Old Dominion University

ODU Digital Commons

Cybersecurity Undergraduate Research

2023 Spring Cybersecurity Undergraduate Research Projects

Unveiling the Dark Web and the Impact of REvil's Cyberattacks

Tanya Sasnouskaya
Old Dominion University

Follow this and additional works at: https://digitalcommons.odu.edu/covacci-undergraduateresearch

 Part of the Information Security Commons

Sasnouskaya, Tanya, "Unveiling the Dark Web and the Impact of REvil's Cyberattacks" (2023). *Cybersecurity Undergraduate Research*. 12.
https://digitalcommons.odu.edu/covacci-undergraduateresearch/2023spring/projects/12

This Paper is brought to you for free and open access by the Undergraduate Student Events at ODU Digital Commons. It has been accepted for inclusion in Cybersecurity Undergraduate Research by an authorized administrator of ODU Digital Commons. For more information, please contact digitalcommons@odu.edu.

Unveiling the Dark Web and the Impact of REvil's Cyberattacks

Tanya Sasnouskaya

School of Cybersecurity, Old Dominion University

Teresa Duvall, CYSE Adjunct Professor ODU

April 14, 2023

Abstract

The United States Navy originally created the Dark Web for intelligence purposes, but it was later promoted by Western countries as a tool for safeguarding privacy and anonymity. Currently, the Dark Web serves as a platform for deliberate information leaks by nations that want to keep certain information out of the mainstream media. This paper provides an overview of the dark web and the browser used to access it. It covers the layers of the internet and highlights REvil ransomware and some of its technical details. By understanding these risks, users can take appropriate preventive measures to protect themselves from potential threats. Additionally, the paper examines the different types of criminal activities and incidents that occur on the dark web, such as the sale of illegal goods and services, cybercrime, and identity theft. This information serves as a wake-up call for readers to become aware of the potential dangers of the dark web and take steps to avoid becoming victims of these criminal activities.

A Game Changer for Internet Privacy

The evolution of the internet has brought about significant changes in the way information is accessed and retrieved online. In the early days of the internet, search engines could easily index and retrieve information from static web pages. However, as the internet expanded and dynamic pages became more prevalent, conventional search engines struggled to retrieve information from these pages efficiently. This led to the emergence of the "invisible web" and "Deep Web," which refer to information that is not visible to conventional search engines due to various factors such as targeted queries, password-protected pages, or non-indexed content. As a result, researchers and internet users have had to develop new methods and tools to access and retrieve information from these hidden areas of the internet,

leading to the emergence of alternative search engines, specialized databases, and other innovative technologies (Weimann, 2016).

In the late 1990s, a team of computer scientists and mathematicians working for the Naval Research Laboratory (NRL), a branch of the U.S. Navy, developed a groundbreaking technology called Onion Routing. Onion Routing enabled anonymous bi-directional communication, meaning that neither the source nor the destination of communication could be identified by a third party. The Onion Routing technology achieved this anonymity by creating an overlay network, which is a network built on top of another network. In the case of Onion Routing, the overlay network was built on top of the internet. This new network, which used the Onion Routing technique, was classified as a Darknet, which meant that it was not publicly accessible and could only be accessed through special software (Kaur & Randhawa, 2020).

The NRL soon realized that for the network to be truly anonymous, it had to be available to everyone and not just the U.S. Government. This realization prompted the NRL to release their Onion Routing technique to the public under an open-source license. The Onion Routing technique became known as The Onion Router (TOR) and quickly gained popularity among those who valued privacy and anonymity. With the combination of Onion Routing and The Onion Router, the Dark Web came into existence. The Dark Web is a subset of the internet that is not indexed by search engines and is only accessible through special software. It is a place where people can communicate and exchange information without fear of being tracked or monitored (Kaur & Randhawa, 2020). The Onion Routing technique used by TOR has become an essential tool for journalists, activists, and people living under oppressive regimes who wish to communicate anonymously and avoid censorship. However, the Dark Web has also become a haven for illegal activities, such as drug trafficking, weapons sales, and child pornography.

Despite its potential drawbacks, the Onion Routing technique and TOR have played a significant role in the development of internet privacy and anonymity. The NRL's decision to release its technology to the public has paved the way for many other privacy-enhancing technologies and has given people around the world the ability to communicate and access information freely and anonymously.

The Levels of "Darkness"

The Internet is a complex network of information that can be divided into three main parts - the Surface Web, the Deep Web, and the Dark Web.

The Surface Web is the most well-known part of the internet and can be accessed through standard search engines. However, it represents only a small fraction of the internet, with the majority of information hidden away in the Deep Web. The surface web, also known as the visible web, is part of the World Wide Web that is accessible to the general public and can be indexed by search engines (Bermudez, et al., 2018). Information on the surface web is accessed through the use of web browsers such as Google Chrome, Firefox, or Safari. To access information on the surface web, users simply need to enter a search query in a search engine, and the search engine will return a list of relevant websites. Users can then click on the links provided to access the websites and view the information they contain. In addition to search engines, users can also access information on the surface web through social media platforms, online news sites, and other online resources. The surface web is constantly evolving, with new websites and information being added every day (Bermudez, et al., 2018).

The Deep Web is mostly used for confidential purposes and contains a vast amount of information that is not publicly available. Examples of Deep Web content include Netflix, online

banking, webmail, dynamic pages, databases, and everything that is password or paywall protected. The Deep Web is not accessible to the general public and is used for confidential purposes.

Finally, the Dark Web is the most secretive and dangerous part of the internet. It is a place where criminals, hackers, and other nefarious individuals conduct illegal activities, such as drug trafficking, weapons sales, and child pornography. The Dark Web is not accessible through standard web browsers and requires special software to access. The Darknet or Dark Web is part of the Deep Web, and, in fact, it is its most deeply concealed layer. Users can only visit it by means of a special browser or using special network protocol definitions so that most actions taken on it are completely anonymous. It is estimated that 96% of the internet is made up of the Deep Web and the Dark Web combined, with the Dark Web being a place of illegal activities and not accessible through standard web browsers (Kaur & Randhawa, 2020).

How the Tor Network Protects Communication

When a package travels through the Tor network, it takes a path that is not direct but rather through several intermediate stations, each receiving a unique decoding means and only knowing the next station in the chain. This means that the communication between two points is encrypted and cannot be easily intercepted or traced. The first node reached by the user can usually be discovered by the internet provider, but subsequent nodes are encrypted and unknown. The node receiving the call can only locate the previous node and not any other nodes on the route. The nodes change every few minutes, making it difficult for private or government surveillance to track the path of communication. In this way, the Tor network provides a protected route for communication that is shielded from surveillance (Topor & Shuker, 2019).

TOR is a unique tool that offers anonymity and security. However, the tool is not hidden from local network providers, who can detect unusual network traffic. While authorities can only see normal network traffic, they cannot see private and anonymous web surfing. Privacy is fundamental on the TOR network, and no site on it can collect information about a user's location, hardware, software, or patterns of use. The TOR browser also allows users to eliminate the use of JavaScript, HTML 5, media, images, icons, symbols, and more (Topor & Shuker, 2019). The Dark Web creates an interesting paradox; it sanctifies privacy and anonymity, yet it is also used by criminals, terrorists, and other hostile elements to trade information with low signatures *(information with low signatures refers to data that is not well-known or commonly recognized as a threat by security software or systems. This can make it more difficult to detect and protect against cyber attacks that use this type of information).*

A Hub of Illicit Activities

The Dark Web has become infamous for facilitating a wide range of criminal activities, from drug trafficking to human trafficking, and from identity theft to cyber-attacks. The following are some examples of the types of crimes that occur on the Dark Web:

1. ***Illegal drug sales***

The Dark Web is notorious for hosting online drug markets where illicit substances are bought and sold using cryptocurrencies like Bitcoin. The most famous example of such a market was the Silk Road, which was shut down by the FBI in 2013. However, there are still many similar markets in operation, such as Dream Market and Wall Street Market (FBI, 2013). Silk Road was an infamous online black market that operated on the dark web. It was created in 2011 by Ross Ulbricht, who operated under the pseudonym Dread Pirate Roberts. The website was

designed to be a platform for anonymous transactions, primarily involving drugs. It quickly became one of the most popular and notorious marketplaces on the dark web, attracting a large number of buyers and sellers from all over the world. Silk Road operated on the Tor network, which allowed users to access the site anonymously through the use of encryption and other security measures. Transactions were conducted using Bitcoin, which provided an additional layer of anonymity for users. Despite its popularity, Silk Road was eventually shut down by the FBI in 2013, and Ulbricht was arrested and charged with a range of crimes, including money laundering, drug trafficking, and computer hacking. He was subsequently sentenced to life in prison without the possibility of parole. Silk Road has since been replaced by other online marketplaces, but its legacy lives on as a cautionary tale about the dangers of the dark web and the risks associated with conducting illegal activities online (FBI, 2013).

2. Cyber-attacks and cybercrime tools

The Dark Web is home to a range of cybercrime tools, such as malware, hacking tools, and stolen data. These tools be used to conduct cyber-attacks, steal personal information, and commit fraud. One example is the infamous botnet known as Mirai, which was used to launch massive Distributed Denial of Service (DDoS) attacks (Young, 2022). In 2016, a group of hackers going by the pseudonym "BestBuy" developed the malware known as Mirai and released it on the dark web. The Mirai botnet attack in 2016 was a large-scale distributed denial of service (DDoS) attack that targeted Internet of Things (IoT) devices, such as routers, cameras, and digital video recorders (DVRs). The attack seriously affected numerous important websites and online services. Thousands of compromised IoT devices with weak security or default login

credentials that their owners had not changed made up the Mirai botnet. A group of hackers who were in charge of the botnet and used it to launch significant DDoS attacks by flooding targeted servers with traffic. On September 20, 2016, a DDoS attack with a peak of 620 Gbps, one of the largest DDoS attacks ever recorded, was launched against security researcher Brian Krebs' website. Later, the attack was discovered to be connected to the Mirai botnet, which was used to launch comparable attacks against other targets, including DNS service provider Dyn (Fruhlinger, 2018).

3. Child exploitation

The Dark Web is a platform known for facilitating the distribution of child pornography and other forms of child exploitation. The Federal Bureau of Investigation (FBI) shut down "Playpen" in 2015. Over 16 million cases of online child exploitation were reported to the National Center for Missing and Exploited Children (NCMEC) in 2020 alone, which represents a significant increase in recent years (FBI, 2017). "Playpen" was established and managed by a group of individuals who shared and distributed images and videos of child pornography on the Dark Web. The forum was shut down following a coordinated international law enforcement operation, and many people involved in its operations were detained and accused of possessing and distributing child pornography. With an estimated 200,000+ users and over 100,000 posts containing explicit images and videos of children, "Playpen" was well-known for its high level of criminal activity. Users were able to access the forum covertly thanks to the Tor network's anonymity (Chertoff & Jardine, 2021). The international law enforcement operation that led to the shutdown of "Playpen" involved the FBI, Europol, and several national law enforcement agencies. This incident highlighted the challenges and dangers associated with engaging in

illegal activities on the Dark Web and the importance of international cooperation in combating online child exploitation.

4. Human trafficking

The Dark Web is used to facilitate human trafficking, particularly for the purposes of sexual exploitation. Websites like Backpage, which was shut down by the FBI in 2018, were used for advertising and facilitating prostitution and human trafficking. Backpage was a classified advertising website infamous for facilitating the sale of illicit goods and services, including human trafficking and prostitution. The FBI began investigating Backpage in 2016, after receiving numerous complaints about the website's involvement in sex trafficking. The investigation revealed that the website's owners had knowingly allowed and even encouraged the sale of sex trafficking ads on their platform, making millions of dollars in the process. In April 2018, the FBI seized Backpage and arrested its owners on charges of facilitating prostitution, money laundering, and sex trafficking. The seizure of Backpage was the result of a coordinated effort between several government agencies, including the FBI, the U.S. Postal Inspection Service, and the Internal Revenue Service (IRS). The shutdown of Backpage was a significant milestone in the fight against human trafficking and online exploitation. The website had become one of the largest online marketplaces for human trafficking, facilitating transactions in multiple countries and generating billions of dollars in revenue. Its demise was a victory for law enforcement agencies and advocacy groups fighting to end human trafficking and exploitation.

The shutdown of Backpage, Playpal, and Silkroad highlighted the challenges of combating illegal activities on the Dark Web. Despite being publicly accessible websites, their owners and users could operate anonymously and evade detection. These incidents emphasized

the need for increased law enforcement efforts and technological solutions to combat online criminal activity.

Russia, REvil and Dark Web

REvil (also known as Sodinokibi) is a ransomware group that operates on the dark web and is believed to be based in Russia or a Russian-speaking country. REvil is the name of both the ransomware and the group operating it. The group has been active since at least April 2019 and is known for conducting large-scale ransomware attacks on organizations worldwide. REvil typically gains access to a victim's network through phishing emails, exploiting vulnerabilities, or by purchasing access to compromised systems from other cybercriminals. Once inside the network, the group deploys its ransomware, which encrypts the victim's files and demands payment in exchange for the decryption key (Constantin, 2021).

REvil emerged as an offshoot of the GandCrab ransomware, which originated from a group that pioneered the concept of big game hunting. GandCrab functions as malware that infects computer systems, encrypts their hard drives, and then demands payment in exchange for the decryption key. This type of ransomware is highly effective, and its developers kept it closely guarded, only sharing certain components of it. Over time, GandCrab became a brand that referred not only to the ransomware, but also to the people behind it. The group primarily targeted large, wealthy companies, but gaining initial access to these networks posed a challenge due to the security measures in place. To overcome this obstacle, ransomware groups employ initial access brokers, and there exists an underground market for purchasing access to specific companies.

Why Russia if there is no Direct Evidence?

The group behind REvil primarily recruited customers who speak Russian from online forums. Although many countries have Russian speakers, only a few countries, such as Russia, allow cyber-criminals to operate without fear of being caught. The United States has no authority to work with Russia to arrest these individuals, and Russia does not appear to care much unless Russian companies are attacked. As a result, GandCrab was able to operate without much trouble, with plenty of people, malware, victims, and customers all contributing to a steady flow of cash (Constantin, 2021). In April 2019, REvil emerged and began its activities by performing typical ransomware actions such as deleting backups, altering wallpapers, and performing a language check. If the computer is set to a language spoken in countries that are members of the Commonwealth of Independent States (CIS), the ransomware will not execute. This suggests that whoever is behind REvil prefers not to target countries that were once part of the Soviet Union (Rhysider, 2022).

Businessmen, not Criminals.

The REvil group observed the profits made by GandCrab as a ransomware service and decided to shift their focus to offering ransomware as a service themselves. This proved to be a more profitable business model as they provided other criminals access to networks and then used their ransomware to infect those networks. REvil then handled the entire process of collecting payments, decrypting systems, and assisting victims, while splitting the ransom with the affiliate who deployed the ransomware. Criminals worldwide became affiliates and used REvil to infect systems with ransomware. The process would start with the affiliate deciding to launch an attack by either going to REvil and becoming an affiliate or buying access to one of

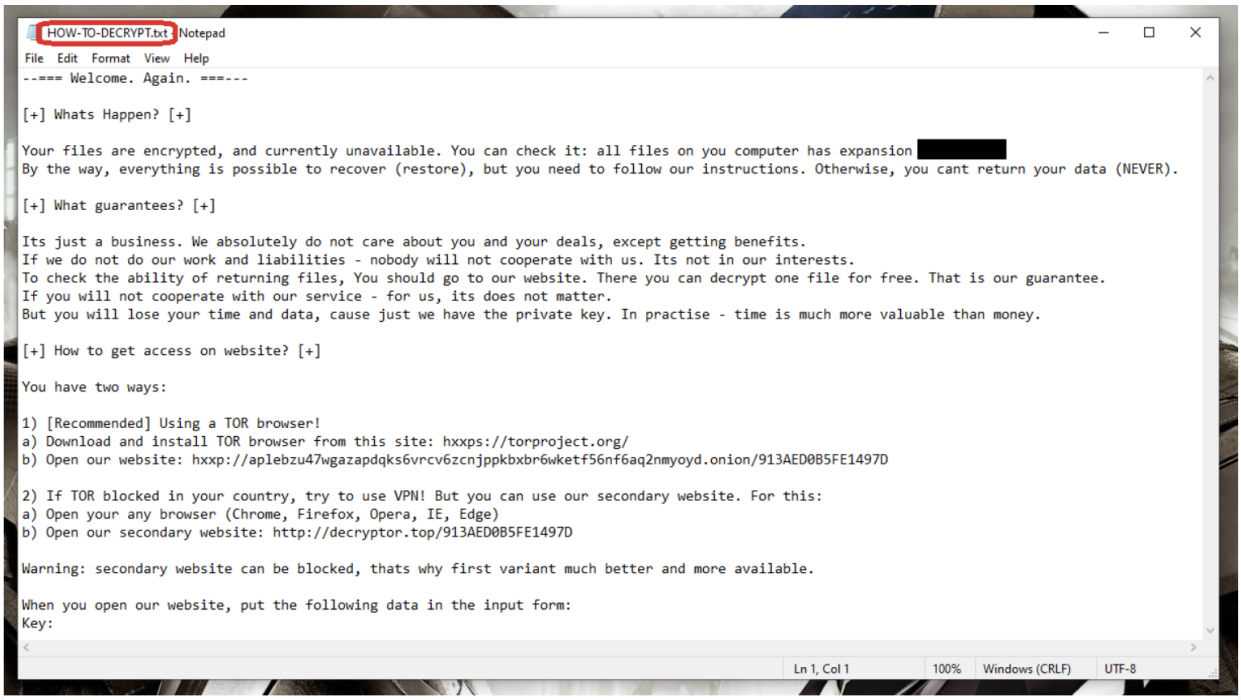
the ransomware platforms and deploying it. REvil would then begin by conducting open source intelligence (OSINT) and identifying a target, followed by searching underground forums to find a way in, purchasing remote desktop protocol (RDP) credentials, cookies, or email account credentials, or conducting initial exploitation themselves (Rhysider, 2022). One of the most common ways that REvil infiltrated networks was by exploiting a vulnerability in a public-facing server.

In order to spread their ransomware, the REvil group would first exploit vulnerabilities in public-facing servers to gain initial access to a network. Once inside, they would conduct reconnaissance and escalate their privileges until they had domain administrator-level access. At this point, they would deploy the ransomware, often via scheduling a task on all computers in the network using the domain administrator credentials. This could result in thousands of machines being locked up overnight, as seen in the case of a South American telecom company where 15,000 workstations were affected. The ransomware note would then appear on each affected machine, instructing victims on how to pay the ransom.

Figure 1

A Message from a REvil Group that you get once your Data Gets Encrypted.

'You have been attacked by REvil. Open for – open the note for instructions on how to pay the ransom.'



The REvil will display this message.

The Dark Web has become a place where criminal activities flourish, with REvil being one of the most prominent examples. Despite its symbolic representation of freedom of speech, privacy, and anonymity in the digital world, REvil is also one of the most dangerous and toxic criminal platforms in the world. What makes it particularly alarming is its ability to operate with immunity to legal jurisdiction and closure.

Cyber-hygiene

The importance of cyber-hygiene is worth mentioning when we are talking about safety online, both on the surface web and deep web. Here are some things that you need to consider online. Consider the use of a Virtual Private Network (VPN). VPN encrypts your internet connection and makes it difficult for anyone to monitor your online activities. Antivirus software can help detect and remove malicious software that may be used to compromise your computer

or steal your personal information. As trivial as it sounds, the use of strong passwords. Avoid using the same password for multiple accounts, and make sure your password is complex and difficult to guess. Never share your personal information on the dark web, such as your name, address, or credit card number. Regularly update your software and operating system to address any security vulnerabilities. Beware of social engineering and always use a trusted search engine to browse the dark web, and be cautious when downloading files from unknown sources. For the business owner, a zero-trust policy sounds more like a must than an option. Zero Trust is a security model that requires strict identity verification for every person, device, and application that wants to access a company's network resources, regardless of whether they are located inside or outside the network perimeter. The zero trust model assumes that all network traffic is untrusted and access to resources is granted based on continuous authentication, authorization, and encryption. Instead of relying on traditional security measures, such as firewalls and perimeter defenses, zero trust enforces a "never trust, always verify" approach to security (IMB, 2023). Last but not least is to be aware of when there is cybercrime happens and be quick to report it. IC3 serves as a central hub for receiving, reviewing, and referring complaints about suspected criminal activity conducted over the Internet. This includes a wide range of crimes, such as online fraud, identity theft, hacking, and other types of cybercrime. "The Internet Crime Complaint Center, or IC3, is the Nation's central hub for reporting cybercrime. It is run by the FBI, the lead federal agency for investigating cybercrime. On their website, you can take two vital steps to protect cyberspace and your own online security. (*Internet crime complaint center (IC3)*).

Conclusion

The Dark Web is a mysterious part of the internet that is not easily accessible through traditional means. It can be visited by anyone, but it is difficult to determine who is behind the websites and they cannot be found using search engines. To access the Dark Web, individuals must use special software such as Tor or I2P. Tor was originally developed by the NRL as a tool for anonymous online communication. This software relies on a network of volunteer computers to route users' web traffic through a series of other users' computers so that the traffic cannot be traced to the original user. Some developers have created tools like Tor2web that allow users to access Tor-hosted content without downloading and installing the Tor software, but this method does not anonymize activity. In this way, the Dark Web remains an enigma, shrouded in secrecy and accessible only to those who know how to navigate it. The World Wide Web is made up of three parts - the Surface Web, the Deep Web, and the Dark Web. While the Surface Web is the most well-known and easily accessible part, it only represents a small fraction of the internet. The majority of information on the internet is hidden away in the Deep Web, which is mostly used for confidential purposes. The Dark Web, on the other hand, is a place of illegal activities and is not accessible through standard web browsers.

The impact of REvil's attacks on the United States and other countries has been significant, both in terms of financial losses and disruptions to critical infrastructure and services. The attacks have also raised concerns about the ability of governments and organizations to prevent and respond to cyber threats, and the need for stronger cybersecurity measures and international cooperation to combat cybercrime.

References

Bermudez Villalva, D.A., Onaolapo, J., Stringhini, G., *et al.* (2018) Under and over the surface: a comparison of the use of leaked account credentials in the Dark and Surface Web. https://doi.org/10.1186/s40163-018-0092-6

Chertoff, Michael & Jardine, Eric. (2021). Policing the Dark Web: Legal Challenges in the 2015 Playpen Case. 1-24.

Constantin, L. (2021, November 12). *Revil ransomware explained: A widespread extortion operation*. CSO Online. Retrieved April 3, 2023, from https://www.csoonline.com/article/3597298/revil-ransomware-explained-a-widespread-extortion-operation.html

FBI. (2013, October 25). *Manhattan U.S. attorney announces seizure of additional $28 million worth of bitcoins belonging to Ross William Ulbricht, alleged owner and operator of "silk road" website*. FBI. Retrieved March 3, 2023, from https://archives.fbi.gov/archives/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website

FBI. (2017, May 5). *'playpen' creator sentenced to 30 years*. FBI. Retrieved March 4, 2023, from https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years

Fruhlinger, J. (2018, March 9). *The Mirai botnet explained: How IOT devices almost brought down the internet*. CSO Online. Retrieved March 31, 2023, from https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

Internet Crime Complaint Center (IC3). *Internet crime complaint center (IC3)* | Home Page. (n.d.). Retrieved April 8, 2023, from https://www.ic3.gov/

Kaur, S., Randhawa, S. Dark Web: A Web of Crimes. *Wireless Pers Commun* 112, 2131–2158 (2020). https://doi.org/10.1007/s11277-020-07143-2

Rhysider, J. (Host). (2022, October 18) REvil – Darknet Diaries [Audio podcast episode]. Retrieved April 3, 2023, from https://darknetdiaries.com/transcript/126/

Topor, Lev & Shuker, Pnina. (2019). Cyber Influence Campaigns in the Dark Web.

Weimann, Gabriel. (2016). Going Dark: Terrorism on the Dark Web, Studies in Conflict & Terrorism, 39:3,195-206, DOI: 10.1080/1057610X.2015.1119546 Gabriel Weimann

What is Zero trust? IBM. (n.d.). Retrieved April 8, 2023, from https://www.ibm.com/topics/zero-trust

Young, K. (2022, January 3). *Cyber case study: The Mirai ddos attack on dyn*. CoverLink Insurance - Ohio Insurance Agency. Retrieved March 4, 2023, from https://coverlink.com/case-study/mirai-ddos-attack-on-dyn/