Tailored Access Operations

[redacted] - TAO

[redacted] - SSG

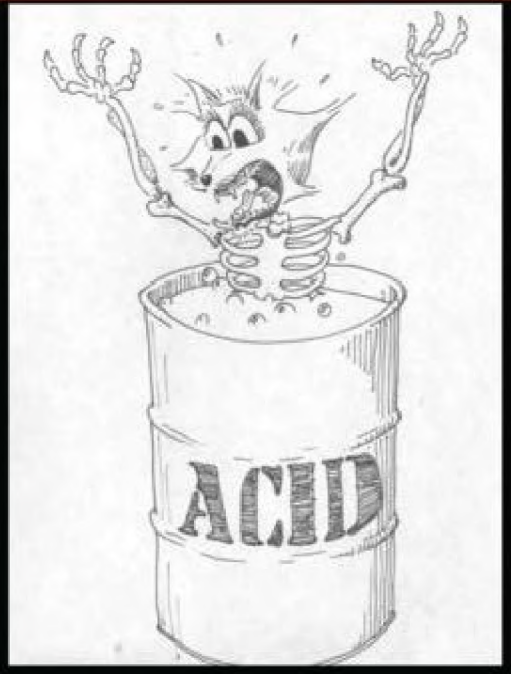
[redacted] - TAO / R&T

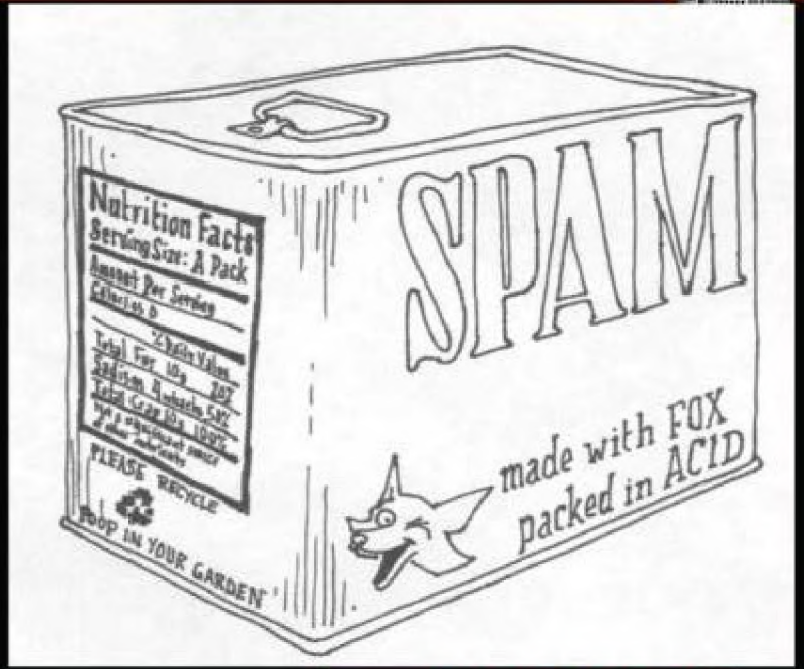
tao inside

OVERALL CLASSIFICATION: TOP SECRET//COMINT//REL to USA,FVEY

SPIEGEL ONLINE

FOXACID





Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20291123

SPIEGEL ONLINE

What is QUANTUM?

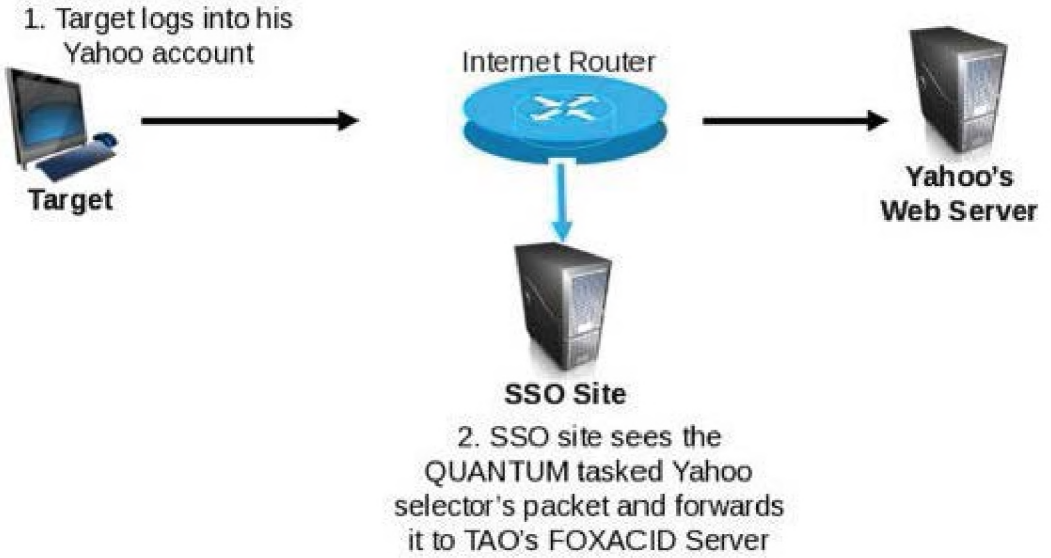
QUANTUM Generic Animation – High Level of How It Works

What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works

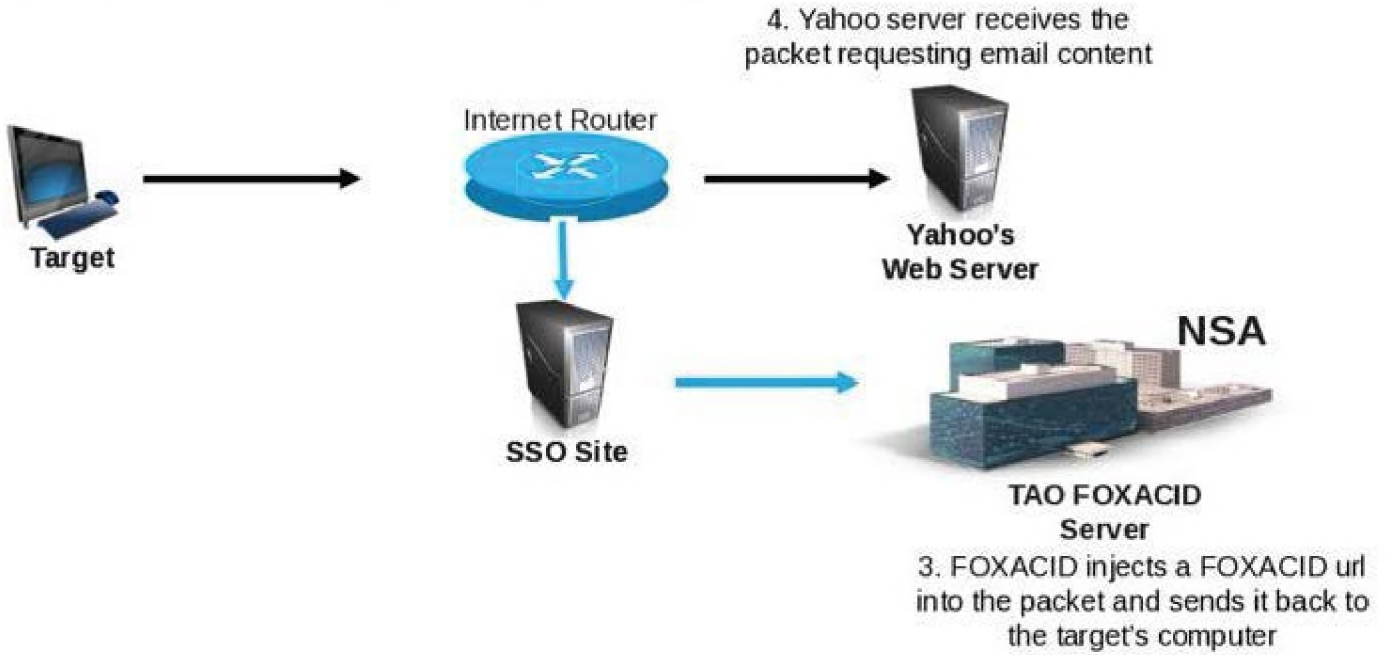
What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works



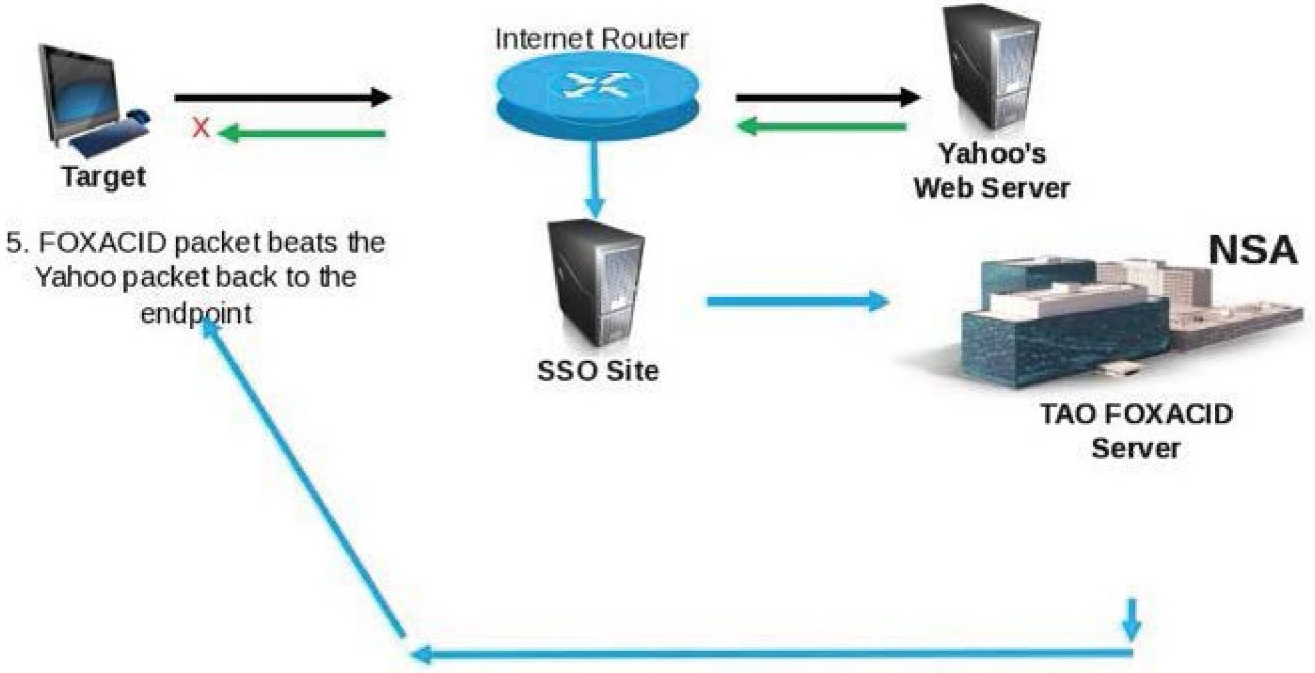
What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works



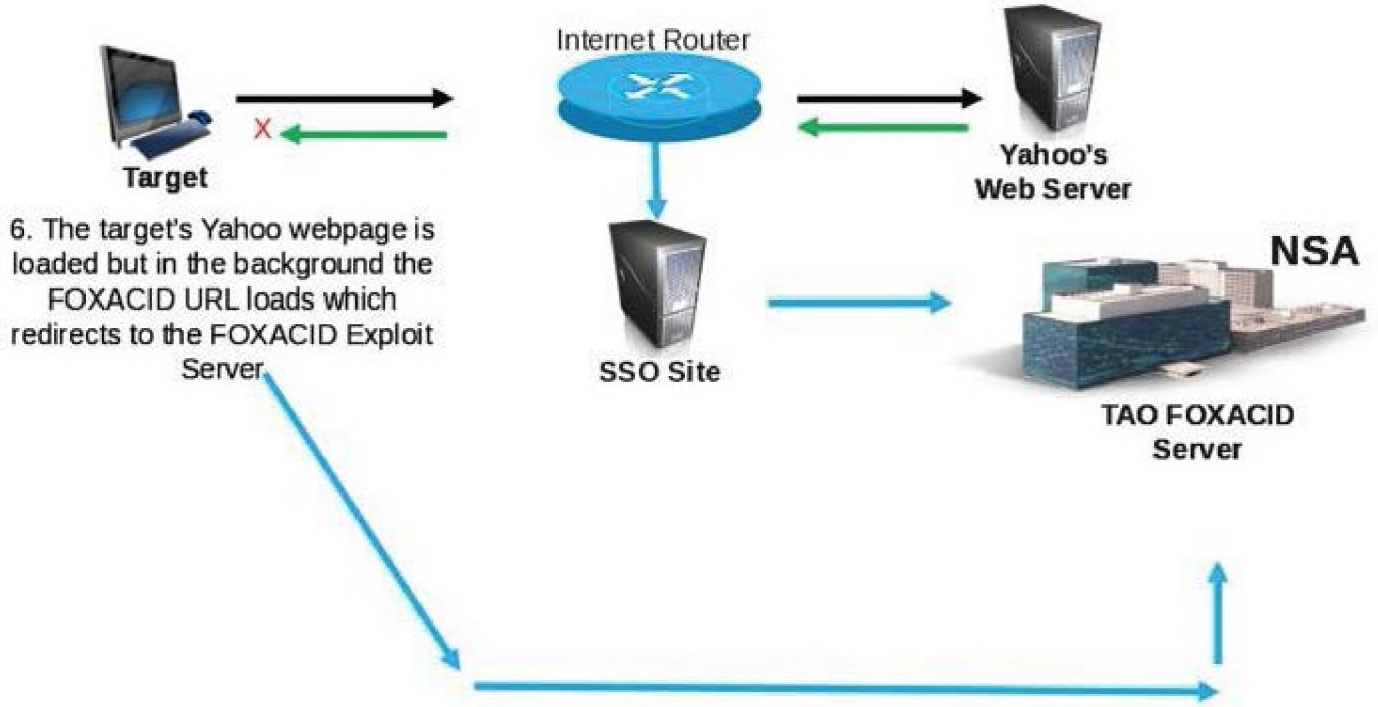
What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works



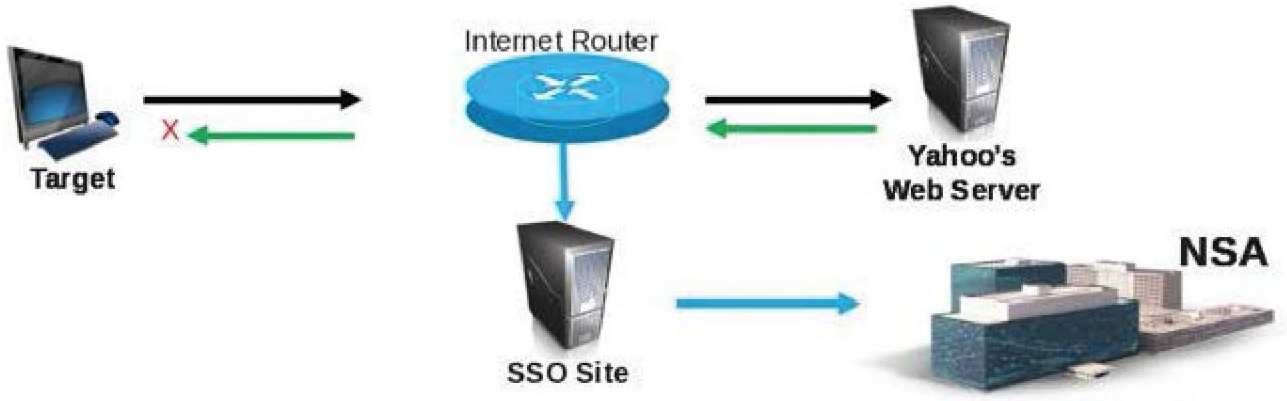
What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works



What is QUANTUM?

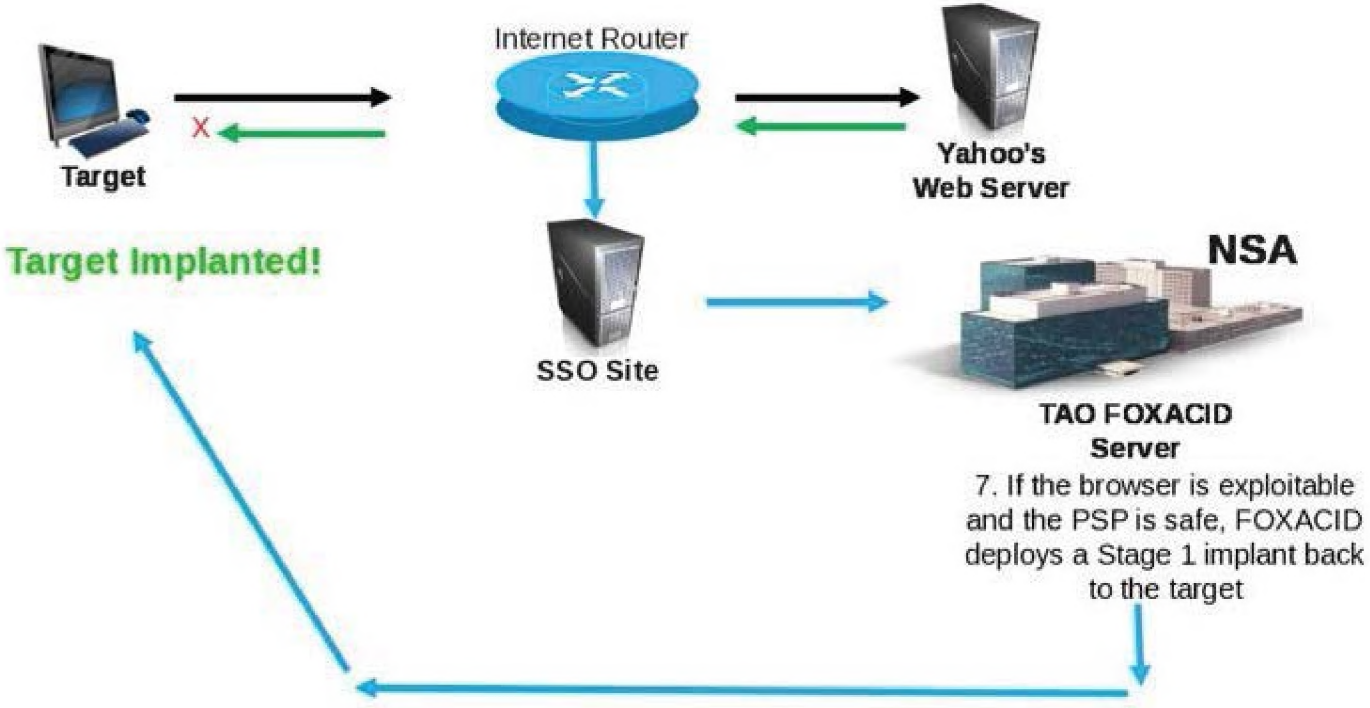
QUANTUM Generic Animation – High Level of How It Works



7. If the browser is exploitable and the PSP is safe, FOXACID deploys a Stage 1 implant back to the target

What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works



QUANTUM Capabilities – NSA

(TS//SI//REL) NSA QUANTUM has the *greatest* success against <yahoo>, <facebook>, and Static IP Addresses. New QUANTUM realms are often changing, so check the GO QUANTUM wiki page or the QUANTUM SpySpace page to get more up-to-date news.

NSA QUANTUM is capable of targeting the following realms:

- IPv4_public
- alibabaForumUser
- doubleclickID
- emailAddr
- rocketmail
- hi5Uid
- hotmailCID
- linkedin
- mail
- mailruMrcu
- msnMailToken64
- mailruMrcu
- msnMailToken64
- qq
- facebook
- simbarUuid
- twitter
- yahoo
- yahooBcookie
- ymail
- youTube
- WatcherID

QUANTUMTHEORY – GCHQ

If a Partnering Agreement Form (PAF) is set up with GCHQ for the CNO project, then the R&T Analyst can utilize GCHQ QUANTUMTHEORY to include additional capabilities such as:

- ALIBABA
- AOL
- BEBO_EMAIL
- DOUBLE_CLICK
- FACEBOOK_CUSER
- GOOGLE_PREFID
- GMAIL
- HI5
- HOTMAIL
- LINKEDIN
- MAIL_RU
- MICROSOFT_MUID
- MICROSOFT_ANONA
- RAMBLER
- RADIUS
- SIMBAR
- TWITTER
- YAHOO_B
- YAHOO_L/Y
- YANDEX_EMAIL
- YOUTUBE
- IP Address

More information on: https://wiki.gchq/[redacted]/QUANTUM_BISCUIT

If you cannot get to the link try: http://[redacted]

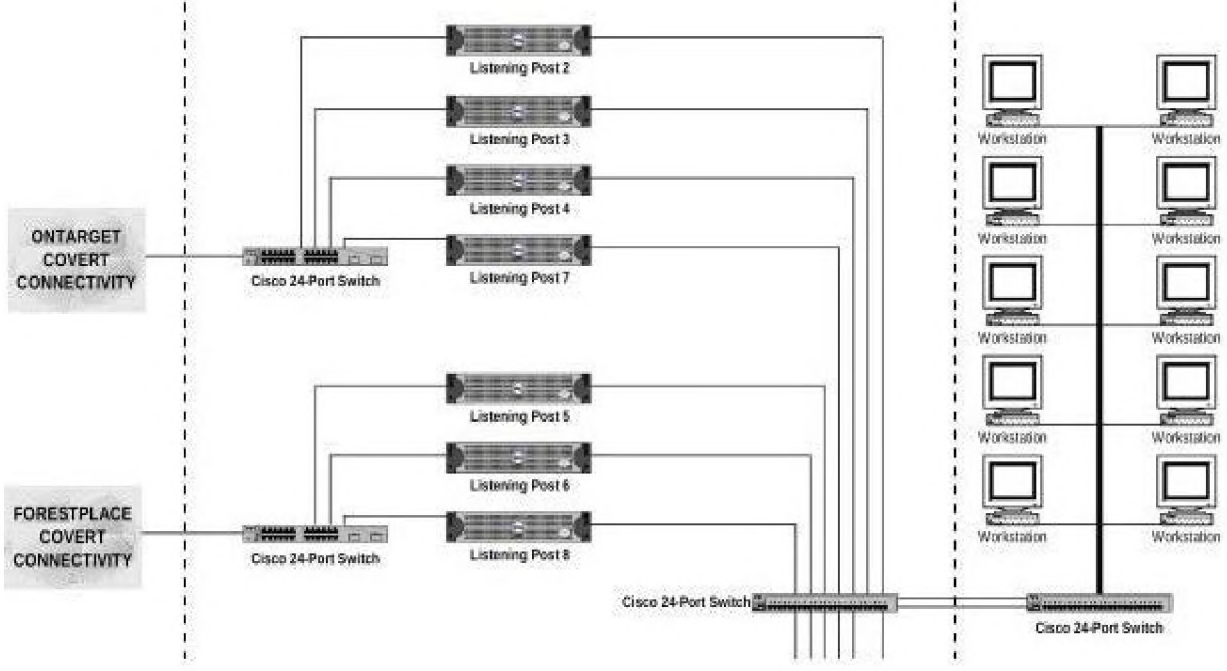
VALIDATOR

VALIDATOR is a part of a backdoor access system under the FOXACID project. The VALIDATOR is a client/server-based system that provides unique backdoor access to personal computers of targets of national interest, including but not limited to terrorist targets. VALIDATOR is a small Trojan implant used as a back door against a variety of targeted Windows systems, which can be deployed remotely or via hands on access to any Windows box from Windows 98 through Windows Server 2003. The LP is on-line 24/7 and tasking is 'queued', that is, jobs sit in a queue waiting for the target to 'call 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 information, change VALIDATOR ID, and Remove itself. VALIDATOR's are deployed to targeted systems and contact their Listening Post (LP) (each VALIDATOR is given a specific unique ID, specific IP address to call home to it's LP); SEPI analysts validate the target's identity and location (USSID-18 check), then provide a deployment list to Olympus operators to load a more sophisticated Trojan implant (currently OLYMPUS, future UNITEDRAKE). An OLYMPUS operator then queue up commands for the specific VALIDATOR ID's given by SEPI. Process repeats itself. Once target is hooked with the more sophisticated implant, VALIDATOR operators tend to cease. On occasion, operators are instructed by SEPI or the SWO to have VAIDATOR delete itself.

SPIEGEL ONLINE

OLYMPUSFIRE

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



SPIEGEL ONLINE