G8 24/7 Cybercrime Network

Rick Green

Computer Crime and Intellectual Property Section

U.S. Department of Justice

History of the Network

- Meeting of the G8 Justice and Interior Ministers – December 1997 called for creation of a network
  - "With regard to high-tech crime, we must start by recognizing that new computer and telecommunications technologies offer unprecedented opportunities for global communication. As nations become increasingly reliant upon these technologies, including wireless communications, their exploitation by high-tech criminals poses an ever-greater threat to public safety."
  - Statement of Principles included
    - No safe havens
    - Investigation and Prosecution must be coordinated among all concerned States

1997 Action Plan

- "Use our established network of knowledgeable personnel to ensure a timely, effective response to transnational high-tech cases and designate a point-of-contact who is available on a twenty-four hour basis."
- "Review our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes."
- "Continue to examine and develop workable solutions regarding: the preservation of evidence prior to the execution of a request for mutual assistance; transborder searches; and computer searches of data where the location of that data is unknown."

The G8 24/7 Network was born

- Point to point network for urgent assistance in cybercrime matters (Single point of contact (POC))
  - English speaking POC;
  - POC must be available 24 hours per day, 7 days per week;
  - POC should be knowledgeable in technical matters;
  - POC should have working knowledge of applicable domestic law
- Primary purpose of the Network is to preserve data for subsequent transfer through legal channels (e.g., mutual legal assistance treaties)
  - Described in the past as a "fast freeze and a slow thaw"

24/7 Network Protocol

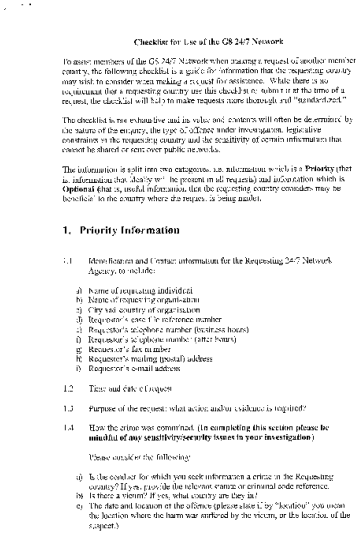
- "The G8 24/7 points of contact are provided for investigations involving electronic evidence that require urgent assistance from foreign law enforcement. High-tech crimes raise new challenges for law enforcement. In investigations involving computer networks, it is often important for technically literate investigators to move at unprecedented speeds to preserve electronic data and locate suspects, often by asking Internet Service Providers to assist by preserving data. Therefore, to enhance and supplement (but not replace) traditional methods of obtaining assistance, the G8 has created the Network as a new mechanism to expedite contacts between Participating States or other autonomous law enforcement jurisdictions of a State (hereinafter referred to as "Participants")."

How the Network Works (The Protocol)

- "To use this Network, law enforcement agents seeking assistance from a foreign Participant may contact the 24-hour point of contact in their own state or autonomous law enforcement jurisdiction, and this individual or entity will, if appropriate, contact his or her counterpart in the foreign Participant. Participants in the Network have committed to make their best efforts to ensure that Internet Service Providers freeze the information sought by a requesting Participant as quickly as possible. Participants have further committed to make their best efforts to produce information expeditiously. This is subject to the understanding that a requested Participant's legal, technical or resource considerations may affect the extent to which - and the time frame within which – the Participant may produce evidence, as well as the process of Mutual Legal Assistance, by which the requesting country seeks release of that information though the usual MLAT or Letters of Request procedure."

Informal Nature of the Network

- Network was deliberately designed with few rules and procedures to stimulate, rather than impede, cooperation.
- A checklist has been developed to guide participants in formulating their requests to maximize the results.



Checklist for Use of the G8 24/7 Network

To assist members of the G8 24/7 Network when making a request of another member country, the following checklist is a guide to information that the requesting country may wish to consider when making a request for assistance. While there is no requirement that a requesting country use this checklist in its submission of a request, the checklist will help to make requests more thorough and "standardized."

The checklist is not exhaustive and its value and contents will often be determined by the nature of the enquiry, the type of offence under investigation, legislative constraints in the requesting country and the sensitivity of certain information that cannot be shared or sent over public networks.

The information is split into two categories, i.e. information which is a **Priority** (that is, information that ideally will be present in all requests) and information which is **Optional** (that is, useful information, that the requesting country considers may be beneficial to the country where the request is being made).

1. Priority Information

1.1 Identification and Contact information for the Requesting 24/7 Network Agency, to include:

a) Name of requesting individual
b) Name of requesting organization
c) City and country of organization
d) Requestor's case file reference number
e) Requestor's telephone number (business hours)
f) Requestor's telephone number (after hours)
g) Requestor's fax number
h) Requestor's mailing (postal) address
i) Requestor's e-mail address

1.2 Time and date of request

1.3 Purpose of the request: what action and/or assistance is required?

1.4 How the crime was committed. **(In completing this section please be mindful of any sensitivity/security issues in your investigation)**

Please consider the following:

a) Is the conduct for which you seek information a crime in the Requesting country? If yes, provide the relevant statute or criminal code reference.
b) Is there a victim? If yes, what country are they in?
c) The date and location of the offence (please also list by "location" you mean the location where the harm was suffered by the victim, or the location of the suspect)

Green, Richard

From: Green, Richard
Sent: Tuesday, October 22, 2013 11:07 AM
To: [redacted]
Subject: [24/7 Data Preservation Request] New Data Preservation Request from the United States (Non-Emergency)
Attachments: Outbound Preservation Req[redacted]22Oct2013.pdf

Greetings from the United States-

Please see the attached non-emergency, but important, data preservation request from the United States. I have also reproduced the request below for your convenience. Please note that if there is a risk that the users of the IP addresses that are the subject of this request will get alerted to the investigation, please **do not take any action** until we discuss the situation further.

The United States, through its 24/7 Cybercrime Network Point of Contact, the Computer Crime and Intellectual Property Section of the U.S. Department of Justice, requests assistance in preserving data which is located in [redacted]. The Federal Bureau of Investigation (FBI) is investigating computer attacks (DDoS) on the websites of financial institutions in the United States. This conduct involves violations of the laws of the United States, specifically Title 18, United States Code, section 1030 (Fraud and Related Activity in Connection with Computers), among others. The FBI has identified a computer in [redacted] that appears to be receiving log entries from the computer attacks.

The United States is requesting assistance from you to preserve the data related to the IP address of the computer in [redacted] and continue that preservation until such time as the United States is able to make an official mutual legal assistance request for the data.

It is critical to the integrity of this investigation that the user(s) of this IP address are not alerted to the existence of this investigation. If it is not possible to preserve the data without alerting the users of this IP address, please DO NOT TAKE ACTION and contact us to discuss the options available.

If it is safe to do so without alerting the users of the IP address in question, please preserve all data related to this IP address, including but not limited to: customer records; connection logs; web logs; back-end databases; any other files or code; configuration data; billing records; communications between hosting company and the customers; and any other content and records associated with the subscriber/customer using the following IP address.

[redacted]

The whois database indicates that this IP address is registered to [redacted].

Please provide confirmation of the preservation of this data at your earliest convenience. Thank you for your cooperation in this matter. If you have any questions please contact me at +1 202-616-3475 or email me at Richard.Green@usdoj.gov.

Best regards,

Rick Green

Richard D. Green
Trial Attorney
Computer Crime and Intellectual Property Section (CCIPS)

A Steadily Growing Network

- From humble numbers in 1998 to 66 countries worldwide today.

A Network More Active Than Ever

- As an example – the United States has received over 100 incoming requests since the first of the year
- The United States has made over 25 outgoing requests to other countries in that same time period

Types of Requests

- Mostly data Preservation Requests
- Some “life or limb” Requests