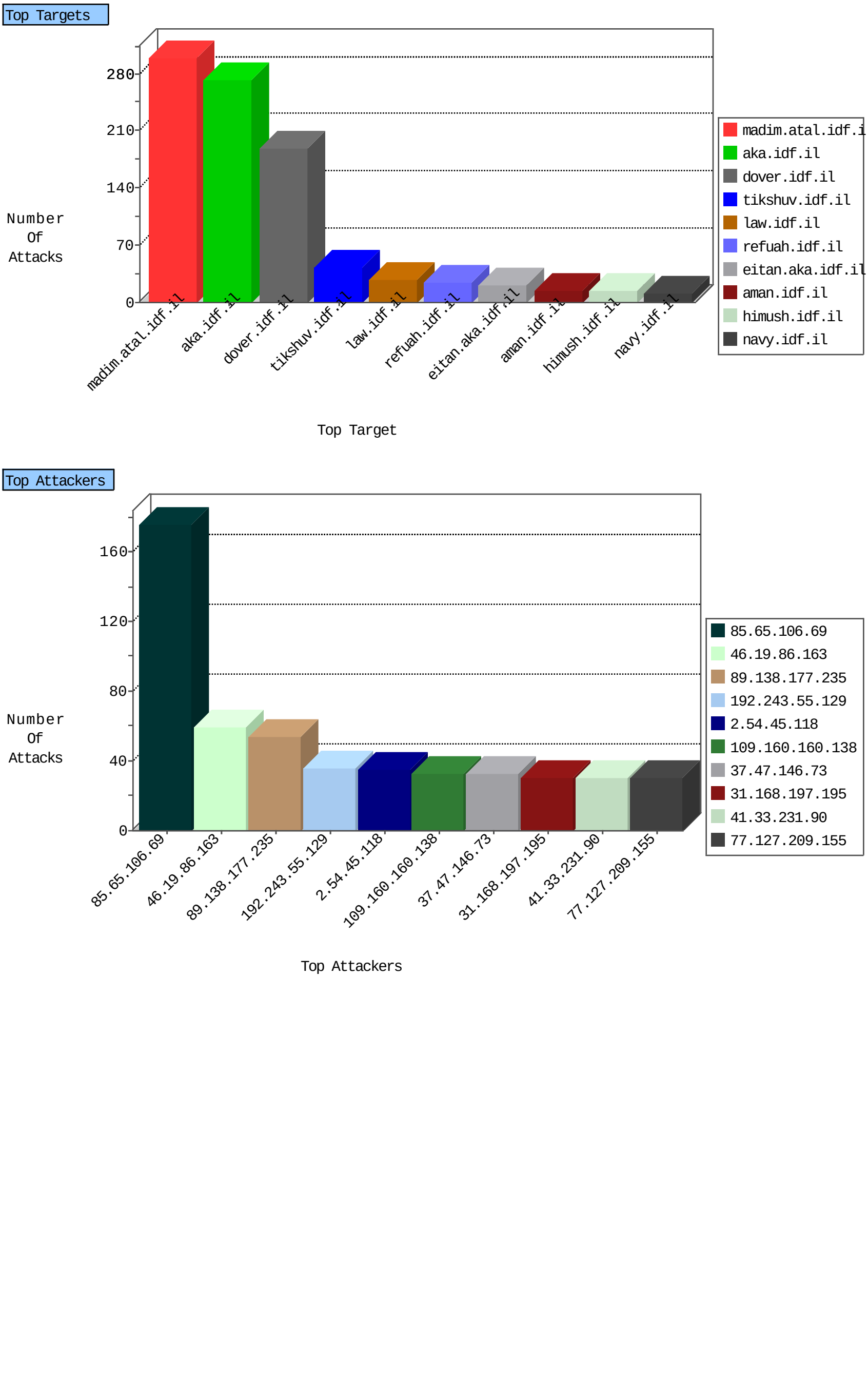
02-19-2016-14:04:04 to 02-19-2016-15:04:04

IDF Under Attack
Daily Report



02-19-2016-14:04:04 to 02-19-2016-15:04:04

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
149.78.83.163	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	3
212.179.221.96	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	1
38.229.33.47	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

02-19-2016-14:04:04 to 02-19-2016-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
40.77.167.25	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
108.59.8.80	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	2
149.88.3.143	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	2
65.55.210.155	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
66.249.78.134	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.2	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1

02-19-2016-14:04:04 to 02-19-2016-15:04:04

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	3
112.196.49.101	147.237.76.31	India	nakchal.idf.il	ET SCAN NMAP -f -sS	1
106.187.90.86	147.237.76.42	Japan	refuah.idf.il	GPL SCAN superscan echo	1
106.187.90.86	147.237.76.30	Japan	himush.idf.il	GPL SCAN superscan echo	1
84.228.161.35	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
176.13.5.55	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
125.24.59.237	147.237.77.121	Thailand	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.76.31	India	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
106.187.90.86	147.237.76.198	Japan	e.yohalan.idf.il	GPL SCAN superscan echo	1
106.187.90.86	147.237.76.31	Japan	nakchal.idf.il	GPL SCAN superscan echo	1
91.201.236.114	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.224.18	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
125.24.59.237	147.237.77.121	Thailand	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
117.218.234.197	147.237.77.19	India	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-19-2016-14:04:04 to 02-19-2016-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
37.47.146.73	Poland	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
82.145.211.20	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
132.71.170.7	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
31.168.197.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	10
80.246.130.151	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
109.67.107.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.66.16.77	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
2.54.45.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.54.45.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.45.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
2.54.45.118	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.45.118	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
5.22.131.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
68.180.229.239	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.197.195	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.13.81	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.66.16.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.219.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.169.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.5.55	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
176.13.5.55	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.168.197.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
31.168.197.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.187.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
189.219.147.193	Mexico	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
192.243.55.129	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.41.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.220.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
80.246.133.208	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.8.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.197.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.182.214.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.157.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.138.94	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

02-19-2016-14:04:04 to 02-19-2016-15:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.106.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	95
85.65.106.69	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 85.65.106.69	Block	81
46.19.86.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	59
89.138.177.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	52
109.160.160.138	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 109.160.160.138	Block	33
176.13.19.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.6.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.18.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.76.119.43	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
212.76.119.43	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 212.76.119.43	Block	2
2.54.167.81	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
212.76.119.43	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 212.76.119.43	Block	2
212.76.119.43	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 212.76.119.43	Block	2
212.76.119.43	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 212.76.119.43	Block	2
212.76.119.43	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 212.76.119.43	Block	2
212.76.119.43	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 212.76.119.43	Block	2
81.218.106.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
212.76.119.43	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 212.76.119.43	Block	2
212.76.119.43	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 212.76.119.43	Block	2
212.76.119.43	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 212.76.119.43	Block	2
149.78.133.43	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$82 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
84.228.17.139	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
212.76.119.43	Israel	147.237.72.166	aka.idf.il	NULL Character in Parameter Name [[#0]]râ€š‘[[#3]]Â?×?×'oâ„ ¢/Ö¾Â¾MCa[[#14]]Â?â€¢ÃžÖ´[[#25]]_×›[[#26]]×"v<.Ö¿×¨M×?â„¢Â´Ö½ in â€“[[#18]]	Block	1
46.210.136.145	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
89.138.168.52	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash/register/changepass.asp	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
212.76.119.43	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Query String >Â«6Â±WsbÂ³•Â¶<[[#22]]Â?:v[[#1]]Âµ×³y×?[[#31]] Â¬×˜8FpÂŽ "×?&[[#8]]×"ÃŠP2Ö¶[[#15]]Â¶ U2Â»Ã¿()[â€šÃ±ÂšÃ»×³sâ€"â€°lÂ¢Â·vpLâ€š × â€ [[#17]]×šÃ›iÃœ×©sÂ²Â·[[#5]]K)[[#5]]yâ€¡[[#29]]â€?[[#7]]Ã?Ö½ÃŸ 3TÂŽ![[#29]]<â€"1Â®×¤pÂ³Ö»vT3×'h[[#3]]Ö´]×ªâ€"}×¥×?Â®XÃ·Uâ€ ¢×¥/0â€¢Ö¾$F&Â?ÂŸÃ™Oâ€°cÂŒ×"×ŸÃ›×£Â°×¥â€¹L×'`[[#27]]ÃœÂŒ [[#31]] ×•ÂŒQ[[#12]]â€™[[#25]]â€š[[#4]][[#1]]tÂ³BÂ·(×¢Â MÂ¸×š [[#24]]Â¹Ö°TÖ»[[#24]]ÂŠ×¡â€¦Â®ae[[#8]]×"×£Âš yÂ©Ö¹b[[#4]][[#11]]kÂ?Ö¼×?8[[#15]]e[[#11]]×ªY[[#12]]IÂ¦N	Block	1
157.55.39.178	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
84.228.17.139	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
212.76.119.43	Israel	147.237.72.166	aka.idf.il	NULL Character in Query String [[#0]]râ€š‘[[#3]]Â?×?×'oâ„ ¢/Ö¾Â¾MCa[[#14]]Â?â€¢ÃžÖ´[[#25]]_×›[[#26]]×"v<.Ö¿×¨M×?â„¢Â´Ö½ on â€“[[#18]]	Block	1
62.84.81.6	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
5.29.165.67	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
185.16.27.210	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
79.182.136.242	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
46.60.61.86	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.76.119.43	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding .{â€¢â€"Ö·Ã™hâ€œ•×¡nsâ€œ%Æ'r	Block	1
213.151.32.163	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
212.76.119.43	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Parameter Name from 212.76.119.43	Block	1
31.44.139.37	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/mailbox.aspx&sa=u&ved=0ahukewjdj83d5oplahukvbqkhykvaicqjbaicg&usg=afqjcnfw8xbjdj46aa_ieeng07gs79p8hq	Block	1
185.93.35.9		147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
91.135.102.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.130.151	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
46.116.192.205	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
176.13.10.128	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
213.151.46.95	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
212.76.119.43	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Query String from 212.76.119.43	Block	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.44.139.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22456-he/idfgdover.aspx&sa=u&ved=0ahukewj2-b3l5oplahxk6xqkhuendvqqfggjmas&usg=afqjcnha4mb6odflnxrv4fsytoz3gjgkjw	Block	1
185.93.35.9		147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1

02-19-2016-14:04:04 to 02-19-2016-15:04:04