JTRIG tools and techniques

(Redirected from JTRIG CITD - Covert Internet Technical Development)

navigation

- Main Page
- Help Pages
- Wikipedia Mirror
- Ask Me About...
- Random page
- Recent changes
- Report a Problem
- Contacts
- GCWeb

search

Go | Search

toolbox

- What links here
- Related changes
- Upload file
- Special pages
- Printable version
- Permanent link

Overview | **JTRIG Capabilities** | Contacts

[edit] JTRIG tools

Contents

We don't update this page anymore, it became somewhat of a Chinese menu for effects operations. Information is now available for JTRIG staff at [[1]]

[edit] Understanding this page

Tools and techniques are developed by various teams within JTRIG. We like to let people know when we have something that we can think we can use, but we also don't want to oversell our capability.

For this reason, each tool indicates its current status. We may put up experimental tools or ones that are still in development so you know what we are working on, and can approach JTRIG with any new ideas. But experimental tools by their nature will be unreliable, if you raise expectations or make external commitments before speaking to us you will probably end up looking stupid.

Most of our tools are fully operational, tested and reliable. We will indicate when this is the case; however there can be reasons why our tools won't work for some operational requirements (eg if it exploits a provider specific vulnerability). There may also be legal restrictions.

So please come and speak to JTRIG operational staff early in your operational planning process.

[edit] Current Priorities

Capability Development Priorities can be fond by following the link below

- CapDev Priorities (Discover)

[edit] Engineering

Tool/System	Description	Status	Contacts
Cerberus Statistics Collection	Collects on-going usage information about how many users utilise JTRIG's UIA capability, what sites are the most frequently visited etc. This is in order to provide JTRIG infrastucture and ITServices management information statistics.	OPERATIONAL	JTRIG Software Developers
JTRIG RADIANT SPLENDOUR	is a 'Data Diode' connecting the CERBERUS network with GCNET	OPERATIONAL	JTRIG Software Developers
ALLIUM ARCH	JTRIG UIA via the Tor network.	OPERATIONAL	JTRIG Infrastructure Team
ASTRAL PROJECTION	Remote GSM secure covert internet proxy using TOR hidden services.	OPERATIONAL	JTRIG Infrastructure Team
TWILIGHT ARROW	Remote GSM secure covert internet proxy using VPN services.	OPERATIONAL	JTRIG Infrastructure Team
SPICE ISLAND	JTRIG's new Infrastructure. FOREST WARRIOR, FRUIT BOWL, JAZZ FUSION and other JTRIG systems will form part of the SPICE ISLAND infrastructure	DEV	JTRIG Infrastructure Team
POISON ARROW	Safe Malware download capability.	DESIGN	JTRIG Infrastructure Team
FRUIT BOWL	CERBERUS UIA Replacement and new tools infrastructure – Primary Domain for Generic User/Tools Access and TOR split into 3 sub-systems.	DESIGN	JTRIG Infrastructure Team
NUT ALLERGY	JTRIG Tor web browser - Sandbox IE replacement and FRUIT BOWL sub-system	PILOT	JTRIG Infrastructure Team
BERRY TWISTER	A sub-system of FRUIT BOWL	PILOT	JTRIG Infrastructure Team
BERRY TWISTER+	A sub-system of FRUIT BOWL	PILOT	JTRIG Infrastructure Team m]
BRANDY SNAP	JTRIG UIA contingency at Scarborough.	IMPLEMENTATION	JTRIG Infrastructure Team
WIND FARM	R&D offsite facility.	DESIGN	JTRIG Infrastructure Team
CERBERUS	JTRIG's legacy UIA desktop, soon to be replaced with FOREST WARRIOR.	OPERATIONAL	JTRIG Infrastructure Team
BOMBAYROLL	JTRIG's legacy UIA standalone capability.	OPERATIONAL	JTRIG Infrastructure Team
JAZZ FUSION	BOMBAY ROLL Replacement which will also incorporate new collectors – Primary Domain for Dedicated Connections split into 3 sub-systems.	IMPLEMENTATION	JTRIG Infrastructure Team
COUNTRY FILE	A sub-system of JAZZ FUSION	OPERATIONAL	JTRIG Infrastructure Team
TECHNO VIKING	A sub-system of JAZZ FUSION	DESIGN	JTRIG Infrastructure Team
JAZZ FUSION+	A sub-system of JAZZ FUSION	DESIGN	JTRIG Infrastructure Team
BUMBLEBEE DANCE	JTRIG Operational VM/TOR architecture	OPERATIONAL	JTRIG Infrastructure Team
AIR BAG	JTRIG Laptop capability for field operations.	OPERATIONAL	JTRIG Infrastructure Team
EXPOW	GCHQ's UIA capability provided by JTRIG.	OPERATIONAL	JTRIG Infrastructure Team
AXLE GREASE	The covert banking link for CPG	OPERATIONAL	JTRIG Infrastructure Team
POD RACE	JTRIG'S MS update farm	DESIGN	JTRIG Infrastructure Team
WATCHTOWER	GCNET -> CERBERUS Export Gateway Interface System	OPERATIONAL	JTRIG Software Developers
REAPER	CERBERUS -> GCNET Import Gateway Interface System	OPERATIONAL	JTRIG Software Developers
DIALd	External Internet Redial and Monitor Daemon	OPERATIONAL	JTRIG Software Developers
FOREST WARRIOR	Desktop replacement for CERBERUS	DESIGN	JTRIG Infrastructure Team
DOG HANDLER	JTRIG's development network	DESIGN	JTRIG Infrastructure Team
DIRTY DEVIL	JTRIG'S research network	DESIGN	JTRIG Infrastructure Team

[edit] Collection

Tool	Description	Contacts	Status
AIRWOLF	YouTube profile, comment and video collection.	[redacted]	Beta release.
ANCESTRY	Tool for discovering the creation date of yahoo selectors.	JTRIG Software Developers	Fully Operational.
BEARTRAP	Bulk retrieval of public BEBO profiles from member or group ID.	JTRIG Software Developers	Fully Operational.
BIRDSONG	Automated posting of Twitter updates.	JTRIG Software Developers	Decomissioned. Replaced by SYLVESTER.
BIRDSTRIKE	Twitter monitoring and profile collection. Click here for the User Guide.	JTRIG Software Developers	Fully Operational.
BUGSY	Google+ collection (circles, profiles etc.)	Tech Leads: [redacted]	In early development.
DANCING BEAR	obtains the locations of WiFi access points.	[Tech Lead: [redacted] Expert User: [redacted]	Fully Operational.
DEVILS HANDSHAKE	ECI Data Technique.	[Tech Lead: [redacted] Expert User: [redacted]	Fully Operational.
DRAGON'S SNOUT	Paltalk group chat collection.	Tech Leads: [redacted]	Beta release.
EXCALIBUR	acquires a Paltalk UID and/or email address from a Screen Name.	JTRIG Software Developers	Fully operational (against current Paltalk version)
FATYAK	Public data collection from LinkedIn.	[Tech Lead: [redacted]	In development
FUSEWIRE	Provides 24/7 monitoring of Vbulliten forums for target postings/online activity. Also allows staggered postings to be made.	JTRIG Software Developers	
GLASSBACK	Technique of getting a targets IP address by pretending to be a spammer and ringing them. Target does not need to answer.	JTRIG Software Developers	Fully operational.
GODFATHER	Public data collection from Facebook.	[Tech Lead: [redacted]	Fully operational.
GOODFELLA	Generic framework for public data collection from Online Social Networks.	[Tech Lead: [redacted]	In Development (Supports RenRen and Xing).
HACIENDA	is a port scanning tool designed to scan an entire country or city. It uses GEOFUSION to identify IP locations. Banners and content are pulled back on certain ports. Content is put into the EARTHLING database, and all other scanned data is sent to GNE and is available through GLOBAL SURGE and Fleximart.	NAC HACIENDA Taskers	Fully operational.
ICE	is an advanced IP harvesting technique.	JTRIG Software Developers	
INSPECTOR	Tool for monitoring domain information and site availability	JTRIG Software Developers	Fully Operational.
LANDING PARTY	Tool for auditing dissemination of VIKING PILLAGE data.	JTRIG Software Developers	Fully Operational.

MINIATURE HERO	Active skype capability. Provision of real time call records (SkypeOut and SkypetoSkype) and bidirectional instant messaging. Also contact lists.	JTRIG Software Developers	Fully operational, but note usage restrictions.
MOUTH	Tool for collection for downloading a user's files from Archive.org.	JTRIG Software Developers	Fully Operational.
MUSTANG	provides covert access to the locations of GSM cell towers.	|Tech Lead [redacted] Expert User: [redacted]	Fully Operational.
PHOTON TORPEDO	A technique to actively grab the IP address of an MSN messenger user.	Tech Lead: [redacted]	Operational, but usage restrictions.
RESERVOIR	Facebook application allowing collection of various information.	JTRIG Software Developers	Fully operational, but note operational restrictions.
SEBACIUM	An ICTR developed system to identify P2P file sharing activity of intelligence value. Logs are accessible via DIRTY RAT.	|Tech Lead: [redacted] User: [redacted]	
SILVER SPECTER	Allows batch Nmap scanning over TOR	JTRIG Software Developers	In Development
SODAWATER	A tool for regularly downloading gmail messages and forwarding them onto CERBERUS mailboxes	JTRIG Software Developers	Fully Operational.
SPRING BISHOP	Find private photographs of targets on Facebook.	Tech Lead: [redacted]	
SYLVESTER	Framework for automated interaction / alias management on online social networks.	Tech Lead: [redacted]	In Development.
TANNER	A technical programme allowing operators to log on to a JTRIG website to grab IP addresses of Internet Cafe's.	JTRIG OSO	Replaced by HAVOK.
TRACER FIRE	An Office Document that grabs the targets Machine info, files, logs, etc and posts it back to GCHQ.	[redacted] TRACER FIRE JTRIG	In Development.
VIEWER	A programme that (hopefully) provides advance tip off of the kidnappers IP address for HMG personnel.	[Tech Lead: [redacted] Expert User: [redacted]	Operational, but awaiting field trial.
VIKING PILLAGE	Distributed network for the automatic collection of encrypted/compressed data from remotely hosted JTRIG projects.	PILLAGE JTRIG Software Developers	Operational
TOP HAT	A version of the MUSTANG and DANCING BEAR techniques that allows us to pull back Cell Tower and WiFi locations targeted against particular areas.	[Tech Lead: [redacted]	In development.

[edit] Effects Capability

JTRIG develop the majority of effects capability in GCHQ. A lot of this capability is developed on demand for specific operations and then further developed to provide weaponised capability.

Dont treat this like a catalogue. If you dont see it here, it doesnt mean we cant build it. If you involve the JTRIG operational teams at the start of your operation, you have more of a chance that we will build something for you.

For each of our tools we have indicated the state of the tool. We only advertise tools here that are either ready to fire or very close to being ready (operational requirements would re-prioritise our development). Once again, involve the JTRIG operational teams early.

Tool	Description	Status	Contacts
ANGRY PIRATE	is a tool that will permanently disable a target's account on their computer.	Ready to fire (but see target restrictions).	[Tech Lead: [redacted] Expert User: [redacted]
ARSON SAM	is a tool to test the effect of certain types of PDU SMS messages on phones / network. It also includes PDU SMS Dumb Fuzz testing.	Ready to fire (Not against live targets, this is a R&D Tool).	[Tech Lead: [redacted] Expert User:]
BUMPERCAR+	is an automated system developed by JTRIG CITD to support JTRIG BUMPERCAR operations. BUMPERCAR operations are used to disrupt and deny Internet-based terror videos or other material. The technique employs the services provided by upload providers to report offensive materials.	Ready to fire.	JTRIG Software Developers
BOMB BAY	is the capability to increase website hits/rankings.	In Development.	[Tech Lead: [redacted]
BADGER	mass delivery of email messaging to support an Information Operations campaign	Ready to fire.	JTRIG OSO
BURLESQUE	is the capability to send spoofed SMS text messages.	Ready to fire.	JTRIG OSO
CANNONBALL	is the capability to send repeated text messages to a single target.	Ready to fire.	JTRIG OSO
CLEAN SWEEP	Masquerade Facebook Wall Posts for individuals or entire countries	Ready to fire (SIGINT sources required)	[Tech Lead: [redacted] Expert User:
CLUMSY BEEKEEPER	Some work in progress to investigate IRC effects.	NOT READY TO FIRE.	Tech Lead: [redacted] Expert User : [redacted]
CHINESE FIRECRACKER	Overt brute login attempts against online forums	Ready to fire.	FIRECRACKER
CONCRETE DONKEY	is the capability to scatter an audio message to a large number of telephones, or repeatedly bomb a target number with the same message.	In development.	[redacted]
DEER STALKER	Ability to aid-geolocation of Sat Phones / GSM Phones via a silent calling to the phone.	Ready to fire.	[Tech Lead: [redacted] Expert User: [redacted]
GATEWAY	Ability to artificially increase traffic to a website	Ready to fire.	JTRIG OSO
GAMBIT	Deployable pocket-sized proxy server	In-development	JTRIG OSO
GESTATOR	amplification of a given message, normally video, on popular multimedia websites (Youtube).		[Tech Lead: ?; Expert User: [redacted]
GLITTERBALL	Online Gaming Capabilities for Sensitive Operations. Currently Second Life.	In development.	
IMPERIAL BARGE	For connecting two target phone together in a call.	Tested.	[Tech Lead: [redacted] Expert User: [redacted]
PITBULL	Capability, under development, enabling large scale delivery of a tailored message to users of Instant Messaging services.	In development.	
POISONED DAGGER	Effects against Gigatribe. Built by ICTR, deployed by JTRIG.		Tech Lead: [redacted]

PREDATORS FACE	Targeted Denial Of Service against Web Servers.		Tech Lead: [redacted]
ROLLING THUNDER	Distributed denial of service using P2P. Built by ICTR, deployed by JTRIG.		Tech Lead: [redacted]
SCARLET EMPEROR	Targeted denial of service against targets phones via call bombing.	Ready to fire.	JTRIG Software Developers
SCRAPHEAP CHALLENGE	Perfect spoofing of emails from Blackberry targets.	Ready to fire, but see constraints.	[redacted]
SERPENTS TONGUE	for fax message broadcasting to multiple numbers.	In redevelopment.	[Tech Lead: [redacted] Expert User: [redacted]
SILENT MOVIE	Targeted denial of service against SSH services.	Ready to fire.	[Tech Lead: [redacted]
SILVERBLADE	Reporting of extremist material on DAILYMOTION.	Ready to fire.	[Tech Lead: [redacted] Expert User: [redacted]
SILVERFOX	List provided to industry of live extremist material files hosted on FFUs.	Ready to fire.	[Tech Lead: [redacted] Expert User: [redacted]
SILVERLORD	Disruption of video-based websites hosting extremist content through concerted target discovery and content removal.	Ready to fire.	[Tech Lead: [redacted] Expert User: [redacted]
SKYSCRAPER	Production and dissemination of multimedia via the web in the course of information operations.	Ready to fire.	[Tech Lead: Section X; Expert Users: Language Team]
SLIPSTREAM	Ability to inflate page views on websites	Ready to fire.	JTRIG OSO
STEALTH MOOSE	is a tool that will Disrupt target's Windows machine. Logs of how long and when the effect is active.	Ready to fire (but see target restrictions).	[Tech Lead: [redacted] Expert User:]
SUNBLOCK	Ability to deny functionality to send/receive email or view material online.	Tested, but operational limitations.	[Tech Lead: Section X; Expert User: [redacted]
Swamp donkey	is a tool that will silently locate all predefined types of file and encrypt them on a targets machine.	Ready to fire (but see target restrictions).	[Tech Lead: [redacted] Expert User: [redacted]
TORNADO ALLEY	is a delivery method (Excel Spreadsheet) that can silently extract and run an executable on a target's machine.	Ready to fire (but see target restrictions).	[Tech Lead: [redacted] Expert User: [redacted]
UNDERPASS	Change outcome of online polls (previously known as NUBILO)	In development.	[Tech Lead: Section X; Expert User: [redacted]
VIPERS TONGUE	is a tool that will silently Denial of Service calls on a Satellite Phone or a GSM Phone.	Ready to fire (but see target restrictions).	[Tech Lead: [redacted] Expert User: [redacted]
WARPATH	Mass delivery of SMS messages to support an Information Operations campaign	Ready to fire.	JTRIG OSO

edit] Work Flow Management

Tool	Description	Contacts
HOME PORTAL	A central hub for all JTRIG Cerberus tools	JTRIG Software Developers
CYBER COMMAND CONSOLE	A centralised suite of tools, statistics and viewers for tracking current operations across the Cyber community.	JTRIG Software Developers
NAMEJACKER	A web service and admin console for the translation of usernames between networks. For use with gateways and other such technologies.	JTRIG Software Developers

[edit] Analysis Tools

Tool	Description	Contacts
BABYLON	is a tool that bulk queries web mail addresses and verifies whether they can be signed up for. A green tick indicates that the address is currently in use. Verification can currently be done for Hotmail and Yahoo.	JTRIG Software Developers
CRYOSTAT	is a JTRIG tool that runs against data held in NEWPIN. It then displays this data in a chart to show links between targets.	JTRIG Software Developers
ELATE	is a suite of tools for monitoring target use of the UK auction site eBay (www.ebay.co.uk). These tools are hosted on an Internet server, and results are retreived by encrypted email.	JTRIG Software Developers
PRIMATE	is a JTRIG tool that aims to provides the capability to identify trends in seized computer media data and metadata.	JTRIG Software Developers
JEDI	JTRIG will shortly be rolling out a JEDI pod to every desk of every member of an Intelligence Production Team. The challenge is to scale up to over 1,200 users whilst remaining agile, efficent and responsive to customer needs.	[Tech Lead: [redacted] Expert User: [redacted]
JILES	is a JTRIG bespoke web browser.	[Tech Lead: [redacted] Expert User:]
MIDDLEMAN	is a distributed real-time event aggregation, tip-off and tasking platform utilised by JTRIG as a middleware layer.	JTRIG Software Developers
OUTWARD	is a collection of DNS lookup, WHOIS Lookup and other network tools.	JTRIG Software Developers
TANGLEFOOT	is a bulk search tool which queries a set of online resources. This allows analysts to quickly check the online presence of a target.	JTRIG Software Developers
SCREAMING EAGLE	is a tool that processes kismet data into geolocation information	
SLAMMER	is a data index and repository that provides analysts with the ability to query data collected from the Internet from various JTRIG sources, such as EARTHLING, HACIENDA, web pages saved by analysts etc.	JTRIG Software Developers

[edit] Databases

Tool	Description	Contacts
BYSTANDER	is a categorisation database accessed via web service.	JTRIG Software Developers
CONDUIT	is a database of C2C identifiers for Intelligence Community assets acting online, either under alias or in real name.	JTRIG Software Developers
NEWPIN	is a database of C2C identifiers obtained from a variety of unique sources, and a suite of tools for exploring this data.	JTRIG Software Developers
QUINCY	is an enterprise level suite of tools for the exploitation of seized media.	[Tech Lead: [redacted] Expert Users: [redacted]

[edit] Forensic Exploitation

Tool	Description	Contacts
BEARSCRAPE	can extract WiFi connection history (MAC and timing) when supplied with a copy of the registry structure or run on the box.	[Tech Lead: [redacted] Expert User:]
SFL	The Sigint Forensics Laboratory was developed within NSA. It has been adapted by JTRIG as its email extraction and first-pass analysis of seized media solution.	[Tech Lead: [redacted] Expert User:
Snoopy	is a tool to extract mobile phone data from a copy of the phone's memory (usually supplied as an image file extracted through FTK.	[Tech Lead: [redacted]
MobileHoover	is a tool to extract data from field forensics' reports created by Celldek, Cellebrite, XRY, Snoopy and USIM detective. These reports are transposed into a Newpin XML format to upload to Newpin.	[Tech Lead: [redacted]
Nevis	is a tool developed by NTAC to search disk images for signs of possible Encryption products. CMA have further developed this tool to look for signs of Steganography.	[Tech Lead: [redacted]