

Sun Tzu was a Hacker - A Examination of the Tactics and Operations from a Real World Cyber Attack

This presentation will cover the operational and tactical techniques used in a “real world” cyber attack, including an analysis of the planning, command, control, execution, and outcome of these cyber attacks. The presentation is exceptional, as the presenters were in a unique position to observe the communications, execution, and responses from both the attacking and defending entities. This presentation is focused on the low level, technical details of the observed attacks, with follow-up intelligence-based analysis of the impact of these details. Specially, this talk will cover:

- Detailed and highly technical examination of the specific tactics and techniques used in Distributed Denial of Service (DDoS) and targeted attacks.
- An examination and presentation of online hacker forums.
- Analysis and presentation of the target lists published by the attackers.
- An examination and description of the methods used for information dissemination to grass roots hacking efforts in support cyber attacks against state assets.
- Dissection and technical overview of the specific tools created and used in support of cyber attacks.
- Dissection of the sophistication of the attackers and the attacking techniques used in real world cyber attacks.
- Examination and explanation of the exact payloads and techniques used to compromise state systems targeted in the attack.
- Detailed and technical analysis of log files from the attacked/compromised systems.
- Comparison of the operational and tactical techniques used in cyber warfare and traditional warfare (using US Marine Corps Doctrinal Publication (MCDP) # 1 – Warfighting).

The information and evidence gathered for this presentation was part of the “GreyGoose” Project (<http://blog.wired.com/defense/2008/09/onine-posse-ass.html>) and will present items not discussed in the in the formal report or in any other presentation. The style of the presentation calls for 2 speakers (Billy Rios and Jeff Carr), one speaker offering technical analysis and one speaker offering Intelligence analysis (this can be changed to a single speaker, but we would prefer a co-presentation). Currently, the presentation covers 60-90 minutes of content; however the content can be adjusted to meet conference time requirements.