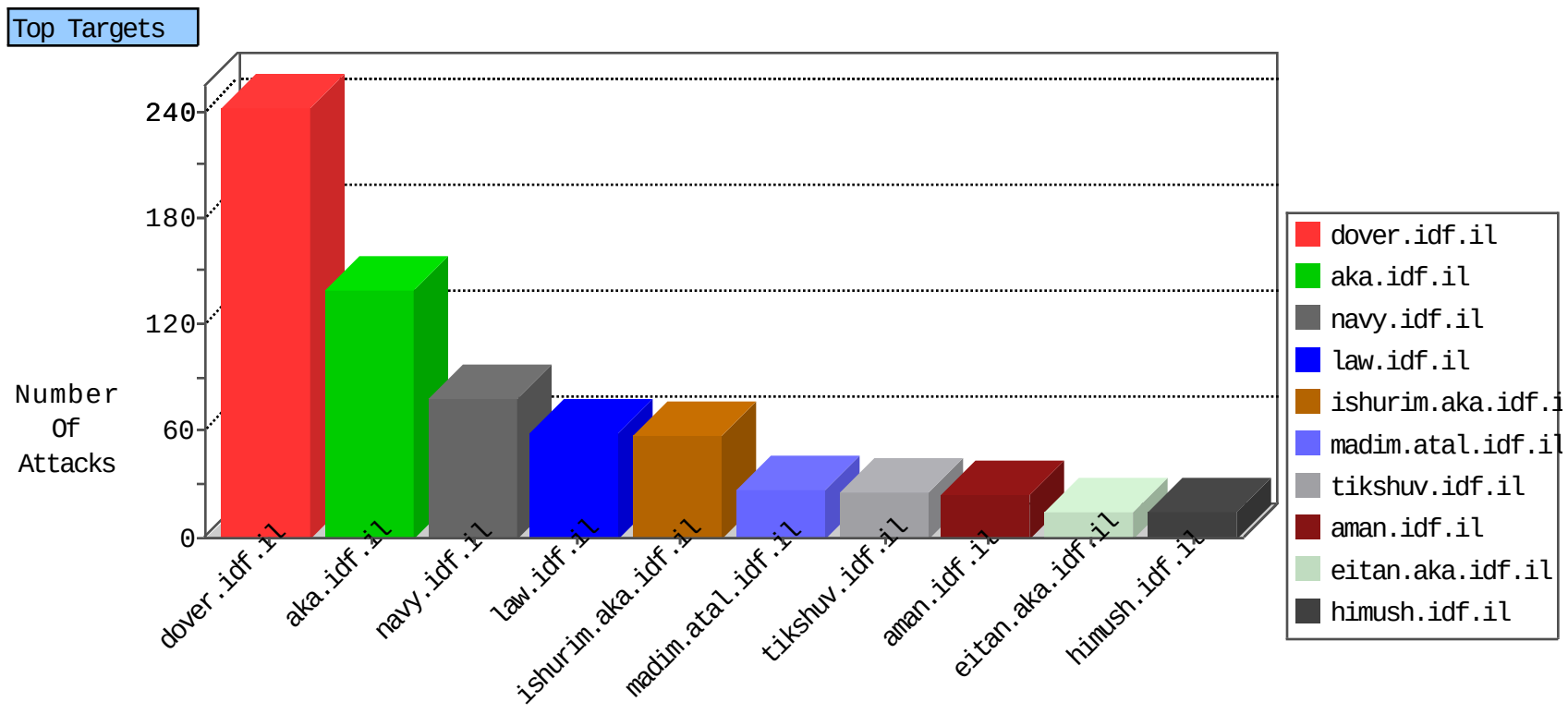
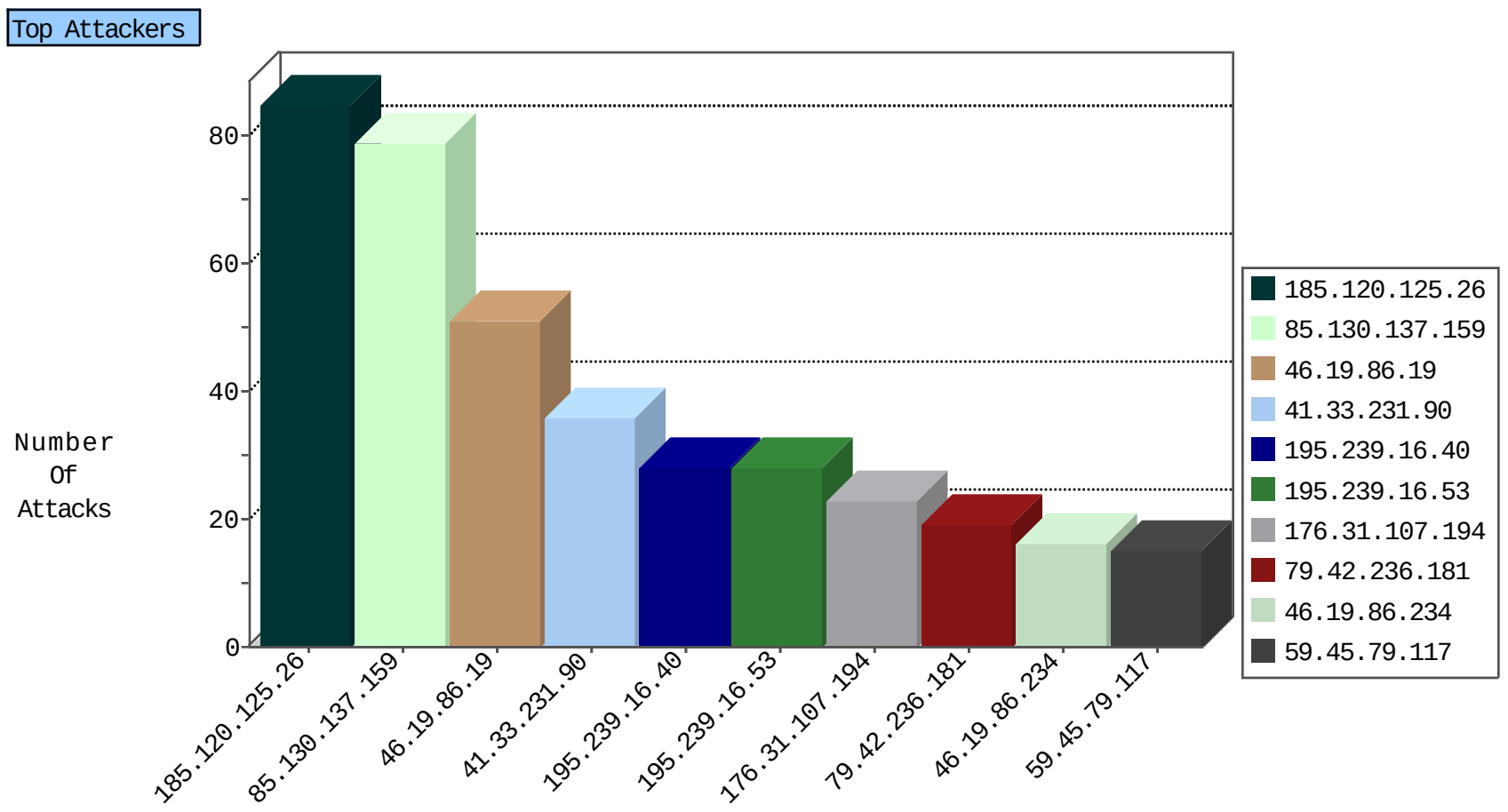
02-07-2016-23:04:06 to 02-08-2016-00:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-07-2016-23:04:06 to 02-08-2016-00:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.178.233	Israel	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	5
89.248.172.154	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
31.202.128.149	Ukraine	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
31.202.128.149	Ukraine	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
104.233.75.217		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
31.202.128.149	Ukraine	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
31.202.128.149	Ukraine	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
31.202.128.149	Ukraine	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
31.202.128.149	Ukraine	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
31.202.128.149	Ukraine	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

02-07-2016-23:04:06 to 02-08-2016-00:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.254.123.18	Romania	147.237.77.216	dover.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
5.254.123.18	Romania	147.237.72.166	aka.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

02-07-2016-23:04:06 to 02-08-2016-00:04:06

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
79.42.236.181	147.237.77.19	Italy	law-forum.idf.il	ET SCAN Potential SSH Scan	2
79.42.236.181	147.237.76.199	Italy	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
79.42.236.181	147.237.0.16	Italy	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
46.166.129.183	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -f -sS	1
183.60.48.25	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.2	147.237.76.198	Russian Federation	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
79.42.236.181	147.237.76.38	Italy	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
115.28.133.234	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
79.42.236.181	147.237.8.46	Italy	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
79.42.236.181	147.237.8.14	Italy	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.8.50	Canada	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
79.42.236.181	147.237.0.19	Italy	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
82.102.136.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
78.193.2.8	147.237.76.202	France	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
79.42.236.181	147.237.77.212	Italy	e.dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
46.166.129.183	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 2048	1
79.42.236.181	147.237.77.121	Italy	e.navy.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
46.121.80.243	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.42.236.181	147.237.76.200	Italy	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.2	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
79.42.236.181	147.237.76.196	Italy	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
115.28.133.234	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
79.42.236.181	147.237.76.30	Italy	himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
115.28.133.234	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
79.42.236.181	147.237.8.28	Italy	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
79.42.236.181	147.237.0.200	Italy	m4u.idf.il	ET SCAN Potential SSH Scan	1
91.207.60.30	147.237.77.61	Ukraine	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
79.42.236.181	147.237.77.226	Italy	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

02-07-2016-23:04:06 to 02-08-2016-00:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.125.26		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	57
46.19.86.19	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	51
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
185.120.125.26		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
85.130.137.159	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
85.130.137.159	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
109.64.228.198	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
63.143.230.202	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
2.52.170.230	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
85.130.137.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
85.130.137.159	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
85.130.137.159	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.86.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
85.130.137.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.146.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.160.190	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
5.22.130.241	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
66.249.78.5	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.144.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.214.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
85.130.137.159	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
87.69.62.179	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
66.249.78.245	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
94.230.86.169	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
85.65.22.88	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.179.49.186	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.22.131.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.7.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.175.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.153.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.4.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.2.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.146.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.111.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.117.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.139.49.251	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	3
37.26.148.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
84.228.32.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.1.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.152.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.109.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.35.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-07-2016-23:04:06 to 02-08-2016-00:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.31.107.194	France	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 176.31.107.194	Block	8
176.31.107.194	France	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 176.31.107.194	Block	6
176.31.107.194	France	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	4
176.31.107.194	France	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	4
109.253.203.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.157.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
65.208.151.114	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	2
109.160.177.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
65.208.151.113	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	2
65.208.151.116	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 65.208.151.116	Block	2
141.212.122.81	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /x	Block	1
65.208.151.113	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/text/javascript	Block	1
85.64.189.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$1 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.78.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding)![Fi}(&X-FO_PdXK/L0-[xhX1YtKq1 in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
65.208.151.119	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1008-he/+navmenu.qc+	Block	1
109.64.108.171	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.86.175	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$3 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
79.182.213.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2617.jpg	Block	1
157.55.39.247	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/901-8504/tikshuv.aspx	Block	1
85.64.222.252	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.78.230	Block	1
66.76.85.15	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
46.120.154.62	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.66.142	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
65.208.151.114	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
89.139.238.134	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.78.245	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in eitan.aka.idf.il/1085-en/eitan.aspx	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
185.6.59.206	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
65.208.151.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 65.208.151.112	Block	1
83.99.198.74	Latvia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3294.jpg	Block	1
65.208.151.114	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/piwik.php	Block	1
37.26.149.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.86.119.211	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2/105452.pdf&sa=u&ved=0ahukewj20amfz-bkahwfxnikhrppbxkqfggdmag&usg=afqjcnfiurn5qihnu1jmcjhpozpfuqhusa	Block	1
188.143.232.26	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1393-en/dover.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf_in_pictures/images/2002/march/balatadotjpg	Block	1
128.194.131.235	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
83.99.198.74	Latvia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.78.80	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
176.31.107.194	France	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/index.php	Block	1
104.236.76.85		147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;f in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
79.179.135.60	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
198.20.69.74	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2662.jpg	Block	1

02-07-2016-23:04:06 to 02-08-2016-00:04:06