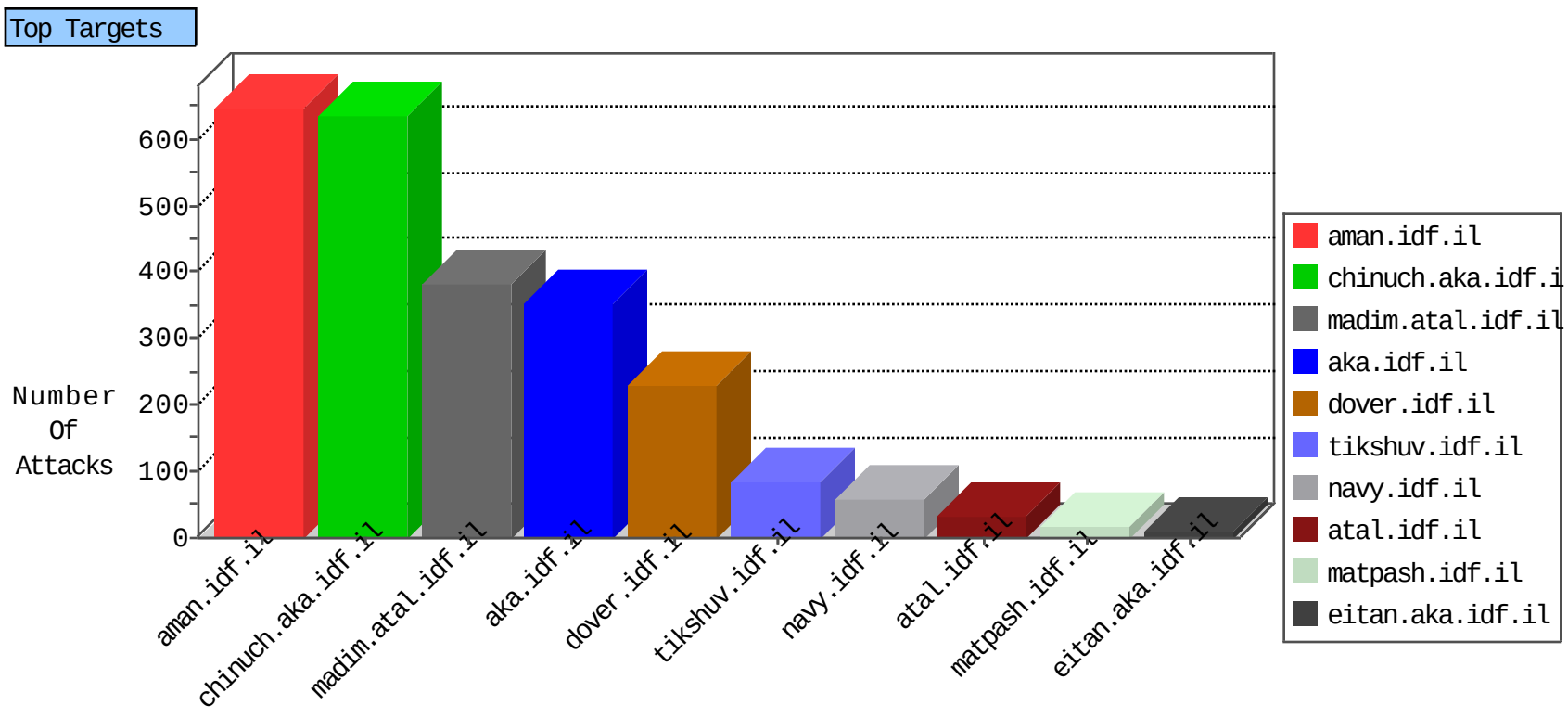
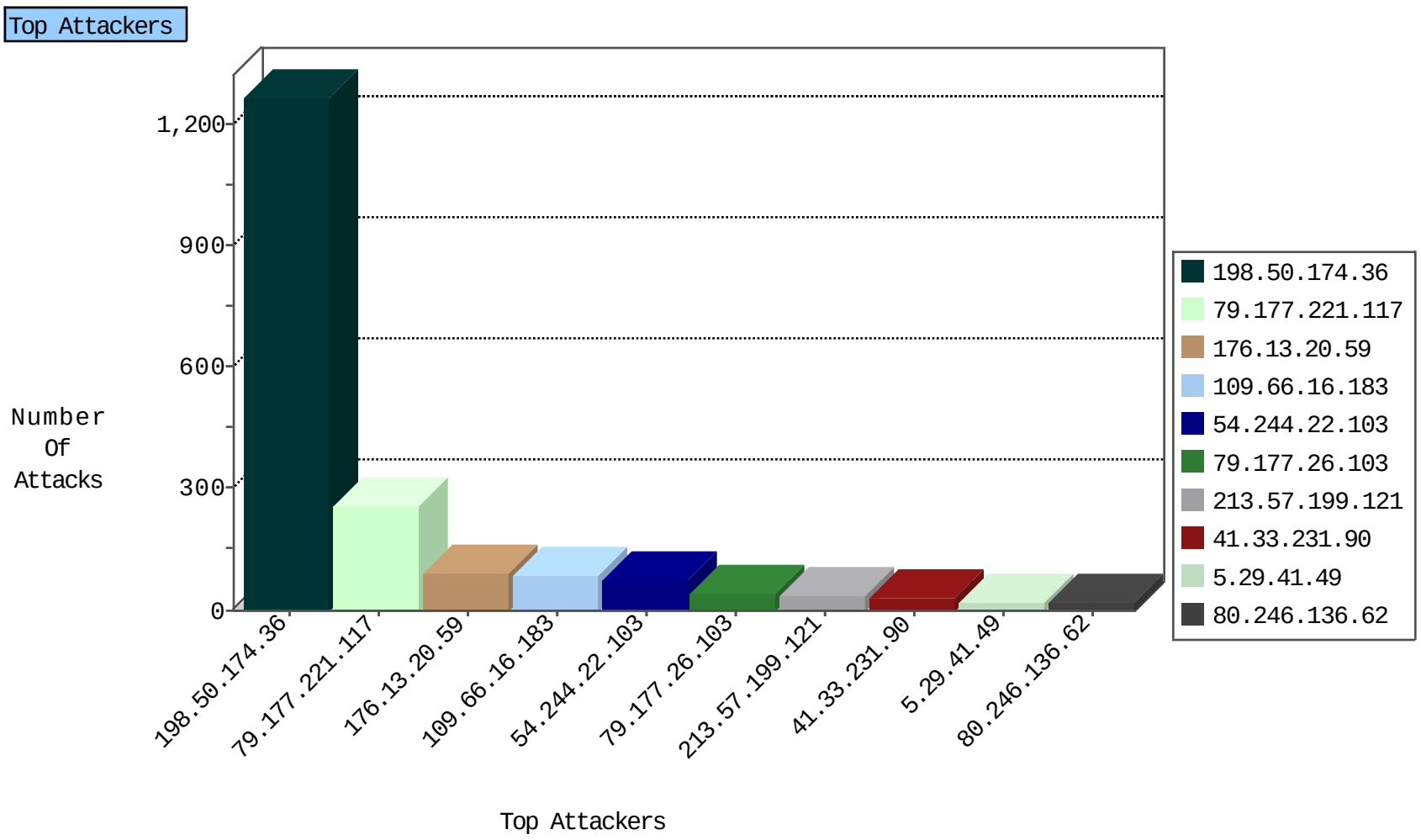
02-04-2016-21:04:07 to 02-04-2016-22:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-04-2016-21:04:07 to 02-04-2016-22:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.214	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	142
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
113.82.141.180	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
113.82.141.180	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
79.176.127.112	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
113.82.141.180	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
113.82.141.180	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

02-04-2016-21:04:07 to 02-04-2016-22:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
78.171.84.89	Turkey	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

02-04-2016-21:04:07 to 02-04-2016-22:04:07

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	4
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
189.219.89.52	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.161	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
125.212.232.146	147.237.76.39	Vietnam	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
109.65.60.27	147.237.72.156	Israel	aman.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
103.41.177.70	147.237.77.19		law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
5.230.148.132	147.237.77.121	Germany	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
218.246.0.97	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.159	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
201.132.31.138	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
201.132.31.138	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
189.219.89.52	147.237.76.177	Mexico	ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.137	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
125.212.232.146	147.237.76.39	Vietnam	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
103.41.177.70	147.237.77.19		law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
220.231.195.122	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
46.19.86.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.114	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
5.230.148.132	147.237.77.121	Germany	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
207.111.254.7	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
88.249.106.23	147.237.0.15	Turkey	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
201.132.31.138	147.237.77.216	Mexico	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1

02-04-2016-21:04:07 to 02-04-2016-22:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
198.50.174.36	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	382
198.50.174.36	Canada	147.237.72.156	aman.idf.il	SYN Attack		reject	352
198.50.174.36	Canada	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	206
198.50.174.36	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	152
198.50.174.36	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	99
198.50.174.36	Canada	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	75
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	67
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	53
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
79.177.26.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
31.168.217.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
93.172.11.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.88.31.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.136.62	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
5.102.254.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
80.246.136.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
79.181.59.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.57.199.121	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	9
213.57.199.121	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
79.177.26.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
213.57.199.121	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence		monitor	7
66.249.78.147	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.26.103	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
109.253.196.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.18.150	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.127.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.26.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.18.150	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.127.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.30.187	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.7.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.29.41.49	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
94.230.86.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.177.26.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	5
84.228.209.153	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.177.26.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.56	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
66.249.88.206	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.57.199.121	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
84.228.209.153	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
141.0.14.114	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.7.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.29.41.49	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

02-04-2016-21:04:07 to 02-04-2016-22:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.221.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	138
79.177.221.117	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.177.221.117	Block	100
176.13.20.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
79.177.221.117	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 79.177.221.117	Block	17
2.54.179.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
87.69.113.127	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 87.69.113.127	Block	15
79.181.147.185	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.181.147.185	Block	8
78.171.84.89	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 78.171.84.89	Block	4
2.52.139.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 109.66.16.183	Block	3
95.32.94.209	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-config.bak	Block	3
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 109.66.16.183	Block	3
79.178.217.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 109.66.16.183	Block	3
109.253.196.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 109.66.16.183	Block	3
78.171.84.89	Turkey	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 109.66.16.183	Block	3
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 109.66.16.183	Block	3
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 109.66.16.183	Block	3
37.8.46.192	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
2.52.139.156	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
46.19.85.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 109.66.16.183	Block	2
78.171.84.89	Turkey	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 78.171.84.89	Block	2
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 109.66.16.183	Block	2
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 109.66.16.183 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
46.121.253.242	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
194.90.66.9	Israel	147.237.72.166	aka.idf.il	Unknown Parameter _ in www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	None	1
84.109.131.124	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$112 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.175.108.33	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
78.171.84.89	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Parameter Value at 25 for h×,Ö²&ÂŠ Â¦aâ€?Æ'1â€?&kr#Â¥i×´[[#3]]{bÃ™â€	Block	1
66.249.78.80	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
213.57.128.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
46.19.85.219	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
159.203.84.24	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/	None	1
87.69.113.127	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
109.66.16.183	Israel	147.237.72.166	aka.idf.il	NULL Character in Method oÃ,ÂžBÃ§5Ã´ÂˆÂ®[85Ã-[[#19]]HÂŸ LÃ²Â»Ã?Ã‡AÂ«P[[#27]]Ã—Â§Â?Ã?'.Ã±Â©Â?[[#28]]Â©ÂºÂšÂ—Ã' ^}Â‹Ã§ÃµÃ½X[[#20]]Ã?•[[#15]]Ã?Â°tÃµMwEqÂ¡Ãˆ vÃ¢Ã¥Ã£ÂŒÃ‡]Â,lÂ™Â„$xÃŸ[[#20]]8UÂ¯-[[#29]]Ã˜Ã-Â?Ã—-Ãž [[#19]]Â¥[[#31]]zÂ‹Ã?Ã?VMÃžÃ™[[#30]]YÂº4Ã'4Ã‹]_@[oÂ«[[#0]]acÃ¼LÃ'Ã¦Ã³ÂœÂž•Ã— [[#11]]Ã¦$[[#25]]`V[[#24]]m#Ã"ÂœÂ¡Â›Â¦[[#14]]Â?+Ã':Ã˜ Â¨u`)Ã?oÃ¼cÂœÂ–iQUÃ•\Â±+ÂŸaTÂ™Â³Ã¿Ã± Ã¤Â¸pSÂ¤kÃ¡[[#25]]4Ã²[9^dÂ²NÂ›bÃ€j[[#7]]y:ÃŽIÃŽW	Block	1
78.171.84.89	Turkey	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
95.86.66.166	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/1048-7663-he/tikshuv.aspx&sa=u&ved=0ahukewjd1ui87n7kahuqv3ikhrocaskqfggumaq&usg=afqjcnhuxxzxw1uwljwbssvbjeis3k8wuq	Block	1
46.163.68.109	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	1
198.58.102.156	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
84.109.131.124	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
37.142.64.12	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$42 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
109.66.16.183	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Query String ×›>Â?y×šÂŽ Â¼Â¨[[#27]]Ö¿Ö¶ÖµgÂ«,=â„¢Ö³XÃ™×˜YÖ¶FjÃšHÂ¼Sq×' [[#4]][z[[#22]]â€¦aÂ?â€˜Ö±â€?â€ t×¡×ƒ×–Ë†ZÃ™.Ö¾[[#7]]Ëœ ×°"GÂ-×,[[#22]]}Ãšâ€™×³â€ W[[#14]]Â³Â-×¨Ã»×¢$ÂŽÂ©Ã™ Ö½xÂ¦p[[#17]]×'[[#20]]h-W[[#30]]Â¥ÃŸ[[#14]]•lÂ®dÂ¨j×€Qâ,¬ÃŸ=on h×,Ö²&ÂŠÂ¦aâ€?Æ'1â€?&kr#Â¥i×´[[#3]]{bÃ™â€	Block	1

02-04-2016-21:04:07 to 02-04-2016-22:04:07

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.210.190	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
109.66.16.183	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1

02-04-2016-21:04:07 to 02-04-2016-22:04:07