Taking Down Websites to Prevent Crime

Alice Hutchings, Richard Clayton and Ross Anderson
Computer Laboratory
University of Cambridge
Cambridge CB3 0FD
Email: firstname.surname@cl.cam.ac.uk

***Abstract*—Website takedown has been used to disrupt criminal activities for well over a decade. Yet little is known about its overall effectiveness, particularly as many websites can be replaced rapidly and at little cost. We conducted lengthy interviews with a range of people actively engaged in website takedown, including commercial companies that offer specialist services, organisations targeted by criminals, UK law enforcement and service providers who respond to takedown requests. We found that law enforcement agencies are far less effective at takedown than commercial firms, who get an awful lot more practice. We conclude that the police must either raise their game, or subcontract the process.**

I. Introduction

Website takedown is a key tool used by financial institutions to defend against 'phishing' – the use of fraudulent websites to steal customer credentials [33]. Takedown is also used to disrupt a range of other crimes, by removing the websites used in advance fee frauds, disseminating malware, distributing child sexual abuse content, recruiting money mules, or for trading stolen credit card details, pharmaceuticals or other illicit goods [34]. Takedown usually requires intervention by service providers, which includes both hosting providers and domain name registrars.

Options for hosting criminal websites include compromising an existing host to add extra pages, using free providers who allow the creation of simple websites, using a paid-for hosting provider (for which the criminal can choose the domain name), or setting up a website as a hidden service that can only be accessed using an anonymity network [33].

The takedown of these websites is achieved in many different ways, undertaken alone or in combination. These include the hosting provider taking down the website, having the owners of a compromised machine remove offending pages, suspending the domain name, or seizing the physical server as part of a wider law enforcement initiative. Website takedown is an example of situational crime prevention, as it aims to change the environment in which crime occurs [8].

Research into takedowns of websites disseminating malware has found that responsiveness by hosting providers depends on the countermeasures adopted by offenders, and the way takedowns are requested [7]. However, little is known about the effectiveness of website takedown as an intervention method to disrupt different types of online crime. In particular, websites can quickly reappear, and legitimate websites can be adversely affected [35], [36]. Moore and Clayton [33] examined the effects of website takedown on phishing, and found that it is helpful, but it cannot completely mitigate phishing attacks as it will never be instantaneous.

II. Research Questions

We interviewed key players who are actively engaged in the website takedown process to explore the issues with it in depth. The questions we tackle in this research are:

1) How do websites differ according to their criminal purpose?
2) What organisations are involved in website takedown?
3) How are websites taken down?
4) What are the challenges with website takedown?
5) What are the intended effects of website takedown?
6) What are the unintended effects of website takedown?
7) What displacement occurs following website takedown?

This paper gives us an insight into the state of phishing after 10 years of co-evolution by the attackers and defenders. Although there are a number of papers discussing specific aspects of takedown, we believe this is the first to survey all the professional participants (other than the criminals) in order to get an overall picture of what works and what doesn't.

III. Methodology

This is a qualitative study, using interviews to garner the views and amalgamate the experience of a sample of people who are knowledgeable about this area. We are not doing quantitative research where we would be attempting to make precise measurements. The majority of papers in the computer science literature are quantitative, in that they count incidents and quantify losses. There is also great value in qualitative research, especially when we need to understand the structure and nature of a problem in order to work out what to measure in later studies.

Our research examines the takedown of websites used for criminal purposes. These included the recruitment of money mules; fake websites, including those used for phishing; malware dissemination; the sale of counterfeit and illicit goods; and child sexual abuse content.

We did not consider takedowns performed for intellectual property infringement and other civil matters, nor similar activities such as the removal of copyright infringing material,

978-1-5090-2922-8/16/$31.00

'filtering' or 'blocking' websites, removing malicious mobile applications from app stores, and taking down (or taking over) botnet command and control (C&C) servers or redirecting malware domains to 'sinkholes'. Also outside our remit were incidents where websites are 'taken down' by offenders, such as website defacement and denial of service attacks.

A. Research Design

We interviewed participants actively involved in various aspects of website takedown. They worked for companies who provide takedown services for hire, organisations impersonated by fake websites in phishing attacks, service providers, or were members of UK law enforcement. In total, 22 interviews were completed, with 24 individuals from 18 organisations participating. Recruitment involved emailing relevant contacts, informing them about the project, and asking if they would be willing to take part.

A semi-structured interview schedule was used, which explored the research questions in depth. Participants were interviewed face-to-face, by telephone, or using VoIP. The interviews took between 40 and 99 minutes, with a mean time of 64 minutes.

B. Participants

Most participants had been involved in website takedown for quite some time, with relevant experience ranging from 6 months to 11 years. Directly relevant experience totalled 121 years, with a conservative estimate of 1.3 million websites having been removed. Participants were from the UK, elsewhere in Europe, and the USA.

Participants TC1 to TC5 are from takedown companies; participants LE1 to LE6 are UK law enforcement; and participants BO1 to BO6 (brand owners) are from targeted organisations, including government agencies. The remaining participants (UC1 to UC5) are uncategorised, as doing so could potentially re-identify them or their organisations. The participant identifiers are used to differentiate responses from different interviews. The handful of interviews that had more than one participant are referred to using the same identifier, therefore there are 22 participant identifiers, yet 24 participants.

C. Analysis

The interviews were analysed using qualitative content analysis procedures. A qualitative research design was selected for its ability to provide a deeper understanding of the topic than may be achieved through a quantitative design. Qualitative research captures nuances and provides richness to data that may not otherwise be quantifiable [4].

Coding of the data for the first four research questions was mainly 'data-driven coding' [18], where the concepts were derived from the data. Questions five to seven were analysed using 'concept-driven coding' [18], with the key theoretical concepts arising from the criminological literature.

IV. Results

A. How do Websites Differ According to Their Criminal Purpose?

Websites may be used for a variety of criminal purposes. However, criminal laws are specific to a jurisdiction, while the Internet takes little account of borders. Therefore, a website that is illegal in one location may not be criminal in the location where it is being hosted, or where the domain name has been registered.

The criminal purpose affects how offending websites are set up. Differences are related to the intended visitor (victim or offender, which includes the consumer of illicit goods), and how the websites are hosted (compromised website, registered domain name, or hidden service on an anonymity network).

Phishing websites intend to attract victims – they are set up in high volume and are active for short periods of time. Their targets are generally quick to respond to these attacks. Phishing pages are often hosted on legitimate sites that have been compromised (TC1, UC1, TC5). TC1 indicated that, for phishing attacks, about 80% are hosted on compromised sites, about 10% are on free hosting services, and the remaining 10% are on paid-for services. TC2 advises that the modus operandi for phishing sites varies for some targets, with fraudulent impersonators of Bitcoin wallet providers typically registering a domain name.

Criminal marketplaces, which have multiple sellers trading in illicit goods such as drugs or stolen data, generally only use the one website, so as to differentiate themselves from their competitors. Buyers and sellers may trade on multiple marketplaces, and the success of a website partially depends on its reputation [21]. Continuity is important, and they will have hosting arrangements little different from legal websites. Some marketplaces are hosted on hidden services, although many are not (BO5).

On the other hand, online stores selling illegal goods, such as unlicensed pharmacies or credit card brokers, may operate multiple websites, usually with registered domain names. However, they may use compromised websites to drive traffic to their store-fronts. For example, illicit pharmacies began using search redirection attacks after search engines barred their advertisements [30], [31].

B. What Organisations are Involved in Website Takedown?

The takedown landscape is intricate, with contributions from private companies, self-regulatory bodies, government agencies, volunteer organisations, law enforcement, and service providers. Each of these has distinct roles and represents different interests, while also performing many tasks in common. Some of the parties involved in website takedown are controversial, due to their previous methods,[1] targets [29], or other activities [10]. In theory, website takedowns can be requested by any individual or organisation. However, with experience comes efficiency, particularly with industry knowledge and, importantly, contacts (TC1).

[1] http://wiki.aa419.org/index.php/New_Bandwidth_Policy

1) Targeted organisations: Brand owners, service providers and government agencies can be targeted by offenders. By no means all of the offending websites that are identified will be taken down by the targeted organisation (BO3). Organisations may see this as a 'whack-a-mole' problem; some will not do anything about sites that are unlikely to do much damage, as they will just reappear anyway. Instead, they may direct their resources towards detecting and stopping attempts to use compromised credentials (BO3). Targeted organisations typically only take down websites that impersonate their brand directly (BO1), even when other websites in the criminal value chain, such as those used for recruiting money mules, could be better targets as they cause harm to industry overall.

2) Commercial takedown companies: When targeted organisations learn of websites impersonating their brand, they may organise takedown themselves, pass the information on to a specialist contractor, or a combination of the two (BO1, BO2, BO3, BO4, BO5, LE3). Commercial takedown companies provide takedown for hire. To take websites down quickly these companies automate the process (TC5). They have cultivated professional relationships with registrars and hosting providers, and some retain staff with the language skills to facilitate takedowns in countries that may otherwise be difficult (TC5).

3) Volunteer groups: Some groups instigate takedowns voluntarily. Artists Against 419 (AA419)[2] targets websites that fall outside the attention of financial institutions, as they do not imitate legitimate organisations but entirely fake companies, such as banks, solicitors, mule recruitment or escrow agents [34]. More unusual has been Anonymous' #OpISIS vigilante campaign, aimed at taking down websites, as well as email and social media accounts, used by Islamic State [2].

4) Industry self-regulation: Such bodies include the UK's Internet Watch Foundation (IWF). The IWF receives complaints about child sexual abuse content on the Internet with the aim of minimising its availability. The IWF requests takedowns for websites hosted in the UK, informs their counterparts in other countries of material hosted internationally, shares information with law enforcement, and provides a URL list for Internet filtering purposes [26].

5) Law enforcement agencies: Law enforcement agencies also conduct takedowns. In the UK most of this is done by the National Crime Agency (NCA), which includes the National Cyber Crime Unit, and by the City of London Police, which includes the Police Intellectual Property Crime Unit (PIPCU) and the National Fraud Intelligence Bureau (NFIB). The NFIB also coordinates takedown for the Financial Conduct Authority, Trading Standards and other police forces (LE2).

By comparison with private and volunteer organisations, law enforcement are involved in relatively few takedowns [34]. The majority of takedowns relate to phishing. However it is difficult to determine the extent of victimisation and financial loss attributed to any particular offender, making it hard to get law enforcement involved (BO2, TC2, BO4, BO5).

[2]http://www.aa419.org AA419's name refers to the advance fee frauds that take on the 419 name from the relevant article in Nigeria's Criminal Code.

TC2 reports phishing sites to the police in the jurisdiction where the site is hosted, although responses are infrequent. TC5 occasionally provides intelligence to law enforcement when they believe it is actionable and useful for investigations. However, LE1 told us that law enforcement rarely receives reports from targeted organisations for brand protection reasons: they do not wish to be publicly associated with fraudulent activities.

In a small number of countries, Italy being one, service providers require takedown requests to be validated by local law enforcement before being actioned (TC5). TC5 advised that the frequency with which they needed to go to law enforcement with such requests depended on how often offenders were using service providers in these jurisdictions, but it was typically one to two percent of takedowns.

6) Quantifying Takedown: We urge some caution when reviewing the number of takedowns across different types of organisations, and recommend this is not done on a comparative basis. The first concern is that takedown may be counted differently by different organisations, such as counting the number of requests sent, rather than the number of takedowns actioned, counting the takedown of re-appearing sites as new takedowns, or counting each unique URL as a separate website, even if ultimately they reach exactly the same webpage. Also, some organisations have limited remits, such as only taking down websites hosted in their jurisdiction, for particular types of crime, or that infringe certain brands, while others undertake additional disruption and investigation activities along with takedowns.

We do not report the number of takedowns reported to us by each participant on an individual basis, as this could identify the people we spoke to. Instead, we provide aggregate statistics. We asked participants the number of takedowns they had been involved in, and the number of years they had been doing takedowns. In some cases estimates were provided, rather than precise numbers. As some participants had been taking down websites much longer than others, we attempted to standardise responses by dividing the total takedowns by the number of years. However there are limitations in this approach, as there may have been more takedowns in recent years. Organisation types that are represented with less than 4 participants are aggregated as 'other'. Responses are included in Table I, and are provided for illustrative, rather than comparative, purposes.

C. How are Websites Taken Down?

Websites are usually taken down in two distinct ways. The first is the issuing of explicit 'Takedown Orders', the second and far more common approach is the use of a voluntary 'Notice and Takedown' regime. Website owners can be alerted directly to the fact that their website has been compromised, and asked to fix it (TC1, TC5). However, firms with a poorer understanding of computer security and technical matters are more likely to have their websites compromised in the first place, and less likely to be able to rectify a compromise promptly (TC1).

TABLE I
AGGREGATED RESPONSES RELATING TO REPORTED TAKEDOWNS BY ORGANISATION TYPE

Organisation type		Takedowns		Experience (years)		Takedowns per year	Percentage of takedowns
	n	Total	Mean	Total	Mean		
Law enforcement	6	3 022	504	25.5	4.3	119	0.23
Takedown company	5	1 004 227	200 845	46.5	9.3	21 596	77.65
Targeted organisation	6	264 702	44 117	18.5	3.1	14 308	20.47
Other	5	21 350	4 270	30.5	6.1	700	1.65
Total	22	1 293 301		121		-	100

1) Takedown Orders: Takedown orders are issued by courts or in some jurisdictions by law enforcement. UC2 and LE3 differentiated between takedowns requested by law enforcement for prevention and disruption purposes, and those that are part of an investigation. The latter may include the seizure of servers (LE3), be coordinated with arrests (LE2), and have judicial oversight.

Court issued warrants or orders must be complied with within the relevant jurisdiction. Various types of actions may be required (LE4). For example, a seize and takedown order will result in subsequent visitors seeing a non-existent domain response to any queries. However, an order to seize and post notice will direct visitors to a notice page for a specified period of time [38].

While there has been very little takedown of hidden services in the past, this changed with Operation Onymous, a coordinated action targeting weapons and drugs sold on online marketplaces operating as Tor hidden services. In November 2014, more than 410 hidden services were taken down and 17 people were arrested [16].

2) Notice and Takedown: This is by far the most common approach to website takedown. Organisations or individuals requesting takedown issue a 'takedown notice' to the provider [33]. The appropriate recipient of a takedown notice depends on what is being taken down (a domain name or the provision of hosting), and upon the nature of the website, such as whether it is hosted on free webspace or on a compromised machine (TC1). The important distinction from Takedown Orders is that these are *requests*, not demands (TC1, UC5). While some takedown notices issued by law enforcement make this distinction clear, other policing agencies have been more forceful and phrase their request as if it were an order (UC2).

Criminal behaviour is generally in contravention of providers' terms of service and so they have a sound basis on which to act when a notice is received (UC5). Some service providers pro-actively monitor their own systems for offending websites (UC1). Others have engaged takedown companies to identify offending websites for them (TC5). One of the participants, from a hosting provider, advised they rarely receive takedown requests, as they remove most offending websites (usually phishing sites) themselves, under their 'acceptable usage policy'. When a website is taken down by this hosting provider the site owner is contacted and advised.

Where abusive domain names are similar to trademarks, the Internet Corporation for Assigned Names and Numbers (ICANN) has a Uniform Domain-Name Dispute-Resolution Policy (UDRP), which is followed by all their registrars [23]. Registrars are also signatories to Registrar Accreditation Agreements (RAAs), which are contracts with ICANN relating to the registration of domain names in the gTLDs (global top level domains). RAAs entered into after 28 June 2013 are subject to the 2013 agreement [24] while the 2009 RAA [22] is applicable for 5 years after signing (so will remain relevant until 2018).

The 2013 RAA requires registrars to maintain a dedicated abuse point of contact, with an email address and telephone number, to receive reports of illegal activity from law enforcement, consumer protection, quasi-governmental and other similar organisations in the jurisdictions in which the registrar has a physical office. Reports of 'illegal activity' (under 'applicable law') that are 'well-founded' are required to be reviewed within 24 hours. Actions taken in response to reports should be 'necessary and appropriate'. Both the 2009 and 2013 RAAs have requirements for WHOIS data accuracy, which is opens up another avenue for complaint when domain names have been registered with false details (TC2).

The applicability of the 2013 RAA for UK law enforcement requests is limited to registrars that have adopted this version and maintain a UK office. There is no guidance provided in relation to what is a 'well-founded' report, which may be problematic when the reports are allegations, with no judicial findings. However, the RAAs do imply that registrars should be responsive and LE2 and LE5 advised that if they failed to have a domain name taken down by a registrar, they escalate the matter to the relevant registry, and, if required, to ICANN.

The procedure for issuing takedown notices varies by the requesting organisation. A participant from a hosting provider told us that takedown companies used their standard reporting procedures, but that 5% of the takedowns they actioned came from law enforcement and were accompanied by a court order. We were told that law enforcement agencies usually complete their own standard form (LE1), while takedown companies get faster service by tailoring requests to the service provider (TC1, TC5): they know that this firm wants them to

open a ticket, that one prefers an encrypted list of URLs, and yet another firm expects you to phone their call centre and be able to speak Mandarin.

3) Other disruption activities undertaken alongside website takedown: Additional takedown activities include taking down telephone numbers, merchant accounts, online advertisements, and email accounts associated with the criminal activity (TC1, LE2, LE4, BO6, TC4). LE5 advised that they had worked with a registry to blacklist the registration of domains using a particular credit card and email address. Takedown companies also input fake details into phishing pages, referred to as baiting, so that banks can detect attempts to use phished credentials (TC1), or input large amounts of fake data, referred to as flooding (TC3). Another activity is to identify what credentials have been obtained (BO2). If the credentials remain on the server in an unsecured file next to the phishing page then it is relatively easy to fetch them (BO4), but when the credentials have been securely stored this can be problematic because the jurisdiction may have laws that prohibit unauthorised access (LE3). When collected credentials have been sent to an email address, a subpoena can be issued to the email service provider (TC3). Other ways to reduce visitors to fraudulent websites include approaching search engines to request they demote websites in search results, or to ask browser vendors to block access to the offending websites (LE1, LE2, TC4). For matters that may fall under civil, as well as criminal, legislation, solicitors may send 'cease and desist' letters (UC3).

D. What are the Challenges with Website Takedown?

1) Challenges for those responding to takedown requests: The main concern for registrars and hosting providers is establishing the legitimacy of the requests they receive. Service providers need to ensure that they are acting appropriately and meeting their obligations to their customers. There is currently no standard procedure or oversight for website takedown, apart from the requirements associated with law enforcement entering a location and seizing a server. The Internet & Jurisdiction project aims to create due process for domain seizures, content takedowns and related issues for requests addressed by courts and public authorities [25].

At present, this lack of any standard procedure has led to service providers being the primary check and balance for takedown requests. Although many service providers hardly trouble to assess the appropriateness of requests, others may refuse particular types of takedown request [42]. Notably, in 2013, the registrar and hosting company easyDNS refused a takedown request received from PIPCU [13]. Specifically, they questioned how the police could claim the material being hosted was illegal, or the website was criminal, without the matter being decided by a court of law. According to easyDNS's takedown policy, takedown notices issued by law enforcement should be accompanied by a court order unless there is an 'imminent threat to safety or health', or there is a threat to the 'stability of the Internet', a concept encompassing malware, phishing, botnets and spamming [14]. UC1 similarly requires a court order to take down offending websites, and the order must be obtained in the jurisdiction where the website is hosted.

Registrars and hosting providers regularly request court orders when receiving takedown requests from law enforcement (LE4) and LE2 advises this happens for about 80% of requests submitted to domain name registrars. LE4 believes the relationship law enforcement has with the service provider influences whether or not a court order is requested, and that they were working to improve those relationships. It appears that in some cases, instead of obtaining a court order, law enforcement agencies have threatened to have registrars' accreditation with ICANN terminated, or to prosecute service providers who do not comply with their requests (UC2, TC4). Such confrontational behaviour poisons relationships generally and is a factor in service providers telling agencies to come back with a court order.

2) Challenges for law enforcement: LE2 and UC3 spoke about the difficulties in getting a court orders which, as we have just noted, are regularly requested. These include the amount of time involved, which reduces the ability to provide a quick response, the cost, and having to go to the appropriate jurisdiction. LE5 advised that if the takedown involves an overseas service provider, they seek a counterpart in that jurisdiction to submit the request for them.

The problems law enforcement face when crossing jurisdictions is a major inhibiting factor for action in relation to offending websites (UC1). The NCA coordinates website takedowns for UK police forces with law enforcement agencies in foreign jurisdictions (LE1, LE4, LE5). The process involves first requesting preservation of the evidence, then obtaining a warrant and physical seizure by the local police. There are good relationships around the world, but the delays associated with cross-jurisdictional enforcement action, including through Mutual Legal Assistance Treaties, are problematic (LE1). The process can take three months, and is reserved for matters involving substantial damage or high intelligence value (LE4). UC2 noted that mutual assistance put pressure on the resources of local police, for whom foreign requests are generally not a priority.

The shortage of law enforcement personnel with the expertise, knowledge and skills to request takedown is another identified difficulty (LE5). Another concern is 'blue-on-blue': where takedowns interrupt other police operations. For example, the IWF at one stage was only requesting that child-abuse websites be taken down some days after they were reported, to give police a chance to collect evidence [34].

3) Challenges for targeted organisations and takedown companies: Responsiveness is the main challenge encountered by those requesting takedown, particularly as there is little economic incentive for some responders to do anything (TC1, BO3, TC3, BO4, BO5, TC4). It was suggested that improvements might result from a standardised API for reporting abuse (BO4). A related challenge is time to takedown (TC5). TC5 advised that they concentrated on building good relationships with the service providers, and automated processes to report websites for takedown, to limit delays and expedite

confirmed abuse reports.

E. What are the Intended Effects of Website Takedown?

Situational crime prevention incorporates multiple criminological perspectives. According to the routine activity approach, crime can be reduced by increasing the capability of guardians, decreasing the suitability of targets, and decreasing the presence of motivated offenders [9]. Rational choice theory [11] suggests that increasing the cost and effort to commit a crime, increasing the perceived likelihood of detection, and reducing the expected benefit, will deter crime.

We explored participants' reasoning behind the crime prevention aspects of website takedown, which we categorise according to the theoretical concepts introduced by situational crime prevention. Also explored is harm minimisation, particularly relating to brand protection, and cost reduction.

1) Decreasing the suitability of targets: Particularly applicable to websites used for phishing and other scams, website takedown may reduce victimisation by ensuring that visitors to a site do not see malicious content (TC5, UC5, [33]).

2) Increasing the capability of guardians: UC1 suggests that, by taking down websites and providing website owners with information about how to fix the vulnerability (which they must do before hosting can resume), they become better guardians of their own website in the future. Information about compromises is also used to inform other customers with similar vulnerabilities (UC1).

3) Decreasing the presence of motivated offenders: UC1 and UC5 claim that, by shutting down offending websites, they discourage offenders from the same hosting company in the future. Also, forum and marketplace takedowns done in tandem with other law enforcement activities may reduce the presence of motivated offenders by decreasing trust in reappearing websites (UC2).

Examples where websites have been shut down, and new websites appearing under police control, can be found in both the online stolen data and drug marketplaces. Following an operation which saw the Shadowcrew stolen data market being targeted by law enforcement, FBI agents infiltrated the DarkMarket forum, culminating in the agency running the server and hosting the communication systems [19]. Similarly, shortly after the Silk Road drug marketplace was closed in 2013, Silk Road 2.0 was established. Again, an undercover agent, this time from the US Department of Homeland Security, was involved in the administration of the new website, which became popular despite widespread rumours the site was operated by law enforcement [12]. This culminated in the arrest of the alleged operator and seizure of the servers as part of Operation Onymous [28].

For websites hosting child sexual abuse images, takedown is often justified solely because it reduces the likelihood that people who have not previously accessed the material will stumble across it (LE3, UC4). Investigations done alongside takedown are aimed at identifying perpetrators and ideally rescuing the victims of abuse (LE3).

4) Reducing the benefits: A reduction in the benefit to offenders discourages them from that crime type (TC2, TC4). For fraud, this is related to victims not being able to reach the website (TC4). However, benefits can also be reduced for 'victimless' websites, such as online markets, where offenders trade in illicit goods and services including drugs, stolen data, and firearms. Almost one quarter of websites with child sexual abuse images are commercial, and some referrals also generate revenue for affiliate marketing schemes (UC4). Here, the intended effect of takedown is the interruption of illicit trading (UC4).

5) Increasing the cost: Website takedown can increase the cost of maintaining and replacing sites used for criminal purposes (TC2, BO4, TC5). This includes the cost of registering domain names, hiring botnets, hosting websites or purchasing compromised websites (UC2, BO4).

6) Increasing the effort: Website takedown increases the effort required to keep a website active. However, this differs by crime type. There may be an increased effort in developing trust and reputation in websites designed to be long-standing, compared with phishing sites, which are generally transient (UC2).

7) Increasing the perceived likelihood of detection: Website takedown can be done in tandem with arrests to increase the perceived risk of being detected and prosecuted (LE3). LE6 advised that, following a high profile arrest and takedown, similar sites were voluntarily taken offline.

8) Brand protection: Another intended effect of website takedown moves away from crime prevention and towards harm minimisation (BO1, TC5). Phishing scams pose a reputational problem for banks, who find their legitimate communications being confused with fraudulent emails, and who wish to retain public confidence in online banking systems (TC1).

9) Cost reduction: The immediate cost for many victims is the direct financial loss, as well as the emotional costs associated with being a victim. Further indirect costs for targeted organisations, such as financial institutions, include responding to reports of phishing sites and dealing with customers who report they may have divulged their personal information (TC1, BO2, TC5).

F. What are the Unintended Effects of Website Takedown?

While most of the time takedown requests are well meaning, they can be errors as well as intentional misuse. These are more likely to occur when service providers do not verify takedown requests [34]. Some requests have been so bad the Electronic Frontier Foundation set up the 'Takedown Hall of Shame' [15]. Quantifying unintended outcomes is problematic, as they may not become known to requesters, and if known they may not be widely publicised.

1) Consequences for legitimate site owners: TC2 and LE3 advise that false positives are extremely rare. Other participants report that accidently taking down legitimate websites is an unintended consequence of takedown, and harms legitimate website owners (UC1, LE2, TC3, LE4, LE5, TC4, UC5). Examples are the takedown of the Dajaz1 and Rojadirecta

websites. The Dajaz1 website had been hosting copyrighted songs, with the permission of the rights holders, while the Rojadirecta website was a sports website which linked to other websites containing copyrighted material, but did not host any infringing material itself. These websites were eventually returned to the registrants after being taken down by law enforcement, but after much time and many legal challenges [27].

Consequences for legitimate site owners can also be felt after the seizure of servers, if they are also being used for lawful purposes (LE1). Targeted firms may not even be aware of all their own legitimate websites, and request takedowns of websites used for marketing or recruitment (BO2, TC2, TC3, TC4, TC5).

The takedown of compromised sites is particularly problematic when not just the offending pages are removed, but the entire site. In this scenario, which TC1 estimates occurs with 20% of hosting providers, the legitimate owner is victimised twice; first the compromise, then the loss of their site. TC5 advised that they were starting to see 'domain shadowing', whereby the credentials for the domain registration are obtained in a phishing attack, and used to add subdomains. It then appears that the domain has been set up for malicious purposes, rather than the account being compromised, and it can be mistakenly suspended.

UC5, who responds to takedown requests, advised that there have been rare instances where there had been typos in domain name requests, or missed hyphens, which had been uncovered during due-diligence procedures.

In addition to loss of visibility and downtime, website owners have to expend time and effort to get their websites back online (UC1, UC5). Takedowns are particularly problematic when websites for critical infrastructure or health systems are compromised, as takedown could adversely affect their operation (TC5, [36]).

2) Intentional misuse of website takedowns: Takedown mechanisms can be intentionally misused, particularly as there is no real legal or economic cost for submitting invalid takedown requests. Misuse includes taking down competitors' sites or making vexatious claims. UC1 and LE2 advise they occasionally receive such requests. Some strongly aggressive brand protection may fit into this category, as well as website takedowns following spilled secrets or whistleblowing.

3) The Streisand Effect: In 2003, Barbra Streisand attempted to sue for violation of privacy after a photograph of her residence, taken to document coastal erosion, was made available on the Internet. Not only was her lawsuit unsuccessful, but her legal action drove many more visitors to the webpage she objected to. This phenomenon has been named the 'Streisand Effect' [32] and was seen after The Pirate Bay website went back online following a 2006 raid and seizure of servers [37]. TC1 advises that the Streisand Effect is relatively rare, being mainly seen with brand abuse and 'freedom of speech' issues.

4) Increased dissemination of malware: Website takedown may also lead to increased malware dissemination. UC2 describes how, in the case of The Pirate Bay copycat sites, sometimes it is better to have the 'devil you know', as replacement sites had poor hygiene, and visitors were often infected with malware.

5) Disrupting other disruption and intelligence gathering activities: Intervention can also disrupt law enforcement monitoring of websites for the sale of stolen data, or the gathering of other evidence on offenders (UC2, [36]).

6) Conflicting with the principles of a free and open society: Takedown may be misused for censorship. Organisations may use it to shush complaints, and government controls over the registration of domain names can be used to suppress dissidents [36].

7) Perceptions of legitimacy: Takedowns that are not perceived as a legitimate use of police power may damage public trust in law enforcement. Perceived legitimacy has been found to be a stronger predictor of compliance with the law than the risk of being caught and punished [40]. Laws, policies and institutions that are seen as overstepping legitimacy can also lessen overall authority of a state [20]. Authorities need to be perceived as legitimate to gain the trust, support and cooperation of the public, as well as compliance with the law [41].

In relation to state use or abuse of authority, it is important to ask whether the state should have a given power; whether there is oversight and supervision in its use, such as judicial authorisation; how the state responds to abuses; and the level of transparency about the use and abuse of power [20]. These questions mostly relate to procedural justice [40].

G. What Displacement Occurs Following Website Takedown?

Displacement occurs when crime prevention activities result in crime moving to alternative locations, targets, methods, offenders, or offence types [39].

1) Replacement: Sometimes websites are simply re-compromised and the offending content put back up. For these sites, the question is whether steps are taken to fix the vulnerability that led to the compromise (TC5). UC1, from a hosting company, informs their clients how to fix the vulnerability before websites are reinstated, so they rarely see the same compromise reappearing. But TC2 advised that with other hosting providers, the site could reappear on multiple occasions. TC5 advised that 10% to 15% of phishing websites would reappear in the same location within a week.

2) Displacement to a new location: In many cases, displacement means registering a new domain name, perhaps with a new registrar, compromising a new website, or changing hosting providers. Participants said this is extremely common, with nearly all using the term 'whack-a-mole'. UC2 described websites as being 'disposable', advising that the process is usually automated. The time taken for websites to reappear depends on the type of criminal activity, with new phishing websites appearing within minutes or hours.

LE5 suggests that a measure of effectiveness is whether malicious websites move away from UK providers. However, if website operators move to hosting providers located in countries that are less likely to comply with requests, it may

hinder other enforcement operations [6]. TC5 advised that they see offenders move to service providers that are slow at responding to takedown requests.

Alternative new locations include anonymity networks, 'bulletproof' providers that refuse to remove websites, and domain registrars that are more tolerant to abuse. 'Silk Road Reloaded', another Silk Road copycat site, is hosted on an 'eepsite' on I2P [17]. But the use of anonymity networks depends on the type of criminal activity. The 'dark net' is used more for marketplaces, forums, child sexual abuse images, and C&C servers, but is not used to host phishing sites (TC1, BO5, LE3, UC4, TC5). Law enforcement participants confirm that very little of the criminal activity that comes to their attention involves hidden services on anonymity networks (LE1, LE4). TC4 advises there is no more criminal activity on anonymity networks compared to the Internet, as hidden services have less visibility and thus less traffic. While some underground forums are now being hosted on anonymity networks, this was not done with the speed or to the extent expected (UC2). In relation to child sexual abuse images, hidden services have been hosting illicit material for some years, but their numbers have not increased significantly over time (UC4).

It is noted that many bulletproof providers and rogue registrars are in countries that are not signatories of the Council of Europe *Convention on Cybercrime* [5]. There are also indicators of corruption in the provision of bulletproof services [21]. While bulletproof providers are used for some criminal websites (LE3, LE4), they are rarely encountered for others, such as phishing, and their use is said to be decreasing (BO4, BO5, UC4, TC5). This may be because of the expense, and/or because most phishing pages are found on compromised websites. TC5 advised that such providers did not permit phishing or malware sites, due to the unwanted attention that they attracted.

New locations may also occur when displacement, or replacement, involves marketplaces moving back from the cyber realm to physical space. This is the opposite of what has occurred with the advent of new technologies and communication platforms. There are potential implications for personal safety, as it has been hypothesised that online drug marketplaces reduce the violence associated with more traditional drug trades [1].

3) Displacement to new targets: TC1 and TC2 observe that when they start taking down websites associated with one target, the offenders eventually change target – to another brand, a different online scam, or other types of offending. TC2 advises that phishing targets are diversifying, targeting webmail, cloud storage and Bitcoin wallet providers, as well as online drug marketplaces.

4) Displacement to new methods: Phishing also provides insights into how offenders displace to new methods. Some examples evolve over time, such as registering nondescript domain names then moving onto fast flux. Sites hosting illicit forums and child sexual abuse images have started encrypting data so that if servers are seized, evidence cannot be accessed (UC2). It is noted that while displacement to new methods can be annoying, they are rarely used. The reported frequency in which they are seen varied from less than 5% (UC1), up to 25% (TC1). TC5 suggested if takedown companies were training offenders to use new techniques, they were doing this very slowly. Organisations requesting takedowns on a large scale keep using new techniques of their own to overcome schemes designed to frustrate them (TC1, TC5).

a) Registering domain names to fictitious or stolen identities: UC2 provides an example where a group initially used one false identity to register all their domain names, but after this was used to track them they changed to using a variety of stolen or completely fictitious identities. Offenders are registering domains using the personal information of people who have purchased counterfeit goods (TC4). LE2 advises of a case where an innocent third party who had a domain registered in their name subsequently received threats from fraud victims. According to TC5, offenders are also phishing for registrar account credentials, and using these to register new domain names and subdomains to the victim.

b) Registering nondescript domain names: Nondescript domain names are those that do not appear similar to a targeted brand or service. Nondescript domain names remove the possibility for the registrar to refuse or suspend a domain name registration under the UDRP (UC3, [34]). High volume, automated registration of nondescript domain names also makes takedown harder because of the volume (LE3). And while, with domain generation algorithms, it may be possible to identify ahead of time what the malicious domain names will be, registrars often refuse to suspend domain names that will only become malicious in the future (LE3).

c) The rock-phish technique: Of the phishing sites analysed by Moore and Clayton [33], 52.6% were attributed to this one gang (though some were duplicates). The rock-phish gang is so named because they originally put all their websites into a /rock directory. The gang evolved their technique, registering nondescript domain names, which all resolve to a single IP address acting as a proxy. This made taking down the website through the hosting provider difficult, as another proxy would be set up.

d) Fast flux: The fast flux method is a further evolution of the rock-phish technique. Rather than having multiple domains resolve to one IP address, they resolve to multiple IP addresses, which change rapidly [34]. LE3 sees fast flux a lot, while TC1, TC2 and BO5 advise the method comes and goes. TC3 advises it now accounts for 1% or 2% of target websites. Fast flux reportedly poses less of a problem than it did previously, as it is often possible to identify and shut down the true content server behind the proxy layer (TC1).

e) Serving different content to different visitors: A number of methods allow different content to be served to different visitors, including cookies and geolocation (TC1, UC1, BO5, LE3, TC5). TC5 advised that geolocation techniques were sometimes used to block offending content so that it was not visible to the relevant police, hosting provider and takedown companies. Websites serving malware exploits often require

a certain version of a browser, or relevant plugins, in order to trigger the malicious content (TC5). Gateway techniques serve content based on the visitor's HTTP referrer value. This is reportedly used with child sexual abuse images, where some visitors will see 'barely legal' content, rather than the illegal images shown to those who visit the site using a different sequence of links (UC2, UC4).

f) Single use URLs: Other times the criminal content of a website is only served up the first time it is visited. Subsequent visits, or visitors, do not see the offending behaviour (TC1, TC2, TC3, BO5, TC5). TC5 advised that these websites could be hard to take down, however were rarely seen as they offer little effectiveness to offenders.

g) BGP hijacking: TC5 advised that they had seen BGP hijacking taking place with hosting providers. BGP hijacking refers to blocks of IP address space being taken over without permission by maliciously placing bogus prefix announcements into the routing tables [3]. Takedown of BGP hijacked sites requires action to be taken by the providers 'upstream' of where the BGP announcement is being made (TC5). TC5 advised that they came across such websites extremely rarely.

5) Displacement to another offender: Dread Pirate Roberts was a moniker used by the operator of the original Silk Road marketplace, taken from the movie *The Princess Bride*. In the movie, the name is used by a succession of pirate captains. In Silk Road, life imitated art; after the first operator was arrested, another Dread Pirate Roberts operated Silk Road 2.0. Replacement and copycat sites are mainly seen with online trading sites and forums (BO5), and child sexual abuse images (LE3). We have already noted that in the case of The Pirate Bay, copycat sites are sometimes more harmful than the original site.

V. Discussion and Conclusion

This is a qualitative research paper, in that we interviewed 24 people to learn from their experience of taking down websites. The insights which we present clearly indicate areas in which quantitative research might now take place in order to put numbers and percentages on the different approaches to the problem. Before we can do that, however, we need a reasonable description of how this all works. This is why qualitative research is so useful; it explores the issue from the perspective of those who are close to the problem. This helps us look for fruitful directions for future research.

Our main practical discovery is that law enforcement agencies are simply not very good at taking websites down compared with the specialist companies that remove wicked websites as their core mission. This is not surprising given that the companies handle several orders of magnitude more business; takedown is a career for specialists rather than a part-time activity for a single officer.

The main way the firms excel is that they adapt to the world as it is, rather than expecting the world to respond to their standard form. They know which firms need you to report abuse to a standard email address, which need you to fill a web form, which want you to open a ticket, and which need you to speak to a call centre. They employ, or can promptly call upon, people who can speak to these call centres in Mandarin or Korean. They also have relationships of trust established with the abuse teams at the various big hosting providers and registrars. In short, they understand the global system, and know how to work it. The default police approach, of getting an order from a local court or threatening to use their local law enforcement powers, does not have all that much impact in a globalised world.

The lesson for the world's police forces is clear. Leaving takedown to untrained officers who do it only occasionally is not a good use of resources. The police should either centralise this activity in a specialist unit that gets enough business to learn to do it properly, or contract it out to a capable commercial firm. In the first case there are issues of training and monitoring, while in the second some attention must be paid to contract design. Of course, in an ideal world, a proper randomised controlled trial of these options would show which one is actually the best.

While most website takedown is done to interrupt and prevent criminal activities, there are different disruption mechanisms at play, such as stopping visitors from accessing the website, or discouraging offenders by making it more harder for them to continue their illicit enterprises. There may be adverse effects, particularly when legitimate websites that have been compromised are also taken offline. All of this must be considered when training officers or hiring contractors.

However takedown is to be done, policymakers must seek to understand the viewpoint of service providers, who must respect the rights of their customers. This is easier for some types of content than others. For phishing pages, malware, or explicit child sexual abuse images, it is usually straightforward to verify complaints. Other websites appear to be legitimate, and need more careful handling, with proper respect for due process.

It is of concern that, in some instances, service providers are being threatened with direct action, either legal or regulatory. This is particularly poor practice since it poisons the well for all. Just as the Snowden revelations of intelligence agency abuse have made surveillance harder, so also do abusive and bullying tactics by a small number of law enforcement agencies train service providers to avoid taking voluntary action but to say instead "come back with a warrant".

VI. Acknowledgements

We thank and acknowledge the following eleven organisations that contributed to this research, as well as the seven anonymous organisations that preferred not to be named: Anti-Phishing Working Group (APWG); Bristows LLP; Claranet; Eastern Region Special Operations Unit (ERSOU); IID; Internet Infrastructure Investigation Ltd; National Fraud Intelligence Bureau (NFIB); Netcraft; PayPal; PhishLabs; and The Registrar of Last Resort. This research was originally performed under the auspices of the Foundation for Information Policy Research (FIPR), with which the second and third authors are associated.

VII. Funding

This work was primarily supported by the UK Home Office under contract number HOS14/050. Some follow up work was completed with the support of the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHSS&T/CSD) Broad Agency Announcement 11.02, the Government of Australia and SPAWAR Systems Center Pacific [contract number N66001-13-C-0131]. The opinions, findings, and conclusions or recommendations expressed are those of the authors and do not necessarily reflect those of the funders.

References

[1] Aldridge, J., Décary-Hétu, D.: Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation. Available at SSRN 2436643 (2014).

[2] Anonymous: #OpIsis. http://pastebin.com/UqmnG2Wr (2015).

[3] Ballani, H., Francis, P. and Zhang, X.: A Study of Prefix Hijacking and Interception in the Internet. SIGCOMM Comput. Commun. Rev. 37(4), 265–276, (2007)

[4] Berg, B. L.: Qualitative Research Methods for the Social Sciences (6th ed.). Boston: Pearson Education, Inc (2007).

[5] Bradbury, D.: Testing the defences of bulletproof hosting companies. Network Security, 2014(6), 8–12 (2014).

[6] *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2014] EWHC 3354 (Ch) (17 October 2014).

[7] Cetin, C., Jhaveri, M. H., Gañán C., van Eeten, M., Moore, T.: Understanding the role of sender reputation in abuse reporting and cleanup. Workshop on the Economics of Information Security, Delft (2015).

[8] Clarke, R V.: Situational crime prevention: Its theoretical basis and practical scope. Crime and Justice, 4, 225–256 (1983).

[9] Cohen, L. E., Felson, M.: Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608 (1979).

[10] Coleman, G.: Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous. London: Verso Books (2014).

[11] Cornish, D. B., Clarke, R. V.: Understanding crime displacement: An application of rational choice theory. Criminology, 25(4), 933–947 (1987).

[12] Deepdotweb: Darknet distrust: The reaction to SR 2.0 in competing marketplaces? http://www.deepdotweb.com/2013/11/11/darknet-distrust-the-reaction-to-sr-2-0-in-competing-marketplaces/ (2013).

[13] easyDNS: Whatever happened to 'due process'? http://blog.easydns.org/2013/10/08/whatever-happened-to-due-process/ (2013).

[14] easyDNS: The Official easyDNS Domain Takedown Policy. http://blog.easydns.org/2012/02/21/the-official-easydns-domain-takedown-policy/ (2014).

[15] Electronic Frontier Foundation: Takedown Hall of Shame. https://www.eff.org/takedowns (2015).

[16] Europol: Global action against dark markets on Tor network. https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network (2014).

[17] Gallagher, S: Under the hood of I2P, the Tor alternative that reloaded Silk Road. http://arstechnica.com/information-technology/2015/01/under-the-hood-of-i2p-the-tor-alternative-that-reloaded-silk-road/ (2015).

[18] Gibbs, G.: Analyzing Qualitative Data. London: SAGE Publications (2007).

[19] Glenny, M.: DarkMarket: Cyberthieves, Cybercops and You. London: The Bodley Head (2011).

[20] Grabosky, P.: Secrecy, transparency and legitimacy. http://www.india-seminar.com/2014/655/655_peter_grabosky.htm (2014).

[21] Hutchings, A., Holt, T. J.: A crime script analysis of the online stolen data market. British Journal of Criminology, 55(3), 596–614 (2015).

[22] ICANN: 2009 Registrar Accreditation Agreement. https://www.icann.org/resources/pages/ra-agreement-2009-05-21-en (2009).

[23] ICANN: Uniform Domain Name Dispute Policy. https://www.icann.org/resources/pages/policy-2012-02-25-en (2012).

[24] ICANN: 2013 Registrar Accreditation Agreement. https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en (2013).

[25] Internet & Jurisdiction: Progress Report 2013/2014. http://www.internetjurisdiction.net/progress-report-2013-14/ (2015).

[26] IWF: Annual Report 2014. Cambridge: Internet Watch Foundation (2015).

[27] Kopel, K.: Operation Seizing Our Sites: How the Federal Government is taking domain names without prior notice. Berkeley Technology Law Journal, 28(4), 859–900 (2013).

[28] Krebs, B: Feds arrest alleged 'Silk Road 2' admin, seize servers. http://krebsonsecurity.com/2014/11/feds-arrest-alleged-silk-road-2-admin-seize-servers/ (2014).

[29] Laidlaw, E. B.: The responsibilities of free speech regulators: An analysis of the Internet Watch Foundation. International Journal of Law and Information Technology, 20(4), 312–345 (2012).

[30] Leontiadis, N., Moore, T., Christin, N.: Measuring and analyzing search-redirection attacks in the illicit online prescription drug trade. Proceedings of the 20th USENIX Security Symposium, San Francisco (2011).

[31] Leontiadis, N., Hutchings, A.: Scripting the crime commission process in the illicit online prescription drug trade. Journal of Cybersecurity, 1(1), 81–92 (2015).

[32] Masnick, M: Since when is it illegal to just mention a trademark online? https://www.techdirt.com/articles/20050105/0132239.shtml (2005).

[33] Moore, T., Clayton, R.: Examining the impact of website take-down on phishing. Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit (2007).

[34] Moore, T., Clayton, R.: The impact of incentives on notice and take-down. In: Johnson, M.E. (ed.): Managing Information Risk and the Economics of Security, 199–223, Springer, New York (2008).

[35] Moore, T., Clayton, R.: Evil searching: Compromise and recompromise of Internet hosts for phishing. In: Dingledine, R., Golle, P. (eds.): 13th International Financial Cryptography and Data Security Conference (FC09), Barbados, LNCS 5628, Springer-Verlag, 256–272 (2009).

[36] Moore, T., Clayton, R.: Ethical dilemmas in take-down research. Second Workshop on Ethics in Computer Security Research (WECSR 2011), St Lucia (2011).

[37] Norton, Q.: Pirate Bay bloodied but unbowed. http://archive.wired.com/science/discoveries/news/2006/06/71089 (2006).

[38] Piscitello, D.: Guidance for Preparing Domain Name Orders, Seizures & Takedowns. https://www.icann.org/en/system/files/files/guidance-domain-seizures-07mar12-en.pdf (2012).

[39] Smith, R. G., Wolanin, N., Worthington, G.: Trends & Issues in Crime and Criminal Justice No. 243: e-Crime Solutions and Crime Displacement. Canberra: Australian Institute of Criminology (2003).

[40] Sunshine, J., Tyler, T. R.: The role of procedural justice and legitimacy in shaping public support for policing. Law & Society Review, 37(3), 513–548 (2003).

[41] Tyler, T. R.: Enhancing police legitimacy. The Annals of the American Academy of Political and Social Science, 593(1), 84–99 (2004).

[42] Van der Sar, E.: Domain registrars deny police requests to suspend pirate sites. http://torrentfreak.com/domain-registrars-deny-police-requests-suspend-pirate-sites-140808/ (2014).