IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 22, Issue 10, Ver. 10 (October. 2017) PP 39-44
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Know Thy Enemies

Dr. Marcia Pinheiro
drmarciapinheiro@gmail.com
IICSE University, DE, USA

Abstract: In this essay, we worry about discussing the issue attribution: Who did what to whom? What looks silly and obvious may actually be the worst problem we have, and this is the case here: From stealing computerstoDarknets, we have a range of possibilities that may make attribution impossible, and we must still match those with gravity of cyber attacks (from naivest to most sophisticated). To the side of the investigative authority, we also have a range of possibilities. One of the least exploited ones might be the best investment: Crowdsourcing matched with an improved version of the IBM i2 Analyst's Notebook. We here explore uncommon paths to track marginals and try to make a good case in favor of each one of those. We also talk about a few glitches with the IBM i2 Analyst's Notebook and the paradox of enforcement.

Keywords: Crime, cyber, internet, attribution, attack

Date of Submission: 16-10-2017 Date of acceptance: 27-10-2017

I. INTRODUCTION

It is said that if you know your enemies and know yourself, you willnot be imperiled in a hundred battles; if you do not know yourenemies but do know yourself, you will win one and lose one; if you donot know your enemies nor yourself, you will be imperiled in everysingle battle[1].

We need to know our enemies and ourselves, and therefore their Internet Protocol (IP)[2], computer, ways of acting, and our IP, computer, and ways of acting. We need to draw a Logical Profile(LP) for our historic enemies (intelligence[3]), since we must hold an entire database on those (they are historic), and do whatever we can to get something close to an LP for our not-yet-explored-enough enemies. This is part of the counterintelligence work[3]. We give an example to better explain LP in the next paragraph.

Logical profiles must include attack patterns[4], and it is worth studying this one:Marcia R Pinheiro's[5]acquaintance, EIS, showed her how he could take control of her computer by means of Skype. EIS then acquires a link between him and Skype on our IBM i2 Analyst's Notebook[6] chart. The details of his crimes would be best described through a list of searchable words and self-editing processes (as we type, the system should look for similar reports and prompt us for a match), which are not yet present in i2. Provided the system is refined enough, we can achieve redundancy zero, and that means always singling out the correct perpetrator when the perpetrator is a historic enemy:We search for Skype and EIS would appear in our list of results. We are here talking about a counterintelligence tool that looks completely acceptable, but enforcement could also consider illegal tools. Partisans of this approach (illegal tools) say that the how does not matter[7]. Our stand is described in the next paragraph.

We defend that authorities should not commit crime to solve crime, so that the best solution for the issue attribution is crowdsourcing, special police, and special alarms. We tell you how this paper is organised in the next paragraph.

In this paper, we do not provide a complete solution for the problem attribution in cyber-attacks, but we discuss what can be done at the most basic level (naivest attacks), and we propose solutions that might be seen as innovative for all remaining levels. On the way to that, we discuss the problems with the system IBM i2 Analyst's Notebook.

II. DEVELOPMENT

There are several levels of attack, but we can say that they range from naivest to most sophisticated: Naivest are things like the perpetrator comes, uses our computer, and we catch them doing that. Most sophisticated are things like the perpetrator spoofs[8] Microsoft and Microsoft sends us a criminal update. Most computers would have settings that allow for Microsoft updates to be downloaded and installed, even because that is recommended by the vast majority of the Information Technology (IT) professionals[9]. That would make an attack of the sort we have just described (spoofing then contamination) not be detected. Yet, after we get information about declarations of the own perpetrator to a third party, say via crowdsourcing, perhaps surveys(*a*

Broward County Sheriff has leveraged his 10,000 Facebook friends to successfully track down stolen goods[10]), we can interview this third party, acquire a profile for the perpetrator, and insert it in our databases. Next time we get a report about a similar attack, we consult the databases and that perpetrator will be one of the names that appear in our list of suspects. This is not different from when we investigate serial killing[11]: we get the pattern of the attack, consult our databases, even if that means Googling, and write a list of possible perpetrators. We talk about one intelligence tool, which is firewalls, in the next paragraph.

Naïve attacks can be detected by cheap firewalls or even free ones, say Comodo's[12]. There is a generalized agreement on the Microsoft firewall, however, which is that it does not work[13,14], so that all IT professionals tend to recommend their own firewalls'[15] and turn off Microsoft protections of that sort to avoid conflict. A reasonable firewall lets us know the IP of the perpetrator and the type of attack. The issues involved are that the perpetrator may use the computer of someone else or an IP disguiser. Finding the IP number is not finding the perpetrator in these cases, even though, with it, we could be locating the Internet Service Provider (ISP) and, subsequently, the ISP[16] client that has that IP. If our IP gives us our perpetrator, we ended up with an easy solution. We talk about the not-so-easy ones in the next paragraph.

Certain attacks, located in the middle range, such as real-time hacking, so say when the person uses Skype to take possession of our machine[17], can only be detected via eyesight so far, it seems. In this case, only anti-hacking could take us to the true IP of the perpetrator, but, as we said, in the previous paragraph, the computer might be borrowed, so that we may have to use their built-in camera to get the right perpetrator. We here have the Paradox of Enforcement[18]: Anti-hacking is hacking, and therefore it is the crime we claim to actually be combatting[19]. It does not look reasonable to put such an effort if we are not marginal. Alternatives go from closing the communication interface, so say shutting down Skype, to communicating for longer with the person with the intentions of acquiring more data about them or allowing enforcement to take action. We talk about alternatives that are readily available for enforcement in the next paragraph.

All these might be effective solutions:

1) Crowdsourcing (Collective Intelligence[20]) and investigative tools of the type: We can build a list of LPs, and then make use of perhaps an improved version of IBM i2 Analyst's Notebook to store data for future consultation. IBM i2 Analyst's Notebook can be improved: It seems to have been built from the mind of a programmer, rather than of a systems analyst's, most of the time. A few issues: two files to determine a schema instead of one; possibility of opening a badly saved schema, say with only one file, edit it to the end, and not be able to save it in the two needed files, and, as a consequence, having a schema that cannot be used in practice;incapacity of importing Excel sheets that be not in 1997 format; not being told what the issues are in enough detail to address them (Excel sheet, two files, etc.); not accepting two line titles for links unless we use the mouse (it should accept the same input in both modes); excess of details to the point of confusing the user (date is not simply date; there is date of end of event and others); all that has to do with the schemas seems to be unnecessary and heavy (why not having all schemas together, and selecting elements each time, so that the rest remains dormant or in off or zipped or something? That is better than editing an old schema, saving, and uploading it in a complicated way); there are not many correct ways to connect the balls plus there are no balloons or anything to tell us what to do next, after connecting three balls; and the input card depends on the way we connect (in some configurations, depending on the links, we get fewer entries) the balls[21], but the system does not warn us about that

2) Obliging software developers to install a back-door for enforcement seems to be a really good option[16]: It is light for the authority, light for the developer, and it is effective in terms of protection to the victim. Notwithstanding, *a back door intoanencryptedsystemcannotbe given only to law enforcement and somehow keptfromcriminalsand political despots.Once an entrywayexists, the system is vulnerable. Indeed, purposeful backdoors can lead to less privacy, morevulnerabilities asnew systems interact with past software and even make governments and service providers tantalizing targetsof cybercrime, as they possess the proverbial keys to thekingdom*[22,23]

3) Limiting the size of the encryption key could be an alternative, but that still obliges the authority to break the key and encryption processes are usually reasonable (no excessive force)[16]anyway. We could forbid encryption, as the most radical, such as Theresa May, prime minister of England, propose[23].*A ban on encryption would make it impossible to do anything online that relies on keeping things private, like sending your credit card details or messaging your doctor.Even if governments were willing to sacrifice their citizen's online privacy, any sort of ban would be futile anyway. Anyone with a little technical know-how could write their own code to encrypt and decrypt data. In fact, the code to do so is so small it easily fits on a t-shirt*[23]

4) Authority could oblige developers to disclose keys whenever they are running an official investigation. *Obligation to disclose keys upon request(investigations) is a good option for those who like dependent authorities: Perhaps in this way we havemorecontrol over them. Human lives may depend on that*

information beingdisclosed however: Having to request things andcounting on the collaboration of others may mean death or lifetime injury[16]

5) Whoever has a computer can make use of a special alarm button, and the button can be part of their installation package: Upon noticing thatwe may be suffering crime, we press the button, which works more or less like the red telephone between the White House and the Kremlin[24]. We could get special training material or even training to learn how to deal with certain situations, so say entertaining the perpetrator through Skype until enforcement gets them
6) To have number 5 in this list, the government would have to create a special police force, which would be a force that investigates and deals with cyber crime with exclusivity[25]. They must consider the Paradox of Enforcement in this case[16,26].The special police is necessary because of the specialisation demanded, but also to avoid simply oppressing people[27]. Australia seems to be on the way to that, since ACORN (Australian Cybercrime Online Reporting Network)[28] could be told to be a start. India is about to create their cyber police stations[29]. Most of the important countries have cyber units or teams inside of their federal police system: That is the case with the United States[30], Australia[31], and Russia[32].

In any case, it would not be necessary for security services to break encryption for everyone in order to read WhatsApp messages on a suspect's phone. Last year, the government passed the Investigatory Powers Act – also known as the "Snooper's Charter" – which allows security services to directly access people's devices when they have a warrant to do so. "If they identify a person of interest, they can hack the device and read what's on it," says Bernal. This means they wouldn't have to crack encryption to intercept the information[33].This was in England[33]. The problem with this solution is, once more, the paradox of enforcement: Committing crime to solve crime. Enforcement does get authorisation from courts to perform searches inside of private residencies. Perhaps this is a similar situation. As long as the reasons for the violation of privacy in this case have the same strength as in the other cases, then it should be OK: No information source should be treated in a more restrictive way when it comes to criminal investigations.In the next paragraph, we talk about breaking into residencies.

In what comes to private residencies, we have that *the Supreme Court has upheld forced entries after the cops only waited 15-20 seconds. Courts don't generally require the police to wait for extended periods because of concerns that defendants will try to dispose of evidence before the police enter. If the police do not knock and announce as required, most courts will not automatically find that the police entry and search were illegal (*there is still the exigent cases, such as domestic dispute and threats). *Instead, they will just consider it a "factor" in determining whether the forced entry in your home and subsequent search were reasonable*[34]. The just-quoted text comes from an American organisation that gives advice for free in legal matters[35]. Police normally seize the cyber item to which the object of their claimed hacking connects, so that there is no risk of disposal of evidence. If one cannot get the courts to agree with them breaking into private residencies unless there are concerns with disposal, then we should not allow enforcement to break into computers, external hard disks, and alike material unless the owner allows them in. The problem is once more the enforcement paradox. In the next paragraph, we talk about the Australian case.

In Australia, it is only in cases such as owner's permission, reasonable belief by officer that someone will commit or has committed a serious offence plus necessity of going inside of the property to arrest that person, stopping a breach of peace (fight and others), stopping a breach of an intervention order or family violence safety notice, non-obedience, in a family violence matter, to police orders, reasonable belief that someone has assaulted or threatened to assault a family member, chasing a run-away from prison or custody, and possession of warrant to arrest someone on the property, that the courts would forgive the authority for breaking in[36]. Therefore, there could be no reason for the courts to allow investigative authorities to break into cyber items in Australia instead of at most authorising seizure.

III. CONCLUSIONS

We could classify attacks to computers via hacking as something between naïve, so say someone taking physical possession of our machine, going to our place and doing it from there, and sophisticated, so say someone spoofing Microsoft servers and sending a malicious program to our machine in order to take control of it. Whilst for naïve attacks we could have the usual enforcement strategies, so say internal CCTV system detecting the perpetrator and us proving he did it via recorded images, for sophisticated attacks, we would have to be using something like crowdsourcing intelligence or a special alarm. If we have the alarm, then it is easy to have the policemen as collaborators. If we do not have it, then it is possible that help is only in Academia.

An obvious way out of being hacked and still determining at least the perpetrator's IP is anti-hacking, but we then get the Enforcement Paradox (to solve crime, we have to commit crime). Enforcement should refrain from doing that, so that strategies such as keeping the perpetrator interacting with the victim for long enough, perhaps mocking around in Skype, and crowdsourcing, or even backdoor, should be preferred to anti-hacking. Anti-hacking is hacking, and therefore it is crime. Firewalls seem to do a good job at the naïve and even middle range levels of attack, but the Microsoft firewall is really not recommended.

We should have a Logical Profile (LP) for each one of our historic enemies: names, patterns, and things like that. We could then actually play with the IBM i2 Analyst's Notebook to try to work out connections and involvement in crime of a particular subject after cataloguing those. With a more developed system, we could determine even more things by using simple search tools. I2 seems to need a lot of improvements. We should also do whatever we can to have the closest thing as possible to an LP for our not-yet-explored-enough enemies.

When people receive their Internet package, they could be given the option to install an alarm button through which they can contact the authorities in no time (just pressing upon suspecting that they are suffering crime). They could be trained to learn how to properly react to a cyber attack, so that things are more effective in what comes to enforcement. The government should create a special police force, specialised in cyber issues, so that its agents could be investigating patterns, motivations, profiles, and all else, and, later on, passing the results of the investigation to the usual police force or acting themselves also in the realm of the courts and incarceration.

Investigative authorities should hack in situations that equate the situations that allow them to break into private residencies only: They should seize the cyber item containing the information they need and seek the perpetrator's authorisation almost all the time, since it is usually only when there is risk of disposal that the court forgives the authority for breaking in in the United States (but we still have the exigent cases, such as domestic dispute, and hearing a threat), and only in cases such as owner's permission, reasonable belief by officer that someone will commit or has committed a serious offence plus necessity of going inside of the property to arrest that person, stopping a breach of peace (fight and others), stopping a breach of an intervention order or family violence safety notice, non-obedience, in a family violence matter, to police orders, reasonable belief that someone has assaulted or threatened to assault a family member, chasing a run-away from prison or custody, and possession of warrant to arrest someone in the property, that Australia forgives the authority for breaking in.

Encryption is a necessary element in the Virtual World[37] and therefore we cannot support Theresa May's thoughts and banish it. Limiting encryption keys also does not sound reasonable because manufacturers have no interest in investing in more encryption than what is needed. Asking vendors to provide encryption keys sounds dangerous, since others would have those. A back-door for enforcement fits the same category of concerns.

Authorities should not have to request that developers disclose keys because that consumes resources that are not always available: A person may die between the time they stop to get a court order and the time the developer discloses keys. The developer may never do that.

REFERENCES

[1] Irwin, Angela 2017 'Week 2 Knowing Ourselves and Knowing our Enemies': Macquarie University. Available at: http://ilearn.mq.edu.au/pluginfile.php/4583694/mod_resource/content/11/PICT849_Lecture 2_S2_2016_Knowing Ourselves and Knowing our Enemies.pdf Accessed 9.10.2017

[2] Russ Smith of Consumer.Net 1997 'IP Address: Your Internet Identity' Available at: https://www.ntia.doc.gov/legacy/ntiahome/privacy/files/smith.htm Accessed 7.9.2017

[3] Celine 2017 'Differences Between Intelligence and Counterintelligence' *DifferenceBetween.net* Available at: http://www.differencebetween.net/science/differences-between-intelligence-and-counterintelligence/ Accessed 11.10.2017

[4] Varied 2015 *Crime Patterns in Time and Space: The Dynamics of Crime Opportunities in Urban Areas*A Newton & M Felson eds. Springer Nature Available at: https://www.springeropen.com/collections/cpts Accessed 9.10.2017

[5] Personal communications

[6] IBM 2017 'IBM i2 Analyst's Notebook' Available at: https://www.ibm.com/us-en/marketplace/analysts-notebook Accessed 29.9.2017

[7] M. E. Musings 'The Lost Traveller' Available at: http://www.ericfeng.com/home/downloads/TheLostTraveller-pleasesharethis.pdf Accessed 12.10.2017

[8] Syngress. (2002).*Scene of the Cybercrime: Computer Forensics Handbook*.Syngress.Page 298. Retrieved from https://books.google.com.au/books?id=BLjomivi1asC&dq=another+ip+was+used+cyber+crime&source=gbs_navlinks_s

[9] Lincoln Spector 2012 'Should I Turn Off Automatic Updates?'*PCWorld from IDG, Answer Line* Available at: https://www.pcworld.com/article/254647/should_i_turn_off_automatic_updates_.html Accessed 9.10.2017

[10] Pinheiro, MR 2017 *Report on Remote Access Scan that Happened in 2017 in the Sunshine Coast, Episode Catalogued as CT21* Sydney: Macquarie University

[11] Federal Bureau of Investigation 2017 'Serial Murder' *Reports and Publications* Available at: https://www.fbi.gov/stats-services/publications/serial-murder#six Accessed 9.10.2017

[12] Group, Comodo 2017 'Comodo Creating Trust Online' Available at: https://www.comodo.com/home/internet-security/firewall.php Accessed 9.10.2017

[13] Anon 2009 'Faster after Disable Windows Firewall....' *Wilders Security Forums* Available at: https://www.wilderssecurity.com/threads/faster-after-disable-windows-firewall.247136/ Accessed 9.10.2017

[14] Rubenking, Neil J 2008 'Security in Windows 7: Firewall and Networking' *PCMag.com* Available at: https://www.pcmag.com/article2/0,2817,2335235,00.asp Accessed 9.10.2017

[15] Markus, Henry S 2000 'Home PC Firewall Guide' Available at: http://www.firewallguide.com/software.htm#More_ Accessed 9.10.2017

[16] Pinheiro, MR 2017 'VPNs and Pedophilia: An Issue or a Solution?' *IOSR Journal Of Humanities And Social Science* 22/10:39–45

[17] Kumar, Mohit 2017 'Critical Skype Bug Lets Hackers Remotely Execute Malicious Code' *The Hacker News* Available at: https://thehackernews.com/2017/06/skype-crash-bug.html Accessed 10.10.2017

[18] Ernest F. Roberts 1961 'No Title' *Journal of Criminal Law and Criminology* 52/2. Available at: http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=5027&context=jclc Accessed 10.10.2017

[19] Pinheiro, Marcia R 2017 'Protecting Australia against Cyberterrorism' *IOSR Journal of Humanities and Social Sciences* 22/9, version 15:01–06. Available at: https://www.researchgate.net/publication/320064730_Protecting_Australia_against_Cyberterrorism Accessed 10.10.2017

[20] [20]Buecheler, Thierry et al. 2010 'Crowdsourcing, Open Innovation and Collective Intelligence in the Scientific Method: A Research Agenda and Operational Framework' in 2010 *Alife XII Conference* Odense

[21] Pinheiro, MR Personal Notes.Irwin, Angela 2017 'PICT849 Cyber Policing and Intelligence'. Available at: http://ilearn.mq.edu.au/course/view.php?id=28700. Accessed 10.10.2017

[22] Eric Jardine 2015 *The Dark Web Dilemma: Tor, Anonymity and Online Policing*. Available at: https://www.cigionline.org/sites/default/files/no.21_1.pdf. Accessed 11.10.2017

[23] Revell, Timothy 2017 'Theresa May's Repeated Calls to Ban Encryption Still Won't Work' *New Scientist* Available at: https://www.newscientist.com/article/2133644-theresa-mays-repeated-calls-to-ban-encryption-still-wont-work/ Accessed 12.10.2017

[24] Bender, Bryan 2015 'The Hotline to Moscow Goes Cold' *Politico* Available at: http://www.politico.com/story/2015/10/white-house-moscow-hotline-214398 Accessed 11.10.2017

[25] Hawthorne, Kyle 2017 'Activity: Implications of Darknet Cybercrime for Policing' *iLearn* Available at: http://ilearn.mq.edu.au/mod/forum/discuss.php?d=961707 Accessed 11.10.2017

[26] Pinheiro, MR 2017 'Activity: Implications of Darknet Cybercrime for Policing' *iLearn* Available at: http://ilearn.mq.edu.au/mod/forum/discuss.php?d=961707 Accessed 11.10.2017

[27] Pinheiro, MR 2017 'Activity: Darknet, Why Worry?' *iLearn* Available at: http://ilearn.mq.edu.au/mod/forum/discuss.php?d=962495 Accessed 11.10.2017

[28] Australian government 2017 'ACORN: Australian Cybercrime Online Reporting Network' Available at: https://www.acorn.gov.au/ Accessed 12.10.2017

[29] Dna, Ashish Mehta 2010 'Cyber Police Station to Come Up in Jaipur' *NDTV Convergence* Available at: https://www.ndtv.com/jaipur-news/cyber-police-station-to-come-up-in-jaipur-442142 Accessed 12.10.2017

[30] US government 2017 'What We Investigate' Available at: https://www.fbi.gov/investigate/cyber Accessed 12.10.2017

[31] Australian Federal Police 2017 'Cybercrime' Available at: https://www.afp.gov.au/what-we-do/crime-types/cybercrime Accessed 12.10.2017

[32] Meduza 2017 'One of Russia's Top Cybercrimes Police Units Is Now Under New Management' Available at: https://meduza.io/en/news/2017/07/28/one-of-russia-s-top-cybercrimes-police-units-is-now-under-new-management Accessed 12.10.2017

[33] Revell, Timothy 2017 'Why Breaking Encryption Is a Bad Idea that Could Never Work' *New Scientist* Available at: https://www.newscientist.com/article/2125895-why-breaking-encryption-is-a-bad-idea-that-could-never-work/ Accessed 12.10.2017

[34] FreeAdvice staff 1995 ‘Can the Cops Break Down my Door to Enter my Home?’ *FreeAdvice Legal* Available at: https://criminal-law.freeadvice.com/criminal-law/arrests_and_searches/police-break-door.htm Accessed 12.10.2017

[35] FreeAdvicel 1995 ‘About FreeAdvice.com’ *FreeAdviceLegal* Available at: https://www.freeadvice.com/company/aboutus.htm Accessed 12.10.2017

[36] Victoria Legal Aid 2015 ‘Police Powers: Your Rights in Victoria’ Available at: https://www.legalaid.vic.gov.au/sites/www.legalaid.vic.gov.au/files/vla-resource-police-powers-your-rights-in-victoria.pdf Accessed 12.10.2017

[37] Techopedia Inc. 2017 ‘Virtual World’ *Techopedia* Available at: https://www.techopedia.com/definition/25604/virtual-world Accessed 13.10.2017

Dr. Marcia Pinheiro. “Know Thy Enemies.” IOSR Journal Of Humanities And Social Science (IOSR-JHSS) , vol. 22, no. 10, 2017, pp. 39–44.