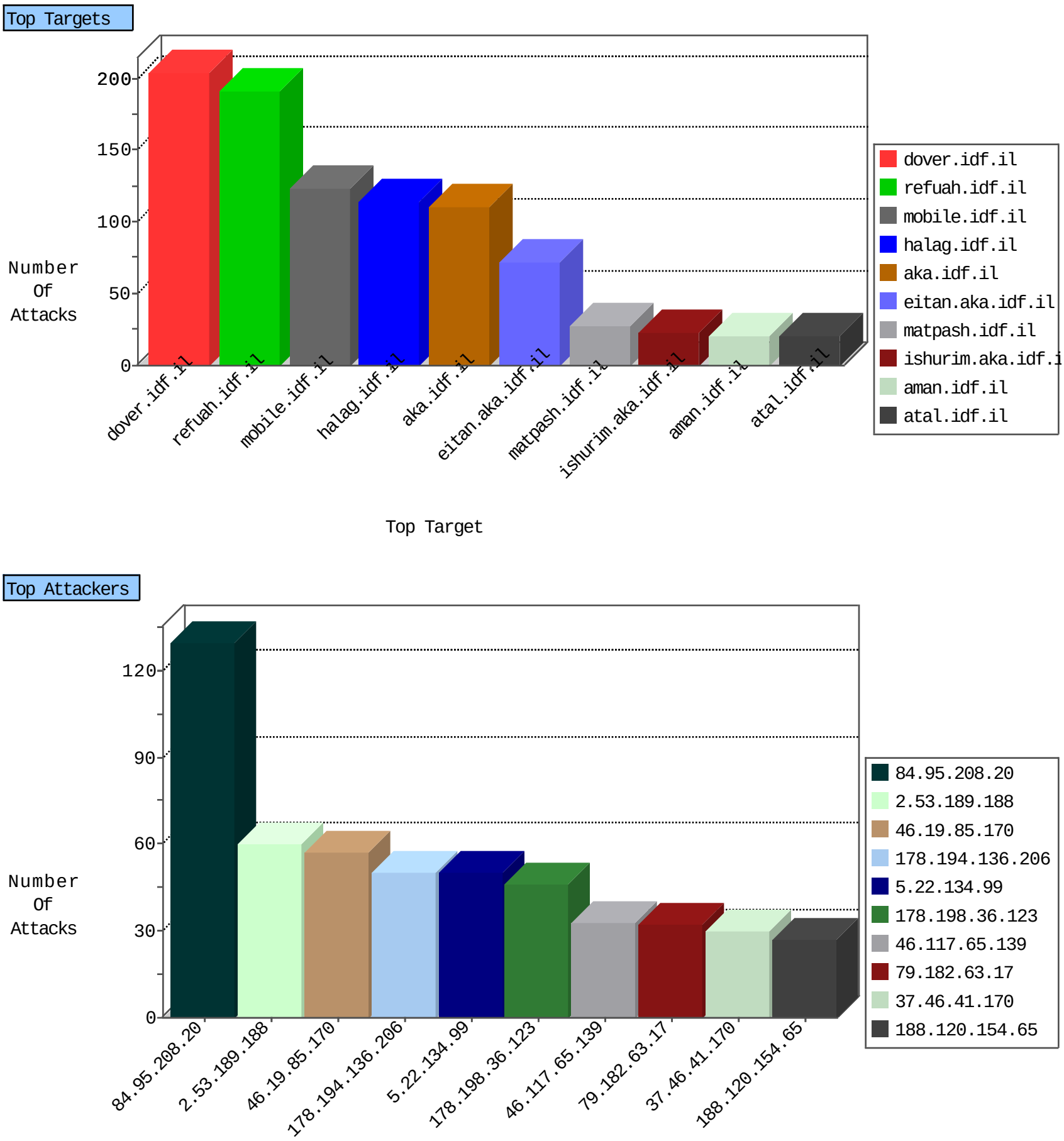
10-02-2016-12:04:07 to 10-02-2016-13:04:07

IDF Under Attack Daily Report



10-02-2016-12:04:07 to 10-02-2016-13:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.3	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
77.127.88.151	Israel	147.237.76.86	navy.idf.il	Black List	drop	1
212.235.72.236	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

10-02-2016-12:04:07 to 10-02-2016-13:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
220.181.125.23	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
82.193.127.15	Ukraine	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1

10-02-2016-12:04:07 to 10-02-2016-13:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
183.80.241.119	147.237.77.234	Vietnam	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
154.16.199.48	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
121.228.232.4	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
62.150.255.205	147.237.76.198	Kuwait	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
219.146.251.139	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
62.150.255.205	147.237.76.198	Kuwait	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
219.146.251.139	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.40.4.208	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
154.16.199.48	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
122.72.53.188	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
118.68.121.191	147.237.76.197	Vietnam	e.himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
62.150.255.205	147.237.76.198	Kuwait	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
219.146.251.139	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
14.223.95.127	147.237.76.177	China	ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.40.4.208	147.237.76.198	Russian Federation	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

10-02-2016-12:04:07 to 10-02-2016-13:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
2.53.189.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
5.22.134.99	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
79.182.63.17	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
46.117.65.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
37.46.41.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
188.120.154.65	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
46.19.85.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
46.19.85.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
101.127.180.93	Singapore	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
79.178.195.12	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
46.19.85.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
178.194.136.206	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	11
178.194.136.206	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
178.198.36.123	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
178.194.136.206	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
178.194.136.206	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	10
178.198.36.123	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	10
178.198.36.123	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	9
178.194.136.206	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
178.198.36.123	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
92.241.50.247	Jordan	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
185.32.179.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
178.198.36.123	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
82.102.169.113	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
79.181.9.171	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
109.253.209.104	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
182.232.48.114	Thailand	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.56.58	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
176.13.0.49	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.102.169.113	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.29	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
5.22.134.99	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.146.246	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
70.208.234.72	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
100.92.127.225		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
208.102.217.93	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.43.87.189	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.126.13.245	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
128.77.112.110	Denmark	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.67.122.99	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.248	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
5.28.179.139	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
185.32.179.17	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

10-02-2016-12:04:07 to 10-02-2016-13:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	46
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	7
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	4
185.32.179.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.52	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.79.20	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
2.53.33.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
87.69.100.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
82.166.140.117	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1362-he/cogat.aspx/	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	1
220.181.125.23	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-8741-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	NULL Character in Method	Block	1
68.180.228.60	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation PageNum in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	1
5.22.134.99	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.253.209.104	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.94.84.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/site/templates/controller.asp	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Abnormally Long Request method	Block	1
77.125.17.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl33 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
188.120.154.65	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
31.168.82.94	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/apple-app-site-association	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
77.138.146.172	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
195.189.227.31	Ukraine	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in Header Name User-Agent Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method	Block	1
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter tab in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
66.249.65.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8833-he/refuah.aspx	Block	1
176.13.0.49	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.111.157.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.117.65.139	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
220.181.125.23	China	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 220.181.125.23	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Method	Block	1

10-02-2016-12:04:07 to 10-02-2016-13:04:07