



SNIA[®] STORAGE
SECURITY SUMMIT
Wednesday, May 11, 2022 • Virtual

Warfare Against Digital Extortion

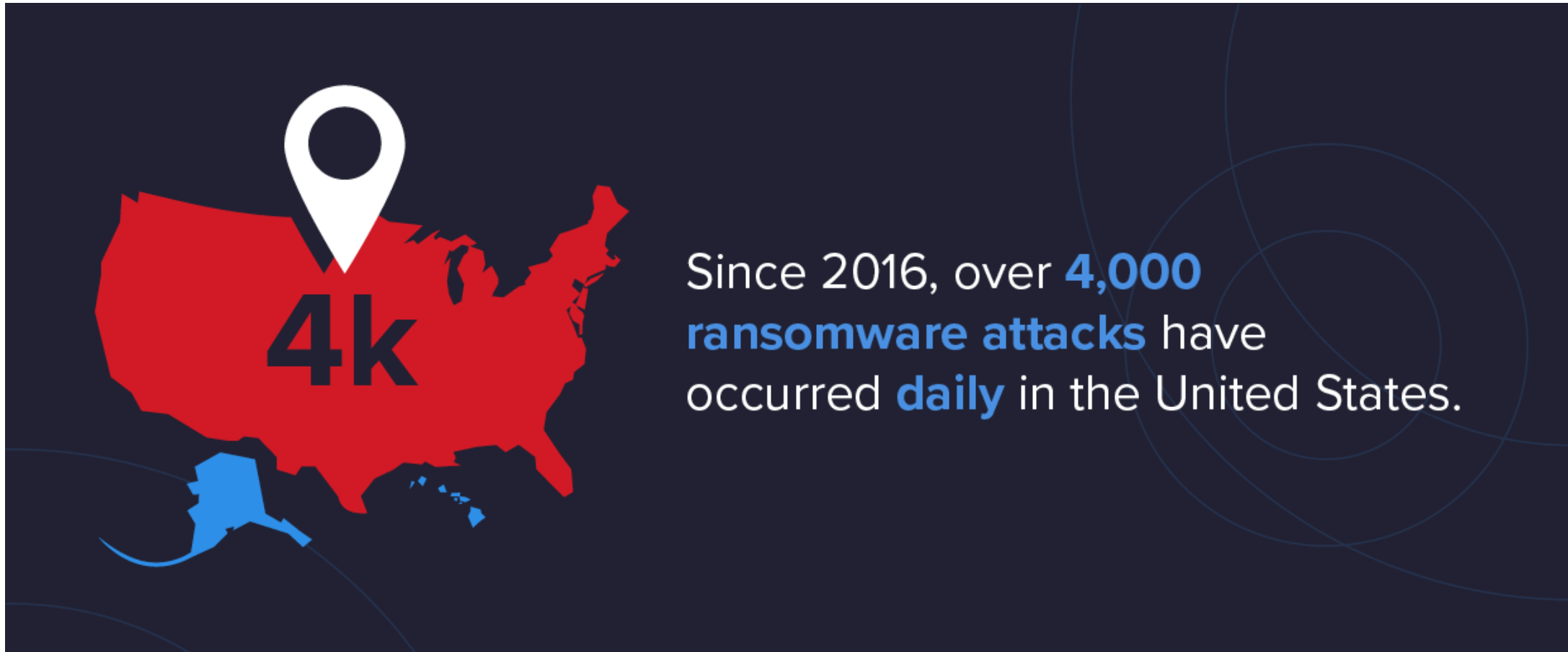
Machine Learning to Secure your Systems

Anand Kayande



A SNIA[®] Event

What is digital extortion? How critical it is?



Know your enemy: How it looks?

Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before the cost of decrypting files will increase **2 times** and will be **1000 USD/EUR**

Prior to increasing the amount left:


103h 37m 58s

Your system: Windows 7 (x64) First connect IP: Total encrypted files:

[Refresh](#) [Payment](#) [FAQ](#) [Decrypt 1 file for FREE](#) [Support](#)

We are present a special software - CryptoWall Decryptor - which is allow to decrypt and return control to all your encrypted files

[How to buy CryptoWall decryptor?](#)



- You should register Bitcoin wallet (click here for more information with pictures)**
- Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.**

Here are our recommendations:

 - [LocalBitcoins.com](#) - This fantastic service allows you to search for people in your community willing to sell bitcoins to you directly.
 - [How To Buy Bitcoins](#) - An international directory of bitcoin exchanges.
 - [Cash into Coins](#) - Recommended for fast, simple service.
 - [Coinbase](#) - Bitcoin exchange based in the United States (Highly rated)
 - [BitStamp](#) - A multi currency bitcoin exchange based in Slovenia. (Highly rated)
 - [CoinJar](#) - CoinJar allows direct bitcoin purchases on their site. They're based in Australia but serve an international market.
 - [anxpro.com](#)
 - [bitvicious.com](#)
 - [ZigZag](#) - ZigZag is a global cash payment network enabling consumers to pay for digital currency.
- Send 1.22 BTC to Bitcoin address:** [Get QR code](#)
- Enter the Transaction ID and select amount:**

1.22 BTC = 500 USD [Clear](#)

Note: Transaction ID - you can find in detailed info about transaction you made (example: 41214a7c5667038383dd9029cf0b34f19a27c12775d3e2ae08114bf0112)
- Please check the payment information and click "PAY".**

PAY

Your sent drafts

Num	Draft type	Draft number or transaction ID	Amount	Status
Your payments not found				

What is flow of Ransomware?

1) Deployment

- a. Strategic web compromise
- b. Drive-by download
- c. Phishing emails
- d. Vulnerabilities

2) Installation

- 1) Reconstruction
- 2) Process evasion

3) Command and Control

- 1) Encryption and locking

4) Extortion

- 1) Bitcoin
- 2) Prepaid vouchers

Segment your forces for the war

General Framework for analyzing ANY binary:

- Static methods
 - Structural analysis
 - Static code analysis
- Dynamic methods
 - Behavioral analysis
 - Debugging
 - Dynamic instrumentation

Structural Analysis of binary files

Typical binary file structure, when unzipped

- 1) Resources
- 2) META-INF
- 3) Classes (binary executables)
- 4) Manifest.xml

Machine learning features to look for:

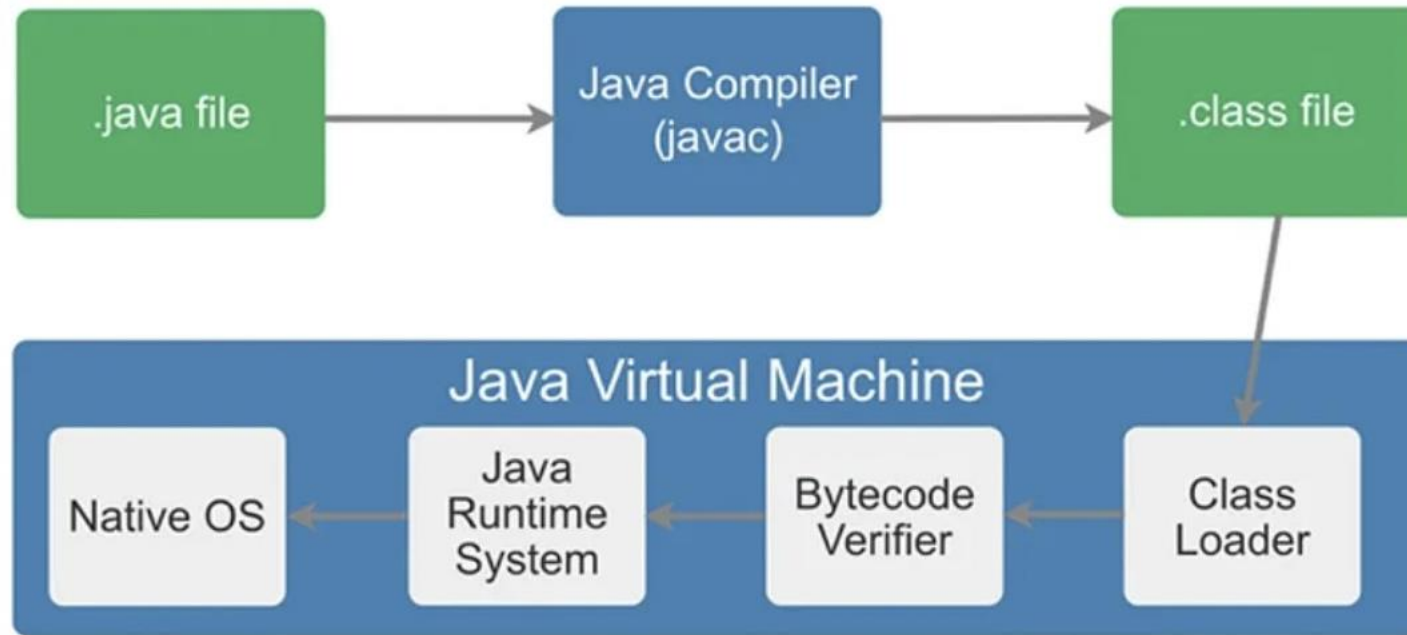
- 1) Access of resources and services
- 2) Origin and creator
- 3) Dependencies

Static Analysis of binary files

Potential threat can be predicted based on parameters. Just for example:

- Hardcoded IP address for a C&C server.
- Links to external download of payloads.
- Asking for administrative permissions.
- Socket Service
- Registry
- Browsers

Dynamic Instrumentation of binary files





Please take a moment to rate this session.

Your feedback is important to us.