DFIR Ransomware Project

… or …

Sampling The Ransomware Families Using A Framework

Brian Carrier

CTO

Basis Technology

Brian Moran

Consultant

BriMor Labs

September 13, 2022

bcarrier@ResponderCon:~$ whoami

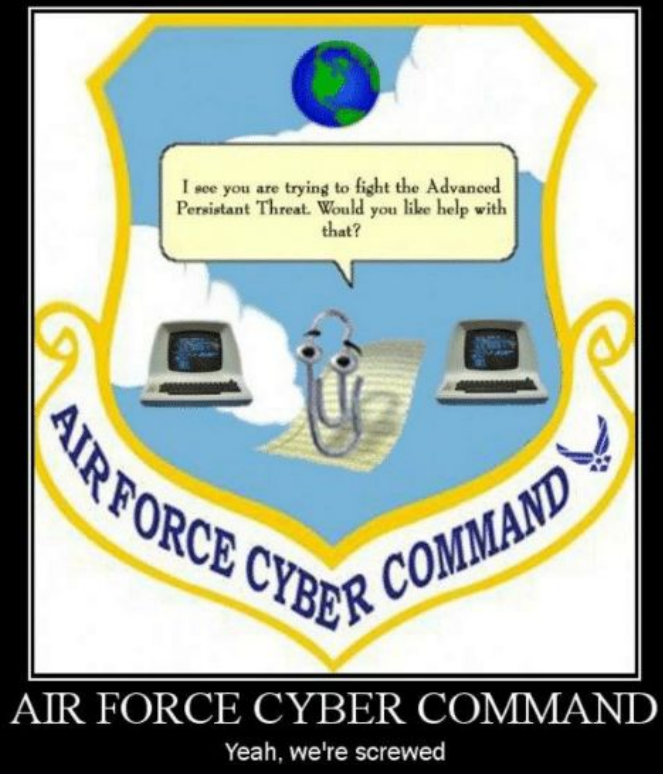
- Hello, my name is Brian Carrier
- <Ad lib some things
  - More details
  - More details

- My hair is awesome

bmoran@ResponderCon:~$ whoami

- Hello, my name is Brian Moran
- 13+ years Air Force career
  - ~20 years mobile exploitation & DFIR focus
  - Started BriMor Labs in 2014
- #DFIRFit

- Random fact about me: U.S. Presidential candidate in 2008 and 2012



Ransomware Variations

- There are many ransomware variants out there, and they are ALL REALLY different
  - Or … are they?
- As you research ransomware families, you'll learn:
  - Novel encryption algorithms
  - Unique threading models that make them more efficient
  - New programming languages
  - Obfuscation technique
  - … and more!
- BUT … while interesting, do they really impact incident responders? (ANSWER: NO!)

Ransomware DFIR Concerns

- Malware researchers provide HUGE value by publishing reverse engineering breakdowns
- But, they are unlikely to focus on items that DFIR folks care about, like
  - How did the attacker(s) get in?
  - What computers/systems were compromised?
  - What, if any, C2 infrastructure was installed?
- Sometimes ransomware type helps answer those questions
- Our goal was to make a resource focused on ransomware families, from a DFIR perspective, focusing on WHAT YOU NEED TO KNOW

Presentation Breakdown

- Overview of the DFIR Ransomware Project
- Review five ransomware families, and how they map out to the framework
- Bruno?
- And, perhaps most importantly, how YOU can get involved!


We don't talk about
Bruno-no-no-no

Do We Need YAFW?

- There are a multitude of frameworks already in existence
- THEN WHY?!?
- Want to create a single stop, community driven, resource available to everyone
- Will only use publicly available information
  - Also will cite any and all sources

THE FRAMEWORK IS MEANT TO BE A REFERENCE FOR A RANSOMWARE INCIDENT
IT IS NOT MEANT TO BE A GUIDE/PLAYBOOK IN WHICH TO FIT A RANSOMWARE INCIDENT

Does This Compliment _____ Framework?

- **Yes**
  - Any framework will have some overlap
    - Because a framework is a framework
      - NOT an investigation guide

- What if something listed is incorrect, or inaccurate?
  - Please contribute!! Trying to help others is one of the most powerful things a responder can do

DFIR Ransomware Project

- Essentially, this is a framework that breaks down characteristics/traits/observables of ransomware into 12 distinct areas
  - ONLY focuses on ransomware itself
    - NOT additional executables
    - NOT FOCUSING on geopolitical and/or nation state activities

DFIR Ransomware Project

Framework Overview

Ransomware Family Background	First Observed			Threat Actor(s)	
Environment	Affected Platforms				
Ransomware Family Specific Artifacts	Extensions	Ransomware Notes	Disabled Services	Other Observable(s)	
Automation	Initial Access	Privilege Escalation	Human Operated	Exfiltration	Propagation

Ransomware Family Background

- **First Observed**
  - This is the date/time frame when the ransomware was first publicly confirmed to be observed
  - You can use this to know if the family is new or old

Ransomware Family Background

- **Threat Actor(s)**
  - Publicly confirmed and attributed usage by any (and all) threat actor groups using it
    - NOT TO BE USED FOR ILLICIT PURPOSES
      - Sole purpose is to establish additional possible TTPs/indicators to look for in YOUR environment

Environment

- **Affected Platforms**
  - Publicly confirmed information on what operating system(s) the ransomware targets/works on
    - Most will be Windows based systems
      - Some are *nix/ESXi
  - You can use this to help scope what other systems could be infected

Ransomware Family Specific Artifacts

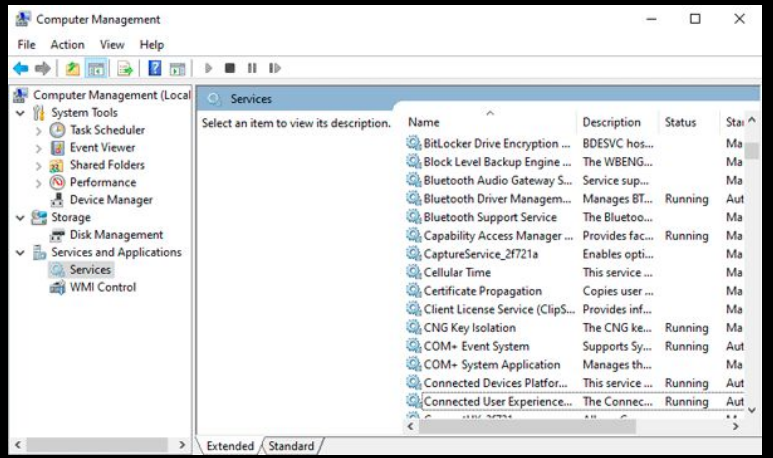
- **Extension(s)**
  - Publicly confirmed file extension(s) that is indicative of the ransomware family that was leveraged in the incident
    - This may vary WIDELY
      - Again, focusing only on publicly available information
  - You can use this to search for scope of incident and get timestamps of when encryption started

Ransomware Family Specific Artifacts

- **Ransomware Notes**
  - A listing of all known ransomware note names and/or file extensions/locations/etc
    - This may vary WIDELY
      - Again, focusing only on publicly available information
  - You can use this to search for scope of incident and get timestamps of when encryption started

Ransomware Family Specific Artifacts

- **Disabled Services**
  - A listing of specific services that the ransomware disables in an environment
    - This may vary WIDELY
  - You can use this to understand why some alerts were not generated

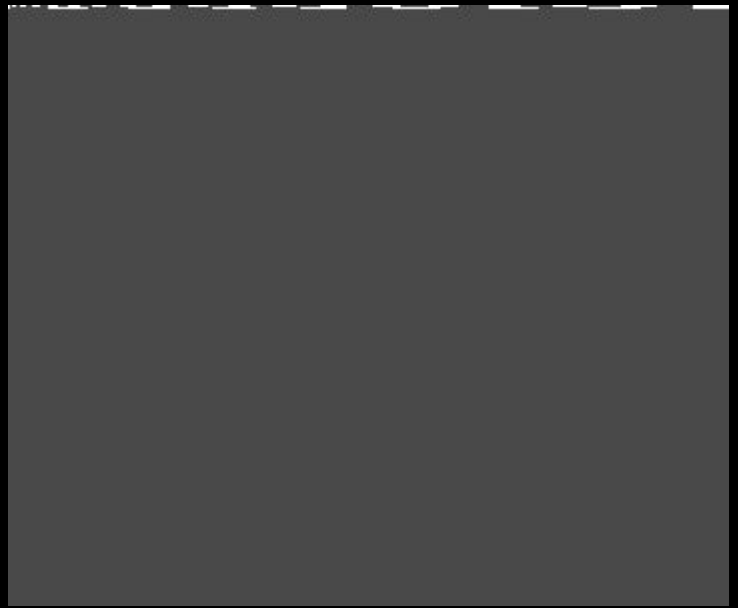


Automation

- **Initial Access**
  - Does the ransomware itself contain built-in functionality to gain access to an environment?
    - If not, the attribution of the actor(s) may help reveal initial access vectors
      - May also be through a variety of common access methods
  - You can use this to know if you need to look for how they got in

Automation

- **Privilege Escalation**
  - Is there built in privilege/ account escalation? How?
    - If not, may also be through a variety of common methods
  - You can use this to scope the incident and determine which were vulnerable



Automation

- **Human Operated**
  - While similar to *propagation*, does the ransomware require human interaction to perform environment reconnaissance and/or target systems/files/etc?
    - If not, actor(s) attribution may help identify reconnaissance methods
      - May also be through a variety of common survey methods
  - You can use this to know if you need to search for C2

Automation

- **Exfiltration**
  - Does the ransomware automatically exfiltrate data?
    - If so, how? And how much? What? When? Where?

Automation

- **Propagation**
  - Does the ransomware spread throughout the environment on its own, without any human interaction?
    - Similar to previous entries under automation
      - This area focuses more on the “spread” of ransomware once in the environment
        - » AKA: Is it pushed from the Domain Controller via a batch script, or is it a worm moving through the environment?
  - You can use this to help trace backwards from encrypted systems

Let’s See It In Action!!

- Let’s take five ransomware families, and detail how they map to the DFIR Ransomware Project
  - Conti
  - BlackCat
  - LockBit 2
  - Hive
  - WannaCry

Ransomware Framework: Conti

- Per Coveware, Conti accounts for roughly 6% of ransomware incidents

Ransomware Family Background

- First Observed: First publicly observed in late 2019
- Threat Actor(s): Conti group (aka Wizard Spider/TrickBot)
  - Also many other names (why can't we just call it one thing?)

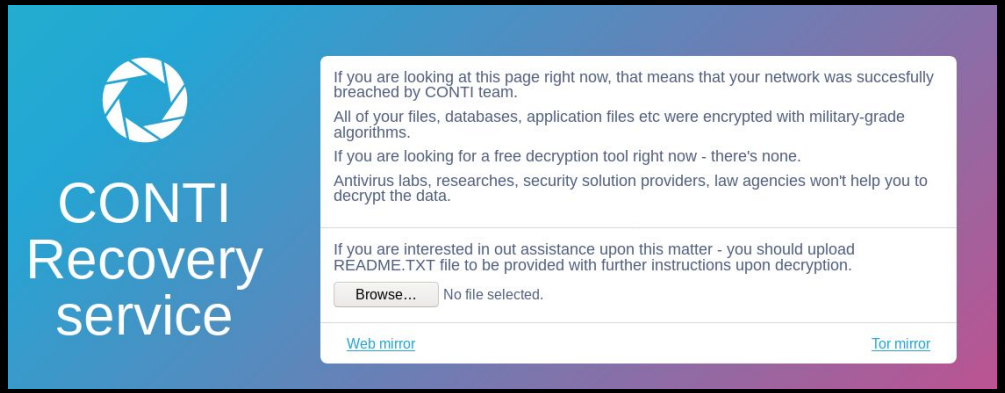
Environment

- Affected Platforms: Windows operating systems

Ransomware Framework: Conti

Ransomware Family Specific Artifacts

- Extensions:
  - .conti
  - 5 alphanumeric characters
- Ransomware Notes:
  - Readme.txt
  - CONTI.txt
  - R3ADM3.txt
  - CONTI_README.txt



Ransomware Framework: Conti

Automation

- Initial Access: No
  - Has been observed using RDP, and phishing/TrickBot
- Privilege Escalation: No
- Human Operated: Yes
- Exfiltration: No
  - Data exfiltration may happen manually by attacker
    - Not part of ransomware executable itself
- Propagation: No

Ransomware Framework: BlackCat

- Per Coveware, BlackCat accounts for roughly 17% of ransomware incidents

Ransomware Family Background

- First Observed: Late 2021
- Threat Actor(s): MS DEV-0504 and MS DEV-0237

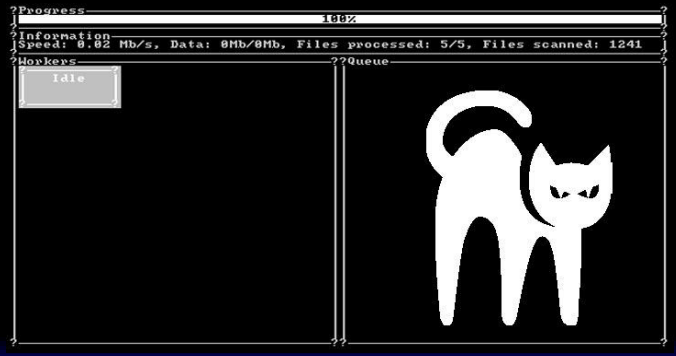
Environment

- Affected Platforms: Windows and ESXi operating systems

Ransomware Framework: BlackCat

Ransomware Family Specific Artifacts

- Extensions: Victim specific
  - Determined in the ransomware configuration file
  - 7 random characters in length
- Ransomware Notes:
  - “RECOVER-<EXTENSION>-FILES.txt”



Ransomware Framework: BlackCat

Automation

- Initial Access: No
  - Initial access via compromised credentials (usually)
- Privilege Escalation: No
- Human Operated: Yes
  - Credentials hard coded into executable, but is “non-wormable”
- Exfiltration: No
- Propagation: No

Ransomware Framework: BlackCat

- Other notable traits
  - Written in Rust
  - Clears Windows Event Log files

Ransomware Framework: LockBit 2

- Per Coveware, LockBit 2 accounts for roughly 13% of ransomware incidents

Ransomware Family Background

- First observed: mid-late 2021
- Threat Actor: UNC2165 (EvilCorp)

Environment

- Affected Platforms: Mainly affects Windows and ESXi operating systems

Ransomware Framework: LockBit 2

Ransomware Family Specific Artifacts

- Extensions: .lockbit file extensions
- Ransomware Notes:
  - Desktop wallpaper
  - Pop up window (spawns from .hta)
  - Restore-My-Files.txt

Ransomware Framework: LockBit 2

Automation

- Initial Access: No
  - Initial Access usually comes via stolen credentials
- Privilege Escalation: Yes … and also UAC bypass
- Human Operated: Yes
- Exfiltration: No
  - Does often leverage StealBit
- Propagation: Yes
  - Creates scheduled task to launch ransomware
  - Uses AD API to perform LDAP queries
  - Resulting output is used to spread to other systems
    - Ransomware is launched via scheduled task(s)

Ransomware Framework: LockBit 2

- Other notable traits:
  - Deletes System, Application, and Security Event Logs
  - Adds itself to “Run” key in Windows Registry
  - Deletes backups
  - Executable checks for, and does not run on, systems with Russian/Eastern European keyboard settings
  - Ransomware executable cleans up after itself
    - Runs “fsutil” to empty executable file
    - Force deletes remnant file in quiet mode

Ransomware Framework: Hive

- Per Coveware, Hive accounts for roughly 6% of ransomware incidents

Ransomware Family Background

- First Observed: Mid 2021
- Threat Actors: TBD

Environment

- Affected Platforms: Windows operating systems

Ransomware Framework: Hive

Ransomware Family Specific Artifacts

- Extensions:
  - .key
  - .hive
- Ransomware Notes: “How_to_decrypt.txt” (most common)

Disabled Services

- Disables (at least) 34 services, associated with security solutions and anything else that might impede the ransomware process

Ransomware Framework: Hive

Automation

- Initial Access: No
  - Usually compromises an environment through RDP with phished credentials
- Privilege Escalation: No
- Exfiltration: No
- Propagation: No

Ransomware Framework: Hive

- Other notable traits:
  - Originally written in GO, have migrated to Rust
  - Multiple versions/iterations of ransomware
  - Public decryptor available for “V5”

So many versions available, it is tough to differentiate

Ransomware Framework: WannaCry

- WannaCry, surprisingly, is STILL around, but not as prevalent as it once was

Ransomware Family Background

- First Observed: May 2017
  - It was around prior, but May 17 the “date”
  - Affecting 300,000+ in 150+ countries in hours will do that
- Threat Actor(s): “Korth Norea”

Environment

- Affected Platforms: Windows operating systems

Ransomware Framework: WannaCry

Ransomware Family Specific Artifacts

- Extensions:
  - .wannacry
  - .wcry
  - .wnry
  - .wncry
- Ransomware Notes: “info.hta”

Ransomware Framework: WannaCry

Automation

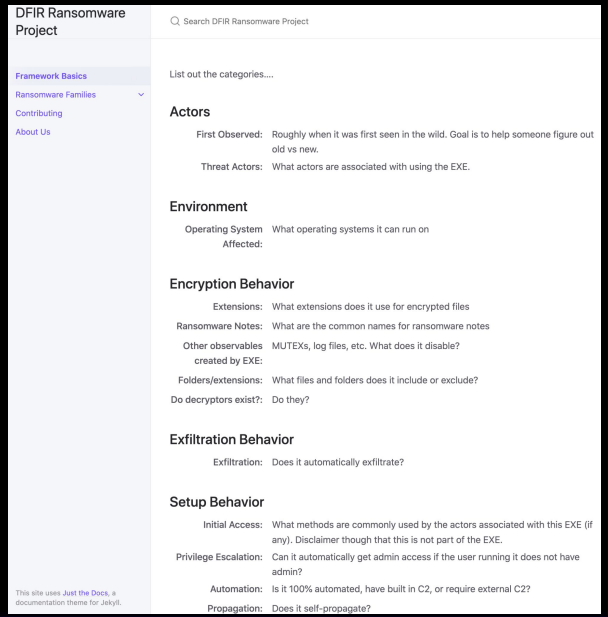
- Initial Access: Yes
  - Initial spread was via EternalBlue (SMB vulnerability)
- Privilege Escalation: No
- Human Operated: No
- Exfiltration: No
  - Not in original version(s)
- Propagation: Yes
  - EternalBlue exploit allowed ransomware to spread as “wormable”

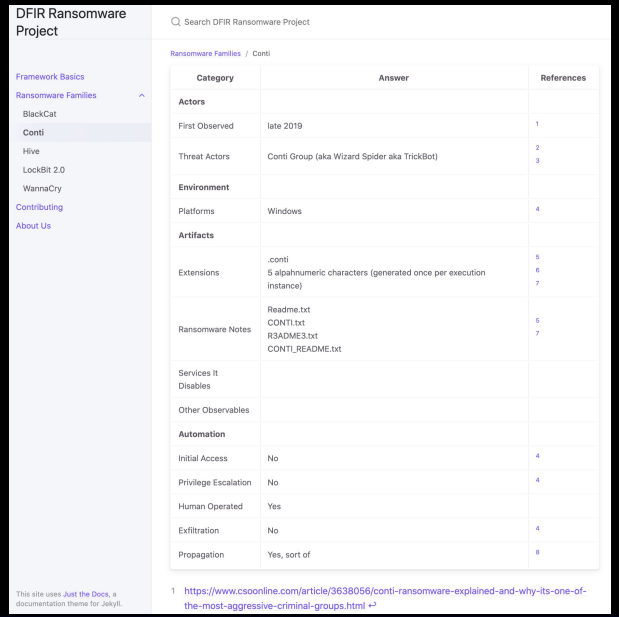
DFIR Ransomware Project

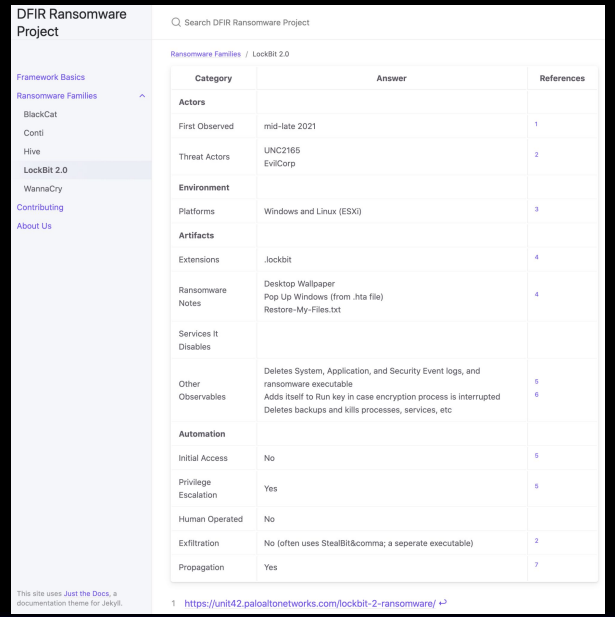
Heather approves

How Can I Help?

https://dfirransomware.org/

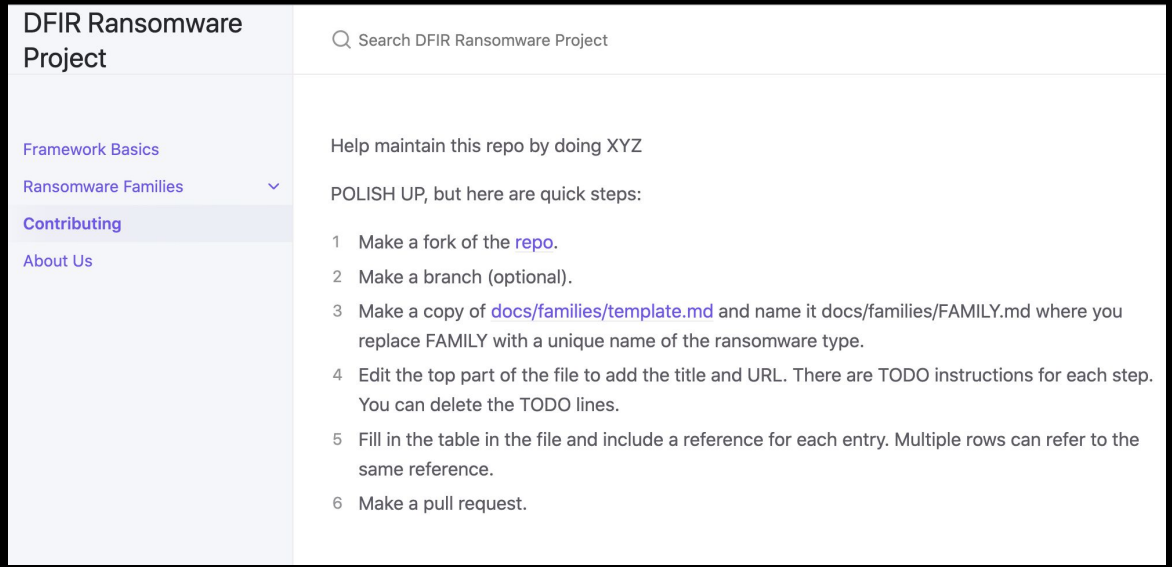






How Can I Help?

- Something missing? Something to add? Please go here: https://dfirransomware.org/contribute/



Questions?

Brian Carrier

Twitter: @carrier4n6

Brian Moran

Twitter: @brianjmoran

CYBER TRIAGE