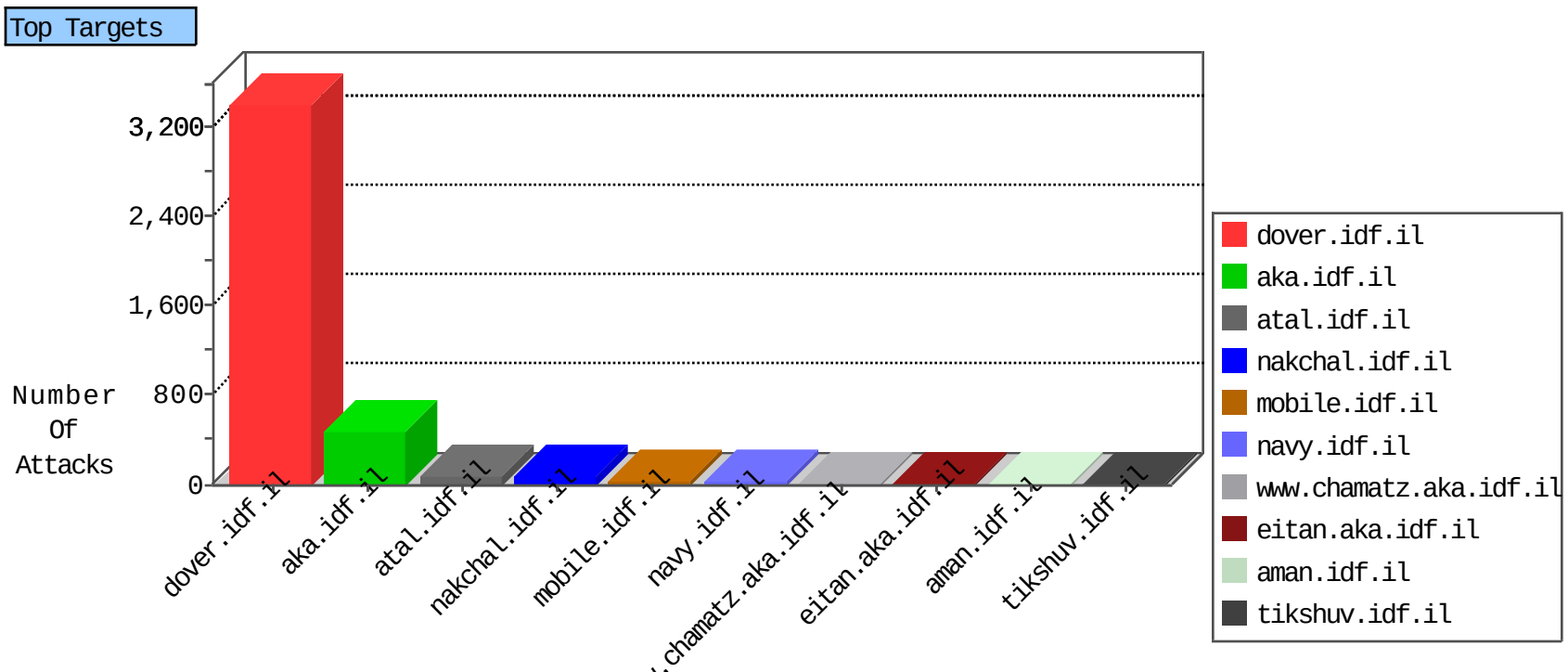
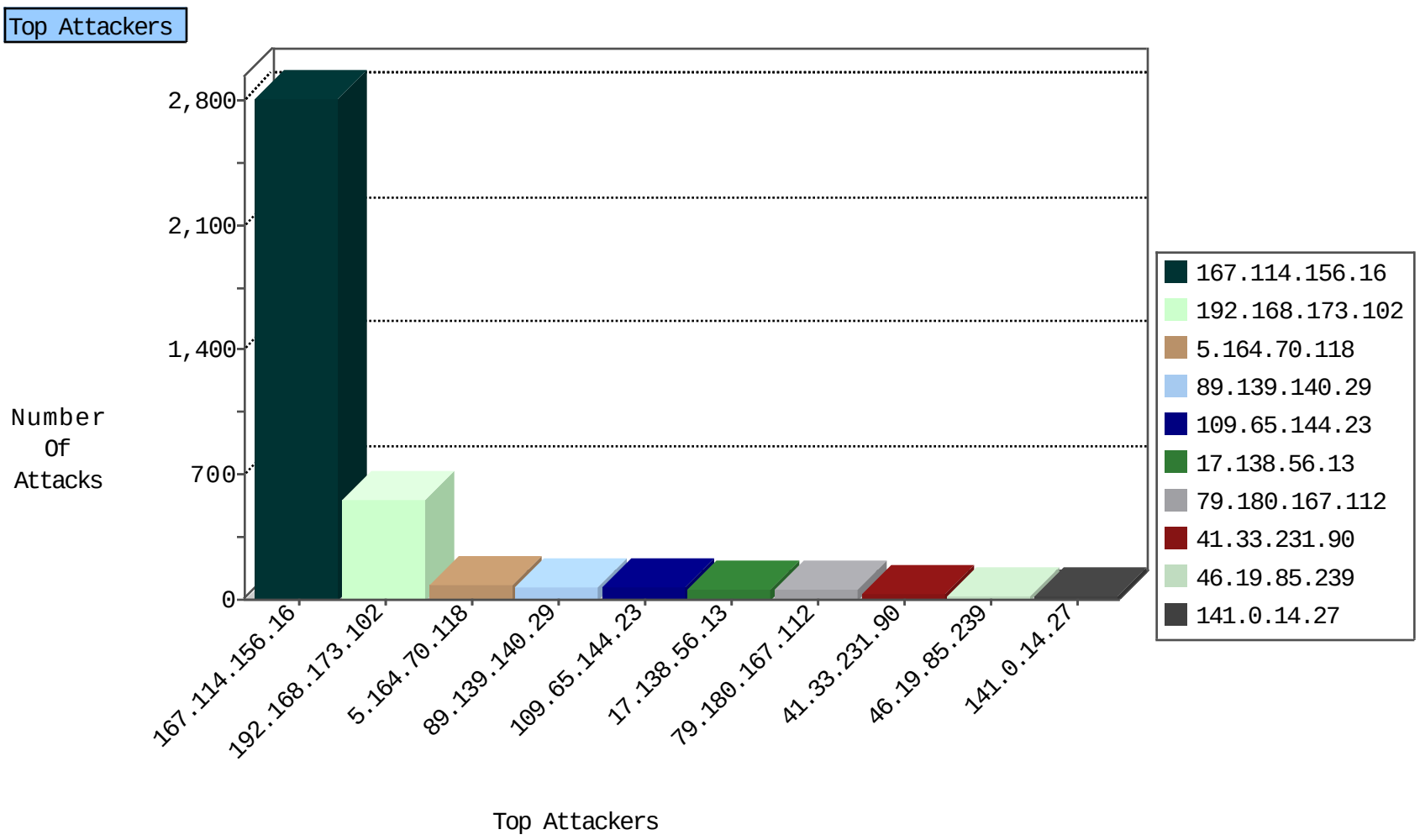
04-09-2016-16:04:09 to 04-09-2016-17:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-09-2016-16:04:09 to 04-09-2016-17:04:09

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	Block_Ip_Web_In	drop	2806
5.164.70.118	Russian Federation	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Http	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
5.164.70.118	Russian Federation	147.237.77.233	atal.idf.il	JLM_Under_Attack_Con_Http	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
93.215.25.203	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
93.215.25.203	Germany	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
93.215.25.203	Germany	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
104.153.31.3	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
93.215.25.203	Germany	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
93.215.25.203	Germany	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
93.215.25.203	Germany	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
93.215.25.203	Germany	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
62.138.2.122	Germany	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
185.103.252.93	Russian Federation	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1

04-09-2016-16:04:09 to 04-09-2016-17:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
63.141.226.178	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1
66.249.69.79	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-09-2016-16:04:09 to 04-09-2016-17:04:09

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
121.31.114.149	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.196.49.101	147.237.77.234	India	halag.idf.il	ET SCAN NMAP -sS window 2048	1
112.196.49.101	147.237.77.234	India	halag.idf.il	ET SCAN NMAP -f -sS	1
81.27.85.28	147.237.8.27	United Kingdom	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.76.38	Latvia	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
122.52.113.21	147.237.8.28	Philippines	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
121.31.42.241	147.237.8.14	China	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.196.49.101	147.237.77.234	India	halag.idf.il	ET SCAN NMAP -sS window 1024	1
93.183.201.2	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1

04-09-2016-16:04:09 to 04-09-2016-17:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	371
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	192
17.138.56.13	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	56
5.164.70.118	Russian Federation	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
5.164.70.118	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	29
109.65.144.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	23
109.65.144.23	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
141.0.14.27	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
77.30.247.253	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.19.85.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
192.115.133.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
109.65.144.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
37.26.148.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
217.132.100.195	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
5.189.190.212	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.65.144.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	9
5.29.20.6	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.115.133.147	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.186.53.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.192	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.65.16	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.112.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.53.6.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.32.114	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.169	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.242.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.196	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	4
81.218.116.129	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.102.195.70	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.239	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.130.189.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.239	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.79	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
79.181.21.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.144.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.229.35.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.84.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.133.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.35.129.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
87.70.150.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.0.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.52.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.24.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-09-2016-16:04:09 to 04-09-2016-17:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.139.140.29	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 89.139.140.29	Block	70
79.180.167.112	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.180.167.112	Block	26
79.180.167.112	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	25
81.218.116.129	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	8
81.218.116.129	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	3
89.139.140.29	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.139.140.29	Block	3
79.180.167.112	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/	Block	2
87.70.21.241	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	2
212.25.119.193	Israel	147.237.76.39	mobile.meitav.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	2
149.78.23.55	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.78.23.55	Block	2
84.108.165.44	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
207.46.13.93	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Abnormally Long Request method	Block	1
93.173.28.127	Israel	147.237.72.156	aman.idf.il	NULL Character in Header Name at	Block	1
41.33.234.234	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method j^‡[[#4]]õ[[#7]]q2gº1ã•¡xû½[[#26]]¶E<•ä\Z?Î~]Sœl¼[[#14]] in URL	Block	1
54.153.33.233	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
149.78.23.55	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
93.173.28.127	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Name	Block	1
84.108.193.61	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
207.46.13.120	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portalmiluim/templates/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Method	Block	1
93.173.28.127	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
41.33.234.234	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
93.173.28.127	Israel	147.237.72.156	aman.idf.il	Distributed Abnormally Long Request	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Illegal Byte Code Character in Method	Block	1
79.180.167.112	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
157.55.39.108	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/giyus/qanda/default.asp	None	1
93.173.28.127	Israel	147.237.72.156	aman.idf.il	Illegal HTTP Version N›ë*dQŽ°ØéÖ[[#24]]e[[#30]]´b]^[[#23]]S[[#24]]nf½I*8PÅ[[#12]]N8$LsÎsnÃKø«'dŽ[[#12]]"Óø[[#28]][[#27]]ËIÏ[[#1]]"¿[[#2]]Ù•fˆœeq¦Ìcp[[#6]][[#22]]Èu›>©)›it•™œ[[#8]]•¶Çì…Xÿp—ô7[[#7]]ƒ•>¨[[#0]]ÑGbBÙî[[#2]]¸ˆÈõ[[#14]]Ô()øÿNR~f1ªVF•_m–»[[#24]]Õž0…"[[#19]]ÝgÛ!YŽ_Ò³W%ß²s ¨![[#5]]&†ÊÐç÷•+Ü[[#27]]*•+L]‹[[#27]]UçŸÂl/Å^aöxG„`ì;8è:[[#11]]Ç`qeŠ[[#29]]œ7&O„cÍ[[#11]][[#20]]¯[[#15]];$_•y?F[[#7]]«`zëK[[#7]]™Ž~å5[[#18]]£þ€…¸<‹,ŒÍWÎÿÔiÖä[[#19]]Ã`'y2,É$Ð"û\I¡Ï†•ÅáQ[[#23]][[#22]]3Î•›.e[[#14]]Éüd•ñó~Í•[[#5]]–à1Ä	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Abnormally Long Request method	Block	1
77.237.138.202	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
118.193.163.150	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
46.19.85.192	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
93.173.28.127	Israel	147.237.72.156	aman.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.65.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/drushim/misrot.aspx	Block	1
157.55.39.143	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/...	Block	1
2.53.6.45	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
93.173.28.127	Israel	147.237.72.156	aman.idf.il	Malformed URL l•¸=fgy[[#17]][[#21]][[#14]]¸p[[#12]]¿×–$ƒ¹¸¦h×o+	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in Method j^‡[[#4]]õ[[#7]]q2gº1ã•¡xû½[[#26]]¶E<•ä\Z?Î~]Sœl¼[[#14]]	Block	1
146.50.79.106	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
46.19.86.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
93.173.28.127	Israel	147.237.72.156	aman.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
199.47.81.11	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1086-14000-	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-17350-en/dover.aspx	Block	1
169.229.3.90	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/ts.php	Block	1

04-09-2016-16:04:09 to 04-09-2016-17:04:09