MHS Leverages XKS for QUANTUM Against Yahoo and Hotmail

TOP SECRET//SI//REL TO USA, FVEY

(TS//SI//REL) MHS Leverages XKEYSCORE Deep-Dive Packet Analysis to Identify Feasibility of QUANTUM Against Yahoo and Hotmail
(TS//SI//REL) Automated deep packet analysis of Yahoo and Hotmail providers gives insight into the potential success of QUANTUM exploitation against these services.
(TS//SI//REL) QUANTUMTHEORY is a set of CNO man-on-the-side capabilities that involves real-time packet inject in response to passive collection of target communications. QUANTUMTHEORY inspects each packet, at one a time, for a set of keywords that determine if the packet originated from a CNE target and if a modified response to that packet might result in exploitation of the client. Because each packet is inspected individually, if keywords occur across packet boundaries the QUANTUMTHEORY technique will not tip the SIGINT system to attempt exploitation of a client. As HTTP headers and the size of cookies grow, the likelihood of all keywords occurring within a single packet reduces. MHS analysts, in collaboration with XKEYSCORE and the ROC, productized DRAGABLEKITTEN, an XKEYSCORE Map/Reduce analytics that leverages packets collected and made accessible to analytics by XKEYSCORE DEEPDAIVE systems.

DRAGABLEKITTEN identifies the QUANTUMTHEORY keywords in a packet capture and generates statistics for each service (currently Hotmail and Yahoo) to determine how often all the keywords occur within a single packet. This would not have been possible without XKEYSCORE providing a platform for analysis to mass-deploy packet-level processing. Approximately 50% of Hotmail and 90% of Yahoo sessions contain the keywords necessary within a single packet to be targeted by QUANTUMTHEORY.

Collaboration: (U/FOOU) name redacted Access Operations Division, TAO/ROC; name redacted XKEYSCORE, R1
POC: (U/FOOU) name redacted INDEX Division, MHS phone number redacted