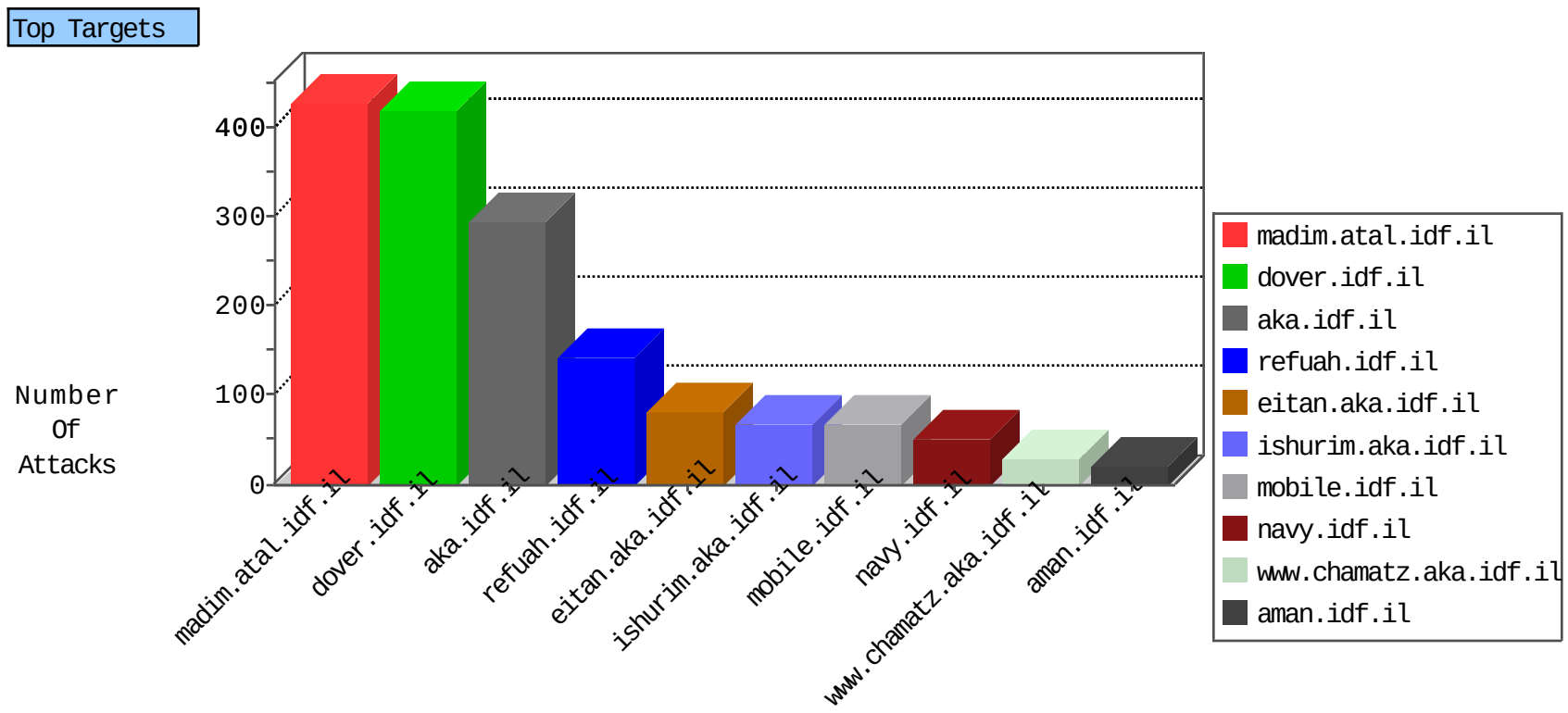
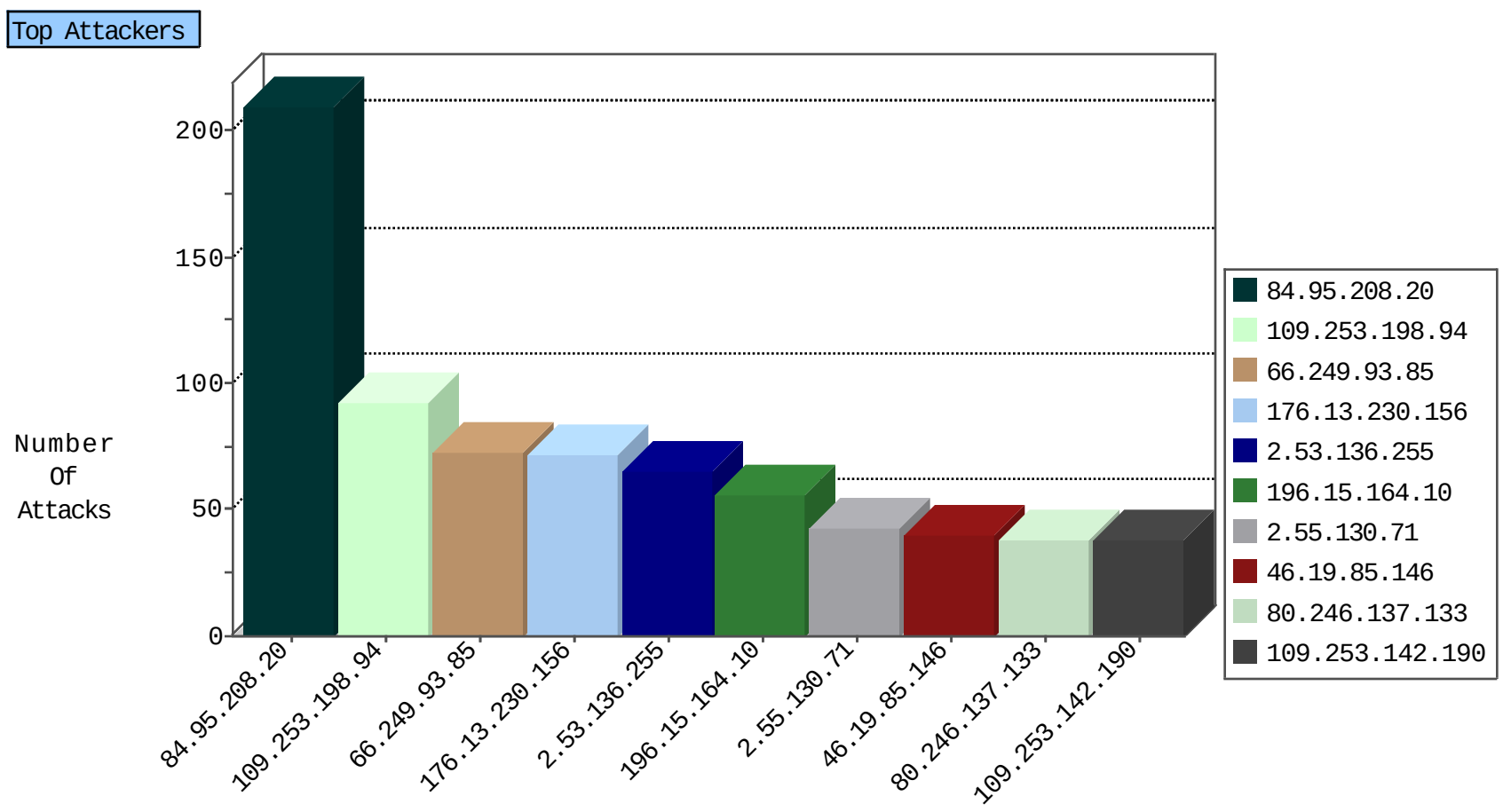
09-26-2016-12:04:00 to 09-26-2016-13:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-26-2016-12:04:00 to 09-26-2016-13:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.93.87	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
109.66.33.99	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
37.237.192.39	Iraq	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	3
109.65.72.179	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
209.126.136.2	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1
209.126.136.2	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.86	navy.idf.il	Black List	drop	1
84.52.98.134	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
209.126.136.2	United States	147.237.76.30	himush.idf.il	Black List	drop	1

09-26-2016-12:04:00 to 09-26-2016-13:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	12
5.29.217.24	Israel	147.237.72.156	aman.idf.il	32390: HTTP: Suspicious User-Agent (Mozilla)	Block	4
91.194.84.106	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
66.249.76.112	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-26-2016-12:04:00 to 09-26-2016-13:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.253.146.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.134.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
82.81.39.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.54.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.162.85	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.138.234.120	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.62.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.215.36.46	147.237.76.38	Kenya	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
208.80.155.255	147.237.77.74	United States	law.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	1
41.215.36.46	147.237.0.19	Kenya	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.187.89	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.148.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.240.250.154	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
13.90.253.185	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
109.64.133.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.1.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.250.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.181.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.128.121	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.177.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.215.36.46	147.237.76.44	Kenya	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.23.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
41.215.36.46	147.237.0.33	Kenya	idf.il	ET SCAN NMAP -sS window 1024	1
192.118.132.220	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
41.215.36.46	147.237.0.16	Kenya	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
31.24.228.20	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1

09-26-2016-12:04:00 to 09-26-2016-13:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.0.205.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
2.53.190.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
223.24.36.2	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
46.19.85.177	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	24
77.138.218.231	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
66.249.93.85	Europe	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
66.249.93.85	Europe	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	22
66.249.93.85	Europe	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
46.19.85.146	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
196.15.164.10	South Africa	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	17
46.19.85.146	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
196.15.164.10	South Africa	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence		monitor	14
87.69.40.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
141.226.218.97	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
31.168.52.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.67	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.67	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
66.249.93.83	Europe	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
196.15.164.10	South Africa	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
66.249.93.83	Europe	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	9
196.15.164.10	South Africa	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
66.249.93.83	Europe	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
87.69.40.170	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
212.143.187.65	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
196.15.164.10	South Africa	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
217.194.203.52	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
176.13.235.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.224.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.192.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.130.8	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.135	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.85	Europe	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	6
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
83.130.75.123	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
87.69.40.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.177	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
83.130.75.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.10.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.27	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.119	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.0.219.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.146	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5

09-26-2016-12:04:00 to 09-26-2016-13:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.198.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	84
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	78
176.13.230.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
2.53.136.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
2.55.130.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
80.246.137.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
109.253.142.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
176.13.12.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
46.19.86.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	20
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	12
60.181.128.232	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 60.181.128.232	Block	11
109.253.222.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
176.13.237.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
193.34.56.101	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	7
84.94.120.47	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	5
109.253.214.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
60.181.128.232	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	4
109.253.209.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
132.72.138.1	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	3
46.19.85.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	3
80.246.136.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.210.187.114	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
120.86.227.104	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 120.86.227.104	Block	3
2.55.28.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.156.40	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	2
46.19.85.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
5.29.205.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
66.249.76.85	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9682-he/refuah.aspx	Block	1
61.8.244.132	Australia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
84.95.85.110	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.19.86.132	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
176.13.228.164	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
79.181.248.167	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.168.226.132	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9032-he/refuah.aspx	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
46.116.90.65	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.248.80	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in Header Name	Block	1
82.80.55.83	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.93.85	Israel	147.237.77.216	dover.idf.il	Distributed URL is Above Root Directory	Block	1
2.55.151.66	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.6	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1

09-26-2016-12:04:00 to 09-26-2016-13:04:00