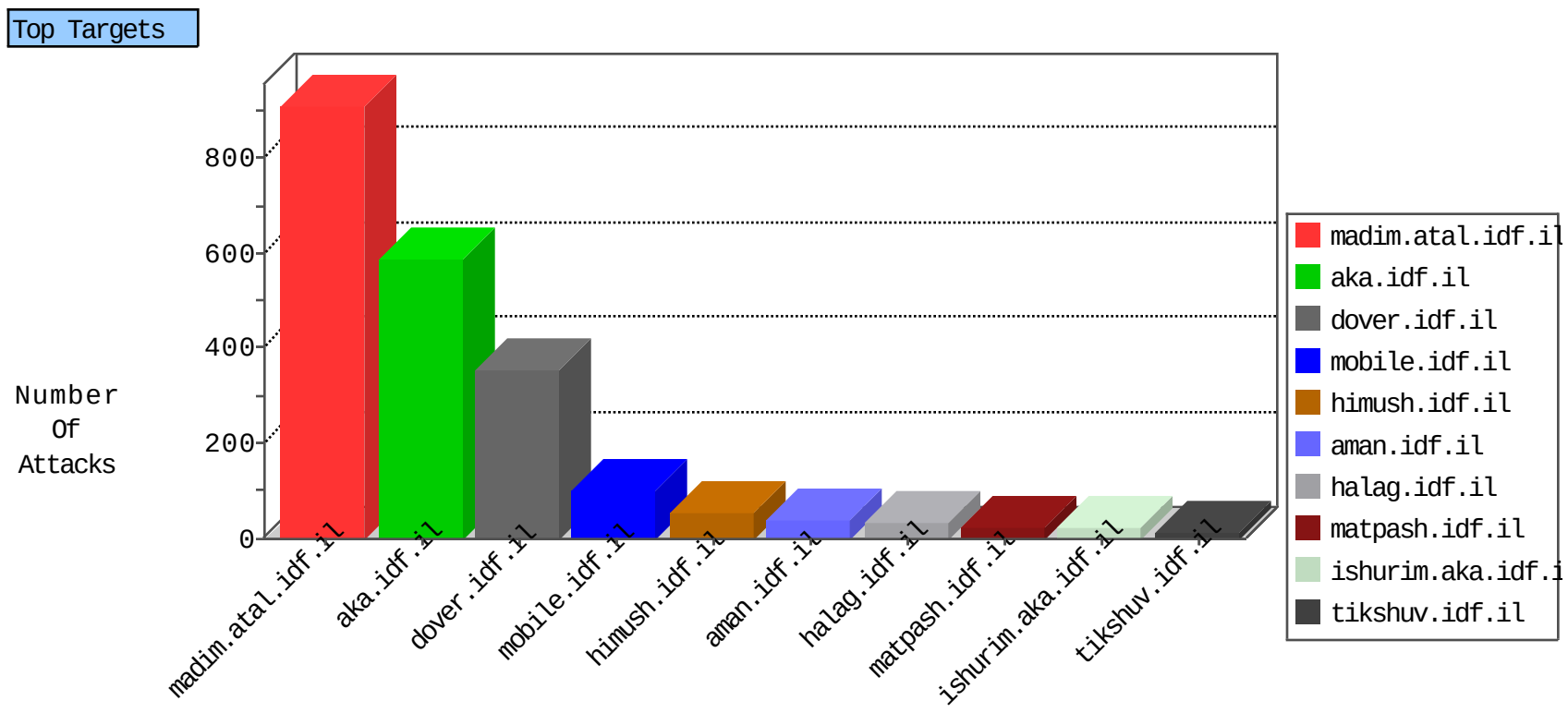
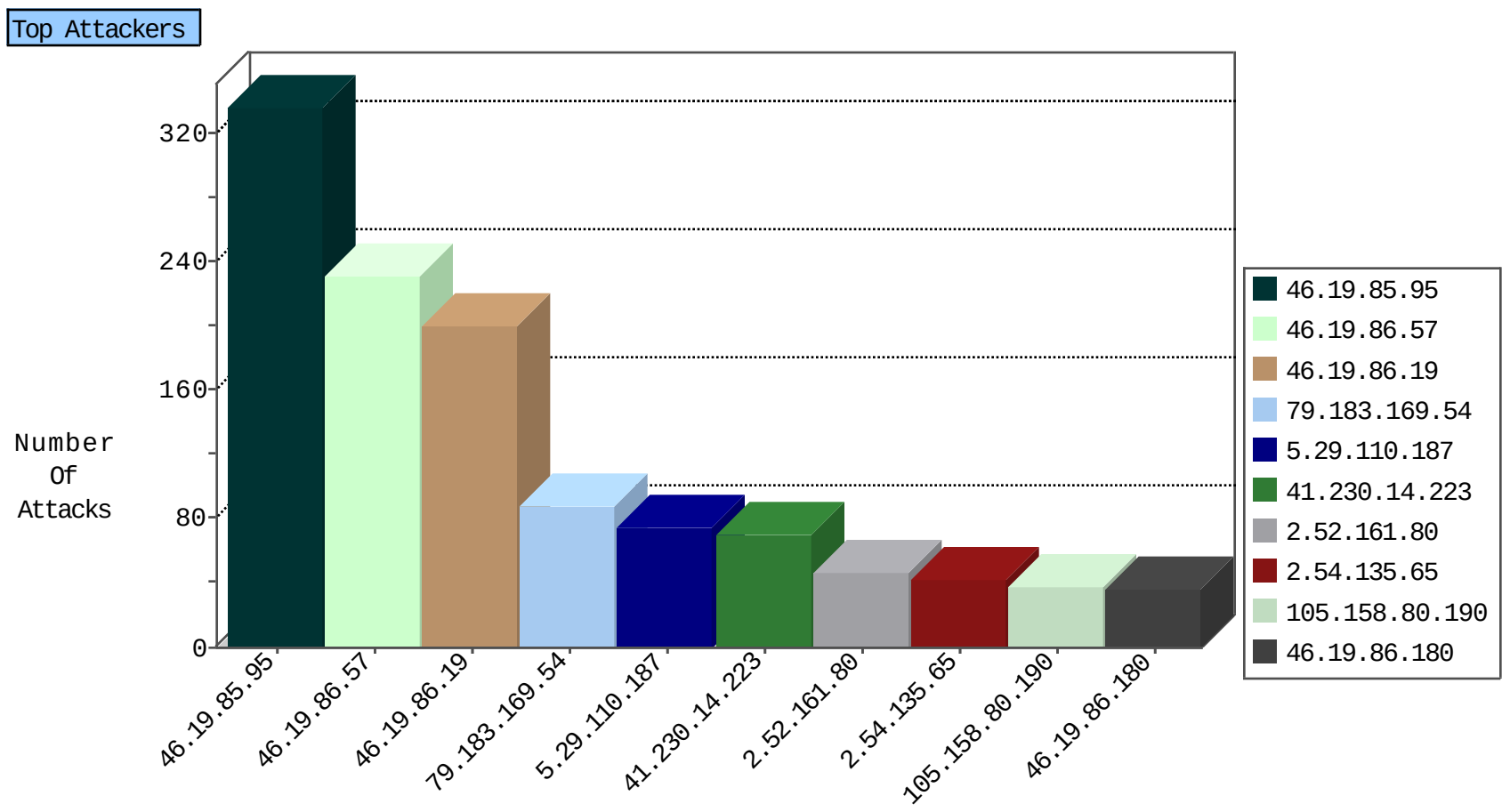
01-31-2016-20:04:03 to 01-31-2016-21:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-31-2016-20:04:03 to 01-31-2016-21:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.158.80.190	Morocco	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	361
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
105.158.80.190	Morocco	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
45.63.16.166		147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
74.91.28.59	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
89.248.174.4	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

01-31-2016-20:04:03 to 01-31-2016-21:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.236.231	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	4
84.111.188.224	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

01-31-2016-20:04:03 to 01-31-2016-21:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.198.103.11	147.237.77.74	China	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
202.198.103.11	147.237.72.166	China	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
202.198.103.11	147.237.77.205	China	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
202.198.103.11	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
105.158.80.190	147.237.77.216	Morocco	dover.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.81.198	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
202.198.103.11	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
125.71.233.191	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
202.198.103.11	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.186.7.69	147.237.76.30	Vietnam	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
202.198.103.11	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.167.1.5	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 4096	1
202.198.103.11	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.246.130.209	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
45.55.236.147	147.237.72.217		e.idf.il	ET SCAN NMAP -sS window 1024	1
202.198.103.11	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
202.198.103.11	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.198.103.11	147.237.77.176	China	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
125.71.233.191	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
202.198.103.11	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
125.71.233.191	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
202.198.103.11	147.237.76.177	China	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.198.103.11	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
104.167.1.5	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
202.198.103.11	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.198.103.11	147.237.72.156	China	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.29.3.100	147.237.77.216	Israel	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	1
222.170.70.222	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.198.103.11	147.237.77.243	China	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.198.103.11	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
202.198.103.11	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
149.88.140.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-31-2016-20:04:03 to 01-31-2016-21:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.230.14.223	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	67
2.52.161.80	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	46
79.183.169.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
82.145.209.81	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	31
79.176.161.107	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
109.75.78.2	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
31.210.183.85	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
109.253.203.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.180.3.33	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
2.54.135.65	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
79.183.169.54	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
2.54.135.65	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
46.19.85.146	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.183.169.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
79.183.169.54	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
84.228.97.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
79.182.201.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.18	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.115.248.2	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.183.169.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
79.180.2.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.44.162	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.26.148.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.46.39.243	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.181.142.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.71	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
82.81.55.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.38.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.210.187.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.38.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
2.52.5.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
94.230.86.145	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.178.125.208	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
80.246.136.46	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
79.178.125.208	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
79.178.125.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
5.29.3.100	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
5.102.254.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
105.158.80.190	Morocco	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	4
2.54.174.156	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.0.160	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.174.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

01-31-2016-20:04:03 to 01-31-2016-21:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	163
46.19.86.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	137
46.19.86.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	112
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.86.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	95
46.19.86.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
5.29.110.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	67
46.19.86.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
46.117.212.125	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	20
185.3.147.125	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	4
46.19.85.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
87.68.250.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.204.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.133.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.0.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.207.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
105.105.115.180	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
46.19.86.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.3.147.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
157.55.39.245	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/home/main/home/default.aspx	Block	2
109.253.212.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.3.147.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.139.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
149.78.141.169	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.228.235.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
94.230.86.159	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403	Block	2
79.180.3.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.29.75.31	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/registrationwizard/register.aspx parameter	None	2
31.154.154.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.172.159.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.127.147.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
182.118.55.166	China	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
46.117.66.233	Israel	147.237.77.233	atal.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 46.117.66.233	Block	1
157.55.39.103	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/home/main/home/default.aspx	Block	1
2.54.145.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.22.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.207.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.227.45	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.103.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.120.126.24		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.35	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
5.29.75.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-he/dover.aspx	Block	1
176.13.21.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.148.219	Israel	147.237.72.166	aka.idf.il	Unknown Parameter moduleToGoTo in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
84.228.5.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-31-2016-20:04:03 to 01-31-2016-21:04:03