Blackcat Ransomeware Group

by Danny Choi and Jordan Johnson

Introduction

- What is this presentation about?
- Breakdown of the presentation

Let’s break it down

- What is Blackcat?
  - ...
- How did the operations work?
- What is Tor?
- What is the Onion?

Affidavit Analysis

Key Points

Probable Cause?

Particularity

Nexus

3. Based on my training and experience, and the facts set forth in this Affidavit, there is probable cause to believe that individuals affiliated with a ransomware strain known as Blackcat (also known as ALPHV or Noberus, but hereinafter "Blackcat") have violated 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). There is also probable cause to search the Flash Drive, as described in Attachment A, to seize the public/private encryption key pairs for websites used by Blackcat-affiliated individuals to perpetuate their criminal activity, as described below and in Attachment B.

Blackcat Panels

18. In addition to victim communication and leak sites, the Blackcat Ransomware Group also operates password-protected Tor-based web panels (i.e., online interfaces that can control different aspects of a server) that allow its affiliates and developers to communicate, manage, and coordinate Blackcat attacks amongst themselves. Law enforcement worked to make undercover contact with individuals who provided credentials to these panels. Specifically, law enforcement engaged a Confidential Human Source ("CHS") who routinely provides reliable information related to ongoing cybercrime investigations.

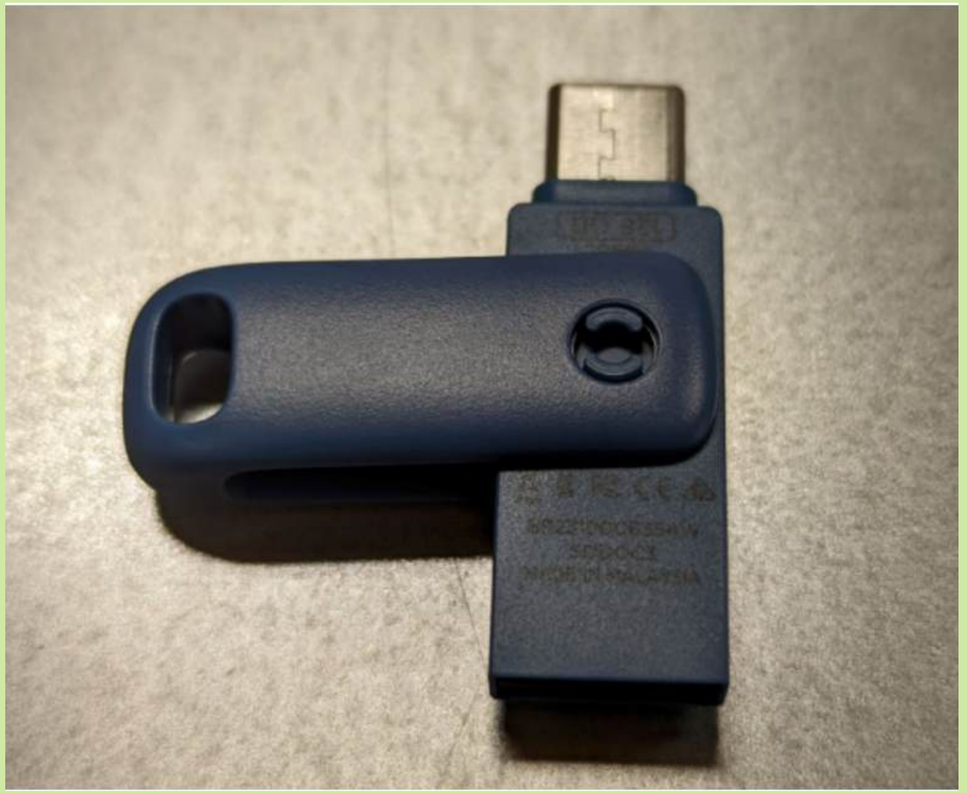
19. The CHS responded to an advertisement posted to a publicly-accessible online forum soliciting applicants for Blackcat affiliate positions. A member of the Blackcat Ransomware Group responded to the CHS and asked questions designed to gauge the CHS's technical proficiency with network intrusion. The CHS responded to these questions to the Blackcat actor's satisfaction. The Blackcat actor then provided

the CHS with access credentials to a Blackcat affiliate panel, available at a unique Tor address. The CHS visited this page, confirmed that this was the log-in page for a Blackcat affiliate panel, and accessed the panel.

Blackcat and the Tor Network

23. The Blackcat Ransomware Group's victim communication sites, leak sites, and panels have been able to remain online because they are set up as hidden services on the Tor network.

24. For example, users who wanted to access the primary Blackcat leak site on the Tor network would download the descriptor for the public key represented as the Tor .onion address for that site. The users would be able to view the primary Blackcat leak site through a rendezvous point. As noted above, control of a Tor .onion domain depends on a user knowing both the public key—the .onion address—and the private key that typically is kept secret by the user who created the site. However, any individual who also possessed the private key associated with a public Tor .onion address would have the complete public/private key pair and could consequently broadcast a new route redirecting traffic for the .onion site to a different server. Put another way, the individual holding the private key to the primary Blackcat leak site could redirect users to whatever different content they wanted the users to see. In essence, control over the public/private key pairs to a Blackcat-linked Tor site grants



Harm and Impact

- Critical infrastructure organizations
- Hospitals and schools
- Financial firms and law practices
- Global impacts

Timeline

01

2021

- Blackcat ransomware emerges.
- Affiliates begin targeting global victims

02

Early 2022

- Florida-based victims reported systems encrypted.
- FBI confirms Blackcat tactics

03

2022-2023

- Hundreds of victims worldwide report stolen data appearing on Blackcat leak sites

04

Mid 2023

- Law enforcement uses a Confidential Human Source (CHS) to gain affiliate panel access

Timeline

05

Late 2023

- FBI seizes 946 public/private key pairs controlling Blackcat's Tor sites.

06

December 2023

- FBI Special Agent Aaron Tijerino files a sealed affidavit

07

Aftermath

- FBI begins outreach to victims, offering decryption tools

Thank You

Work Cited:

Blackcat Affidavit