1	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN Potential SSH Scan	1
94.216.151.62	147.237.0.15	Germany	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
37.26.149.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.220.116	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.11.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
212.199.244.112	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.166.129.183	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
209.126.116.147	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.255.156	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.7	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
168.235.196.172	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
37.122.211.1	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
37.122.211.1	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential SSH Scan	1
84.108.52.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.17.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
69.30.254.186	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
62.0.24.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.210.216.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.25.79.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.166.129.183	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
199.203.153.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-02-2016-10:04:09 to 02-02-2016-11:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
168.235.196.172	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	121
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.85.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
197.32.117.35	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.85.103	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	29
197.32.117.35	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
46.19.85.103	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
2.54.175.62	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
85.130.252.241	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.10.124.76	Hungary	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.138.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.29.206.9	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
37.26.148.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.149.189	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	12
46.19.85.112	Israel	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	12
66.102.8.243	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
66.102.8.243	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
37.26.149.189	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		alert	10
46.19.85.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.21.47	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.52.21.47	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
81.218.158.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.12.155.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.137.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.102.8.243	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
66.102.8.238	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
66.102.8.238	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
66.102.8.238	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
138.134.102.16	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.87	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.102.8.233	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.102.8.233	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
80.246.140.63	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.46.39.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.130.132.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.46.232	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.25	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.140.164	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.189	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.32.179.237	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.7	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.12.155.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.7	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
177.244.16.54	Mexico	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.12.155.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.65.139	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
177.244.16.54	Mexico	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
176.12.155.107	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

02-02-2016-10:04:09 to 02-02-2016-11:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.155.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	216
176.12.155.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
176.12.155.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	65
2.52.179.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
37.26.149.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
46.120.232.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
46.19.85.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
185.32.179.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.86.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
176.12.155.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
2.54.148.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
176.12.155.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
80.246.139.58	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.246.139.58	Block	10
46.19.85.36	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
46.19.85.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.52.51.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	6
46.19.85.196	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	6
2.52.50.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
40.77.167.32	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/main/home/default.aspx	Block	4
176.12.155.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.43.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.155.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.178.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.46.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.155.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.138.121	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
138.134.102.16	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
2.54.43.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.178.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Distributed Abnormally Long Request	Block	1
66.249.64.18	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
195.22.126.180	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/xmlrpc.php	Block	1
184.168.193.218	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
80.246.139.58	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catI in www.aka.idf.il/main/giyus/general.aspx	None	1
216.72.40.185	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 216.72.40.185	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	1
197.32.117.35	Egypt	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method eRiÂ†Â?}ÃŸ Â»R[[#28]][[#25]]Â¥`pÃ¹h[[#3]]Ã¡/>Ã Â«Ã IIhFÂ?Ã»Ã°Â?[[#27]]Â™Â€ ^Â¥ÃŸÂ„Ã†Â°[[#25]][[#12]]Â˜[[#0]]Ã?Ã•Â™Â»;Ã®Â†/([[#24]]Ã• Â®[[#4]]Ã¨{[[#20]]3&,Ã¶3[[#3]]Ã a3Ã°Ã¾Ãž 5Â?g[[#27]]XÃ¿=[[#3]][[#31]][[#28]]Â€Â½>lÃ?Â¹Ã″ Â³-?[[#28]][[#16]][[#14]]Â•Â¬Ã¿\2Ã°Ã…ÂŒÂ¿Ã€[[#11]]Ã‹VÂ‡[[#0]]Â˜ Â™'Ã°Â¨Ã°Â®	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	1
192.115.67.2	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Method Â½WÃ¿2BÂ¨[[#0]]Ã?Â¯Ã¼ezxBj'SG[[#29]][[#8]]Â±Ã?Â–Â¿	Block	1
178.95.80.42	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
81.218.60.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/sachar	Block	1
197.32.117.35	Egypt	147.237.77.216	dover.idf.il	NULL Character in Method eRiÂ†Â?}ÃŸ Â»R[[#28]][[#25]]Â¥`pÃ¹h[[#3]]Ã¡/>Ã Â«Ã IIhFÂ?Ã»Ã°Â?[[#27]]Â™Â€ ^Â¥ÃŸÂ„Ã†Â°[[#25]][[#12]]Â˜[[#0]]Ã?Ã•Â™Â»;Ã®Â†/([[#24]]Ã• Â®[[#4]]Ã¨{[[#20]]3&,Ã¶3[[#3]]Ã a3Ã°Ã¾Ãž 5Â?g[[#27]]XÃ¿=[[#3]][[#31]][[#28]]Â€Â½>lÃ?Â¹Ã″ Â³-?[[#28]][[#16]][[#14]]Â•Â¬Ã¿\2Ã°Ã…ÂŒÂ¿Ã€[[#11]]Ã‹VÂ‡[[#0]]Â˜ Â™'Ã°Â¨Ã°Â®	Block	1
5.29.206.9	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1

02-02-2016-10:04:09 to 02-02-2016-11:04:09