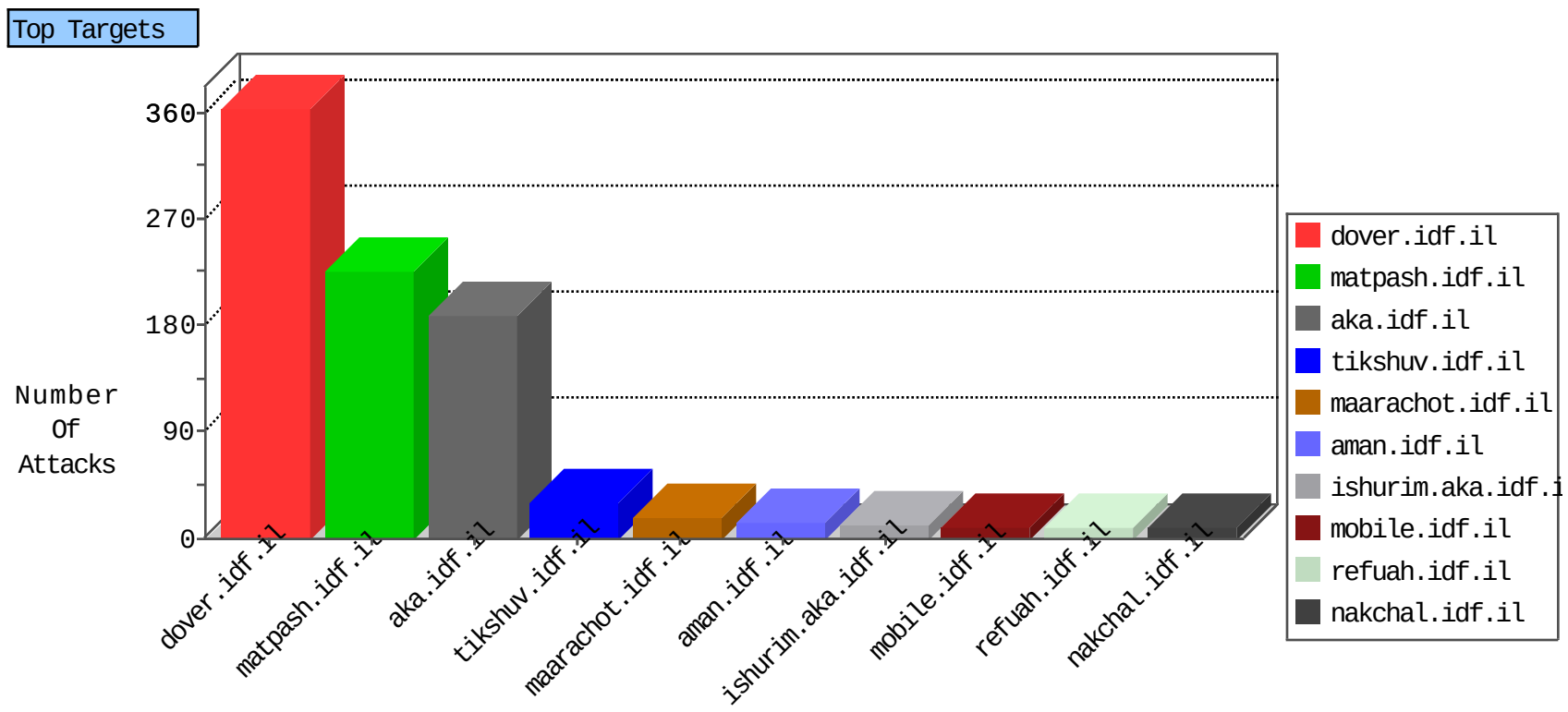
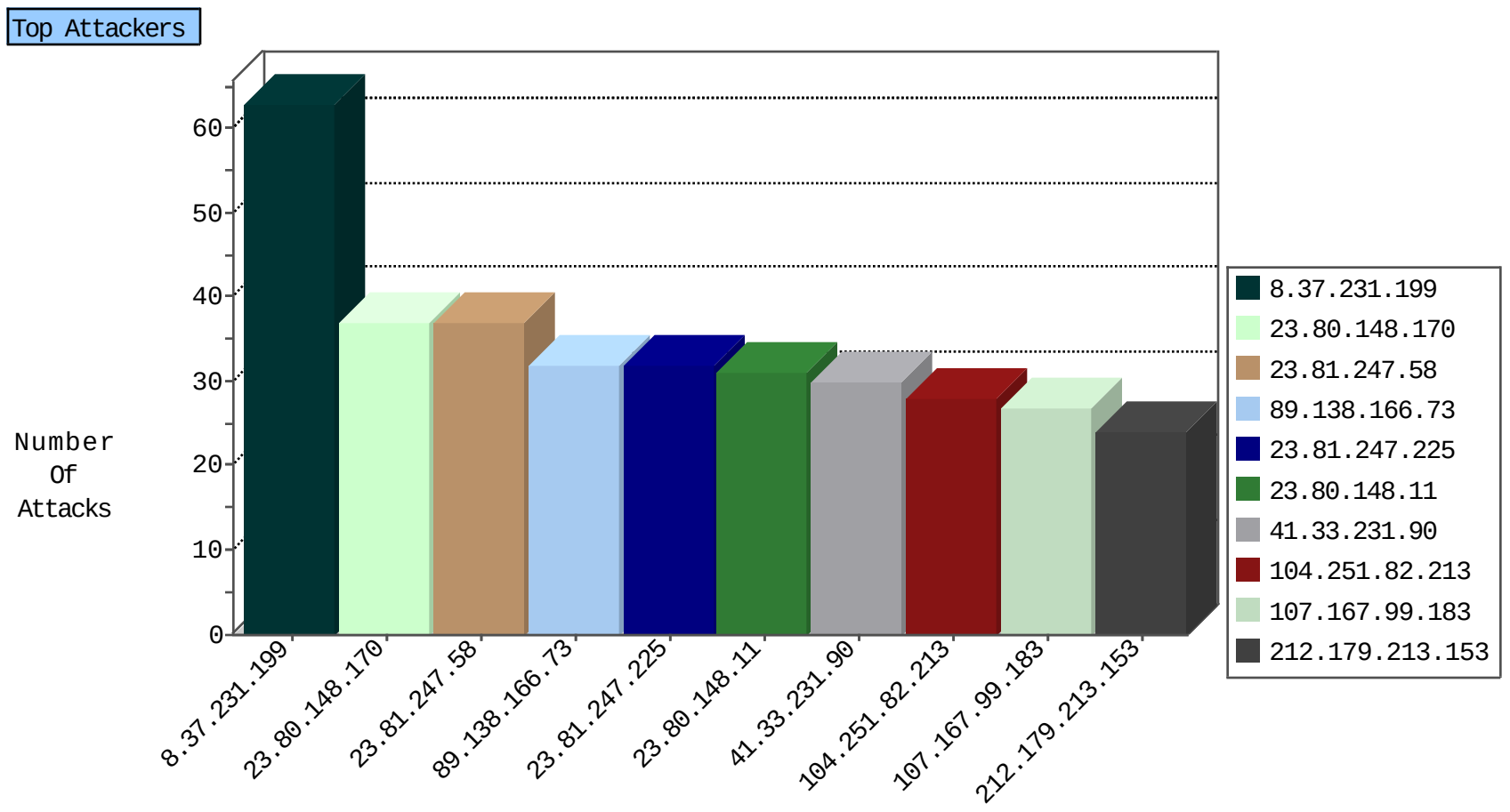
02-22-2016-00:04:07 to 02-22-2016-01:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-22-2016-00:04:07 to 02-22-2016-01:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
8.37.231.199	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
51.255.232.67	United Kingdom	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
82.81.48.191	Israel	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1

02-22-2016-00:04:07 to 02-22-2016-01:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.173.235.227	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.202.49.23	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
149.202.49.23	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
95.35.151.89	Israel	147.237.77.216	dover.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	1

02-22-2016-00:04:07 to 02-22-2016-01:04:07

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
179.43.141.234	147.237.72.156	Switzerland	aman.idf.il	ET SCAN NMAP -sS window 1024	1
123.196.117.70	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
119.134.114.228	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.20.69.74	147.237.72.217	United States	e.idf.il	ET DROP Dshield Block Listed Source	1
185.103.252.2	147.237.76.38		e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
173.14.248.34	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
123.196.117.70	147.237.72.167	China	ishurim.aka.idf.i	ET SCAN Potential SSH Scan	1

02-22-2016-00:04:07 to 02-22-2016-01:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.231.199	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	61
23.80.148.170	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	37
23.81.247.58	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	37
23.81.247.225	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	32
23.80.148.11	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
104.251.82.213		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	28
107.167.99.183	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	27
104.251.90.165		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	24
104.251.82.167		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	21
2.52.156.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.228.251.166	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
212.179.213.153	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
212.179.213.153	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
5.28.163.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.250.133.152	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.22.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.177.223.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.210.188.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.116.147.209	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.250.133.152	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence		monitor	4
94.230.86.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
86.175.216.45	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.176.166.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
89.139.90.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.176.166.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
77.127.18.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.14.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
77.125.95.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
177.29.123.17	Brazil	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.14.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.125.162.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.74.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.56.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
148.251.13.51	Germany	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

02-22-2016-00:04:07 to 02-22-2016-01:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.166.73	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.138.166.73	Block	18
89.138.166.73	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	10
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	8
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.19.86.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
78.97.175.254	Romania	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	2
128.232.110.28	United Kingdom	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	2
89.138.166.73	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	2
46.19.85.235	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method ted-With: in URL com.facebook.katana	Block	2
79.180.108.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
77.125.162.178	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 77.125.162.178	Block	2
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	2
5.29.24.197	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 5.29.24.197 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
89.138.166.73	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	2
80.246.136.158	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
207.46.13.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	2
141.212.122.129	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to /x	Block	2
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	2
109.67.49.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
217.132.64.140	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
46.19.85.235	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	2
157.55.39.214	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	2
79.178.194.152	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
5.29.24.197	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
68.180.231.40	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/youtu.be/dsh2chqxxt0	Block	2
46.19.86.233	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	2
207.46.13.170	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	2
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	2
2.52.2.116	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	2
46.19.85.235	Israel	147.237.77.216	dover.idf.il	Malformed URL com.facebook.katana	Block	2
157.55.39.222	United States	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
79.178.194.152	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	2
91.108.88.238	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	2
72.197.51.252	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	2
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	2
5.22.130.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
78.97.175.254	Romania	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/kkkkkkk=658c24f5kkkkkkk_658c24f5	Block	2
141.0.14.73	Europe	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/5dc935ee3fe96098f0b7f87901e5bdf86b555295/	Block	2
84.108.120.67	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	2
157.55.39.132	United States	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
5.28.148.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
80.246.136.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
188.120.151.135	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1

02-22-2016-00:04:07 to 02-22-2016-01:04:07