Encrypt, Extort, Evolve

The Changing Face of Ransomware

ACUMENCYBER

Introduction – Who am I

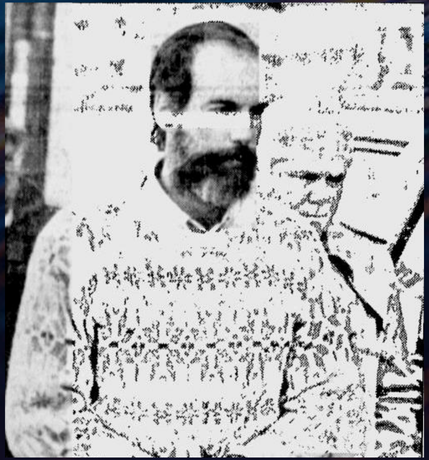
Cian Heasley

Principal Consultant @ Acumen Cyber

Cyber Threat Intelligence & Threat Hunting

ATT&CK, Sigma Contributor

What is Ransomware?

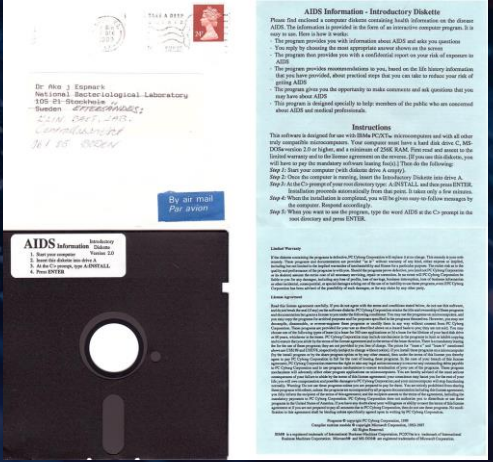


Dr Joseph Popp

Godfather of Ransomware

The Origin of Ransomware

- In 1989 26,000 AIDS researchers worldwide received a floppy disk in the mail, disks were mailed from the U.K.
- The disks contained a virus that activated after 90 reboots of the infected PC
- The virus caused files and directories to be inaccessible and displayed a “license” fee demand of $189 payable to a P.O. Box in Panama
- American Harvard educated evolutionary biologist **Dr. Joseph Louis Popp** was arrested
- Popp was later freed as he was considered psychologically unfit to stand trial, he died in 2006
- The virus Popp created and mailed from the U.K. is credited with expediting the passage of the U.K. Computer Misuse Act of 1990 in to law



TAKE A DEEP

Dr Ake j Espmark
National Bacteriological Laboratory
~~105 21 Stockholm~~
~~Sweden~~ EFTERSÄNDES:
KLIN. BAKT. LAB.
Centrallasarettet
[illegible]

By air mail
Par avion

AIDS Information Introductory Diskette Version 2.0

1. Start your computer
2. Insert this diskette into drive A
3. At the C> prompt, type A:INSTALL
4. Press ENTER

AIDS Information - Introductory Diskette

Please find enclosed a computer diskette containing health information on the disease AIDS. The information is provided in the form of an interactive computer program. It is easy to use. Here is how it works:

- The program provides you with information about AIDS and asks you questions
- You reply by choosing the most appropriate answer shown on the screen
- The program then provides you with a confidential report on your risk of exposure to AIDS
- The program provides recommendations to you, based on the life history information that you have provided, about practical steps that you can take to reduce your risk of getting AIDS
- The program gives you the opportunity to make comments and ask questions that you may have about AIDS
- This program is designed specially to help: members of the public who are concerned about AIDS and medical professionals.

Instructions

This software is designed for use with IBM® PC/XT™ microcomputers and with all other truly compatible microcomputers. Your computer must have a hard disk drive C, MS-DOS® version 2.0 or higher, and a minimum of 256K RAM. First read and assent to the limited warranty and to the license agreement on the reverse. [If you use this diskette, you will have to pay the mandatory software leasing fee(s).] Then do the following:

Step 1: Start your computer (with diskette drive A empty).
Step 2: Once the computer is running, insert the Introductory Diskette into drive A.
Step 3: At the C> prompt of your root directory type: A:INSTALL and then press ENTER. Installation proceeds automatically from that point. It takes only a few minutes.
Step 4: When the installation is completed, you will be given easy-to-follow messages by the computer. Respond accordingly.
Step 5: When you want to use the program, type the word AIDS at the C> prompt in the root directory and press ENTER.

Limited Warranty

[illegible]

License Agreement

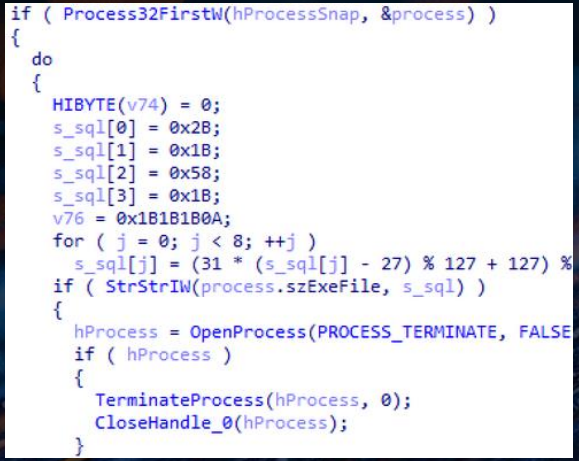
[illegible]

[illegible]

AIDS Diskette

Envelope & Instructions

What is Ransomware?



```
if ( Process32FirstW(hProcessSnap, &process) )
{
  do
  {
    HIBYTE(v74) = 0;
    s_sql[0] = 0x2B;
    s_sql[1] = 0x1B;
    s_sql[2] = 0x58;
    s_sql[3] = 0x1B;
    v76 = 0x1B1B1B0A;
    for ( j = 0; j < 8; ++j )
      s_sql[j] = (31 * (s_sql[j] - 27) % 127 + 127) %
    if ( StrStrIW(process.szExeFile, s_sql) )
    {
      hProcess = OpenProcess(PROCESS_TERMINATE, FALSE
      if ( hProcess )
      {
        TerminateProcess(hProcess, 0);
        CloseHandle_0(hProcess);
      }
```

Conti Ransomware

Source Code

Ransomware – Software

“Software introduced on to systems through criminal methods and used to extort money from an individual or organization by encrypting or otherwise blocking access to applications or files on an infected computer system until a sum of money is paid.”

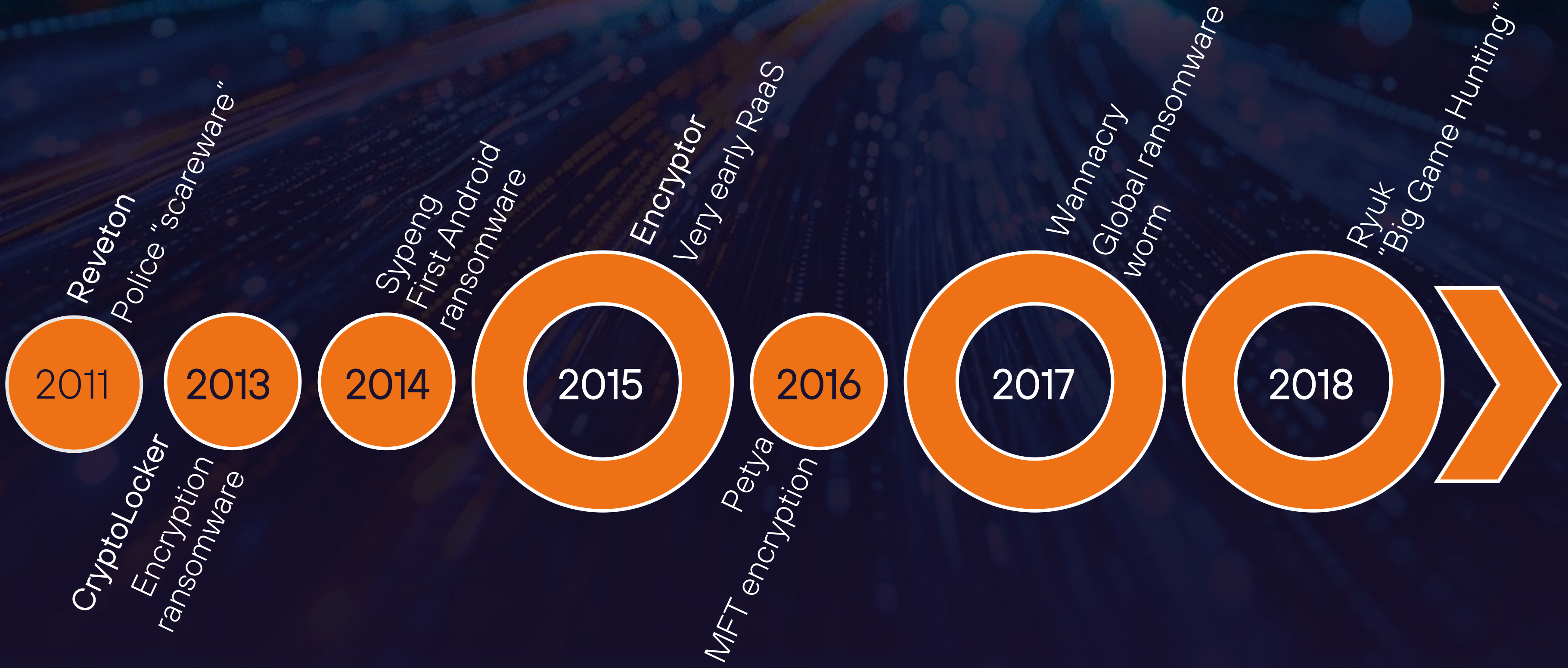
Vitaly Kovalev

Alleged Conti Leader

Ransomware – Criminal Tactic

Ransomware is a criminal tactic that involves holding data to ransom, with financial demands up backed by extortion threats that may involve permanent encryption of data, the leaking or sale of stolen data, DDoS attacks, further damage to compromised systems, ransom demands from affected third parties or harassment of employees or clients.

Ransomware – Early Years



2011

Reveton

Police "scareware"

2013

CryptoLocker

Encryption ransomware

2014

Sypeng

First Android ransomware

2015

Encryptor

Very early RaaS

2016

Petya

MFT encryption

2017

Wannacry

Global ransomware worm

2018

Ryuk

"Big Game Hunting"

ACUMENCYBER

Ransomware – Business Model Matures

2018

- Ransomware competing with “crypto-jacking” malware in the market
- “Big Game Hunting” era begins, entire organisations are targeted
- Average ransomware payments estimated at $10,000
- RDP brute forcing to deliver ransomware onto corporate networks
- Mass phishing and banking trojans (Trickbot, Emotet) also used

2019

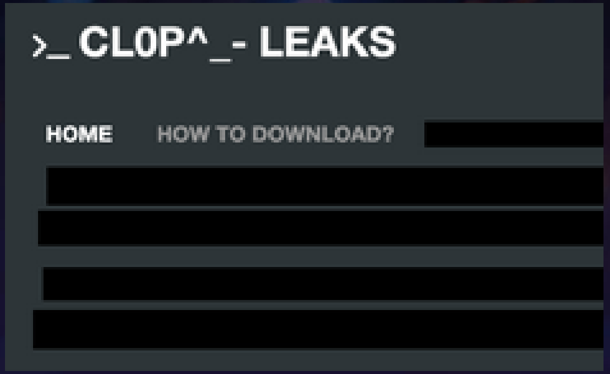
- Average ransomware payment estimated at $25,000
- Maze ransomware gang pioneers “double extortion”
- Maze demanded $3.2 mil from Allied Universal

Ransomware – Current State

Decentralised "Traditional" RaaS

- ❑ "Brand" built in e-crime markets
- ❑ Extortion site maintained
- ❑ Assistance with negotiations
- ❑ Ransomware executables maintained (maybe)

Centralised Groups



>_ CL0P^_- LEAKS

HOME HOW TO DOWNLOAD? [redacted]

[redacted]

- ❑ Favours campaigns over ad hoc attacks
- ❑ Core team with technical responsibilities
- ❑ May work with RaaS style operators

Ransomware – Current State

Shinyhunters are an organized group, targeting engineering & devops platforms via phishing or social engineering to steal data

Scattered Spider act as a loose knit group of ransomware operators, data thieves, social engineering & phishing specialists

- ❑ Have partnered with ALPHV, DragonForce & Qilin

If "scattered lapsus$ hunters" make their own RaaS gang we could see:

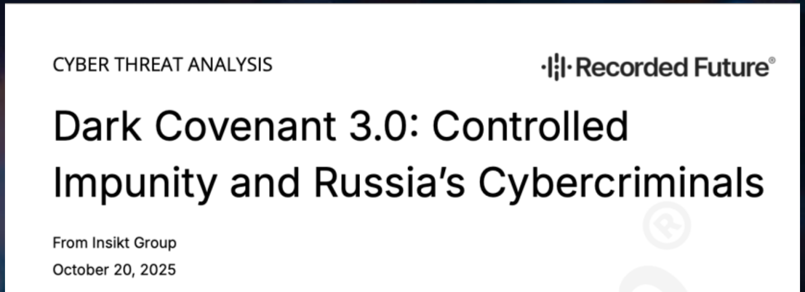
- ❑ Realignment in ransomware ecosystem
- ❑ Western operators and affiliates abandon Russian gangs
- ❑ Russian dominance in the ransomware scene lessens

Ransomware – Current State

"Controlled Impunity"

- ❑ Examples must be made
- ❑ "In group" & "out group"
- ❑ High profile arrests & trials:
  - ❑ September 2024 – "Bio" (Conti)
  - ❑ Nov 2024 – wazawaka
  - ❑ Jun 2025 – REvil sentenced
  - ❑ October 2025 – Meduza devs

- ❑ Increased paranoia in Russian e-crime ecosystem
- ❑ Group rivalry – DragonForce attacks other groups
- ❑ Fractured scene, more variants, quicker turnover



CYBER THREAT ANALYSIS

Recorded Future®

Dark Covenant 3.0: Controlled Impunity and Russia's Cybercriminals

From Insikt Group
October 20, 2025

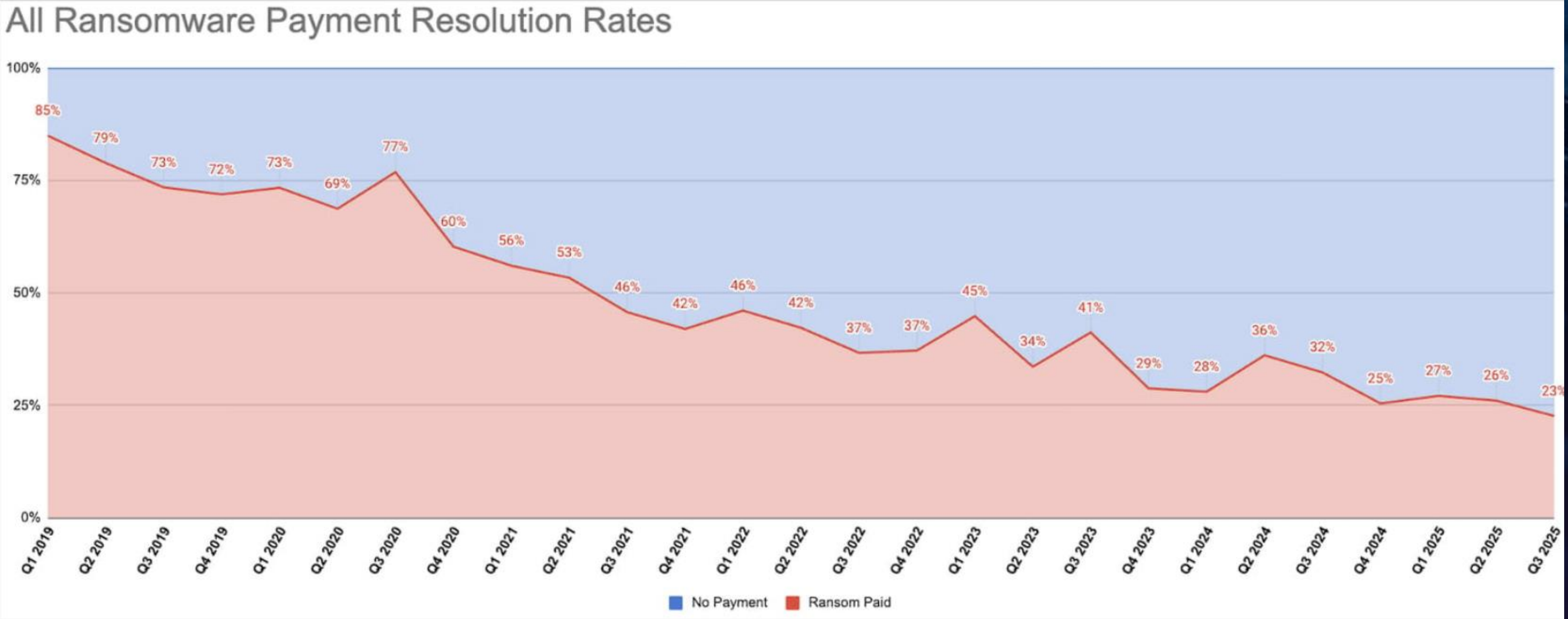
Revil arrests, Russia, January 2022

Mamont Android trojan arrests, Russia, March 2025

Ransomware – Current State

- Coveware researchers released a report earlier this year:

  - □ In Q3 of 2025, 23% of victims paid - ransomware payments are at an all time low
  - □ Data theft only is more popular with gangs but only 19% of victims paid in Q3 2025



Source: Coveware

Ransomware – The Future

- □ New methods to force negotiation or payment
- □ Triple, quadruple, etc extortion - spaghetti at the wall
- □ “Quantity” versus “Quality” of targets for payouts
- □ Phishing will become a background hum
- □ Mass exploitation campaigns will become more popular
- □ Social engineering specialization will fill phishing gaps

Ransomware – The Future

Western ransomware gang

- ❑ Able to do "close operations", similar to APTs
- ❑ Alignment of fluent social engineers & operators
- ❑ Change of calculus around Russia, China, etc
- ❑ Absorbs existing Western computer crime

Hacktivists become proficient with ransomware

- ❑ Multiple hacktivist groups already pitching RaaS
- ❑ New political & ideological motives enter ecosystem
- ❑ Move away from DDoS, OT and SCADA vandalism
- ❑ Greater focus on fund raising & monetization
- ❑ Professionalization & organization

Q&A

ACUMENCYBER

Get In touch

☎ 0330 236 8388

✉ securityoperations@acumencyber.com

📍 7 Gateway Court,
Eastworks
Glasgow
G40 4DS

acumencyber.com