Virtual Forum Against Cybercrime

Newsletter

May
Issue: 11

Editorial VFAC

Another month has passed in what is becoming a very important year for the fight against cybercrime with industries and governments seemingly paying serious attention to the pertinent issues.

We would like to thank those that have been able to provide us with feedback on improving the VFAC project over the last month. We also will be contacting more of you to make sure that we gather as much information as possible.

A great thanks to Dr. El-Guindy for his article on the growing importance of 'Cyber' to national security and discussions of conflict. Cyberwarfare is an issue with near boundless complexities and we can only benefit from such informed analysis and the discussion that it promotes.

I would like to again encourage you to contribute to the newsletter by contacting me via email at *vfacybercrime@gmail.com*.

Recent Publication Article

Managing Identities

Managing Identities: From Government e-commerce to National Security

Dr. Philip Seltsikas

This paper is concerned with the challenges and issues facing US State and Federal government in attempting to develop, implement and maintain electronic identity management systems. Primary data was collected from four key stakeholders in two US States and from five key stakeholders at the US Federal government (two 'agencies').

A qualitative analysis identifies four dominant themes and a trend that is shifting government identity management efforts from supporting government e-commerce transactions to improving national security.

Central to this trend are key structural changes in the Federal management and budgeting of identity management initiatives. Projects that involved multi-million dollar investments in facilitating government e-commerce transactions appear to have lost momentum, putting those huge investments at risk. Furthermore, the research findings suggest that US government electronic identity implementers depend heavily on exogenous standards, with anecdotal evidence indicating that this may be a very risky approach.

Conferences, etc. Events

Black Hat USA 2012	United States	2012-07-21
British Society of Criminology Conference 2012: Criminology at the Borders	United Kingdom	2012-07-04
24th Annual FIRST Conference on Computer Security Incident Handling	Malta	2012-06-17
CoE Octopus Conference on Cooperation against Cybercrime	France	2012-06-06
IFIP SEC2012 Conference	Greece	2012-06-04
Fighting Cybercrime: Between Legislation and Concrete Action	Italy	2012-05-24
ERA Conference on Fighting Cybercrime: Between Legislation and Concrete Action	Italy	2012-05-24
ITEC Cyber Security Training and Education Workshop	United Kingdom	2012-05-23
IEEE Symposium on Security & Privacy	Afghanistan	2012-05-20
ASIACCS 2012: 7th ACM Symposium on Information, Computer and Communications Security	South Korea	2012-05-01

Virtual Forum Against Cybercrime

Issue: 11
May

News & Trends

News

[2012-04-23] The high profile case against Kim Dotcom, the founder of Megaupload, an online file sharing service, appears to be suffering more setbacks after the United States District Court Judge overseeing the case has apparently told the FBI that the case may never go to trial. Dotcom's U.S based lawyer stated that they, "...don't believe Megaupload can be served in a criminal matter because it is not located within the jurisdiction of the United States." Furthermore, the criminal copyright charges currently leveled against Mr. Dotcom only carry a maximum four year sentence, less than the five years required for extradition to the United States. The unbridled enthusiasm with which the authorities have pursued this case seems extraordinary given the complications of multiple jurisdictions and the expense involved. If the effort was intended to send the message through the press that they take content crime seriously it is in danger of backfiring.

China featured heavily in the news this month. MS Office Trojan files with malware intended for Mac Computers that seem designed for a targeted attack against pro-Tibetan activists were discovered [2012-04-03]. Other unusual activity such as the flooding of activist's twitter feeds and Pro-Tibet hash tags was also noted at the same time. China then became a subject of focus from Anonymous, the group defacing a large number of websites in the country with anti-government messages and links to pages detailing how to bypass state censorship [2012-04-05]. Another hacker claimed to have hacked a Chinese military contractor and released details of information that the company supposedly had on U.S. operations in Afghanistan and some allegedly shady deals, although the validity of the documents has been denied [2012-04-09]. Anonymous also announced their aim to bring down "the great firewall of China" but released no information on how they intended to do that [2012-04-12]. Philipp Winter and Stefan Lindskog of Karlstad University in Sweden revealed details on the Chinese systems for preventing the use of TOR networks, and methods that could be effective in countering these systems [2012-04-04]. It is not unlikely that Anonymous may be planning to utilize this research in their plans. It should be noted however, that quite a number of claims from Anonymous have never been realized.

As part of a newspaper's investigation of the police work involved in catching the "Craigslist Killer", the evidence provided to the police by Facebook was made publicly available [2012-04-01] and included as part of the story written by the paper. The report contained photos, partially redacted names and conversations from persons that were not part of the investigation, all of which is now in the public domain. According to the police involved, due to the amount of data provided by Facebook it is nearly impossible to release the document without providing details of others that are connected to them. Although Facebook has agreements with its users about the privacy of their data, the police do not and neither does the newspaper. This does raise questions on the practicalities of an SNS providing only information related to a specific person without compromising the privacy of all of that person's connections, and the responsibility for maintaining the privacy of those persons after the documents have been handed to Law Enforcement.

Twitter has filed lawsuits against five entities that sell tools to enable spamming on the Twitter network. Twitter put the cost of counteracting the spam generated by these agents at close to a million dollars [2012-04-09]. Pastebin has announced that it will hire staff for the express purpose of removing sensitive information put online at its site by hacktivists [2012-04-03].

Iran suffered a malware attack that seriously affected their oil production systems [2012-04-24]. Although they claim to be back online now, these attacks are another indication that serious campaigns are being waged in cyberspace that are having an impact on real world operations. While nations such as China and the U.S. now happily admit to joint cyber war games [2012-04-18], there have been no admissions of having put the lessons learned into practice.

Virtual Forum Against Cybercrime

Issue: 11
May

Submitted Article

Middle East: From Cold War to Cold Cyberwar

By Dr. Mohammed El-Guindy

Since history is a mirror to the future, we will take a look at the "Cold War" era and its effect on the Middle East in order to understand how a "Cold Cyberwar" would affect us sooner or later.

Cold War Era

There were two major players in the "Cold War" the U.S. (United States of America) and the former U.S.S.R. (Union of Soviet Socialist Republics). The U.S. led the western world and the Soviet Union led the communist world. The US and Soviet Union were staring each other down and kept their allied states from causing major wars, even when involved in localized military actions. Although the U.S. and the U.S.S.R. did not want to introduce nuclear weapons into the conflict, they changed the geopolitical map across the world.

The Cold War might be considered "Cold" between the U.S. and the U.S.S.R., but it was "hot" in other states because these two superpowers fuelled conflict through proxies in Africa, the Middle East, Asia, and Eastern Europe to further their ideologies and agendas. The region of the Middle East was an important battleground for the Cold War superpowers. It was affected by conflicts between the U.S. and the Soviet Union due to natural resources and oil in particular that shaped the new Middle East geopolitical map. For example, Egypt as the heart of the Middle East switched loyalty from the U.S.S.R. to the U.S. in the middle of the Cold War from the "Suez crisis to Camp David Accords" which could be considered the root of most political, economic, and religious conflicts in the Middle East.

The fall of Soviet Union officially ended the Cold War and left the world map with new borders, allied forces, new superpowers, and new phenomena such as the so called "War on Terror" to fabricate a new US enemy. Policymakers in the US may even consider the "War on Terror" as comparable to Cold War, but this doesn't seem to be correct.

Tension and the arms race between the U.S. and the U.S.S.R. during the Cold War era resulted in advancements in science and technology which later shaped the 2nd half of the 20th century and introduced the Space Race, Atomic Energy, Satellite technology, ICBMs, and finally the "Information Age".

Cyberspace Era

Cyberspace is widely considered the new battlefield in addition to Land, Sea, Air, and Space. Cyber warfare will not be mere science fiction due to cyber conflicts, cyber intelligence, digital espionage, cyber terrorism, and other related cyber-attacks. Although the move to the Internet has been a struggle for the global powers, the advantage always lies with those who take the offense.

A sign of the reality of Cyberwar is the infection of Iran's centrifuges in Natanz which was implanted by an Israeli proxy (an Iranian) via a memory stick, as said a former US intelligence official. I had stated before in one of my earlier reports that physical access is needed to infect the SCADA systems in Iranian nuclear facility and that would not be possible without double agent.

Richard A. Clarke, in his book "Cyberwar: The Next Threat to National Security and What to Do about It"(2010), he talks about the new weaponry of war. Wars used to be waged with steel, then firearms, and eventually nuclear weapons. Today's new stealth weapons include hackers, bots, denial of service attacks and censorship policies.

Many governments around the world have started to realize the importance of cyberspace and tried to control it and utilize it in many ways ranging from open source intelligence to surveillance. Let's see how the major players are dealing with cyberspace.

In 2010 the Government of the United Kingdom (U.K.) considered threats from cyberspace a tier one priority as a genuine threat to national security. In the Strategic Defence and Security Review publication they stated that "The Government will introduce a transformative national cyber security programme to close the gap between the requirements of a modern digital economy and the rapidly growing risks associated with cyber space. The National Cyber Security Programme will be supported by £650 million of new investment over the next four years, working to one national programme of activity with supporting strategies in other departments".

Virtual Forum Against Cybercrime

Issue: 11
May

Submitted Article

The government of France stated that cyberspace is one of its areas of sovereignty as published in its Strategy document. A plan for Open Source Spying for French Military Strategy has also been leaked.

In January 2012, the United States announced in a U.S. military document that they intended to treat cyberspace as a military battleground. The U.S. government may launch missiles and start military actions if they are attacked in cyberspace. Israel has also made a statement to this effect.

Israel is also very active in cyberspace and has special Cyberwarfare capabilities. They are preparing their own “Cyber Defenders” unit or (C4I i.e. command, control, communications, computers and intelligence) which is part of the Israeli Defence Force (IDF).

China is one of the big players in cyberspace weaponry, as has been stated by many sources and documented by evidence. “In today’s information age, the People’s Republic of China has replaced and even improved upon KGB methods of industrial espionage to the point that the People’s Republic of China now presents one of the most capable threats to U.S. technology leadership and by extension its national security”, stated Dan Verton, Cyber warfare Expert.

One of the latest congressional reports revealed that “Chinese capabilities in computer network operations have advanced sufficiently to pose genuine risk to U.S. military operations in the event of a conflict”. An interesting story published by the Guardian newspaper claims that the U.S. Departments of Defense and State, along with their Chinese counterparts, held two secret Cyberwar games last year that “were designed to help prevent a sudden military escalation between the sides if either felt they were being targeted.” The Guardian says that another is planned for this May.

Finally, senior security figures have confirmed that Chinese spies hacked into computers belonging to BAE systems, Britain’s biggest defense company, to steal details about the design, performance, and electronic systems of the West’s latest fighter jet. Related video by NTDTV was published on the Internet.

The rising controversy over Chinese tech giant Huawei and their linkage to surveillance, espionage, and military ties has allowed the politicization of the issue and politicians have been able to ban the company from government contracts in the U.S., Australia, and the U.K.

While both the United States and China have all the required advanced technology in place to start a Cyberwar, they will not use their destructive capabilities as it could have impact on both sides. This situation is the same as it was between the U.S. and the Soviet Union in the Cold War era. I believe that the U.S. and China will start to build their own allies and share cyber security expertise. One obvious example is the alliance of “Russia, China, North Korea, and Iran” vs. “The U.S., NATO, and Israel”. Additional nation states such as Pakistan, India, and Bangladesh are also moving forward to enter the Cyberwarfare era.

In the Middle East there are no countries with Cyberwarfare capabilities except Iran which invests heavily in its offensive and defensive capabilities in cyberspace. News has also surfaced that reported Iran’s use of its Cyber warfare capabilities to down a U.S. stealth drone.

Although there are many cyber attacks that have originated from within Middle Eastern countries especially during Arab uprising, these should not be categorized as Cyberwar actions. These cyber attacks are considered “Hacktivism” rather than Cyberwarfare.

While the world is gearing up for Cyberwar and preparing for cyber conflict in the 21st century, Middle Eastern countries are still struggling with Cybercrime legislation, cyber criminals, freedom of speech and information, mainstream media, and other globalization issues.

History lessons tell us that not only was the Soviet Union the loser of the Cold War, but also that Middle Eastern countries have been the losers in the post Cold War era and in the age of globalization. MENA Countries allied with the Soviet Union or the U.S. have lost control over their resources through new re-colonization methods.

Instead of military actions, today’s superpowers will write malicious codes!

This article was adapted from an article published at the author’s blog at: http://netsafe.me/2012/04/21/middle-east-from-cold-war-to-cold-cyberwar/

Dr El Guindy is a well-known Cybercrime Expert in the Middle East and works as a consultant for national and international organizations and the president of the ISSA (Egypt chapter).

Virtual Forum Against Cybercrime
Issue: 11
May

Submitted Article

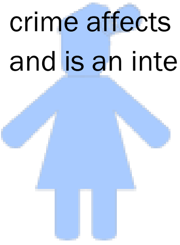
Video Chat Extortion and Sexual Abuse

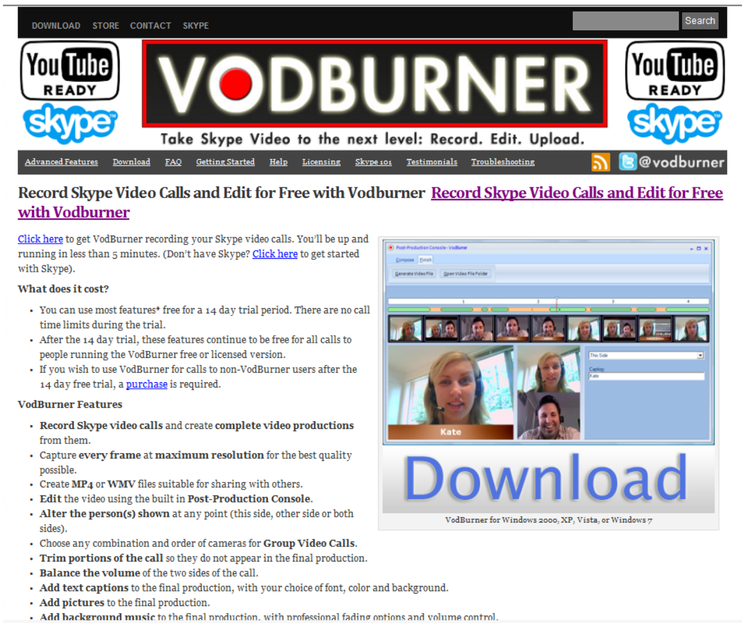
By Michael Joyce

Korean Institute of Criminology

The proliferation of multimedia technology and the growth of Social Networking Services have brought us to an era of unprecedented connectivity. The spread of laptops and other devices such as smart phones have allowed a great number to connect with video and audio over the Internet. Social Networking Services such as Facebook and Google+ with their large user bases and their simple systems for connection have made it easier to connect with people around the globe. It is now possible to be reunited with an old friend in a distant nation, and chat with them face to face, in real time. Unfortunately, the connections that are facilitated are not always healthy, and the video chat technology can be subverted. The prevalence of these systems has made them attractive to fraudsters and deviants as a tool for fraudulently extorting money and abusing Internet users worldwide. These services are used for in a form of romance or dating scam that, rather than integrating elements of advance fee fraud is instead combined with grooming, extortion, cyber harassment and sexual abuse.

The number of victims of web cam extortion is very difficult to quantify as there is a great reluctance of victims to report the crime. However, police investigations around the world have revealed that this crime has already claimed a great number of victims. In a single case in the United States of America an attorney involved with the matter stated that he was worried that a single perpetrator had victimized hundreds. An investigation in Singapore earlier this year found a group had extorted more than $100,000 from individuals via web cam extortion. Even from just these two accounts, it is easily recognizable that this form of crime affects many people, involves large sums of money and is an international problem.





Take Skype Video to the next level: Record. Edit. Upload.

Record Skype Video Calls and Edit for Free with Vodburner Record Skype Video Calls and Edit for Free with Vodburner

Click here to get VodBurner recording your Skype video calls. You'll be up and running in less than 5 minutes. (Don't have Skype? Click here to get started with Skype).

What does it cost?

- You can use most features* free for a 14 day trial period. There are no call time limits during the trial.
- After the 14 day trial, these features continue to be free for all calls to people running the VodBurner free or licensed version.
- If you wish to use VodBurner for calls to non-VodBurner users after the 14 day free trial, a purchase is required.

VodBurner Features

- **Record Skype video calls** and create **complete video productions** from them.
- Capture **every frame** at **maximum resolution** for the best quality possible.
- Create **MP4** or **WMV** files suitable for sharing with others.
- **Edit** the video using the built in **Post-Production Console**.
- **Alter the person(s) shown** at any point (this side, other side or both sides).
- Choose any combination and order of cameras for **Group Video Calls**.
- **Trim portions of the call** so they do not appear in the final production.
- **Balance the volume** of the two sides of the call.
- **Add text captions** to the final production, with your choice of font, color and background.
- **Add pictures** to the final production.
- **Add background music** to the final production, with professional fading options and volume control.

VodBurner for Windows 2000, XP, Vista, or Windows 7

Software for recording Video Chat is freely available online

A Methodology of Webcam Extortion

Analysis of victim reports from online support forums and news reports has shown a common methodology utilized in the commission of these scams.

The scammer first will locate a potential victim using a public online chat service such as Lycos or UKChatterbox, through chat-roulette or by friending on Facebook. After a relationship has been established and the scammer believes that the individual is vulnerable the potential victim is invited to chat via a real-time communication service with video capability such as the Microsoft's Instant Messenger Service or Skype.

It is likely that during these conversations the scammer will attempt to extract information from the victim to locate and possibly compromise the victim's online Social Networking Service accounts and/or email accounts. By social engineering the scammer may elicit responses that allows the deduction of passwords, or answers to security questions, allowing easy access to those accounts and the details therein.

Once connected in a video chat the scammer proposes cybersex to the victim and may expose themself and/or perform provocative acts and actively encourage the victim to do the same. There have been some reports that the scammer may have presented pre-recorded video, possibly

Submitted Article

of other victims or an avatar through dynamic compositions of video clips, to give the impression of a real person interacting with the victim. It is assumed that this is not commonplace and the scammer does generally interact with the victim directly.

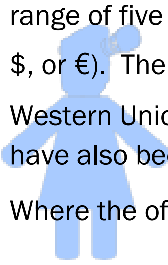
If the victim does reciprocate then the scammer records the actions of the victim. Software that allows the recording of video chats is freely available online, even if the chat program does not natively support the function. The fraudster having gotten the compromising video needed, will then generally terminate the conversation.

The scammer then uploads an “undignified” video clip of the victim from the chat session to an online video hosting service such as YouTube or to a pornography hosting service that allows user submissions.

The scammer then contacts the victim and sends them a link to the video that they have uploaded. The scammer may name the video using the victim’s name, inflammatory phrases (e.g. pedophile etc.) and other information about the victim, such as place of work, age, etc.   This is done to increase the potential for the video to be returned on a search for the victim, to increase the risk and hence the fear of discovery.

The victim at this stage is presented with a list of Facebook friends or email contacts to which the scammer threatens to send a link of the video, if a payment is not made.   The fraudster may alternatively threaten the victim that the person that they interacted with was under the age of consent, making the chat session illegal and that the video will be sent to the police if payment is not made. This tactic possibly used in cases where the victim seems unwilling, or sufficient information on the victim’s associates was unavailable.

Initial payment demands that have been reported online are generally between $USD 300~1000, generally in the range of five hundred of the victim’s local currency (e.g. £, $, or €). The preferred method of payment appears to be Western Union, but cases where Paypal has been used have also been reported.



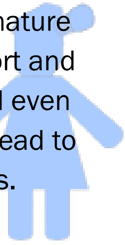
Where the offender is not financially motivated it is likely that the demand is for the victim to create other videos, often requesting that the victim perform particular and more degrading acts. If the victim capitulates and a transaction is made successfully, repeat attempts are made to extract more money or video content from the victim.

Victim Suffering

The damages to the victims are more than the financial loss. The victim also suffers emotional distress at the violation of their personal life and the fear of public exposure. The speed, availability and “always on” nature of the internet creates additional fear as they feel that their personal details could be exposed to any number of known or unknown people at any time.

The intrusion into and potential exposure of their private life can leave a victim with self-conscious emotions including a sense of shame as well as guilt for not having avoided the situation and fear about the possible repercussions. The experience is often highly traumatic for the victim and may cause sleep deprivation, stress, impede cognitive and emotional functioning and hamper personal relationships. The victim could be seriously affected by the event for some time after it happens and suffer from symptoms of Post-Traumatic Stress. Counseling may be required for people to return to a normal state of functioning after becoming a victim to this form of crime.

In cases where the victim is able to respond positively they may seek help by contacting the police or other authority figure or seek advice or examples from an expert source such as support forums online. Due to the sexual nature of this form of offense the provision of social support and counseling to victims would be beneficial and could even be crucial for their health. This form of abuse has lead to victim suicide and should be treated as very serious.



Victims Support

Information and Counseling

There are a number of websites online that can provide support and information to victims such as www.haltabuse.org. These services provide information for victims to help them understand the crime, appropriate actions that they can take, access support groups and find

Virtual Forum Against Cybercrime Issue: 11 May

Submitted Article

counseling through online services and local law enforcement services. Government services on fraud such as the www.scamwatch.gov.au website by the Australian government provide a good source of information on a number of scam types, including grooming and relationship/dating scams at a reputable source as well as a mechanism for reporting crimes to the police.

Removal of Content

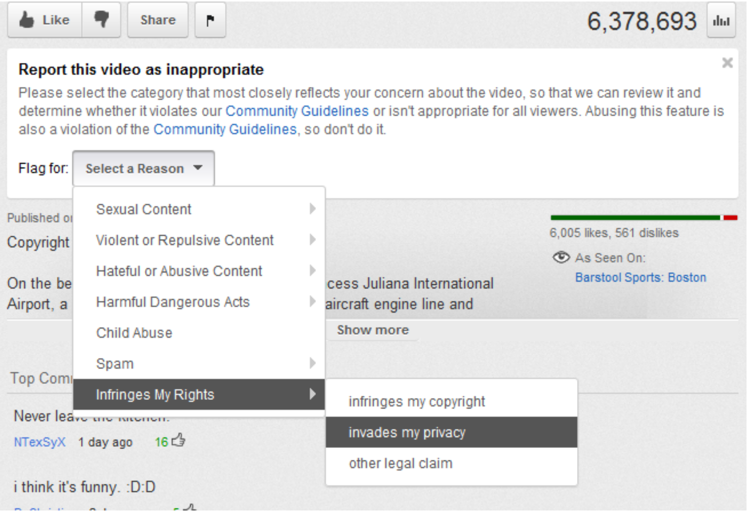
Preventing the distribution of the video content is more difficult as there are a large number of systems available to put the content online. This makes it difficult for victims to locate any videos that may have been uploaded. However, the observed behavior is to use a service that is designed for users to upload and distribute video content rather than distributing the content through peer to peer or email systems. This is most likely because of the ease and relative anonymity with which these services allow for the sharing and viewing of video content.

Where the fraudster uploads videos using specific information about the victim in naming the content it may be easier to locate. However, there is no guarantee that they will, and if they do they may not follow any naming convention, or even spell the victim's name correctly.

Anonymous commentary from victims has been that it is generally not difficult to have the material uploaded by criminals removed by these sites once located. A review of popular video sharing sites, including those mentioned by victims, reveals that the clarity of the required processes and the efforts of websites to facilitate the removal of content by victims vary.

Dailymotion could be considered a clear leader in its efforts to assist victims and prevent the misuse of its services in this manner. The website has a page dedicated to explaining the kind of content that is not permitted on its site and explains three different methods of notification on this page. One of the methods is a form that is accessible by clicking on a red flag icon on the video display page.

YouTube offers a Safety Center which provides advice about a variety of issues that users may encounter during the use of their services. There is however no advice relating to this specific type of problem. YouTube does provide a tool for flagging inappropriate content which does provide an option that is obviously appropriate to this form of abuse. It does however, require users to be logged in with either a Google or YouTube account which creates additional complications for those do not have an account of this type.



Report this video as inappropriate

Please select the category that most closely reflects your concern about the video, so that we can review it and determine whether it violates our Community Guidelines or isn't appropriate for all viewers. Abusing this feature is also a violation of the Community Guidelines, so don't do it.

Flag for: Select a Reason

YouTube's On-page Reporting System

Facebook does have systems in place to allow for the reporting of content. The systems do not seem to have been designed with this abuse of their system in mind and presents information that is confusing, which may be difficult for a victim of this form of crime to identify with. If the user follows the help articles that appear appropriate to this particular situation, they are presented with information that advises them to "talk to the person who posted it". Other help pages dealing with abuse offer assistance with reporting content for removal but there is no link between this page and that information. The reporting tools that Facebook provides are not intuitive and do not follow the more generally used 'red flag' icon format for the reporting of content. When reporting content, the user is required to choose between the issue being personal or the content containing nudity, and the option for the content being both is not available.

Vimeo has no clear information on how one may complain about or flag a video uploaded by another user for removal. Uploading a video of the type used in this form of fraud

Submitted Article

contradicts the terms of service but the method of lodging a complaint is not clear.

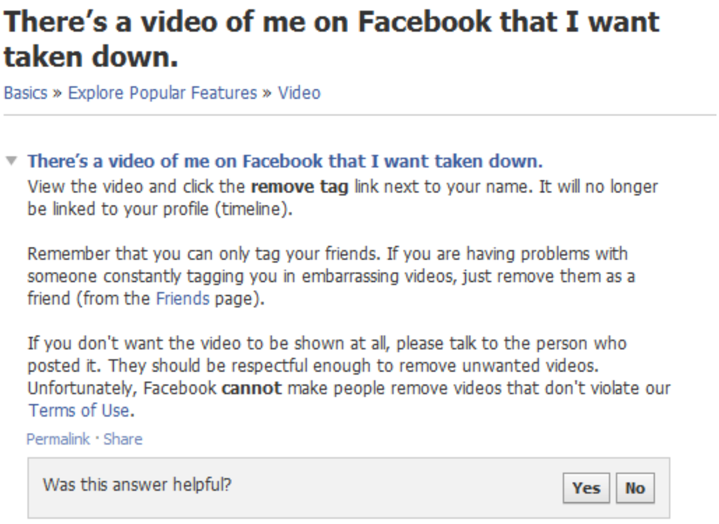
A site that was specifically mentioned as being utilized in this form is a pornography website that allows for users to upload content. Although the terms and conditions state that this type of content is not to be uploaded and a system for reporting content similar to YouTube and Dailymotion is provided. The website provides a form and information about making complaints, but the effort appears to be on copyright infringement rather than privacy infringements. There is no clear assistance or processes available to victims of this form of fraud. This is not to state that online pornography websites are indirectly complicit in this form of fraud. To the contrary, online reports from victims have stated that websites of this type can be very willing to remove content in an expeditious manner. The lack of clear processes or assistance in reporting content creates unnecessary difficulties for victims who wish to have content removed.

Unfortunately if the videos are included in a search engine index it does take time for the link to be removed and the content or some part thereof may remain cached for a longer period of time. Google does provide a system for registering for content to be removed from the search engine and cache results but these do require a user to have a Google account.

It is understandable that service providers are reluctant to increase the ease with which the public can have content uploaded by other members of the public removed from their systems. If the systems are not carefully moderated it could be utilized as a method of harassing users (by having all of their content removed) rather than a tool for preventing harassment. However, it does appear that there is some room for improvement in terms of presenting information and processes to victims of this form of crime in a way that is appropriate, reassuring and also provides advice on how to contact law enforcement or locate other support services.

Recommendations

Unfortunately the nature of the crime reduces the likelihood that crimes are reported, making it difficult to confidently state the extent of the problem or the success of any efforts to deal with the crime. Nonetheless this is an issue that should be of great concern to the online community as it creates great harm. Victims are at risk of not only financial loss but also the suffering caused by the sexual and intrusive nature of the crime. As the level of technology and the availability of broadband increases worldwide, so does the number of potential victims of this form of crime if it is not counteracted effectively. The “consumerisation” of techniques that were previously limited to skilled hackers, such as tools to easily identify the IP address and physical location of a Skype user, increases the possible harm and reduces the technical barriers to this form of criminal activity. The damage done by this kind of fraud and abuse is severe, and could get worse in the future.



There's a video of me on Facebook that I want taken down.

Basics » Explore Popular Features » Video

▼ There's a video of me on Facebook that I want taken down.

View the video and click the **remove tag** link next to your name. It will no longer be linked to your profile (timeline).

Remember that you can only tag your friends. If you are having problems with someone constantly tagging you in embarrassing videos, just remove them as a friend (from the Friends page).

If you don't want the video to be shown at all, please talk to the person who posted it. They should be respectful enough to remove unwanted videos. Unfortunately, Facebook **cannot** make people remove videos that don't violate our Terms of Use.

Part of Facebook's F.A.Q. that could be improved

To reduce the potential harm from this form of crime we would welcome greater education about the risk of video chatting online. Many users are unaware that online chats can be recorded, or that this form of fraud exists. Awareness of this form of fraud will reduce the likelihood that persons will be convinced to expose themselves or perform personal acts in view of their computers web cam. Although many law enforcement agencies are well equipped to deal with this form of fraud and abuse, by ensuring that law enforcement services internationally are aware of this form of crime, the appropriate investigation methodologies and the needs of the victim, the effectiveness of the re-

Virtual Forum Against Cybercrime

Issue: 11 May

sponses will be increased.

The private sector has responded generally well to developing systems to deal with online abuse such as the adoption of self-regulation principles like the EU Safer Social Networking Principles. This form of fraud and abuse does not appear to have been specifically included in the design of their abuse handling systems. The creation of use specific tools for victims of this form of fraud could create benefit in easing the suffering of victims by providing reassuring and appropriate information, streamlining the removal of infringing content and providing links to reputable sources of information and counseling.

Through the concerted and concentrated effort of both public and private organizations a reduction in the pool of potential victims and harm caused, as well as an increase in the apprehension of offenders could be achieved.

Michael Joyce is the moderator of the Virtual Forum Against Cybercrime and a researcher in the Korean Institute of Criminology's Cybercrime Research Unit.

The author would like to acknowledge the helpful advice of Dr. Jeong Sook Yoon from the Korean Institute of Criminology regarding the impact of this form of crime on victims.

Reference information and further reading:

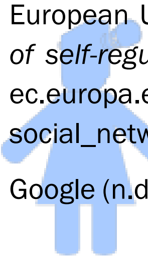
Dailymotion (n.d.) Legal Prohibited Content, retrieved March 2, 2012 from :

http://www.dailymotion.com/legal/prohibited

Dailymotion (n.d.) Frequently Asked Questions Topic: Report abuse, Retrieved March 2, 2012 from:

http://www.dailymotion.com/faq#report_abuse

Donery, J(2012, May 1) *Skype flaw allows for collection of user IP addresses*, retrieved from http://www.v3.co.uk/v3-uk/news/2171809/skype-flaw-allows-collection-user-ip-addresses



European Union (n.d.) *Safer social networking: the choice of self-regulation,* retrieved March 2, 2012 from : http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm

Google (n.d.) *YouTube Help Safety Center*, retrieved April 26 2012 from:

https://support.google.com/youtube/bin/request.py?&contact_type=abuse

Facebook (n.d.) *How to Report Abuse*, retrieved March 2, 2012 from: https://www.facebook.com/help/reportlinks

Facebook (n.d.) *There's a video of me on Facebook that I want taken down,* retrieved March 2, 2012 from: https://www.facebook.com/help/?faq=111977535557635#There's-a-video-of-me-on-Facebook-that-I-want-taken-down.

Facebook (n.d.) *Video Uploading and Viewing Video*, retrieved March 2, 2012 from:

https://www.facebook.com/help/videos/uploading

Fong, K (2012, 29 February) '*Internet Love Scam' ring busted*, retrieved from:

http://sg.news.yahoo.com/blogs/singaporescene/internet-love-scam-ring-busted-163710105.html

(n.d.) *Webcam 'sex' Scams & Blackmail Attempts* Internet Love Scams.org retrieved April 25, 2012 from: http://www.internet-love-scams.org/forums/forumdisplay.php?s=eaf29ada557083ef9ecff8e836035b5e&f=41

Tracy, Joe (2012, February 23) *URGENT: Romance Scammers Now Using Fake Webcam Footage to Deceive Victims* retrieved from: http://www.onlinedatingmagazine.com/datingnews/fakewebcamfootage.html

Mulvihill, Geoff, (2012, 17 March) *US Student guilty in webcam suicide case*, retrieved from: http://www.stuff.co.nz/world/americas/6593321/US-student-guilty-in-webcam-suicide-case

Wilson, C (2012, 11 April) *Indiana Man charged with Sexual Exploitation*, retrieved from: http://www.nbcwashington.com/news/local/Indiana-Man-Charged-With-Child-Sexual-Exploitation-146925075.html

http://www.scamwatch.gov.au/

Vimeo (n.d.) Terms of Service, Retrieved March 2, 2012 from: http://vimeo.com/terms

www.haltabuse.org

http://www.romancescams.org/Blackmail.html