BLACKCAT RANSOMWARE GROUP CASE STUDY

Overview

- In this presentation I will be discussing the affidavit of the Blackcat Malware Group. This will include key participants, how the crime was investigated, and the outcome of the court proceedings. This will also address how probable cause, the particularity of the place searched, and the particularity in the things to be seized was established. Along with examples of how the media covered the crime.

Key Participants in the Crime and Investigation

- Perpetrators – The Blackcat Ransomware Group which are the developers of the blackcat malware and the affiliates who are responsible for identifying and attacking high-value victim institutions with the ransomware.
- Victims – Institutions around the world within the Southern District of Florida. These would include critical infrastructure entities, medical facilities, school districts, law firms, and financial firms.
- Agencies – FBI

EXAMPLES OF HOW THE MEDIA COVERED THE CRIME

https://www.cisecurity.org/insights/blog/breaking-down-the-blackcat-ransomware-operation

https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant

How the crime was investigated

- According to the affidavit, hundreds of Blackcat victims worldwide have reported they were receiving links to unique victim communication sites after they have been attacked an had their data appear in Blackcat's leak sites. The leak site discloses information about victims and the data they have stolen. This primary leaded site links to other leak sites on Tor where stolen victim data are publicly available.
- The blackcat Ransomware Group also operates password-protected Tor-based web panels that allows their affiliates and developers to communicate, manage, and coordinate Blackcat attacks with each other. Law enforcement worked undercover to contact individuals who provided credentials to the panels in which they engaged a Confidential Human Source (CHS) who consistently provides reliable information regarding ongoing cyber crime investigations.
- The CHS responded to an advertisement that was posted to a public online forum that was soliciting applicants for Blackcat affiliate positions. A member of the Blackcat Ransomware Group responded to the CHS and asked specific questions to determine the CHS's technical proficiency in network intrusion. The CHS responded to the Blackcat Ransomware Group member's satisfaction. Then provided the CHS with access credentials to a Blackcat affiliate panel, available at a unique Tor address.
- The CHS visited the page and confirmed that this was the login page for a Blackcat affiliate panel and accessed the panel. Law enforcement accessed the panel pursuant navigated the panel, and determined how it works. The affiliates use the panel to manage each ransomware attack on a victim throughout the attack lifecycle thus includes the ransomware deployment through payment and decryption of victim data. Law enforcement eventually eventually gained visibility into the Blackcat Ransomware Group's network.

The outcome of the court proceedings

- The outcome of the court proceedings is that there is probable cause for a warrant authorizing the search of a SanDisk Flash Drive, to seize private keys to Tor sites used by the Blackcat Ransomware Group to maintain it criminal plans.

How probable cause was established

- Probable cause was established when the FBI identified and collected 946 public/private key pairs for Tor sites, and affiliate panels. They also identified public Tor addresses associated with victim communication sites, and it was confirmed that many of the sites were among the public/private key pairs collected. The FBI visited the Blackcat Ransomware Group primary leak site that was provided to victims that were attacked as well.
- The FBI also visited many secondary leak sites from the primary leak site that hat hosted stolen victim data for extortion purposes. The FBI confirmed that the visited sites were among the public/private key pairs.
- The Blackcat affiliate address that was provided to the CHS in the undercover operation was also confirmed in the public Tor addresses collected. They also visited a sampling of the collected Tor addresses that were public with associated private keys and confirmed that visited sites were consistent with known Blackcat victim communication sites, leak sites, and panels.

How particularity in the place searched was established

- How particularity in the place to be searched was established is that the public/private keys were put on a SanDisk flash drive and collected by the FBI. They then put it in a storage at the addresses 2030 SW 145TH Avenue, Miramar Florida which is an FBI facility located in the Southern District of Florida.
- The FBI Agent also mentions that he knows the Flash Drive has been stored in a manner in which its contents are, to the extent material to the investigation, in the same state as they were when the FBI first came into the possession of it.

How particularity in the things to be seized was established

- How particularity in the things to be seized was established is that the FBI and the Agent have knowledge of the Blackcat Ransomware Group using public/private encryption keys associated with Tor sites they used for purposes to accomplish criminal plans. These public/private encryption keys are the ones in which which the FBI has collected on the Flash Drive.
- According to the affidavit, the Blackcat Ransomware Group's actions are 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) which includes Tor sites hosting and facilitating Blackcat-linked victim communications sites, leak sites, and panel sites.

How the nexus between evidence and crime was established

- How the nexus between evidence and crime was established is that the FBI noticed the victims of the Blackcat Ransomware Group were reporting that there was a general attack flow. They would report receiving links to unique victim communication sites and have their data appear on Blackcat's leak sites. One the FBI was able to gain access as an Blackcat affiliate with help of a Confidential Human Source (CHS) they could see all the victims that were attacked.
- Affiliates are able to see the victim, entity, full ransom price demanded, discount ransom price, expiration date, cryptocurrency transactions, type of computer system compromised, ransom demand not, chats with the victim, and more.
- The FBI gained visibility into the Blackcat Ransomware Group's network and collected 946 public/private keys for Tor sites that they used to host communication and victim sites and affiliate panels. The FBI then identified public Tor addresses associated with victim communication sites and were able to confirm that many of the the sites were among the public/private key pairs collected. They also visited the primary and many secondary links and were able to confirm they also were among the public/private key pairs collected.