AO 91 (Rev. 11/11) Criminal Complaint

AUSAs William E. Ridgway and Devlin N. Su
Senior Counsel Ryan K. Dickey (CCIPS)

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

FILED

JUL - 8 2016

THOMAS G. BRUTON
CLERK, U.S. DISTRICT COURT

UNITED STATES OF AMERICA

v.

ARTEM VAULIN,
also known as "tirm"

CASE NUMBER:
UNDER SEAL

16CR 438

MAGISTRATE JUDGE GILBERT

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

Count One

From at least as early as in or about November 2008, to on or about July 8, 2016, in the Northern District of Illinois, Eastern Division, and elsewhere, Artem Vaulin, also known as "tirm," defendant herein, conspired with others to: (1) willfully infringe, for purposes of commercial advantage and private financial gain, at least ten copies and phonorecords of one or more copyrighted works with a total retail value of more than $2,500 during a 180-day period, in violation of Title 17, United States Code, Section 506(a)(1)(A) and Title 18, United States Code, Section 2319(b)(1); and (2) willfully infringe, for purposes of commercial advantage and private financial gain, a copyright by distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, when defendant knew and should have known that that work was intended for commercial distribution, in violation of Title 17, United States Code, Section 506(a)(1)(C) and Title 18, United States Code, Section 2319(d)(2), all in violation of Title 18, United States Code, Section 371.

Count Two

From at least as early as in or about November 2008, to on or about July 8, 2016, in the Northern District of Illinois, Eastern Division, and elsewhere, Artem Vaulin, also known as "tirm," defendant herein, conspired with others to: (1) knowingly conduct and attempt to conduct a financial transaction affecting interstate and foreign commerce, which involved the proceeds of the specified unlawful activity of conspiracy to commit criminal copyright infringement, knowing that the transaction was designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of said specified unlawful activity, and that while conducing and attempting to conduct such financial transaction knew that the property involved in the financial transaction represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i); and (2) knowingly transmit and transfer funds from a place in the United States to a place outside the United

States, knowing that the funds involved in the transmission and transfer represented the proceeds of some form of unlawful activity, and knowing the that transmission and transfer was designed in whole or in part to conceal and disguise the nature, the location, the source, and the ownership and the control of the proceeds of specified unlawful activity, namely, conspiracy to commit criminal copyright infringement, in violation of Title 18, United States Code, Section 371, all in violation of Title 18, United States Code, Section 1956(h)

Count Three

On or about June 27, 2016, in the Northern District of Illinois, Eastern Division, and elsewhere, Artem Vaulin, also known as "tirm," defendant herein, willfully infringed, for purposes of commercial advantage and private financial gain, a copyright by distributing a work being prepared for commercial distribution in the United States, namely, the copyrighted motion picture "Captain America: Civil War" (which had not yet been commercially distributed) by making it available on a computer network accessible to members of the public, when defendant knew and should have known that the work was intended for commercial distribution, in violation of Title 17, United States Code, Section 506(a)(1)(C) and Title 18, United States Code, Sections 2319(d)(2) and 2.

Count Four

For the 180 days leading up to and including July 8, 2016, in the Northern District of Illinois, Eastern Division, and elsewhere, Artem Vaulin, also known as "tirm," defendant herein, willfully infringed, for purposes of commercial advantage and private financial gain, copyrights in certain motion pictures, television programs, musical recordings, electronic books, video games, and other computer software, by reproducing and distributing over the Internet, at least ten copies and phonorecords of one or more copyrighted works which had a total retail value of more than $2,500, in violation of Title 17, United States Code, Section 506(a)(1)(A) and Title 18, United States Code, Sections 2319(b)(1) and 2.

This criminal complaint is based upon these facts:

X Continued on the attached sheet.

JARED DER-YEGHIAYAN
Special Agent, Homeland Security Investigations

Sworn to before me and signed in my presence.

Date: July 8, 2016

Judge's signature

City and state: Chicago, Illinois

Jeffrey T. Gilbert, U.S. Magistrate Judge
Printed name and Title

UNITED STATES DISTRICT COURT)
)
NORTHERN DISTRICT OF ILLINOIS)

AFFIDAVIT

I. INTRODUCTION AND AGENT BACKGROUND

I, Jared Der-Yeghiayan, being duly sworn, state as follows:

1. I am a Special Agent with the U.S. Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations. I have been so employed since approximately 2010. As part of my duties as a Homeland Security Investigations Special Agent, I investigate criminal violations relating to cybercrime, copyright, and other intellectual property offenses and have received specialized training in those areas.

2. This affidavit is made in support of a criminal complaint alleging that Artem Vaulin, also known as "tirm":

- Conspired with others to commit criminal infringement of a copyright, in violation of Title 17, United States Code, Sections 506(a)(1)(A) and 506(a)(1)(C),[1] and Title 18, United States Code, Sections 2319(b)(1) and

[1] Title 17, United States Code, Section 506(a)(1) provides that "[a]ny person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed:

> (A) for purposes of commercial advantage or private financial gain;
> * * * or
> (C) by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution.

Section (a)(3) defines a "work being prepared for commercial distribution" to include "a motion picture, if, at the time of unauthorized distribution, the motion picture (i) has been made available for viewing in a motion picture exhibition facility; and (ii) has not been

2319(d)(2), all in violation of Title 18, United States Code, Section 371 (Count One);

- Conspired with others to commit money laundering, in violation of Title 18, United States Code, Section 1956(h) (Count Two);

- Willfully infringed, for purposes commercial advantage and private financial gain, copyrights by distributing a work being prepared for commercial distribution and by making it available on a computer network accessible to members of the public, in violation of Title 17, United States Code, Section 506(a)(1)(C) and Title 18, United States Code, Sections 2319(d)(2) and 2 (Count Three); and

- Willfully infringed, for purposes of commercial advantage and private financial gain, copyrights by reproducing and distributing during a 180-day period 10 or more copies of copyrighted works, which had a total retail value of more than $2,500, in violation of Title 17, United States Code, Section 506(a)(1)(A) and Title 18, United States Code, Sections 2319(b)(1) and 2 (Count Four) (collectively, the Subject Offenses).

3. This affidavit also is submitted in support of a seizure warrant for the funds currently contained in Regionala Investiciju Banka account number LV32RIBR00185170N0000JSC, held under the name GA Star Trading Ltd. **(Subject Account)**, on the grounds that there exists probable cause that such account contains property derived from proceeds traceable to the Subject Offenses, and thus is subject to seizure pursuant to 18 U.S.C. §§ 981(b), 981(a)(1)(C), and 2323(a)(1)(C).

4. Finally, this affidavit is submitted in support of seizure warrants for the following domain names:

---

made available in copies for sale to the general public in the United States in a format intended to permit viewing outside a motion picture exhibition facility."

a. kickasstorrents.com (**Subject Domain 1**), kastatic.com (**Subject Domain 2**), and thekat.tv (**Subject Domain 3**),[2] which are registered with Verisign, Inc., headquartered at 21355 Ridgetop Circle – Lakeside III, Dulles, Virginia 20166;

b. kat.cr (**Subject Domain 4**) and kickass.cr (**Subject Domain 5**), which are registered with Nic.cr National Academy of Sciences, located at Barrio Francisco Peraltla, de Casa Italia 100 sur y 15 oesta, San Jose, 4444, Heredia, Costa Rica;

c. kickass.to (**Subject Domain 6**), which is registered with Tonic Domains Corp. with the mailing address PO Box 42, Pt San Quentin, California 94964; and

d. kat.ph (**Subject Domain 7**), which is registered with PHRegistrar.PH Web Services (Valley Journal Publishing) G/F ACSFI Bldg. 100P. Zamora St. Buag, Bambang, Nueva Vizcaya, 3702 Philippines (collectively, the **Subject Domains**), on the grounds that there exists probable cause that the **Subject Domains** are property used to facilitate the Subject Offenses, and thus are subject to seizure pursuant to 18 U.S.C. §§ 981(b) and 2323(a)(1)(B).

5. The statements in this affidavit are based on my personal knowledge and from persons with knowledge regarding relevant facts. Because this affidavit is

[2] On or about July 1, 2016, I searched for subdomains for the **Subject Domains** by running inquiries on public websites that permit subdomain searches. These searches revealed no subdomains. Based on these searches, I do not believe that additional websites will be seized as a result of the government's request to seize the Subject Domains.

being submitted for the limited purpose of establishing probable cause in support of the items above, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are sufficient to establish probable cause.

6. This affidavit includes summaries and quotations of certain communications that were obtained by law enforcement pursuant to federal search warrants. Some of those communications included writings in Ukrainian and Russian. While a Ukrainian and Russian language translator has attempted to translate the writings accurately, to the extent that quotations are included, they are preliminary, not final, translations. In addition, the bracketed words and phrases that have been inserted into the communications provide my understanding of such communications based on my training and experience, and the context of the communications. The communications in this affidavit are quoted as they appear in the communication, including the grammatical and spelling errors.

7. I know from my training and experience that the following definitions apply to the activity discussed in this affidavit:

a. *IP Address*: The Internet Protocol address (or simply "IP" address) is a unique numeric address used by computers on the Internet. An IP address can appear as a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be

assigned an IP address so that Internet traffic to and from that computer may be properly directed from its source to its destination.

b. *Server*: A server is a computer that provides services to other computers. Examples include web servers that provide content to web browsers and email servers which act as a post office to send and receive email messages.

c. *Whois*: A "Whois" search provides publicly available information as to which entity is responsible for a particular IP address. A Whois record for a particular IP address will list a range of IP addresses that that IP address falls within and the entity responsible for that IP address range. For example, a Whois record for the IP address 10.147.53.25 might list an IP address range of 10.147.53.0 – 10.147.53.255 and list Company ABC as the responsible entity. In this example, Company ABC would be responsible for the IP addresses 10.147.53.0 through 10.147.53.255.

d. *Domain Name*: A domain name is a simple, easy-to-remember way to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond with a particular IP address. For example, "usdoj.gov" is a domain name.

e. *Domain Name System*: IP addresses generally have corresponding domain names. The Domain Name System (DNS) is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or "labels," that are delimited by periods, such as

"www.example.com." The hierarchy of domains descends from right to left; each label specifies a subdivision, or subdomain, of the domain on the right. The right-most level conveys the "top-level" domain. For example, the domain name "www.example.com" means that the computer assigned that name is in the ".com" top-level domain, the "example" second-level domain, and the web server. For each top-level domain, there is a single company, called a "registry," that determines which second-level domain resolves. Certain top-level domains have been assigned to specific countries. For example, ".de" is a top-level domain for Germany, ".mx" is a top-level domain for Mexico, and ".me" is a top-level domain for Montenegro.

f. *Registrar & Registrant*: Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchaser of the domain name. The individual or business that purchases, or registers, a domain name is called a "registrant." Registrants control the IP address, and thus the computer, to which their domain name resolves. Thus, a registrant may easily move a domain name to another computer anywhere in the world. Registrars typically maintain customer, billing, and contact information about the registrants who used their domain name registration services.

g. *BitTorrent*: "BitTorrent" is a protocol used for peer-to-peer file sharing and permits the quick transfer of large amounts of information over the Internet. Instead of downloading data from a single source, BitTorrent allows a user to connect to a "swarm" of hosts to simultaneously download and upload the

information. The file being transferred is broken into many smaller segments and, as each user receives that segment of the file, it is then made available for upload to other members of the swarm by that particular user. The segments can be received in any order and data transfers can be stopped and re-started at any time, without loss of the already-received segments. As a result, BitTorrent is an efficient means of transferring large files.

II. FACTS ESTABLISHING PROBABLE CAUSE IN SUPPORT OF THE CRIMINAL COMPLAINT AND THE SEIZURE WARRANTS

8. Agents with Homeland Security Investigations and the Internal Revenue Service have been investigating Kickass Torrents, often referred to as "KAT," a widely-popular co mmercial website that since 2008 has enabled millions of users to reproduce and distribute without authorization hundreds of millions of infringing copies of copyrighted works, including motion pictures, television programs, musical recordings, electronic books, video games, and other computer software media, collectively valued at well over a billion dollars. During that time period, KAT has relied on a network of computer servers around the world to operate, including computer servers located in Chicago, Illinois.

9. As further described below, due to the popularity of the copyright infringing content, KAT is estimated to be the 69th most frequently visited website on the entire Internet, receiving over 50 million unique visitors per month. KAT's immense popularity enables its operators to earn millions of dollars a year in online advertising revenue, which is directed to overseas bank accounts held in the

name of other corporate entities. As explained below, Artem Vaulin, also known as "tirm," has been an owner and operator of KAT since at least November 2008. During a significant part of the conspiracy, Vaulin has operated KAT under the auspices of a Ukrainian-based front company called "Cryptoneat."

A. Background on KAT

10. Based on my review of KAT, conversations with other individuals who have used KAT, and my training and experience, I believe that KAT provides a sophisticated and user-friendly environment in which its users are able to search for and locate content, a significant portion of which is protected by U.S. copyright laws. In particular:

a. KAT indexes and arranges torrent files so that users can choose between various search and browsing facilities to assist them in locating content or specific categories of content to download. These facilities include the provision of various RSS feeds[3] that continually alert users to the addition of new torrent files of their selected interest to the website's directory.

b. KAT requires a user who uploads a torrent file to provide the website with detailed information about that torrent file, giving KAT the ability to index the torrent files, make it available for searching, and assist other users in choosing whether or not to download it.

[3] Based on my training and experience, I know that RSS (or Rich Site Summary) is used to publish frequently updated information, such as on a website.

c. KAT provides users with the option of uploading and downloading the content associated with the BitTorrent file via a tracker.

d. KAT provides users with assistance and advice about how to download the indexed torrent files and their associated content.

e. KAT provides users with advice regarding the trustworthiness of particular torrent files, and the likely quality of the content associated with those torrent files. This includes a "FAQ" page that identifies the ultimate source of particular content (e.g., referring to infringed copies of movies, the FAQ page explains that "CAM" refers to a "theater rip," i.e., surreptitious recording of a movie with a camera, that a "telesync (TS)" is the same as a "CAM" but with "an external audio source," that "telecine (TC)" refers to a copy made "digitally from the reels," and that a "DVDScr" is a copy made from a prerelease version used for promotional use), as reflected below (from on or about June 27, 2016 from **Subject Domain** 4):

Search query

BROWSE UPLOAD COMMUNITY

FAQ

SEARCH FAQ

ALL | COMMUNITY | DOWNLOAD AND UPLOAD | GENERAL SITE | GENERAL TORRENTS | PROFILE | OTHER | MY QUESTIONS

What do "BDRip", "DVDRip" and other qualities mean on Torrent titles?

English

in General.Torrents

This is to describe what kind of source has been used to encode the release.

CAM:
A cam is a theater rip usually done with a digital video camera. A mini tripod is sometimes used, but a lot of the time this wont be possible, so the camera may shake. Also seating placement isn't always idle, and it might be filmed from an angle. If cropped properly, this is hard to tell unless there's text on the screen, but a lot of times these are left with triangular borders on the top and bottom of the screen. Sound is taken from the onboard microphone of the camera, and especially in comedies, laughter can often be heard during the film. Due to these factors picture and sound quality are usually quite poor, but sometimes we're lucky, and the theater will be fairly empty and a fairly clear signal will be heard.

TELESYNC (TS):
A telesync is the same spec as a CAM except it uses an external audio source (most likely an audio jack in the chair for the hearing impaired). A direct audio source does not ensure a good quality audio source, as a lot of background noise can interfere. A lot of the times a telesync is filmed in an empty cinema or from the projection booth with a professional camera, giving a better picture quality. Quality ranges drastically, check the sample before downloading the full release. A high percentage of Telesyncs are CAMs that have been mislabeled.

TELECINE (TC):
A telecine machine copies the film digitally from the reels. Sound and picture should be very good, but due to the equipment involved and cost telecines are fairly uncommon. Generally the film will be in correct aspect ratio, although 4:3 telecines have existed. A great example is the JURASSIC PARK 3 TC done last year. TC should not be confused with TimeCode , which is a visible counter on screen throughout the film.

SCREENER (SCR):
A pre VHS tape, sent to rental stores, and various other places for promotional use. A screener is supplied on a VHS tape, and is usually in a 4:3 (full screen) a/r, although letterboxed screeners are sometimes found. The main draw back is a "ticker" (a message that scrolls past at the bottom of the screen, with the copyright and anti-copy telephone number). Also, if the tape contains any serial numbers, or any other markings that could lead to the source of the tape, these will have to be blocked, usually with a black mark over the section. This is sometimes only for a few seconds, but unfortunately on some copies this will last for the entire film, and some can be quite big. Depending on the equipment used, screener quality can range from excellent if done from a MASTER copy, to very poor if done on an old VHS recorder thru poor capture equipment on a copied tape. Most screeners are transferred to VCD, but a few attempts at SVCD have occurred, some looking better than others.

DVD-SCREENER (DVDscr):
Same premise as a screener, but transferred off a DVD. Usually letterbox , but without the extras that a DVD retail would contain. The ticker is not usually in the black bars, and will disrupt the viewing. If the ripper has any skill, a DVDscr should be very good. Usually transferred to SVCD or DivX/XviD.

DVDRip:
A copy of the final released DVD. If possible this is released PRE retail (for example, Star Wars episode 2) again, should be excellent quality. DVDrips are released in SVCD and DivX/XviD.

Figure 1: KAT "FAQ"

f. KAT provides users with advice and assistance regarding how to circumvent blocking measures taken as a result of court orders.

g. KAT offers users a choice between approximately 28 languages and uses "Reputation" and "Achievement" systems that reward users for posting unauthorized copies of copyrighted content.

h. KAT does not disclose information about the identity of the owners, operators, or administrators.

i. Examples of KAT's interface is depicted below (as of on or about July 7, 2016 from **Subject Domain 4**) for movies, television shows, and software:

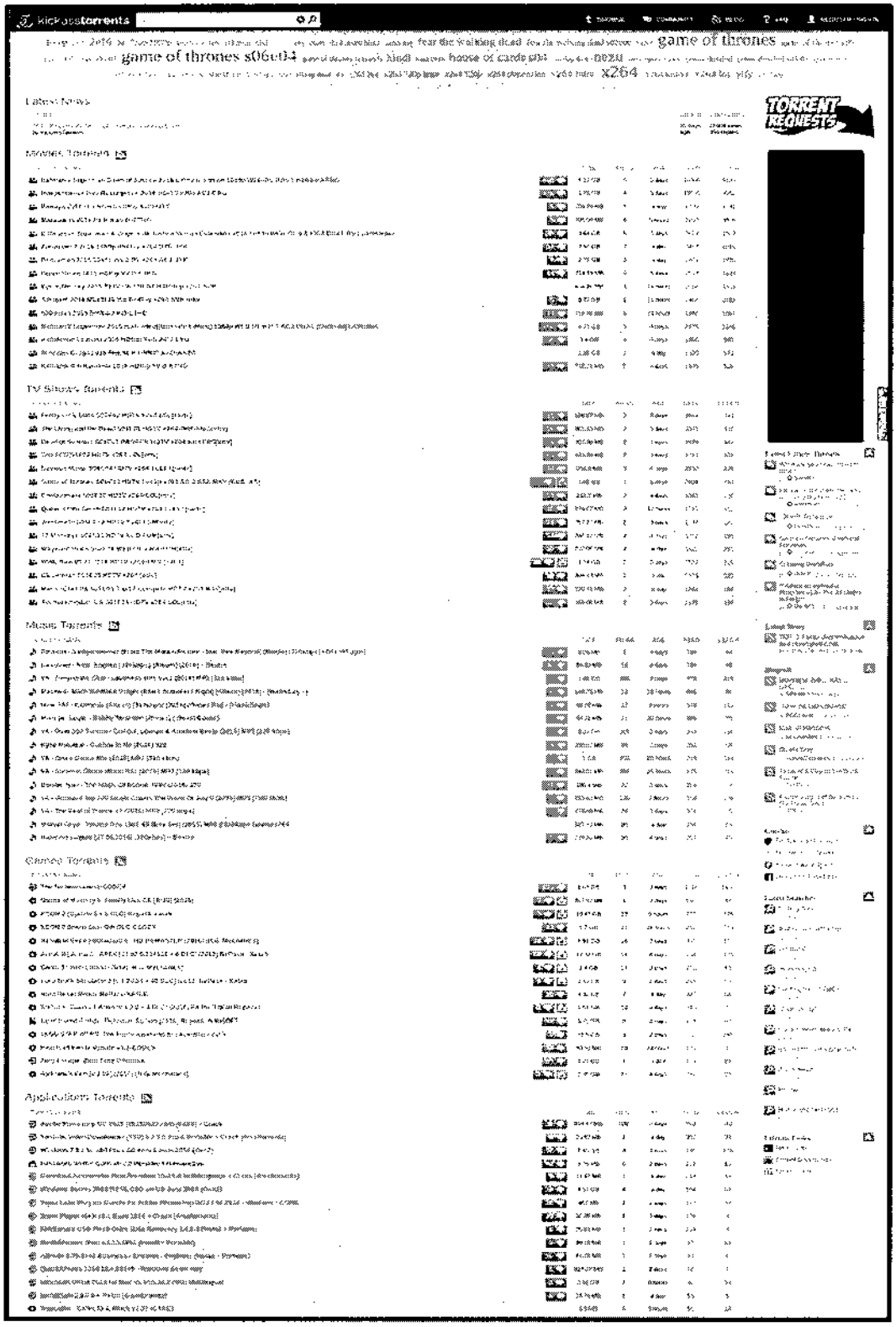

Figure 2: KAT Interface

11. According to alexa.com, a website that tracks Internet traffic, KAT was the 69th most popular website in the world as of June 20, 2016 (Alexa data is based on traffic from the previous three months), averaging over fifty million unique visitors per month.

12. Based on my review of court records, it appears that in the past several years KAT has been held to have infringed copyrights by courts in the United Kingdom, Ireland, Italy, Denmark, Belgium, and Malaysia, among other countries, with Internet Service Providers (ISPs) in those countries having been ordered to block access to KAT.

13. I have viewed KAT's historical content using archive.org, a website that includes, among other content, the "Wayback Machine." According to archive.org, the Wayback Machine is a historical archive of preserved webpages. Websites are periodically "crawled" and captured for preservation. According to archive.org (when visited on or about December 22, 2015), the various websites that have hosted KAT have been crawled thousands of times stretching back to January 31, 2009. According to records from archive.org and other websites, KAT has been hosted at the following domains (among others) during the following approximate date range:

Date Range	Domain
November 2008 through April 2011	**Subject Domain 1** (kickasstorrents.com)
April 2011 through June 2013	**Subject Domain 7** (kat.ph)
June 2013 through December 2014	**Subject Domain 6** (kickass.to)
December 2014 through February 2015	kickass.so
February 2015 through June 2015	**Subject Domain 6** (kickass.to)
June 2015 through the present	**Subject Domain 4** kat.cr

14. Based on my training and experience, and on open source information and court records, I believe that KAT has moved its domains because of domain seizures and copyright lawsuits. For example, according to public databases and news reports:

a. On or about March 29, 2013, an individual who disseminates information about torrent sites sent an email to admin@kat.tt, stating, "I noted that KAT change[d] to the .tt domain. Is there any reason in particular for this move?" The user of admin@kat.tt replied, "Old domain blocked in Italy, UK and UAE. Just want to check how much time it will take to block new domain in this countries." After the individual published information on the Internet about the change, admin@kat.tt responded: "I just wonder if it's possible to get rid of

UPDATE part of the post? Just don't want to come up against UK authorities, you know."[4]

b. On or about June 14, 2013, a complaint was made by the Philippine Association of the Record Industry that resulted in the Intellectual Property Office in the Philippines issuing a temporary restraining order requiring the ".ph" registry to suspend **Subject Domain 7** (kat.ph).

c. On or about February 9, 2015, the kickass.so domain was seized by the ".so" registry, which is associated with a Somalian top-level domain.

d. In early June 2016, KAT launched an anonymous hidden version of its website reachable via the TOR network (available at an ".onion" address),[5] which it described as "[g]ood news for those who have difficulties accessing KAT due to the site block in their country."

15. Based on a review of historical material on KAT, I have found that the format and content of the website remains largely the same (including the presence of advertising), despite the many domain name changes. For example, using archive.org as a reference, there is a topic of conversation listed in the menu sub-forum of the community forum on kat.ph titled, "links to complete sets of tutorials,

---

[4] Based on emails and other records, I am aware that operators of KAT had set up the kat.tt domain, but it does not appear the domain was used for an extended period of time.

[5] "TOR" or "The Onion Router" is a special network of computers on the Internet distributed around the world that is designed to conceal the true IP addresses of the computers on the network, and, thereby, the identities of the network's users. TOR likewise enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites. Such "hidden services" operating on TOR have complex web addresses, generated by a computer algorithm, ending in ".onion."

rules, [and] other tech stuff required here on KAT." The same topic of conversation can also be viewed in previous iterations of KAT, as well as the current location (**Subject Domain 4**).

16. Although KAT may have first been created and hosted at **Subject Domain 1** (kickasstorrents.com), through my investigation I have identified other websites associated with the main website that were created at or near the same time and supported the main website such as www.kickasstorrents.biz ("KAT Website 2"), www.kickasstorrents.org ("KAT Website 3"), and www.kickasstorrents.info ("KAT Website 4").

17. As part of the investigation, I have communicated with representatives of the Motion Picture Association of America (MPAA)[6] regarding this investigation. The representatives provided me with information the MPAA had developed about KAT, among other websites. The representatives stated that the MPAA closely monitors KAT and that a significant portion of the movies available on KAT are protected by copyright. The representatives also specified that the MPAA has not granted permission to KAT to index, link, frame, transmit, retransmit, provide

[6] According to its representative, the MPAA is an organization that represents each of the major motion picture studios in the United States, specifically: Paramount Pictures Corporation; Sony Pictures Entertainment, Inc.; Twentieth Century Fox Film Corporation; Universal City Studios, LLC; Universal City Studios Productions, LLP; Warner Brothers Entertainment, Inc.; Walt Disney Studios Motion Pictures; and their respective affiliates. Among other responsibilities, the MPAA advocates for and enforces the intellectual property rights of its member studios. In addition to motion pictures, MPAA member studios also possess the copyright to many television shows.

access to, or otherwise aid or assist those who distribute and reproduce infringing copies of copyrighted motion picture or television content of MPAA members.[7]

18. Based on my review of website captures from archive.org, KAT has consistently made available movies that are still in theaters and displayed advertising throughout its website. A screen shot of **Subject Domain 1** from on or about January 31, 2009, for example, reflects over five million available torrents and over 7 million users who were actively downloading material. The screen shot reflects the top five "most popular" torrents for each of the following categories: "movies," "tv shows," "music" and "games." The screen shot further reflects that each of the movies had thousands of active downloads. Moreover, at least three of the five movies had not yet been released on DVD. The following table reflects additional examples of movies I identified as being available on KAT domains, along with the theater and DVD release dates for those movies, based on imdb.com and dvdreleasedates.com, respectively:

[7] In or about March 2016, the MPAA provided an estimation of loss exceeding $324,000 for six recent movie titles available on **Subject Domain 4** (Deadpool, The Revenant, Sisters, Star Wars: The Force Awakens, Ride Along 2 and Zootopia) based on the number of Torrent downloads for those movies on the site.

Date	Domain	Movie	Released in Theaters	Released on DVD
July 6, 2009	**Subject Domain 1**	Transformers: Revenge of the Fallen	June 24, 2009	October 20, 2009
		Ice Age 3: Dawn of the Dinosaurs	July 1, 2009	October 27, 2009
July 31, 2011	**Subject Domain 7**	Captain America the First Avenger	July 22, 2011	October 25, 2011
		X-Men First Class	June 3, 2011	September 9, 2011
May 3, 2014	**Subject Domain 6**	The Amazing Spiderman 2	May 2, 2014	August 19, 2014
		Walk of Shame	May 2, 2014	July 17, 2014

19. Between on or about June 24, 2016, and on or about June 30, 2016, HSI Special Agents downloaded from the Northern District of Illinois the following prerelease movies from KAT (at **Subject Domain 4**): Batman V Superman: Dawn of Justice, Captain America: Civil War, Central Intelligence, Deadpool, Finding Dory, Independence Day: Resurgence, Teenage Mutant Ninja Turtles: Out of the Shadows, X-Men Apocalypse, and Now You See Me 2. KAT's website indicated that many of these movies had been downloaded hundreds of thousands of times. For example, in just a few days, Batman V Superman: Dawn of Justice had been downloaded over 532,000 times and Captain America: Civil War had been downloaded over 470,000 times. The file name for Captain America: Civil War included the description "TC," which according to KAT's FAQ page refers to a version that is copied "digitally from the reels," i.e., the film stock delivered to movie theaters for projection. Many of these movies included a copyright notice in

the film, which identifies the studio that owns the copyright for the movie. I obtained copyright certificates for many of these movies, including Captain America: Civil War (for which Marvel Entertainment LLC is the copyright holder). Based on data provided by representatives of the copyright holders, the total retail value of the downloaded copies of the copyrighted works referenced in this paragraph exceeds $1,000,000.

20. KAT's website purports to comply with the removal of copyrighted materials being linked by its website but review of evidence provided by industries that represent the copyright holders such as the MPAA, the Recording Industry Association of America (RIAA), and Entertainment Software Association (ESA) reflects that the operators do not remove all of the copyrighted content and are not compliant with removal requests. In particular, the ESA and the RIAA have provided me with email exchanges with purported operators of KAT.

21. As an example, on June 1, 2016, the IFPI provided a DMCA[8] notice by email to copyright@kat.cr (an email address KAT's website lists for "Copyright complaints") and to admin@kat.tw titled "DMCA Notice." That notice identified the sender, explained that it represents companies in enforcing their copyrights, identified a list of KAT web addresses for infringing copies of sound recordings, and

[8] As part of the Digital Millennium Copyright Act (DMCA), Title 17, United States Code, Section 512 provides a safe harbor from civil liability for service providers so long as they do not receive a financial benefit directly attributable to the infringing activity, are not aware of the presence of infringing material or know any facts or circumstances that would make infringing material apparent, and upon receiving notice from copyright owners or their agents, act expeditiously to remove the allegedly copyright infringing material.

requested that KAT delete or disable the web addresses. A response was sent the following day from copyright@kat.ph

> Greetings,
>
> Your request has been reviewed, but cannot be processed due to one (or more) of the following reasons:
> 1) The Claim wasn't written in English language;
> 2) You provided no evidence showing that you are the copyright holder or that you are acting on behalf of the copyright holder;
> 3) You provided no evidence showing that the content is legally copyrighted;
> 4) There were more then 30 torrents mentioned in the Claim email;
> 5) Your content is hosted on a different website.
>
> Please, make sure to fulfill all the conditions mentioned above before sending a claim.
> You can find more detailed information regarding the DMCA email layout via the following article - https://kat.cr/dmca/
>
> Respectfully,
> KAT team

22. Correspondence received from the International Federation of the Phonographic Industry, the RIAA, and the ESA indicates that KAT has sent this same response to requests to remove copyright infringing material from each of these entities.

B. KAT's Advertising Revenue and the Undercover Operation

23. Given the popularity of KAT, and the presence of significant advertising on KAT that I have observed, it appears the website generates significant revenue. For example, the website siteprice.org, which estimates the advertising revenue that websites generate, estimated (as of on or about June 20, 2016) that KAT generates approximately $16,967,865 in annual advertising

revenue and is worth approximately $54,593,622. In addition, in February 2013, the England and Wales High Court, in finding that KAT infringed copyrights, cited an expert report that estimated KAT's annual advertising revenue "on a very conservative basis" to range from $12,525,469 and $22,383,918.

24. Communications and website postings from KAT obtained as part of the investigation also explain KAT's reliance on advertising sales as its source of revenue since near the time of its inception. One of KAT's founders explained its business model in a chat on or about October 10, 2010, to an individual asking whether KAT would become a "pay site." He explained that there are "no paid services on kickasstorrents," but rather that the site had "banner ads," and noted that "people will understand you have to make money :)". Likewise, in a screen shot of **Subject Domain 1** from on or about December 22, 2010, KAT's official user rules page invited users interested in placing advertising to reach out to the site's owners. A blog posting on **Subject Domain 1** from on or about October 12, 2010, by "kickasstorrents" further explains that "since day one" the site has uses advertising as a way to avoid having to charge users "fees or payments."

25. On or about November 13, 2015, an undercover IRS Special Agent (UC-1) sent a request to the email address pr@kat.cr (an email account listed on KAT's website for "press"),[9] inquiring about advertising on KAT. Additionally on or about November 17, 2015, UC-1 sent a private message on the KAT forums to the

[9] KAT's website has made an email account available for "press" since at least as early as in or about August 2009.

administrator "Mr. White" and followed up with another email to admin@kat.cr. On or about November 24, 2015, UC-1 received a response from the email address admin@kickass.to regarding UC-1's inquiry and the two exchanged several emails during which UC-1 provided the KAT representative with a link for an undercover website purportedly advertising a program to study in the United States. The KAT representative agreed to provide UC-1 advertising for $300 per day. During one of the exchanges, on or about December 9, 2015, a representative of KAT, using admin@kickass.to, provided UC-1 with banking information for payment to advertise on KAT's website—a Latvian-based account held at Regionala Investiciju Banka, account #LV32RIBR00185170N0000JSC, in the name of "GA Star Trading Ltd, 9 Barrack Road Belize City, Belize" (the **Subject Account**). After providing the banking information, the KAT representative instructed UC-1, "Could you please make sure that you don't mention KAT anywhere?" in connection with payment to the bank for advertising.

26. On or about February 8, 2016, UC-1 reinitiated contact with the KAT representative. On or about February 19, 2016, the KAT representative responded with the same banking information for the **Subject Account**. The KAT representative stated UC-1 "Please make sure that the bank details are entered correctly and you don't mention KAT or 'for advertising' anywhere. Could you please also inform me when you send the payment?"

27. On or about March 9, 2016, as part of the undercover operation, IRS wire transferred $1,500 from a location in Chicago to the **Subject Account** for the payment of an advertising fee, consisting of advertising for five days at $300 per day. The next day, the KAT representative confirmed that the payment was received.

28. On or about March 14, 2016, the KAT representative informed UC-1 that a download button featuring the UC-1's website was posted on the KAT website for five days as promised. The next day, agents verified and made a recording of the advertising. UC-1 discovered that users were redirected to the undercover website when they clicked the "Download faster" link for the prerelease movie Deadpool, as depicted below in Figure 3:

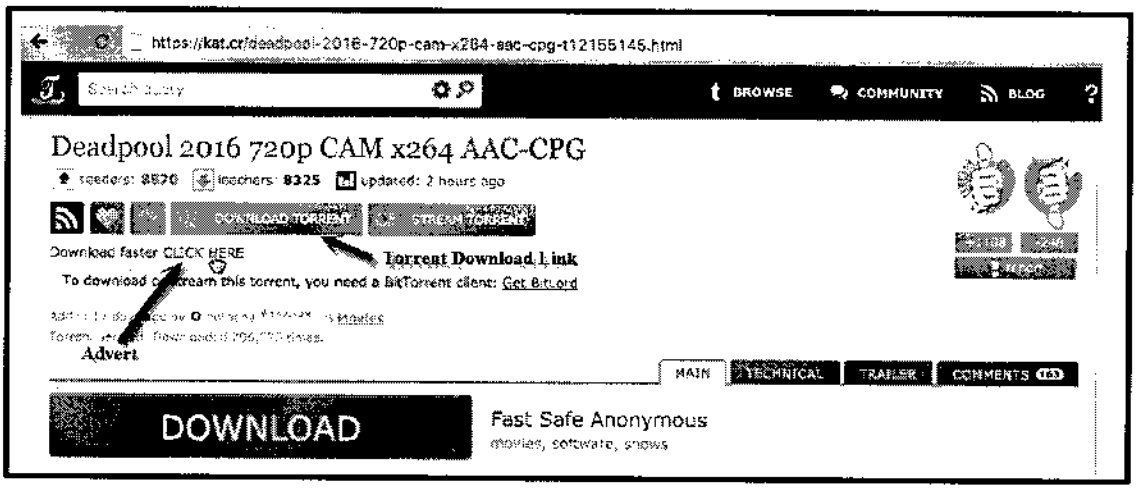

Figure 3: Undercover Advertisement

29. On or about March 19, 2016, UC-1 inquired about advertising on the KAT website again. The KAT representative replied on or about March 21, 2016, stating that the advertisement banners had been sold out until the end of the

month. The following day, the KAT representative provided UC-1 with three different banner ad options, with fees ranging from $1,000 to $3,200 per day.

30. On or about May 11, 2016, in response to a request from UC-1 for a new bank account, the KAT representative provided UC-1 with another account to receive funds for advertising, an Estonian-based bank held at AS Eesti Krediidipank, account number *6107, in the name of "Glomeratus LTD, Beneficiary address: 1 Straits Parade, Bristol, BS16 2LA, UK." The KAT representative wrote: "Please pay attention to the bank details. They should be entered correctly. Also please don't mention KAT and 'for advertising anywhere.' Could you please inform me when you send the payment?" On or about May 13, 2016, the KAT representative provided UC-1 with another payment method for advertising, a WebMoney account as well as an account for a Russian-based payment system. On or about July 1, 2016, as part of the undercover operation, IRS wire transferred $1,000 from a location in Chicago to the Glomeratus LTD bank account to purchase additional advertising.

31. The investigation obtained bank records from Latvia pursuant to a request under the Mutual Legal Assistance Treaty. Those records reflect that the **Subject Account** received a total of approximately €28,411,357 in deposits between on or about August 28, 2015, and on or about March 10, 2016. The account balance as of March 10, 2016, was €14,656. A sizable portion of the funds appear to

be related to advertising revenue.[10] For example, there are deposits totaling €199,828 from a Dutch online advertising company Adperium with a memo line "KAT TC REVENUES." The deposits also include €110,125 over the course of fifteen periodic deposits from on or about September 1, 2015, to on or about March 2, 2016 from a known KAT advertising partner, MGID, sent from a Bank of America account in the United States.[11]

C. KAT's Use of Social Media

32. The operators of KAT also use social media to advertise and provide updates about the website. Records from Facebook identified that on or about February 19, 2010, a Facebook account was created, titled "official.KAT.fanclub." Based on historical screen captures of KAT's website, I have determined that since at least August 2010 the KAT Facebook Account has been the account linked to KAT as its official Facebook account. The account was registered to the email address pr@kat.ph. Based on my review of screenshots of KAT, I know that KAT has used the email address pr@kat.ph to receive inquiries after switching to the domain kat.ph in or about April 2011. A majority of the messages I have reviewed

---

[10] Although some of the transactions do not reference advertising, I know from my review of Vaulin's email accounts that he tries to conceal the nature of his transactions.

[11] I am aware MGID is an advertising partner for KAT based on emails collected via search warrant in this investigation in which representatives of MGID discuss advertising with operators of KAT. According to its website, MGID facilitates online advertising and has a location in Los Angeles, California and Kiev, Ukraine. One email the investigation has obtained was sent from on or about November 24, 2011, from a person holding himself out as a "mediabuyer" from MGID who sought to "buy[] ads" from another website and represented that MGID "already work[s] with . . . kat.ph."

from the KAT Facebook Account reflect updates that the KAT administration had taken on the website. For example:

a. On or about January 27, 2013, the KAT Facebook Account posted a message stating: "Kat.ph will get back online soon. For now feel free to use kickasstorrents.com."

b. On or about November 17, 2014, the KAT Facebook Account posted a message stating:

> Hi everyone!
> We are moving to kickass.so now. As you know we change our domain regularly. Nothing more has been changed for you, so don't worry, you can use Kickass as usually, it's automatically redirected.

c. On or about March 17, 2015, the KAT Facebook Account posted a message stating: "Hi all! Today kickass.to is on technical maintenance, so KAT can be down from time to time. Don't worry, we'll be back asap!"

d. On or about January 21, 2016, the KAT Facebook Account posted a message stating:

> Make sure you are browsing genuine Kickasstorrents and not some fake site. Our domain is https://kat.cr/ and the list of safe proxies is here https://kastatus.com/, everything else – fake.

D. The KAT Computer Servers in Chicago

33. Through the investigation, I identified two IP addresses (66.90.101.199 and 66.90.101.200) that were associated with KAT, both of which were owned and subleased by a Chicago-based hosting company.

34. According to records provided by the Chicago hosting company, the IP address 66.90.101.199 was first available on November 10, 2011, and had been held by the same customer since that time (as of in or about January 2016). According to a reverse DNS search[12] conducted by the hosting company on or about May 5, 2015, that server was the mail client "mail.kat.ph."[13] The hosting company also reported that it had performed a reverse DNS search on or about March 7, 2012, which also reflected that the server was the mail client "mail.kat.ph."

35. As explained above, the website kat.ph (**Subject Domain 7**) was once the domain that hosted KAT. Captures from archive.org show that KAT was accessible from **Subject Domain 7** as early as on or about April 8, 2011, through on or about June 12, 2013, and that the mail client mail.kat.ph was used for that website.

36. According to records provided by the Chicago hosting company, the IP address 66.90.101.200 was first available on November 15, 2011, and had been held by the same customer since that time (as of in or about January 2016). According to a reverse DNS search conducted by the hosting company on or about May 5, 2015, the server was listed as the secondary name server (or "NS2") for the domain hostednsor.com (ns2.hostednsor.com).[14] A review of hostednsor.com's

---

[12] A reverse DNS (or Domain Name Server) search or lookup is the determination of a domain name that is associated with a given IP address using the Domain Name System

[13] A mail client is an application that enables one to send, receive, and organize email.

[14] Based on my training and experience, I know that a name server is a web server that enables customers to manage their domain names and update information about those

hosting history reflects, among other things, that it became an active domain and active name server on approximately June 20, 2012. The website was originally registered and remains registered using a privacy protection service that protects the true domain owner's identity and contact information.

37. Review of the name server history for the original KAT website **Subject Domain 1** shows that the website acted as its own name server from on or about November 8, 2008, through on or about July 5, 2012, at which point it began using the name server hostednsor.com (i.e., the Chicago hosting company server with IP address 66.90.101.200), and had remained as such as of on or about January 12, 2016. Further review of historical name server records show that kastatic.com (**Subject Domain 2**)[15] switched its name servers on or about June 20, 2012, to hostednsor.com and that historically the following KAT related websites, including all of the websites that have hosted KAT, have utilized at one point and time from mid-2012 through December 2015 hostednsor.com as its name server: **Subject Domains 3 through 7**.

---

domains in DNS databases. In particular, a name server enables customers to modify the IP address associated with their domain names and/or redirect traffic from one domain to another. There are two main types of name servers—primary and secondary. Secondary name servers are important because they provide security in the form of redundancy. They also lessen the load placed on the primary server and ensure that there is always a server working to deliver data.

[15] Based on my review, kastatic.com is another website associated with the administrators of KAT that supports the visual and operational aspects of the KAT website. Specifically, it is used to support kat.cr's webpage styling and images with Cascading Style Sheets and Javascript that assists in making the website operational.

38. On or about December 15, 2015, I performed multiple reverse DNS searches on the following KAT-affiliated websites: **Subject Domains 1, 3, 4, and 5**. I found that all of the websites were actively utilizing the Chicago hosting company server IP address 66.90.101.200 as one of their name servers.

39. On or about January 25, 2016, pursuant to a search warrant, a forensic image was made of the server hosting IP addresses 66.90.101.199 and 66.90.101.200. Based on my review of the forensic image, I observed that its hostname is "us1.ext.kat.ph" and that it was running the Linux Gentoo operating system. I also located multiple files that contained unique user information, access logs, and other information. These files include a file titled "passwd" located in the "etc" directory,[16] which was last accessed on or about January 13, 2016, and which identified the users who had access to the operating system. I also discovered files that contained a log of the SSH[17] connections to the server from on or about January 13, 2016, through on or about January 20, 2016.

E. The KAT Computer Servers in Canada

40. As part of the investigation, HSI agents determined that KAT was using the following four static[18] IP addresses to support **Subject Domain 4**

[16] The /etc/passwd file is a user database that contains fields reflecting the username, real name, home directory, and other information about each user.

[17] "Secure Shell" or "SSH" is a communications protocol that allows computers to securely connect to one another through the internet. Through an SSH connection, an individual may login and issue and execute commands on a computer server.

[18] A "static" IP Address is fixed. Web sites use static IP addresses so that they can be located at any time.

(kat.cr): 67.212.88.10; 205.204.64.122; 68.71.58.34 and 67.212.88.146 (the "KAT Canadian IP Addresses"). HSI agents conducted a Whois inquiry of these IP addresses using the IP search engine "centralops.net," which reflected that they all were hosted by a Canadian Internet Service Provider.

41. On or about April 12, 2016, in response to a Mutual Legal Assistance Treaty request to the Central Authority of Canada, the Royal Canadian Mounted Police received the business records and made a forensic image of the original hard drives associated with the KAT Canadian IP Addresses. Thereafter, those records and forensic images were turned over to HSI.

42. Based on my review of the forensic images for three of the four servers,[19] I observed that the hostnames were "ca4.ext.kat.ph," "ca3.ext.kat.ph," and "ca1.ext.kat.ph," that they were all running the same Linux Gentoo operating system, and that they contained files with user information, SSH access logs, and other information, including a file titled "passwd" located in the "etc" directory. I also located numerous files associated with KAT, including directories and logs associated to their name servers, emails and other files.

F. Artem Vaulin's Operation of KAT Through the Company Cryptoneat

43. Through this investigation, as further described below, I have identified several individuals who are associated with the operation and ownership

[19] I was unable to access the one of the forensic images because the hard drive appears to have failed.

of KAT. One of those individuals is Artem Vaulin, also known as "tirm." I have also identified a company named Cryptoneat, which is used at least in part to conceal the operation of KAT and which is purportedly owned by Vaulin.

44. As I have observed on current and past screen captures of the KAT website, there is a page titled "People," which publicizes the current usernames of KAT administrators and staff. Screenshots of the KAT "People" page from in or about February 2010 list the website's administrators as users "tirm," "Alex," "counterzer0," "chill," "tolum," and "yd." Another screenshot of KAT's "People" page, from on or about August 8, 2010 (on **Subject Domain 1**), listed one of the website administrators as "tirm The Owner, too busy for all your problems," as shown below:

Magic People, Kickass People!

The big guys, doing important stuff

Administrators

- tirm The Owner
  too busy for all your problems
- chill The Offline Administrator
  also a busy guy
- Tolum The Legal Guy
  deals with the legal issues
- leyedwillie Site Administrator
  anytime

Wizards

- Alex The Main Wizard
  coding 25/8
- counterzer0 The Vice Wizard
  coding 24/7
- wildt The Small Wizard
  coding 24/7
- yd The Designer
  created the website design and constantly works on improving it
- 100asa The Tester
  Kickass Quality Analyst

KickassTorrents staff

- Kickass_Sid Jack of All Trades
  The guy responsible for all translation/tech/mod abuse issues, you got a problem - write him.
- lsg2007 The Modfather
  The guy responsible for all forum/site/mod issues, you got a problem - write him.
- LRS Head of the Mods
  US Time
- runeman Head of the Mods
  European Time
- BigSeals23 The Rules Enforcer
  Be aware!

2008-2010 KickassTorrents.com

- change language
- lite
- Achievements
- trends
- Latest Searches
- api
- about
- privacy
- dmca
- rules
- stats
- logos
- people
- contacts

Figure 4: KAT "People" Page from August 2010

45. As of on or about February 3, 2011, I observed that the administrators, including the reference to tirm, were removed from KAT's "People" page.

46. As part of this investigation, I also reviewed historical messages posted by tirm, KAT's purported "Owner." For example, on or about July 19, 2010, a user posted a message in KAT's "Site Problems" sub-forum stating that the website description box did not open when uploading to the website; tirm replied to the message stating "fixed." Then, on or about July 16, 2010, a user on KAT posted a message in the "Feature Requests" section of the forum asking, "How come their's no pic on the profile's just wondering?" tirm again replied "fixed." These postings and others indicate that tirm was actively engaged in the early running of KAT in addition to being listed as an administrator and the website's owner.

1. Vaulin's Involvement in KAT at Its Inception

47. A review of historical Whois information for KAT Website 2 identified that it was registered on or about January 19, 2009, to Artem Vaulin with an address located in Kharkiv, Ukraine. The telephone number of +380 506693769 ("Vaulin Phone Number") and the email address admin@yabloggy.com were listed as contact information. The Whois records reflected that it was registered to Vaulin through at least on or about February 26, 2011. Vaulin was listed as registering KAT Website 3 on the same day as KAT Website 2, with the same contact information. KAT Website 3's registration information remained registered to Vaulin through at least on or about September 7, 2010. On or about February 27,

2009, KAT Website 4 was registered under Vaulin's name, which remained so through at least on or about December 16, 2010.

48. Records from Internet Service Provider GoDaddy also indicate that Vaulin created KAT Websites 2, 3 and 4. According to GoDaddy records, Vaulin purchased all three website domains on or about January 18, 2009. According to GoDaddy records, on or about January 11, 2010, Vaulin paid to renew all three websites for another year until they expired on or about January 17 and 18, 2011. Those records also reflect that on or about January 18, 2009, Vaulin paid to place the website www.kickasstorrents.net on backorder to buy since it was unavailable at the time for purchase. I reviewed historical screen captures of KAT Website 2 and KAT Website 3, and they appeared to be websites that supported KAT Website 1 by offering search boxes that would search data contained on KAT's main website domain, **Subject Domain 1**.

49. Shortly after KAT Website 1 was purchased, on or about November 11, 2008, Vaulin sent an email from his account avaulin@gmail.com[20] to his other partners with the description "kickasstorrent mock up v2" in the subject line and a picture attachment, depicting what appears to be a proposed website interface for "kickasstorrents." The mock-up includes "Latest Movie," "Latest TV Show," "Latest Music," and "Latest Games" sections, including sample movies with the names

[20] Although this account was closed on or about April 16, 2013, emails found in Vaulin's tirm@me.com account indicate that Vaulin operated it, such as an email dated on or about October 19, 2010 titled "test" with no other content in the body of the email that was sent from Vaulin's tirm@me.com account to his avaulin@gmail.com account.

"DvDrip" in the title. The image is nearly identical to the appearance of the KAT website, which became public shortly thereafter.

50. Finally, on or about an email on November 23, 2009, Vaulin, using the account avaulin@gmail.com, sent an email to another individual who disseminated information about torrent sites. It stated: "i changed my gmail. now it's admin@kickasstorrents.com."[21]

2. Vaulin's Operation of KAT

51. During the course of this investigation, I have identified an Apple email account tirm@me.com that belongs to Vaulin.[22]

52. Records provided by Apple showed that tirm@me.com conducted an iTunes transaction using IP Address 109.86.226.203 on or about July 31, 2015. The same IP Address was used on the same day to login into the KAT Facebook Account. Then, on or about December 9, 2015, tirm@me.com used IP Address 78.108.181.81 to conduct another iTunes transaction. The same IP Address was logged as accessing the KAT Facebook Account on or about December 4, 2015.

---

[21] Based on my training and experience, and on evidence collected in this investigation, I know that an "admin" or administrator account is a user account that permits the user to make changes to other user accounts, install software and hardware, and access all files on the computer.

[22] It appears that the account is Vaulin's for a number of reasons, including: (1) the account was registered November 20, 2010, in the name "Artem Vaulin" with an address located in Kharkiv, Ukraine, and the Vaulin Phone Number; (2) the backup email address, admin@yabloggy.com, is the same address listed in the Whois registration for KAT Websites 2, 3 and 4; (3) the backup account is artem@cryptoneat.com, which is registered to Artem Vaulin and for which tirm@me.com is listed as the rescue email; and (4) the tirm@me.com contains a number of identifying items, such as copies of Vaulin's Ukrainian passport and driver's license, personal banking information, and other business records in Vaulin's name.

53. I identified a number of emails in the tirm@me.com account relating to Vaulin's operation of KAT. In particular, between on or about June 8, 2010, and on or about September 3, 2010, there are approximately thirty-one emails from the email address alerts@kickasstorrents.com to Vaulin's tirm@me.com account. Each of these "alerts" began with "KickassTorrents" followed by a "feature" number and a reason for the alert. These alerts appear to reflect KAT-related tasks Vaulin created and assigned to individuals helping with KAT's operations. The following are examples of these alerts:

a. On or about June 23, 2010, Vaulin received an alert with the subject line, "[KickassTorrents – Bug#159] (Resolved) Create post page for blogs." The email identified a task which "Artem Vaulin" authored and stated:

> Issue #159 has been updated by [Individual A].
> -Status changed from New to Resolved
> -Assigned to changed from [Individual A] to [Individual B]
> -% Done changed from 0 to 100
> In revision 6741
>
> Feature #159: Create post page for blogs
> -Author: Artem Vaulin
> -Status: Resolved
> -Priority: Normal
> -Assigned to: [Individual B]
> -Category:
> -Target version: Sprint 2

b. On or about June 29, 2010, Vaulin received an alert with the subject line, "[KickassTorrents – Feature#185] (Closed) Create Facebook Block," for a task "Artem Vaulin" authored. The email stated:

Issue #185 has been updated by [Individual C].
-Status changed from New to Closed
-% Done changed from 0 to 100

Feature #185: Create Facebook Block
-Author: Artem Vaulin
-Status: Closed
-Priority: Normal
-Assigned to: [Individual C]
-Category:
-Target version: Sprint 3

c. On or about June 30, 2010, Vaulin received an alert with the subject line, "[KickassTorrents – Feature#56] (Closed) Monitor import from other sites." The email stated:

Issue #56 has been updated by [Individual D].
-Status changed from In Progress to Closed

Feature #56: Monitor import from the other sites
-Author: Artem Vaulin
-Status: Closed
-Priority: Immediate
-Assigned to: [Individual D]
-Category:
-Target version: Sprint 2

The page is in admin. List of sites. Next to each is the number of total torrents. Download count for the past 24 hours. Time of the last link to the site. Time of the last successful link to the site.

54. On or about August 6, 2011, Vaulin received a forwarded email from a KAT employee that was sent from the AP Film Chamber, an Indian-based organization that services the film industry, to kickasstorrents requesting data as it relates to the Digital Millennium Copyright Act regarding the IP address of

certain KAT users who uploaded copyright infringing material. The subject line was "Ignore?," to which Vaulin replied, "Of course."

55. A review of an email account of another KAT employee revealed approximately 248 additional emails sent between on or about May 11, 2012, and on or about December 11, 2012, from the email account bugs@geekyteam.com to Vaulin at his tirm@me.com account with subject lines beginning with "KAT" followed by "bug," "task," or "wiki."[23] As an example, an email on or about December 10, 2012 had the subject line, "[KAT – Task #5972] Renew 500ky" and appears to be an "urgent" task created by "tirm," relates to issues with KAT's integration with its social media accounts (Facebook and Twitter), and appears to include instructions for Individual C.

56. Vaulin also paid attention to KAT's popularity, tracking its Alexa ranking. For example, on or about May 8, 2010, Vaulin sent an email to another person stating, "Hi [redacted]. Why you haven't [**Subject Domain 1**] in your torrent list article? it's alexa 500 torrent site)." Moreover, Vaulin reviewed material on KAT and provided information about that material, such as on or about March 29, 2011, when an individual reached out to Vaulin at his tirm@me.com account with the subject line "new movies." The individual asked about the movies Kung Fu Panda and The Hangover, remarking that people were

[23] In this context, these terms appear to relate to the reporting of software bugs (i.e., an error or flaw in a computer program or system), and the task of eliminating those software bugs.

asking for those movies. Vaulin replied that same day, noting that Kung Fu Panda was added six hours ago and that The Hangover was just added.

57. On or about March 16, 2012, Vaulin received four emails into his tirm@me.com account in close succession from the accounts admin@kat.ph and admin@kickasstorrents.com, each having the word "test" in the subject line. After this, Vaulin's tirm@me.com had very few emails relating to KAT. Based on my training and experience, it appears that Vaulin was sending the emails from the various KAT administrative accounts to himself to see if they were working, at which point Vaulin began using KAT's internal email system for KAT business.

58. On or about May 24, 2012, an individual chatted with Vaulin at admin@kickasstorrents.com about a recent court order in Italy blocking access to kat.ph and a potential criminal investigation. The individual wrote that a source said "the blocking in Italy is on both DNS and IP of www.kat.ph and the old dns" and that "the investigation on the criminal organization behind the site is still making progress." Vaulin responded, "hm, interesting."

3. Vaulin's Involvement in KAT's Financial Operations

59. Vaulin's tirm@me.com account included emails relating to advertising payments to KAT. For example:

a. On or about May 15, 2010, Vaulin received an email with the subject line "kickasstorrents april payment." Vaulin then exchanged emails about the receipt of funds and requested payment for the month of May. Based on the

context of these emails and the nature of KAT's revenue source, I believe these payments relate to advertising.

b. On or about December 12, 2011, Vaulin sent an email to m@kat.ph with an Excel spreadsheet attachment titled "popunders."[24] This spreadsheet contained a list of 16 countries in one column and another column titled "Amount (k)," which appears to be a reference to an amount in the thousands and reflects a total of 36,203,000 in funds, though the currency is unspecified.

60. On or about August 8, 2012, KAT's Frequently Asked Questions page of its website listed the question, "Is it possible to make a donation to the site?" followed by the response, "Yes, you can donate with bitcoin[25] to this address: [Bitcoin Address]" ("KAT Bitcoin Donation Address"). Records received from the bitcoin exchange company Coinbase revealed that the KAT Bitcoin Donation Address sent bitcoins it received to a user's account maintained at Coinbase. This account was identified as belonging to Artem Vaulin located in Kharkov, Ukraine, with a backup email address of tirm@me.com. The telephone number listed on the Coinbase account was the Vaulin Phone Number, i.e., the number listed for KAT Websites 2, 3 and 4. The KAT Bitcoin Donation Address shows at least one

[24] Popunders is a digital form of advertising used on KAT's website that opens up advertisement windows under the user's main browser window.

[25] Bitcoin is a form of decentralized, convertible digital currency that exists through the use of an online, decentralized ledger system. The currency is not issued by any government, bank, or company, but rather is generated and controlled through computer software operating via a decentralized network. To acquire Bitcoin, a typical user will purchase them from a Bitcoin seller or "exchanger." It is also possible to "mine" bitcoin by verifying other users' transactions.

transaction being moved from its account on or about August 20, 2014, to a Coinbase account in Vaulin's name. A total of $72,767 worth of Bitcoin (valued at the time of transaction) was deposited into Vaulin's Coinbase account.

61. The records returned by Facebook also provided the IP logins to the KAT Facebook Account since on or about October 21, 2014. Notably, IP address 78.108.178.77 accessed the KAT Facebook Account about a dozen times in September and October 2015. This same IP Address was used to login to Vaulin's Coinbase account 47 times between on or about January 28, 2014, through on or about November 13, 2014.

62. Finally, a review of Vaulin's tirm@me.com account also reveals ties to GA Star Trading (i.e., the beneficiary name for the **Subject Account** that received the undercover funds for KAT advertising and which received over 28 million Euros in less than seven months). For example:

a. In or about February 2016, the GA Star Trading account received deposits totaling approximately €600,000 from Castleton Trading. Based on corporate records found in Vaulin's tirm@me.com email account, it appears that Vaulin has a controlling interest in Bitcoin Innovations Ltd. Those corporate records also identified Castleton Trading as a shell company that held 500 of the 2,000 shares of Bitcoin Innovations Ltd. Moreover, agents identified several personal bank accounts through the review of Vaulin's tirm@me.com account. The review of Vaulin's Baltic International Bank (Latvia) statement for an account

ending in *5001 revealed several deposits from Castleton Trading LP. The April 2015 deposits totaled approximately €65,250 and identified the transactions as "payments for software development."

b. On or about February 12, 2015, an individual sent Vaulin an email with the subject line "Beriott_bank request." I know from my review of the Latvian bank records, correspondent bank records, and open sourced search of U.K. corporate documents that GA Star Trading previously operated as Beriott Trading Ltd.

4. Vaulin's Ties to the KAT Computer Servers in Chicago and Canada

63. As mentioned above, while reviewing the KAT Chicago and Canadian Servers, I found on both servers a "passwd" file, identifying the users who have access to the operating system. On both the KAT Chicago and Canadian servers, I observed that one of the home directories was for a user by the name "nike." During the search of Vaulin's Apple iCloud account I discovered that Vaulin has an instant message account he uses with the username "nike."

64. I also reviewed several files from the KAT Chicago and Canadian servers that contained SSH access logs. One of the KAT Canadian servers had records that began logging on or about September 6, 2015, through on or about October 4, 2015. In this log a user accessed the server approximately 99 times

during that time period as the "root"[26] user and using the same unique DSA[27] key to access the server each time. Based on my training and experience, this indicates that a single user with the same unique key was the only user during that period of logging with direct root user access to this server. I also observed on the KAT Chicago server the root user accessed server through SSH at least 35 times between on or about January 13, 2016, and on or about January 20, 2016.

65. The SSH logs for the KAT Canadian servers also showed that this unique root user accessed the server from three different IP addresses during this period. The KAT Chicago server SSH logs showed two different IP addresses were accessing as root, which were the same IP addresses as the KAT Canadian servers. During my investigation I have also observed those three IP addresses being using by Vaulin to access his email account tirm@me.com throughout 2015 and in January 2016 and his Coinbase account multiple times in 2014 and 2015. I also observed the same three IP addresses accessing the KAT Facebook account.

66. While reviewing the business records for the KAT Canadian Servers, as well as reviewing records the KAT Chicago services, I observed that one of the clients responsible for renting the servers used the same email address c[redacted]y@gmail.com. This same client was responsible for renting the KAT

---

[26] A Root user in a Linux operating system has access to all commands and files on the operating system.

[27] A "Digital Signature Algorithm" or "DSA" key is a digital key that uses a public and private key set that can be used to validate a user's identity when accessing secure locations online.

Chicago servers. While searching through Vaulin's tirm@me.com account I found an email from this same account to Vaulin on or about July 31, 2010. The subject of the email was "US Server" and stated: "Hello, here is access to the new server" followed by a private and public IP address located in Washington DC, along with the user name "root" and a password. The email also contained a list of additional IP addresses. I researched the IP address provided from the client to Vaulin and found that this IP was used to host the website solarmovie.com[28] from on or about August 13, 2010, through on or about April 10, 2011.

5. Vaulin's Use of Cryptoneat as a Front Company for KAT

67. According to Whois records, the website cryptoneat.com was registered on or about August 20, 2014, by Vaulin using tirm@me.com. As of on or about June 20, 2016, Vaulin's LinkedIn profile identifies him as the founder of Cryptoneat and lists the company's creation date as November 2009. The LinkedIn profile also lists his skills as Project Management, Strategic Planning, Management, and Customer Service, and that he speaks English, Ukrainian, and Russian. On Cryptoneat's Instagram and Facebook page I have viewed what pictures of Vaulin purportedly at Cryptoneat's office. Cryptoneat advertises that they have anywhere between 11 to 50 employees on its LinkedIn page. The only product advertised on its website is a mobile application for identifying, pairing, and rating wines.

[28] Solarmovie.com (now solarmovie.ph) is a website that is visually identical to KAT and which provides streaming links to movies and television series without authorization from copyright holders. As of on or about June 27, 2016, one on of the IP addresses hosting solarmovie.ph was one IP address away (185.47.10.11) from an IP address that was being used to host KAT (185.47.10.12 and 185.47.10.13).

68. Many of the employees found on LinkedIn who present themselves as working for Cryptoneat are the same employees who received assignments from Vaulin in the KAT alert emails, described above in ¶52. In particular, the following three individuals list Cryptoneat as their exclusive employer during the time they were carrying out tasks for KAT at Vaulin's direction, as follows:

Cryptoneat Employee	Position at Cryptoneat	Year Hired	Date Of Departure
Individual D	Lead Engineer	2008	Still Employed
Individual A	Software Development	2010	December 2014
Individual C	Lead Designer	2010	Still Employed

69. A historical job listing posted on Cryptoneat's website from in or around June 2015 reflected that Cryptoneat was seeking a "Frontend Developer." The job description stated the following:

> Cryptoneat is a product (non-outsourcing) startup developing an array of own products, high-load applications with more than 5 000 000 unique visitors, some of which are in Top-100 of Alexa's rating. The company was founded in 2008 by Ukrainian developers from Kharkov.
>
> We create a variety of solutions with different scope: media portals, search engines, market exchanges, mobile apps, etc.

70. This job listing matches KAT in a number of ways. First, it refers to "high-load applications with more than 5,000,000 unique visitors." Based on my training and experience, I know that the vast majority of websites do not have visitors as high as 5,000,000, a figure that KAT generally receives. Second, the job listing states that the websites it owns include "some . . . which are in Top-100 of

Alexa's rating," which also fits KAT's description.[29] Third, the Cryptoneat job listing states that the company was founded in 2008 by Ukrainian developers from Kharkov, which is about the time Vaulin, who is from Kharkov, registered several of the KAT websites.

71. The Cryptoneat employees I located through LinkedIn and Facebook include a number of job titles that, based on my training and experience, are consistent with the requirements necessary to run very large and heavy traffic-based websites like KAT, instead of a mobile web application for wine pairing, as Cryptoneat claims on its website. These and other facts indicate to me that Cryptoneat was founded and operated to run KAT at least in part, with the same employees that started KAT still working at Cryptoneat.

III. SEIZURE OF THE DOMAIN NAMES

A. Statutory Basis

72. Title 18, United States Code, Section 2323(a)(1)(B) provides, in relevant part, that any property used, or intended to be used, to commit or facilitate criminal infringement of a copyright is subject to both civil and criminal forfeiture to the United States government.

73. Title 18, United States Code, Section 2323(a)(2) provides that the procedures set forth in Chapter 46 of Title 18 (18 U.S.C. § 981, *et seq.*) shall extend to civil forfeitures under Section 2323(a). Title 18, United States Code, Section

[29] Note that many Top 100 Global Alexa websites are very well known companies or websites, such as cnn.com (ranked 95), ask.com (ranked 89), dropbox.com (ranked 82), alibaba.com (ranked 80), and craigslist.org (ranked 72) (all as of on or about June 24, 2016).

981(b)(1) authorizes seizure of property subject to civil forfeiture based upon a warrant supported by probable cause. Title 18, United States Code, Section 981(b)(3) permits the issuance of a seizure warrant by a judicial officer in any district in which a forfeiture action against the property may be filed and executed in any district in which the property is found.

B. The Subject Domains

74. There exists probable cause that the **Subject Domains** are property used or intended to be used to commit or facilitate violations of Title 17, United States Code, Sections 506(a)(1)(A) and 506(a)(1)(C), and Title 18, United States Code, Sections 2319(b)(1) and 2319(d)(2), all in violation of Title 18, United States Code, Section 371, and thus are subject to forfeiture pursuant to 18 U.S.C. § 2323(a)(1)(B). As discussed above and as reflected in the chart below, as of on or about July 7, 2016, **Subject Domain** 4 is the main KAT site; **Subject Domain 1**, **Subject Domain 4**, **Subject Domain 6**, and **Subject Domain** 7 were used as the main KAT site during the conspiracy (see above, ¶13) and currently redirect users to **Subject Domain 4**; **Subject Domain 3** and **Subject Domain 5** also host KAT[30]; and **Subject Domain 2** supports the visual and operational aspects of **Subject Domain 4** (see above, ¶36 and footnote 14). All of the **Subject Domains** were found in the logs on the Canadian servers reflecting that the Canadian servers were synchronizing updates for the **Subject Domains**. As described above

[30] These two domains rely on the same IP addresses and computer infrastructure as the main KAT domain (**Subject Domain 4**), so the content appears identical to the user.

in ¶36-37, all of the **Subject Domains** at some point used the KAT Chicago server as one of their name servers.

Domain	Registry	Description	Hosts or Redirects to kat.cr	KAT Canadian Server Logs
Subject Domain 1 kickasstorrents.com	Verisign	Main KAT site 11/08 to 4/11	X	X
Subject Domain 2 kastatic.com	Verisign	Supports kat.cr images		X
Subject Domain 3 thekat.tv	Verisign	Also currently hosts KAT	X	X
Subject Domain 4 kat.cr	Nir.cr	Main KAT site 5/15 to present	X	X
Subject Domain 5 kickass.cr	Nir.cr	Also currently hosts KAT	X	X
Subject Domain 6 kickass.to	Tonic Domains Corp.	Main KAT site 6/13 to 12/14 a 2/15 to 6/15		X
Subject Domain 7 kat.ph	PHRegistrar	Main KAT site 4/11 to 6/13	X	X

C. Seizure Procedure

75. As detailed in Attachment A, upon execution of the seizure warrants for **Subject Domains 1, 2, and 3**, Verisign, the registry for the ".com" and ".tv" top-level domains, shall be directed to restrain and lock the domains, pending transfer of all right, title, and interest in the domains to the United States upon completion of forfeiture proceedings, to ensure that changes to those domains cannot be made absent court order or, if forfeited to the United States, without prior consultation by HSI.

76. In addition, upon seizure of the **Subject Domains 1, 2, and 3** by HSI, Verisign will be directed to point those domains to a particular IP address, which

will display a web page notifying users, including the registrant, of the seizure of those domains.

77. The seizure warrants for the remaining **Subject Domains** will be sent through Mutual Legal Assistance Treaty requests to Costa Rica (for **Subjects Domains 4 and 5**), Tonga (for **Subject Domain 6**), and the Philippines (for **Subject Domain 7**) to seize and redirect the name server to an HSI-owned server.

IV. CONCLUSION

78. Based on the above information, I respectfully submit that there is probable cause to believe that Artem Vaulin, also known as "tirm," has committed the Subject Offenses, that there exists probable cause to believe the **Subject Account** contains proceeds obtained directly or indirectly as a result of the Subject Offenses, and that the **Subject Domains** constitute personal property used or intended to be used to commit or facilitate the Subject Offenses and are therefore subject to seizure.

FURTHER AFFIANT SAYETH NOT.

Jared Der-Yeghiayan
Special Agent
Homeland Security Investigations

Subscribed and sworn
before me on July 8, 2016

Honorable Jeffrey T. Gilbert
United States Magistrate Judge

ATTACHMENT A

I. Seizure Procedure

A. The seizure warrant will be presented in person or transmitted via facsimile or email or via a Mutual Legal Assistance Treaty request to personnel of the corresponding domain name registry listed in Section II ("Subject Registry"), for the Subject Domain names listed in Section II, for which it serves as the top-level domain registry, to make any changes necessary to restrain and lock the domain name pending transfer of all rights, title, and interest in the domains to the United States upon completion of forfeiture proceedings.

B. Upon seizure of the Subject Domains, the Subject Registry shall point the those domains to **ns1.seizedservers.com** and **ns2.seizedservers.com**, at which the Government will display a web page with the following notice:

> *THE DOMAIN NAME HAS BEEN SEIZED as part of a joint law enforcement operation by Homeland Security Investigations and the Internal Revenue Service in accordance with a court order obtained by the United States Attorney's Office for the Northern District of Illinois and the Department of Justice's Computer Crime and Intellectual Property Section issued pursuant to 18 U.S.C. §§ 981 and 2323 for conspiracy to commit copyright infringement by the United States District Court for the Northern District of Illinois*

C. Upon seizure of the Subject Domains, the Subject Registry shall take all steps necessary to restrain and lock the domain at the registry level to ensure that changes to the domains cannot be made absent a court order or, if forfeited to the United States government, without prior consultation with Homeland Security Investigation. The DNS record should be altered to remove any applicable name servers.

D. Upon seizure of the Subject Domains, the assigned registrars shall modify any records, databases, tables, or documents that are used by the registrars to identify the owner of the Subject Domains to reflect the seizure of the Subject Domains. These changes relate to the following records, if they exist:

1. The "Technical Contact" and "Administrative Contact" fields will reflect the following information:

   a) Name: U.S. Immigration and Customs Enforcement
   b) Address: National Intellectual Property Rights

		500 12th Street SW Washington, DC 20024
c)	Country:	USA
d)	Telephone:	1-866-IPR-2060 (477-2060)
e)	Email:	IPRCenter@dhs.gov
f)	Fax:	202-307-2127

2. Any remaining fields will be changed so they do not reflect any individual or entity.

E. The Subject Registry shall take any steps required to propagate the changes detailed in Section D to any applicable DNS servers.

II. Subject Domains and Subject Registries

Subject Domains	Subject Registry
kickasstorrents.com kastatic.com thekat.tv	Verisign, Inc. 21355 Ridgetop Circle Dulles, Virginia 20166
kat.cr kickass.cr	Nic.cr National Academy of Sciences Barrio Francisco Peraltla de Casa Italia 100 sur y 15 oesta San Jose, 4444, Heredia, Costa Rica
kickass.to	Tonic Domains Corp. PO Box 42, Pt San Quentin, California 94964
kat.ph	PHRegistrar.PH Web Services (Valley Journal Publishing) G/F ACSFI Bldg. 100P. Zamora St. Buag, Bambang, Nueva Vizcaya, 3702 Philippines