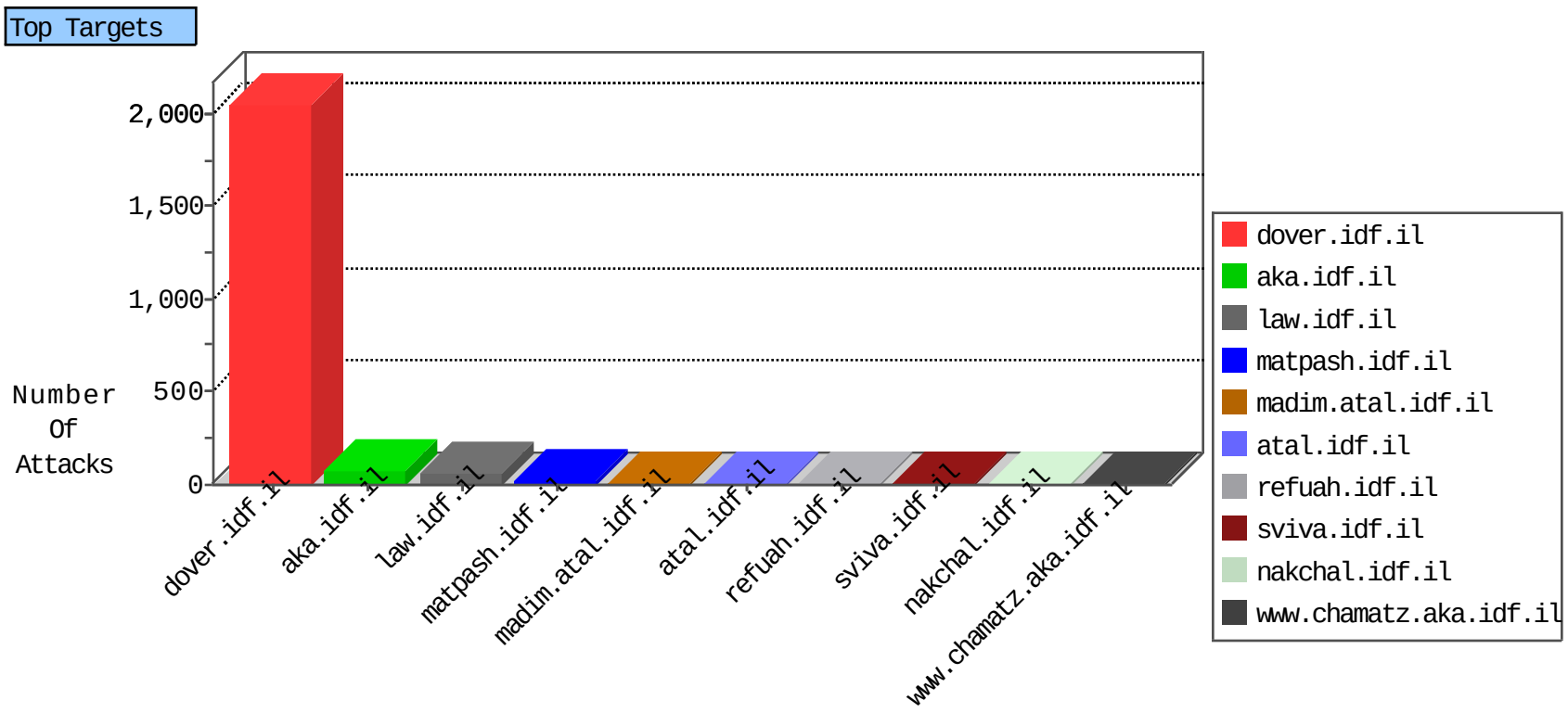
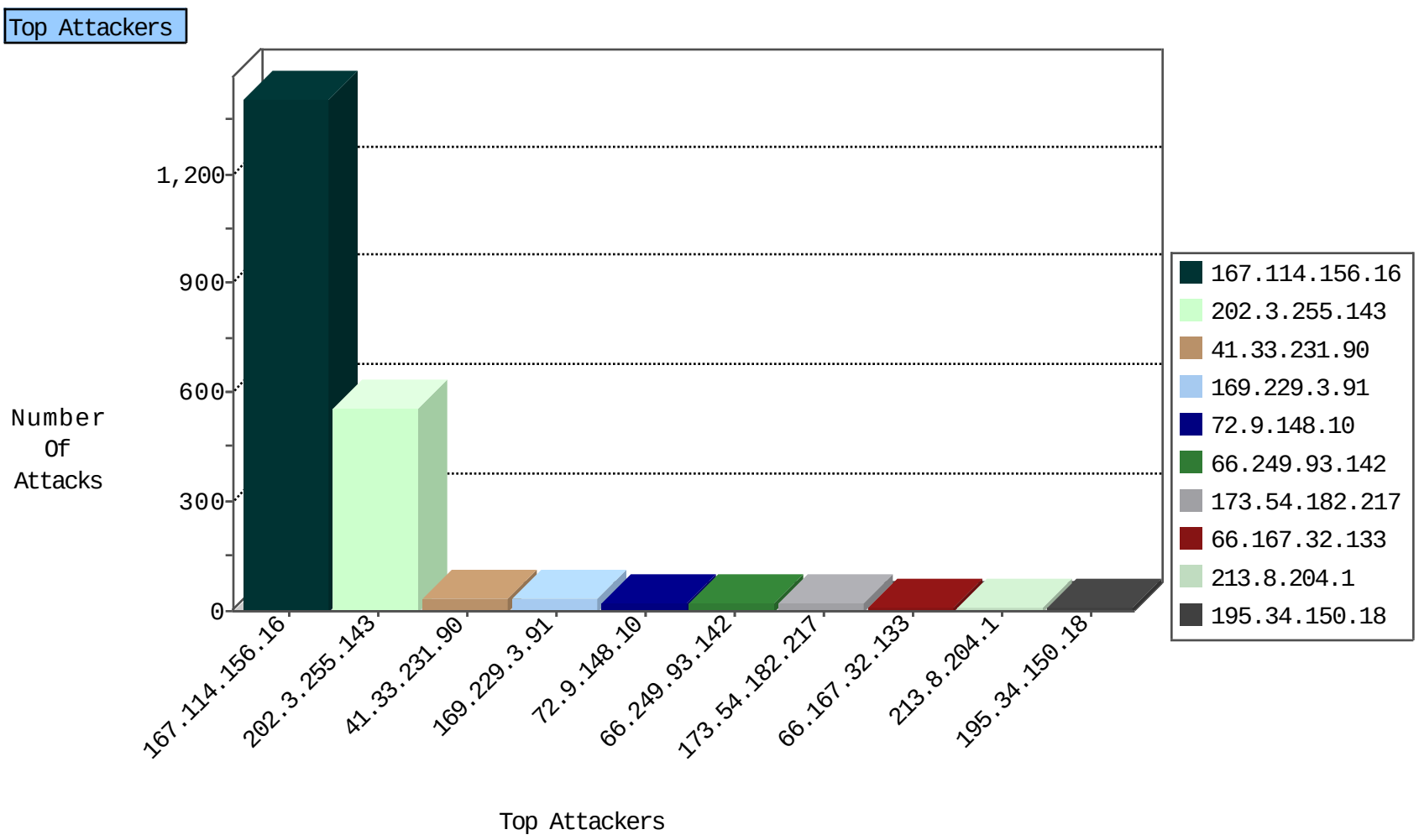
01-18-2016-01:06:50 to 01-18-2016-02:06:50

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-18-2016-01:06:50 to 01-18-2016-02:06:50

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3004
106.85.76.186	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
171.83.32.145	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

01-18-2016-01:06:50 to 01-18-2016-02:06:50

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.96.128.60	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
184.173.233.226	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
195.140.210.83	Germany	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
216.249.107.200	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

01-18-2016-01:06:50 to 01-18-2016-02:06:50

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	520
66.96.128.60	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
216.249.107.200	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	3
184.173.233.226	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	3
191.240.136.5	147.237.77.226	Brazil	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
191.240.136.5	147.237.76.199	Brazil	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
187.160.190.9	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.248.172.140	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
72.228.149.143	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
191.240.136.5	147.237.76.200	Brazil	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
187.160.190.9	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
72.228.149.143	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1

01-18-2016-01:06:50 to 01-18-2016-02:06:50

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	24
66.249.93.142	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	20
173.54.182.217	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
213.8.204.1	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	10
66.167.32.133	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
173.54.182.217	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
66.249.93.148	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
109.253.195.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
109.186.13.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.182.148.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.188.113	Israel	147.237.77.216	dover.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
212.76.127.10	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
212.76.127.44	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
176.13.18.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
79.180.241.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.219.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.177.58	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
80.178.150.48	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
157.55.39.225	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.52.163.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.93.145	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
5.22.135.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
180.76.15.22	China	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.102.254.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
204.79.180.181	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
178.255.215.87	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.203	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.243.31.2	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.46.39.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.88	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.154.226.90	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
79.179.177.58	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.91	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.84	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
178.255.215.87	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
84.94.190.248	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
73.245.195.227	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.204	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.243.31.2	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.89	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
201.195.147.154	Costa Rica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
173.236.152.135	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
79.179.177.58	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.143.25	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	4
66.167.32.133	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	3
46.19.86.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.189.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.143.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.1.207.7	Netherlands	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/1/3191.pdf'	Block	2
96.228.26.234	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Malformed URL >Â¿[[#18]]Âœ[[#26]]×©	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
2.54.160.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.156	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/sip_storage/files/7/1437.pdf/	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
180.76.15.22	China	147.237.77.234	halag.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Illegal Byte Code Character in Header Name	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple Illegal Byte Code Character in URL from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Unknown HTTP Request Method Ã®PIÃ¸Ã p[[#29]]I(Âª9^[[#17]]Â¯Â¶[[#7]][[#24]]Ã¦<Ã¯WÃœA in URL >Â¿[[#18]]Âœ[[#26]]×©	Block	1
96.228.26.234	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
208.90.57.196	United States	147.237.77.170	maarachot.idf.il	URL is Above Root Directory maarachot.idf.il/../../	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Multiple Malformed URL from 169.229.3.91	Block	1
185.25.148.240	Poland	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
109.253.192.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Illegal Byte Code Character in Method Ã®PIÃ¸Ã p[[#29]]I(Âª9^[[#17]]Â¯Â¶[[#7]][[#24]]Ã¦<Ã¯WÃœA	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple NULL Character in Method from 169.229.3.91	Block	1
46.120.221.187	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
169.229.3.91	United States	147.237.76.30	himush.idf.il	NULL Character in Method	Block	1
207.46.13.44	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/&sa=u&ved=0ca0qfjaaahukewij6_kykpfgahwjxhqkhvtgdnu&sig2=ndaz6msozbm1ftpnczrgha&usg=afqjcnhcdsh5ryhkeugapxldsq7fowjwnw	Block	1
173.54.182.217	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 173.54.182.217	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Multiple Illegal Byte Code Character in URL from 169.229.3.91	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
5.102.254.99	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_CERTIFICATE_REQUEST)	None	1
217.69.136.204	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
129.45.62.93		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/:85/airforce/homepage.aspx	Block	1
195.154.194.111	France	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Illegal Byte Code Character in URL >Â¿[[#18]]Âœ[[#26]]×©	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
62.210.226.9	France	147.237.72.156	aman.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Abnormally Long Request method	Block	1
207.46.13.94	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/horaot	Block	1
173.54.182.217	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/×§×ž×¢	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1