[redacted]

National Security Agency
Attn: FOIA/PA Office (DJ4)
9800 Savage Road, Suite 6248
Ft. George G. Meade, MD 20755-6248

Dear NSA FOIA/PA Office:

This is a Freedom of Information Act request, as described in `http://www.nsa.gov/public_info/foia/foia_handbook.shtml`.

I am seeking the following records:

- The source code for the JETPLOW firmware persistence implant for Cisco PIX and ASA series firewalls. (See Appendix A, which was obtained from `http://www.spiegel.de/international/world/a-941262.html`)

Cisco PIX and ASA firewalls are widely deployed by US industry. If the NSA has discovered firmware exploits for these devices, then other entities have surely discovered the same (or similar) exploits. The existence of such exploits (1) exposes users of PIX and ASA firewalls to network attacks, and (2) generally reduces the level of security for the assets these PIX and ASA firewalls were intended to protect.

I am seeking this information for public good, and because I believe this information is in the general public interest. I intend to pass copies of the source code to Cisco, to security researches, and to (in the most responsible manner possible) publish the source code on the internet. By studying PIX and ASA firmware exploits as an attack vector, we can better secure these devices, and due to their wide deployment, increase the overall level of security on the internet.

I note that the JETPLOW catalog page lists a unit cost of $0, so I hope that you will waive fees for fulfilling this FOIA request.

Thanks for your time and attention. I look forward to your response.

Sincerely,

Stephen A. Revilak
[redacted]

Appendix A – JETPLOW Catalog Page

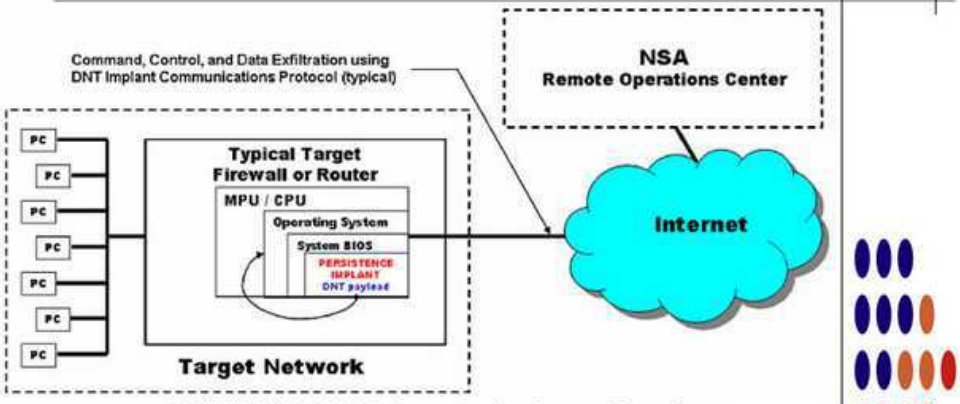
TOP SECRET//COMINT//REL TO USA, FVEY

JETPLOW

ANT Product Data

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant. JETPLOW also has a persistent back-door capability.

06/24/08



(TS//SI//REL) JETPLOW Persistence Implant Concept of Operations

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant and modifies the Cisco firewall's operating system (OS) at boot time. If BANANAGLEE support is not available for the booting operating system, it can install a Persistent Backdoor (PBD) designed to work with BANANAGLEE's communications structure, so that full access can be reacquired at a later time. JETPLOW works on Cisco's 500-series PIX firewalls, as well as most ASA firewalls (5505, 5510, 5520, 5540, 5550).

(TS//SI//REL) A typical JETPLOW deployment on a target firewall with an exfiltration path to the Remote Operations Center (ROC) is shown above. JETPLOW is remotely upgradeable and is also remotely installable provided BANANAGLEE is already on the firewall of interest.

Status: (C//REL) Released. Has been widely deployed. Current availability restricted based on OS version (inquire for details).

Unit Cost: $0

POC: [redacted], S32222, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 76243
17 January 2014

Mr. Stephen A. Revilak
[redacted]

Dear Mr. Revilak:

This is an initial response to your Freedom of Information Act (FOIA) request dated 5 January 2014, which was received by this office on 15 January 2014, for "The source code for the JETPLOW firmware persistence implant for Cisco PIX and ASA series firewalls." This letter acknowledges that we have received your request and provides some administrative information. Your request has been assigned Case Number 76243. Due to a significant increase in the number of requests being received by this Agency, we are experiencing delays in processing. We will begin to process your request and respond to you again as soon as we are able on a first-in, first-out basis.

Correspondence related to your request should include the case number assigned to your request, which is included in the first paragraph of this letter. Your letter should be addressed to National Security Agency, FOIA Office (DJ4), 9800 Savage Road STE 6248, Ft. George G. Meade, MD 20755-6248 or may be sent by facsimile to 443-479-3612. If sent by fax, it should be marked for the attention of the FOIA office. The telephone number of the FOIA office is 301-688-6527.

Sincerely,

[redacted]

FOIA Customer Representative

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 76243B
20 November 2015

STEPHEN A REVILAK
[redacted]

Dear Mr. Revilak:

This responds to your Freedom of Information Act (FOIA) request of 5 January 2014, which was received by this office on 15 January 2014, for "the source code for the JETPLOW firmware persistence implant for Cisco PIX and ASA series firewalls."

As previously informed, your letter has been assigned Case Number 76243. Please refer to this case number when contacting us about your request. There is certain information relating to this processing about which the FOIA and applicable Department of Defense (DoD) and NSA/CSS regulations require we inform you. For purposes of this request and based on the information you provided in your letter, you are considered an "all other" requester. As such, you are allowed 2 hours of search and the duplication of 100 pages at no cost. Because there are no assessable fees for this request, we did not address your request for a waiver of fees. Your request has been processed under the provisions of the FOIA.

Your request seeks records about *alleged* NSA intelligence activities and/or programs. However, your request appears to be premised on media reports that purport to describe documents originating from the NSA or that discuss alleged NSA intelligence activities and programs. Thus, we cannot acknowledge the existence or non-existence of specific documents purported to be originated by NSA, nor can we acknowledge the accuracy or inaccuracy of media reports about alleged NSA activities, to include any media publication of documents purported to be originated by NSA.

We have determined that the fact of the existence or non-existence of the materials you request is a currently and properly classified matter in accordance with Executive Order 13526, as set forth in Subparagraph (c) of Section 1.4. Thus, your request is denied pursuant to the first exemption of the FOIA which provides that the FOIA does not apply to matters that are specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign relations and are, in fact properly classified pursuant to such Executive Order.

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. The third exemption of the FOIA provides for the withholding of information specifically protected from disclosure by statute. Thus,

your request is also denied because the fact of the existence or non-existence of the information is exempted from disclosure pursuant to the third exemption. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 3024(i); and Section 6, Public Law 86-36 (50 U.S. Code 3605).

You may appeal this decision. If you decide to appeal, you should do so in the manner outlined below.

- The appeal must be in writing and addressed to the:

  NSA/CSS FOIA/PA Appeal Authority (DJ4),
  National Security Agency
  9800 Savage Road STE 6248
  Fort George G. Meade, MD 20755-6248

- It must be postmarked no later than 60 calendar days of the date of this letter.
- Please include the case number provided above.
- Please describe with sufficient detail why you believe the denial of information was unwarranted.
- NSA will endeavor to respond within 20 working days of receiving your appeal, absent any unusual circumstances.

In order to correct the misinformation flowing from certain unauthorized disclosures of classified national security information, and to reassure the American public as to the numerous safeguards that protect privacy and civil liberties, since June 6, 2013, the Director of National Intelligence has declassified certain information pertaining to surveillance conducted by the NSA pursuant to law. I generally refer you to http://icontherecord.tumblr.com/tagged/declassified for information about declassified NSA activities and programs.

Sincerely,

[redacted]

JOHN R. CHAPMAN
Chief, FOIA/PA Office
NSA Initial Denial Authority