

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA)	
)	
Plaintiff,)	Civil Action No. 16-1780
)	
v.)	
)	
“flux”)	
a/k/a “ffhost,”)	
)	
and,)	
)	
“flux2”)	
a/k/a “ffhost2”)	
)	
Defendants.)	

**DECLARATION OF SPECIAL AGENT AARON O. FRANCIS IN SUPPORT OF
MOTION FOR PRELIMINARY INJUNCTION**

I, Aaron O. Francis, declare as follows:

1. I am a Special Agent with the Federal Bureau of Investigation in Pittsburgh, Pennsylvania. I make this declaration in support of the United States of America’s Motion for Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where noted and, if called as a witness, I could and would testify completely to the truth of the matters set forth herein.

2. I incorporate as if more fully declared herein my Declaration in Support of Application for Emergency Temporary Restraining Order (“TRO Declaration”) in the above captioned matter.

See Dkt. No. 3, Atch. 1.

ADDITIONAL GOZNYM DOMAINS

3. On or about November 27, 2016, the DGA for the GozNym malware was changed by the actors responsible for the malware. As a result, an additional set of domains was scheduled to be generated over the course of one year. Fraunhoffer promptly worked to reverse engineer the GozNym DGA. As of November 28, 2016, Fraunhoffer was able to determine 71 of the approximately 353 domains that would be created by the DGA. These 71 domains were included within Appendix B of the Temporary Restraining Order (“TRO”) signed by this Honorable Court. (*See* Dkt. Nos. 7-11).

4. Since the time of Your Honor granted the TRO, Fraunhoffer has continued to work to identify domains that would be generated by the DGA.

5. On or about December 7, 2016, Fraunhoffer provided the FBI with the complete list of 353 domains that would be generated by the new GozNym DGA. The FBI removed the 71 domains that were originally included in Appendix B on November 29, 2016. The remaining domains are included in Appendix B.1 to the concurrently filed Motion for Preliminary Injunction.

DOMAINS REGISTERED PRIOR TO EXECUTION OF TRO

6. From the time the FBI finalized Appendix B to the TRO – unregistered domains – until the TRO was signed and the operation commenced, approximately 20 domains that were in Appendix B to the TRO were registered by malware actors.

7. As a result of these registrations, the registries were unable to block the domains from being registered. As such, those domains have remained under the control of the malware actors and are likely to be used by the Defendants to further their criminal conduct.

8. In order to be able to be able to control those domains, they need to be redirected in the same manner in which the domains in Appendix A of the TRO were addressed. These specific, registered domains are included in Appendix A.1 to the concurrently filed Motion for Preliminary Injunction.

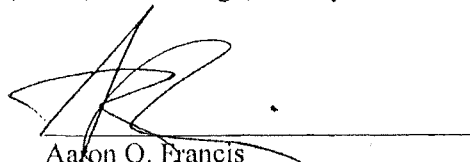
ADDITIONAL EFFORTS AT SERVICE

9. From December 1 – 2, 2016, the FBI served all filed documents relating to the TRO (Dkt. Nos. 2 – 4 and 7) on the defendants at five known jabber accounts (one for flux and four for flux2). On December 2, 2016, the FBI served documents related to the temporary restraining order on flux and flux2 at three known email accounts (one for flux and two for flux2).

10. Further, the Department of Justice uploaded those same documents for service onto its website (<https://www.justice.gov/opa/documents-and-resources-december-5-2016-announcement-takedown-international-cybercriminal>) and advertised a link to that site in a widely distributed press release.

I declare under penalty of perjury under the law of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 8th day of December, 2016, in Pittsburgh, Pennsylvania.


Aaron O. Francis
Special Agent
Federal Bureau of Investigation