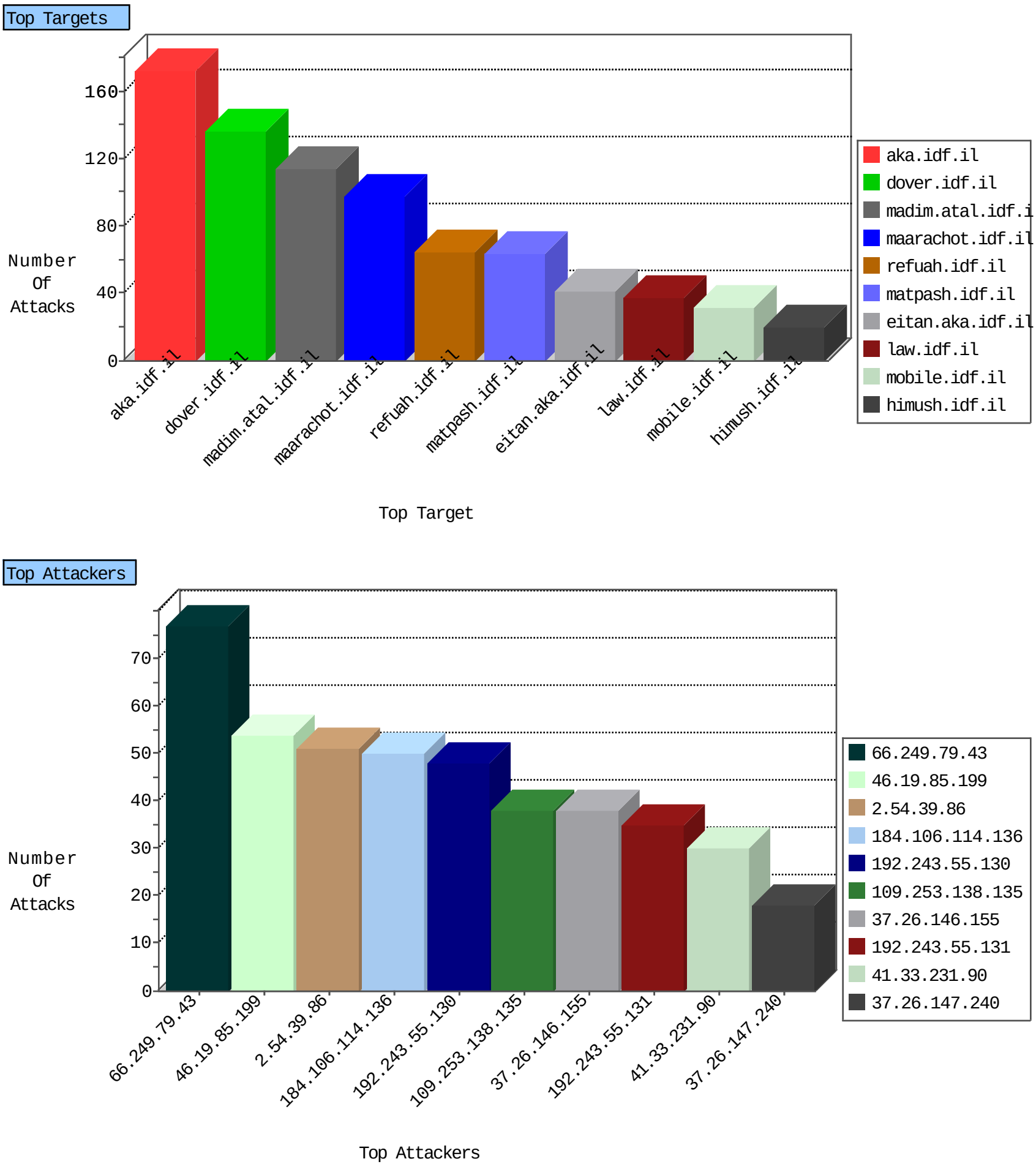
02-19-2016-10:04:07 to 02-19-2016-11:04:07

IDF Under Attack
Daily Report



02-19-2016-10:04:07 to 02-19-2016-11:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
115.239.228.10	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Http	drop	2

02-19-2016-10:04:07 to 02-19-2016-11:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.106.114.136	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	9
184.106.114.136	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
184.106.114.136	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
2.54.13.227	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1

02-19-2016-10:04:07 to 02-19-2016-11:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.79.43	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	77
184.106.114.136	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	26
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
120.63.149.196	147.237.76.44	India	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.216.119.94	147.237.76.44		e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
198.180.198.185	147.237.0.33	United States	idf.il	ET SCAN NMAP -f -sS	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
178.77.232.108	147.237.77.216	Czech Republic	dover.idf.il	portscan: TCP Distributed Portscan	1
146.185.250.105	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.105	147.237.8.45	Russian Federation	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
89.216.119.94	147.237.76.44		e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
198.180.198.185	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 2048	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.105	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.105	147.237.72.14	Russian Federation	dover.idf.il(old	ET SCAN Potential SSH Scan	1

02-19-2016-10:04:07 to 02-19-2016-11:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
37.26.146.155	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
2.54.10.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
212.76.127.219	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
37.26.147.240	Israel	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	10
89.139.147.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
37.46.41.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.147.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.21.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.147.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.177.34.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.179.218.166	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
5.22.135.156	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
199.30.24.119	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
213.151.35.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
176.13.11.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.12.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.151.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.54.140.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.210.218.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.218.166	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
77.127.177.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.54.40.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.167.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.225.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
5.102.254.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.99.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-19-2016-10:04:07 to 02-19-2016-11:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.39.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
109.253.138.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
87.69.178.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
87.70.43.59	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	9
197.38.197.170	Egypt	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	8
197.38.197.170	Egypt	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	8
109.253.202.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
217.132.6.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.177	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/pdf/files/Ã–â€™Ã–â„¢Ã–Â“Ã–â„¢Ã–â€¢Ã–Â Ã–â€¢Ã–Âª	Block	2
80.246.133.172	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
217.132.6.136	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	2
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1086-en/dover.aspx	Block	1
197.38.197.170	Egypt	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
141.0.14.72	Europe	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.29.247.168	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method Â‰Ã»Â¥@Y0r[[#0]]"![[#27]]Â“Ã©Ãš[[#1]]{rÂ–Â‰Ãµ$xoÃ¢Â³QÃžÂ„[[#1]]+Ã³MÃ‡Ã®\Ã‡Ã†6R[[#22]]Ã‰Â?{<ÂŸSÂœ4VÂ»Â‘%sÂ†Âš in URL ÂŠy×™u}7[[#3]]×£pÖ»yÖ¶b[[#21]]×¢Â±Ö¼[[#22]]×©6× p×ž	Block	1
5.29.247.168	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
207.46.13.149	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/signals/atar/	Block	1
79.178.108.209	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
184.168.192.163	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/xmlrpc.php	Block	1
54.173.223.170	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
5.29.247.168	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 3	Block	1
109.100.100.232	Romania	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
80.230.37.125	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
2.54.136.161	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
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	1
197.38.197.170	Egypt	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
141.0.14.217	Europe	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.124	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
5.29.247.168	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name ÂµÂ¿Ã Ã„[[#12]][[#5]]0Ã†[[#6]]Ã®Ã”ÃƒÂ³Ã–Ã´>[[#23]]<Âƒo[[#30]]C[[#23]]ÃŠ[[#16]]ÃŽÂ¤Ã¯Â±IÂ°Â·[[#18]]RÃ¯G	Block	1
79.178.108.209	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
61.135.190.69	China	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on 147.237.0.19/	Block	1
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
5.29.247.168	Israel	147.237.72.166	aka.idf.il	Malformed URL ÂŠy×™u}7[[#3]]×£pÖ»yÖ¶b[[#21]]×¢Â±Ö¼[[#22]]×©6× p×ž	Block	1
109.100.100.232	Romania	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
5.22.135.156	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 5.22.135.156	Block	1
74.84.136.105	United States	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
149.78.56.166	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatesMonth in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.85.196	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
5.29.247.168	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
87.71.13.56	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
213.151.35.221	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.178.108.209	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
195.67.74.166	Sweden	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
5.29.247.168	Israel	147.237.72.166	aka.idf.il	NULL Character in Method Â‰Ã»Â¥@Y0r[[#0]]"![[#27]]Â“Ã©Ãš[[#1]]{rÂ–Â‰Ãµ$xoÃ¢Â³QÃžÂ„[[#1]]+Ã³MÃ‡Ã®\Ã‡Ã†6R[[#22]]Ã‰Â?{<ÂŸSÂœ4VÂ»Â‘%sÂ†Âš	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.29.116.158	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
74.84.136.105	United States	147.237.72.166	aka.idf.il	Multiple signatures from 74.84.136.105	Block	1
180.76.15.142	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1

02-19-2016-10:04:07 to 02-19-2016-11:04:07