Analyzing the Ransomware Attack on D.C. Metropolitan Police Department by Babuk

Emily Caroscio, Jack Paul, John Murray, and Suman Bhunia
Department of Computer Science and Software Engineering, Miami University, Oxford, Ohio, USA 45056
Email: caroscen@miamioh.edu, pauljr2@miamioh.edu, murra101@miamioh.edu, bhunias@miamioh.edu

Abstract*—Ransomware attacks are a fast-growing cybercrime that pose a large threat to society. These attacks can result in losing significant amounts of data and money for their victims. Many industries such as aerospace, governmental organizations, etc., have been targeted in the last couple of years. This paper examines the recent attack incidents by one of the famous ransomware groups, Babuk, on the aerospace industry and a police department. It provides an in-depth analysis of the methodology of the attack and examines the impact at a local and global level. A total of 250 gigabytes of data were stolen from one of the victims, the D.C. Metropolitan Police Department. Babuk first had to gain access by infiltrating the system to attack the victims successfully; however, there is no clear evidence on how this was specifically done. Babuk likely gained access by scanning for vulnerable ports in the victim's system, sending employees a phishing email with a malicious link, or cracking passwords that the victim used for admins in their system. After gaining access, Babuk had to maintain access while stealing and encrypting files. Finally, they demanded ransom from the victims and threatened to post the sensitive data if the ransom was not paid. The attack has impacted not only specific organizations but also public security officials. This paper provides an in-depth analysis of the possible attack methodologies and defense strategies against such ransomware attacks. The defense strategies may include changing government policies, regulating cryptocurrency, and adhering to FBI-listed advice.

***Index Terms*—Ransomware, Attack, Zurich Airport, Serco, Police, Babuk, Cybercrime, Data Breach, Cybersecurity**

I. Introduction

Cybercriminals across the globe can attack vulnerable organizations with great ease using malicious software. By doing so, criminals impact the confidentiality, integrity, and availability of sensitive data that businesses and governments use in their day-to-day operations. One of the most common forms of malicious software is known as ransomware. Ransomware can be used to steal and encrypt data from a victim, essentially holding it *"hostage"* until the victim pays the attacker for it to be decrypted [1]. Most ransomware programs operate by using some form of asymmetric cryptography scheme to encrypt data in ciphertext. These schemes generate public/private key pairs that are unique for both the victim and the attacker. The pairs are set up in such a way that only the attacker is able to generate a decryption key to unencrypt the victim's data. Ransomware groups typically threaten their victims into paying for the decryption key in Bitcoin, thus completing their malign intentions [1].

On a yearly basis, ransomware continues to affect industries as one of the fastest growing forms of cybercrime in the world. Within the first half of 2021 alone, there were 121 reported ransomware attacks, up 64% from the year before [2]. In 2020, ransomware was a $20 billion industry, and it continues to grow on a daily basis; average ransomware payments rose 82% in 2021 to $570,000. One reason for ransomware's massive popularity as of late is its ease of use against any organization in any industry. On the dark web, ransomware kits are sold for as little as $175 USD, and typically require no technology background to deploy against a target [2]. Ransomware attacks have become so popular that some experts estimate that a ransomware attack occurs once every 14 seconds around the world. Organizations within all industries are vulnerable to attack, especially those in government and the aerospace and aviation industries.

On January 31st, 2021, Serco revealed to the press that they had been subjected to a large ransomware attack. Serco is a massive contract organization that operates within a variety of industries including defense and aerospace, healthcare, and government. Just a few months later, on April 26th, the D.C. Metropolitan Police Department (DCMPD) confirmed they were subject to a massive ransomware attack. The DCMPD is one of the largest and most important police departments in the United States. The attackers were allegedly a foreign-based group named Babuk. In 2021, Babuk was also allegedly responsible for attacks on at least five other major organizations [3]. Some of Babuk's targets within the aerospace and aviation industry include Serco, PDI Group, and the Zurich Airport [4]–[6].

When an organization becomes victim to a ransomware attack, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) requests they contact the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) immediately. The CISA and FBI say paying the ransom may enable cybercriminals to continue attacking, and in some cases paying the ransom is illegal [7]. Another reason they insist to not pay the ransom is because the attacker may not end up giving the decryption key anyway. In Babuk's case, the decryption key may be faulty and not work.

As shown in Figure 1, Babuk's ransomware strategy takes on a similar structure to many other ransomware groups. After targeting the DCMPD, the group used their ransomware to infiltrate the DCMPD's systems. Once they had gained

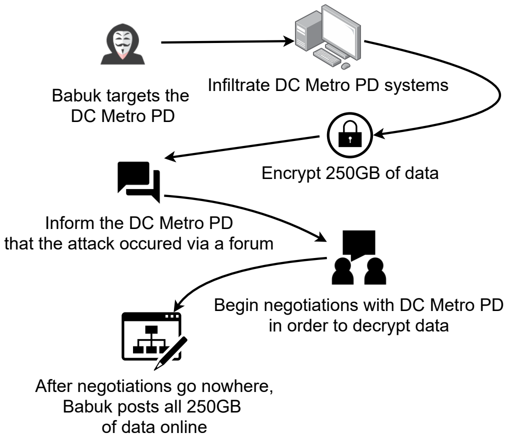

Babuk targets the DC Metro PD
Infiltrate DC Metro PD systems
Encrypt 250GB of data
Inform the DC Metro PD that the attack occured via a forum
Begin negotiations with DC Metro PD in order to decrypt data
After negotiations go nowhere, Babuk posts all 250GB of data online

Figure 1: A schema of Babuk's attack on the DCMPD

access, the group was able obtain and encrypt 250 gigabytes of sensitive information regarding the department and their operations in the greater D.C. metro area. After encryption, the group forced the police department to reach out to them in order to regain control over the data. In this instance, they requested $4 million dollars from the DCMPD in exchange for the private key, or else the sensitive information would be posted on their forum. The police department countered the offer by saying they would pay $100,000, which was not enough for Babuk [8]. All 250 gigabytes of data were posted online on May 13th, 2021 [3].

This paper highlights the importance of the consequences that ransomware attacks can have on affected victims. Experts believe that the DCMPD attack is the largest cyberattack to ever be perpetrated on a U.S. police department [8]. Data stolen during the attack was comprised of sensitive documents pertaining to hundreds of individuals regardless of their affiliation with the DCMPD. This attack shows that ransomware is becoming a major concern for not only businesses but also government agencies and entities as well, and represents overarching troubles that ransomware will continue to cause until permanent defense solutions can be implemented. This paper will focus not only on organizational changes that can be made to prevent specific Babuk ransomware attacks but also broad changes that can be made to prevent ransomware as a whole.

The rest of the paper is organized as follows. First, we will discuss the backgrounds of the victims, Serco and DCMPD, and the attacker, Babuk. In the following section, we describe the attacks on the aerospace industry and particularly the attack on Serco. Information regarding Babuk's attack patterns and habits will also be reviewed. In the following section, we will explain the details of how the D.C. Metropolitan Police ransomware attack was carried out. This includes considerations of how access was gained, how access was maintained, and details of how the ransom was demanded by Babuk. After this, the overall impact of the DCMPD attack is elaborated. This will include both specific consequences that the DCMPD dealt with as well as broader impacts that ransomware attacks have in the U.S. Finally, we will explain the possible countermeasures that can be taken against ransomware attacks such as this.

II. Victim and The Attacker

Babuk's attack on Serco occurred in February 2021. As previously stated and outlined in Fig. 2, DCMPD first notified the press of their attack in late April 2021. In this section, we study the background of Serco, the DCMPD and the ransomware group Babuk.

A. *Serco Aerospace Contractor*

Serco is a British contracting company that operates in many different industries, specifically those within the public sector. Their worldwide contract work within the aerospace and defense industry is one of the largest facets of their work. This work includes base management and aircraft modernization and maintenance. In 2018, Serco's revenue from contracts within this industry totaled £947 million, making them one of the largest contractors for the aerospace industry worldwide [9].

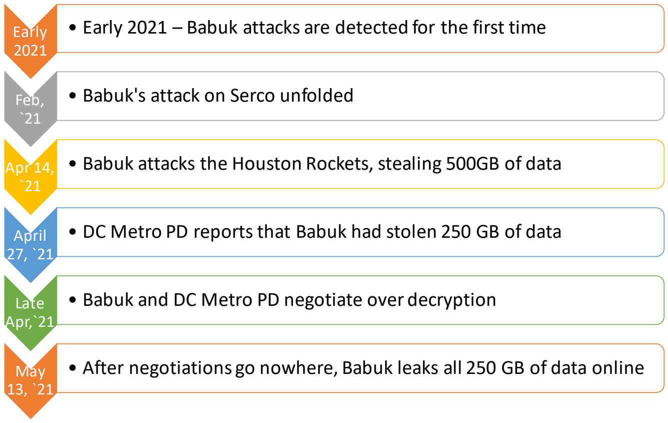
B. *D.C. Metropolitan Police Department Data*

The DCMPD is one of the most prominent police departments in the U.S. The department is one of the largest in the nation, and serves greater metropolitan area of the District of Columbia [10]. Because the department is located in the capital of the United States of America, they carry out work more important than a typical police department. In fact, officers from the DCMPD were called in to help control the crowd at the U.S. Capitol during President Joe Biden's inauguration on January 6th, 2021 [11]. The heightened responsibility that the DCMPD handles on a daily basis is one of the many reasons why they are such an important police department in the U.S.

In their normal operations, police departments typically deal with various types of data. This includes criminal history records, law enforcement incident reports, records of judicial actions and decisions, and watch lists of known and suspected terrorists [12]. Not only does this data help law enforcement and government agencies detect and prevent crime before it occurs, but it also allows them to share data with different policing agencies. Police departments also store information relevant to their officers, including personal and employment data, as well as important information about their general operations. These copious amounts of sensitive data make police departments more vulnerable than ever to cyberattacks. This was certainly the case for the DCMPD when they were targeted by Babuk [8], [13], [14].

C. *Babuk Hacker Group*

There is ongoing research about the alleged attackers, who are known as Babuk. The foreign-based group thinks of themselves as *"security auditors"* who request payments from the companies they *"provide their services"* to [3]. On their forums, Babuk tells victims that they would be much worse off if their data were in more villainous possession. In other purported attacks, Babuk have operated by using


Early 2021 • Early 2021 – Babuk attacks are detected for the first time

Feb, `21 • Babuk's attack on Serco unfolded

Apr 14, `21 • Babuk attacks the Houston Rockets, stealing 500GB of data

April 27, `21 • DC Metro PD reports that Babuk had stolen 250 GB of data

Late Apr,`21 • Babuk and DC Metro PD negotiate over decryption

May 13, `21 • After negotiations go nowhere, Babuk leaks all 250 GB of data online

Figure 2: Timeline of Babuk’s attacks

a *“ransomware-as-a-service”* model. That being said, it is believed the group have become more focused on data extortion after the DCMPD attack. As seen in the timeline (Figure 2), Babuk was first detected in early 2021. Babuk’s ransomware uses similar operating methods compared to many other ransomware groups, and a technical analysis of their ransomware found it shared extreme similarities to another type of ransomware named Vasa Locker [15].

In a public post from the group’s data leak site, Babuk describes their intentions as *“network testers”* with *“non-malicious software”*. While Babuk does force victims into negotiation to decrypt their data, the group does have several types of organizations they do not attack. These include hospitals, non-profit organizations, schools, or companies with an average revenue of less than $4 million [15].

The group uses a series of English-speaking and Russian-speaking forums for operations [3]. The English-speaking forums are used primarily for leaking certain amounts of victim data and for communicating messages to the general public, while the Russian-speaking forums are used for communication between members and advertising recruitment to the group.

D. Babuk’s Ransomware Attacks Strategies

The group uses their ransomware to meticulously attack enterprises in the *aerospace, transportation, healthcare, plastic, electronics, and agricultural* industries. Before the attack on the DCMPD, Babuk had already used their ransomware to target at least five victims in these sectors in the first half of 2021 [15]. The group has been successful in at least one of these attacks, as one company paid them $85,000 to decrypt data stolen by Babuk’s ransomware.

Babuk’s attacks also varied in geography, with major attacks occurring in the United States, Spain, Italy, India, and China [15]. According to cybersecurity experts, their continued success is a result of operating out of jurisdictions which provide them protection from international law. This is due to ineptitude or indifference from countries that they operate out of. [13]. Additionally, when Babuk threatens victims that sensitive information will be posted online, they request payment in Bitcoin in order to recover the data. Because the sending and receiving of Bitcoin is not overseen by one government or organization, this makes it much easier for Babuk to avoid international authorities [16].

One specific instance of Babuk’s ransomware attacks occurred to the Houston Rockets, a professional basketball club in the NBA. Babuk used ransomware to steal and encrypt 500 gigabytes of the organization’s data [17]. The data stolen were all important documents to the organization and included third-party contracts as well as corporate, customer, employee and financial information. This information was highly sensitive and was not meant to be seen by the general public. For example, one leaked document, titled *“Team Sale”*, led many to speculate whether the team’s owner was looking into selling the team or not. This attack bore many similarities to the attack against the DCMPD and Serco attacks that Babuk undertook.

III. Ransomware attacks on Aerospace Industry

Within the aerospace industry specifically, ransomware attacks can have massive repercussions on an organization. A recent threat analysis by FireEye shows that cyberattacks on companies in this industry aim to steal intellectual property from aerospace and defense companies and use it against them by developing countermeasures or working to monitor and subvert a nations’ aerospace and defense systems [18]. Information stolen from aerospace and defense companies can include budget information, product designs and blueprints, research reports, and testing reports/results.

A. Recent Ransomware Impacts on Aerospace Industry

Recent attacks on the aerospace industry target the many vulnerabilities which different types of aerospace software contain. Specifically, increasing amounts of software and hardware integration leave vulnerabilities for malicious hackers to exploit [19]. Other research has shown that attacks on aerospace software can also originate from lower layers including the OS kernel. Purposes for these attacks are usually to corrupt core data and failure-tolerant systems within aerospace software [19]. Failures in either of these systems create massive ramifications for the overall safety of an aircraft.

B. Ransomware Attacks on Airports

Although Babuk has conducted an attack in this domain, it is also being targeted by other groups with higher stakes. In February 2022, there was a ransomware attack by an unknown group at the Zurich Airport which caused 22 flights to be delayed [6]. Swissport, the main ground services and air cargo operator at the Zurich Airport, had their IT systems subjected to a ransomware attack from an anonymous group. No critical systems were subjected to attack, and Swissport operators were quick to respond to the attack once it had been detected. When aerospace systems are targeted, more than just data can be affected, as attacks on critical systems can affect the integrity of an airport’s security as well as the safety of an aircraft for passengers and pilots. Some known named Cybercrime groups are Maze and Netwalker. In June 2020, there was an attack on ST Engineering, where 1.5TB of sensitive aerospace data was

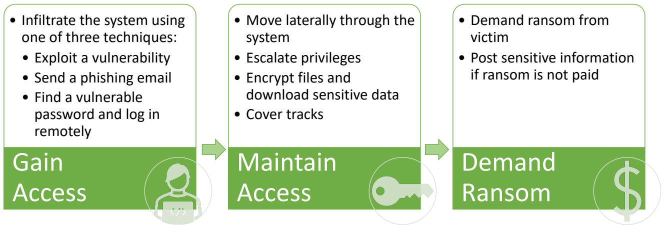

• Infiltrate the system using one of three techniques:
• Exploit a vulnerability
• Send a phishing email
• Find a vulnerable password and log in remotely
Gain Access
• Move laterally through the system
• Escalate privileges
• Encrypt files and download sensitive data
• Cover tracks
Maintain Access
• Demand ransom from victim
• Post sensitive information if ransom is not paid
Demand Ransom

Figure 3: Ransomware attack phases that Babuk typically uses on their victims, including the DCMPD [22].

stolen [20]. In another attack targeting the aerospace industry, the malware had gone undetected for at least two years just being discovered in September 2021 [21].

C. Babuk's Ransomware Attacks on Aerospace Industry

Babuk's unsophisticated malware attacked Serco in February 2021. Babuk gained access to Serco's systems and claimed to have stolen more than 1TB of data from them [4]. The specific systems that were under attack and impact the attack had on the company are unknown [4]. Another company in the defense and aerospace industry, PDI Group, was also attacked by Babuk in 2021 [5]. During this attack, 700GB of data ranging from contracts and customer payment information to personal information of employees and non-disclosure agreements regarding intellectual property were stolen from PDI Group. Similarly to the DCMPD attack, Babuk leaked sensitive documents online in order to pressure the victim to pay the ransom [5].

IV. Attack Methodology

In every cybercrime there is a set of phases used by the attackers in order to successfully infiltrate and attack a system. Malicious software, often referred to as "*malware*" is software purposefully designed to cause harm to computers and/or users in order to gain access to sensitive information. When cybercriminals use malware, there are a variety of different techniques that can be used to attack a victim. One common attack technique is a form of malware called ransomware [1], [23]. The specific attack that the Babuk group used was the ransomware-as-a-service model. Figure 3 shows the three main phases of a Babuk Ransomware attack. All of the following information is based off of three main technical analyses of source code from this Babuk attack and prior ones. Two of the analyses were done by McAfee [15], [22] and the other by Chuong Dong on his security blog [24].

The source code used throughout different Babuk attacks had evolved into different mutexes and the ones discussed in this paper are shown in Table I. The rest of this section discusses possible points of gaining access, what happened when access ultimately was gained, and how ransom was demanded from the victim.

A. Gain Access

The first phase for this attack was to gain initial access into the DCMPD's system. To successfully have done this the attackers first had to complete reconnaissance. This means they attempt to find as much information they can about the DCMPD, including what types of software's they use. Babuk then needed to scan the system for vulnerabilities to see where they could enter the system. There are three possibilities for how Babuk gained this initial access to the DCMPD's system.

Table I: Babuk Ransomware Versions

Version	Source	Details
Version 1 (v1)	[15], [24]	This version analyzed was the first version of the ransomware detected.
'DoYouWantToHaveSexWithCuong-Dong' version	[3]	This version is believed to be used in the DCMPD attack and talks about the new updates to the encryption.
April 2021 Version (babuk_v2)	[22]	This version was analyzed from April 2021 and talks about some changes from the original version.

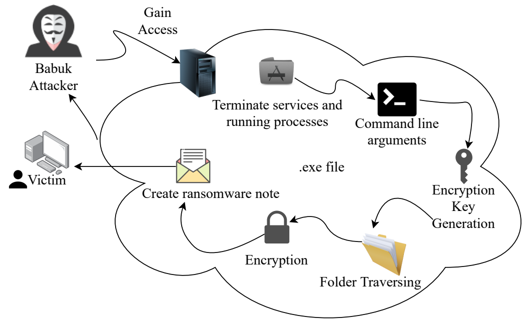


Figure 4: Attack Methodology Breakdown, specifically how they maintained access after compromising DCMPD system [24]

The information about how access was actually gained was not released by the police department. The first possible way would have been to exploit a vulnerability that may have been found during *scanning and enumeration* [22]. There are tools to do this and Babuk had done it before by exploiting a public-facing application, in the specific case the application had been Microsoft. Another possibility to gain access to the system would be via phishing email. If Babuk sent a fake email with a malicious link or attachment and that was clicked on or downloaded, they could get initial access. Phishing emails are sometimes hard to spot because they can be made to look very legitimate. The last possibility is that Babuk found a vulnerable password and could gain remote access into the system by guessing this password [22].

Babuk's ransomware is programmed in an open source language called Golang. In a McAfee technical analysis, it is mentioned that Golang written on a Linux system can run on either Windows or Mac [22].

B. Maintain Access

Figure 4 shows the life-cycle of the malware after Babuk has successfully gained access into the DCMPD system. They terminate databases, office applications, and anti-malware services in order to further avoid detection [3]. Examples of the main services Babuk will terminate

Table II: Shell functions used by Babuk ransomware for lateral propagation after gaining access to the DCMPD network [24], [25]

Shell Function	Description
`ShellExecuteW`	Executes `cmd.exe /c vssadmin.exe delete shadows /all /quiet` to delete shadow volumes
`SHEmptyRecycleBinA`	Empties the recycle bin of victim's machine
`FindFirstFileW` `FindNextFileW`	Recursively uses these method calls to traverse through directories and subdirectories of a system

`SetFileAttributesW`
`lstrlenW lstrcpyW`
`lstrcatW MoveFileExW`
	Functions used to append the `.babyk` extension to encrypted files.

`QueryServiceStatusEx`
`OpenServiceA`
`EnumDependentServicesA`
`CloseServiceHandle`
`GetLastError`
	Functions used to terminate certain services (mostly antivirus scanners) to avoid alerts

`CreateToolhelp32Snapshot`
`lstrcmpW OpenProcess`
`TerminateProcess`
`CloseHandle`
	Functions used to terminate certain processes (mostly database and office-applications) to prepare files for encryption

include: `sql.exe, firefox.exe, outlook.exe, onenote.exe, powerpnt.exe`. Examples of the main anti-malware services stopped include: `GxVss, GxBlr, GxFWD, DefWatch` [3]. They began to move laterally through the system. Babuk uses command line operations which allows for flexibility. It executes many shell function calls (Table II) to covertly propagate their access. The functions used to terminate the services if found are `QueryServiceStatusEx, OpenServiceA, EnumDependentServicesA, CloseServiceHandle` and `GetLastError`. The functions used to terminate processes if found are `CreateToolhelp32Snapshot, lstrcmpw, OpenProcess, TerminateProcess` and `CloseHandle`. The ransomware runs commands and destroys the "shadow volumes" of the victim machine which covers the tracks of the commands being ran [15]. The function used is `ShellExecuteW`, which deletes these shadow copies. Then the command `SHEmptyRecycleBinA` is used to empty the recycle bin of the victims machine to prevent any possibility to regain and recover data [25]. This ensures that the victim needs the decryption key from the attacker in order to have the files back.

The next action performed is file encryption. In Version 1 of the malware the files are enumerated up to 16 folders deep. This means if there was a 17th nested folder it would be ignored [15]. The malware traverses and encrypts files using recursive methods. The functions run are `FindFirstFileW` and `FindNextFileW` which go through the directories on the victim's system [24]. Babuk then uses the HC-128 algorithm for file encryption with the Elliptic-curve Diffie–Hellman (ECDH) scheme for file key encryption. The specific elliptic curve used for cryptography was Curve25519 [3]. According to a technical analysis done on Version 1, Babuk had used the Chacha8 algorithm with the keys generated from Curve25519 and SHA-256 [22]. When the files are encrypted, the extension `.babyk` is appended to all files using the functions `SetFileAttributesW, lstrlenW, lstrcpyW, lstrcatW`, and `MoveFileExW` [25]. These files are impossible to decrypt without the private key, so without that the files may be lost forever. While encrypting files, Babuk leaves off certain files and folders like "Windows" and "Firefox" in order to prevent the victim's machine from crashing. The mutex version of the source code believed to be used for the DCMPD attack has the name "DoYouWantToHaveSexWithCuongDong." This refers to researcher Chuong Dong who analyzed Version 1 of the Babuk malware. After he posted his technical analysis, Babuk made changes to the code to create other mutex versions [3].

C. Demand Ransom

After the Babuk ransomware had infiltrated the system, the last step was to demand ransom from their victim. They left a file titled "`How to Restore Your Files.txt`" with a ransom note on the system that has contact information and proof that the files have been taken [3]. In the case of DCMPD, the department did not find out their systems had been compromised until it was posted on the Babuk forum. The instructions to contact the attacker are listed and state to download the Onion Router from a dark-web repository[1], then open it and follow a link in the browser[2]. Babuk changes these links for each specific attack. The note also provided a link to where the information will be leaked to the public on the Dark Web [3].

V. Impact

As previously stated, Babuk had claimed to have stolen in total 250 gigabytes of data from the DCMPD [14]. The data stolen was compromised of both sensitive information on individuals as well as larger federal documents. More specifically, sensitive documents pertaining to individual police officers were leaked to the public. Social security numbers, marriage history, financial details, criminal history, employment history, answers to polygraph tests, and social media activity of officers were all included in the leak. Documents leaked concerning the DCMPD included psychiatric evaluations, details of past drug use, finances, backgrounds checks, sexual abuse, disciplinary actions, and other confidential documents.

A. Impact on DCMPD and Public

As shown in Figure 5, data leaks released by Babuk on the DCMPD had a very damaging impact on the officers involved as well as the department itself. After the data was leaked, D.C. Police Union chairman Gregg Pemberton stated, "How we will ever hire anyone to work here is beyond me" [8]. Ransomware expert and threat analyst Brett Callow explained that because of the risks that officers and civilians faced from

[1] https://www/torproject.org/download/

[2] http://babukq4e2p4wu4iq.onion/login.php?

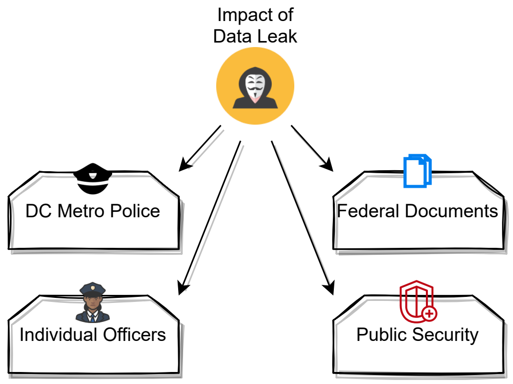


Figure 5: Organizations and areas who are impacted by the attack

these leaks, it is “possibly the most significant ransomware incident to date” [8].

The impact of these leaks has also had dire legal implications for the victim. D.C. Police Union filed a grievance for a collective bargaining agreement violation against the city [8]. This violation of the collective bargaining agreement had been a direct result of the information leaks and the union requested an investigation by the city’s inspector general.

However, the documents leaked did not only affect individual officers from both the Washington, DCMPD and other agencies; unfortunately, sensitive federal documents were also leaked. These documents include highly sensitive security information related to US presidential inauguration as well as detailed steps of an FBI investigation, which listed suspects and general data pulled from cell towers to aid in the investigation [8], [13], [26]. Copies of these documents being freely available online endangered many more people outside of the DCMPD. Since many individuals have had their private information released to the public along with documents that could threaten public security, the attitudes regarding cybersecurity in the DCMPD have shifted.

B. Broad Impact of Ransomware

Babuk’s attack on the DCMPD was only a single attack that represents a larger and growing problem. The impact of ransomware attacks has grown massively in the past few years. In October 2021, the number of publicly reported data breaches had already surpassed the total number of data breaches from 2020 [27]. A cybersecurity firm named Cybersecurity Ventures estimates that costs associated with damage from ransomware will amount to $265 billion dollars by 2031 [28]. Cybersecurity Ventures also believes that by 2031, novel ransomware attacks will be attempted every 2 seconds against businesses, consumers, and individual devices.

However, ransomware is not the only form of cybercrime that is increasing. Mobile devices being attacked with malware have increased 54% across the globe, and software update supply chain attacks having implanted malware on software packages have increased by 200% between 2016 and 2017. The costs of these attacks are growing to tremendous amounts as well. It is estimated that financial costs incurred by entities hacking US companies, most of whom are foreign-based, are between $225 billion to $600 billion annually [29].

Table III: Rate of Enforcement of Crimes (where enforcement is frequency of an enforcement action being taken by authorities for a given crime) [29], [30]

Crime	Rate of Enforcement
Cyber Crime	<1%
Violent Crime	46%
Murder and Non-negligent Manslaughter	61%
Rape	33%
Robbery	31%
Aggravated Assault	52%
Property Crime	17%
Burglary	14%
Larceny-theft	18%
Motor Vehicle Theft	14%
Arson	24%

One reason why ransomware and other cybercrimes have been able to increase so greatly is due to low enforcement rates for cybercrimes. Table III shows the rate of enforcement of cybercrime compared to other forms of crime in the U.S. It is incredibly difficult for federal authorities such as the FBI and NSA to track down and charge cybercriminals with criminal charges for their actions. This low enforcement rate when compared to other crimes makes cybercrime a “*low-risk, high-reward*” option for criminals who have the know-how to carry out these types of attacks.

VI. Possible Countermeasures

Figure 6 outlines several key areas that could act as possible defense strategies against ransomware attacks. When it comes to cybersecurity, several government agencies such as the FBI and CISA offer general tips on how an organization can protect itself. These tips include using strong passwords, ensuring that an organization is using the most current versions of software, conducting regular virus scans, backing up data consistently, and making members aware of phishing scams [23].

A. Continuous Penetration Testing of System

Frequent penetration testing of a system should be carried out to discover the attack surface and vulnerabilities in systems. More specifically, Antivirus company, McAfee offers suggestions on how to defend against Babuk themselves [15]. McAfee states that defenders should look out for behaviors with correlation to open source penetration testing tools or hacking frameworks such as winPEAS, SharpHoud, CobaltStrike, Metasploit, or Covenant because Babuk has posted that they recruit individuals with penetration testing skills [15]. Table IV outlines how each out these tools are normally used for ethical hackers to legally test organizations for vulnerabilities. Indicators of Compromise, also known as IoC’s, can help indicate when a cybersecurity attack has occurred. You can use IoC’s during response to an attack to prevent that specific attack from occurring again [31]. Monitoring traffic on a Companies system can help locate any suspicious activity and to act early in the case that malicious access was gained.

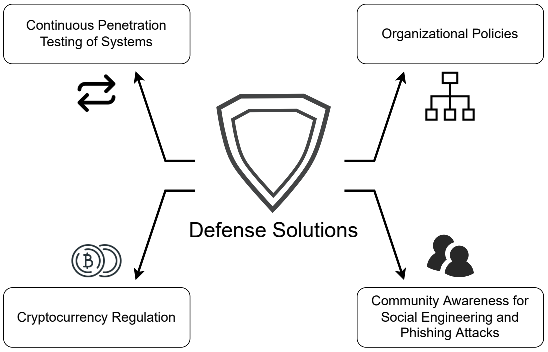

Continuous Penetration Testing of Systems
Organizational Policies
Defense Solutions
Cryptocurrency Regulation
Community Awareness for Social Engineering and Phishing Attacks

Figure 6: Defense Solutions of Babuk Attack

Table IV: Penetration Tools and Hacking Frameworks [15]

Penetration Testing Tools/Hacking Frameworks	Description
winPEAS	Used for privilege escalation on Window hosts.
SharpHoud	Collects data from domain joined Windows systems as well as domain controllers.
CobaltStrike	A software which emulates threats for penetration testing.
Metasploit	An open source penetration testing framework that is used to improve security.
Covenant	A control framework and a .NET command that detects attacks.

B. *Organizational Policies*

Another method of defence against cyberattacks such as this is changing government policies. As illustrated in Table III, there is a large enforcement gap when dealing with cybercrimes. One suggestion is to build better cyber defences but also increase effort into pursuing human attackers. It argues that this strategy could both decrease the finite amount of hackers nation wide, discourage others from pursuing cybercrime, and makes sense given the estimated $225 billion to $600 billion annual cost to US companies in 2017 [29]. However, despite the tremendous cost caused to the US economy by cybercrime the Department of Defense had only spent $7.2 billion on broad cybersecurity measures in the same year [29]. Though there have been some recent policy changes, such as a recent Executive Order from US President on cybersecurity that requires companies to report specific information about data breaches and establishes the Cybersecurity Safety Review Board, there are still many more defence methods that can be put into place [32].

C. *Cryptocurrency Regulation*

Cryptocurrency is widely used in ransomware attacks. This is due to that fact that cryptocurrency is easy to use and hard to trace when dealing with amounts of money. The regulation of cryptocurrencies both nationally and internationally could aim in investigations of cybercrime. Specifically, one study found that regulating Bitcoin globally that is done clearly, consistently, and cost effectively could help target malicious Bitcoin users [33]. Increasing global regulations for Bitcoin exchanges can help increase transparency between senders and receivers, especially malicious ones. Because Bitcoin uses blockchain for operations, none of its transactions are truly anonymous. Bitcoin exchanges use identifying documents to accurately trace the sender and receiver of the exchange [16]. These documents contain “know-your-customer” IDs, which can be used by law enforcement or government agencies to help track malicious Bitcoin traders and bring them to the justice system.

D. *Community Awareness for Social Engineering and Phishing Attacks*

Phishing is one of the most common ways that malicious actors are able to gain access to a system in a ransomware attack. Nearly one quarter of ransomware victims report that phishing was how attackers initially penetrated their system, and of those victims, over one half had conducted anti-phishing training in their organization to some degree [34]. Teaching employees about what phishing is and how to detect it within their system is a crucial step to preventing large-scale ransomware attacks in an organization. Microsoft lists calls to action or threats, poor spelling and grammar, unexpected links and/or attachments, and mismatched email domains as common hallmarks of phishing messages [35]. If an employee receives a phishing email, they should never open any links or download any attachments from the email. Reporting and deleting the email is the easiest way to prevent it from propagating ransomware onto a company’s network. Keeping an organization’s members knowledgeable about their security policies and practices is a major defense against ransomware attacks.

It is important to stay up to date on emerging cybercrime trends. Many attacks target software that is out-of-date or needs newer security patches. If the current trends are being researched this will help to keep any company’s cybersecurity up to par and be one step ahead of the hacker groups. This especially matters when software being used is old or out dated. Police computers are vulnerable for this exact reason, as they have older software with vulnerabilities that are typically targeted by ransomware groups [36].

VII. Conclusion

Babuk’s targeted attacks should serve as an example that no organization should take the ever-present threat of ransomware lightly. The pivotal attacks of Babuk’s ransomware show the wide range of organizations vulnerable. The data encrypted by the group could result in much more damage to not only to affected organizations like the DCMPD and Serco, but also the industries in which they operate. Babuk’s strategy of data encryption during the ransomware attack also shows how important it is for systems to better protect their data before it is stolen. In the case of DCMPD’s attack, the stolen data was actually leaked and Babuk likely could have made far more important information available on the dark web had they been less resistant to their ransomware process. It is important for organizations especially in the industries with highly sensitive data to re-evaluate their ransomware prevention strategies and be wary of the constantly evolving threats that ransomware groups pose to their data. Only through constant and effective prevention strategies can organizations discourage hacker activities and prevent data breaches like the ones Babuk has perpetrated against. Using strategies such as increasing awareness of phishing attacks, implementing a solid incident response plan to combat ransomware and other forms of malware, updating or patching legacy software, and following the latest government regulations are all safe and effective ways that large organizations can use to increase their ransomware awareness. Research areas for future ransomware prevention include malware mutex detection through techniques like YARA rules and safer decryption methods for ECDH encryption and other similar encryption techniques. Additionally, research into global regulation of bitcoin transactions is another strategy to help deter cybercriminals using ransomware to profit off of vulnerable businesses.

References

[1] A. Tandon and A. Nayyar, *A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat: Proceedings of ICDMAI 2018, Volume 2*, pp. 403–420. 01 2019.

[2] “2021 Ransomware Statistics, Data, Trends.” https://www.cybersecuritydive.com/news/babuk-ransomware-group-emerges-with-new-claims-against-us-companies/597416/, 2021.

[3] “Threat analysis: Babuk ransomware.” https://www.acronis.com/en-us/articles/babuk-ransomware/, 2021.

[4] A. Martin, “COVID-19: NHS Test and Trace ’unaffected’ by cyber attack at Serco, firm says.” https://news.sky.com/story/covid-19-nhs-test-and-trace-unaffected-by-cyber-attack-at-serco-firm-says-12204747, 2021.

[5] D. Jones, “Babuk ransomware group emerges with new claims against US companies.” https://www.cybersecuritydive.com/news/babuk-ransomware-group-emerges-with-new-claims-against-us-companies/597416/, 2021.

[6] “Ransomware attack on Swissport causes delay at Zurich Airport.” https://www.airport-technology.com/news/ransomware-attack-swissport-zurich-airport/, 2022.

[7] “Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments.” https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf, 2020.

[8] A. Suderman, “DC police victim of massive data leak by ransomware gang.” https://apnews.com/article/police-technology-government-and-politics-1aedfcf42a8dc2b004ef610d0b57edb9, 2021.

[9] “Serco in Defence.” https://www.serco.com/sector-expertise/defence, 2022.

[10] “MPDC: Mission and Value Statement.” https://mpdc.dc.gov/page/mpdc-mission-and-value-statement, 2021.

[11] M. Austermuhle, “D.C. Metro Police Describe Being First Responders To Insurrection At The Capitol.” https://www.npr.org/2021/01/16/957695863/dc-metro-police-describe-being-first-responders-to-insurrection-at-the-capitol, 2021.

[12] “LAW ENFORCEMENT INFORMATION SHARING.” https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-archive/ise-additional-resources/2142-law-enforcement-information-sharing.

[13] J. Diaz, “D.C. Police Department Victim Of Apparent Ransomware Attack.” https://www.npr.org/2021/04/27/991116344/d-c-police-department-victim-of-apparent-ransomware-attack, 2021.

[14] T. Brewster, “Ransomware Hackers Claim To Leak 250GB Of Washington, D.C., Police Data After Cops Don’t Pay 4 Million Ransom.” https://www.forbes.com/sites/thomasbrewster/2021/05/13/ransomware-hackers-claim-to-leak-250gb-of-washington-dc-police-data-after-cops-dont-pay-4-million-ransom/?sh=60b3b3b058d0, 2021.

[15] A. Mundo, T. Seret, T. Roccia, and J. Fokker, “Technical Analysis of Babuk Ransomware.” https://www.mcafee.com/enterprise/en-us/assets/reports/rp-babuk-ransomware.pdf, 2021.

[16] M. Prathap, “Bitcoin does not make payments anonymous — just really hard to trace.” https://www.businessinsider.in/investment/news/bitcoin-does-not-make-payments-anonymous-just-really-hard-to-trace/articleshow/85068905.cms, 2021.

[17] R. R. Doug Olenick, “Houston rockets investigate ransomware attack.” https://www.databreachtoday.asia/houston-rockets-investigate-ransomware-attack-a-16415, 2021.

[18] “Cyber threats to the aerospace and defense industries.” https://www.fireeye.com/current-threats/reports-by-industry/aerospace-threat-intelligence.html, 2021.

[19] E. Ukwandu, M. A. Ben-Farah, H. Hindy, M. Bures, R. Atkinson, C. Tachtatzis, I. Andonovic, , and X. Bellekens, “Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends.” https://www.mdpi.com/2078-2489/13/3/146, 2021.

[20] F. Erazo, “Ransomware Attack Exposes 1.5TB of Stolen Aerospace Data.” https://cointelegraph.com/news/ransomware-attack-exposes-15tb-of-stolen-aerospace-data, 2020.

[21] R. Lakshmanan, “Malware Attack on Aviation Sector Uncovered After Going Unnoticed for 2 Years.” https://thehackernews.com/2021/09/malware-attack-on-aviation-sector.html, 2021.

[22] N. Thibault Seret, Noël Keijzer, “Babuk : Moving to VM and * nix Systems Before Stepping Away.” https://www.mcafee.com/enterprise/en-us/assets/reports/rp-babuk-moving-to-vm-nix-systems.pdf, 2021.

[23] “Ransomware 101.” https://www.cisa.gov/stopransomware/ransomware-101, 2020.

[24] C. Dong, “Babuk Ransomware.” https://chuongdong.com/reverse%20engineering/2021/01/03/BabukRansomware/, 01 2021.

[25] S. Tripathi, “Babuk Ransomware.” https://www.subexsecure.com/pdf/malware-reports/2021-04/babuk-ransomware.pdf, 2021.

[26] P. H. Dalton Bennett, “Hackers post hundreds of pages of purported internal D.C. police documents.” https://www.washingtonpost.com/local/public-safety/dc-police-hackers-ransomware-babuk/2021/05/13/d0280fb4-b3f7-11eb-a980-a60af976ed44_story.html, 2021.

[27] C. Brooks, “MORE Alarming Cybersecurity Stats For 2021!.” https://www.forbes.com/sites/chuckbrooks/2021/10/24/more-alarming-cybersecurity-stats-for-2021-/, 2021.

[28] D. Braue, “Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031.” https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/, 2021.

[29] M. Eoyang, A. Peters, I. Mehta, and B. Gaskew, “To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors.” https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors, 2018.

[30] “Crime in the U.S. 2019.” https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019, 2020.

[31] “What are Indicators of Compromise?.” https://www.proofpoint.com/us/threat-reference/indicators-compromise, 202.

[32] F. Ordonez, “In Wake Of Pipeline Hack, Biden Signs Executive Order On Cybersecurity.” https://www.npr.org/2021/05/12/996355601/in-wake-of-pipeline-hack-biden-signs-executive-order-on-cybersecurity, 2021.

[33] C. D. Angela S.M. Irwin, “Following the cyber money trail: Global challenges when investigating ransomware attacks and how regulation can help.” https://www.emerald.com/insight/content/doi/10.1108/JMLC-08-2017-0041/full/html, 2019.

[34] “Phishing continues to be one of the easiest paths for ransomware.” https://www.zdnet.com/article/phishing-continues-to-be-one-of-the-easiest-paths-for-ransomware-report/, 2021.

[35] “Protect yourself from phishing.” https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44, 2021.

[36] “Insurance Lessons from the Cyber Attack at DC’s Police Department.” https://terraclaim.com/blog/cyber-security-lessons-from-the-attack-on-dc-police, 06 2021.