






The Story of Yorkedy

The intelligent Botnet



How can I build a botnet?!



 » La Casa Del Bots - Automated Installs/Bots Shop-Mix&Geo El Profess0r [Pages: 1 2 3 4 ... 6]	EXCLUSIVE	50	2,827	★★★★☆	10 hours ago Last Post: Atroxcity
 HIGH QUALITY updates service [MIX, EU, US] kubuntu_ru [Pages: 1 2 3 4 ... 15]		141	18,640	★★★☆☆	01-28-2019, 03:00 AM Last Post: Sticky Bot
 XHVNC - Hidden Virtual Computing C++ FULL HIDDEN CONTROL STABLE AND MORE..... Shad0Byte [Pages: 1 2 3 4 ... 13]		123	5,422	★★★★☆	01-27-2019, 05:36 PM Last Post: Shad0Byte
 Auto-buy Video Tutorial - botnet for MINNING & KEYLOGGING + Automated Botshop J.P.Belmondo		7	424	☆☆☆☆☆	01-27-2019, 02:25 AM Last Post: Ikeyoung17
 INTX HTTP BOTNET ADVANCED REMOTE SYSTEM RECOVER BROWSERS BOTKILLER And MORE... Shad0Byte [Pages: 1 2 3 4 5]		47	3,523	★★★★★	01-26-2019, 10:03 AM Last Post: Shad0Byte

How can I buy a botnet?!



2019 NEW PRICES SHOP

World HQ Mix

500 bots HQ - 75\$

1.000 bots HQ - 120\$

2.000 bots HQ - 200\$

5.000 bots HQ - 450\$

Geo target HQ

Mini of 500 Loads - Price and pack in shop

<http://casadelbots.xyz>

Jabber:professor@thesecure.biz

Telegram:@casadelbots

Detection rate: **3/24** (No encryption used, No icon/file info used)

Scan Link

Price: **119.99\$**

Buy It Now!

Note: thanks for **Zettabit** for helping a lot with the panel.

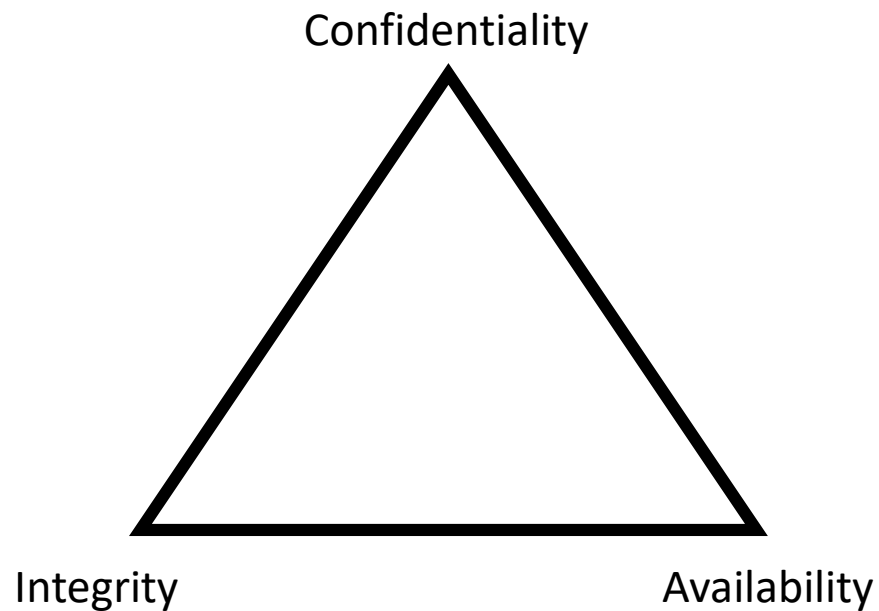
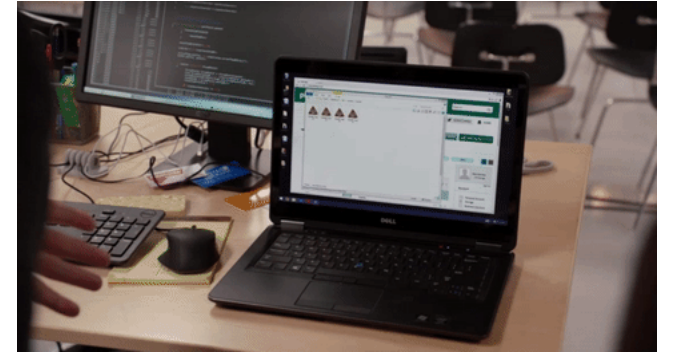
Payment methods: BTC/ETH/BCH

W_Z WARZONE



What's so interesting?

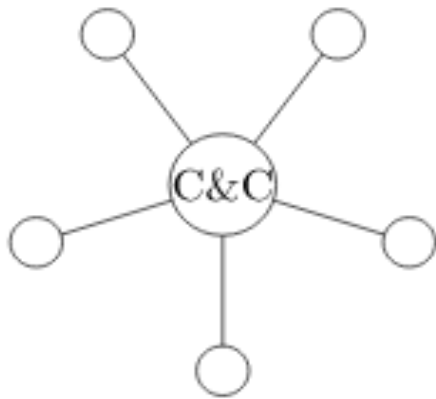
- You could be compromised right now
- Different bots, unique [purposes](#)



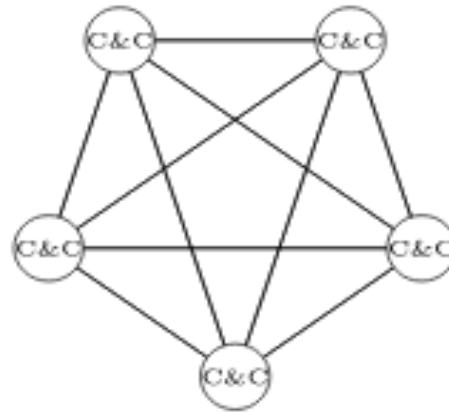
What do they look like?



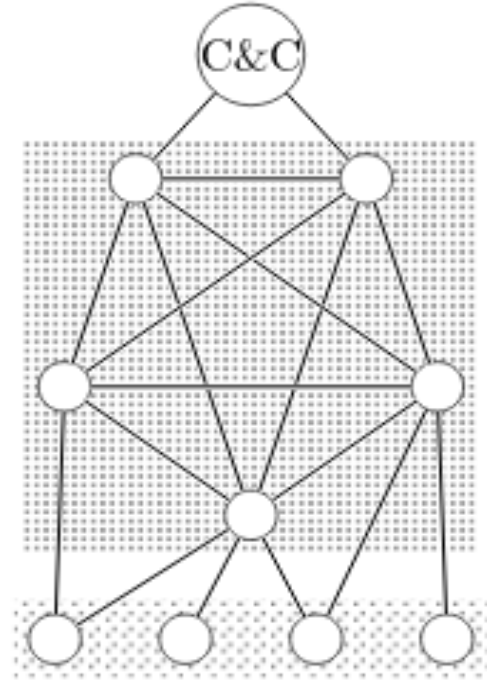
- Brilliant topologies



(a) Centralized botnet: One or multiple C&C server(s), multiple bots.

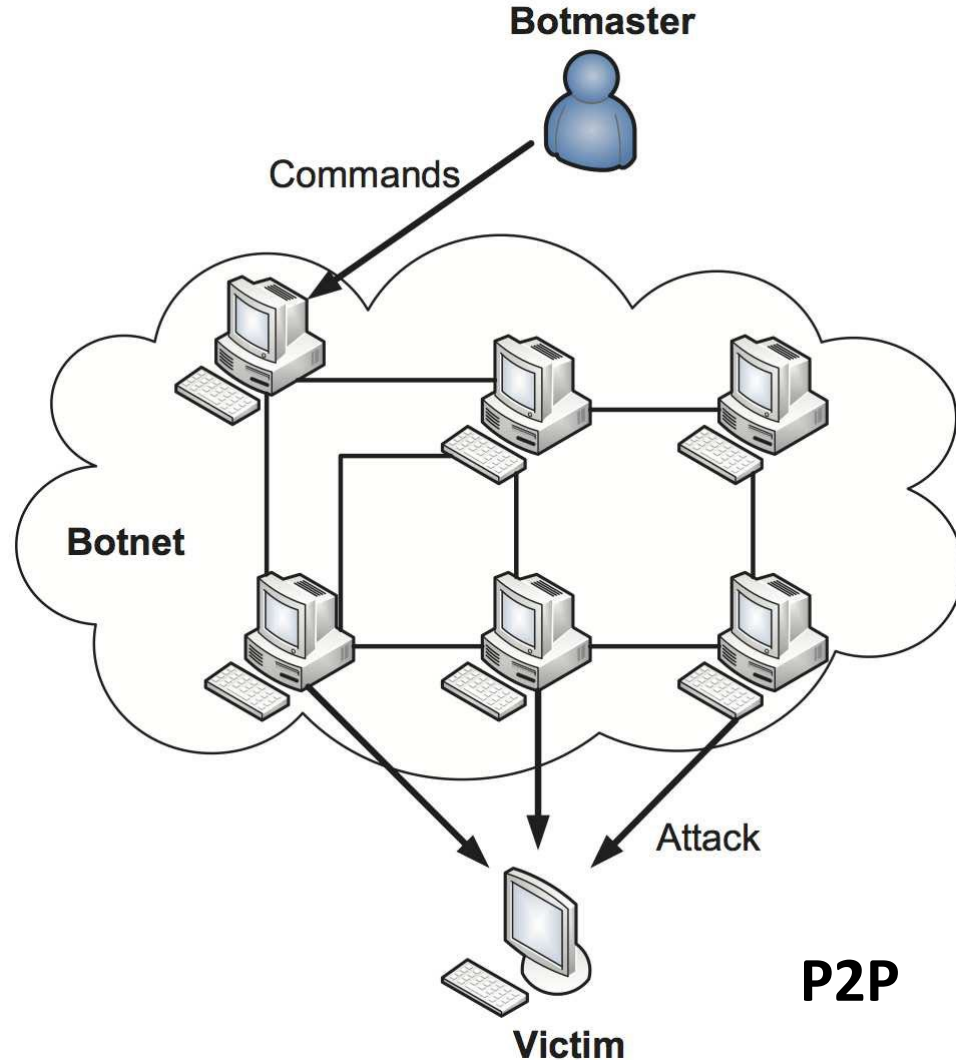
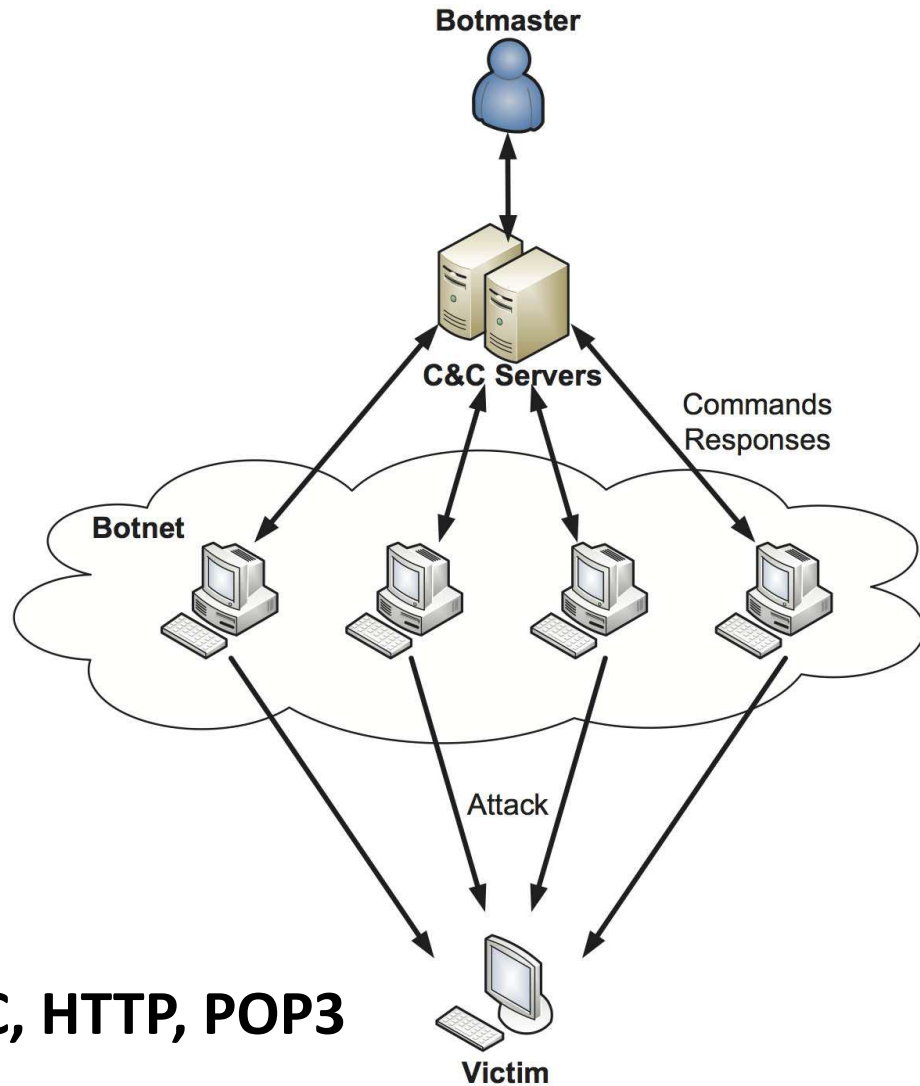


(b) Fully meshed P2P botnet: No dedicated C&C server, every bot can send commands.



(c) Hybrid P2P/C&C botnet: Combines P2P and centralized.

What do they look like?



What do they look like?



Instant Relay Chat (Port 6667)

Pros: easy to use, lots of resources

Cons: Easily detected(constant connection), single point of failure

HTTP & POP3

Pros: Harder to detect

Cons: Commands are not instant single point of failure (can be fixed)

P2P

Pros: No single point of failure, publisher subscriber architecture

Cons: Takes time to propagate command to each node



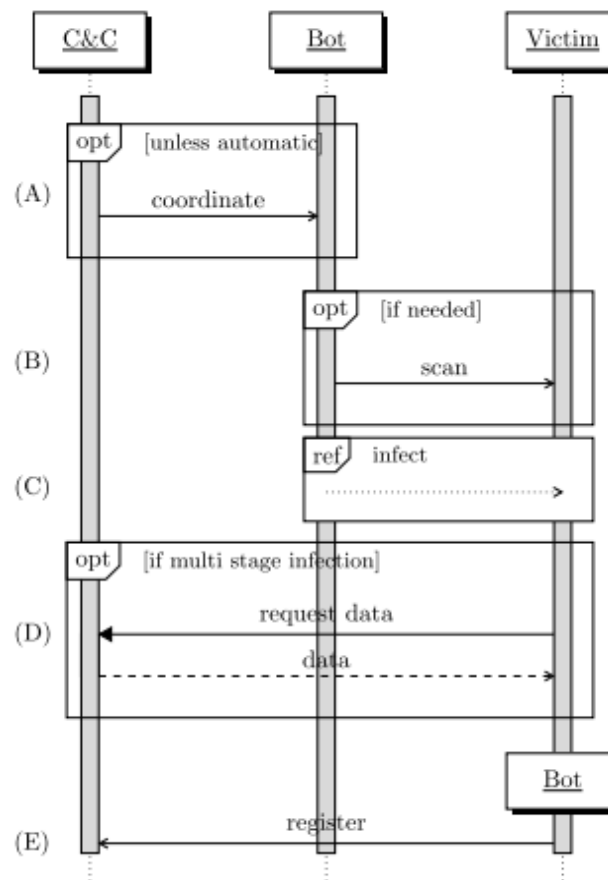
How do they act?

- **Active Propagation:**

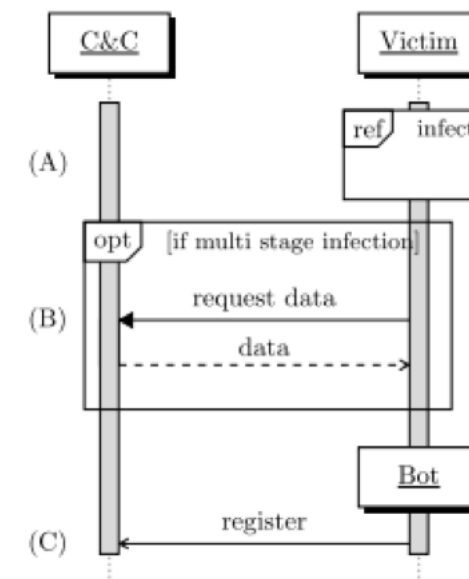
- Botmaster tells bots what to look for
- Ping, UDP or TCP port scans
- Vulnerability is exploited
- Botnet installation
- Register the infected

- **Passive Propagation:**

- Emails, websites, storage media
- "Drive-by Downloads"



(a) Active: Bots infect new machines via network with an optional scan step followed by the actual exploit.



(b) Passive: The victim is compromised indirectly.



Botnet Celebrities

Botnet	Year ¹	C&C Protocol	Topology	Encryption	Comp.	Purpose	Related/Family
Conficker	2008	HTTP, SMB, UDP, TCP	central; later P2P, central	RC4 (P2P)	-	distribute malware	Downadup, multiple versions (A – E)
Stuxnet	2005	HTTP, TCP, SMB named pipe	P2P, central	XOR	-	disrupt SCADA	Duqu, Duqu 2.0, Flame, Gauss, miniFlame
Zeus	2006	UDP, TCP, HTTP	central; later hybrid P2P/central	RC4	zlib	steal credentials	multiple variants, Gameover, Murofet, Licat

Conficker: Military bases in French and UK

Stuxnet: Supervisory Control and Data Acquisition (SCADA) in Iran's nuclear power plant

Zeus: \$70 million in stolen bank reserves, drive-by downloads

Adwind - Phishing emails - infected ~450k computers

Methbot - Programmatic video advertising - 3 million per day

How do they act?

- Persistence and [Evasion](#)
 - Injects into browser, registry
 - Rootkits
- Looking into the future
 - Smartphones
 - BotClouds



Fin

