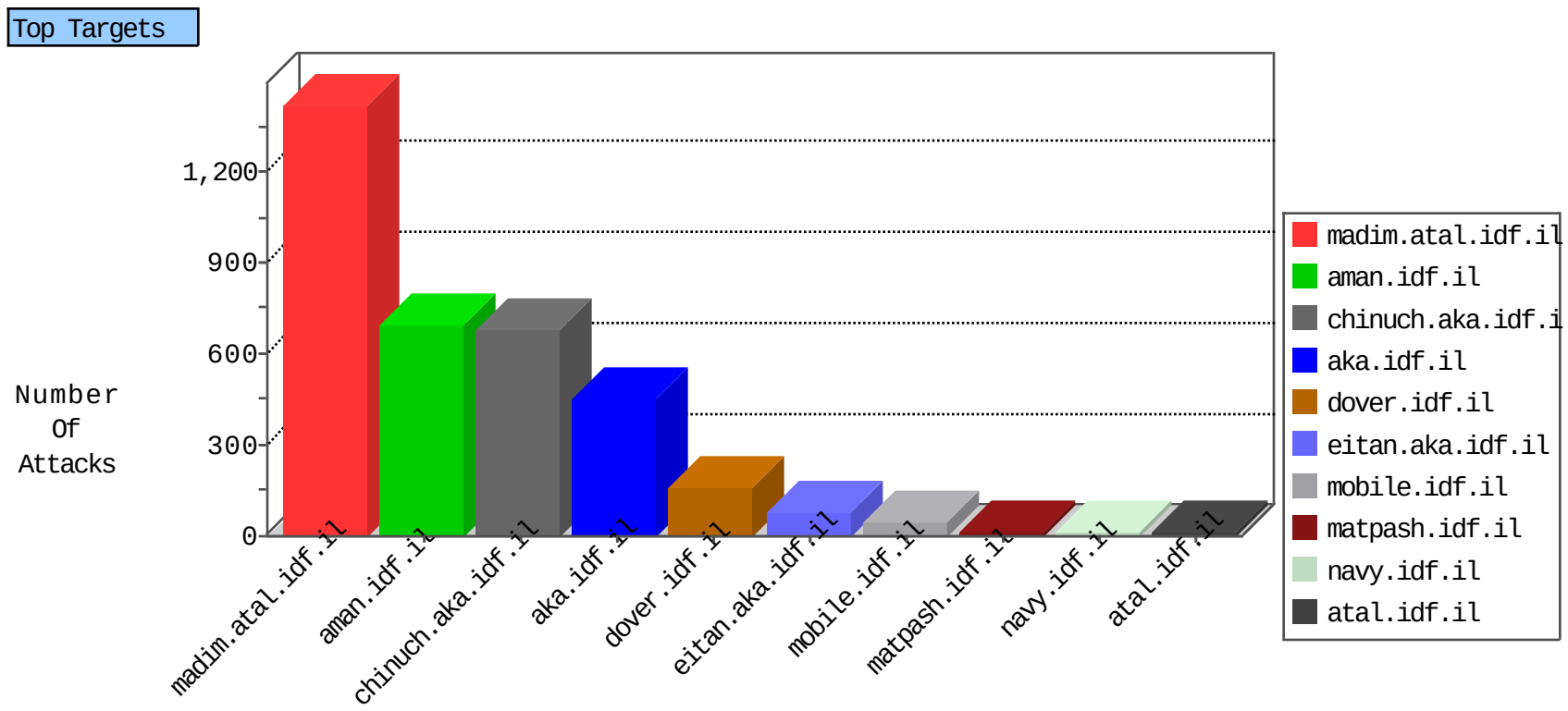
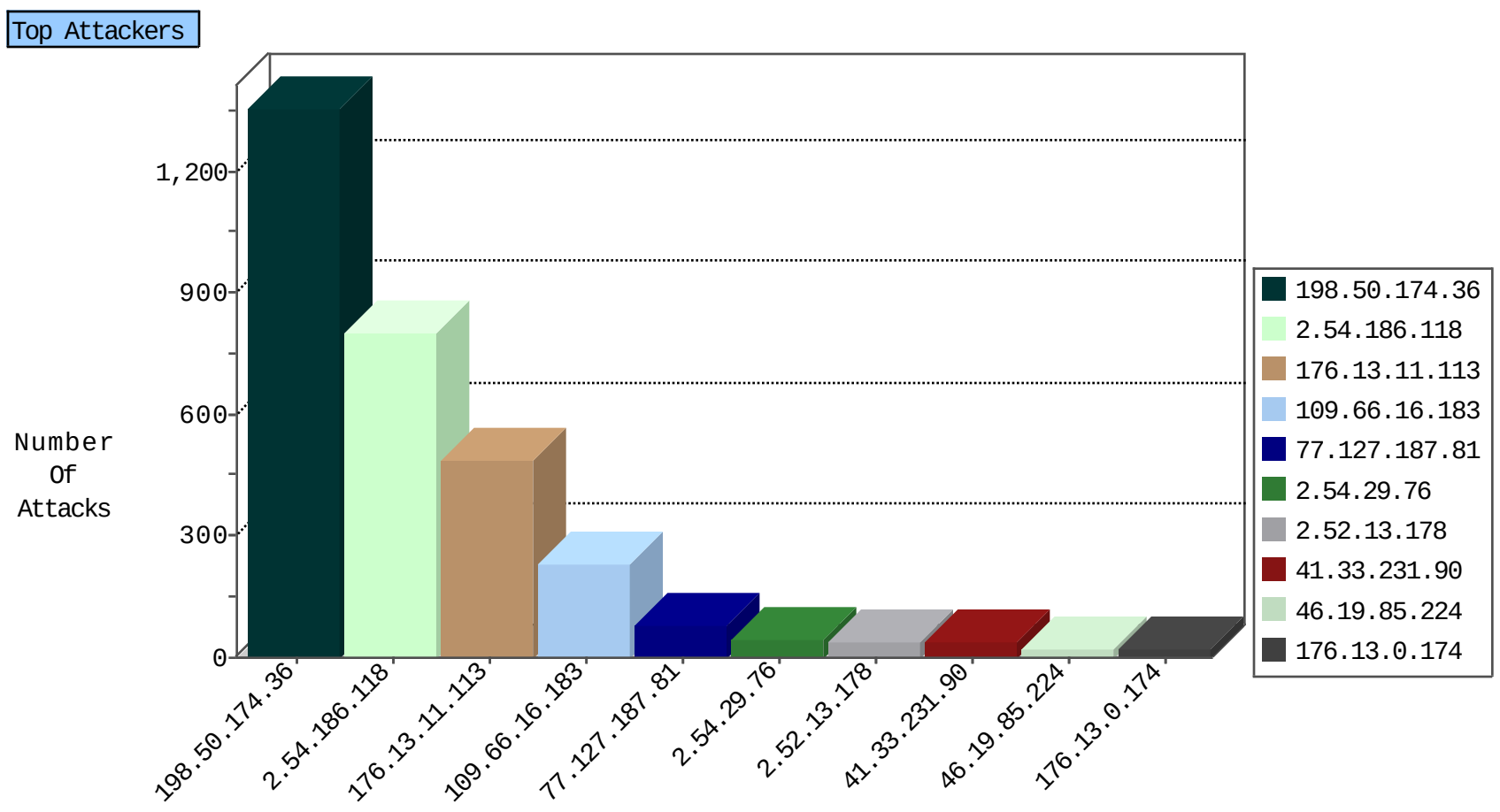
02-04-2016-22:04:01 to 02-04-2016-23:04:01

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-04-2016-22:04:01 to 02-04-2016-23:04:01

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	6
37.26.148.237	Israel	147.237.72.166	aka.idf.il	SYN Flood unverified cookie	drop	4
115.239.228.10	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
222.186.30.233	China	147.237.0.17	m.my-kosher-kravi.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
61.182.170.38	China	147.237.76.202	e.halag.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
177.4.179.20	Brazil	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
31.168.66.178	Israel	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
66.249.81.206	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
177.4.179.20	Brazil	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
66.249.93.180	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
185.130.5.201		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

02-04-2016-22:04:01 to 02-04-2016-23:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-04-2016-22:04:01 to 02-04-2016-23:04:01

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
80.246.137.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.76.42	Sweden	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
185.106.92.137	147.237.76.196		e.sviva.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
221.226.31.210	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -f -sS	1
183.3.202.115	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
221.6.32.82	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -f -sS	1
180.97.106.161	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
210.217.58.231	147.237.76.201	Korea, Republic of	e.atal.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
210.217.58.231	147.237.76.196	Korea, Republic of	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
210.217.58.231	147.237.76.38	Korea, Republic of	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
95.86.73.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.217.58.231	147.237.0.16	Korea, Republic of	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.76.34		yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.77.243	Sweden	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
61.182.170.38	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.137	147.237.76.196		e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
221.226.31.210	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
58.253.96.122	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
183.3.202.115	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
221.6.32.82	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
180.97.106.162	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.161	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
210.217.58.231	147.237.76.200	Korea, Republic of	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
210.217.58.231	147.237.76.44	Korea, Republic of	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -f -sS	1
210.217.58.231	147.237.76.34	Korea, Republic of	yohalan.idf.il	ET SCAN Potential SSH Scan	1
93.104.213.84	147.237.77.212	Germany	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1

02-04-2016-22:04:01 to 02-04-2016-23:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
198.50.174.36	Canada	147.237.72.156	aman.idf.il	SYN Attack		reject	372
198.50.174.36	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	346
198.50.174.36	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	216
198.50.174.36	Canada	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	200
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	198
198.50.174.36	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	115
198.50.174.36	Canada	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	104
77.127.187.81	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
46.19.85.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
2.52.2.205	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.86.150	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
31.168.68.54	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.131.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
62.128.45.204	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
79.179.116.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.157.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.228.50.193	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.16.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.37.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.81.49.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
31.168.172.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.131.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.194.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.39.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.198	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.128.175	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
109.186.172.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.182.129.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.211	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	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
79.182.129.18	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.26.149.151	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.137.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.152.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.129.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.179.154.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.2.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.200.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.46.39.243	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.80.158.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.224.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-04-2016-22:04:01 to 02-04-2016-23:04:01

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
2.54.60.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.129.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.186.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	450
2.54.186.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	244
176.13.11.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	235
176.13.11.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	144
2.54.186.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
176.13.11.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
2.54.29.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	46
2.52.13.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	40
176.13.0.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
176.13.20.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
87.69.113.127	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 87.69.113.127	Block	4
176.13.2.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.66.16.183	Block	3
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 109.66.16.183	Block	3
109.253.132.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 109.66.16.183	Block	3
84.109.112.133	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$50 in aka.idf.il/main/giyus/questionnaire.aspx	None	3
185.32.179.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 109.66.16.183	Block	2
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 109.66.16.183	Block	2
109.65.177.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 109.66.16.183	Block	2
46.19.86.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 109.66.16.183	Block	2
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 109.66.16.183	Block	2
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 109.66.16.183	Block	2
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 109.66.16.183 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
109.253.135.150	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 109.66.16.183	Block	2
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 109.66.16.183	Block	2
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1116-he/dover.aspx	Block	1
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 2F%2Fm.facebook.com%2F%22%5D; in URL _pk_id.20.8afc=894c6c0e6cf5f4e0.1448647152.4.1452800255.1452800247.	Block	1
217.132.241.90	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.46.36.68	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/international_training/transportation.asp	Block	1
87.68.43.96	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
79.177.162.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.66.16.183	Israel	147.237.72.166	aka.idf.il	NULL Character in URL	Block	1
54.251.144.191	Singapore	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /	Block	1
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Query String from 109.66.16.183	Block	1
46.19.85.15	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
192.198.151.36	Europe	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$6 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
80.179.78.82	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$4 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/video http:/www.youtube.com/v/tv4zoxi3kn	Block	1
37.46.36.68	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	1
176.228.50.193	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.178.30.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Too Many Headers per Request - 38 Headers	Block	1
66.249.65.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/927-he/atal.aspx	Block	1
109.66.2.228	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$103 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1