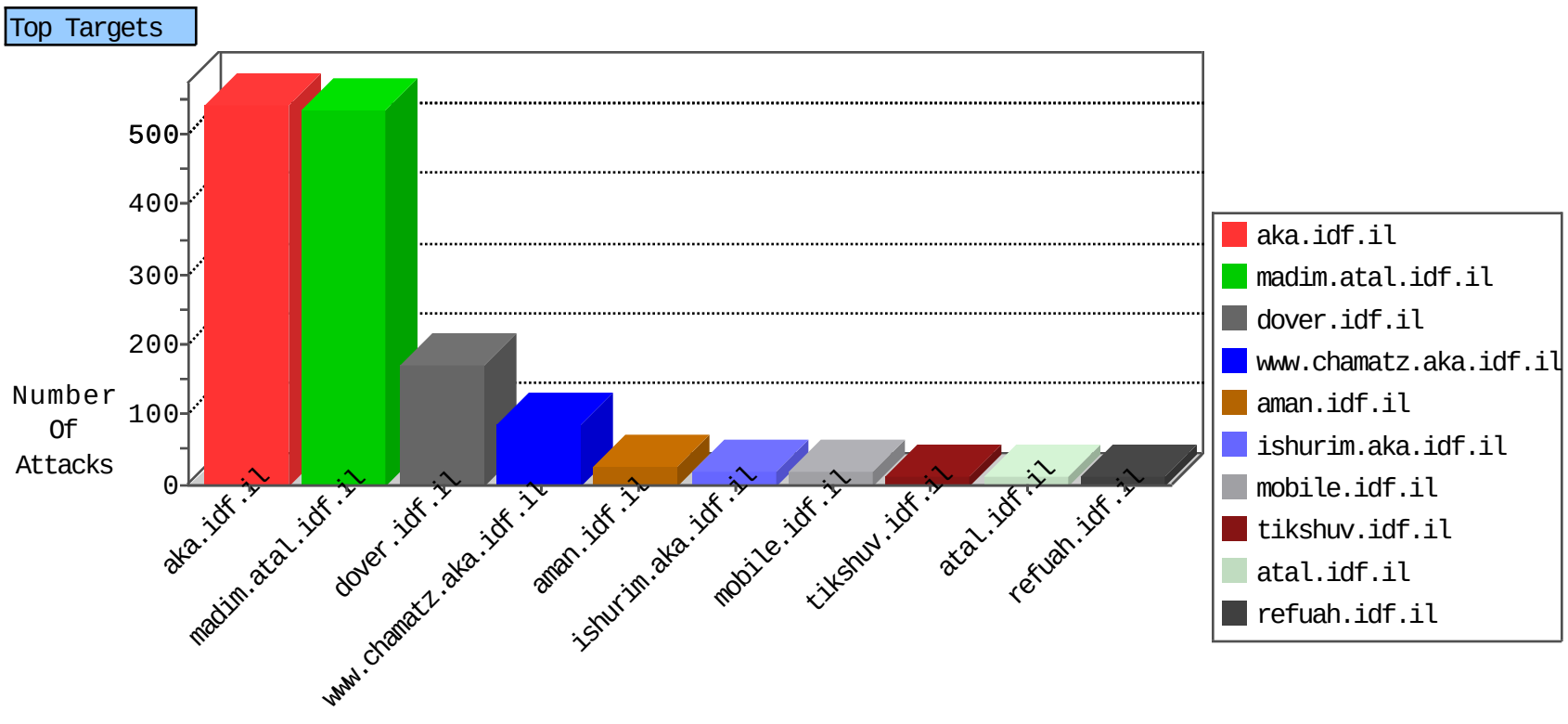
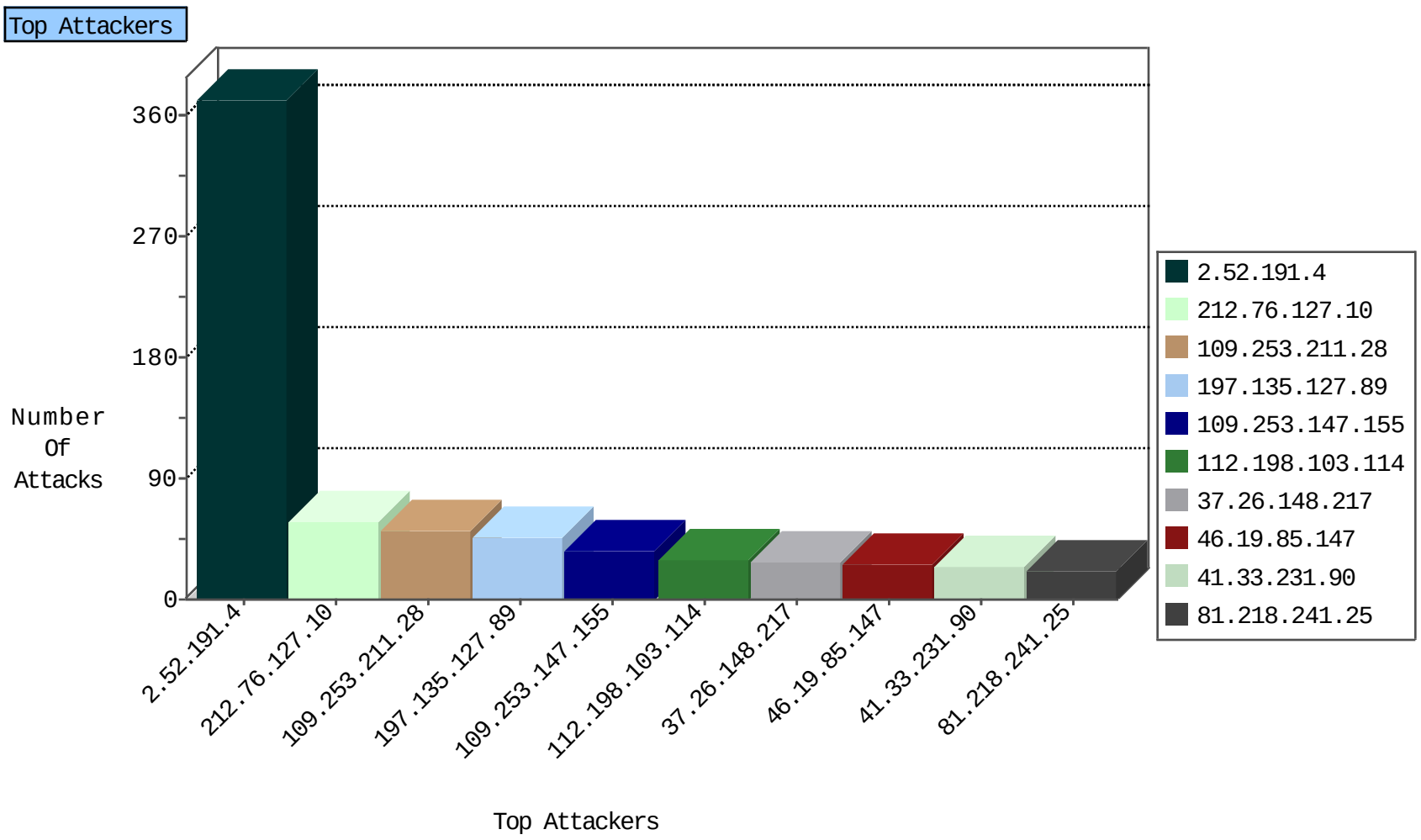
02-03-2016-14:04:06 to 02-03-2016-15:04:06

IDF Under Attack
Daily Report



Top Target



Top Attackers

02-03-2016-14:04:06 to 02-03-2016-15:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	12
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
176.195.94.231	Russian Federation	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
71.6.158.166	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

02-03-2016-14:04:06 to 02-03-2016-15:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
187.38.150.123	Brazil	147.237.77.216	dover.idf.i	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1

02-03-2016-14:04:06 to 02-03-2016-15:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.22.131.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.109.97.62	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
117.34.78.168	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
109.65.197.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.78.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.36.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.148.22.26	147.237.76.176	Lithuania	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
218.240.136.218	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.240.136.218	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
31.210.188.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
109.66.124.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.187.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.212.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
52.32.180.178	147.237.76.31	United States	nakchal.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
46.148.22.26	147.237.72.217	Lithuania	e.idf.il	ET SCAN Potential SSH Scan	1
218.240.136.218	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.7.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-03-2016-14:04:06 to 02-03-2016-15:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.76.127.10	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	57
46.19.85.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	25
197.135.127.89	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
212.76.127.219	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
141.0.14.83	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
197.135.127.89	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
212.76.127.111	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
109.253.150.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.113.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.15.229	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.190.141	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
197.135.127.89	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
80.246.139.109	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.5	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.168.65	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
5.22.135.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.191.4	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
5.22.134.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.179.1.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
91.200.12.106	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
2.54.15.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.118.36.53	Israel	147.237.72.167	ishurim.aka.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
91.200.12.106	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
212.76.127.44	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.141	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	3
46.19.85.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.221.105.197	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.86.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.6.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.23.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.161.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.60.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.223	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.230.16.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.195.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.159.33	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.176.145.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.5.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.146.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
147.236.238.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.165.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-03-2016-14:04:06 to 02-03-2016-15:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.191.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	158
2.52.191.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	142
2.52.191.4	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.52.191.4	Block	67
109.253.211.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
109.253.147.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
37.26.148.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
109.253.145.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
109.66.119.93	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
79.177.6.87	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.177.6.87	Block	11
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	10
2.54.34.226	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
109.64.201.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
109.253.211.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
37.142.222.233	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 37.142.222.233	Block	5
2.54.13.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.217.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.211.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.198.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.141	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.19.86.141	Block	3
46.19.86.141	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.19.86.141	Block	3
31.210.187.132	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	3
46.19.86.141	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
80.241.255.91	Georgia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	3
46.19.86.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/3/	Block	3
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
192.116.111.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
213.57.212.191	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$56 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
46.19.86.26	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$27 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
46.19.85.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.183.201.223	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	2
109.66.125.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
109.67.103.219	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
84.228.130.216	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	2
46.19.86.37	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$78 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
188.143.232.22	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 188.143.232.22	Block	2
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	2
2.54.47.26	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	2
2.52.158.189	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$45 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
37.142.64.22	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$116 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
79.182.21.142	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$90 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.66.125.15	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
185.3.144.83	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$7 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
5.29.204.176	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
46.19.86.193	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$67 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
87.69.190.81	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name [[#28]]Ãª Â·Ã©[[#7]]Â°$Â®Â‰EÃ¤Â¡;Â Ã•rÃ†PÂ°Â?Â™FÃ‹ZÂ'Â' 6vqÃ¦NJÃ?7Ã©Ã?Â´lÂ“R[[#16]]]Â¦6Ã°ÃšÃ[[#11]]9Ã¾Â?D[[#18]]Â'ÂŒ Ãª[[#8]]Ã‹Ã”gt[[#2]]Ã®~Ã»[[#30]]<#Ã²[[#3]]%[[#0]]g[[#21]]Ã„Â°Â¯Ã' Ã½Â€%SaÃ»[[#4]]Ã„-fÂº=[[#31]][[#30]]Â¹Â“Â¾3Ã´Â” [[#19]]u4+Â¥Ã¹pÂ”jÃ‡[[#5]]Ã©[[#7]]C7z[[#6]]Ã½sÂ'Ã¡[[#24]]Ã'Ã• =Ã‰7Ã¿Â?gÃšuÃ©ÂµÃ ÂƒÃ¢ÃµÃ€Â-Â¬Â'n[[#3]][[#14]]Â?xÂ‹ yÂ¡[[#6]]Ã¶Ã?Â¬[[#22]]Â†[[#28]][[#0]]	Block	1
216.218.206.68	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1

02-03-2016-14:04:06 to 02-03-2016-15:04:06

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.182.201	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$56 in aka.idf.il/main/giyus/questionnaire.aspx	None	1

02-03-2016-14:04:06 to 02-03-2016-15:04:06