EMPTY DDOS THREATS STILL NET ATTACKERS $100,000

threatpost

y Michael Mimoso Follow @mike_mimoso

April 26, 2016 , 2:43 pm

With some members of the so-called Armada Collective in jail, another actor has decided to co-opt their technique of sending threatening DDoS extortion messages to businesses worldwide.

Only difference is, this group isn't following through with its threat, and it's still collecting serious money.

Key members of the Armada Collective, also known as DD4BC (DDoS for Bitcoin), were put away in January by Europol during Operation Pleiades. The group had extorted virtual coins from businesses for more than two years before the arrests. According to reports from Akamai and Recorded Future, the group would threaten DDoS attacks of a significant magnitude—anywhere from 500 Gbps and 1 terabyte-per-second—but usually followed through with smaller attacks.

"If you don't pay by [date], attack will start, yours service going down permanently price to stop will increase to 20 BTC and will go up 10 BTC for every day of attack. This is not a joke," says the note.

The emails threaten 1 Tbps attacks that will elude detection, and demand anywhere from 10 to 50 Bitcoin in payment; 50 Bitcoin is approximately $23,000 USD.

botnets

cs642

computer security

adam everspaugh

ace@cs.wisc.edu

today

* Malware & botnets
  / Uses
  / Command and Control
  / Size estimation

Botnets

- Botnets:
  - Command and Control (C&C)
  - Zombie hosts (bots)
- C&C type:
  - centralized, peer-to-peer
- Infection vector:
  - spam, scanning, worm (self-propagating virus)
- Usage: ?

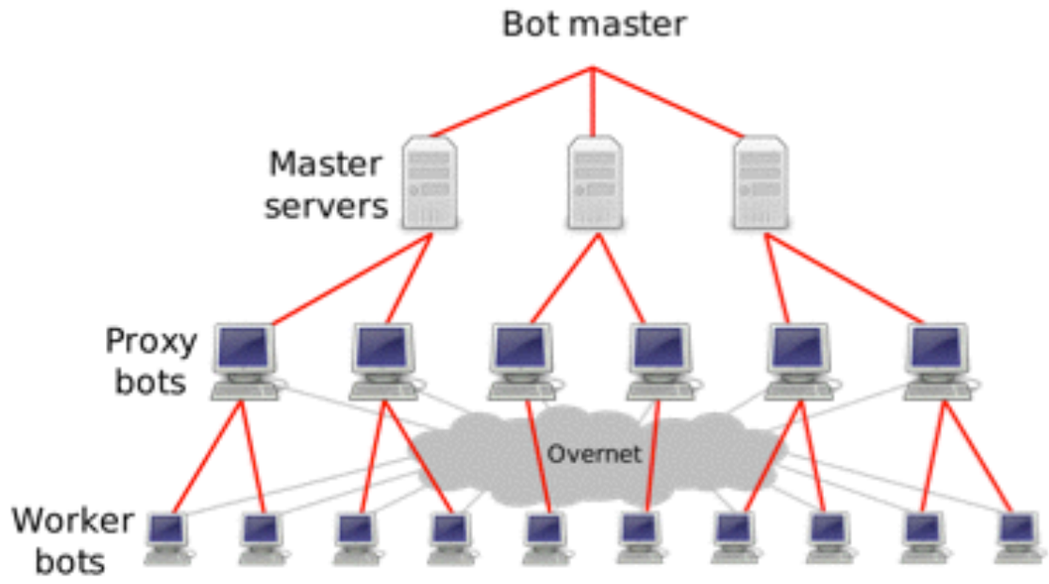


Figure 1: The Storm botnet hierarchy.

How to make money off a botnet?

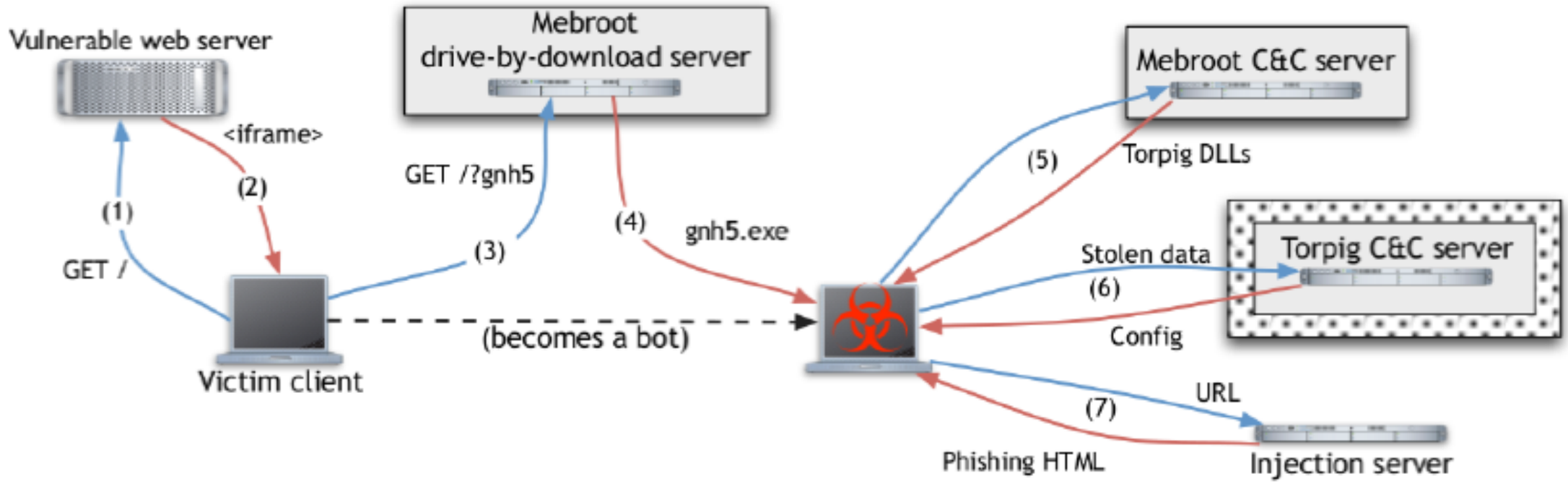
think-*pair*-share

- Rental
  - "Pay me money, and I'll let you use my botnet… no questions asked"
- DDoS extortion
  - "Pay me or I take your legitimate business off web"
- Bulk traffic selling
  - "Pay me to direct bots to websites to boost visit counts"
- Click fraud, SEO
  - "Simulate clicks on advertised links to generate revenue"
  - Cloaking, link farms, etc.
- Theft of monetizable information (eg., financial accounts)
- Ransomware
  - "I've encrypted your harddrive, now pay me money to unencrypt it"
- Advertise products

Torpig Botnet

- 2005-2009?
- 50k-180k bots
- 2008: "Most advanced piece of crimeware ever built"
- Use *domain flux* to contact command and control (C&C) servers
- Hijacked by UC Santa Barbara researchers and studied for 10 days

[*Your Botnet is My Botnet: Analysis of a Botnet Takeover*, 2009, Stone-Gross et al.]



How to join a Torpig botnet

1: Click on dodgy link to vulnerable website

2-4: Download Mebroot malware

5: Mebroot downloads Torpig DLL (your a bot!)

6: Upload all you sensitive data to Torpig C&C

7: Profit! (not yours)

What are defenses?

think-*pair*-share

Domain Flux

- Each bot generates candidate domain names for C&C servers
- Probe each one, use the first one that talks the C&C protocol
- Researchers ran the algorithm forward several weeks
- Discovered un-registered domains and registered them
- Setup their own C&C server
- Your botnet is my botnet

```
suffix =  ["anj", "ebf", "arm", "pra", "aym", "unj",
    "ulj", "uag", "esp", "kot", "onv", "edc"]

def generate_daily_domain():
    t = GetLocalTime()
    p = 8
    return generate_domain(t, p)

def scramble_date(t, p):
    return (((t.month ^ t.day) + t.day) * p) +
        t.day + t.year

def generate_domain(t, p):
    if t.year < 2007:
        t.year = 2007
s = scramble_date(t, p)
c1 = (((t.year >> 2) & 0x3fc0) + s) % 25 + 'a'
c2 = (t.month + s) % 10 + 'a'
c3 = ((t.year & 0xff) + s) % 25 + 'a'
if t.day * 2 < '0' ||  t.day * 2 > '9':
    c4 = (t.day * 2) % 25 + 'a'
else:
    c4 = t.day % 10 + '1'
return c1 + 'h' + c2 + c3 + 'x' + c4 +
    suffix[t.month - 1]
```

Listing 1: Torpig daily domain generation algorithm.

Stealing a botnet

- Researchers bought two domains and hosting
- Put up C&C server to capture all reported information by bots
- Controlled Torpig botnet for 10 days
- Captured 70 GBs of stolen information
- Used these data to study how big the botnet was and what it did (crime)

- C&C hijack to take-down a botnet is called *sinkholing*

Estimating botnet size

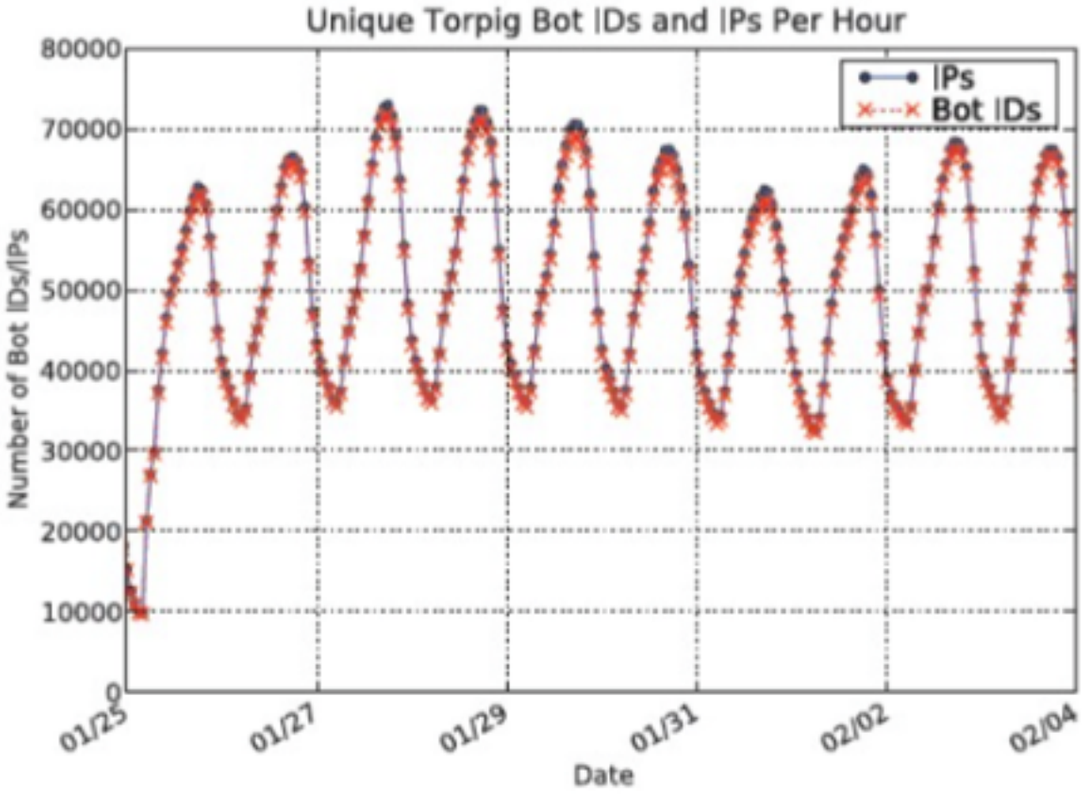


Figure 9: Unique Bot IDs and IP addresses per hour.

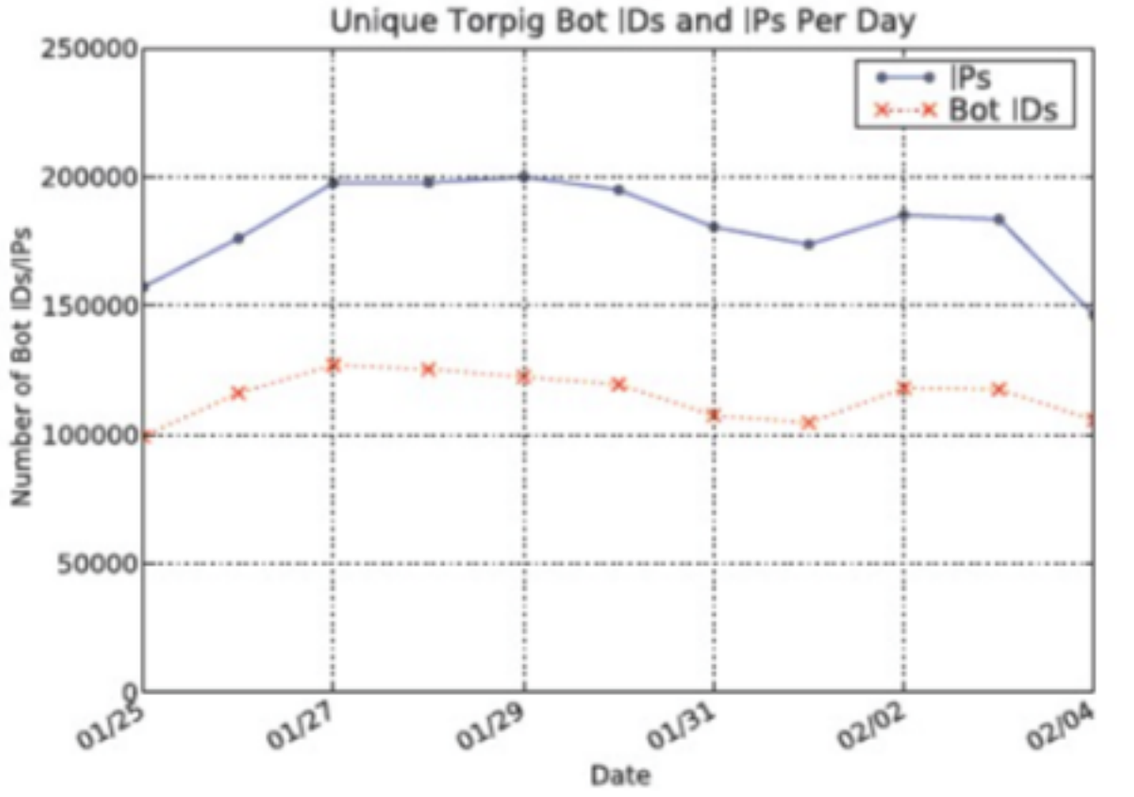


Figure 10: Unique Bot IDs and IP addresses per day.

Torpig bots report to C&C servers using a unique botnet ID

Useful for correctly estimating size

Table 1. Data items sent to our C&C server by Torpig bots.

Data type	Data items
Form data	11,966,532
Email	1,258,862
Windows password	1,235,122
POP account	415,206
HTTP account	411,039
SMTP account	100,472
Mailbox account	54,090
FTP account	12,307

Stealing Financial Accounts

In 10 days, stolen accounts from:

- Paypal (1770)
- Poste Italiane (765)
- Capital One (314)
- E*Trade (304)
- Chase (217)

Country	Institutions (#)	Accounts (#)
US	60	4,287
IT	34	1,459
DE	122	641
ES	18	228
PL	14	102
Other	162	1,593
Total	410	8,310

Table 3: Accounts at financial institutions stolen by Torpig.

Ethics

Two principles to protect victims

- PRINCIPLE 1.
  - The sinkholed botnet should be operated so that any harm and/or damage to victims and targets of attacks would be minimized.
- PRINCIPLE 2.
  - The sinkholed botnet should collect enough information to enable notification and remediation of affected parties.

recap

* Malware + botnets
  / Botnet uses
  / Architecture
  / Domain flux, C&C hijacking