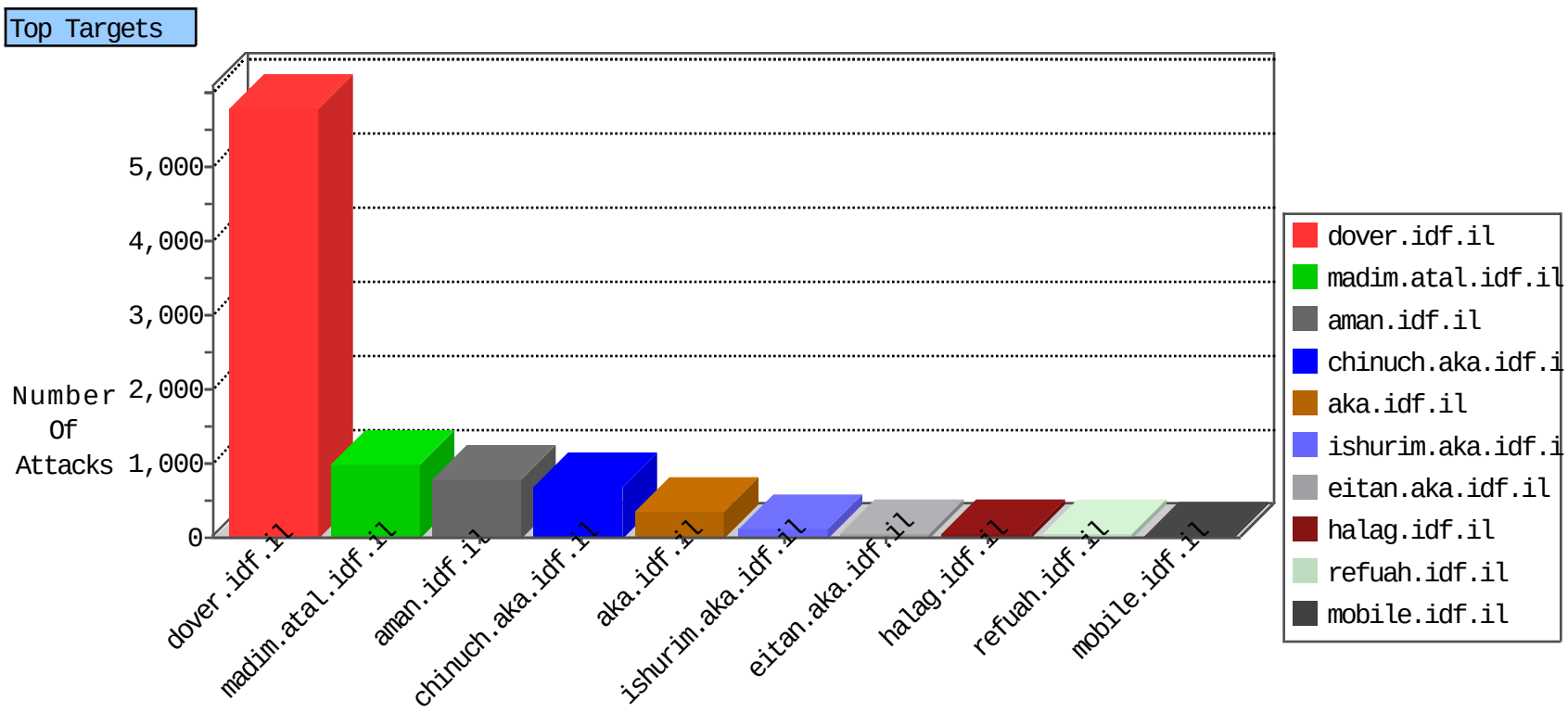
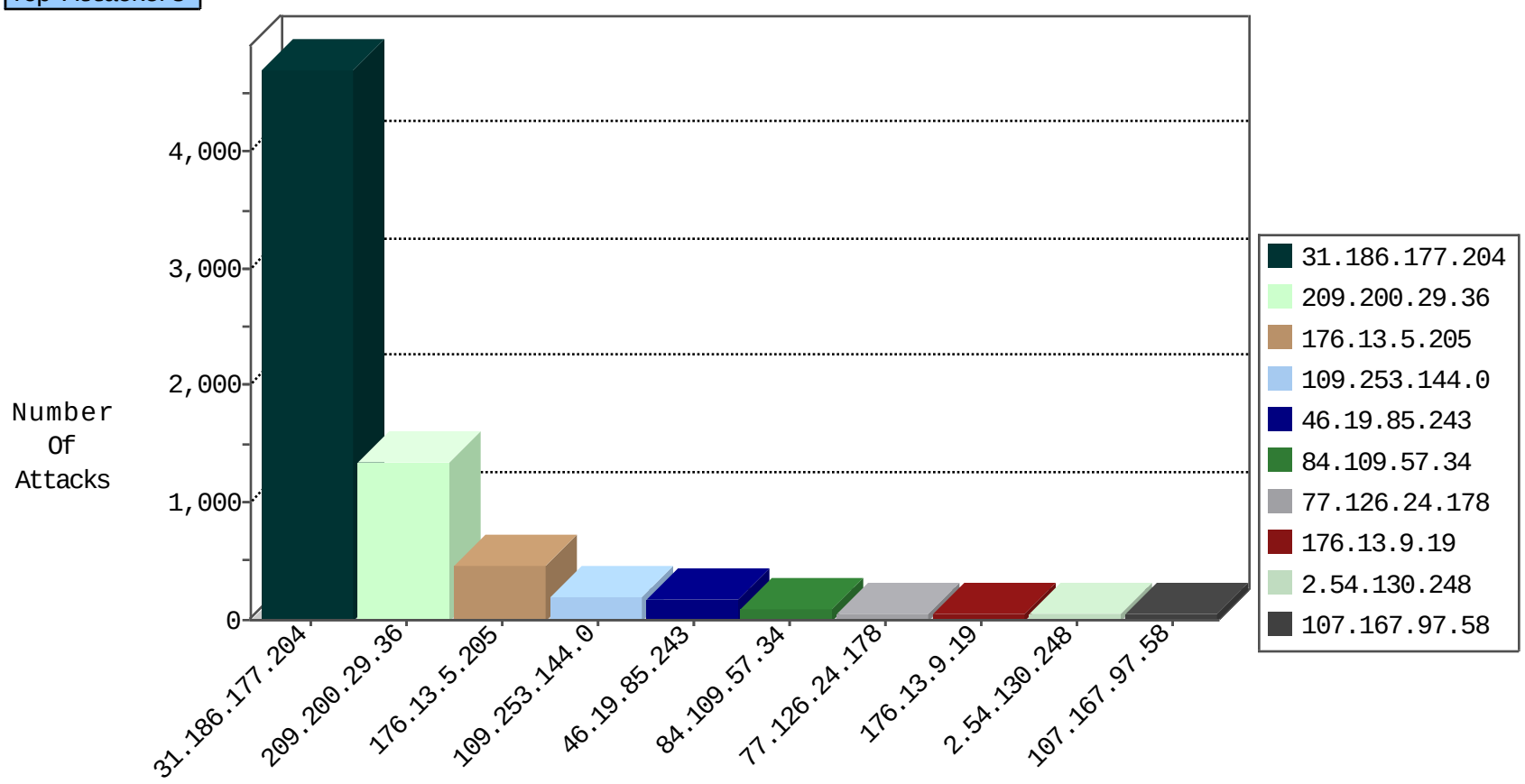
01-27-2016-17:04:08 to 01-27-2016-18:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-27-2016-17:04:08 to 01-27-2016-18:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.186.177.204	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	6345
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	82
79.181.56.211	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	13

01-27-2016-17:04:08 to 01-27-2016-18:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.139.225	Israel	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
176.13.12.252	Israel	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-27-2016-17:04:08 to 01-27-2016-18:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.57	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
84.108.220.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
37.26.146.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.246.237.178	147.237.8.50	Poland	e.tikshuv.idf.i	ET SCAN NMAP -sS window 1024	1
31.186.177.204	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
193.47.165.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.82.106.200	147.237.76.201	India	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.231.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.17.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.6.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.13.173	147.237.77.176	United Kingdom	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.122.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.160.144.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.162.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.56.245	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.120.49.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.172.144.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.246.237.178	147.237.8.50	Poland	e.tikshuv.idf.i	ET SCAN NMAP -sS window 2048	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
31.210.178.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.246.237.178	147.237.8.50	Poland	e.tikshuv.idf.i	ET SCAN NMAP -f -sS	1
185.120.125.55	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
176.228.136.200	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.149.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.177.19.12	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
79.180.219.112	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.65.251.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.155.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.106.108.116	147.237.77.216	Japan	dover.idf.il	Tehila - Perl LWP with fake user agent	1
107.182.27.248	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
93.172.118.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-27-2016-17:04:08 to 01-27-2016-18:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.186.177.204	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3930
209.200.29.36	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	669
209.200.29.36	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	668
84.109.57.34	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
77.126.24.178	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	57
2.54.130.248	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
107.167.97.58	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	46
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
79.177.10.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
31.13.160.70	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
31.13.160.70	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
82.80.139.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
80.179.22.139	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
119.76.65.62	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
80.179.22.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
84.111.180.57	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
5.22.135.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.29.117.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
5.29.117.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
207.46.13.158	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	9
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
185.89.217.231		147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
147.236.34.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.57.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.26.148.190	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.134	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.162.137	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
5.102.254.199	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
31.210.187.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.46.38.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.114.91.234	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.44	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
185.127.10.40		147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
212.179.225.7	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.186.177.204	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Automated Vulnerability Scanning	Block	629
176.13.5.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	272
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	150
109.253.144.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	132
176.13.5.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
176.13.5.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	65
176.13.9.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
109.253.144.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	31
109.253.201.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
176.13.12.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
109.253.144.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	12
46.19.86.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
176.13.9.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
109.253.206.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.52.20.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
37.26.146.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
79.182.34.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
37.26.146.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.201.207	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ********** ********** ********** **********, Observed ********** ********** ********** **********	None	3
185.32.179.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.194.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.28.170.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.117.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.34.160.178	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/dover.aspx'	Block	2
5.22.135.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
83.244.109.234	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	2
83.244.109.234	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
46.19.85.1	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
109.64.219.114	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.176.134.202	Israel	147.237.0.16	my-kosher-kravi.idf.il	Parameter Type Violation Master$ContentPlaceHolder1$email in my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
213.8.72.90	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
185.3.147.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.111.180.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
112.204.76.159	Philippines	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
2.54.57.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.136.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.209.99	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.85.39	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.108.7.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.90.147.211	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.210	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.130.57	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1501-he/atal.aspx	Block	1