SCTE CABLE-TEC EXPO®22
SEPTEMBER 19-22 • PHILADELPHIA, PA

2022 Fall
Technical Forum
SCTE® • CABLELABS® • NCTA

I Didn't See It Coming: The Rise of The Bot

A Technical Paper prepared for SCTE by

Don Jones
Director, Strategic Fraud Intelligence
Comcast Cable
Denver, Colorado
303-712-3588
Don_Jones@Comcast.com

Claire Nobles
Project Manager 5, Technical Fraud Management
Comcast Cable
Cheyenne, WY
303-246-1188
Claire_Nobles@Comcast.com

Andrew Frederick
Principal Engineer, Comcast Technology Solutions
Comcast Cable
Andrew_Frederick@Comcast.com

Table of Contents

Title **Page Number**

1. Introduction

A single click of the mouse can cost you your house. A 2021 news article by network solution provider Barracuda measures “bad bots mak[e]ing up nearly 40% of all traffic” (N/A, 2021). It all starts with a single click. Every day, millions of people are asked to click on a link that could cost them everything they own. Malicious links are presented by email, by phishing websites, by dangerous ads on less than reputable websites, by gaming cheats and cracks, and even SMS (Short Message Service) text messaging.

With the exponential growth of the Internet, the threat of these kinds of attacks is supported by a burgeoning underground economy that has only increased the complexity and frequency of their attacks. Tactics are not limited to offering something for nothing. Recent phishing frauds focus on telling the victim something will happen unless they opt out and will often attempt to appeal to their victims at an emotional level. Malicious botnets have different purposes ranging from identity theft to distributed denial-of-service attacks against critical infrastructure. Victims of identity theft based on botnet infections rarely know how they were compromised, leaving the door open for victims to continuously be re-compromised. The end goal of most botnets is monetary gain through identity theft, but the proliferation of botnets also lends itself well to their use as a cyber weapon. The threat vectors vary for users, Internet Service Providers (ISP), retail companies or governments. Though there are legitimate uses of botnets, malicious payloads span a range from questionably legal tactics to blatantly malicious activity. This paper shares ways to identify the initial signs of danger, minimize exposure to these threats and to help bring focus to the recognizable indicators of malicious links.

2. What is a Botnet?

A bot, short for robot, is a software executable application that performs tasks that are automated and repetitive, typically via scripts on the internet. A botnet is a network of bots working together to complete a set of automated tasks that are managed and monitored by a command-and-control system (C2). This C2 is also referred to as a botmaster or botherder. Botnets act like many soldiers being issued orders and reporting back to their general. Botnets are typically used because they can complete tasks quicker and more efficiently than a human.

Botnets have both legitimate and illegitimate purposes. A few examples of both types of botnets are:

- Legitimate botnets
  - Search engines
  - Chat bot communications
- Illegitimate botnets
  - Info-stealers
  - RAT’s (Remote Access Trojan/Tool)
  - Ransomware
  - Crypto Miners

Legitimate botnets are essential in enabling the discovery of added content like new websites. This paper focuses on infection methods and payload types of illegitimate botnets. Malicious botnets seek to subvert security controls and to generate revenue at the expense of their victims.

3. History of Botnet Technology

One of the first bots was ELIZA, a chatter bot, that was created at Massachusetts Institute of Technology (MIT) by Joseph Weizenbaum in 1966. According to an eBook Machines Who Think: A Personal Inquiry into the History and Prospects of Artificial Intelligence, "ELIZA was intended to simulate – or caricature, as Weizenbaum himself suggests – the conversation between Rogerian psychoanalyst and patient, with the machine in the role of the analyst" (McCorduck, 1979). Since then, botnets have evolved drastically in sophistication and purpose.

Botnets use a variety of communication protocols. One of the original protocols is Hypertext Transfer Protocol (HTTP), which was until recently, the most used protocol by many websites. Many of these websites have now moved to Hypertext Transfer Protocol Secure (HTTPS), adding in a security encryption layer. One of the more popular protocols created and still being used is Internet Relay Chat (IRC), which was introduced in 1988 by Jarkko Oikarinen of the University of Oahu. Creators of more advanced botnets added the use of P2P (Peer 2 Peer) in addition to encrypted protocols like The Onion Router (TOR) SOCKS5 proxies and Simple Mail Transfer Protocol (SMTP). Most modern botnets rely on blockchain for a more distributed command and control communication network. Botnet communication keeps pace with all technological evolution.

As the technology of botnets has evolved so has the intent of the botnet. Since 1998, there have been many other malicious botnets that have been unleased on the internet with names like Melissa, Code Red, Storm Worm, Mirai, and Smominru. A white paper titled The Historical Perspective of Botnet Tools best expresses the growth of botnets from a historical perspective. "As researchers continue to unveil the botnet trend and its mode of propagation within networking platforms the botmaster would continue to create different techniques meant to surpass the earlier botnet tool version used" (Osagie, Enagbonma and Inyang, 2019). These botnets have expanded their targets from attacking computers to cell phones, smart cars, and all types of Internet of Things (IoT) devices.

Overall, malicious botnets continue to evolve in their communication methods, target platforms and intentions over the decades. While botnet technologies have evolved, so have the infections methods.

4. Infection Methods

Today, most malicious bots are installed through several primary channels, email, text messages, malicious advertising and program/game cheats or cracks.

4.1 Phishing

Phishing refers to email sent with malicious links or attachments or fake websites that attempt to appear legitimate. Using social engineering tactics to gain the readers confidence or trust, carefully worded email with malicious attachments or links to malicious or fake websites designed to defraud the victim is one of the most effective cyber-attacks that exist. Attachments such as Adobe PDF (Portable Document Format), Microsoft Excel spreadsheets and even pictures can contain distinct types of malicious payloads as categorized below. Opening any attachment effectively "executes" the code inside that attachment with the associated program. Although anti-virus programs catch some of this malicious code, often the malicious code escapes detection through code obfuscation or encryption. More often, a phishing email contains a link to a malicious or cloned website.

Since most email uses Hypertext Markup Language (HTML), hyperlinks, or links to websites, which allows the text to be different than the underlying link to a website. For example, the text that reads "http://GoodGuyWebsite.xyz/" appears to point to GoodGuyWebsite.xyz. However, hovering the mouse reveals the link to the target Uniform Resource Locator (URL) is actually "www.BadGuyWebsite.xyz". Another way of using formatting to forge URLs of familiar websites is the use of character manipulation. An example might appear to be a link to "www.maybeLegitimate.xyz/" but could be easily confused with a link to “rnaybeLegitimate.xyz” depending on the font. Careful examination reveals that the “M” has been replaced with an “R“ and an “N”. Malicious actors often use the original company’s artwork and logos to increase the appearance of the email's validity and the links to malicious sites. Phishing web sites, using genuine appearing artwork, will ask the victim to login and provide their credentials, which is the goal of this type of attack. A shift in tactics was observed in May 2021 when security firm Proofpoint discovered that a malicious actor set up a fake site that appeared to be a video piracy site called BravoMovies.

Instead of encouraging the victim through reward or fear of missing out, the criminals claimed the victim's free trial they had signed up for had expired and their credit card was going to be charged, unless they cancelled. According to the Proofpoint article, BazaFlix: BazaLoader Fakes Movie Streaming Service, the email contained only a phone number, where a human operator directed the victim to the malicious website. The cancellation instructions were only available through a downloaded Microsoft Excel Spreadsheet which contained the malicious code. Phishing schemes tend to lose efficacy with each additional victim action, but as Proofpoint pointed out, “...despite being counterintuitive, the techniques used by the threat actors in this, and similar, campaigns help bypass fully automated threat detection systems” (Larson and Mesa, 2021). SMShising, is like phishing in that the actors attempt to persuade the victim to perform an action, however, the risk surface of mobile devices is far greater than a personal computer.

4.2 SMShing

SMShing is the act of enticing victims to click on hyperlinks delivered via SMS messaging on their mobile device or by opening a malicious attachment such as a PDF, Microsoft Excel Spreadsheets, or pictures. Often, malicious actors impersonate large businesses that most people are familiar with. The efficacy of SMShing attacks is often remarkably high, given several varied factors. Gartner Research published the paper called Tap Into the Marketing Power of SMS, which quantified the efficacy of SMS messaging as a sales medium. “Various sources report SMS open and response rates as high as 98% and 45%, respectively — in contrast to corresponding figures of 20% and 6% for email” (Pemberton, 2016). URL shortening services help to create the illusion of legitimacy to links (i.e., the link tinyurl.com/amazon could be redirected to any unknown website), further complicating the ability to identify a SMShing attempt. Compounding the risk level, most mobile devices lack antivirus protection. SMShing is a form of social engineering, which often uses a time-based pretext.

A common technique is to employ a call to action that expires quickly, such as a limited time exclusive offer that expires in one hour. This prompts the targeted user to suspend judgment about risk/reward since there is often a time component that can cloud judgment. The objective is to convince the victim to open an attachment or visit a website that appears legitimate, that either steals the information the victim enters or installs malicious code. Another social engineering technique used is to convince the victim that not responding to the message will have consequences. For instance, a message saying a credit card will be charged if the victim does not act. While SMShing attacks grow in popularity, malvertising has matured significantly.

4.3 Malvertising

Malvertising (Malicious Advertising) is the act of spreading malware through web or application-based advertisements. Advertisements are one of the most profitable areas of online commerce. Criminals monetize on the advertising platforms by distributing malicious payloads through legitimate ad delivery platforms. The threat to online and application users increases in proportion to the reputation quality of the website or application.

Brand protection companies like Trustworthy Accountability Group (TAG) and White Bullet help to combat malicious ads from being placed on reputable websites. This concerted effort to protect specific brands shifts the delivery of malicious ads to websites or in applications that are less reputable. For instance, White Bullet and Digital Citizens Alliance (DCA) published a study in 2021 called Breaking B(ads) measuring the volume of malicious ads in video piracy websites and applications. "White Bullet reviewed 664 billion ad impressions and found that roughly one in three piracy websites and apps have risky advertising that exposes consumers to fraud and malware" (N/A, 2021). The more reputable a company is, the less of a likelihood that malicious ads will be placed on their website or application due to the corporate diligence in brand protection. The advantage of employing malvertising to deliver malicious payloads is that it does not require compromised hosts to spread a malicious payload and the audience reach is limited only by budget.

4.4 Game and Program Cracks and Cheats

Game and application activation cracks and cheats are created to bypass free trial periods on many different applications and games and to add hidden features like in game invincibility and hidden levels. Often packaged together with the trial application files available on torrent sites, the directions for applying the patch or crack explains to disable any antivirus protection to avoid "false" positives. In doing so, the victim purposely shut down their protection long enough to be infected. Game cheats can differ in that the malicious payload is not immediately installed but often lies in wait for the victim to invoke. Game cheats often bypass the antivirus identification by creating in game links to malicious payloads rather than delivering that payload itself.

5. Payload Types

5.1. Info Stealers

The Information Stealer (info stealer) is the most prolific malicious botnet payload type being distributed, often through malvertizing, game/application cracks and cheats. Info-stealers focus on stealing the victim's information and exfiltrating it to the C2 servers. The information it extracts can be defined by the person running the campaign but usually includes system and browser information by default. Computer information, which includes operating system and system level information, antivirus's running, IP (Internet Protocol) address, machine name and all installed browsers stored information are usually default targets. The browser information consists of all cached URLs, all stored (or remembered) usernames and passwords, all cached form information and stored (or remembered) credit card information in clear text from all installed browsers. Most stealers (Redline, LokiBot, Dark Crystal RAT etc.) can also be configured to exfiltrate all PDF's, Microsoft Word documents, pictures, or text files in specific folders, like "My Documents," "Desktop" etc. These payloads can be configured to search for cryptocurrency wallets, social media applications and Multifactor Authentication (MFA) keys as well. Exfiltration of the information takes mere seconds. The explosion in volume of these infections goes completely unnoticed by the victims but can be measured independently.

A 2021 white paper called An Analysis and Investigation of InfoStealers Attacks during COVID'19: A Case Study, attempted to measure the growth of info stealers in the window of the COVID-19 pandemic. "Resultantly, a significant increase in the quantity and variety of cyber-attacks is observed since <the> emergence of COVID-19. Cybercriminals promptly leveraged this pandemic premise to rebrand general attack vectors. These attacks are typically info stealers and vary from attacks of minimal intricacy such as 404 Keylogger to the latest and more frequent attacks such as Lokibot" (Sharma, et al, 2021). The paper explains that the second largest country attacked, "...USA (40%) ..." (Sharma, et al, 2021), is the focus of this case study. The gravity and scope of the impact is multilayered and compounded.

The scope of the credentials is most often extremely broad. Because botnets can extract data from all the victims' browsers, all accounts are compromised, not just one. When a victim realizes their email has been hacked, they may change their password, but if their social media password is different, they may not change all account passwords. To make matters worse, the victim rarely knows their machine is still currently infected. Each time they change the password on the account they know has been compromised and then allows the browser to store that information, the new passwords are captured in an endless loop of re-compromise. Though they are the most predominant payloads deployed, Remote Access Trojans (RAT) serve a diverse set of criminal intentions with equally devastating effects, but the degree impact varies depending on the victim.

5.2. RATs & RESIPs

RATs allow criminal actors to remotely control a victim's computer or mobile device. Unlike info-stealers, RATs allow criminal actors to use the victim's device in any way they would like, exactly as if they were physically using the victim's device. Modern uses of RATs include, but are not limited to, advertising click fraud, credential stuffing, Business Email Compromise (BEC) and Distributed Denial of Service (DDoS) attacks. A paper published in IEEE's (Institute of Electrical and Electronics Engineers) 2020 European Symposium on Security and Privacy Workshops titled Growth and Commoditization of Remote Access Trojans attempts to measures the growth of this type of bot, states "Remote Access Trojans (RAT) are a special type of remote access software commonly used for malicious purposes, where (i) the installation is done without user consent, (ii) the remote control is done secretly, and (iii) the program hides itself in the system to avoid detection" (Valeros and Garcia, 2020). Accurate in the strictest sense, but, due to the profitability of this type of botnet, a new type of RAT has emerged that is offered as a legitimate commercial service. Residential IP Proxy as a Service (RESIP) companies offer the ability to use a consumer's device as a proxy, allowing them to tunnel through the device, assuming its digital identity.

Hola VPN (Virtual Private Network) is a free VPN software/browser that provides users the ability to spoof their location and device type to avoid content access restrictions. The free version comes with a separate software package from Bright Data (formerly Luminati) that hosts the RESIP proxy service on the person's device in lieu of paying for the premium service. Bright Data is one of over a dozen different companies in the RESIP space. The difference between a Remote Access Tool (like Remote Desktop) and a Remote Access Trojan is consent. A white paper called RESIP Host Detection: Identification of Malicious Residential IP Proxy Flows, at the time of its writing in 2021, measured the number of hosts offered by these companies at over 300 million, collectively. "Once a user installs the free HolaVPN, she is recruited as one of Luminati's (Bright Data's) exit nodes" (Tosun et al, 2021). When criminals use these exit nodes for fraud or cybercrimes, the Internet Service Providers (ISP) logs only show that the exit node (the consumers device) generated the actions of the criminal actor, making it appear the victim is the criminal actor. RAT's allow criminals to use other people's digital identities to defraud others. RESIP companies charge by the gigabyte for their victims mobile and home internet usage. Other payloads, such as cryptocurrency miners, have a more direct relationship to the infected victim's device.

5.3. Crypto Jacking

A crypto jacking (cryptocurrency hijacker & miner) solves computational math problems in exchange for cryptocurrency. The explosive increase in value of crypto currency drove the development of malicious deployments of crypto hijacking miners that target high performance computer environments like virtual machines (VM) and cloud computers. A 2017 paper called Mining on Someone Else's Dime: Mitigating Covert Mining Operations in Clouds and Enterprises describes the suitability of crypto miners in commercial computational environments. “The sheer amount of resources needed for a covert cryptomining operation are readily available in a cloud setting” (Tahir et al, 2017). The costs to the victims are manifested as higher power consumptions, more heat generation as well as the loss of availability of Central Processor Unit (CPU) & Graphics Processor Unit (GPU) resources for legitimate use. Though most profitable in high performance computing environments, crypto jackers are content with exploiting the average consumers devices as well. Often times, crypto jackers run leverage javascript in browsers to launch the covert mining. Ransomware is another botnet payload type that directly impacts the victim's device.

5.4. Ransomware

Ransomware is malicious software which limits or fully prevents a person’s access to their infected device (computer, tablet, phone, or other devices) by encrypting the contents of a hard drive. Ransomware also exfiltrates the data it has encrypted to the C2 server. To regain access to the infected device and the information stored on it, the victim is required to pay a ransom. Ransomware is the technologically advanced way to perform traditional crimes like theft or coercion. “In 2013, scareware arrived in the form of Reveton, which locked and prevented access to the infected devices (known as a Locker). After locking the computer (,) the ransomware falsely alleged that the computer (and user) had engaged in unlawful activities and needed to pay a fine to unlock the computer.” (O’Kane, Sezer and Carlins, 2018). The scope and impact of ransomware attacks depends on the victim.

When ransomware infects computer systems in companies, the ransom tends to be much larger and usually based on the company's value. When a botnet detects it is in an enterprise environment, the botnet may try to infect other computers (lateral movement) on the network before activating. Infecting additional computers on the company network allows the ransomware to encrypt and exfiltrate more data. Defending the risks of ransomware in the business environment includes backing up data, limiting access to data, isolating/segmenting systems, anti-malware software, education/training of staff related to malware, phishing tactics, and a dedicated cyber security team monitoring for threats on the network. Ransomware not only encrypts the contents buts sends a copy of the files to the ransomware group or actor. Since most businesses use data backup systems, the loss of access to their data is usually limited to the last good backup. This includes information like contracts, emails from high-level executives, market research, intellectual property, and other valuable information. Since most companies have access to their back up data, bad actors shift their tactics to extortion, threatening to publish the information, not just deny access to it. Ransomware has transformed from a platform that denies access to information to an extortion as a service business model. Ransomware is indiscriminate, it impacts individual consumers just as often as large companies, though the impact is quite different.

On personal devices, this equates to the loss of all data like personal pictures and stored documents. The use of reputable anti-virus software is one level of protection against ransomware, another protective measure is to backup data to other locations. This could be one or two hard drives that are used solely for the purpose of data backups that are not connected to the internet. While this will help in recovering some of the information, all usernames, passwords, all credit cards, and all form information (like ship to/bill to addresses) that are retained by browsers are exposed to the criminal actor. All these various payloads are significant threats to all connected devices. Protection should always be applied in layers. In addition to having industry recognized anti-virus protection, there are some obvious signs of the dangers that lie ahead.

6. Indicators of Risk

Whether using a mobile device, personal computer, or web connected television, downloading, and opening any attachments should only be done when the sender is known and trusted. Malicious actors depend on the victim's curiosity being piqued or reaction to being threatened in some way. Though filters in email and antivirus programs identify some malicious attachments, often many variants make it through with the victim's assistance. Fake URLs and links that make it through automated protection can often be identified with a closer examination.

A URL starts with a protocol, like HTTP or HTTPS. As the name indicates, entering any information into a website without the “S” is unsecured and readable to an attacker. The “S” should also be accompanied by a locked padlock symbol in the address bar. Following the protocol and the forward slashes, the domains are defined. Consider the example “https://subdomain.domain.top level domain (TLD)”. Most legitimate websites are in the .com, .org and .gov TLD’s. Unrecognized TLD’s should always bear scrutiny. The domain, along with the TLD are the most important part of the URL. Any typos, missing letters or characters, or unfamiliar variations of domain names should also inspire closer scrutiny. The subdomain is malleable and should be considered informative but not authoritative. For instance, Google.com is vastly different than Google.hackexample.com. Protecting devices and systems requires both behavioral effort as well as reputable automated solutions.

Antivirus programs are not foolproof but, as the adage goes, you get what you pay for. Free antivirus programs are often viruses in disguise. All companies monetize their products, the RESIP example demonstrates the unseen price a victim pays for a free product. Applying the same level of protection across all devices, like mobile and tablets that connect to the internet, especially those that are used to access secure websites ensures having a baseline level of automated protection of those devices. Anti-virus, anti-malware and automated solutions can provide some protection, but exercising prudence minimizes the reliance on automated solutions. Before downloading an attachment or clicking a link, be certain the source is someone or some company that is known and trusted. Double check the spelling of the sending email address and the contents of the email. Often, foreign malicious actors use broken English. Hover over links in email to examine underlying hyperlinks. Free products are often paid for in ways that are unknown. Game and application cracks and cheats often contain info stealer payloads. Protect mobile devices with antivirus programs as diligently as a personal computer. Use of MFA, passwordless authentication and password managers minimize account password exposures. Never allow web browsers to store passwords or credit card information. Info stealers can extract them all at once. Never reply to an unknown sender of unsolicited SMS messages. Phishing attacks often use the pretext of an offer that is limited time only, time is critical. They also use previous data breaches and open-source intelligence to gather information on the victim. Never share SMS text codes with anyone else.

7. Conclusions

The rise of the volume of botnets is only dwarfed when compared to the risks that the botnet payloads create. The persistent exposure of all account and credit card data stored or saved in browsers that info stealers access ensures continual re-compromise until the infection is eradicated. RATs can impersonate a victims’ network identity and be wielded as a massive network attack weapon. Ransomware has evolved to include extortion, not just denying access to the victims’ data but publishing it as well. Crypto jackers exploit computer resources rather than information so the cost to the victim often goes unnoticed. Free products come with costs that are not as direct as paying with money. In a digital world, every character is important. Reputable automated protection solutions are only one layer, applied prudence and critical assessment of all digital communications and transactions is still the primary line of defense.

Abbreviations

C2	Command and Control
CPU	Central Processor Unit
DCA	Digital Citizens Alliance
GPU	Graphics Processor Unit
HTML	Hypertext Markup Language
HTTP/HTTPS	Hypertext Transfer Protocol/Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
IRC	Internet Relay Chat
ISP	Internet Service Provider
MIT	Massachusetts Institute of Technology
MFA	Multifactor Authentication
P2P	Peer to Peer
PDF	Portable Document Format
RAT	Remote Access Tool or Trojan
RESIP	Residential Internet Protocol Proxy as a Service
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
TAG	Trustworthy Accountability Group
TLD	Top Level Domain
TOR	The Onion Router
URL	Uniform Resource Locator
VPN	Virtual Private Network

Bibliography & References

McCorduck, P. (1979). Machines Who Think: A Personal Inquiry into the History and Prospects of Artificial Intelligence. San Francisco, CA: W.H. Freeman, pp. 293.

N/A, (2021). Barracuda research reveals skyrocketing levels of bot traffic. Retrieved from: https://www.barracuda.com/news/article/833#.YjHmrnrMliuU

Sharma, R., Sharma, N., and Mangla, M. (2021). An Analysis and Investigation of InfoStealers Attacks during COVID'19: A Case Study, 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC*)*, pp. 1.

Valeros, V. and Garcia, S. (2020). Growth and Commoditization of Remote Access Trojans, 2020 IEEE (Institute of Electrical and Electronics Engineers) European Symposium on Security and Privacy Workshops, pp. 1.

Tosun, A., De Donno, M., Dragoni, N., & Fafoutis, X. (2021). RESIP Host Detection: Identification of Malicious Residential IP Proxy Flows. IEEE (Institute of Electrical and Electronics Engineers) International Conference on Consumer Electronics, p. 4.

Tahir, R. *et al.* (2017). Mining on Someone Else's Dime: Mitigating Covert Mining Operations in Clouds and Enterprises. In: Dacier, M., Bailey, M., Polychronakis, M., Antonakakis, M. (eds) Research in Attacks, Intrusions, and Defenses. RAID 2017. Lecture Notes in Computer Science, vol 10453. Springer, Cham.

Larson, S and Mesa, M (May 26, 2021). BazaFlix: BazaLoader Fakes Movie Streaming Service. Proofpoint Threat Insight Blog

Osagie, M., Enagbonma, O. and Inyang, A. (2019). The Historical Perspective of Botnet Tools. Current Journal of Applied Science and Technology, Benson University, Nigeria. p. 7.
O'Kane, P., Sezer, S., and Carlin D. (2018). Evolution of Ransomware. The Institution of Engineering and Technology, UK. p.3.

Pemberton, C. (2016). Tap Into the Marketing Power of SMS, Gartner Research. Retrieved from https://www.gartner.com/en/marketing/insights/articles/tap-into-the-marketing-power-of-sms

N/A, 2021. Breaking B(ads): How Advertiser-Supported Piracy Helps Fuel A Booming Multi-Billion Dollar Illegal Market, Digital Citizens Alliance. Retrieved from: https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Breaking-Bads-Report.pdf