

# The De-RaaS'ing of Ransomware

**Allan Liska**

*Ransomware Sommelier / Recorded Future*

# Who Am I?

- Ransomware researcher at Recorded Future
- Co-Author/Author of two books about ransomware



# The World's Largest Intelligence Company



**Mission** Securing our world with Intelligence



**1,500+** Clients



**\$200M+** ARR



**850+** Employees



**Offices** in Boston, Washington, Göteborg, London, Tokyo, Dubai, Singapore



**Industry Leader #1**  
Frost+Sullivan Leader, Fast Company World's Most Innovative Companies

## Recorded Future Intelligence Cloud



**9 modules** deliver Intelligence across the Enterprise



**Intelligence Graph** largest Intelligence repository



**Integrations** 100+ integrations with leading security applications



**Insikt Group** 200+ threat research analysts



**Trusted by 30+** national governments



**#1** cybersecurity news site, podcast



**8 of 10** largest companies in the world



**42** of Forbes Global 100



**Are the number of ransomware attacks up  
or down in 2022?**

# Ransomware Extortion Sites

**2021**

**2022**

**1706**

**1757**

Through September 9th

# Ransomware Extortion Sites

**2021**

**2022**

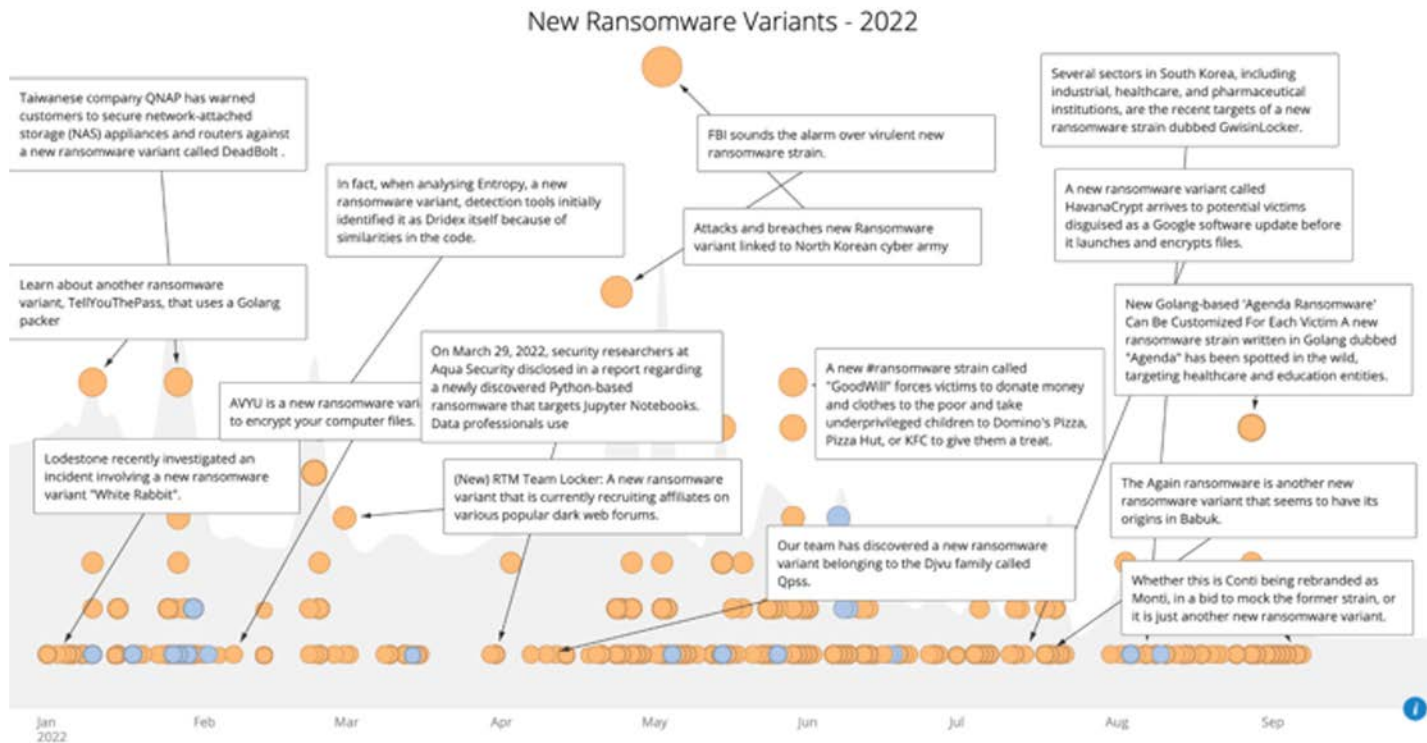
**44**

**98**

Collection from different Data Leak Sites (DLS)

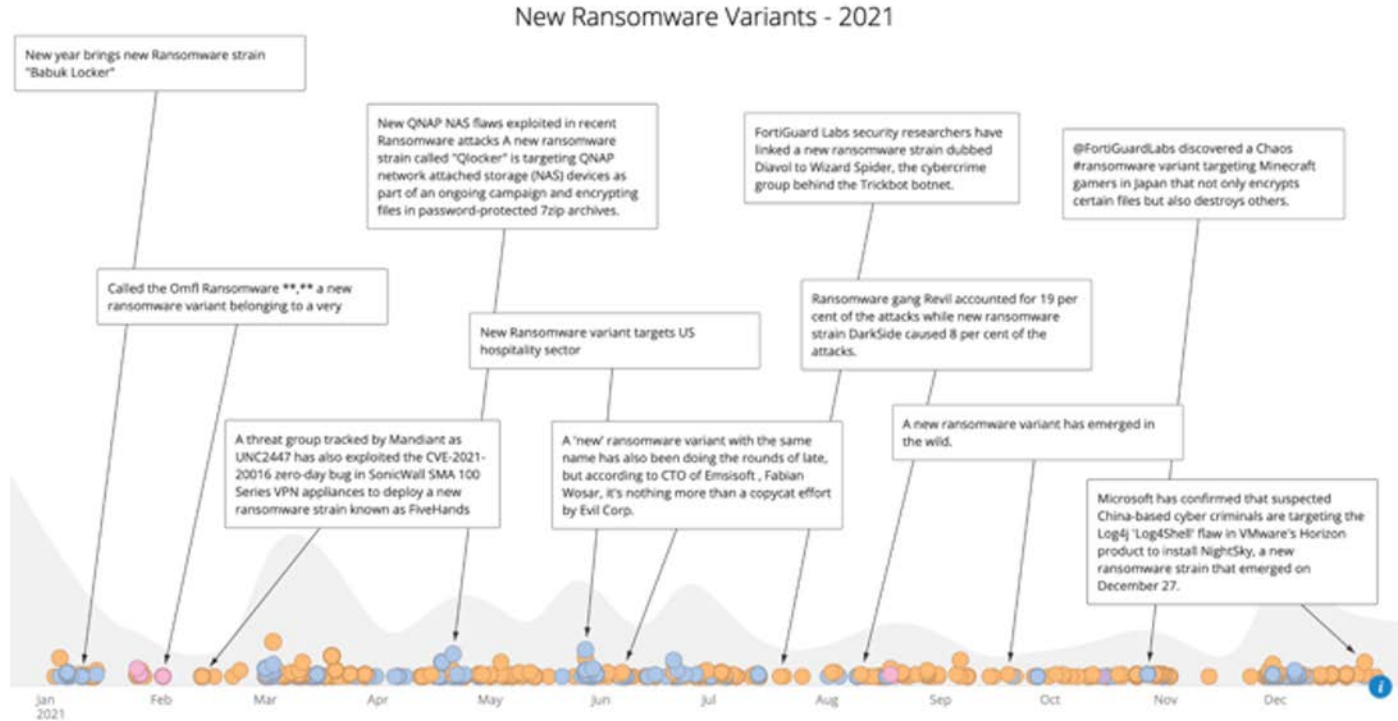
# Explosion in Ransomware Groups

**170 new ransomware variants reported in 2022**



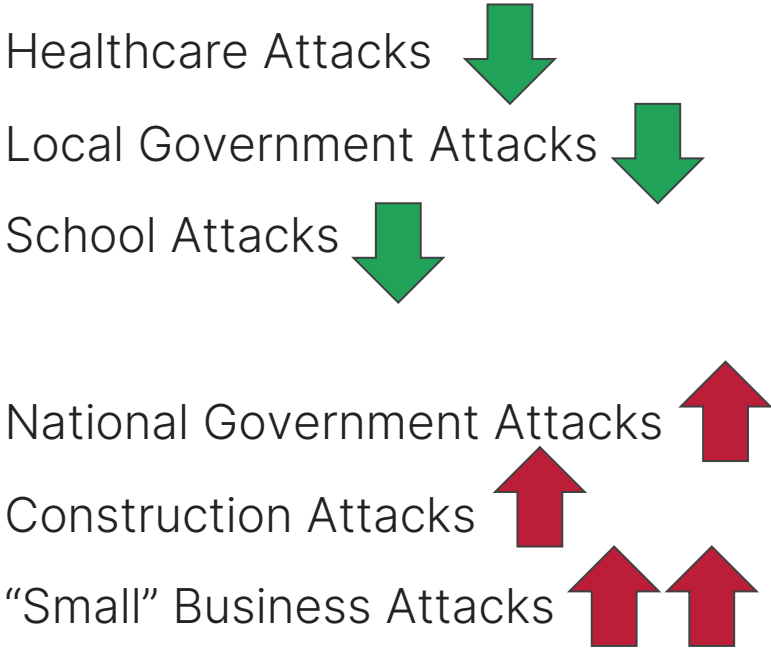
# Explosion in Ransomware Groups

**183 new ransomware variants reported in all of 2021**





# We Need to Think Beyond DLS



# Ransomware is Global



## Iran

Moses Staff  
Pay2Key  
Project Signal



## UK/Brazil

Lapsus\$

## China

ColdLock  
DearCry  
Rook



## DPRK

VHD  
Maui  
H0lyGh0st

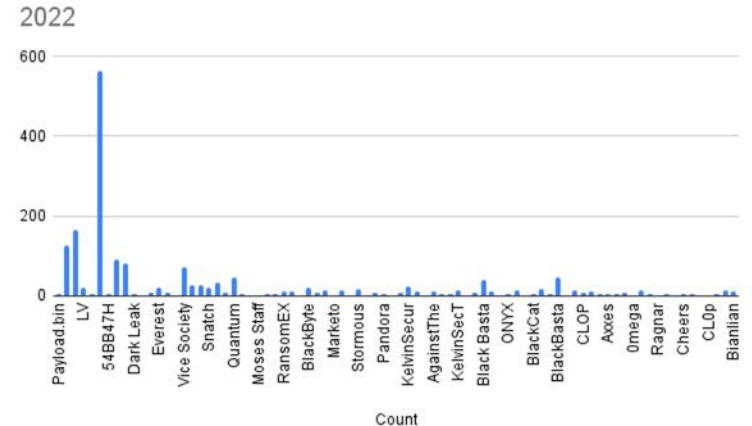
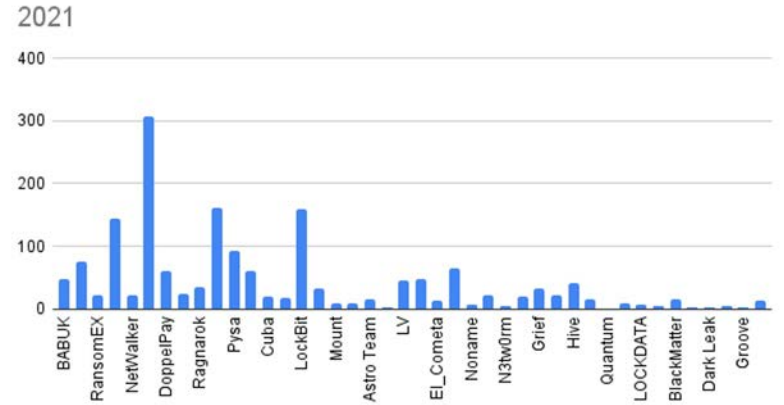




**You know you are like 20 minutes into this presentation and you still haven't gotten to the point, right?**

# The Problem

- Increasingly ransomware groups are rejecting the RaaS model and opting to “go it alone”
- In 2021, while Conti was the clear leader in RaaS groups, there were many others to choose from.
- In 2022, there is LockBit and then...everyone else.



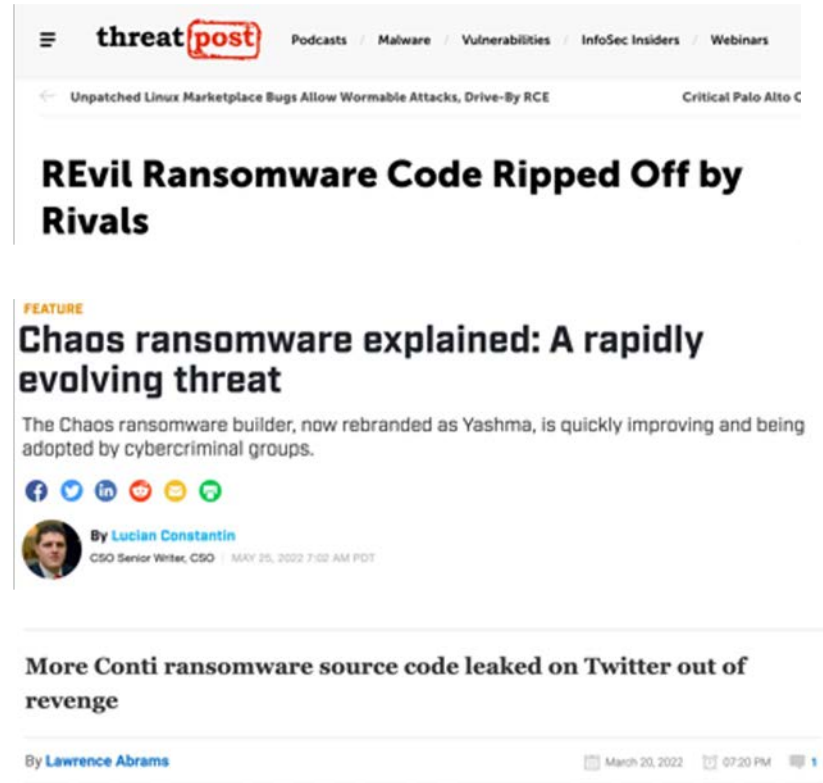
# The Problem

- But, a lot of affiliates are skittish about joining big RaaS operations because big now means targeted by EVERY intelligence agency.
- Which means many of these new ransomware groups are smaller 4-5 person groups.
- These may be harder for security companies and national governments to infiltrate and track down.



# The Good News

- Outside of some of the nation state groups, most of the new ransomware groups are not using new code.
- Instead, we are seeing a lot of code re-use
  - Conti
  - REvil
  - Chaos



The screenshot shows the threatpost website interface. At the top, there is a navigation bar with the threatpost logo and links for Podcasts, Malware, Vulnerabilities, InfoSec Insiders, and Webinars. Below the navigation bar, there is a breadcrumb trail: Unpatched Linux Marketplace Bugs Allow Wormable Attacks, Drive-By RCE > Critical Palo Alto C. The main article headline is "REvil Ransomware Code Ripped Off by Rivals". Below this, there is a "FEATURE" section with the headline "Chaos ransomware explained: A rapidly evolving threat". The sub-headline reads: "The Chaos ransomware builder, now rebranded as Yashma, is quickly improving and being adopted by cybercriminal groups." Below the sub-headline are social media sharing icons for Facebook, Twitter, LinkedIn, Reddit, Email, and Print. The author information is "By Lucian Constantin, CSO Senior Writer, CSO" with a date of "MAY 25, 2022 7:52 AM PDT". Below this, there is another article headline: "More Conti ransomware source code leaked on Twitter out of revenge". At the bottom of the screenshot, there is a byline "By Lawrence Abrams" and a date "March 20, 2022 07:20 PM".

# The Good News

- We are also not seeing a lot of new techniques when moving around the network, from these groups.
- Still a lot of:
  - CobaltStrike
  - AdFind
  - Mimikatz
  - Bloodhound
  - PowerShell
- The same detection techniques still work.
- But, it can be a lot more difficult to identify these new variants, especially...



*This image has nothing to do with the material, but I like it and I think we need a palate cleanser*

# Sanctions!

- With all the new variants, it is hard to track who is behind which variant.
- Unfortunately, this means it is very possible to pay a ransom to a sanctioned entity and can get your organization into trouble.





# Law Enforcement

- I know a lot of incident responders don't like to hear this, but If you are dealing with a new ransomware variant, you should contact law enforcement.
- **ESPECIALLY IF YOUR CLIENT/ORGANIZATION IS LEANING TOWARD PAYING THE RANSOM**
- It appears we are entering the next phase of ransomware which will be dominated by smaller groups, often more difficult to track down.
- The era of RaaS domination is probably coming to end (especially when someone gets around to taking out LockBit).
- But, good fundamental security practices can still stop ransomware.

# Thank You!

