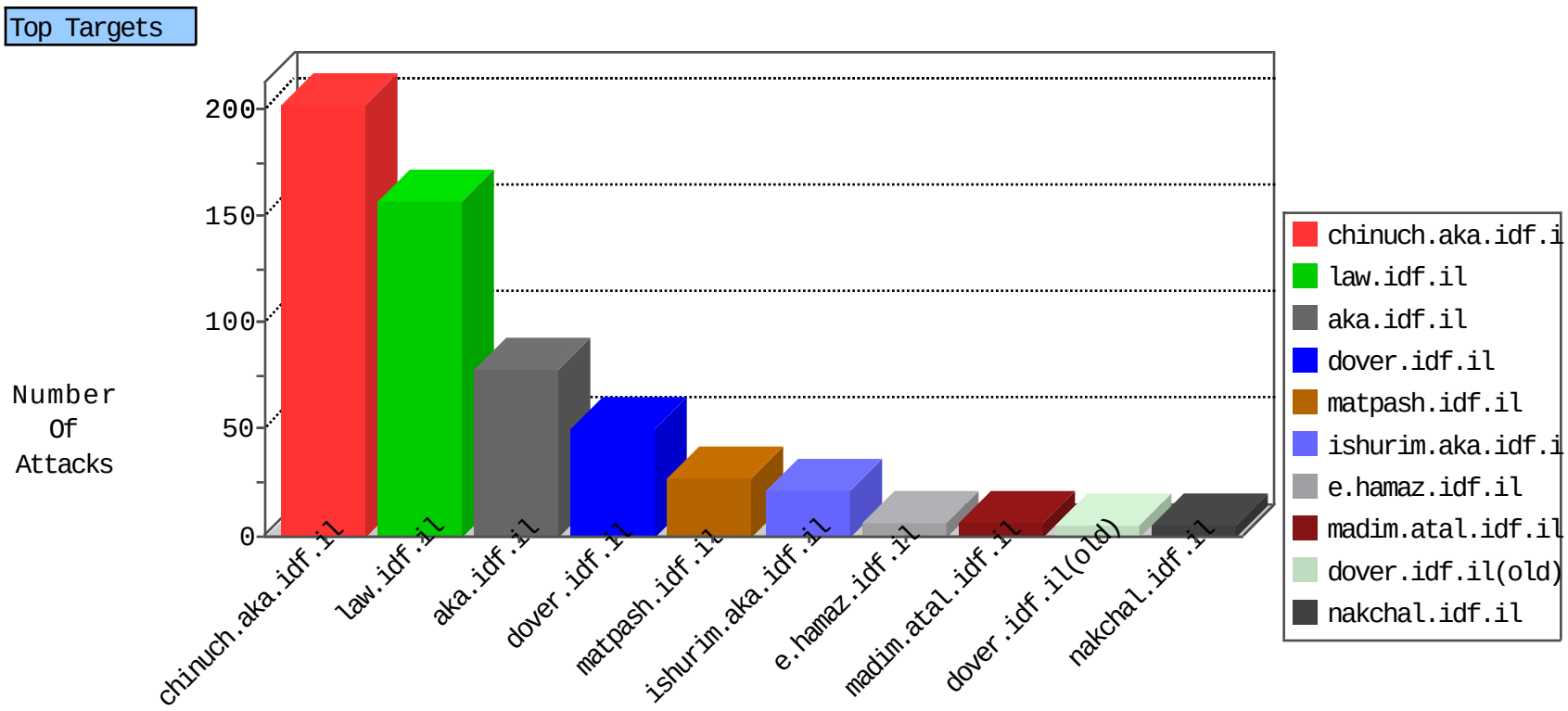
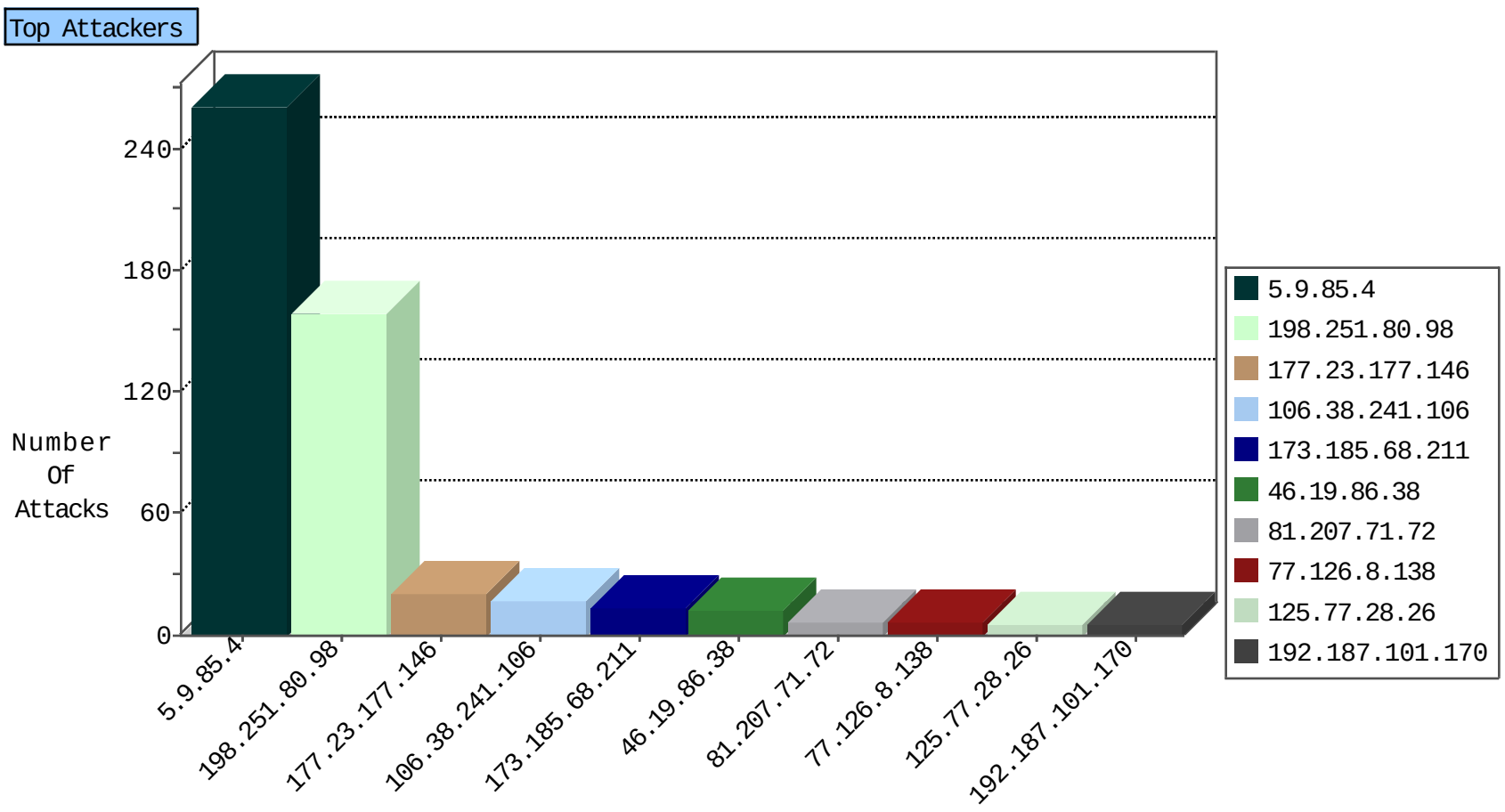
09-24-2016-02:04:08 to 09-24-2016-03:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-24-2016-02:04:08 to 09-24-2016-03:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
142.54.174.85	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
63.141.231.198	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
198.204.224.235	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
204.12.220.84	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
69.30.226.219	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
198.204.224.236	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
122.10.84.186	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
208.110.84.68	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
69.30.226.222	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
198.204.224.238	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	1
122.10.84.249	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
63.141.242.197	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
208.110.84.69	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
198.204.224.235	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
69.30.227.219	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
198.204.224.238	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
142.54.174.82	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
63.141.242.198	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	1
208.110.84.70	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
198.204.224.235	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
104.238.146.105	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
45.32.193.80	Netherlands	147.237.76.198	e.yohalan.idf.il	Black List	drop	1

09-24-2016-02:04:08 to 09-24-2016-03:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.85.4	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	156
5.9.85.4	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	49
5.9.85.4	Germany	147.237.76.147	chinuch.aka.idf.il	C1000074: HTTP: majestic bot	Permit	32
5.9.85.4	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	24
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	17
69.30.234.2	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.254.97.218	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
198.20.69.74	United States	147.237.77.212	e.dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
199.58.86.209	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1

09-24-2016-02:04:08 to 09-24-2016-03:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
163.172.238.45	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
46.161.40.17	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.238.45	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.187.89	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
81.170.162.82	147.237.77.227	Sweden	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
41.215.36.46	147.237.77.178	Kenya	e.matpash.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1

09-24-2016-02:04:08 to 09-24-2016-03:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	41
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	36
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	34
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	30
177.23.177.146	Brazil	147.237.72.167	ishurim.aka.idf.il	Header Rejection	header rejection pattern found in request	monitor	21
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	18
173.185.68.211	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
81.207.71.72	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.187.101.170	United States	147.237.72.14	dover.idf.il(old)	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
5.36.134.3	Oman	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
124.199.125.36	Afghanistan	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
176.13.1.89	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
185.32.179.220	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.247.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
185.40.64.65	Ireland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
125.77.28.26	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.176.119.184	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
176.13.248.83	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.55	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
125.77.28.26	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
185.40.64.65	Ireland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
141.212.122.63	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.232.110.28	United Kingdom	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
79.179.36.156	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.67.97.202	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.55	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
125.77.28.26	China	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.142.242.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
185.40.64.65	Ireland	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
128.232.110.28	United Kingdom	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1
141.212.122.59	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
125.77.28.26	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
218.22.211.69	China	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
188.44.55.20	Russian Federation	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
141.212.122.54	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.253.207.150	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.60	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
125.77.28.26	China	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
188.44.55.20	Russian Federation	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.54	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
2.53.173.207	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.62	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

09-24-2016-02:04:08 to 09-24-2016-03:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.126.8.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	3
217.66.158.41	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1395-en/dover.aspx	Block	2
204.52.135.166	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/kadatz/	Block	1
66.249.65.160	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-9067-he/atal.aspx	Block	1
66.249.75.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-22714-ar/dover.aspx	Block	1
66.249.66.72	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
109.65.79.170	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2391.jpg	Block	1
157.55.39.66	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.108	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/31ms02082010.aspx	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2424.jpg	Block	1

09-24-2016-02:04:08 to 09-24-2016-03:04:08