Cybercrime Case Study: BLACKCAT

Amiah Armstrong, Jasmyn Wilhelm and Louis Ferrara

TABLE OF CONTENTS

Blackboard to Blackcat

A rhyming narrative by Amiah Armstrong.
Pictures by Jasmyn Wilhelm.

PART 1

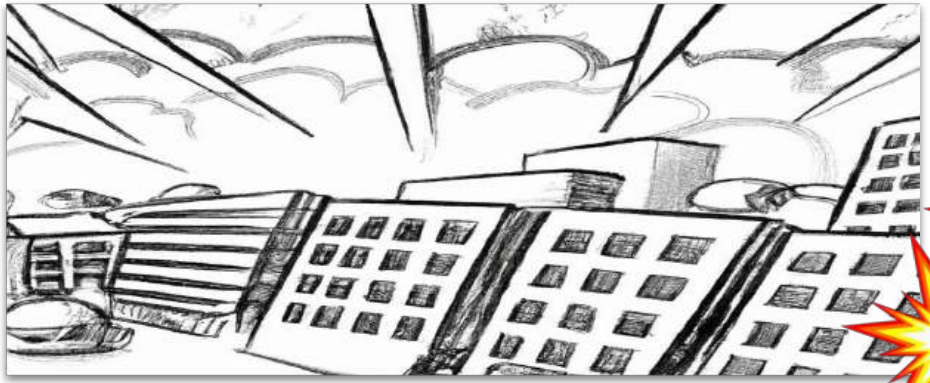
The story follows a man named Robert, a teacher who joins the infamous cybercrime group, Blackcat. Each slide is split into two parts: key excerpts from his journey on the left and detailed answers for each question on the right.

Robert was a teacher in the **South District of Florida**.
Was once a normal man, but then his mind filled with disorder.
He loved his students dearly, but his paycheck? Wasn't a fan.
So he sought to get more money with the evilest of plans.

Instead of grading papers, he surfed the web like a hound.
An organization named the **Blackcat Ransom Group** was found.
It took him months of practice, research, and much more convincing.
But finally, they let him join the organization like he's been dreaming.

Who were the key participants in the crime and investigation?

- There were a ton of victims, many being within the South District of Florida. Whereas the perpetrators were members of the Blackcat Ramson group.
- Within this specific story, Robert is the main perpetrator.



He learned to encrypt a victim's data and use it as a weapon.
A ransom was then demanded. The victims were oh-so frightened.
They gave him what he wanted, not wanting their data to leak.
Blackcat got richer, and so did Robert's paycheck each week.

The work he did was dangerous, but he did not fret.
Even when knowing the **FBI Miami Division** was on his back.
His high level teaching position gave him a shield.
He thought, "Who would believe a teacher would steal?"

He targeted **medical firms, financial firms, critical infrastructures, law districts.**
He sent ransoms to victims from **across the world** and his own **school district**.
"The power!" He yelped. "The money I've earned!"
"Blackcat Ransomware is making them squirm!"

Who were the key participants in the crime and investigation?

- The agency that investigated Blackcat's crimes was the FBI Miami Division.
- Victims include, but was not limited to, Medical firms, financial firms, critical infrastructures, law districts, and school districts.

When he had time, he would read articles at a fast pace.
Relishing on his crimes with a grin on his face.

Krebson Security

One was about Change Healthcare, who paid $22 million dollars to Blackcat.
The hack caused so many problems, patient's couldn't get their prescriptions back!
Numerous healthcare providers and insurance companies suffered.
Robert had no remorse, and Blackcat got stronger.

Security Week

Ebsworth law firm in Australia was also hit with an attack.
Blackcat stole 4 terabytes of data, and Robert was a part of that.
The data that was taken was then published on the dark web.
Robert grinned with delight, his future free of any dread!

How did the media cover the crime?

The media had a stark reaction to Blackcat's crimes. They instilled lots of fear in their articles, insinuating that anybody and everybody can get attacked at any moment.

"The affiliates still have this data, and they're mad they didn't receive this money, Smilyanets told Wired.com. "It's a good lesson for everyone. You cannot trust criminals; their word is worth nothing."

CYBERCRIME

Australian Government Says Its Data Was Stolen in Law Firm Ransomware Attack

The Office of the Australian Information Commissioner (OAIC) says some of its files were stolen in a ransomware attack on law firm HWL Ebsworth.

The Office of the Australian Information Commissioner (OAIC) says some of its files were stolen in a ransomware attack on law firm HWL Ebsworth.

One of the largest law firms in Australia, HWL Ebsworth says in an incident notice on its website that it became aware of the incident on April 28, after the Alphv/BlackCat ransomware gang boasted about the hack, and that it immediately informed the Australian authorities and started investigating the incident.

TRENDING

1 OpenAI Says Iranian Hackers Used ChatGPT to Plan ICS Attacks

2 Splunk Enterprise Update Patches Remote Code Execution Vulnerabilities

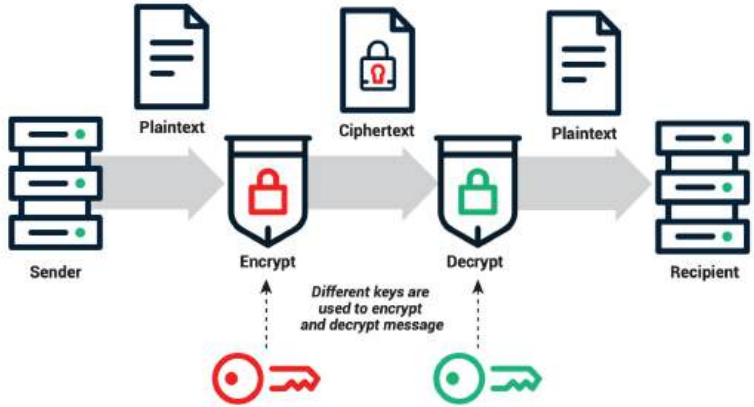
At least, that's what he thought. Until the **FBI utilized CHS**.
The **Confidential Human Source** group caused a lot of stress.
They **infiltrated networks to breach BlackCat's systems,**
And through secret access, they communicated with victims.

They also got a **search warrant** to seize a bunch of keys.
They thieved the thieves and **seized the keys, 946 of these**.
The evidence against Blackcat was stacking up so high.
"My evil deeds are nearly through", Robert said with a sigh.

How was the crime investigated?

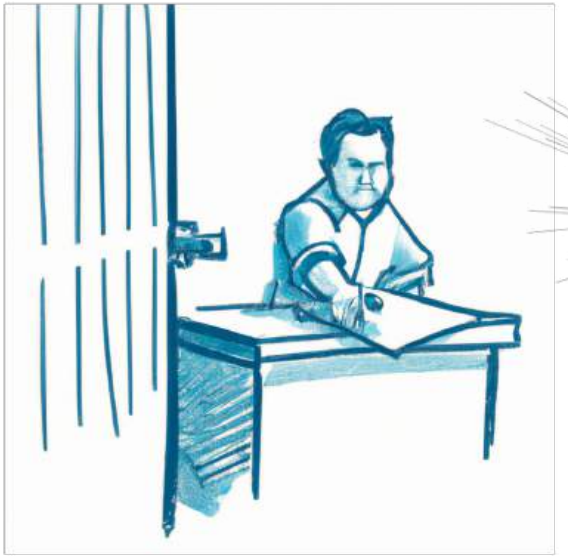
- The Confidential Human Source is an individual who has gained direct access to criminal organizations and report their findings. Those same people also were able to contact victims.
- The FBI got a search warrant and took 946 public/private key pairs, all found on a flashdrive.
- The FBI helped over 400 victims worldwide, giving decryption tools in order to get their information back.

Was found inside :O



Robert's reign began to crumble and so did Blackcat's.
There were **no court proceedings or arrests**, though his future lies flat.
Trials came from within the org, and the group lost its grip.
As members turned informants, the organization began to slip.

His paycheck went back to normal as he left the thieving group.
He's back to grading papers, drowning in an endless loop.
Until he heard a knock on the door. The coffee shook in his cup.
He held his breath when he heard, "FBI, open up!"



What was the outcome of the court proceedings?

- Currently, there is no knowledge on any court proceedings or arrests involving Blackcat. The evidence collected against Blackcat is currently being preserved to be used in future legal proceedings.
- There are implications that the group tore themselves apart due to mistrust, but nothing confirmed.

The End :D

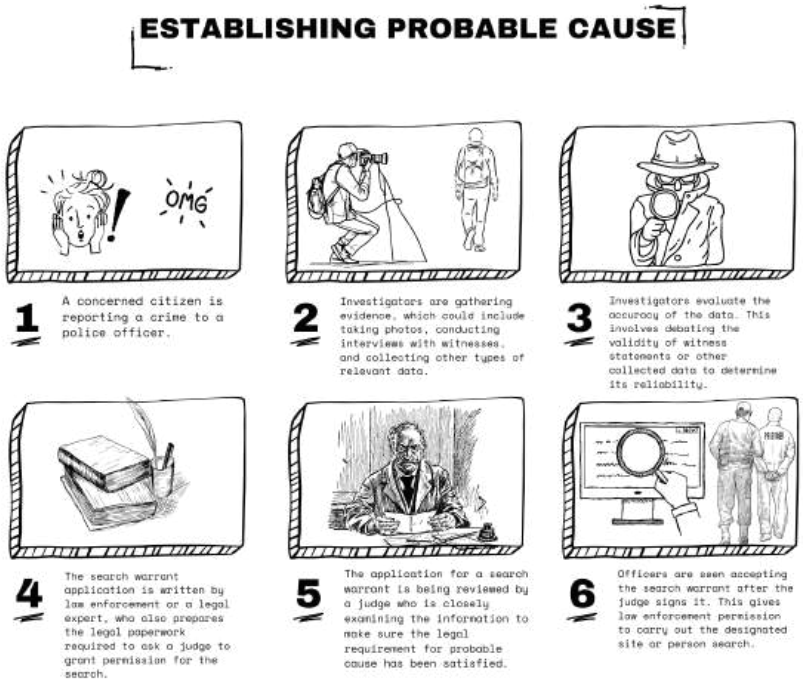
Fourth Amendment Review: Search Warrant Affidavit Compliance

Evidence and composition by Louis Ferrara and Jasmyn Wilhelm

PART 2

Part 2 is a deep dive into the affidavit that was selected. It will explain how the application satisfies the requirements of the Fourth Amendment, focusing on key aspects such as probable cause, things to be seized, and the nexus between evidence and crime.

Establishing Probable Cause for Search Warrant Application



Description of evidence from search warrant application

ATTACHMENT B

Items to be Seized

All public/private encryption key pairs associated with Tor sites used by the Blackcat Ransomware Group for purposes of effectuating a criminal scheme in violation of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B) (computer fraud), 18 U.S.C. § 371 (conspiracy to commit computer fraud), and 18 U.S.C. § 1956(h) (conspiracy to commit money laundering), including Tor sites hosting and facilitating Blackcat-linked victim communications sites, leak sites, and panel sites.

Probable cause was established in the search warrant application by presenting facts to show that a crime had occurred.

Specifically, the application referenced the time frame (December 2021-current) that the Blackcat ransomware group was using ransomware to illegally collect data to blackmail and extort their victims. The FBI had an informant who obtained information and evidence as to the inner workings of the Blackcat group and how they would use public and private keys on the Tor network to communicate without detection. Over the course of the investigation 946 unique keys were obtained and stored on the flash drive that is the subject of the search warrant request.

There is probable cause to believe that there is relevant evidence to the crimes committed by the Blackcat group on the Flash drive.

Establishing Particularity in the Place to Be Searched

Law Enforcement Obtained the Public/Private Key Pairs to 946 Blackcat-Linked Tor Sites

25. During this investigation, law enforcement gained visibility into the Blackcat Ransomware Group's network. As a result, the FBI identified and collected 946 public/private key pairs for Tor sites that the Blackcat Ransomware Group used to host victim communication sites, leak sites, and affiliate panels like the ones described above. The FBI has saved these public/private key pairs to the Flash Drive.

26. As noted above, each Blackcat victim received a unique public Tor address through which to engage in negotiations. The FBI has conducted extensive and ongoing outreach to victims. This outreach includes a decryption operation using a tool the FBI developed, which the FBI has offered to over 400 victims around the world. The FBI has also identified public Tor addresses associated with victim communication sites and has confirmed that several of these victim communication sites were among the public/private key pairs collected.

The search warrant application provided facts to demonstrate that a search of the flash drive would result in evidence relevant to the Blackcat Ransomware Group criminal activities. The application noted that in the course of the investigation "the FBI identified and collected 946 public/private key pairs for Tor sites that the Blackcat Ransomware Group used to host victim communication sites, leak sites, and affiliate panels" and that the FBI had stored the key pairs on the flash drive. The key pairs were critical to members of Blackcat being able to communicate with each other and with victims online without detection so they are relevant evidence to the investigation.

Particularity in the Things to be Seized

To establish particularity in the person or things to be seized the individual requesting a search warrant must describe in detail the evidence expected on the device.

The FBI satisfied this requirement with a detailed explanation of the 946 unique key pairs that were obtained during the investigation of the Blackcat Group and how those key pairs were integral to the criminal enterprise as it allowed the suspects to communicate online without detection. The search warrant application included the date range (December 2021 to present date of the application), type of records (946 public/private key pairs) and what evidence the records might reveal (the key pairs link to leak sites that are used during the ransomware attacks).

Law Enforcement Obtained the Public/Private Key Pairs to 946 Blackcat-Linked Tor Sites

25. During this investigation, law enforcement gained visibility into the Blackcat Ransomware Group's network. As a result, the FBI identified and collected 946 public/private key pairs for Tor sites that the Blackcat Ransomware Group used to host victim communication sites, leak sites, and affiliate panels like the ones described above. The FBI has saved these public/private key pairs to the Flash Drive.

26. As noted above, each Blackcat victim received a unique public Tor address through which to engage in negotiations. The FBI has conducted extensive and ongoing outreach to victims. This outreach includes a decryption operation using a tool the FBI developed, which the FBI has offered to over 400 victims around the world. The FBI has also identified public Tor addresses associated with victim communication sites and has confirmed that several of these victim communication sites were among the public/private key pairs collected.

27. The FBI also visited the primary leak site the Blackcat Ransomware Group provided to victims during attacks and several additional Tor sites that appear to support the functioning of this primary leak site. The FBI also visited several secondary leak sites, linked from the primary leak site, that hosted stolen victim data that the Blackcat Ransomware Group published for apparent extortion purposes. The FBI has confirmed that the visited sites were among the public/private key pairs collected.

9. A Tor hidden service generates its .onion address by creating "public/private keypairs." Public/private key pairs are elements of "asymmetric cryptography." In asymmetric cryptography, one key is used to encrypt the material and the other is used to decrypt it. In the case of Tor hidden services, the public key, which is the .onion address, allows users to access the hidden service and may be

4

widely disseminated. The private key, which is intended to be kept secret, controls the use of the .onion.

10. Users seeking to visit the site of a hidden service are not able to connect to the hidden service directly. Instead, hidden services broadcast their public keys to "introduction points," which are nodes in the Tor network that facilitate connections between hidden services and their users. There are many possible introduction points in the Tor network. Once the public keys are broadcast, the hidden service will package its public key and information about its chosen introduction points. This package, called a "hidden service descriptor," must be signed by the hidden service's private key. In this way, any entity that has the private key associated with the .onion address can create a new hidden service descriptor with a new set of introduction points.

11. The hidden service descriptor is uploaded to a "distributed hash table." A user who wants to access the hidden service will download the hidden service descriptor associated with the site's .onion address. The user can then send an encrypted message to one of the hidden service's introduction points, which would pass the message along to the hidden service, along with information about a

Establishing Nexus between Evidence and Crime

The Blackcat Ransomware Group search warrant application successfully established a nexus between the evidence on the flash drive (the target of the search warrant) and the crimes committed by the Blackcat Group.

Since it cannot be assumed that the judge reviewing the search warrant application is an expert in digital forensics the warrant application begins by explaining what ransomware and Tor software are before going into detail about how the public and private keys that are expected to be on the flash drive allowed the criminals to communicate with their victims on websites that were set up as hidden services.

WORK CITED

Arghire, I. (2023, June 20). *Australian government says its data was stolen in law firm ransomware attack*. SecurityWeek. https://www.securityweek.com/australian-government-says-its-data-was-stolen-in-law-firm-ransomware-attack/

BlackCat ransomware group implodes after apparent $22M payment by Change Healthcare. (2024, March 5). https://krebsonsecurity.com/2024/03/blackcat-ransomware-group-implodes-after-apparent-22m-ransom-payment-by-change-healthcare/

Shanklin, W. (2023, December 19). The DOJ says it disrupted the Blackcat ransomware group. *Engadget*. https://www.engadget.com/the-doj-says-it-disrupted-the-blackcat-ransomware-group-174755936.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAF33wpsHgu0cAcpV7zxcci9TbaaTc5Pvfy2kMv0XB6SHSJqWq4C6PcIcmEdAkrG7LYv5IvN5AaFjkBdRJ7OituT02NRmr8lyLSu8gQO8gEMLEYkyOvxiupFoS8qYdqkFlAel98jkz5mXdWP6KL2vHAhsVTHtSCTD0PBraP9QktI0

Pictures on slides four, five, and eight were sketched and then brought to life by Canva Editing AI.