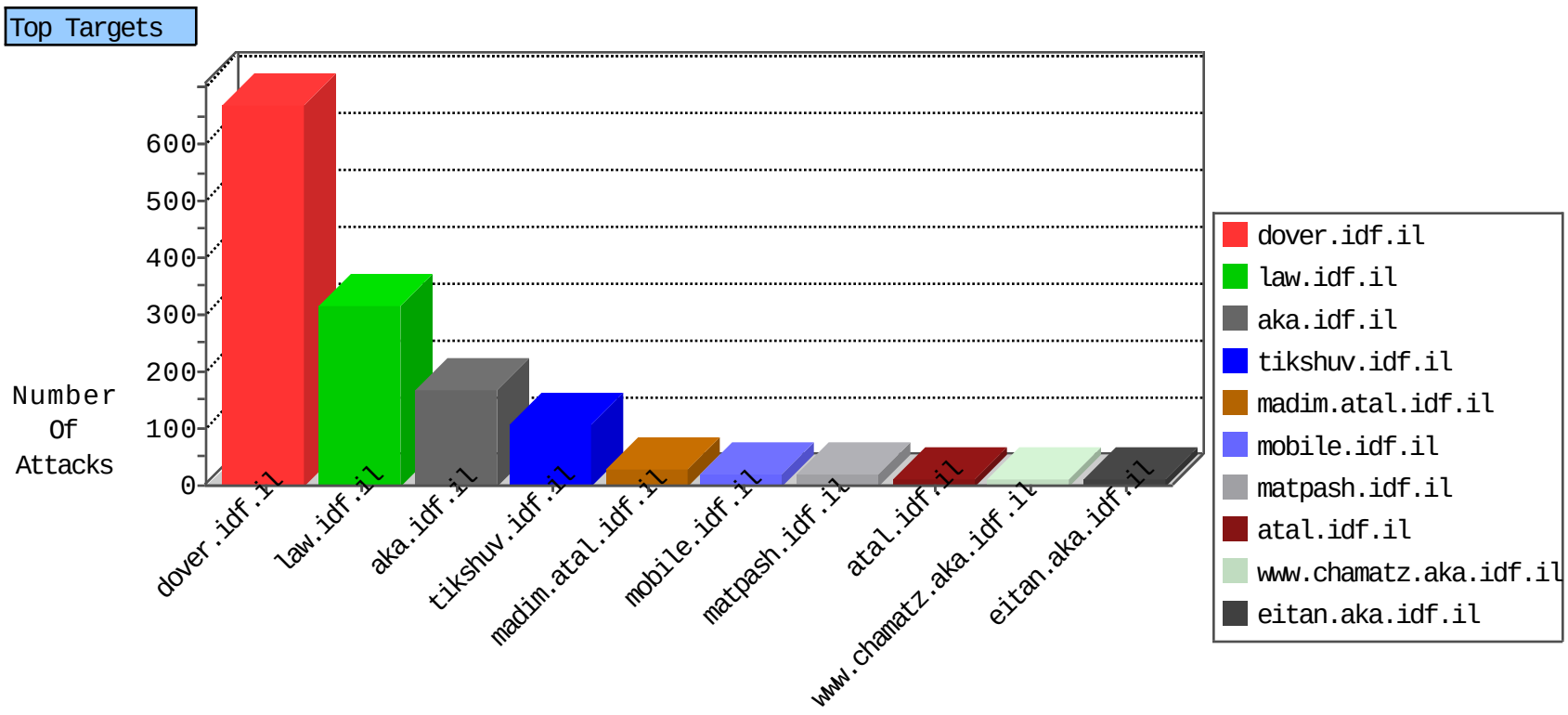
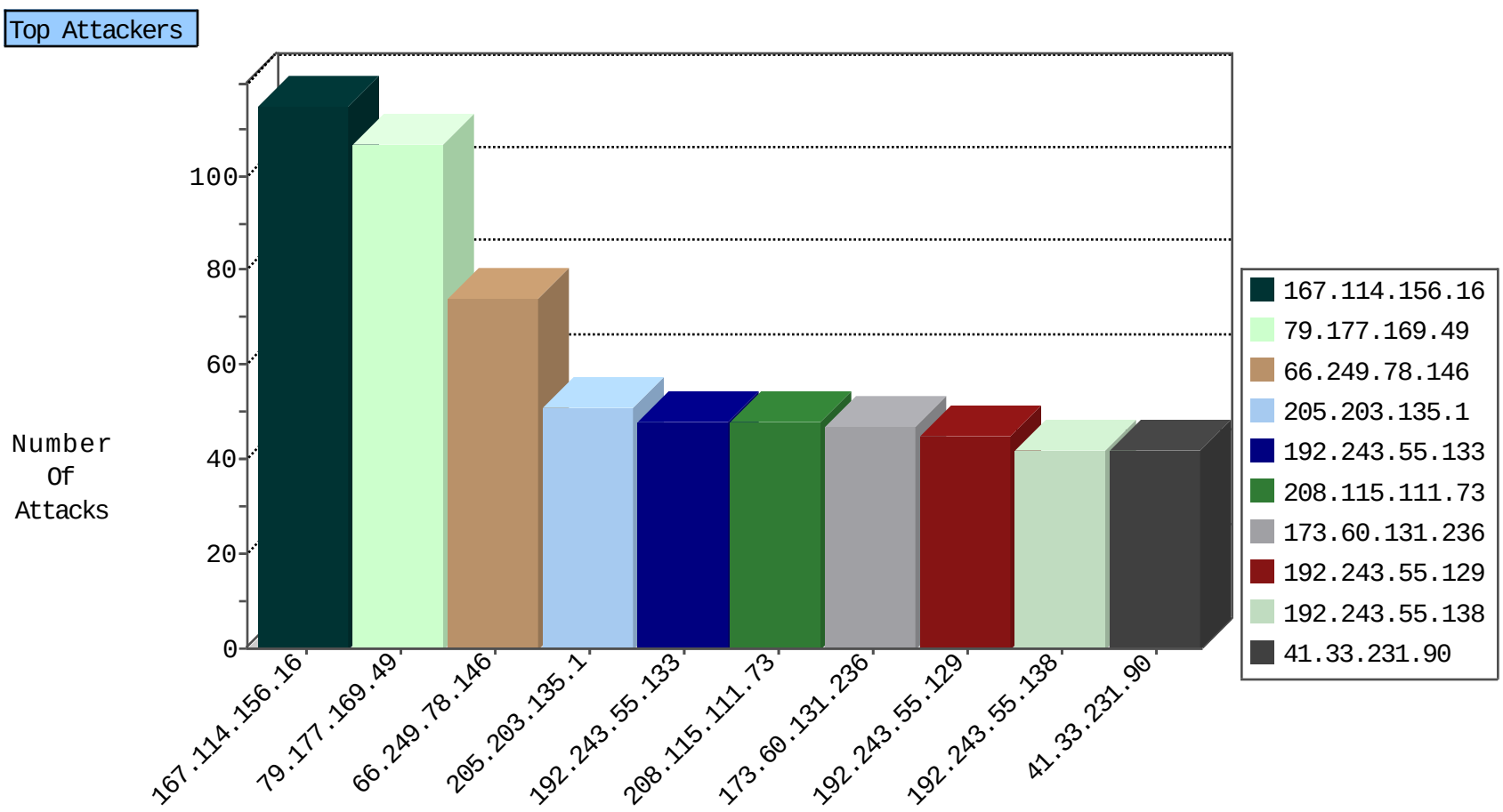
04-23-2016-10:04:06 to 04-23-2016-11:04:06

IDF Under Attack Daily Report





04-23-2016-10:04:06 to 04-23-2016-11:04:06

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	HTTP-POST-Segmented-DoS	dest-reset	5968
66.249.64.233	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3417
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	864
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	9
89.46.102.242	Romania	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

04-23-2016-10:04:06 to 04-23-2016-11:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-23-2016-10:04:06 to 04-23-2016-11:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.66	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	8
185.110.132.54	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.54	147.237.8.24	Ukraine	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.54	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.54	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
202.67.237.220	147.237.76.44	Hong Kong	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
191.189.109.75	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.82.78.38	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
185.110.132.54	147.237.77.233	Ukraine	atal.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.54	147.237.77.61	Ukraine	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.54	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.54	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.54	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.54	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
128.199.214.89	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
195.81.248.101	147.237.76.200	United Kingdom	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
187.161.31.17	147.237.8.14	Mexico	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.110.132.54	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.54	147.237.76.201	Ukraine	e.atal.idf.il	ET SCAN Potential SSH Scan	1

04-23-2016-10:04:06 to 04-23-2016-11:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
173.60.131.236	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
79.177.169.49	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	45
79.177.169.49	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
87.160.153.8	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
107.167.104.219	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
178.63.55.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
207.241.231.194	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	19
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
91.197.61.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
109.67.134.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
149.56.130.239	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.116.28.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.99.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
208.115.113.92	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
78.69.138.95	Sweden	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.177.169.49	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.129	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
171.25.193.78	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
207.244.70.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.177.169.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.138	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
5.170.198.159	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

04-23-2016-10:04:06 to 04-23-2016-11:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.56.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
46.19.86.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
37.26.149.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
84.95.211.153	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	3
84.95.211.153	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
82.166.125.47	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/rec.asp	Block	1
212.179.227.232	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
45.32.239.214	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/jpg/image.jpg	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in Header Name (øJ&	Block	1
84.111.137.209	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
79.176.56.12	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEntrance in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
191.252.48.220	Brazil	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
84.95.211.153	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 84.95.211.153	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/tmuna/default.asp	Block	1
213.57.47.94	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in Method %[[#5]][[#20]]	Block	1
109.64.177.32	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
79.180.127.107	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 79.180.127.107 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
192.243.55.129	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	1
66.249.75.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
23.20.197.30	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Illegal Byte Code Character in Method	Block	1
68.180.229.215	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
213.57.244.9	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Malformed HTTP Header Line 1	Block	1
62.76.74.239	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/chinuch.aspx	Block	1
130.185.155.74	Sweden	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
79.180.127.107	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.97	Block	1
207.46.13.11	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/×–×″	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Method	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Malformed URL	Block	1
66.102.9.81	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
130.185.155.74	Sweden	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/wp-login.php	Block	1
82.140.218.48	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/pniot.aspx'	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation docId in tikshuv.idf.il/site/unit.aspx	Block	1
40.77.167.65	United States	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	147.237.77.176	matpash.idf.il	Abnormally Long Request method	Block	1
84.108.157.208	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method %[[#5]][[#20]]	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1

04-23-2016-10:04:06 to 04-23-2016-11:04:06