Blurring the lines: when residential proxies become DDoS botnets

Jérôme Meyer

Security researcher, Nokia Deepfield

jerome.meyer@nokia.com

Context

Context

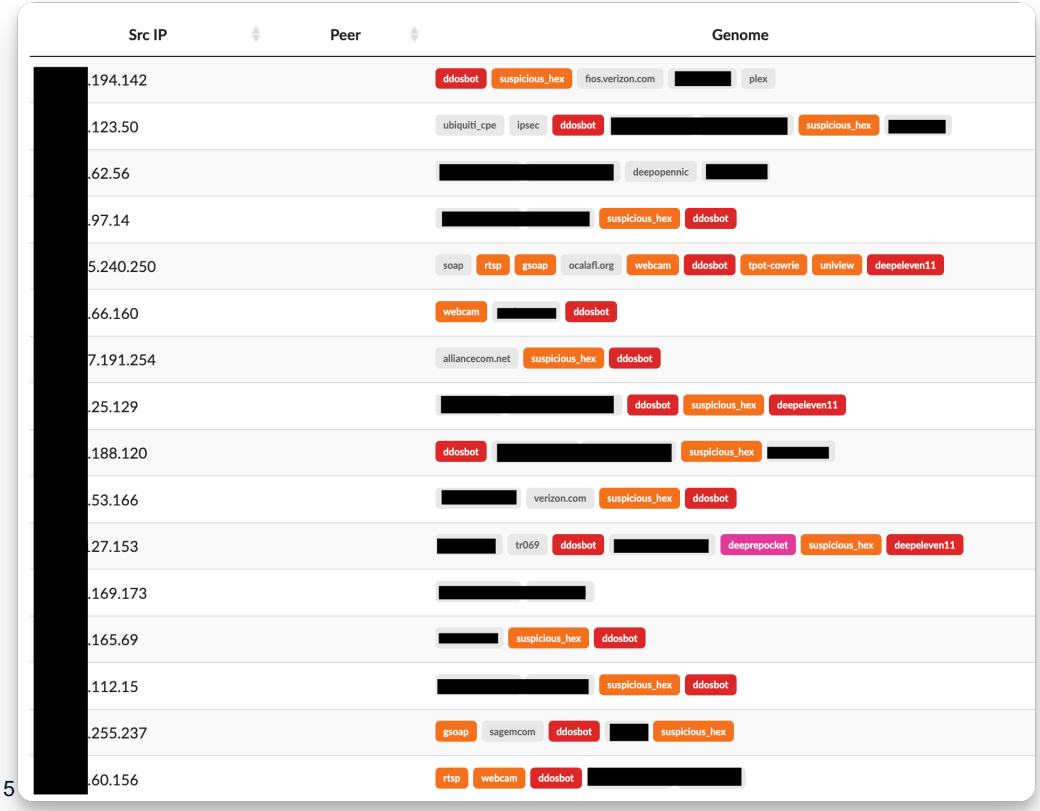
- Focused on distributed denial of service (DDoS) current and emerging threats
- Primary data sources
  - Sampled network telemetry (IPFIX/NetFlow/packets) from collaborating service providers
  - Active crawling of all IPv4 and all active IPv6 address space
  - Active residential proxy discovery

DDoS then (2020-2024)

- Volumetric DDoS quickly became IoT botnet-based (today >60% of total DDoS tonnage)
- Compromised DVRs, routers (Mikrotik, TP Link, …)
- Occasionally, the more entertaining parking meters or open Jupyter Server
- Scale:
  - **~1M** daily active bots
  - Low tens of thousand sources per attack

How DDoS looked then (to us)

Mirai-based botnet (mainly security cameras)



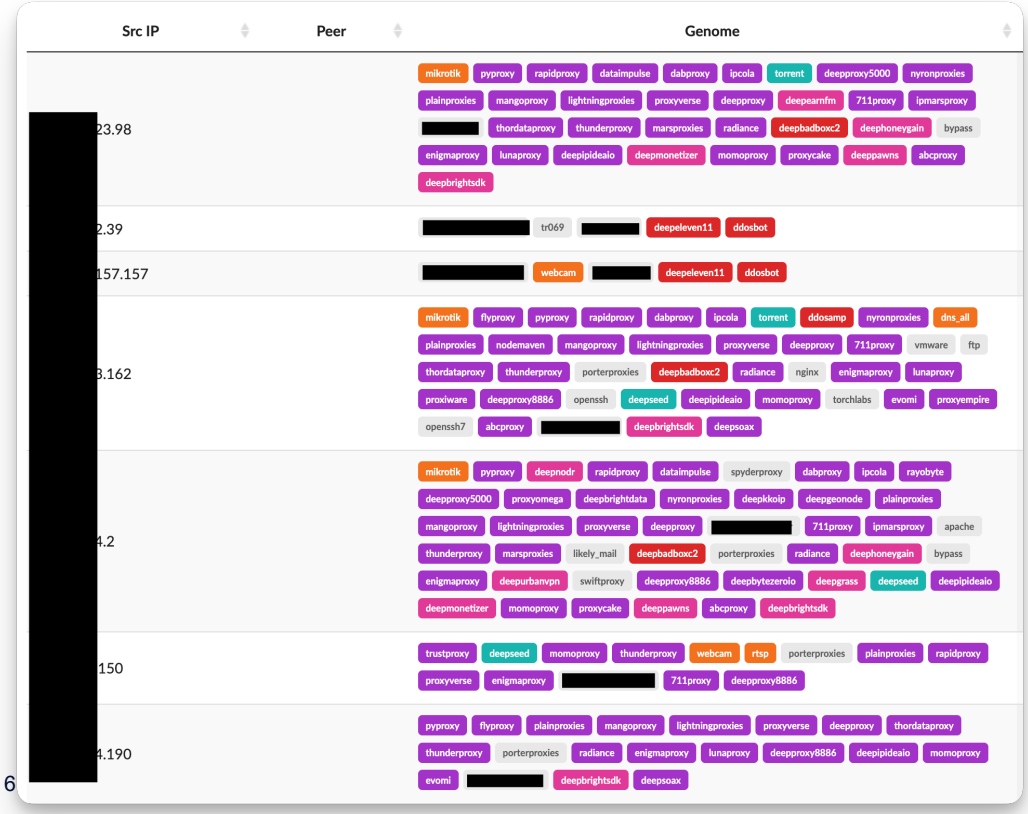
Src IP	Peer	Genome
[redacted].194.142		ddosbot suspicious_hex fios.verizon.com [redacted] plex
[redacted].123.50		ubiquiti_cpe ipsec ddosbot [redacted] suspicious_hex [redacted]
[redacted].62.56		[redacted] deepopennic [redacted]
[redacted].97.14		[redacted] suspicious_hex ddosbot
[redacted].5.240.250		soap rtsp gsoap ocalafl.org webcam ddosbot tpot-cowrie uniview deepeleven11
[redacted].66.160		webcam [redacted] ddosbot
[redacted].7.191.254		alliancecom.net suspicious_hex ddosbot
[redacted].25.129		[redacted] ddosbot suspicious_hex deepeleven11
[redacted].188.120		ddosbot [redacted] suspicious_hex [redacted]
[redacted].53.166		[redacted] verizon.com suspicious_hex ddosbot
[redacted].27.153		[redacted] tr069 ddosbot [redacted] deeprepocket suspicious_hex deepeleven11
[redacted].169.173		[redacted]
[redacted].165.69		[redacted] suspicious_hex ddosbot
[redacted].112.15		[redacted] suspicious_hex ddosbot
[redacted].255.237		gsoap sagemcom ddosbot [redacted] suspicious_hex
[redacted].60.156		rtsp webcam ddosbot [redacted]

36,686	19	2.7	508.2
DDOS SRC IP	DDOS DST IP	PEAK TBPS	PEAK MPPS

- Probable CVE
- Active in Botnet (48h)

How DDoS looked now

Overlap with residential proxy / BADBOX 2.0



36,924	515	3.9	343.2
DDOS SRC IP	DDOS DST IP	PEAK TBPS	PEAK MPPS

- Probable CVE
- Active in Botnet (48h)
- Active in Proxy (24h)
- Active in Monetization (48h)

What changed

- Unlike most compromised IoT, often not directly crawlable
- Mix of supply chain attack (BADBOX 2.0) + user installs (traffic sharing / passive income apps)
- Massive capital inflows from (some) AI companies for web scraping
- Scale:
  - **~100M** sources (30M active daily)
  - **Hundreds** of thousand sources per attack

What next

- Working with others in industry to tackle growing problem (financial/structural incentives + technical solutions)

- Happy to chat during the break!


NOKIA