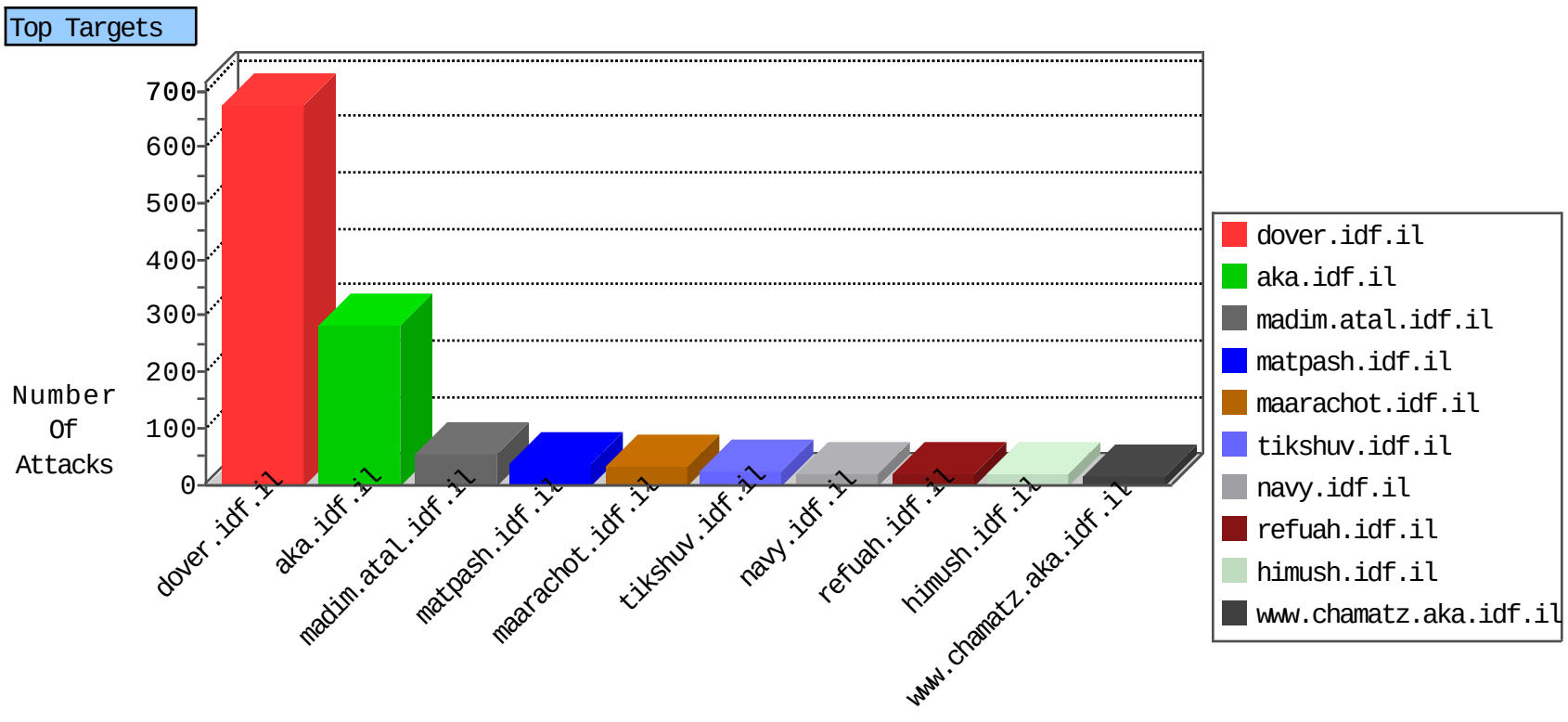
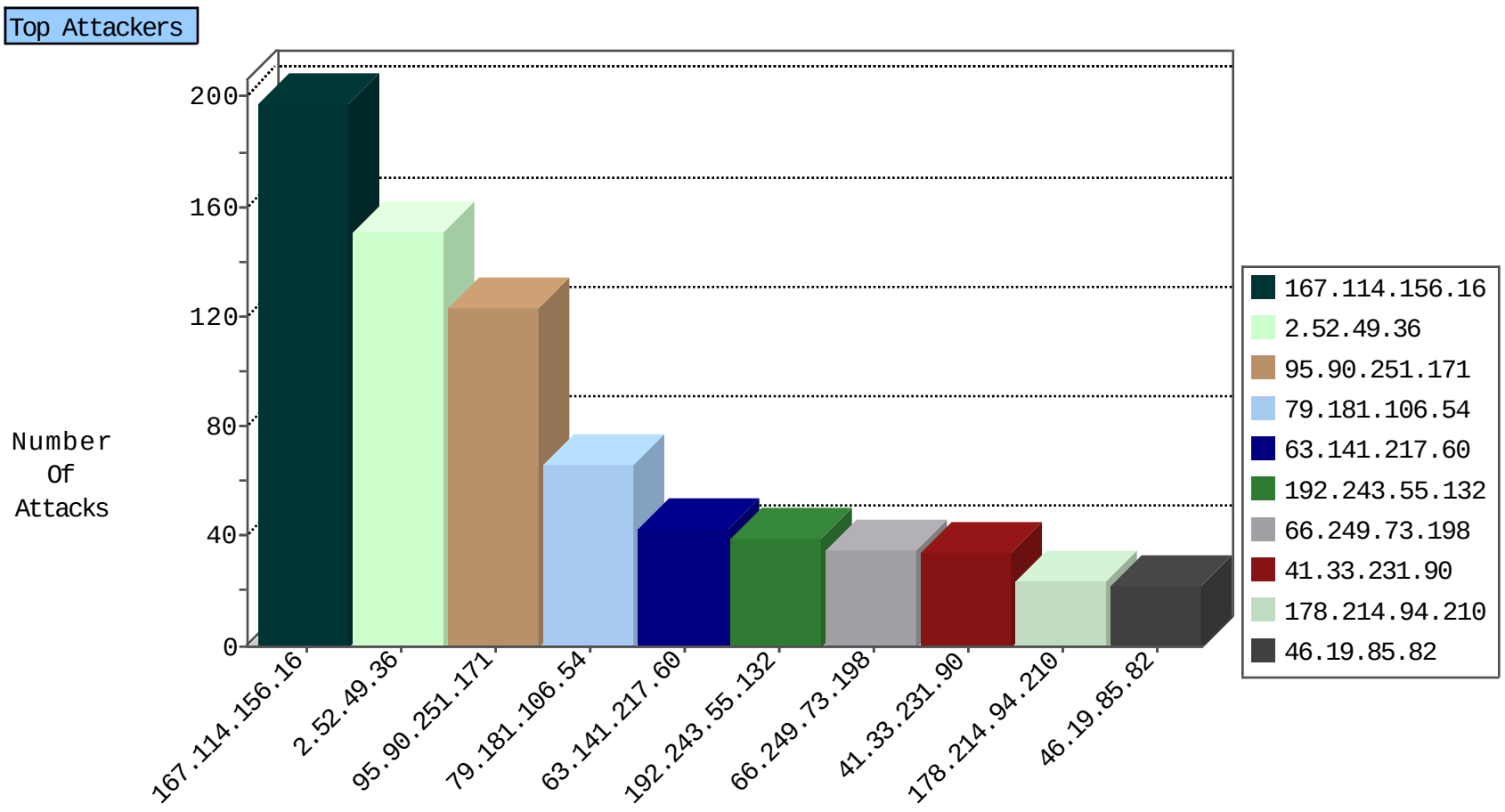
01-08-2016-17:04:03 to 01-08-2016-18:04:03

IDF Under Attack
Daily Report



Top Target



Top Attackers

01-08-2016-17:04:03 to 01-08-2016-18:04:03

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	2773
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	521
63.141.217.60	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	8
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
194.177.16.3	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
220.181.108.77	China	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
65.181.113.88	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
141.212.122.128	United States	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
141.212.122.129	United States	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
115.230.124.164	China	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1

01-08-2016-17:04:03 to 01-08-2016-18:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.187.121.66	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
104.45.132.180	United States	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	1

01-08-2016-17:04:03 to 01-08-2016-18:04:03

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	3
104.128.144.131	147.237.77.243	Canada	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
80.248.146.42	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.49.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.12.39.85	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.9.240	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
94.102.48.195	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.69.146	147.237.8.27	Netherlands	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	1

01-08-2016-17:04:03 to 01-08-2016-18:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
95.90.251.171	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	123
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
2.52.49.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	30
2.52.49.36	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	30
2.52.49.36	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
2.52.49.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	30
2.52.49.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
77.127.217.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
63.141.217.60	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
178.214.94.210	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
178.214.94.210	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
109.66.51.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
31.168.3.26	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	10
109.186.188.83	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.88	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.88	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
176.13.9.240	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
84.108.71.176	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
31.210.188.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.146.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
63.141.217.60	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.68.166.126	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
79.176.149.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.179	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.9.240	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.3.144.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.217.239	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.177.166.228	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.178.170.38	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.3.147.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.177.132.103	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.46.39.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
94.230.86.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.88	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
217.132.135.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.120.125.13		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.88	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
98.252.51.195	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.181.6.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.150.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.45.133.193	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.132	Dominica	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
37.26.146.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.228.35.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.67.103.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-08-2016-17:04:03 to 01-08-2016-18:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
213.57.49.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
109.66.2.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.120.142.235	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	7
79.181.106.54	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 79.181.106.54	Block	7
79.181.106.54	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.181.106.54	Block	6
79.181.106.54	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 79.181.106.54	Block	6
79.181.106.54	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 79.181.106.54	Block	6
185.3.146.254	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 185.3.146.254	Block	5
79.181.106.54	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 79.181.106.54	Block	5
79.181.106.54	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 79.181.106.54	Block	5
79.181.106.54	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 79.181.106.54	Block	4
79.181.106.54	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 79.181.106.54	Block	4
79.181.106.54	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 79.181.106.54	Block	3
149.50.78.71	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.181.106.54	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 79.181.106.54	Block	3
185.3.146.254	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	3
149.78.77.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
40.77.167.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 40.77.167.42	Block	2
74.208.16.87	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 74.208.16.87	Block	2
79.181.106.54	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 79.181.106.54	Block	2
109.64.37.45	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.106.54	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
5.29.170.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
149.78.3.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
40.77.167.42	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1111-he/nakhal.aspx	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
84.94.119.65	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
109.225.14.186	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
79.181.106.54	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
2.54.128.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.68.22.145	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;utm_medium in www.aka.idf.il/main/home/default.aspx	None	1
79.181.106.54	Israel	147.237.72.166	aka.idf.il	Too Many Headers per Request - 37 Headers	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefront/index.stm 	Block	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
115.230.124.164	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to zc.qq.com/cgi-bin/common/attr	Block	1
79.181.106.54	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Query String from 79.181.106.54	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
109.64.37.45	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
79.181.106.54	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Query String [[#16]]^[[#8]][[#16]]× â€ Â¬Â¢Â°8. × [[#8]]×?hCÂ¬FbÃ·[[#2]]Æ'Â-ÂŒXÖ°[[#11]]FÃ™ u[[#16]]×ƒ×³Ö³×¢O×—/:g×"%<cÂ¿lÂµ.LÂ¡×"×' [[#15]]6G~[[#11]]HÂ¨râ€?aLQ[[#29]]Ö¸×±[[#14]]@×?[[#30]]×ƒ Ö¿Â?[[#21]]Ã?3Â¦Â«×š×•,=Â¯LÂ¯Ö¾N×™Â?9Â°×œÃœlË†Ã™ Ö²Ö´×?×¡â€°[[#18]] ×¤rÂ?Â¼Â£×ƒm•Ã™â,¬	Block	1
207.46.13.112	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
84.108.218.93	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/tmuna/	Block	1
176.13.16.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.225.14.186	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
87.68.22.145	Israel	147.237.72.166	aka.idf.il	Unknown Parameter utm_source in www.aka.idf.il/	None	1
79.181.106.54	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1

01-08-2016-17:04:03 to 01-08-2016-18:04:03