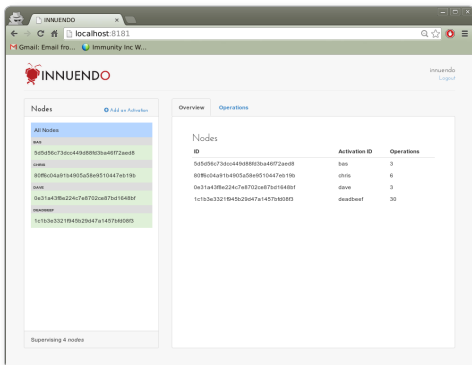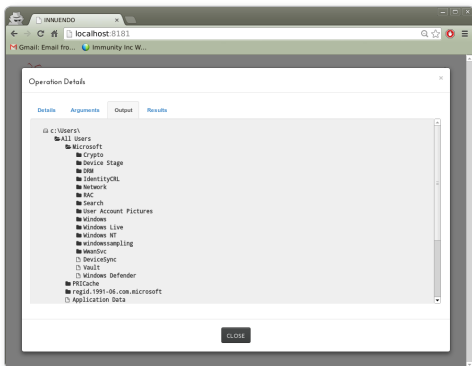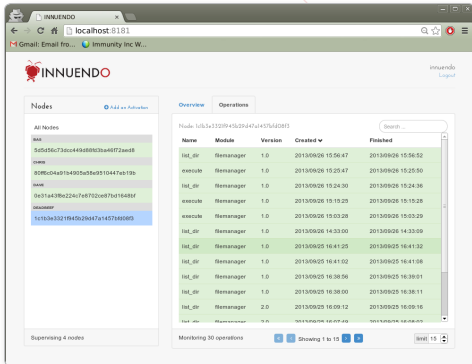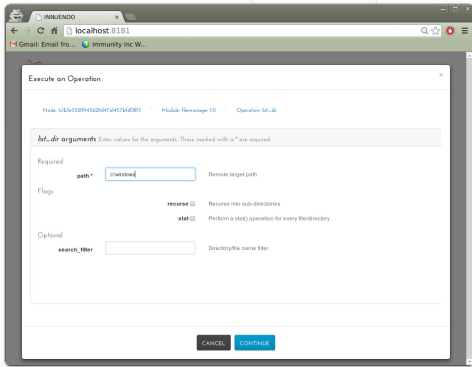# INNUENDO

INNUENDO – An Advanced Penetration Testing tool for modeling Advanced Attackers

INNUENDO raises the bar for the state of the art in persistence and data exfiltration solutions. Based on a flexible, modular architecture, **INNUENDO** offers nation-grade advanced attack capabilities to commercial penetration testing teams.

■ **INNUENDO** breaks from the current penetration testing model by using a message passing protocol that is completely decoupled from any transport layer. This allows for a wide range of communication channels which are easily integrated into your **INNUENDO** solution. Examples include: HTTPS, DNS, ICMP, PDF, Social Media, and steganographic injection into popular image hosting services.

■ Persistence can be maintained via any one of many ways, determined at deploy time. That means no static indications of compromise! Persistence methods are modular and updatable throughout the life of the deployment.

■ **INNUENDO** functionality can be written, deployed and updated in Python without ever touching disk and is encrypted and signed for a specific **INNUENDO** instance on deployment.

■ Each deployed **INNUENDO** has a unique SHA1 hash which prevents one-stop binary fingerprinting.

INNUENDO can be deployed entirely from memory via e.g. a **CANVAS** exploit, a post-exploitation **CANVAS** module, or from another **INNUENDO** instance. **INNUENDO** can run as an injected DLL or as its own process.

INNUENDO instances employ strong encryption for C&C messages, which renders the communications opaque to listeners and frustrates post-event forensics.

FROM THE TOP

EXECUTE AN OPERATION – A file system operation being queued for execution by a remote INNUENDO instance. / OPERATIONS – Here you can see the history of all operations executed by an INNUENDO instance and their current status. / LIST DIRECTORY OUTPUT – Directories and files are listed nicely and selecting a file to queue for download is just one click away. / OVERVIEW – Each activation ID can be limited so that it cannot spread beyond your intended audience.