(TS//SI//NF) DGO Enables Endpoint Implants via QUANTUMTHEORY

By [[REDACTED]] on 2011-09-26 1548

(TS//SI//NF) In another example of the emerging collaboration between the Endpoint and Midpoint missions, the QUANTUM team had another marked success during the week of 12 September 2011. TAO’s R&T analysts identified an opportunity to use QUANTUMINSERT to exploit a Pri-1 CT target, Badruddin Haqqani, the senior leader in the Haqqani network located in the Miram Shah in Pakistan’s tribal area. Badruddin’s importance has recently come under closer scrutiny by U.S. Government policymakers due to his involvement in the attack on coalition forces in Afghanistan with a large truck-borne IED.

(TS//SI//NF) QUANTUMINSERT is meant to briefly hijack connections between a specific target and a web connection in order to redirect the target to a TAO server (FOXACID) for implantation. To implement this, SIGDEV analysts worked with SSO’s DANCINGOASIS (DGO) collection management to put four specific signal case notations on cover. Using the tips from the collection from DANCINGOASIS, 47 shots from QUANTUMINSERT were taken resulting in 22 FOXCONTACTs, including nine from this specific target. This meant nine opportunities to implant the target. One of these was successful, resulting in the VALIDATOR implant being installed on the target computer. This allows TAO to formulate and execute plans for further exploitation of the target’s computer.

…

(TS//SI//NF) QUANTUMTHEORY success at SARATOGA

By [[REDACTED]] on 2011-04-15 0758

(TS//SI//NF) QUANTUMTHEORY culminated its first week running at SARATOGA with a successful exploit of a Pakistani target for TAO’s R&T organization. QUANTUMTHEORY (QT) is a set of CNO Man-on-the-Side capabilities that involve real-time responses to passive collection. After the recent TURMOIL upgrade at SSO’s SARATOGA access, TAO operators were able to run QUANTUMHAND which exploits the computer of a target accessing his facebook account. Briefly, when quantum is tipped that a target is using Facebook, quantum pretends to be the Facebook server and sends a response to the target. This fake response contains a link to TAO’s FOXACID server, which implants the target’s computer. In just a week, nearly 100 “shots” have been fired on 14 targets using QUANTUM from over 1300 tips received from SARATOGA. More targets are being added. This collaboration between TD, SSG, TAO, and SSO is another successful example of the emerging emphasis on Endpoint-Midpoint Integration.