

Where is my Ransom?

Hunting for Ransomware Gangs using radare2 and YARA

Kevin Gomez — 5th September 2020

EKANS



By Dra

Ransomware warning: Now attacks are stealing

Cyber criminals are going to get v



>_ CLOP^_ - LEAKS

HOME IHI-C
PLANATOL.DE

UPDATES

Ransomware-as-a-Service: Ransomware Operators Find Ways to Bring in Business

02 de septiembre de 2016

Successful **ransomware** attacks continue to headline as profits gained by cybercriminals. In 2015, a ransomware family called Clop^_ leaked an alarming US\$325 million for its operators for a single family.

Ransomware works quite effectively on computers through spam email or infected files. Once installed, ransomware encrypts the system and then asks victims for a ransom to the files. If the ransom is paid, the key—though there is no guarantee.

The increasing cases of ransomware-as-a-service (RaaS) **business model**. This model allows for cybercriminals, allowing malware to be spread by multiple distributors, with distributors don't even need much coding experience can launch a ransomware attack.



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



October 02, 2019

Alert Number
I-100219-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

HIGH-IMPACT RANSOMWARE ATTACKS THREATEN U.S. BUSINESSES AND ORGANIZATIONS

This Public Service Announcement (PSA) is an update and companion to [Ransomware PSA I-091516-PSA](#) posted on www.ic3.gov. This PSA contains updated information about the ransomware threat.

WHAT IS RANSOMWARE?

Ransomware is a form of malware that encrypts files on a victim's computer or server, making them unusable. Cyber criminals demand a ransom in exchange for providing a key to decrypt the victim's files.

Ransomware attacks are becoming more targeted, sophisticated, and costly, even as the overall frequency of attacks remains consistent. Since early 2018, the incidence of broad, indiscriminant ransomware campaigns has sharply declined, but the losses from ransomware attacks have increased significantly, according to complaints received by IC3 and FBI case information.

Although state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector.

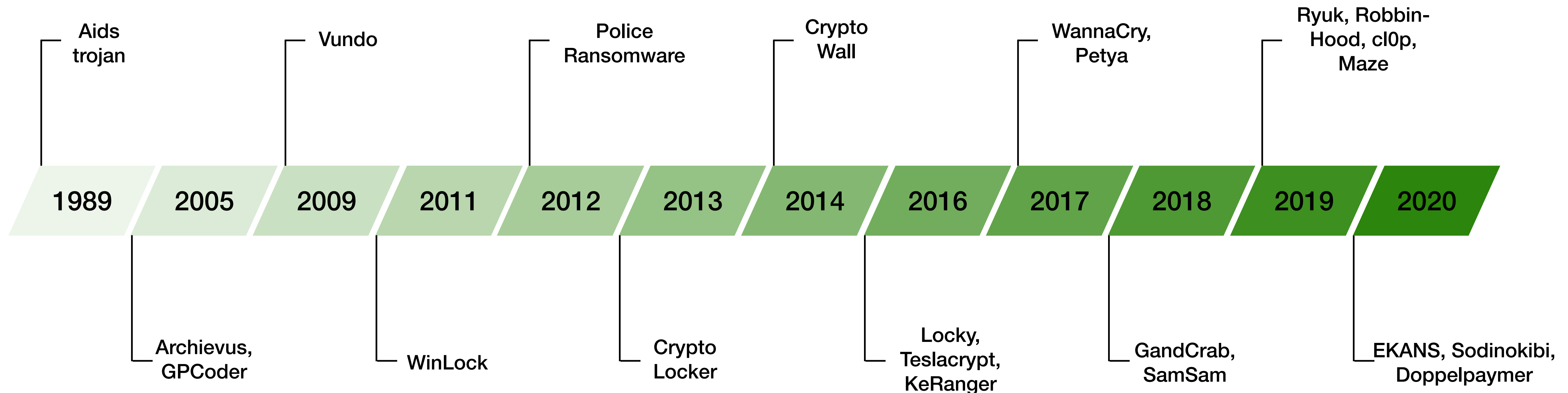


Why ransomware attacks are bad to your business

WATCH NOW



What changed?



What do I want to achieve?

- Learn about ransomware and evolvments within families
- Find newest samples of different families
- Detect code sharing between families
- And maybe, see potential incidents based on VirusTotal uploads

How to achieve those?

- Utilise Yara as a classification and identification tool
- VirusTotal and Hybrid Analysis for hunting
- Radare2 and Cutter for malware analysis

YARA

Name of the rule and optional tags

Add context to the rule

Define what to look for

Trigger condition of the rule

```
1  rule r2con2020
2  {
3      meta:
4          description = "Determine if r2con 2020 is awesome"
5          author = "@kgbuquerin"
6          date = "2020-09-05"
7          reference = "https://www.radare.org/con/2020/"
8
9      strings:
10         $s0 = "r2con" fullword
11         $s1 = "is" wide ascii
12         $s2 = "pretty"
13
14         $b1 = { 61 77 65 73 6f 6d 65 }
15
16         $x0 = "boring" xor
17
18     condition:
19         all of ($s*) and $b1 and not $x0
20 }
```

What did I do?

1. Collect initial samples
2. Create first rule
3. Test rule against different test-sets
4. Hunt for more samples
5. Create better rules
6. Goto 3

Maze

Ransomware

cl0p

Ransomware

To summarise



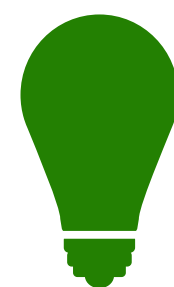
- Learn about ransomware families
- Find newest versions



- Detect code sharing across them



- See incidents by VirusTotal uploads



- Test your rules properly
- Use unique strings
- Think about opcodes

Thank you for your attention!

Have fun at  R2EON



@kgbuquerin



<https://github.com/kgbuquerin>