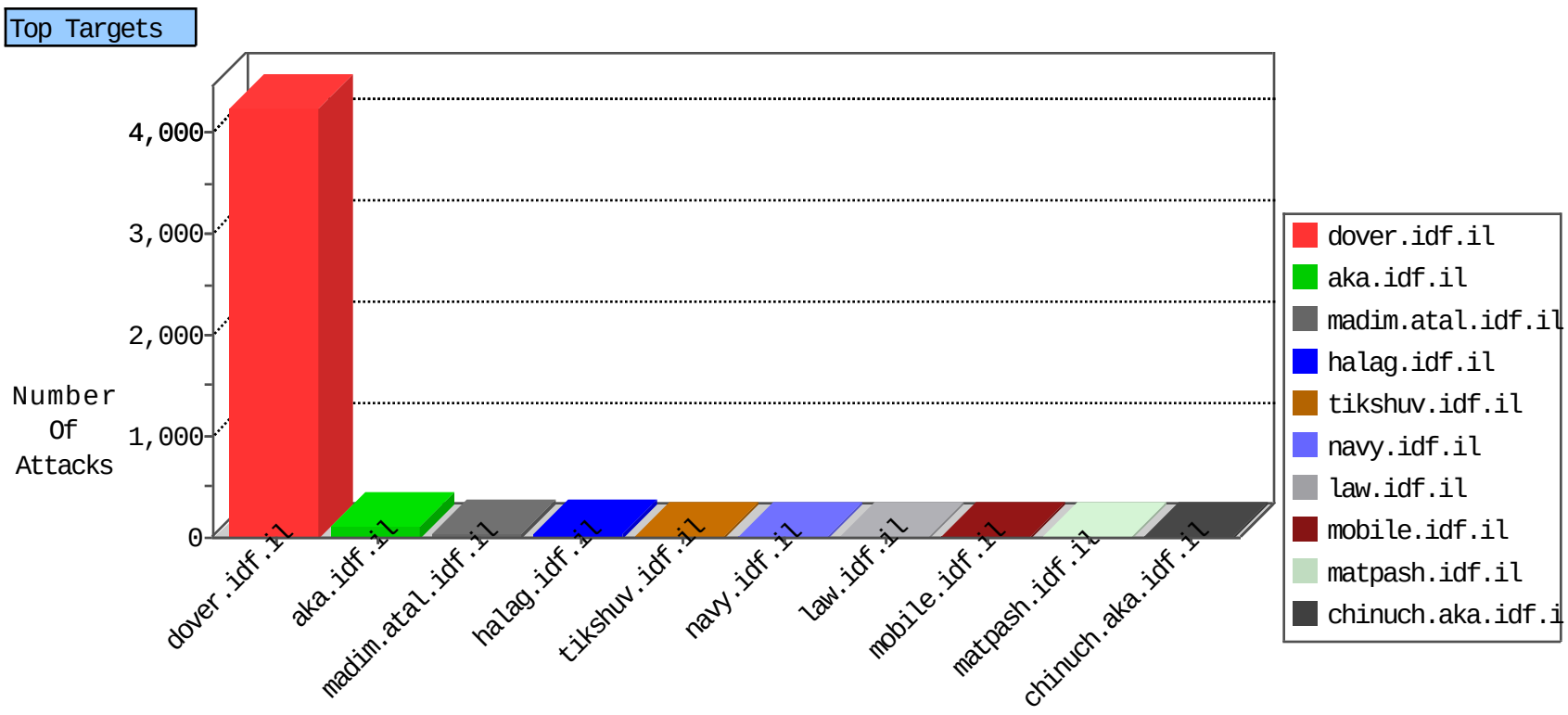
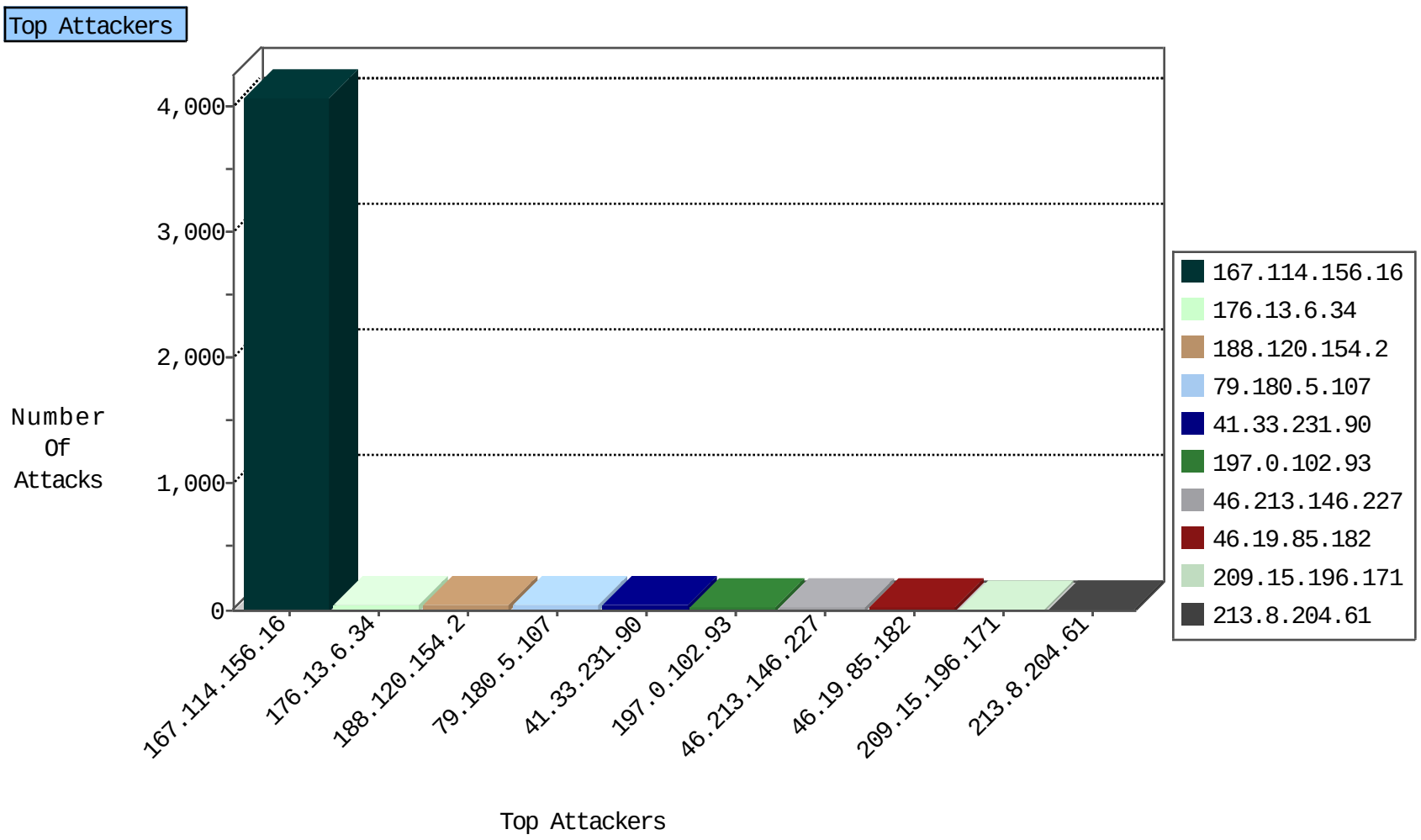
04-14-2016-01:09:05 to 04-14-2016-02:09:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-14-2016-01:09:05 to 04-14-2016-02:09:05

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	Block_Ip_Web_In	drop	4060
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
80.82.78.38	Netherlands	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
80.82.78.38	Netherlands	147.237.77.74	law.idf.il	block-sp-traf1	forward	2
94.102.49.116	Netherlands	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
115.235.144.50	China	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1

04-14-2016-01:09:05 to 04-14-2016-02:09:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.204.61	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	13
61.135.189.114	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
62.210.148.246	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
197.0.102.93	Tunisia	147.237.77.216	dover.idf.il	2809: HTTP: IIS TRACK Method	Block	2
193.109.69.219	Russian Federation	147.237.77.216	dover.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
197.0.102.93	Tunisia	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1
197.0.102.93	Tunisia	147.237.77.216	dover.idf.il	0361: HTTP: Protected File Access (/etc/passwd)	Block	1
66.249.66.154	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	1
197.0.102.93	Tunisia	147.237.77.216	dover.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
66.249.66.158	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	1
197.0.102.93	Tunisia	147.237.77.216	dover.idf.il	19690: HTTP: Microsoft IIS Integer Overflow Vulnerability	Block	1
41.37.188.107	Egypt	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-14-2016-01:09:05 to 04-14-2016-02:09:05

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
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
98.119.105.221	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
80.82.78.38	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
50.62.137.87	147.237.77.176	United States	matpash.idf.il	SERVER-WEBAPP Mambo upload.php access	1
198.20.69.74	147.237.77.235	United States	sviva.idf.il	ET DROP Dshield Block Listed Source	1
197.0.102.93	147.237.77.216	Tunisia	dover.idf.il	GPL WEB_SERVER TRACE attempt	1
197.0.102.93	147.237.77.216	Tunisia	dover.idf.il	ET DOS SSL Bomb DoS Attempt	1
128.199.63.237	147.237.77.216	Netherlands	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
98.119.105.221	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
88.148.116.169	147.237.0.33	Spain	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.4.79.76	147.237.77.235	Germany	sviva.idf.il	ET SCAN Potential SSH Scan	1
197.0.102.93	147.237.77.216	Tunisia	dover.idf.il	SERVER-WEBAPP TRACE attempt	1
197.0.102.93	147.237.77.216	Tunisia	dover.idf.il	GPL WEB_SERVER /etc/passwd	1

04-14-2016-01:09:05 to 04-14-2016-02:09:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.120.154.2	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.180.5.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
209.15.196.171	Canada	147.237.72.166	aka.idf.il	drop	SAM rule	drop	16
46.213.146.227	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
46.213.146.227	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
197.0.102.93	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
77.126.43.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.182	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
87.69.23.35	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
84.95.208.20	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
46.19.85.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
46.19.85.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.182	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.3.147.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.208	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.242.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
93.172.3.19	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.66.50	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.255.253.94	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.33.101.151	Italy	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
113.91.64.70	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
113.91.64.70	China	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	2
197.0.102.93	Tunisia	147.237.77.216	dover.idf.il	SSL Enforcement Violation	TLS Servers Cipher Suites Vulnerability Scanning Tools	reject	2
77.237.138.202	Czech Republic	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
157.55.39.234	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.22.131.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.64.182.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.26.148.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
197.0.102.93	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
61.135.189.114	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.193	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.46.39.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.192	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.148.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
94.230.86.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
80.82.78.38	Netherlands	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.3.147.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.201	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
120.132.68.87	China	147.237.76.34	yohalan.idf.il	drop		drop	1
77.240.96.200	Czech Republic	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
159.226.95.66	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.192	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.148.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
106.186.113.132	Japan	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

04-14-2016-01:09:05 to 04-14-2016-02:09:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.6.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.188.30.189	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
46.188.30.189	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.188.30.189	Block	5
109.253.214.71	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
79.176.86.19	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
46.32.124.228	Jordan	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	2
157.55.39.234	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/news/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/default.asp	Block	1
197.0.102.93	Tunisia	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
85.143.21.13	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
2.25.118.198	United Kingdom	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1393-en/dover.aspx	Block	1
46.188.30.189	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
197.0.102.93	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/rails/info/properties/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/resources/common/topakamenu/styles/dinamicmenu.css	Block	1
45.55.182.56	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	1
185.77.91.113	Turkey	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/index.php	Block	1
79.180.5.107	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;list in www.aka.idf.il/kamlar/klali/default.asp	None	1
50.62.137.87	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
197.0.102.93	Tunisia	147.237.77.216	dover.idf.il	Unknown HTTP Request Method NETSPARKER in URL www.idf.il/ar/	Block	1
113.91.64.70	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/ishurim/exampcert/	Block	1
188.120.154.2	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
80.82.78.38	Netherlands	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.baidu.com/cache/global/img/gs.gif	Block	1
50.62.137.87	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-content/themes/geoplaces3/library/includes/upload.php	Block	1
2.25.118.198	United Kingdom	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
157.55.39.234	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.234	Block	1
68.180.230.184	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1397-he/atal.aspx	Block	1
197.0.102.93	Tunisia	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 197.0.102.93	Block	1
80.82.78.38	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to www.baidu.com/cache/global/img/gs.gif	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
2.25.118.198	United Kingdom	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1393-en/dover.aspx	Block	1

04-14-2016-01:09:05 to 04-14-2016-02:09:05