VALIDATOR

VALIDATOR is a part of a backdoor access system under the FOXACID proje
VALIDATOR is a client/server-based system that provides unique backdoor ac
personal computers of targets of national interest, including but not limited to t
targets. VALIDATOR is a small Trojan implant used as a back door against a v
targeted Windows systems, which can be deployed remotely or via hands on ac
any Windows box from Windows 98 through Windows Server 2003. The LP is
24/7 and tasking is 'queued', that is, jobs sit in a queue waiting for the target to
home', then the job(s) are sent one at a time to the target for it to process them.
Commands are Put a file, get a file, Put, then execute a file, get system informa
change VALIDATOR ID, and Remove itself. VALIDATOR's are deployed to
systems and contact their Listening Post (LP) (each VALIDATOR is given a sp
unique ID, specific IP address to call home to it's LP); SEPI analysts validate t
identity and location (USSID-18 check), then provide a deployment list to Olyr
operators to load a more sophisticated Trojan implant (currently OLYMPUS, fu
UNITEDRAKE). An OLYMPUS operator then queue up commands for the spe
VALIDATOR ID's given by SEPI. Process repeats itself. Once target is hooke
more sophisticated implant, VALIDATOR operators tend to cease. On occasio
operators are instructed by SEPI or the SWO to have VAIDATOR delete itself.

OLYMPUSFIRE

OLYMPUSFIRE is an exploitation system that uses a software implant on Microsoft Windows based target PC to gain complete access to the targeted I target, when connected to the Internet, will contact a Listening Post (LP) loc NSA/USSS facilities, which is online 24/7, and get its commands automatica These commands include directory listings, retrieving files, performing netm The results of the commands are then returned to the LP, where the data is cc and forwarded to CES and analysis and production elements.