<CFS>

Short abstract (c.25 words): We report and discuss the results of our initial survey to measure the impact and prevalence for the average citizen of cybercrime in the UK.

Long abstract (c.120 words): Relatively little is known about the scale and cost of cybercrime in the UK, as current industry and academic efforts have produced largely unreliable estimates, often focusing primarily on large businesses. To address this, the authors developed one of the first customer surveys centred on the impact and prevalence of cybercrime to the average UK citizen. Just under one fifth of individuals surveyed had been victims of online crime, and of these, 6% reported being victimised more than once. Surprisingly, 2.3% reported losses in excess of £10,000 from online crime. We discuss the methodology used, its advantages, limitations, and main findings. We also reflect on the media coverage, and propose some cautionary notes for generalising and interpreting results. We additionally offer future research directions.

Cybercrime prevalence and impact in the UK

Julio Hernandez-Castro
jch27@kent.ac.uk

Eerke Boiten
E.A.Boiten@kent.ac.uk

Introduction

The internet has now become central to the way people live their lives – transforming businesses and providing new tools for everyday communication [1]. It is estimated that around 80 per cent of households in Great Britain had an internet connection in 2012 [2]. Internet users are spending increasing amounts of time online, undertaking a greater range of online and social networking activities [3].

However, the internet also presents increasing opportunities to cyber criminals. The nature of some traditional crime types has been transformed by the use of information communications technology (ICT) in terms of scale and reach, and includes areas such as financial transactions, sexual offending, harassment and threatening behaviour, and commercial damage and disorder.

New forms of criminal activity have also been developed targeting computers and computer networks, such as malware and hacking. Threats exist not just to individuals and businesses, but to national security and infrastructure and the borderless nature of cybercrime means that the UK can be targeted from anywhere in the world. The cyber threat has been assigned a 'Tier One' threat status in the government's national security strategy – one of the highest priorities for action [4].

Consequently, it is crucial we increase our knowledge and understanding of cybercrime. To date, efforts to measure the prevalence of online crime in the UK have been inconsistent and have often produced unreliable estimates [5]. Among the more robust recent findings, the Crime Survey for England and Wales (CSEW) found over one-third (37%) of adult internet users reported experiencing a negative online incident in 2011/2012, with computer viruses being the most common experience reported; experiences of unauthorised access to, or use of, personal data in the past 12 months was reported by 7% of adult internet users [6]. However the data from the CSEW does not necessarily relate to criminal activity, and these negative experiences would not often be recorded as crime. In order to address the dearth of research relating to the prevalence of online crime and its consequences to the general public, the University of Kent's Centre for Cyber Security Research developed and administered one of the first surveys on the impact and prevalence of cybercrime among UK citizens.

Our aims were two-fold: First, we wanted to check whether the relatively new platform offered by Google Surveys could be of any use to security researchers, particularly for finding relevant information on cybercrime prevalence. We examined multiple documents and studies, arguably many directly or indirectly supported by Google, and came to the conclusion that findings by this method, if used with care, can be compared, in some cases favourably, to the ones

produced by more traditional survey methods. There is an increasing corpus of evidence supporting this hypothesis [7], and recently even some highly regarded researchers have incorporated Google Surveys into their output [8]. Surveys get their responses from users that, as a result of answering the questions, are offered access to protected online content – for example, to magazine articles protected by a paywall. We were concerned about this incentive, and how it may induce users to pick quick and biased answers to access their desired contents as quickly as possible. Apparently, though, this does not occur too frequently and, in addition to this, Surveys offers answer randomization to minimize these undesirable biases. So, for a number of reasons, we believe we can cautiously (see section on Future Works) answer in the affirmative to this first question, and we plan to continue to employ this tool in future surveys.

Our second was that we wanted to test whether the recent and quite surprising findings of Google's security researcher Elie Bursztein concerning the USA population would be reproduced for the UK population [9].

Our results showed that they are, indeed. When asked the same question *"*Has anyone ever broken into any of your online accounts including email, social network, banking, and online gaming ones*?"* a surprising 18.3% (virtually identical to the 18.4% found by Bursztein) answered positively. Even more worrying is possibly the fact that 6% of those surveyed said this had happened more than once (for 6.4% for USA-Bursztein). The results on this question can be seen in Figure 1.

<INSERT FIG.1>

Figure 1. Answers in the UK to the question Has anyone ever broken into any of your online accounts including email, social network, banking, and online gaming ones?

Google Surveys has some interesting characteristics, like the possibility of accurately locating the survey respondents and classifying and interpreting data according to this inferred location automatically. Its age classification capabilities are also very relevant. These two features were important for our research at hand.

The Google Survey tool analyses the data collected, looking for statistically significant correlations, and highlights them, calling them insights. It is the task of the researcher to decide whether these insights are false positives, just a by-product of trying multiple combinations, or not, and whether they are consistent.

In our case, we believe that the two insights suggested by Google Surveys were statistically significant, consistent and meaningful. They were also quite interesting: the first is that those aged in the range 55-64 answered "No" to this question rather more often than the rest. This result was consistent across areas (Wales, Scotland, England) and particularly acute (this constituted the second insight) in England (with 91.3% compared to an average of 70.4%). The differences are statistical significant within the 95% confidence intervals computed. Of course, we can at the moment only speculate on the reasons behind this. Older people might be more cautious online, or spend less time, have fewer activities and accounts, or perhaps they keep an overall better security.

This result appeared quite counter-intuitive to us, but we cannot call it exceptional, as for most other types of crime older people tend to be less victimised. It is also well-known that elderly people seem to have more fear of crime, but they are generally less exposed to it [10]. This might be a less clear cut fact in the digital than in the real world, as it seems there is an increase of online schemes targeting the elderly [11]. However, there may be other explanations: it may also be the case that they are less aware of breaches of accounts actually having taken place. We plan to investigate the reasons underlying this result in future surveys.

We investigated further whether these security compromises led to any kind of undesirable financial implications for those affected. For that, we arranged a survey with the question "How much money have you lost due to online or computer-based fraud in the last 2 years?" Once again we used Google Customer Surveys, interrogating more than 1,500 people. The results were quite interesting with a large majority of the people having lost nothing (83.1%) but a significant fraction of them (11.6%) having lost more than £65, for an average over the whole population of £1,50 in losses over the last two years due to online computer based fraud.

We tried to gain a better grasp on how cybercrime is affecting average citizens by running one last survey that delved into the topic opened by the last question. We asked "How much money have you lost in the last year due to any kind of computer criminal activity?" and the results were quite shocking (see Figure 2).

<INSERT FIG.2>

Figure 2. Answers in the UK to the question How much money have you lost in the last year due to any kind of computer criminal activity?

This time there was an even larger group of people not affected economically at all by online-crime losses, but there was a very significant percentage of the population (2.3%) that claimed to be quite badly hit with losses over £10,000. This admits a number of different interpretations, including possibly a need for a more precise definition of what "cybercrime" actually is. We will try to learn a little more about how and why this happens in future surveys.

Media coverage

We were both happy and surprised by the extensive coverage that our small and limited study received from the UK media. It was covered in different ways at the national level by The Times, The Independent [12], The Guardian [13],

and The Daily Mail [14], and by online media such as TechReport [15]. It also received some international exposure, in places like China and Vietnam. Television also covered the news, and in the following days both of us were interviewed in different media including BBC Radio [16].
On reflection, we believe this clearly shows that there is an interest in this type of news, where cybersecurity and cybercrime is not necessarily linked with national security, critical infrastructures or nuclear power stations, but with the perspective of the average citizen, when losses are not an estimation in the billions but real money lost from your own bank account. An additional explanation for the media impact is of course that this news piece was launched August, not a period of the year full with interesting news.
Our initial delight with the media coverage was quickly tempered, when we started to see how journalists from even the most prestigious media made unfounded inferences from our data. We were particularly worried to the conversion of our percentage of respondents to a percentage of the population, and that figure quickly transformed into millions of UK citizens affected.
There was not even consensus in their extrapolation: Some claimed 10 million Britons were affected, others published a slightly more prudent figure of 9 million. This really surprised us, because despite knowing full well that such a claim would have made our piece of news much more attractive, we explicitly refrained from making it, in the knowledge that it could easily be wrong. Journalists quickly multiplied percentages times UK population, which is an easy but methodologically unsound approach.
They forgot, for example, that any measure has an error margin that could easily be around 3% (Google Surveys provides 95% confidence intervals) and that any claim based on that had better be conservative and use the lower end of said interval. More importantly, they forgot that the survey did not cover people below 18 years old (a total of 14,270,037 out of the 63,182,178 in the last Census [17]) nor, of course people that have never used the Internet (an estimated 14% of the population).
If we were compelled into translating our figures into millions of UK citizens, our estimation would be much closer to around 6 million, taking into account for example, that although 86% of the UK population have 'ever' used Internet, some are quite infrequent users, etc., quite less spectacular than the published by most media, but still interestingly high.

Conclusions & Future Work

It seems that online crime has a clear impact on the lives of many UK citizens, with their accounts and credentials being compromised significantly and in some cases multiple times. This and other incidents online translate into financial losses that, despite not affecting large numbers of people, have quite a large impact on a few (around 3% of the population) that are very badly hit.
More research is due focusing on these crimes that are the most likely to affect the average citizen, and that so far have been neglected in favour of the attacks that affect large companies and SMEs. Studying the evolution of this type of cybercrime over time, and how to effectively act upon it with different prevention and mitigation strategies is a promising research line.
We will continue to produce this survey and compare and analyse future findings, to study how the numbers of online victims and crimes evolves over time. We are currently in the process of elaborating the next survey, and plan to run it twice a year.
In future news releases we will give more explicit information about the reliability of the data provided, in particular we will include some guidance in the form of a cautionary note on what figures may or may not be valid to be inferred from our survey data. We are also liaising with Social Science researchers within the University of Kent Cyber Security Centre, to develop more elaborate methodologies that may lead to more insightful and precise results.

About the authors

<INSERT IMAGE.1>
Julio Hernandez-Castro is a Lecturer in the School of Computing, University of Kent. He specialises in Computer Security, with a keen interest in Cybercrime, RFID Security, Steganography & Steganalysis and CAPTCHAs.

<INSERT IMAGE.2>
Eerke Boiten is a Senior Lecturer at the School of Computing of Kent, the leader of the CryptoForma EPSRC Network of Excellence, and the Director of the Kent Interdisciplinary Cyber Security Center.

Resources

Google in-house validation whitepaper on Surveys
http://www.google.com/insights/consumersurveys/static/consumer_surveys_whitepaper_v2.pdf

References

[1] McGuire, M. & Dowling, S. (2013) Cyber crime: A review of the evidence. Summary of key findings and implications. Home Office Research report 75, retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf

[2] Internet Access 2012: Households and individuals. UK: Office for National Statistics. Retrieved September 2013. Available at: http://www.ons.gov.uk/ons/rel/rdit2/internet-access---households-andindividuals/ 2012/stb-internet-access—households-and-individuals--2012.html

[3] Ofcom (2012) Communications Market Report. London: Ofcom. Retrieved from Ofcom, September 2013. Available at: http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/CMR_UK_2012.pdf

[4] HMSO (2010) A Strong Britain in an Age of Uncertainty: The National Security Strategy. London: HMSO.

[5] Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M. J. and Levi, M. (2012) Measuring the cost of cybercrime. Retrieved September 2013. Available at: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

[6] ONS (2012b) Crime Survey for England and Wales, 2011/12 [computer file]. UK: ONS. Retrieved September 2013. Available at: http://www.ons.gov.uk/ons/rel/crimestats/crime-statistics/focus-on-property-crime--2011-12/index.html

[7] Methodological Analysis from the Pew Research Center
http://www.google.com/insights/consumersurveys/pew

[8] Paul Krugman, the Prize Nobel winner, used Surveys for an article at the New York Times
http://krugman.blogs.nytimes.com/2013/08/13/what-people-dont-know-about-the-deficit/?_r=0 and
http://www.nytimes.com/2013/08/16/opinion/krugman-moment-of-truthiness.html?ref=paulkrugman&_r=0

[9] Eli Burzstein's study can be found at
elie.im/blog/security/18-4-of-us-internet-users-got-at-least-one-of-their-account-compromised/

[10] The Elderly as Victims of Crime, Abuse and Neglect. Marianne Pinkerton. Australian Institute of Criminology Trends & Issues, June 1992
http://192.190.66.70/documents/5/7/E/%7B57ED2491-7C7D-498F-A12C-7626D80D6339%7Dti37.pdf

[11] Phishing for Elderly Victims: As the Elderly migrate to the Internet, Fraudulent Schemes Targeting them Follow. Eric L. Carlson. The Elder Law Journal, 2007

[12] Independent coverage by James Vincent: One in five UK citizens have had online accounts hacked on the 26th August 2013
http://www.independent.co.uk/life-style/gadgets-and-tech/news/one-in-five-uk-citizens-have-had-online-accounts-hacked-8784772.html

[13] Guardian coverage by Rupert Jones: Cybercrime hits more than 9 million UK web users on the 23rd August 2013
http://www.theguardian.com/technology/2013/aug/23/cybercrime-hits-nine-million-uk-web-users

[14] The Daily Mail coverage by an anonymous reporter: The scourge of cyber crime: One fifth of Brits have had their e-mail, social network or bank accounts hacked - and some have lost more than £10,000 on the 24th August 2013
http://www.dailymail.co.uk/news/article-2401285/Cyber-crime-1-5-Brits-e-mail-social-network-bank-accounts-hacked.html

[15] TechWorld coverage by John E. Dunn on 27th August: UK online fraud losses higher than realised, University study suggests
http://news.techworld.com/security/3465704/uk-online-fraud-losses-higher-than-realised-university-study-suggests/

[16] ITV coverage: 'Almost one in five Brits' fallen victim to cybercrime on the 23rd August 2013.
http://www.itv.com/news/update/2013-08-23/almost-one-in-five-brits-fallen-victim-to-cybercrime/

[17] Office for National Statistics (ONS) 2011 Census on Age Structure
http://www.ons.gov.uk/ons/rel/census/2011-census/key-statistics-and-quick-statistics-for-local-authorities-in-the-united-kingdom---part-1/rft-ks102uk.xls