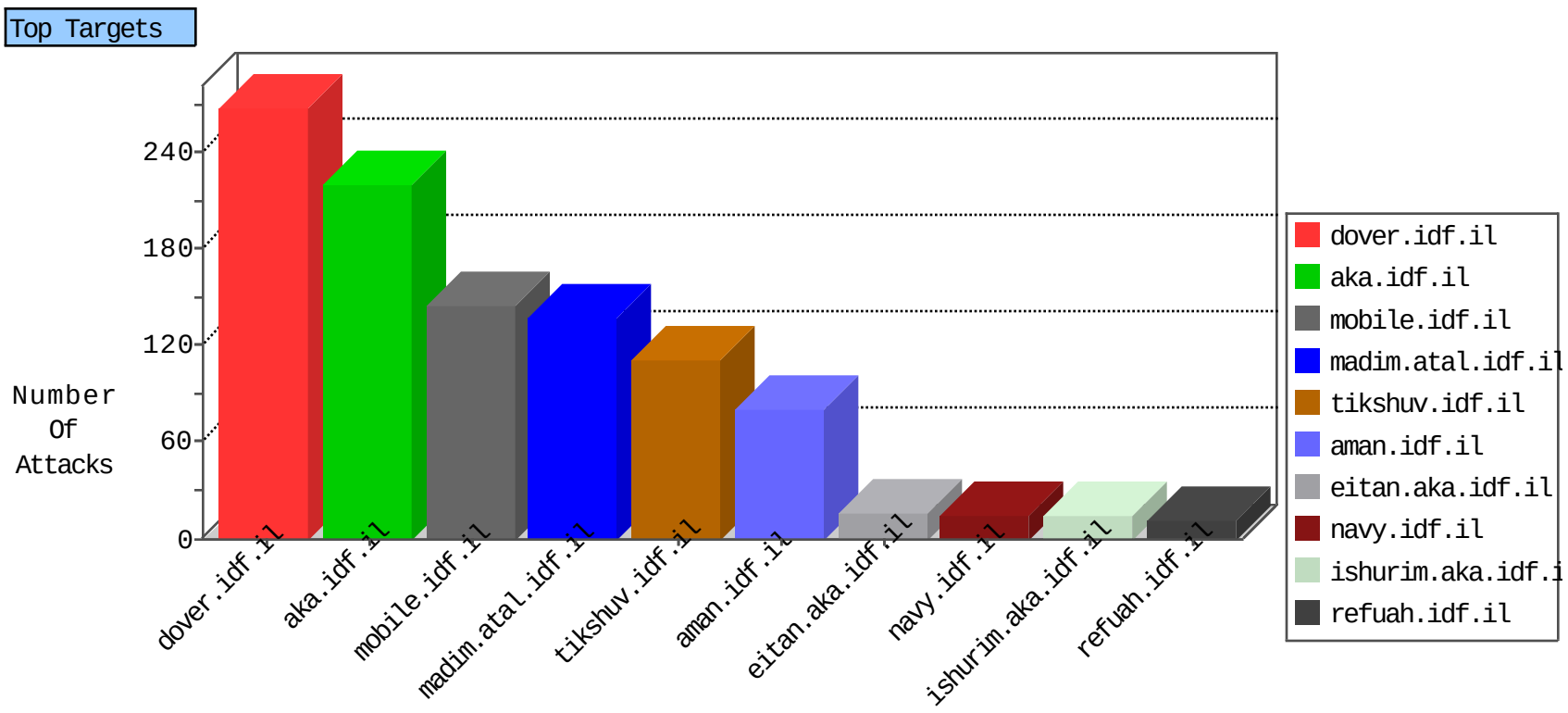
02-02-2016-21:04:01 to 02-02-2016-22:04:01

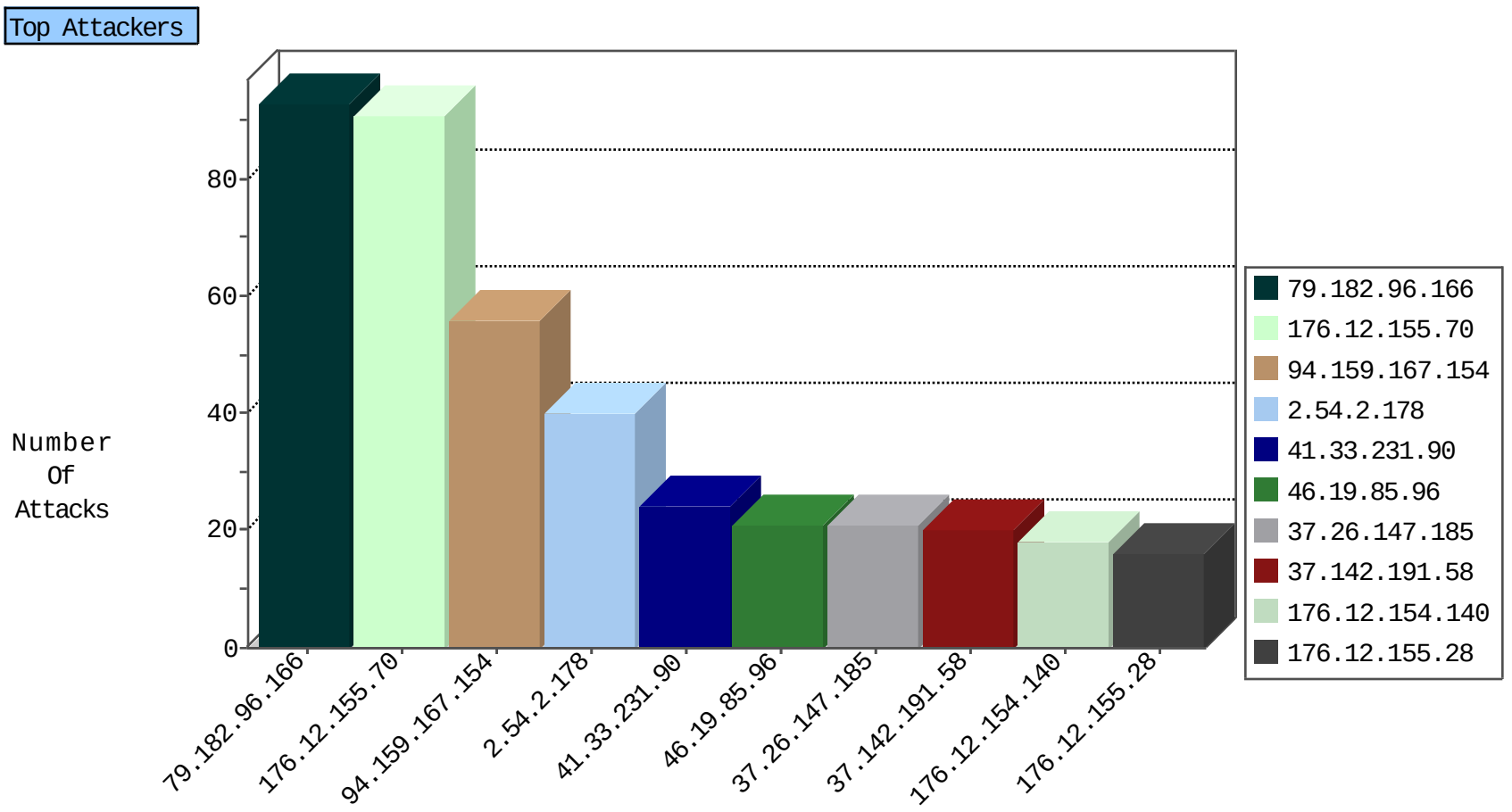
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-02-2016-21:04:01 to 02-02-2016-22:04:01

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	32
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
200.53.9.113	Brazil	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
142.54.169.165	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1
185.130.5.201		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
192.96.201.131	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

02-02-2016-21:04:01 to 02-02-2016-22:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-02-2016-21:04:01 to 02-02-2016-22:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
199.191.56.187	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	2
199.191.56.187	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	2
188.0.236.123	147.237.77.212	Moldova, Republic of	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
183.82.106.200	147.237.0.35	India	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
173.55.32.113	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
125.26.218.244	147.237.76.30	Thailand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.178.219.117	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.191.56.187	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
66.249.64.253	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
199.191.56.187	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.96	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.0.236.123	147.237.77.216	Moldova, Republic of	dover.idf.il	ET SCAN NMAP -sS window 1024	1
188.0.236.123	147.237.77.74	Moldova, Republic of	law.idf.il	ET SCAN NMAP -sS window 1024	1
183.82.106.200	147.237.0.35	India	akaws.idf.il	ET SCAN NMAP -f -sS	1
149.88.253.219	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.86.90.145	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.227.96	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.151.53.217	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
189.219.208.8	147.237.0.35	Mexico	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-02-2016-21:04:01 to 02-02-2016-22:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.182.96.166	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	93
94.159.167.154	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
94.159.167.154	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
37.26.147.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.142.191.58	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
2.54.2.178	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
2.52.54.124	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.25	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
79.177.225.225	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.12.155.28	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.2.178	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	10
109.64.138.126	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	9
81.218.197.25	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	8
217.132.12.193	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.52.152.55	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.149	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
94.230.86.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.177.208.83	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
89.138.127.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.211	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.61.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.49.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.120.206.165	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.2.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.182.228.228	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.2.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
31.210.187.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.54.2.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.3.147.226	Israel	147.237.72.156	aman.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
66.249.78.170	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.65.109.210	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
98.82.54.39	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
157.55.39.132	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.96	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.170	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
157.55.39.222	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.96	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.179.54.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.231.14.242	Kuwait	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.29.161.56	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
31.210.186.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

02-02-2016-21:04:01 to 02-02-2016-22:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.155.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
176.12.154.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
176.12.155.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
80.179.11.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
2.52.25.199	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	6
46.19.85.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
37.142.191.58	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.12.155.28	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.52.54.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.185	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.52.58.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
76.115.96.90	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.25	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.12.155.26	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
79.177.225.225	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.120.206.165	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
149.78.94.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.115	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	2
157.55.39.27	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/modiin/modiin/default.aspx	Block	2
109.64.9.254	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.64.9.254	Block	2
217.132.13.245	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
84.111.104.217	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
37.26.146.154	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
212.199.205.69	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
176.12.155.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Parameter Type Violation on madim.atal.idf.il/mobile/1088-he/meretz.aspx parameter ctl00$ContentPlaceHolder1$txtStreet	Block	1
46.120.19.161	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.64.9.254	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
5.29.161.56	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.181.113.82	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
66.249.66.126	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.66.126	Block	1
185.3.144.54	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
46.19.85.132	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method anguage: in URL he-il,he	Block	1
89.138.127.36	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.57.57.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.175.0.137	Germany	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/shared/usercontrols/headerupper/	Block	1
79.183.141.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.82	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
198.58.102.155	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
176.12.154.140	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
89.139.35.34	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
2.54.129.155	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.57.164.188	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.176.106.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.253	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
149.78.206.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
23.95.40.53	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/rk=0/rs=8syg0mmqekqpzw9ooh4bhisoqii-	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/elram	Block	1
212.76.99.52	Israel	147.237.72.166	aka.idf.il	Unknown Parameter sa in www.aka.idf.il/main/rabanut/general.aspx	None	1

02-02-2016-21:04:01 to 02-02-2016-22:04:01