ZeuS v3
p2p network
monitoring
Tomasz Bukowski
CERT Polska
Agenda

• The history of this case
• Data distribution in new ZeuS [v3]
• ZeuS-p2p network
• p2p messages
• Our crawler
• p2p network structure
• Data propagation speed
The history ...

- **September 2011**
  - first news about zeus p2p/murofet
- **October 2011**
  - First articles on the web
- **November 2011**
  - We got the binary sample!
  - We suspected that the botnet will be inactive soon ...
- **December 2011** - first results of analysis
  - Incubated sample is still active
  - Alpha version of crawler started - colected 10000 nodes
  - Beta version of crawler running till 20 Jan 2012
- **January 2012**
  - Crawler reports lower rate of valid answers
  - We suspected that the botnet will be inactive soon (again? :P)
  - After closer look -> there was bigger update at 15 Jan!
- **February 2012**
  - Still alive!
ZeuS v3 - Data distribution

The diagram illustrates the process of data distribution in ZeuS v3. The botmaster communicates with compromised servers through a Domain Generation Algorithm (DGA) to generate malicious domain names. These domains are used to deliver malware to the victim's computer.
ZeuS p2p network

• Based on kademlia

• Any ID = SHA1 hash [20 bytes]

• Communication on high TCP and UDP port

• Infected computer - node :
  • node-ID
  • node-IP
  • node-UDP-port
ZeuS p2p network - message types

- **Version Query**: version of configuration file, TCP port for data transmission
- **Nodes Query**: 10 nodes ([nodeID, IP, and UDP port])
get node from DB

send Version Query

save result

send Nodes Query

save new nodes into DB
Crawling results

- Nodes count in DB on start: 1
- After 4 weeks: over 925,000 nodes
  - ~870,000 with valid IP/PORT/ID [null values etc.]
- Uniq-IP: ~560,000
- Uniq-ID: ~230,000
- 20,000 ID have more than 10 IP addresses
Crawling results

Children count distribution
Crawling results

Parent count distribution
Crawling results - zp2p network
Crawling statistics

number of answers
number of queries

1 day
Results of analysis of collected ‘version responses’ over time:

- 85% of responses after 7 days
- sqrt scale

ZeuS p2p network - information propagation
ZeuS p2p network - information propagation

1 hour!
List of IP + ASN + CC
collected by crawler!
Questions?

Contact:

www.cert.pl

info[at]cert.pl

tomasz.bukowski[at]cert.pl