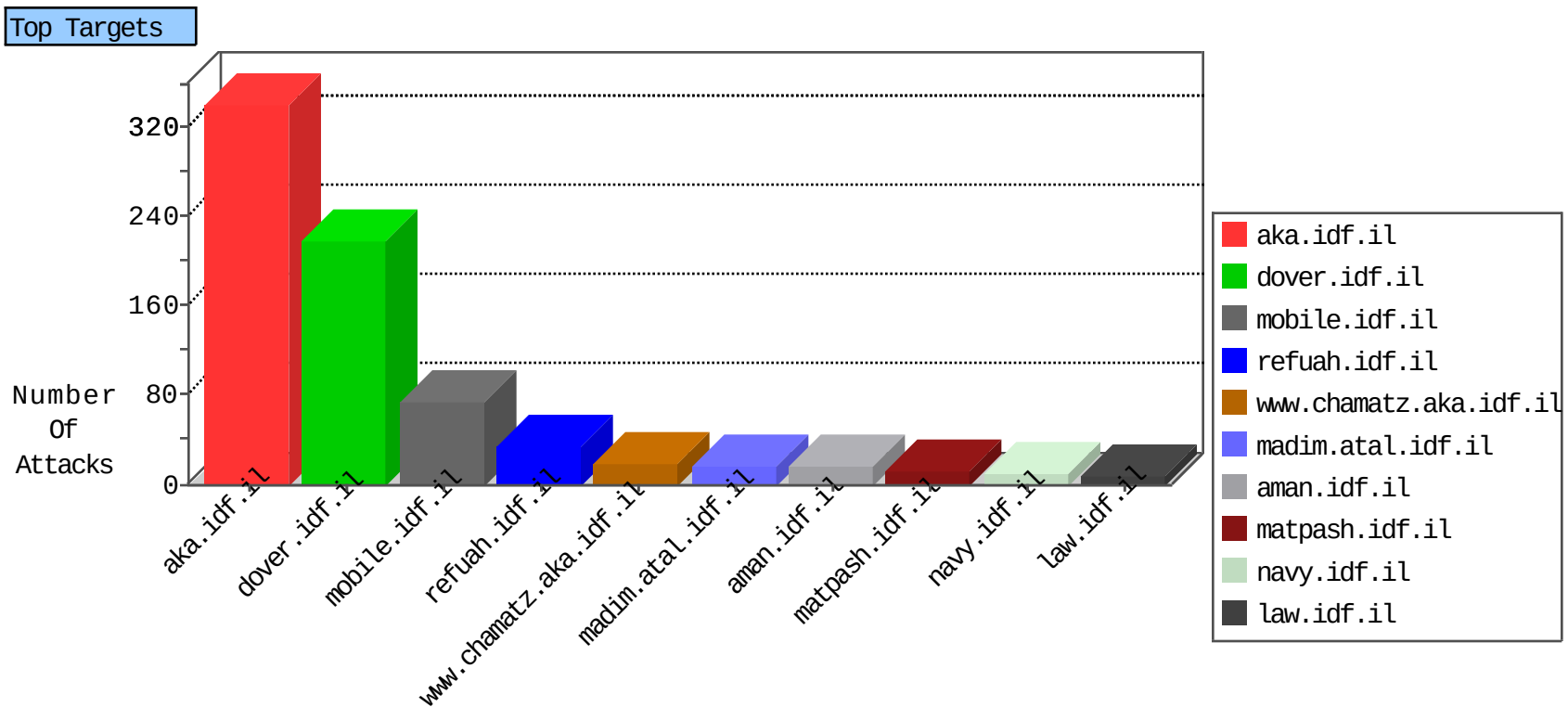
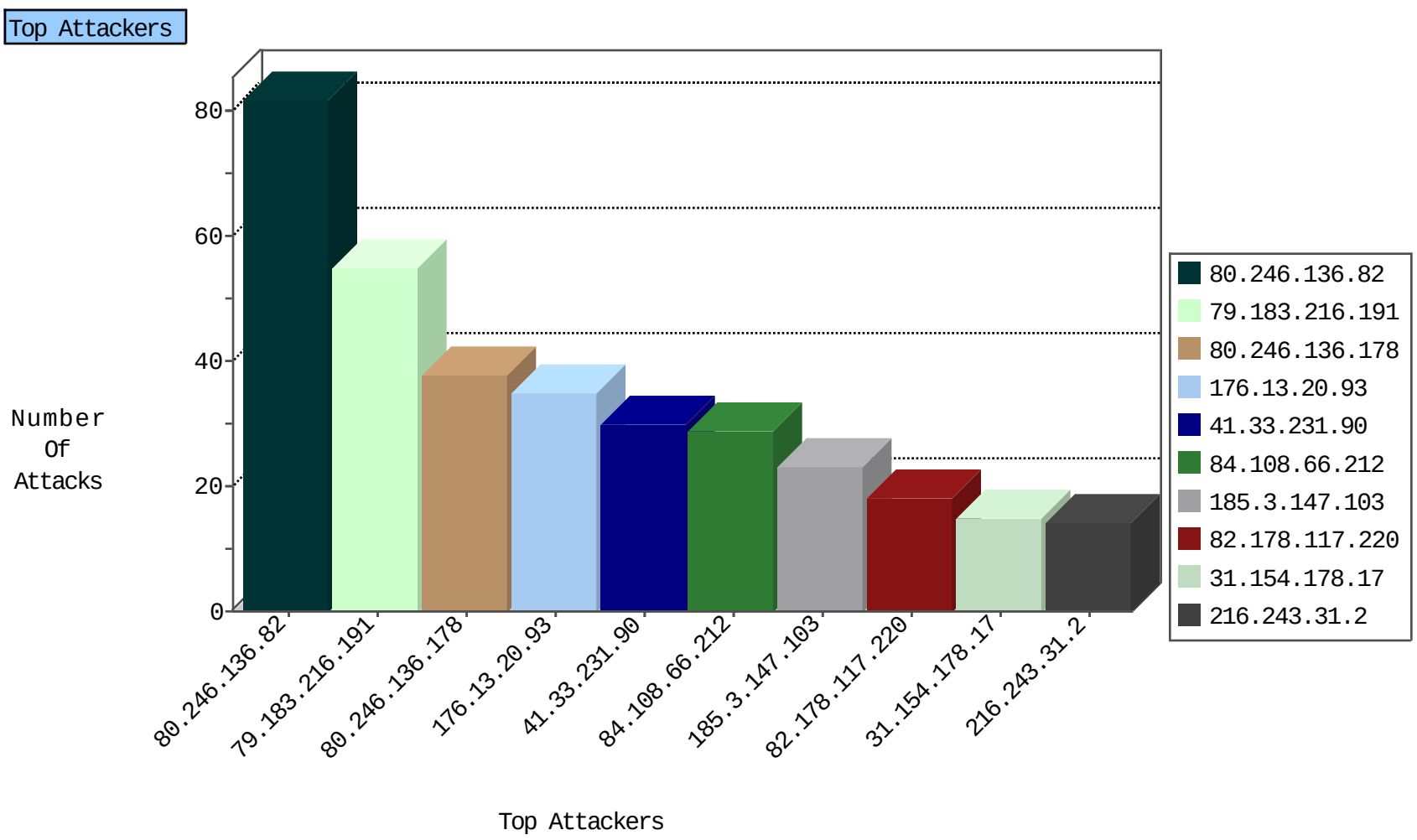
02-05-2016-21:04:08 to 02-05-2016-22:04:08

IDF Under Attack Daily Report





02-05-2016-21:04:08 to 02-05-2016-22:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.82	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
80.246.136.82	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
46.19.86.70	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
149.202.65.25	Germany	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

02-05-2016-21:04:08 to 02-05-2016-22:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-05-2016-21:04:08 to 02-05-2016-22:04:08

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
209.126.116.147	147.237.72.14	United States	dover.idf.il(old	ET SCAN NMAP -sS window 1024	1
177.225.12.35	147.237.0.33	Mexico	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.151.52.161	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.8.24	United States	e.lifestyle.idf.	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

02-05-2016-21:04:08 to 02-05-2016-22:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.20.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
84.108.66.212	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
80.246.136.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	27
80.246.136.82	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
80.246.136.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
80.246.136.82	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
31.154.178.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.178.206.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
185.3.147.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.183.216.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
80.246.136.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
188.120.148.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.11.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
217.132.48.239	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	8
37.46.39.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.246.136.82	Israel	147.237.77.216	dover.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	8
5.102.254.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
172.56.34.229	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
149.78.94.154	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
82.178.117.220	Oman	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
82.178.117.220	Oman	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.178.164.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.86.125	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.97.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.194.177	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
82.178.117.220	Oman	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
2.52.147.183	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.32.179.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
188.120.148.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.81.250.149	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.188.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.38.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
217.132.48.239	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
77.245.11.190	Jordan	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
66.249.78.144	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.254.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	3
84.229.161.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.243	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
149.78.240.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.49.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.18.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.140.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.36.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.105.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.127.152.61	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	7
80.245.119.25	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	5
80.245.119.25	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.245.119.25	Block	5
176.13.20.93	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
185.32.179.168	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	4
185.3.147.103	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	4
79.183.216.191	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 79.183.216.191	Block	3
149.78.11.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.183.216.191	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.183.216.191	Block	3
79.183.216.191	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 79.183.216.191	Block	3
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
217.132.140.130	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	3
2.52.172.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.183.216.191	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 79.183.216.191	Block	3
79.183.216.191	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
79.183.216.191	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 79.183.216.191	Block	3
79.183.216.191	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 79.183.216.191	Block	3
79.183.216.191	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 79.183.216.191	Block	3
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	3
79.183.216.191	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 79.183.216.191	Block	3
185.3.147.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.183.216.191	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 79.183.216.191	Block	3
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	3
84.108.194.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	2
79.183.216.191	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 79.183.216.191	Block	2
46.19.85.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.183.216.191	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method Ã†	Block	1
212.76.112.64	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m	Block	1
109.67.202.42	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 109.67.202.42 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
77.127.152.61	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
46.190.4.69	Greece	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
79.183.216.191	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request request version	Block	1
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	1
84.114.136.195	Austria	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/giyus/general/default.asp	None	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
109.67.202.42	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.183.216.191	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version Ã?Â¤Â»r[[#21]]Ã¹[[#7]]Â¼Ã“Ã°ÃŽ Â?mBAÂ±9Ã°[[#14]]]CÃ»Â¯Ã®D&[[#5]]Â‡Ã?[[#24]]Ã¡Â¿Â™,Â• O[[#29]]GÃ?ÂžÃ°[[#30]]lÃ¨ÂŠ+Â¾'Ã?[[#31]]Ã˜ /m[[#3]]M[[#28]]Ã·Ã¶ZDÃ Ã¢2Â†Ã“Â±Â—ÂƒÂƒEÂ´@Ã¸Â¡1q[[#1]]Z!Â›	Block	1
84.108.194.177	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.178.18.97	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
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
52.70.130.19	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	1
79.183.216.191	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at Â–Â£[[#24]]zÂ,[[#1]]QÃ®Ã‹Â®Ã¶Ã±1iÃƒ VÂ–Â¿[[#4]]sÃ¸Â²P[[#26]]Ã f5xMÂ‹Ã¡~8'[[#28]]ÃµÂ¥@q[[#30]]Â?Â,Ã»!Âœ Ã»Â™9c[[#0]][[#19]](ÂœqZÃ?*!Ã¹,Â§Â»[[#20]][Âœ [[#26]]Ã¥Â»PÃ¾[[#5]] $Â¬Â¡Â? Â™[[#12]]x>[[#4]]Ã?Ã³AÃ²[[#28]]Â©Â-[[#4]]AÃ–Ã,[[#4]] ‰KÃ°>Ã?.ÃŸÃ¡Z[[#15]]7zÃ¥[[#28]]Âš Ã?Ã»\Ã½[[#14]]Â?VH[[#25]]HÂ©IÂ´$Ã,Q[[#1]]Ãš sYO[[#8]]Â?Â•[[#14]]Â’Ãƒ	Block	1
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp?moduleid=2&catid=22703&docid=22724	Block	1
85.65.145.133	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1