Ransomware as a Service (RaaS)

The Black Hat Industry is More Professional Than You Think

NT230 - Malware's Modus Operandi

Information Security Lab (InSecLab), University of Information Technology
Vietnam National University Ho Chi Minh City

June 17, 2024

Overview

1. The overview of Ransomware

2. Ransomware as a Service

3. Methods of RaaS Protection and Detection

The overview of Ransomware

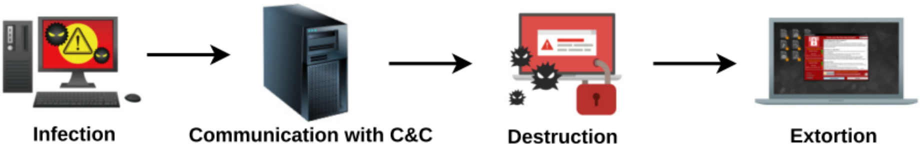
Ransomware

Figure: Ransomware, named ”Mã độc tống tiền” in Vietnamese

Ransomware: Definition

- Ransomware (ransom software) is a subset of malware designed to restrict access to a system or data until a requested ransom amount from the attacker is satisfied.
- Based on the employed methodology, ransomware is generally classified into two types:
  - Cryptographic ransomware: encrypts the victim's files
  - Locker ransomware: prevents victims from accessing their systems.

Ransomware: Generalized overview of attack phases of ransomware



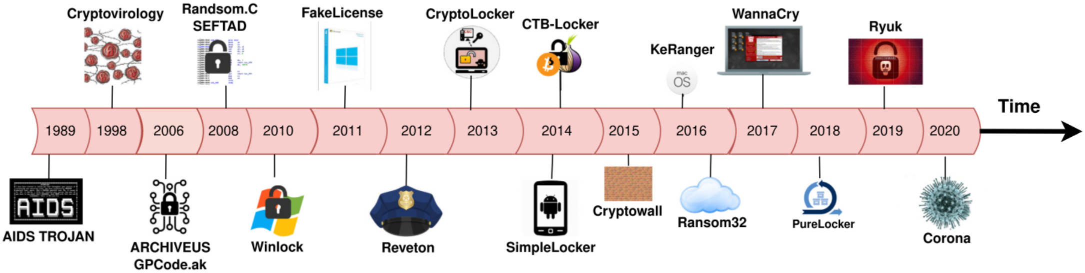
Infection

Communication with C&C

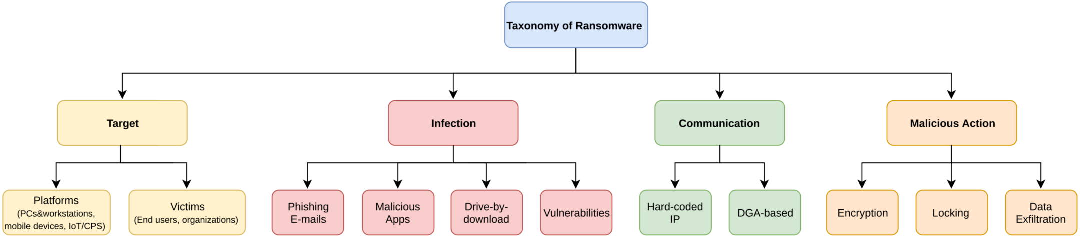
Destruction

Extortion

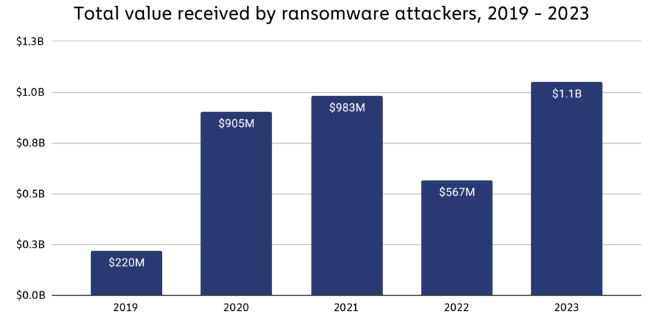
Ransomware: Evolution of major ransomware families from 1989 to 2020



Taxonomy of ransomware

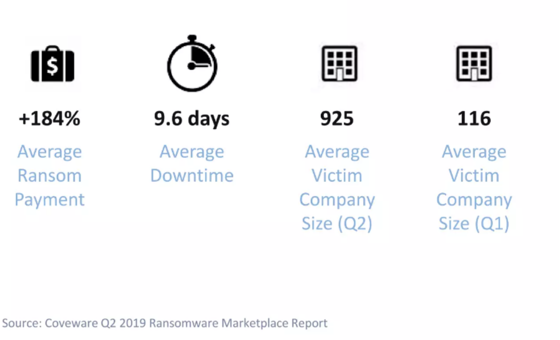


Ransomware Payments Exceed $1 Billion in 2023



© Chainalysis

The State of Ransomware (1)



+184%
Average Ransom Payment

9.6 days
Average Downtime

925
Average Victim Company Size (Q2)

116
Average Victim Company Size (Q1)

Source: Coveware Q2 2019 Ransomware Marketplace Report

Figure: Ransomware Marketplace Report by Coveware (2019)

The State of Ransomware (2)

Ransomware payments drop to record low as victims refuse to pay.

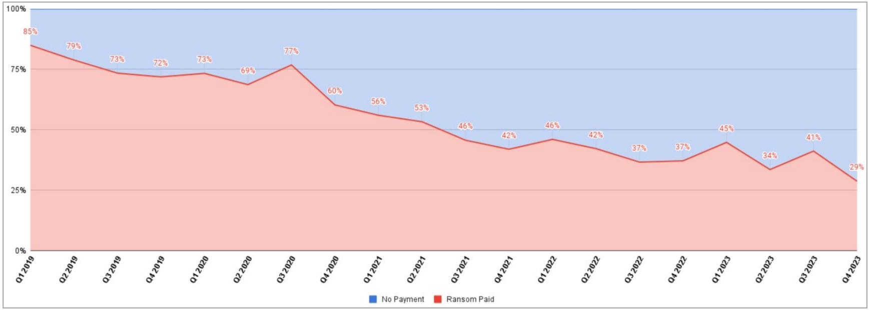


Figure: Ransomware Payment rates - Source: Coveware 2024

The State of Ransomware (3)

Coveware says that ransom payments in Q4 2023 had an average amount of $568,705, a 33% drop from the previous quarter, while the median ransom payment was $200,000.

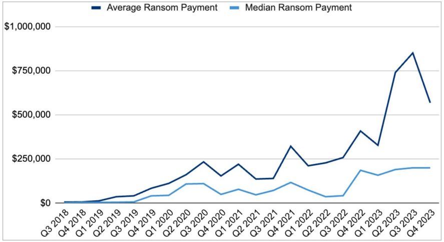


Figure: Ransomware Payment Size - Source: Coveware 2024

The State of Ransomware (4)

In Q1 - 2024, anti-forensic tactics led to a rise in attacks where the original attack vector remained unknown.

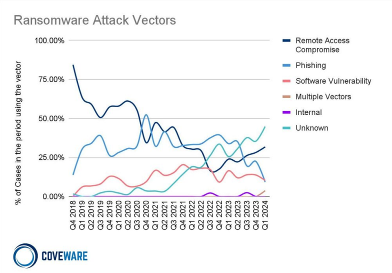


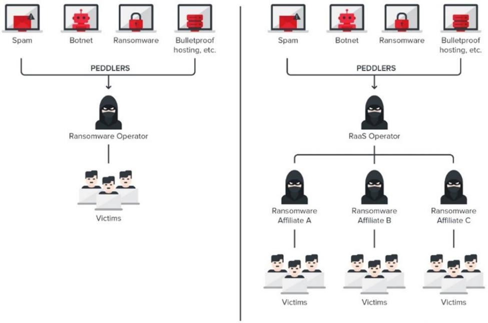
Figure: Attack Vectors in Q1 2024 - Source: Coveware 2024

Ransomware as a Service

What is Ransomware as a Service (RaaS)?

- Ransomware as a service (RaaS) is a business model that involves selling or renting ransomware to buyers, called affiliates.
- RaaS can be credited as one of the primary reasons for the rapid proliferation of ransomware attacks, as it has made it easier for a variety of threat actors – even those who have little technical knowledge – to deploy ransomware against targets.
- *RaaS is based on the* ***software-as-a-service (SaaS)*** *model, in which software can be accessed online on a subscription basis.*

Ransomware vs. RaaS



©2021 TREND MICRO

Figure: Comparison of direct ransomware operations (left) and RaaS operators (right)

Ransomware as a Service (RaaS)

- Ransomware-as-a-Service (RaaS) emerged in 2015.
- RaaS aimed to provide user-friendly, and easy-to-modify ransomware kits that could be purchased by anyone in underground markets.
- That was a momentous step for the evolution of ransomware, as it could be easily repackaged to infect any platform, which made it platform-agnostic.
- RaaS escalated the number of ransomware attacks around the world

RaaS: BlackCat

- Active Since: 2021
- Number of victims (2023): 170

RaaS: LockBit 3.0

- Active Since: 2020
- Number of victims (2023): 474

RaaS: CLoP

- Active Since: 2020
- Number of victims (2023): 106

RaaS: Black Basta

- Active Since: 2022
- Number of victims (2023): 101

RaaS: Royal

- Active Since: 2022
- Number of victims (2023): 110

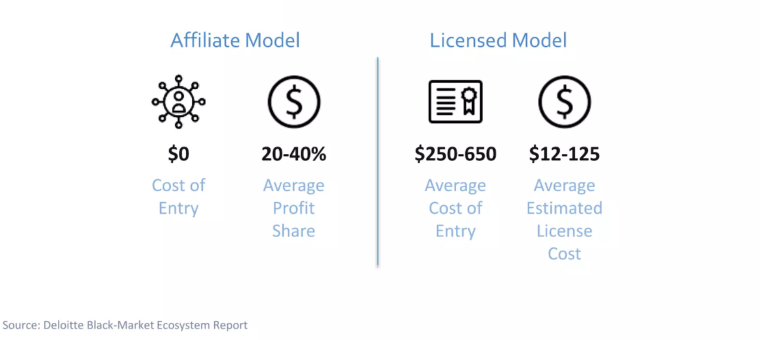
RaaS: Akira

- Active Since: 2023
- Number of victims (2023): 37

RaaS: BianLian

- Active Since: 2022
- Number of victims (2023): 46

The State of RaaS: Marketplace



Affiliate Model

$0
Cost of Entry

20-40%
Average Profit Share

Licensed Model

$250-650
Average Cost of Entry

$12-125
Average Estimated License Cost

Source: Deloitte Black-Market Ecosystem Report

Figure: Ransomware as a Service Marketplace Report by Deloitte

RaaS: How is a Service provided?

Services are offered in a variety of forms such as:

- Unlimited access by paying a one-time fee
- Monthly subscriptions
- Profit sharing wherein the developer gets a share of every successful attack and ransom earned

RaaS: Value Chain for the RaaS economy

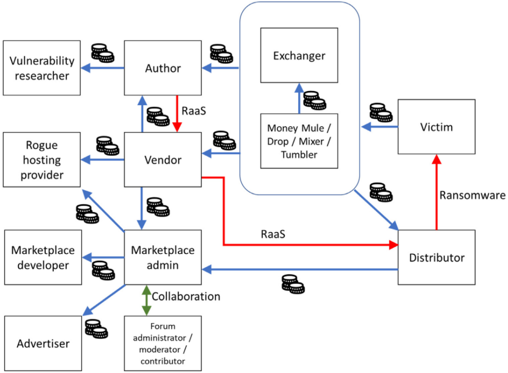


Figure: Value chain for the RaaS economy

RaaS Value Chain: Actor Descriptions (1)

1. Vulnerability researcher (VR): discover and sell information about zero-day vulnerabilities to others who can write the exploit code.
2. Authors: are professional developers who create the malware that takes advantages of vulnerabilities, some of which are purchased from VR
3. Vendor: do marketing and sale on marketplaces or on their private website. Vendors can be authors, or sellers of any other goods.
4. Victim: suffers from ransomware infections and may lose their data or pay the ransom. They may need the help of an exchanger to obtain the ransom amount in cryptocurrency.
5. Marketplace admin: provides a market platform that vendors and distributors can use for trade.

RaaS Value Chain: Actor Descriptions (2)

1. Marketplace developer advertiser: person with technical expertise that develops the marketplace platforms for the administrators.
2. Forum admin/moderator/contributor: People responsible for managing the forum contents and membership access. Usually have a close relationship with the admin of one or more marketplaces.
3. Rogue hosting provider/ Money Mule/ Drop/Mixer/Tumbler: Provide website hosting services on the darknet that reduces the risk of getting caught. Transaction received from victims are transferred through an intermediary, either a professional money launderer or someone who unknowingly forwards the money.
4. Exchanger: Exchangers own verified accounts and use their immunity to offer currency exchange services to cybercriminals.

Ransomware as a Service (RaaS): Starting for Sales

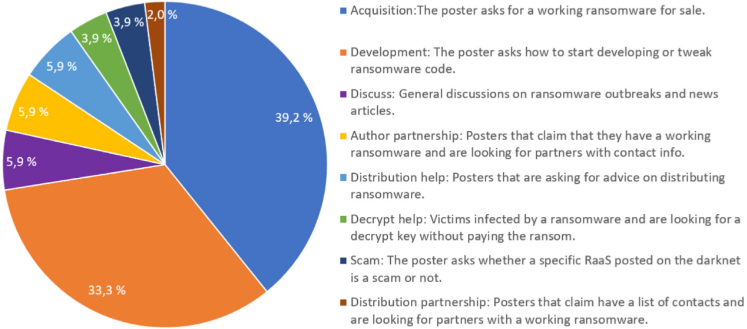
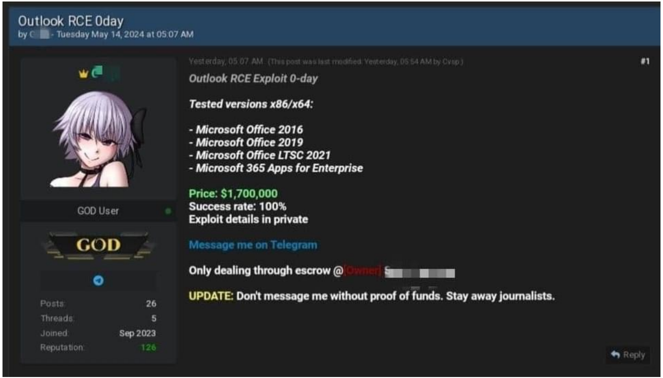


Figure: Question categories related to ransomware in the Hidden Answers forum

RaaS: Selling 0-day vulnerabilities for Malware Authors



Outlook RCE 0day
by [redacted] - Tuesday May 14, 2024 at 05:07 AM

Yesterday, 05:07 AM (This post was last modified: Yesterday, 05:54 AM by Cvsp.) #1

Outlook RCE Exploit 0-day

Tested versions x86/x64:

- Microsoft Office 2016
- Microsoft Office 2019
- Microsoft Office LTSC 2021
- Microsoft 365 Apps for Enterprise

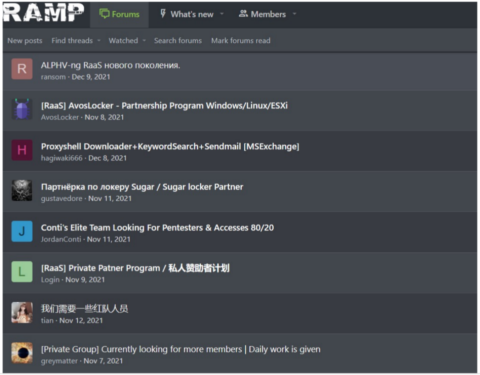
Price: $1,700,000
Success rate: 100%
Exploit details in private

Message me on Telegram

Only dealing through escrow @[Owner] [redacted]

UPDATE: Don't message me without proof of funds. Stay away journalists.

RaaS: Affiliate recruitment adverts



ALPHV-ng RaaS нового поколения.
ransom · Dec 9, 2021

[RaaS] AvosLocker - Partnership Program Windows/Linux/ESXi
AvosLocker · Nov 8, 2021

Proxyshell Downloader+KeywordSearch+Sendmail [MSExchange]
hagiwaki666 · Dec 8, 2021

Партнёрка по локеру Sugar / Sugar locker Partner
gustavedore · Nov 11, 2021

Conti's Elite Team Looking For Pentesters & Accesses 80/20
JordanConti · Nov 11, 2021

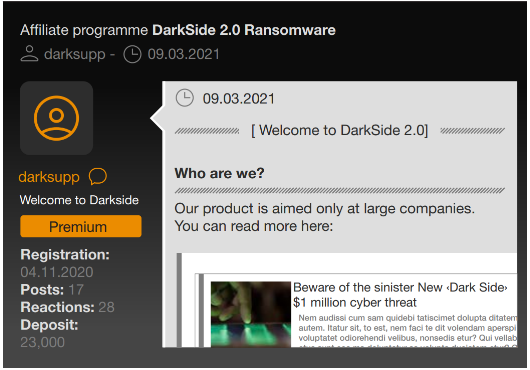
[RaaS] Private Patner Program / 私人赞助者计划
Login · Nov 9, 2021

我们需要一些红队人员
tian · Nov 12, 2021

[Private Group] Currently looking for more members | Daily work is given
greymatter · Nov 7, 2021

Figure: Conti, AvosLocker, BlackCat are currently active ransomwares by RAMP forum (Source: PwC)

RaaS: Affiliate recruitment adverts



Affiliate programme **DarkSide 2.0 Ransomware**

darksupp - 09.03.2021

darksupp

Welcome to Darkside

Premium

Registration: 04.11.2020
Posts: 17
Reactions: 28
Deposit: 23,000

09.03.2021

[Welcome to DarkSide 2.0]

Who are we?

Our product is aimed only at large companies.
You can read more here:

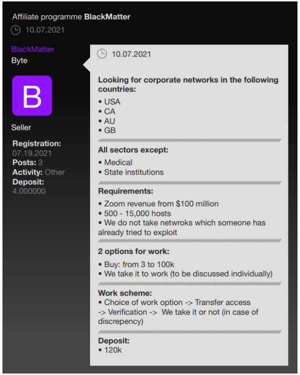
Beware of the sinister New ‹Dark Side› $1 million cyber threat

Nem audissi cum sam quidebi tatiscimet dolupta ditatem
autem. Itatur sit, to est, nem faci te dit volendam aperspi
voluptatet odiorehendi velibus, nonsedis etur? Qui vellab

Figure: ”Welcome to Darkside 2.0” announcement post (Source: PwC)

RaaS: Access as a Services (AaaS)

White Apep (aka BlackMatter, DarkSide) seeking access to corporate networks on the forum Exploit



Affiliate programme **BlackMatter**
10.07.2021

BlackMatter
Byte

Seller

Registration: 07.19.2021
Posts: 3
Activity: Other
Deposit: 4.000000

10.07.2021

Looking for corporate networks in the following countries:

- USA
- CA
- AU
- GB

All sectors except:

- Medical
- State institutions

Requirements:

- Zoom revenue from $100 million
- 500 - 15,000 hosts
- We do not take netwroks which someone has already tried to exploit

2 options for work:

- Buy: from 3 to 100k
- We take it to work (to be discussed individually)

Work scheme:

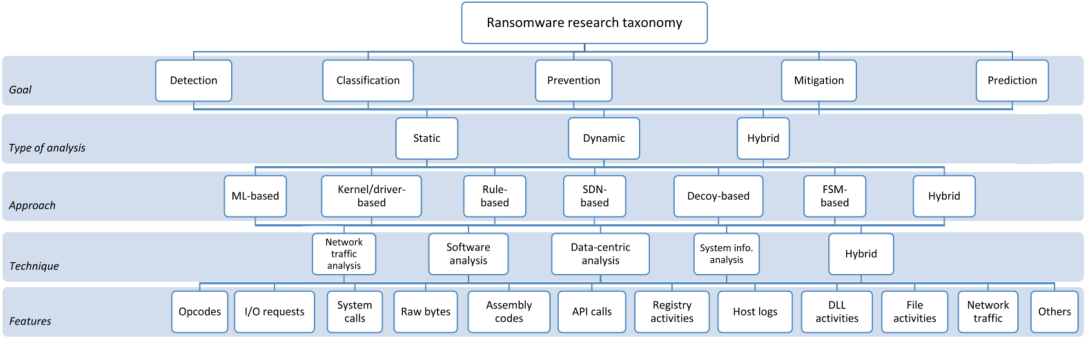
- Choice of work option -> Transfer access -> Verification -> We take it or not (in case of discrepency)

Deposit:

- 120k

Methods of RaaS Protection and Detection

Ransomware Research Taxonomy



Ransomware research taxonomy

Goal: Detection, Classification, Prevention, Mitigation, Prediction

Type of analysis: Static, Dynamic, Hybrid

Approach: ML-based, Kernel/driver-based, Rule-based, SDN-based, Decoy-based, FSM-based, Hybrid

Technique: Network traffic analysis, Software analysis, Data-centric analysis, System info. analysis, Hybrid

Features: Opcodes, I/O requests, System calls, Raw bytes, Assembly codes, API calls, Registry activities, Host logs, DLL activities, File activities, Network traffic, Others

Figure: Research Taxonomy of Ransomware

Methods of RaaS Protection and Detection

1. Preparation comes from a few angles
   - Environment: Layered Security
   - Systems/Data: Backups
   - Users: Security Awareness Training
2. Detection can be accomplished in a number of ways:
   - Endpoint: Abnormal processes, application behavior
   - Backups: Excessive changes to backup sets
   - Systems: Honeypots

Anti-Malware Alone is Not Enough – You Need a Multi-Layered Approach

Thwarting Encryption and Prepare Backups:

- Intercepts all encrypt commands
- Makes a secure local copy
- Restore your files in minutes

Honeypots for Deceiving Ransomware & Incident Response

- Honeypots added to catch zero-day malware
- Alerts when attacked
- Catches variants to the new ransomware
- Immediately blocks the user account, minimizes restoration effort

Thank you for your attention

NT230 – Malware's Modus Operandi

Information Security Lab (InSecLab), University of Information Technology
Vietnam National University Ho Chi Minh City

June 17, 2024