Configuring Zeus: A case study of online crime target selection and knowledge transmission

Alice Hutchings

Richard Clayton

University of Cambridge

Zeus

- "Man in the browser" malware
  - steals credentials & cookies
  - can alter web pages to hide what it is doing
- Other components, so essentially a "platform"
- Development started in 2005
- Widely deployed from 2007 to ~2012

Zeus Configuration

- Configuration file needed for each target bank
  - specifies which URLs are relevant
  - specifies what to keylog (or screenshot)
  - can dynamically alter pages (“webinjects”)
  - can redirect to another site etc. etc.
- Configuration files not trivial to create
- Files were encrypted (but decryptors were developed by white hats & widely circulated)

Research

- Tajalizadehkhoob et al. (WEIS 2014)
  - examined 11 000 configuration files & 1.2 million webinjects and found lots of similarities
  - they suggested that the configuration files were being shared, sold or stolen…
- We wanted to look for evidence of this…
  - so searched 120 criminal forums for discussions
  - found 65 public messages on 9 forums
    - written in English/German/Russian

Aside

- Our paper is “qualitative”
- We’re not presenting lots of data and doing statistics on it (i.e. it is not “quantitative”)
- Instead we look to understand what is going on and present illustrative examples
  - this is important when seeking to understand the structure and nature of a problem and perhaps to do groundwork for future quantitative research

Sharing, Selling, Stealing

- There's evidence for all three mechanisms

1. 2008 (webinjects were then provided)

   "Hi, I got ahold of Zeus 1.1 but its missing the config file. Can anyone point me to where I can find one?"

2. 2009 advert for binary (or builder for €3500)

3. *It is not good to steal from your own people. Those who unpack other people's configs are not just a deceivers but bitches. Instead of being useful to do something they do bull shit. Where are you fuck come from!?*

Sharing of information

- Various discussions found sharing general tips about configurations, how to spread the malware, how to configure control panels etc
- Some evidence of it being a barter economy!

[username] i helped you to sut up this shit where is ur part of deal ???????????

What changed over time? #1

- Security researchers created decryption tools
- So the criminals used these to steal contents of configuration files, with varying success:

Very big cons is that the result is a complete mess with injects. there are some people who founds this mess completely useful:) As dear [username] said to me: it is better to rewrite everything from scratch than collect unclear pieces!

What changed over time? #2

- Source code of #2.0.8.9 was leaked
  - and "malware as a service" appeared

[RESELLING] Zeus 2.0.8.9 FULL SETUP + WEBINJECTS + VNC + INSTALLS Hello Guys, I'm reselling my account of Zeus 2.0.8.9 bin which included: – Zeus 2.0.8.9 already installed and ready to use; – Zeus Webinjects included; – Zeus Config.bin; – Zeus .EXE FUD; – Zeus VNC + tutorial;
– Zeus 1k Installs (worldwide) included. Is hosted on offshore hosting and have a bulletproof domain. First month is free (included on price). If you want to continue using it you have to pay $50 / month. Price: $250 (LR or WMZ) ESCROW WELCOMED

Final Remarks

- Other communication methods do exist!
- Clear evidence of collaboration
- Configurations were “shared, sold and stolen”
- Evidence of risks in using Zeus
  - discussion of backdoors in the systems
  - there were webinjects for WebMoney !
- Some messages were deleted as a precaution
  - which is why we found fewer than we expected

Configuring Zeus: A case study of online crime target selection and knowledge transmission

https://www.cl.cam.ac.uk/~rnc1/configuringzeus.pdf

https://lightbluetouchpaper.org

https://cambridgecybercrime.uk