Catch Me If You Can: Cyber Anonymity

David M. Rohret, Michael E. Kraft

Computer Sciences Corporation, Inc.
Sr. Prin. Systems Engineer
Email: drohret@ieee.org

Computer Sciences Corporation, Inc.
Network Security Engineer
Email: mkraft5@csc.com

Abstract

Advances in network security and litigation have empowered and enabled corporations to conduct Internet and desktop surveillance on their employees and customers, while Governments have spent billions to monitor cyberspace to include entering agreements with corporations to provide surveillance data on adversarial groups, competitors, and citizenry (Reuters, 2010). Although the initial intent of network and Internet monitoring may be honourable; terrorists, hackers, and cyber-criminals already have access to the necessary tools and methodologies to continue in their activities unabated. This paper will demonstrate a step-by-step case study using a 'paranoid' approach to remaining anonymous using only open-source tools.

Keywords: Anonymity, Network, Internet Surveillance, Remailer, Hacker, Big Brother

Terms Defined

The terms Internet anonymity, and the abstract or hypothetical optimum of remaining anonymous, have differing definitions based on the 'completeness' of anonymity desired. In several definitions 'anonymous', is simply remaining obscure (Answers.com, 2010), and not necessarily completely hidden from site. In other definitions, anonymous refers to remaining nameless, without shape or form (Worldnet 2010), and this is the definition the authors will use throughout this paper. This theme also extends to other terms that describe deception, the destruction of data or misdirection; specifically, the completeness of the action being described. The word 'government' will also be used in a manner that includes all government entities, including law enforcement, military, and intelligence agencies.

Overview

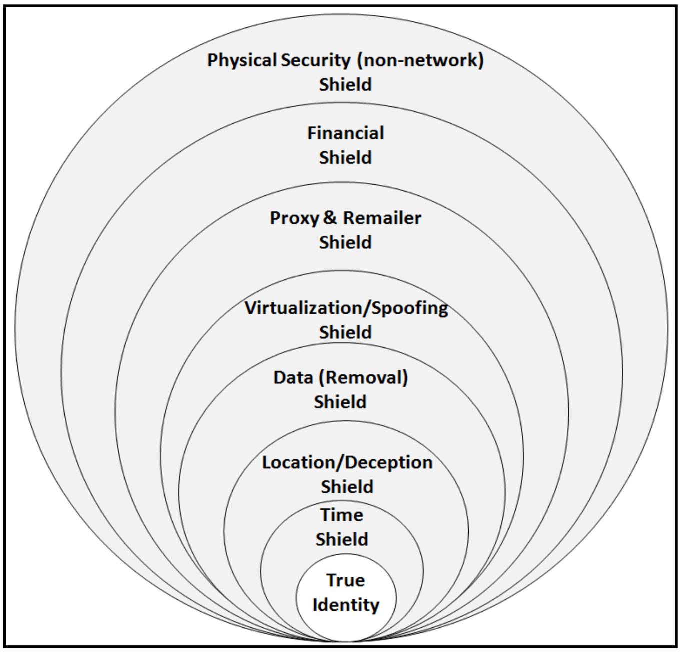
Network-centric red teams are charged with emulating known adversaries and hackers (remote and insider threats) using, for the most part, only open-source and publically accessible tools and software. Unlike penetration testers, who use exploits to validate vulnerabilities, red teams are responsible for viewing networks or systems from every angle to defeat defences in place. This will include, but is not limited to, physical security, biometrics, social engineering, and of course, preventing the blue team from assigning attribution to the red teams actions. In this type of security stress-test a client is able to fully realize their systems security posture, which encompasses much more than a vulnerability scan and penetration test.

ISSN 1445-3312 print/ISSN 1445-3347 online

Governments and corporations have realized the advantages of communications and data transfers via the Internet for economical and defensive purposes. They have also realized the dangers and costs of cyber crimes, malicious hacking, espionage, and cyber warfare; developing new technologies and implementing new legislation to defend networks and to trace/track attacks to their electronic point of origin (EPO). Without verification and validation courts will not convict and governments are unwilling to counter attack as clear attribution cannot be assigned. In order to remain anonymous or assign blame to another party, the authors routinely use the Praestigiae Cone (Rohret & Jett, 2009) shown in Figure 1. The Praestigiae Cone can be visualized as seven protective layers (cone architecture) used in multiple steps to shield the hacker, adversary, or citizen operating from a safe vantage point. The organization or individual attempting to identify what the shields are hiding can attack any of them at one time, but cannot move from one layer to the next without first solving the initial 'who-is' puzzle for the one they have identified. Making the task of identifying the actual user's identity more difficult in each shield is time-sensitive; creating a fast moving defensive environment that is held hostage to an adversary's (or users) schedule.

As difficult as it is for law enforcement and government agencies to crack all seven layers, it only takes one mistake or missed-step by an adversary or hacker to allow investigators to see their true identity. Therefore, the authors have provided a brief description of known capabilities to establish the requirement for an adversary to take the seemingly paranoid precautions identified later in this paper to remain anonymous.

Figure 1. The Praestigiae Cone is used to hid and deceive one from those trying to identify the original source of an attack or network traffic (Rohret & Jett, 2009


Physical Security (non-network) Shield
Financial Shield
Proxy & Remailer Shield
Virtualization/Spoofing Shield
Data (Removal) Shield
Location/Deception Shield
Time Shield
True Identity

Identifying and Tracking Internet Users

"...the FBI successfully infected the anonymous source's computer, and they soon discovered his identity" (Begun, 2009).

In order to quantify the actions taken to remain anonymous we must first identify the many ways an individual or group can be located, tracked, and discovered. By no means are the methods described below solely used for cyber crimes or cyber warfare, but they are a major part of a government's arsenal in fighting cyber crime and dissidents. Because there are so many different tools and techniques used by different governments and agencies, the authors have generalized techniques using specific examples to represent the greater capabilities. This brief overview will help to demonstrate why a paranoid approach is required to protect an anonymous identity on the Internet.

Trojans, Beacons, and Worms

The above quote from Daniel Begun illustrates one way to identify illegal media downloads or snoopy hackers. The process is as easy as providing interesting material on known download sites with embedded Trojans or beacons that notify law enforcement of the violation. Although effective, it's difficult for government agencies to target specific groups or individual violators as this process is more of a reverse phishing expedition. For targeting specific groups such as cyber criminals or adversarial governments, similar techniques would be used with live data or in a well-designed honeypot that seemingly held the type of data the targeted group would maintain on their site. The music industry has had minor successes using this technique (Associated Press, 2005).

Financial Transactions

Financial transactions can easily be associated with an individual anywhere they take place. For an international economy to work, governments and corporations, often at odds with one-another, must work together to prevent crimes that threaten markets and currencies. Because the world has rapidly become digitized, credit cards, Internet paying services, and smart phone purchases allow anyone with a bank account to be a consumer. Furthermore, most businesses and banks now utilize video surveillance at the point of transaction creating a scenario where even cash purchases of a serial numbered commodity or a financial document can lead investigators to a digital picture of the perpetrator. The United States agency, *The Financial Crimes Enforcement Network* (FinCEN) was established in 1990 and is considered the leading expert in solving crimes involving financial transactions, to include cyber-crimes (Kimery, 2010; FinCEN, 2010).

Digital and Cellular Communications

"It's time for you to get some new cell phones, quick," was the warning given to Brian Ross and his ABC News investigation team (Ross, 2006) by someone they considered an NSA insider. This older news story describes an agency leak that identified how intelligence agencies, (and presumably law enforcement agencies) are able to track individuals using telecommunications for activities they (the agency) deem interesting or counter to national security. Radio Frequency (RF) triangulation to pin-point locations is also possible with the use of good spectrum analyzers and a direction finder. This applies to 802.11, 802.16, and other Internet Protocol (IP) over radio and wireless standards.

Tracking Internet Traffic

The most common method of identifying malicious Internet activity and attempting to identify the culprit is through network and Internet surveillance. Intrusion detection systems, intrusion prevention systems, intelligent and stateful firewalls, packet sniffers, etc, provide network administrators powerful tools for identifying attack signatures and sophisticated pattern analysis' that help investigators attribute an attack or malicious actions to a specific group or individual. This is not to say they know the actual identity of the group or individuals involved, but rather, they can match patterns of attacks or actions with enough confidence to suggest that the same perpetrators were involved. These capabilities have become more precise in recent years as corporations and governments cooperate in sharing information and sensor data. For example, the marriage between the search engine giant Google and the NSA made headlines sending shock waves through the Internet community creating worries that anyone can be ‘spied’ on at any time (Reuters, 2010). An adversary or malicious hacker must also assume international arrangements and agreements have been implemented providing worldwide coverage and tracing capabilities.

Computer Forensics

Possession of a suspect’s computer is the golden egg for investigators. The term computer forensics, for use in this paper, refers to identifying incriminating evidence on the suspects system or a storage device used by the suspect. Entire computer laboratories are dedicated to forensic analysis for identifying incriminating evidence; ranging from simple low-tech techniques to highly sophisticated electron interferometry. An example of a low-tech analysis would consist of the capture of a system that is still running and accessible; whereas electron interferometry involves reading open and closed memory gates on a system’s memory at temperatures below negative 60 Celsius, even if the system has been shut down for several minutes (Vourdas & Sanders, 1998).

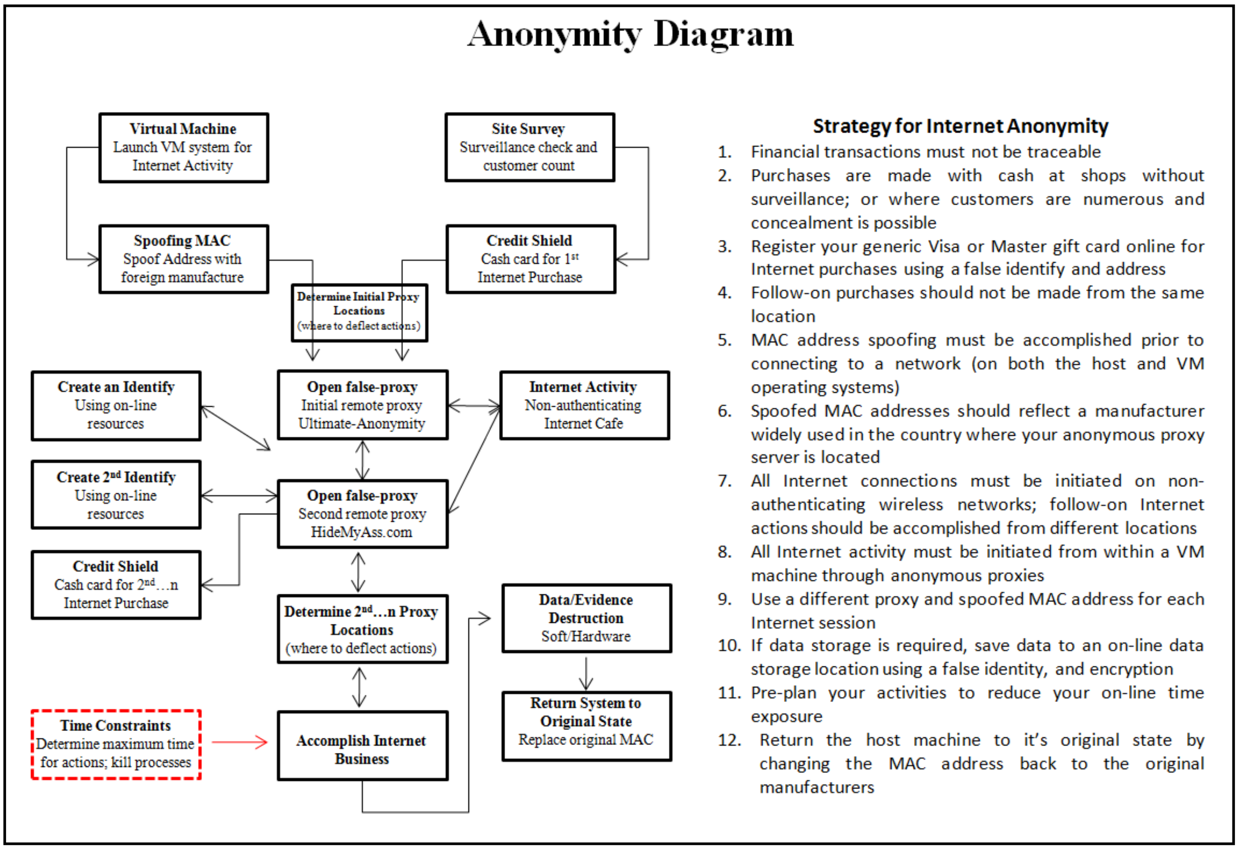
Physical Investigations

‘Feet’ on the ground to identify patterns and locations are part of the final stage of an investigation to identify and/or catch a suspect. This includes using video surveillance from Internet cafes frequented by the suspect or an old fashioned stake-out to catch them in the act. Cyber crime investigations have become common and can be high profile, prompting law enforcement agencies to allocate significant resources to solve cases, preventing attacks and data theft.

A Paranoid Approach to Remaining Anonymous

Why a paranoid approach to anonymity? Governments, adversaries, corporations, cyber criminals, even cheating spouses require a repeatable process they can employ to accomplish sensitive activities across the World Wide Web without detection or retribution. In a recent article prepared for the North Atlantic Treaty Organization (NATO) Parliamentary Assembly (Myrli, 2010) the cost of cyber crimes to governments and corporations is reported to be over US $100B annually. In response to cyber crime, governments and corporations spend billions more on technology and methodologies to identify and track cyber criminals (Fenwick, 2010). Not only have governments increased expenditures and resources to combat cyber crime, there is now unprecedented cooperation among governments and corporations to provide data and information sharing to identify and/or capture offenders (Golubev, 2005). Therefore, for an adversary or cyber criminal to successfully use the internet for nefarious reasons, and remain anonymous, they must take a holistic view of the security available to their intended targets. That is to say, they must assume each capability is available and successfully deployed. Just as a network security officer does not have the luxury of only defending against some or most of the vulnerabilities on their network, a cyber criminal or cyber warrior cannot depend on a law enforcement agency to only use some of the methods described in section 3 to identify who committed a cyber crime.

This paper is the result of research into adversarial capabilities in cyber warfare, specifically, how a network-centric red team, acting as the adversary, would prevent positive attribution after conducting network reconnaissance or an attack. The following case study reflects precautions and actions used to create the shields identified in the Praestigiae Cone in Figure 1; using combinations of publically available technology, services, and research. Figure 2 outlines the process of achieving the seven shields, resulting in complete anonymity. The details are explained using a scenario based on an actual case involving a red team assessment on an enterprise network.


Anonymity Diagram
Virtual Machine
Launch VM system for Internet Activity
Site Survey
Surveillance check and customer count
Spoofing MAC
Spoof Address with foreign manufacture
Credit Shield
Cash card for 1st Internet Purchase
Determine Initial Proxy Locations
(where to deflect actions)
Create an Identify
Using on-line resources
Open false-proxy
Initial remote proxy Ultimate-Anonymity
Internet Activity
Non-authenticating Internet Cafe
Create 2nd Identify
Using on-line resources
Open false-proxy
Second remote proxy HideMyAss.com
Credit Shield
Cash card for 2nd…n Internet Purchase
Determine 2nd…n Proxy Locations
(where to deflect actions)
Data/Evidence Destruction
Soft/Hardware
Return System to Original State
Replace original MAC
Time Constraints
Determine maximum time for actions; kill processes
Accomplish Internet Business

Strategy for Internet Anonymity

1. Financial transactions must not be traceable
2. Purchases are made with cash at shops without surveillance; or where customers are numerous and concealment is possible
3. Register your generic Visa or Master gift card online for Internet purchases using a false identify and address
4. Follow-on purchases should not be made from the same location
5. MAC address spoofing must be accomplished prior to connecting to a network (on both the host and VM operating systems)
6. Spoofed MAC addresses should reflect a manufacturer widely used in the country where your anonymous proxy server is located
7. All Internet connections must be initiated on non-authenticating wireless networks; follow-on Internet actions should be accomplished from different locations
8. All Internet activity must be initiated from within a VM machine through anonymous proxies
9. Use a different proxy and spoofed MAC address for each Internet session
10. If data storage is required, save data to an on-line data storage location using a false identity, and encryption
11. Pre-plan your activities to reduce your on-line time exposure
12. Return the host machine to it's original state by changing the MAC address back to the original manufacturers

Figure 2. A quick view of the process required to remain anonymous

Scenario

The red team's goal was to emulate a hackers capability to remotely identify and disable an automated network-controlled surveillance system that included wireless video, fence and ground sensors, autonomous vehicle sentries, and network security; without being identified as the adversary. The red team assumed all networks were monitored and Internet service providers, search engines, and even proxy services would provide information to authorities in a timely manner. Each action taken by the red team, and all services purchased and used, are publically available and legal. The following steps provided Internet and network anonymity, allowing the red team to accomplish its mission without allowing security managers to assign attribution to the attack.

Physical Security and Financial Shields

The red team's first step was to build laptop systems specifically for their requirement. This included downloading free VM software for the installation of multiple operating systems. By using freely distributed VM software, the red team was able to avoid having information identifying their use of VM software through registration services or processes (Oracle, 2010). Operating systems already configured for use in a VM environment were also available for public download and each download and installation was accomplished from a non-authenticating Internet cafe. Two anonymity proxy services were required and were purchased using two separate MasterCard gift cards; paid for with cash separately at two convenience stores that were found not to be using video surveillance.

Virtualization and Spoofing Shields

Creating a system providing protection against evidence retrieval is vital for a red team emulating adversarial techniques. Virtual operating systems provide developers and administrators the capability to create instances of an entire network for testing and evaluation, similarly, cyber criminals and adversaries use virtual networks for pre-exploit testing and as disposable systems following an attack or exploitation. If all other layers of anonymity fail, it is imperative that attribution cannot be determined from information, logs, or data found on the attackers host system. In this case study, our red team used multiple pre-built virtual machines on re-usable host systems, creating temporary and disposable attack platforms. Continuing our paranoid approach, we used open-source resources to download and install the following files using a false identify:

- Virtual Machine Hosting Software: The authors downloaded Microsoft's Virtual PC 2007 software. With Microsoft Virtual PC 2007, you can create and run one or more virtual machines (each with its own operating system) on a single computer. This provides you with the flexibility to use different operating systems on a single host platform (Microsoft, 2010).

- Virtual Machine Images: Virtual operating system images can be obtained in several ways; they can be loaded directly into the VM system (using un-registered software) or downloaded already built. Windows XP or Vista VM images are available at no cost from the National Institute of Standards and Technology (NIST, 2010), and a Linux distribution was obtained from an open-source location (Back|Track-Linux.org, 2010). Hacker forums, how-to publications, and trial downloads also provide sources for acquiring operating systems to populate your virtual machines without a financial or registration trail.

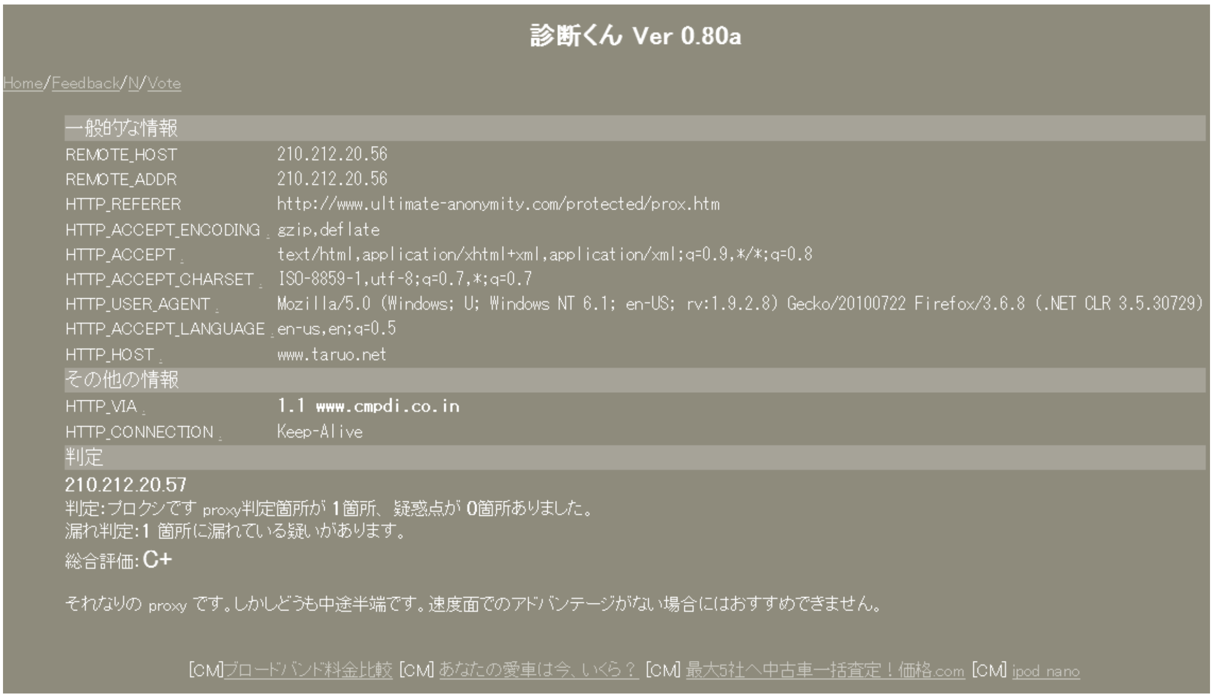
- Host and VM System MAC Spoofing: Every network interface card (NIC) is assigned a unique serial number called a media access control (MAC) address. An investigator or network security officer can trace a MAC address in a similar way that an IP address is traced by simply using a packet sniffing tool, like Wireshark, and filtering traffic by the MAC. Many novice hackers or careless cyber criminals will neglect spoofing MAC addresses prior to an attack, and just as often, forget to change them back to the original following an attack. In the red team's quest to eliminate any trace of their attacking systems on their host platforms, they used publically available freeware called Spoofmenow.exe (SourceForge, 2010) to change the MAC addresses of both the VM system and their host platforms. Once the red teams actions were completed (for each session), they returned the host system to the original MAC address and deleted the VM system. This action would prevent investigators from identifying the host system as the computer used for an attack, even if no other evidence was available. It was necessary to change the VM system's MAC address for two reasons; first, changing the MAC address to a manufacturer that reflected the location of the proxy server used for the attack, created a better deception of where the attack originated from. Secondly, and just as importantly, to avoid identifying the system used as a VM system. Most vulnerability scanners will identify the MAC address of a VM system as a virtual machine.

Proxy and Remailer Shields

The side effect of increased capabilities by law enforcement is an increase in on-line services to help defeat law enforcement capabilities, such as anonymous proxies and remailers. Proxies are servers that act as go-betweens, making requests for data on behalf of clients. A proxy receives a 'request' for a file, website, or other resource from a client, connects to the remote site, and obtains the information sending it back to the client. Remote proxies can allow you to surf the Web privately without being monitored and are widely used by individuals who download copyrighted media or those who circumvent network security measures in order to view blocked Websites(Hazel Morgan, 2010).

An anonymous remailer is an email service which receives client messages (with embedded instructions on where to send them) and then forwards the messages without revealing where they originally came from. By not maintaining a users list or a log of the addresses their messages were sent to, a remailer can ensure any message which has been forwarded leaves no internal information behind that could be used to break identity confidentiality(Wikipedia, 2010).

Two proxy services were used by the red team; the first proxy service, Ultimate-Anonymity (Ultimate-Anonymity, 2010), was purchased using the first cash gift card and a false identity at a non-authenticating wireless cafe. Red team members quickly set their proxy location to a proxy in India via an encrypted VPN. Using an on-line IP lookup after starting the anonymous proxy service the red team confirmed they were seen on the Internet as originating from the location in India, as shown in Figure 3. The second proxy service, HideMyAss.com (HMA), was purchased using the second gift card from another non-authenticating wireless cafe while connected through the first proxy, using a different false identity (HideMyAss.com, 2010). HMA's user-friendly interface allowed the red team to choose multiple proxies in the Netherlands and Russia, changing IP addresses every 10 minutes.



```
診断くん Ver 0.80a

Home/Feedback/N/Vote

一般的な情報
REMOTE_HOST               210.212.20.56
REMOTE_ADDR               210.212.20.56
HTTP_REFERER              http://www.ultimate-anonymity.com/protected/prox.htm
HTTP_ACCEPT_ENCODING      gzip,deflate
HTTP_ACCEPT               text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_CHARSET       ISO-8859-1,utf-8;q=0.7,*;q=0.7
HTTP_USER_AGENT           Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.8) Gecko/20100722 Firefox/3.6.8 (.NET CLR 3.5.30729)
HTTP_ACCEPT_LANGUAGE      en-us,en;q=0.5
HTTP_HOST                 www.taruo.net
その他の情報
HTTP_VIA                  1.1 www.cmpdi.co.in
HTTP_CONNECTION           Keep-Alive
判定
210.212.20.57
判定:プロクシです proxy判定箇所が 1箇所、疑惑点が 0箇所ありました。
漏れ判定:1 箇所に漏れている疑いがあります。
総合評価:C+

それなりの proxy です。しかしどうも中途半端です。速度面でのアドバンテージがない場合にはおすすめできません。

[CM]ブロードバンド料金比較 [CM] あなたの愛車は今、いくら？ [CM] 最大5社へ中古車一括査定！価格.com [CM] ipod nano
```

Figure 3. Once connected to a proxy server operated by Ultimate-Anonymity in India, as demonstrated by this screen shot of an IP lookup, the red team was able to purchase a second proxy service through the first encrypted anonymous proxy service; allowing a deeper level of anonymity than before.

Although anonymous proxy services advertise they do not maintain user logs and delete user information in a timely manner, it was assumed by the red team the anonymous proxy services would cooperate with investigators. Therefore the red team would not use each proxy service for more than one session, repeating the process for each follow-on action, using different proxy locations, session locations, and new identities.

Data (Evidence) Removal Shield

There are various levels of paranoia which will dictate how one might try and destroy the computer evidence. One might have little paranoia and decide to just delete the virtual machine from the computer. A more nervous approach might include using a disk cleaner wiping a hard drive in accordance with the DoD 5220.22-M standard (usaid.gov, 2010), which features multiple overwrites of random characters. Open source programs like Darik's Boot and Nuke (DBAN) is a self-contained boot disk that securely wipes the hard disks of most computers. DBAN will automatically and completely delete the contents of any hard disk that it can detect, which makes it an appropriate utility for bulk or emergency data destruction (Sourceforge, 2010). Lastly, after completing disk scrubbing, the extreme case of paranoia might include destroying the computer by physically damaging the hard drives and memory.

Location/Deception and Time Shields

As discussed earlier, time is the adversary's or cyber criminal's ally. The end goal is to accomplish an action without being identified or having it attributed to your team. By using a disciplined approach and restricting the amount of time each session is executed, each proxy service is used, and an identity is held, investigators will be kept busy allocating resources to identify computers and users that no longer exist. Even if investigators are able to eventually locate one of the EPOs, the perpetrator will have completed their mission and moved onto a new location with a new identity. Solving computer crimes requires resources and specific skill sets that are not always readily available even to the most advanced cyber crime organizations. By remaining difficult to trace and providing multiple targets that are easily erased, authorities will not be able to focus their efforts in a timely enough manner to locate and positively identify the offender.

The key component of keeping time as your ally is preventing a positive identification of your location. By location the authors refer to both the physical location of the attacker and their perceived location. Earlier we discussed the use of multiple non-authenticating Internet cafes and the use of multiple foreign proxies, one tunneled through the other, but there are other methods to hide your true locations; the use of third-party hackers and on-line resources that provide exploitable computers. Third-party hacking services are available and can be purchased using a gift card while logged onto a proxy service. Furio Gaming (Furio Gaming, 2010) is one such service that will either hack a system for you or will provide you the tools to do so. This service represents itself as a gaming and hacking company and is located in a foreign country providing a layer of anonymity in itself. Other on-line services, such as Shodanhq.com (SHODAN, 2010), provide an easy-to-use research tool allowing hackers to identify systems worldwide that are exploitable in every country. By identifying and exploiting a vulnerable system in a country that may not cooperate with the country you are working in, a cyber criminal can execute their objectives with little fear of attribution. Other methods for individuals or organizations with greater resources would be to setup and configure their own anonymous proxies in countries and locations that have liberal or non-existent cyber laws. For large scale cyber attacks or highly profitable schemes, this method may be more applicable and more robust.

Summary

The inexpensive solution to cyber anonymity outlined in this case study can easily be implemented with minimal resources and without expert skill levels. Movies and television shows, such as '24' (IMDB 24, 2010) and 'Live Free or Die Hard' (IMDB Live Free or Die Hard, 2010) depict governments and advanced cyber techniques that can pinpoint network and Internet users in real time; but for the most part, these capabilities do not exist. The fact remains tracking a cyber criminal requires extensive resources and is a time consuming process involving multiple agencies and governments. It is also imperative government decision makers be wary of assigning attribution to a specific country or group for an attack as the current state of cyber defence and investigations rely heavily on the offending group to make a mistake that provides positive identification. The authors do not intend to imply such capabilities cannot be or are not being developed, but rather the current state of Internet security and cyber laws do not provide sufficient capabilities and processes for positive attribution. And as this case study has demonstrated, even if authorities are able to follow the electronic trail to the EPO, that trail will only lead to a non-traceable false identity. Catch me if you can.

References

Answers.com. http://www.answers.com/topic/anonymity Anonymity definition. [Accessed: 10 Oct 2010].

Associated Press. Teen Convicted of Illegal Net Downloads. http://www.msnbc.msn.com/id/7122133/. [Accessed: 7 March 2009.].

Back|Track-Linux.org. VMware Fusion 3.1. http://www.backtrack-linux.org/downloads/. [Accessed: 1 Oct 2010].

Begun, Daniel, A. FBI Uses Spyware to Capture Cyber Criminals. Hothardware.com, Monday, April 20, 2009. http://hothardware.com/News/FBI-Uses-Spyware-to-Capture-Cyber-Criminals/. [Accessed: 1 Oct 2010].

Bradley, Tony. NSA 'Perfect Citizen' Raises 'Big Brother' Concerns, PC World, July 08, 2010 02:02 PM ET, http://www.networkworld.com/news/2010/070810-nsa-perfect-citizen-raises-big.html. [Accessed: 15 Oct 2010].

Fenwick, Samual, Dr. Cyber security – believe the hype? Industrial Fuels and Power. http://www.ifandp.com/article/006583.html. [Accessed: 18 Aug 2010].

FinCEN. http://www.fincen.gov/. [Accessed: 7 Oct 2010].

Furio Gaming. http://www.furiogaming.com/index.php?page=home. [Accessed: 7 Oct 2010].

Golubev, Vladimir. International Cooperation in Fighting Cybercrime. Computer Crime Research Center, http://www.crime-research.org/articles/Golubev0405. [Accessed: 30 Oct 2010].

Hazel Morgan, e. C. (2010, March). Information on How Proxies Work. http://www.ehow.com/facts_6054712_information-proxies-work.html. [Accessed: 22 Oct 2010]

HideMyAss.com; Anonymous remailer and proxy service, http://www.HideMyAss.com. [Accessed: 21 Apr 2010].

IMDB. 24 (2001 - 2010). http://www.imdb.com/title/tt0285331/. [Accessed: 11 Oct 2010].

IMDB. Live Free or Die Hard (2007). http://www.imdb.com/title/tt0337978/. [Accessed: 8 Sep 2010].

Kimery, Anthony. Big Brother Wants to Look in your Bank Account
http://www.wired.com/wired/archive/1.06/big.brother_pr.html. [Accessed: 25 Sep 2010].

Markoff, John. Surveillance of Skype Messages Found in China. New York Times: Internet. [Accessed: 7 Sep 2010].

Microsoft. Microsoft Virtual PC 2007.
http://www.microsoft.com/downloads/en/details.aspx?FamilyId=04D26402-3199-48A3-AFA2-2DC0B40A73B6&displaylang=en. [Accessed: 10 Aug 2010].

Myrli, Sverre. 173 DSCFC 09 E bis – NATO and Cyber Defence. NATO Parliamentary Assembly, http://www.nato-pa.int/default.asp?SHORTCUT=1782. [Accessed: 9 Sep 2010].

NIST. National Institute of Standards and Technologies. http://csrc.nist.gov/ [Accessed: 15 Jul 2010].

Oracle. Oracle VM VirtualBox. http://dlc.sun.com/virtualbox/vboxdownload.html.
[Accessed: 10 Oct 2010].

Reuters. Google, NSA to team up in cyberattack probe. [Accessed: 19 Mar 2010].

Rohret, David, M. And Jett, Andrew. Red Teaming; A Guide to Non-kinetic Warfare. 2009.
Ross, Brian. Federal Source to ABC News: We Know Who You're Calling. ABC News. http://blogs.abcnews.com/theblotter/2006/05/federal_source_.html. [Accessed: 23 Jun 2010.

SHODAN. http://www.shodanhq.com/. [Accessed: 13 Oct 2010].

Sourceforge. (n.d.). Darik's Boot And Nuke (DBAN). http://www.dban.org/. [Accessed: 10 Oct 2010].

SourceForge.http://sourceforge.net/projects/spoof-me-now/files/Spoof-Me-Now%20%28No%20Installer%29.zip/download. [Accessed: 30 Sep 2010].

Ultimate-Anonymity. Anonymous remailer and proxy service. http://www.ultimate-anonymity.com/. [Accessed: 28 Aug 2010].

USAid.gov. www.usaid.gov. http://www.usaid.gov/policy/ads/500/d522022m.pdf. [Accessed: 23 Oct 2010].

Vourdas, A., and Sanders, B. Determination of quantized electromagnetic-field state via electron interferometry 1998 *Europhys. Lett.* 43 659 doi: 10.1209/epl/i1998-00414-0.

Whitehead, Tim. Every email and web site to be stored. Telegraph.co.uk. http://www.telegraph.co.uk/technology/news/8075563/Every-email-and-website-to-be-stored.html [Accessed: 20 Oct 2010].

Wikipedia. Anonymous remailer. Wikipedia: http://en.wikipedia.org/wiki/Anonymous_remailer. [Accessed: 10 Jul 2010]

Worldnet. the State of being anonymous; nameless. http://wordnetweb.princeton.edu/perl/webwn?s=anonymity: [Accessed: 10 Oct 2010].