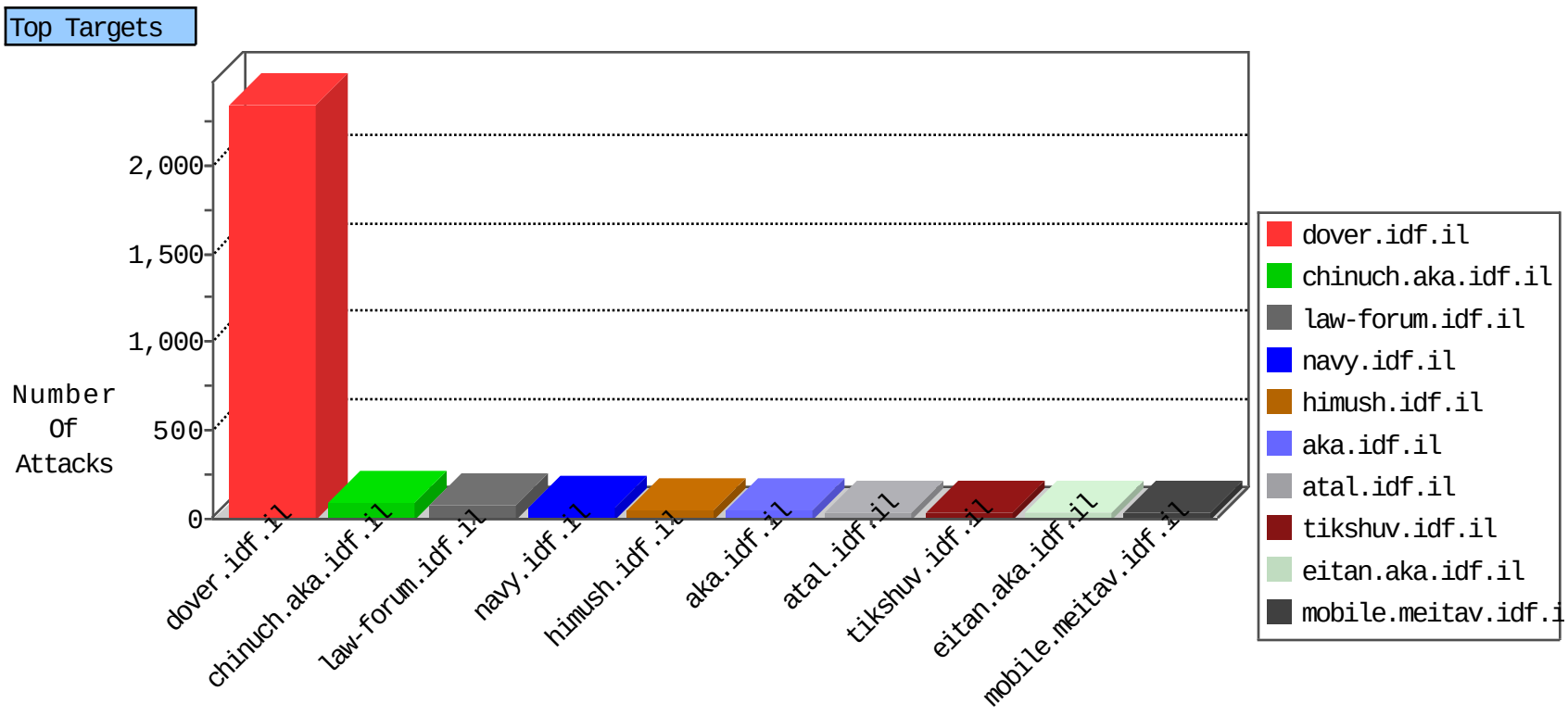
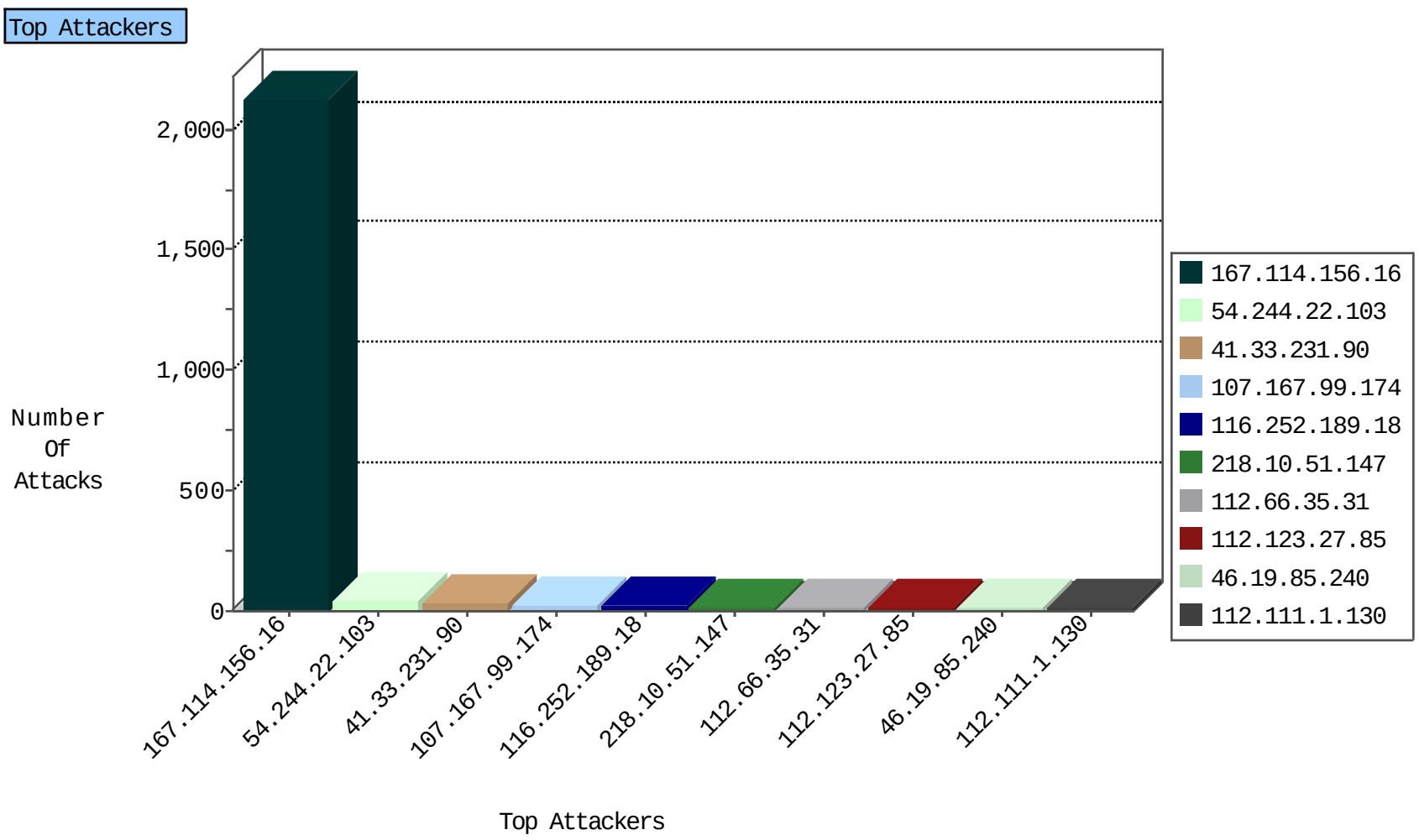
01-23-2016-03:04:01 to 01-23-2016-04:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-23-2016-03:04:01 to 01-23-2016-04:04:01

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	3043
74.91.28.61	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
204.42.253.132	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

01-23-2016-03:04:01 to 01-23-2016-04:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
14.104.187.41	China	147.237.77.19	law-forum.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
219.156.101.159	China	147.237.76.30	himush.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
112.66.44.117	China	147.237.77.233	atal.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
180.110.203.139	China	147.237.76.30	himush.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
51.254.143.240	United Kingdom	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
112.111.1.130	China	147.237.76.200	eitan.aka.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
198.50.134.71	Canada	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
106.7.248.43	China	147.237.77.19	law-forum.idf.il	C155: HTTP: OPTIONS methods	Permit	1
116.113.74.159	China	147.237.76.147	chinuch.aka.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
218.10.51.147	China	147.237.76.200	eitan.aka.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
106.7.249.234	China	147.237.77.216	dover.idf.il	C155: HTTP: OPTIONS methods	Permit	1
119.108.155.135	China	147.237.76.39	mobile.meitav.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
218.10.62.192	China	147.237.76.147	chinuch.aka.idf.il	C155: HTTP: OPTIONS methods	Permit	1
112.66.35.31	China	147.237.76.86	navy.idf.il	C155: HTTP: OPTIONS methods	Permit	1
172.245.218.130	United States	147.237.76.42	refuah.idf.il	0543: HTTP: php.cgi Access	Block	1

01-23-2016-03:04:01 to 01-23-2016-04:04:01

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	2
112.123.27.63	147.237.77.19	China	law-forum.idf.il	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	1
112.94.190.179	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
222.75.35.43	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	1
111.162.159.226	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
59.174.44.231	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	1
190.249.184.162	147.237.76.197	Colombia	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
58.249.26.241	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
146.185.250.2	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.165.215	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
122.139.83.222	147.237.76.86	China	navy.idf.il	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	1
112.123.27.85	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	1
112.111.1.130	147.237.77.233	China	atal.idf.il	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	1
222.94.97.91	147.237.77.205	China	prisha.idf.il	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	1
112.66.35.31	147.237.77.233	China	atal.idf.il	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	1
195.216.176.244	147.237.8.14	Latvia	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
61.155.203.54	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
190.249.184.162	147.237.76.197	Colombia	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
59.174.44.116	147.237.77.205	China	prisha.idf.il	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	1
183.160.231.174	147.237.76.86	China	navy.idf.il	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	1
58.20.99.149	147.237.76.30	China	himush.idf.il	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	1
125.211.38.205	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
123.139.16.244	147.237.76.30	China	himush.idf.il	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	1
119.81.188.158	147.237.77.121	Hong Kong	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1

01-23-2016-03:04:01 to 01-23-2016-04:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	32
107.167.99.174	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.240	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	9
157.55.39.169	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.114	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
157.55.39.168	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.225.59.72	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.39.89	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
207.46.13.152	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.241.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
199.30.25.42	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
97.93.201.229	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.29.72.172	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.253	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.240	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
40.77.167.102	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
90.174.2.57	Spain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.46.13.136	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.102.254.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.254	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.78.153	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
81.169.237.146	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	2
221.204.146.130	China	147.237.77.205	prisha.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
5.29.72.172	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
116.113.73.198	China	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
58.20.99.14	China	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
111.162.156.170	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.240	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
109.253.198.146	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
122.96.23.0	China	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.203	United States	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.46.39.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
85.10.210.199	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
116.252.189.23	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
171.25.193.25	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
222.94.96.113	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
62.102.148.67	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
113.135.99.80	China	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1

01-23-2016-03:04:01 to 01-23-2016-04:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
172.245.218.130	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 172.245.218.130	Block	3
116.252.189.18	China	147.237.76.147	chinuch.aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	3
116.252.189.18	China	147.237.76.147	chinuch.aka.idf.il	Distributed NULL Character in Method	Block	3
171.107.26.204	China	147.237.77.19	law-forum.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
111.162.153.129	China	147.237.77.19	law-forum.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
118.81.5.37	China	147.237.77.19	law-forum.idf.il	Distributed NULL Character in Method	Block	2
117.36.21.253	China	147.237.76.147	chinuch.aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
112.66.35.31	China	147.237.76.86	navy.idf.il	Distributed NULL Character in Method	Block	2
111.162.153.129	China	147.237.77.19	law-forum.idf.il	Distributed NULL Character in Method	Block	2
117.36.21.253	China	147.237.76.147	chinuch.aka.idf.il	Distributed NULL Character in Method	Block	2
118.81.5.37	China	147.237.77.19	law-forum.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
124.126.222.196	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	2
112.66.35.31	China	147.237.76.86	navy.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
185.32.179.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
59.174.46.101	China	147.237.76.30	himush.idf.il	Illegal HTTP Version RTSP/1.0	Block	1
111.85.179.212	China	147.237.77.216	dover.idf.il	Distributed NULL Character in Method	Block	1
112.111.1.130	China	147.237.76.147	chinuch.aka.idf.il	Distributed NULL Character in Method	Block	1
116.113.73.246	China	147.237.76.86	navy.idf.il	Distributed NULL Character in Method	Block	1
123.139.24.149	China	147.237.77.19	law-forum.idf.il	Distributed Unknown HTTP Request Method	Block	1
218.10.51.147	China	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
112.66.36.79	China	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Header Name	Block	1
113.240.194.190	China	147.237.77.19	law-forum.idf.il	Distributed Abnormally Long Request	Block	1
118.81.5.37	China	147.237.77.19	law-forum.idf.il	Distributed NULL Character in Header Name	Block	1
157.55.39.114	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/procedure.asp	Block	1
219.156.101.159	China	147.237.77.19	law-forum.idf.il	Distributed Unknown HTTP Request Method	Block	1
112.123.27.85	China	147.237.76.86	navy.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
116.252.190.91	China	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/status	Block	1
125.211.38.117	China	147.237.76.86	navy.idf.il	Distributed NULL Character in Method	Block	1
219.156.101.159	China	147.237.76.86	navy.idf.il	Distributed Abnormally Long Request	Block	1
58.20.99.149	China	147.237.76.147	chinuch.aka.idf.il	Distributed Unknown HTTP Request Method	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
112.66.45.175	China	147.237.76.147	chinuch.aka.idf.il	Distributed NULL Character in Header Name	Block	1
115.204.92.71	China	147.237.76.30	himush.idf.il	Distributed NULL Character in Method	Block	1
123.139.22.167	China	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
180.109.231.108	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
222.75.35.251	China	147.237.76.86	navy.idf.il	Distributed Unknown HTTP Request Method	Block	1
61.52.62.177	China	147.237.76.147	chinuch.aka.idf.il	Distributed Abnormally Long Request	Block	1
112.66.35.31	China	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
222.75.35.114	China	147.237.76.147	chinuch.aka.idf.il	Distributed Illegal HTTP Version	Block	1
60.216.138.149	China	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
111.162.153.129	China	147.237.77.233	atal.idf.il	NULL Character in Method	Block	1
112.123.27.85	China	147.237.76.39	mobile.meitav.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
116.252.189.18	China	147.237.76.200	eitan.aka.idf.il	Distributed Illegal HTTP Version	Block	1
125.118.7.155	China	147.237.76.147	chinuch.aka.idf.il	Distributed Malformed URL	Block	1
218.10.51.147	China	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on /	Block	1
58.20.99.115	China	147.237.76.147	chinuch.aka.idf.il	Illegal Byte Code Character in Method	Block	1
106.7.248.96	China	147.237.76.86	navy.idf.il	Distributed NULL Character in Method	Block	1
112.66.41.10	China	147.237.76.147	chinuch.aka.idf.il	Distributed Unknown HTTP Request Method	Block	1
114.97.92.152	China	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to /	Block	1

01-23-2016-03:04:01 to 01-23-2016-04:04:01