AGORA International Journal of Administration Sciences,
http://univagora.ro/jour/index.php/aijas
ISSN 2359-800X
No. 1 (2017), pp. 7-13

SEXTORTION – THE NEWEST ONLINE THREAT

I.V. Humelnicu

Ioana Veronica Humelnicu
European Security Specialist
Social Media/ Awareness Specialist - N.G.O. Abolishion
*Correspondence: Ioana Veronica Humelnicu, Asociația Abolishion, Oradea, 36 Republicii St.
E-mail: ioana.humelnicu@abolishion.org

Abstract

Sextortion is a wide-ranging problem and not isolated to one website or app. Perpetrators used many forms of technology to reach victims and 45% of victims reported contact with perpetrators on more than one platform. With connectivity on the rise, sextortion could be an increasingly pervasive threat.

Key Words

Sextortion, social media, blackmail, sexual exploitation, human trafficking

Introduction

In a constant developing world, the techniques used by traffickers are constantly being updated, finding new ways and new methods of exploitation. Now human trafficking is not limited by geography anymore, but spread out over the borders of national states though the powerful yet dangerous platform which is the online.

In this perfect context, a new online threat is born – sextortion – a cybercrime which can be seen as a new form of sexual abuse.

Definition

Sextortion – is a form of sexual exploitation through blackmail in which an individual threatens that he or she will publish pictures of a person with sexual content if the person concerned does not fulfil a list of requirements. Traffickers may obtain those images by various means. They can access an unauthorized storage device of such data or save an image without the consent of the blackmailed person.

In some cases, the image can be sent by victims even unknowingly. Regardless of how the image was obtained, if it was distributed without the consent of the person in the picture, we're talking about an act of abuse with intimate images that traffickers use to exploit the victim. [1]Other reasons for sextortion are revenge or humiliation

"It's a new form of sexual assault because you can do it without being in the person's presence - and you can do it at scale," said Senior Fellow Benjamin Wittes.[2]

The techniques

The techniques used by the criminals are very efficient.

The criminals create fake accounts on online platforms, using the vast world of social media networks and online gaming. Their identities are created depending on the context and the target. Then they contact the victim and start an online grooming process. They earn their

[1] https://www.wearethorn.org/child-sexual-exploitation-and-technology/, accessed today 18.11.2015.
[2] http://money.cnn.com/2016/05/11/technology/brookings-institution-sextortion-study/ accessed today 29.11.2016

trust step by step, building a virtual relationship with the victim and at some point, they will obtain sexually compromising materials with the victim. Then the next step is sextortion. The criminals will blackmail the victim, threatening them, saying that they will publish this online if they don't pay a certain amount of money or if they refuse to send more sexual materials.

Social media and text messages are often the source of the sexual material and the threatened means of sharing it with others. An example of this type of sextortion is where people are extorted with a nude image of themselves they shared on the Internet through sexting. They are later coerced into performing sexual acts with the person doing the extorting or are coerced into posing or performing sexually on camera, thus producing hardcore pornography.[3]

Another method used for acquiring material for sextortion is hacking.

In 45% of cases, perpetrators acquired sexual images of respondents without their knowledge or consent.[4]

The criminal is breaking the computer's security network through different methods like installing a malware program on the victim's computer. In many cases the criminal persuades the victims to install a program which it turns out to be a Trojan horse. This Trojan horse will install a malware in the computer without the victim's knowledge. After that the criminal will gain access to the personal files on that computer, like photos, video, contacts and important details about the victim. More than this, the criminal can access the victim's webcam and can record, take photos and film the victim without them ever being aware of this. The criminal will gather materials and will start blackmailing the victim.

In other cases, the criminals used other ways to acquire materials such as:

• Recorded webcam sessions without respondent's knowledge or consent (18% of all respondents)

• Recorded images other ways without the respondent's knowledge or consent (12%)

Perpetrators also acquired images from other people, including other people voluntarily sharing the images with the perpetrators or perpetrators taking them illicitly from other peoples' cell phones (9%); created fake or Photo-shopped images (8%); or hacked into devices or online accounts to get images (5%).[5]

Who are the victims:

The main target category when it comes to sextortion are minors because they are easily manipulated

- "71% of the cases involve only victims under the age of 18
- 14% of the cases involve a mix of minor and adult victims
- 12% of the cases involve only adults."

Nearly all adult victims are female, but both minor girls and boys are victimized.[6]

- "78 % of the incidents involved female children
- 12 % involved male children
- In 10 % of incidents, child gender could not be determined
- The average age at the time of the incident was approximately 15 years old, despite a wider age-range for female children (8-17 years old) compared to male children (11-17 years old);"[7]

"Results of the 2016 National Strategy survey indicate that sextortion is by far the most significantly growing threat to children, with more than 60% of survey respondents indicating this type of online enticement of minors was increasing."[8]

[3] https://en.wikipedia.org/wiki/Sextortion accessed today 28.11.2016

[4] Janis Wolak, David Finkelhor, *Sextortion - Findings from an online survey about threats to expose sexual images*, Crimes Against Children Research Centre, University of New Hampshire, p. 19

[5] *Ibidem*

[6] http://www.brookings.edu/research/reports2/2016/05/sextortion-wittes-poplin-jurecic-spera

[7] Benjamin Wittes, Cody Poplin, Quinta Jurecic & Clara Spera, *Sextortion: Cybersecurity, teenagers, and remote sexual assault*, Center for Technology Innovation at Brookings, page 8

How are the victims recruited?

- 42% of sextortion victims met their perpetrators online.[9]
- Social Media manipulation is used in 91% of cases involving minor victims
- Computer hacking is used in 43% of cases involving adults.[10]

Recruiters are very well organized when it comes to getting images with the victim. They will study carefully the victims profile on different social media platforms and learn everything they can about the victim.

"Within a couple of quick clicks, you can find out a lot of information about someone."

[…] a variety of manipulation tactics are used by sexual predators. They will develop bonds with kids through flattery ("You're so pretty" or "You're so hot"). Girls are often a target for sextortion, but […] boys are victimized, as well.[11]

Where does it happen?

Sextortion most commonly occurred via phone/tablet messaging apps, social networking sites and video chats. [12]

- 54% on social networking platforms (Facebook, Tagged, Instagram, others)
- 41% on messaging or photo messaging platforms (Kik, Snapchat, others)
- 23% on video voice call programs (Facetime, Skype, webcam sites, others)
- 12% on email
- 9% on dating platforms (OKCupid, Tinder, others)
- 6% on video sharing social media platforms (Vine, Oovoo, Tumblr, others)
- 4% on gaming platforms
- 8% Missing data [13]

An example of this form of exploitation and where it happens are on online games. The teenager starts playing a game online, networking with thousands of users worldwide. At one point, he needs money online to pass to the next level. One of the users offers to help him with the money in return for provocative pictures of him. After the teenager sends the image, the user is proving to be a trafficker and blackmails him with the sent picture. The trafficker threatens that he will send the picture to the parents and will publish it online if the victim does not do what he says.

Why?

The reasons why the criminals use sextortion vary and depends from case to case, but the most common objectives are these:

76% - To acquire additional, and often increasingly more explicit, sexual content (photos/videos) of the child

6% - To obtain money from the child

6% - To have sex with the child

12% - the objective could not be determined [14]

Being an online danger, this phenomenon is not limited geographically. It's not necessary for the criminal to be physically present to recruit his victims. This is the reason why sextortion has such a high risk and gravity. The market for the victims is huge and is not limited by geographic boundaries.

---

[8] National Strategy on Child Exploitation Prevention and Interdiction, US Departmen[t of Justice, April 2016, p. 75

[9] https://www.wearethorn.org/child-pornography-and-abuse-statistics/

[10] http://www.brookings.edu/research/reports2/2016/05/sextortion-wittes-poplin-jurecic-spera, p. 8

[11] http://www.beakidshero.com/posts/newest-form-child-exploitation-sextortion/ accessed today 29.11.2016

[12] http://www.missingkids.org/Sextortion accessed today 29.11.2016

[13] https://www.wearethorn.org/sextortion/ accessed today 29.11.2016

[14] http://www.brookings.edu/research/reports2/2016/05/sextortion-wittes-poplin-jurecic-spera

"The sextortion schemes we uncovered are complex operations that involve people across cultures and nations working together to effectively run a very lucrative business," the report says. "These once again prove that cybercriminals are not just becoming more technologically advanced— creating stealthier mobile data stealers, using complex stolen data drop zone infrastructures, and outsmarting banks to better evade detection—they are also improving their social engineering tactics, specifically targeting those who would be most vulnerable because of their culture." [15]

Once the object of blackmail is posted online, it can be accessed by millions of users from all over the world through the internet.

Online social platforms, chats and video chats are the perfect locations for this activity to take place.

More than this, these exploitation techniques evolve constantly and the mobile phones and tablets are the perfect tool used by criminals to commit these kinds of abuse.

Technology

Sextortion is a wide-ranging problem and not isolated to one website or app. Perpetrators used many forms of technology to reach victims and 45% of victims reported contact with perpetrators on more than one platform. With connectivity on the rise, sextortion could be an increasingly pervasive threat.[16]

There are numerous mobile applications that facilitate targeting, online grooming and recruitment of the victims and after that their coercion to get involved in sexual activities.

In many cases the criminals move the conversations from a platform to another one to avoid being detected. They might start a conversion on a certain social network and then after a while they will move the conversation on a video chat platform or on mobile phone using anonymous and dubious messaging apps. The criminals might use different reasons, like audio problems, to persuade the victim to download and install certain apps that would solve the problem. Once installed, these apps contain viruses/malware which will steal the victim's personal information, like contacts, photo, videos and data that will be used to blackmail the victim.

Sexting

Sexting refers to sending erotic text messages, photos and movies using the cell phone.

We must make a clear distinction between sextortion and sexting. Sexting is an action that takes place with the consent of all parties involved in the communication while sextortion doesn't have the consent.

Percent of teens who have sent or posted nude or semi-nude photos or videos of themselves:

- 20% of teens overall
- 22% of teen girls
- 18% of teen boys
- 11% of young teen girls between the ages 13-16
- 15% of teens who have sent or posted nude/semi-nude images of themselves say they have done so to someone they only knew online.

51% of teen girls say pressure from a guy is a reason girls send sexy messages or images

12% of teen girls felt "pressured" to send sexually suggestive messages or images.

[15] http://www.networkworld.com/article/2900829/security0/mobile-sextortion-schemes-on-rise-trend-micro-reports.html

[16] https://www.wearethorn.org/sextortion/ accessed today 29.11.2016

1 in 10 sext senders say they have sent these messages to people they don't even know.[17]

Sexting is the method that facilitates sextortion

These are just some of the methods and techniques used by traffickers to recruit victims. And after recruiting them, they end up being sold online as an object, again and again and again. „*People are posted and sold online several times a day, says Asia, a survivor of sex trafficking. As the announcement posted with me ... it's like looking for a car online ... I had a picture, a description and a price."*[18]

Effects

Sextortion has serious negative effects on the victims and some of the consequences are tragic. Victims of sextortion suffer from a strong emotional and sexual abuse.

„Victims confessed that they felt trapped in a form of sexual slavery and lived in a constant state of anxiety, fear and helplessness. One of the victims testified that she felt hollow inside and an FBI agent involved in the study said that sextortion can have devastating emotional effects."[19]

Beside these immediate effects, the victims can suffer depression, dropping out of school, low performance in school, can inflict self-harm and in extreme cases they can even commit suicide.

Law

Because this phenomenon is new, sextortion is not regulated as a crime.

In terms of the Criminal Code of Romania20, in accordance with Chapter I - *Offences against public order and peace* in art.374, offenses and penalties are specified with general aspects as well as penalties regarding *child pornography.*

"Brock Nicholson, head of Homeland Security Investigations in Atlanta, Georgia, recently said of online sextortion, "Predators used to stalk playgrounds. This is the new playground."[21]

How to avoid being sextorted

1. Never send compromising materials (photos/videos/recordings) of yourself to anyone.
2. Turn off your computer when you are not using it.
3. Cover your webcam when you are not using it or any other camera connected to the internet.
4. Make sure you have an up to date anti-virus software.
5. Don't download any programs or apps from people you don't know.
6. Don't open attachments from people you don't know.
7. Watch out for messages from strangers via email or social networking sites and never click on the links form those messages.
8. Don't accept friend request from people you don't know. Fake profiles are easy to create.
9. Don't interact with strangers requesting a video call or cybersex.

What to do if being sextorted

1. Talk about what happened – It's important to understand that you are a victim in this case and that the criminals rely on your silence to continue their abuse.

[17] http://www.guardchild.com/teenage-sexting-statistics/ accessed today 30.11.2016

[18] http://www.huffingtonpost.com/2014/07/25/sex-trafficking-in-the-us_n_5621481.html, accessed today 19.11.2015

[19] http://newcountry999.com/social-media-manipulation-is-most-common-form-of-sextortion-study-finds/ accessed today 05.06.2016

[20] New Criminal Code of Romania / Romanian Criminal Code

[21] Benjamin Wittes, Cody Poplin, Quinta Jurecic & Clara Spera, *op.cit,* page 3,

2. Don't comply with their demands – they will not stop, they will ask for more and more.
3. Interrupt any contact with the criminals – any more contact will expose you more to the criminal's manipulations. Unfriend and block any account on social media that is related to the criminals and deactivate your account for a while.
4. Don't delete any data – any material can be used as evidence to build up a case against the criminal.
5. If the video or other content is posted online, report it immediately to the online content host.
6. Contact the local police, cyber police or ANITP.

Conclusion

The online world can be a dangerous environment especially if we are not aware of its danger. It has become a powerful weapon in the hands of the criminals and the technological developments have created an unlimited market for them. Without geographic limits, human trafficking can develop at ease in different, new forms. This makes it harder for the criminals to be identified and prosecuted.

The forms of exploitation are more and more diverse and recruitment methods more and more advanced, subtle and intelligent. Until now, the traffickers used brutal force to recruit their victims but now this force has changed to intelligent manipulation and persuasive tactics, advanced marketing and management strategies and superior informatics abilities.

We have become very vulnerable because we are not aware of the danger present online. We post without thinking, without protecting ourselves, without being aware of what information we share and how that information can be accessed and used by the criminals against us. We accept friend requests from people we don't know, we share personal information with them, we send photos and videos, we install all sorts of apps without thinking one second that in this way we make ourselves the perfect target.

The criminals constantly update their methods and so should we. We need to embrace all the changes in the online world and start using them to protect ourselves, our families and our communities. It is up to us to be the solution.

Bibliography

General

1. Benjamin Wittes, Cody Poplin, Quinta Jurecic & Clara Spera, Sextortion: *Cybersecurity, teenagers, and remote sexual assault, Center for Technology Innovation at Brookings*
2. Janis Wolak, David Finkelhor - *Sextortion - Findings from an online survey about threats to expose sexual images*, Crimes Against Children Research Center, University of New Hampshire, 2016

Speciality works and related Legislation

3. Noul Codul Penal al României - Legea 286/2009; [The New Penal Code of Romania-Law 286/2009];
4. National Strategy on Child Exploitation Prevention and Interdiction, US Department of Justice, April 2016

Electronic sources

https://www.wearethorn.org/child-sexual-exploitation-and-technology

http://money.cnn.com/2016/05/11/technology/brookings-institution-sextortion-study/

https://en.wikipedia.org/wiki/Sextortion
http://www.brookings.edu/research/reports2/2016/05/sextortion-wittes-poplin-jurecic-spera
https://www.wearethorn.org/child-pornography-and-abuse-statistics/
http://www.beakidshero.com/posts/newest-form-child-exploitation-sextortion/
http://www.missingkids.org/Sextortion
https://www.wearethorn.org/sextortion/
http://www.networkworld.com/article/2900829/security0/mobile-sextortion-schemes-on-rise-trend-micro-reports.html
http://www.guardchild.com/teenage-sexting-statistics/
http://www.huffingtonpost.com/2014/07/25/sex-trafficking-in-the-us_n_5621481.html
http://newcountry999.com/social-media-manipulation-is-most-common-form-of-sextortion-study-finds/
https://www.justice.gov/psc/national-strategy-child-exploitation-prevention-and-interdiction
http://www.makeuseof.com/tag/sextortion-evolved-scarier-ever/
https://www.netsafe.org.nz/webcam-safety-avoiding-sextortion-and-blackmail/
http://cyberbullying.org/sextortion
http://www.cagoldberglaw.com/5-steps-take-youve-sextorted/