Intel SGX: the ransomware strongbox?

Mathilde Venault - c0c0n 2022

About me

> Security Researcher at CrowdStrike

> RE Windows undocumented mechanisms

> Ex-volunteer firefighter

> Previously talked at Black Hat 2020 & c0c0n 2020

CROWDSTRIKE

Introduction

623, 300, 000

ransomware attacks in 2021, according to statista.com

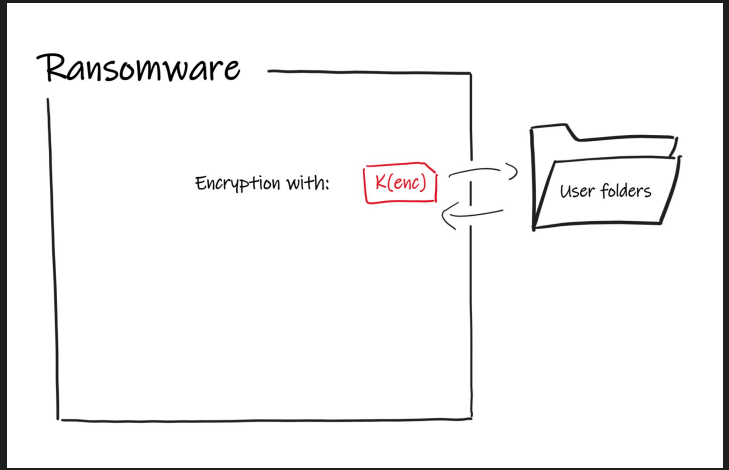
CROWDSTRIKE

Ransomware key management

Overview of this cryptographic challenge

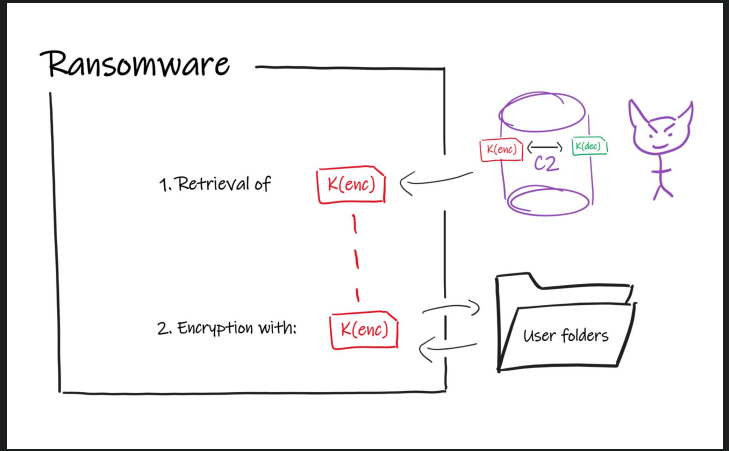
Key management methods

1. **Encryption key embedded in the binary**



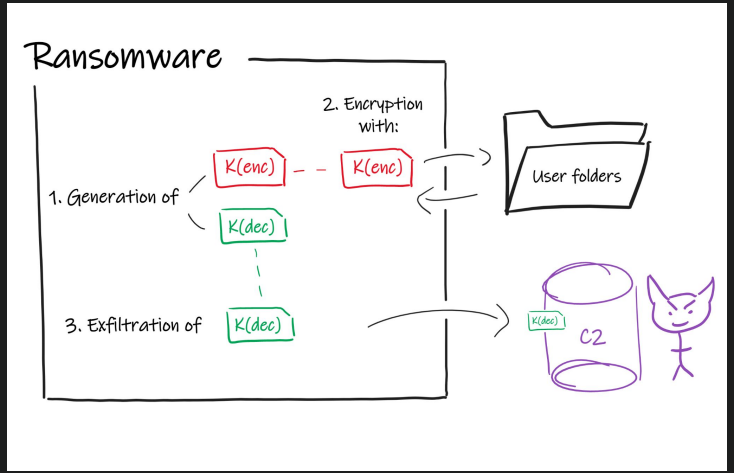
Key management methods

1. Encryption key embedded in the binary
2. **Encryption key retrieved from the C2**



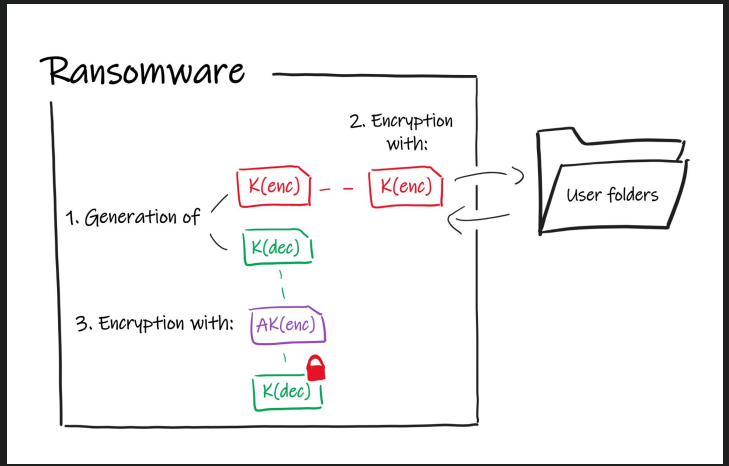
Key management methods

1. Encryption key embedded in the binary
2. Encryption key retrieved from the C2
3. **Locally generate keys; send the decryption key to the C2**



Key management methods

1. Encryption key embedded in the binary
2. Encryption key retrieved from the C2
3. Locally generate keys; send the decryption key to the C2
4. **Locally generate keys; encrypt the decryption key with the attacker's key embedded in the binary**



CROWDSTRIKE

Comparison

METHODS	Requires internet	Exposed to forensic methods	Same decryption key for each victim
Encryption key embedded in the binary		X	X

CROWDSTRIKE

Comparison

METHODS	Requires internet	Exposed to forensic methods	Same decryption key for each victim
Encryption key embedded in the binary		X	X
Encryption key sent from the C2	X		

CROWDSTRIKE

Comparison

METHODS	Requires internet	Exposed to forensic methods	Same decryption key for each victim
Encryption key embedded in the binary		X	X
Encryption key sent from the C2	X		
Decryption key sent to the C2	X	X	

CROWDSTRIKE

Comparison

METHODS	Requires internet	Exposed to forensic methods	Same decryption key for each victim
Encryption key embedded in the binary		X	X
Encryption key sent from the C2	X		
Decryption key sent to the C2	X	X	
Local generation & encryption of decryption key with the attacker's key embedded in the binary		X	

CROWDSTRIKE

RansomClave, the solution?

> Researchers of Royal Holloway, University of London presentend RansomClave

> Consists in a new model of ransomware based on Intel SGX

> Published details on "*RansomClave: Ransomware Key Management using SGX*"*

*https://arxiv.org/pdf/2107.09470.pdf

CROWDSTRIKE

Intel SGX technology

The technology for a trusted execution environment

Overview

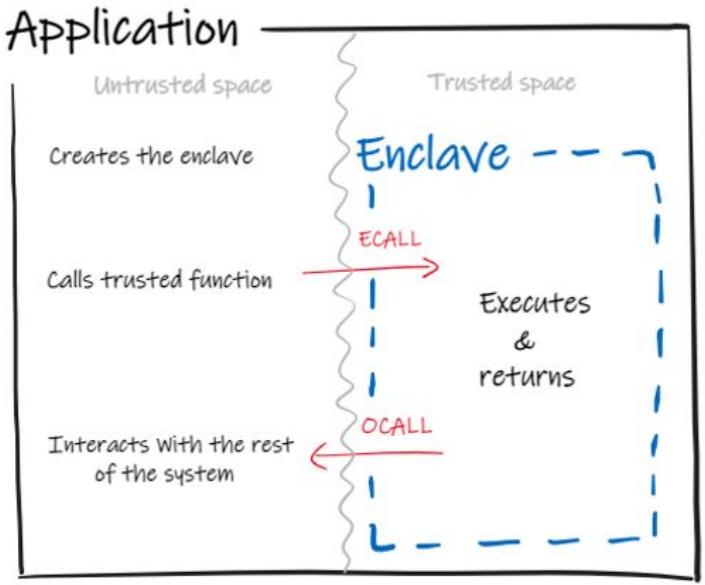
> Launched in 2015 by Intel, deprecated for recent CPUs

> New set of CPU instructions

> Isolate portion of code in memory on a reserved part of the CPU

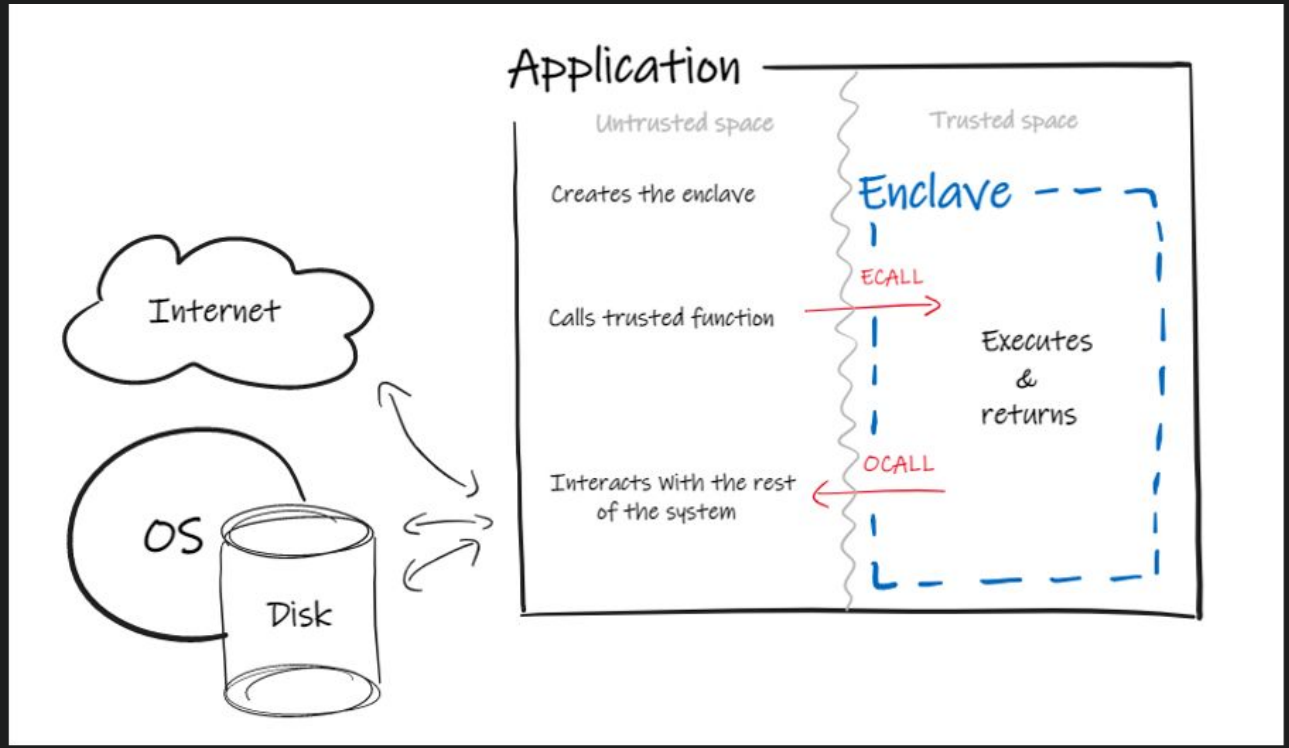
CROWDSTRIKE

Architecture



CROWDSTRIKE

Architecture



CROWDSTRIKE

Requirements

Hardware	Software	Valid signature
The CPU between 6th (released in 2015) and 11th generation (released in 2021)	Intel SGX feature has to be enabled in BIOS	The enclave must be compiled with a valid signature

CROWDSTRIKE

Signature process

In debug mode

> A **debug signature** is automatically provided by a Visual Studio tool

> Requires dependencies to be on the local system

In release mode

> A **Commercial Use License Agreement** needs to be signed

> The submission of a **Whitelist Registration Form** has to be approved by Intel

CROWDSTRIKE

Sealing

> The goal: keeping the enclave's data secret across reboots

> Encryption of the data based on a key unique to the enclave

> The author chooses to rely either on the **MRSIGNER** or on the **MRENCLAVE**

CROWDSTRIKE

Encryption using enclaves

Hiding secrets inside the enclave

CROWDSTRIKE

RansomClave: the concept

Generate keys inside the enclave

> No other process can intercept the decryption key

> The decryption key does not remain in memory after the attack

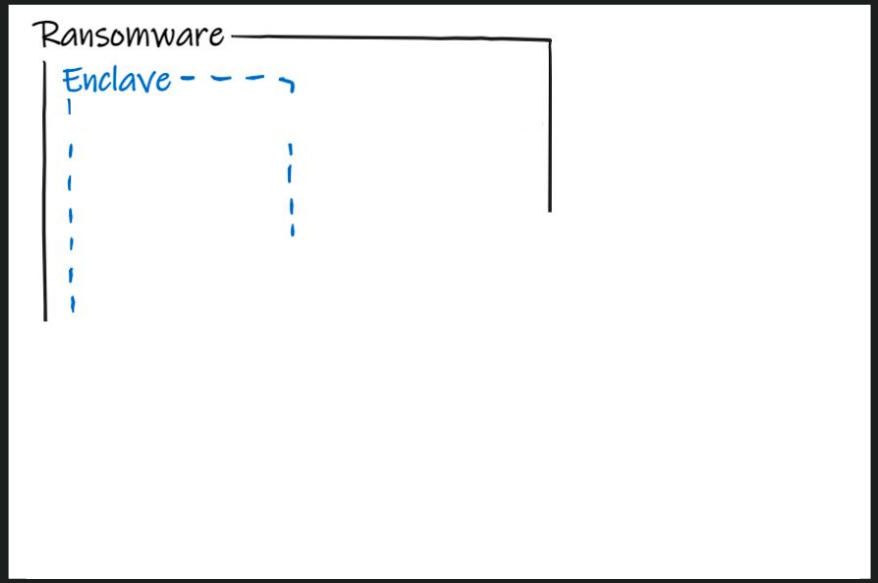
Seal the decryption key

> No internet connection required, the decryption key remains on the system

> Only the enclave that has sealed the decryption key can unseal it

Roadmap of the attack

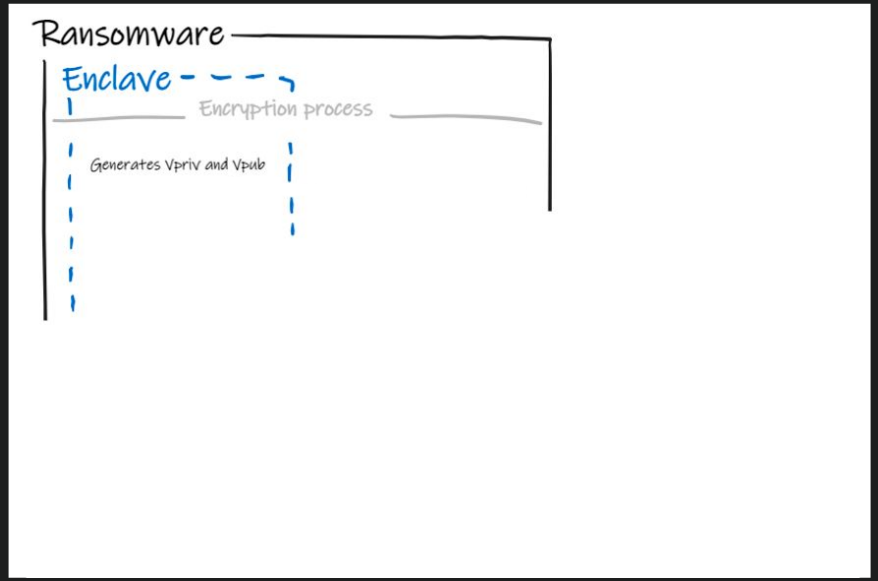
> Step 1: infecting a target system



Roadmap of the attack

> Step 1: infecting a target system

> Step 2: generating cryptographic keys using enclaves

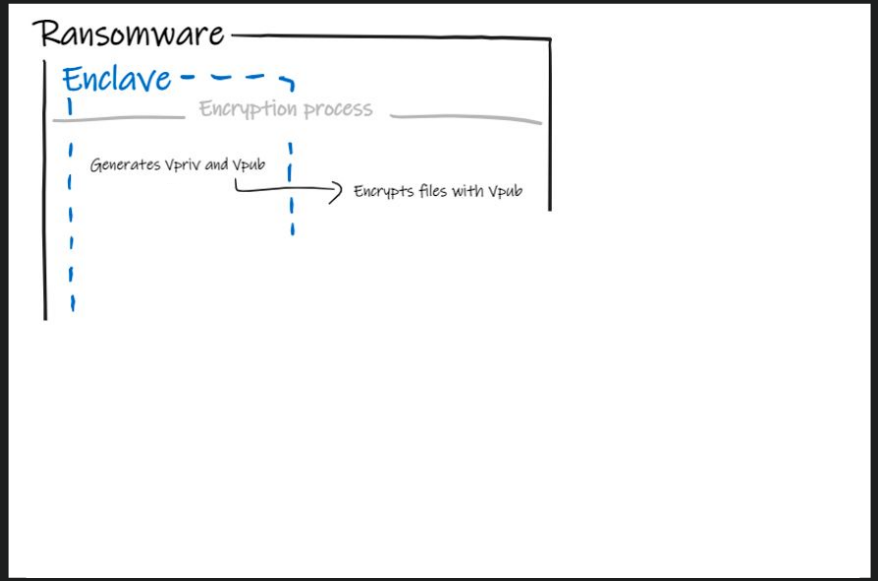


Roadmap of the attack

> Step 1: infecting a target system

> Step 2: generating cryptographic keys using enclaves

> Step 3: encrypting victim's data



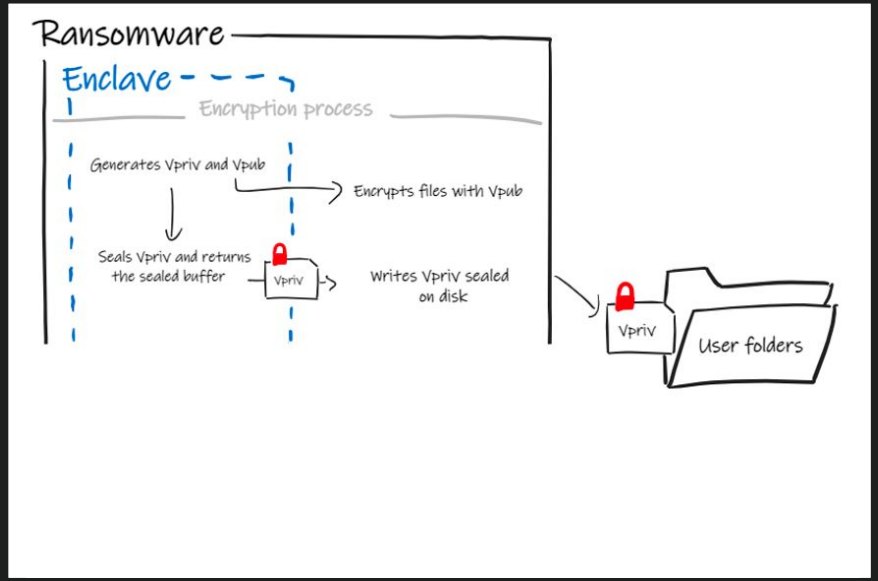
Roadmap of the attack

> Step 1: infecting a target system

> Step 2: generating cryptographic keys using enclaves

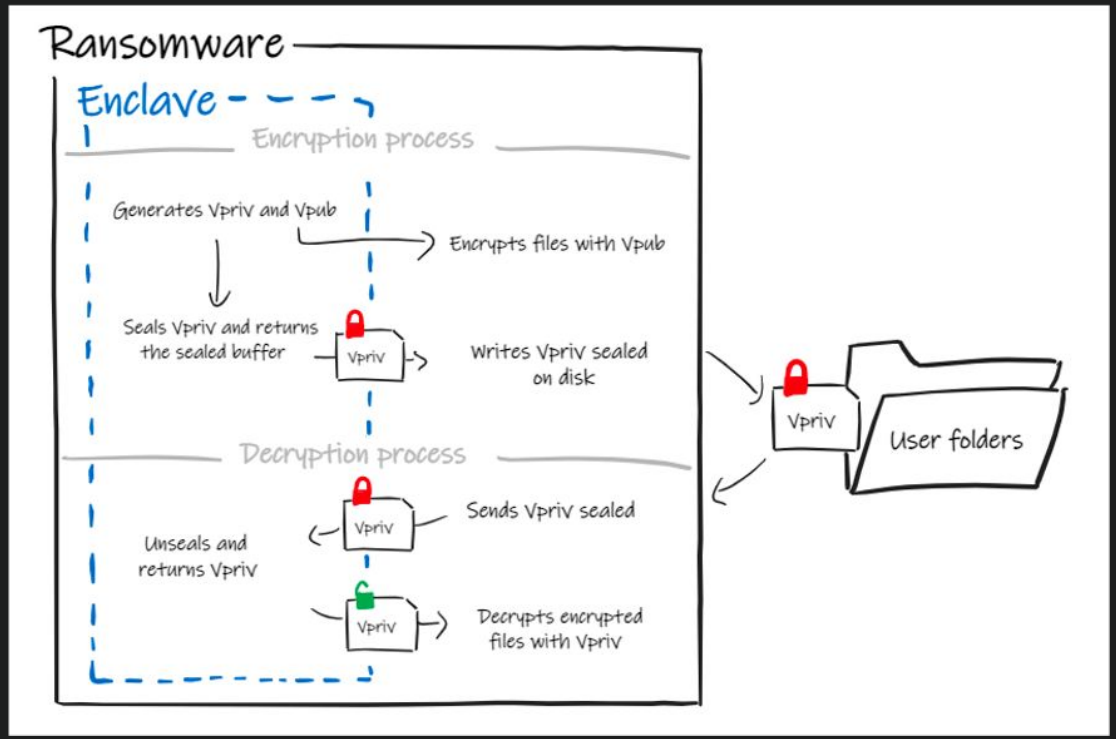
> Step 3: encrypting victim's data

> Step 4: sealing the decryption key



CROWDSTRIKE

Roadmap of the attack



CROWDSTRIKE

Benefits

The decryption key can’t be retrieved by classic forensic tools

No command-and-control server required

One binary, different decryption keys

CROWDSTRIKE

Time for a demo!

Limitations

Can RansomClave be used into the wild?

CROWDSTRIKE

Limitations

- Hardware requirements
- Software requirements
- Signing requirements
- Security of the sealed decryption key
- Surely…but slowly
- Vulnerabilities to side channel attacks

CROWDSTRIKE

Limitations

Hardware requirements

Software requirements

Signing requirements

Security of the sealed decryption key

Surely…but slowly

Vulnerabilities to side channel attacks

CROWDSTRIKE

Challenges & Possible Solutions

Hardware requirements

Perform fingerprinting before attacking a system

CROWDSTRIKE

Limitations

- Hardware requirements
- **Software requirements**
- Signing requirements
- Security of the sealed decryption key
- Surely…but slowly
- Vulnerabilities to side channel attacks

CROWDSTRIKE

Challenges & Possible Solutions

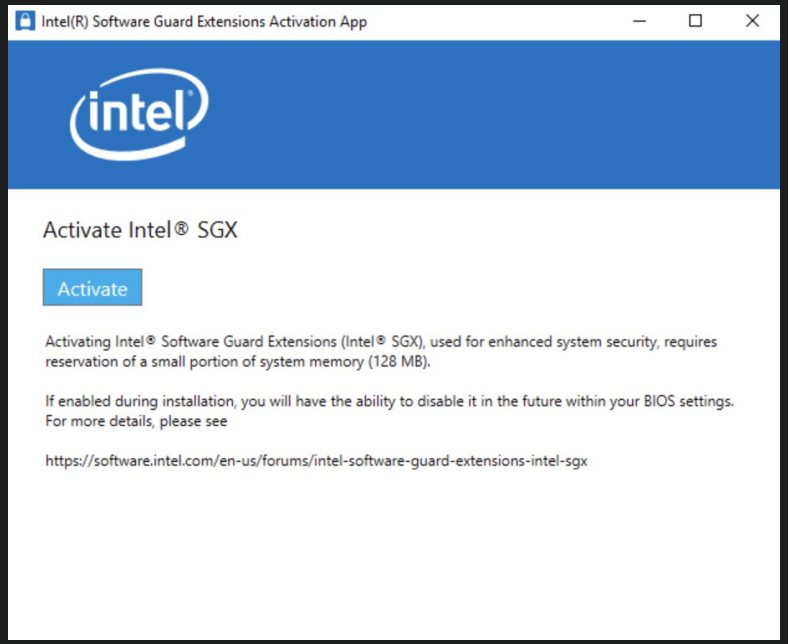
Software requirements

Perform fingerprinting and if Intel SGX isn't enabled, take some pre-infection measures to enable it

CROWDSTRIKE

Challenges & Possible Solutions

Software requirements



CROWDSTRIKE

Limitations

- Hardware requirements
- Software requirements
- **Signing requirements**
- Security of the sealed decryption key
- Surely…but slowly
- Vulnerabilities to side channel attacks

CROWDSTRIKE

Challenges & Possible Solutions

Signing requirements

Use debug enclaves & embed dependencies within malicious binaries

CROWDSTRIKE

Limitations

- Hardware requirements
- Software requirements
- Signing requirements
- **Security of the sealed decryption key**
- Surely…but slowly
- Vulnerabilities to side channel attacks

CROWDSTRIKE

Challenges & Possible Solutions

Security of the sealed decryption key

Make sure the enclave's binaries are removed after the attack in order to prevent the recreation an app capable of interfacing with the enclave

CROWDSTRIKE

Limitations

- Hardware requirements
- Software requirements
- Signing requirements
- Security of the sealed decryption key
- **Surely…but slowly**
- Vulnerabilities to side channel attacks

CROWDSTRIKE

Challenges & Possible Solutions

Surely…but slowly

Export the encryption key and encrypt data outside of the enclave

CROWDSTRIKE

Limitations

- Hardware requirements
- Software requirements
- Signing requirements
- Security of the sealed decryption key
- Surely…but slowly
- **Vulnerabilities to side channel attacks**

CROWDSTRIKE

Challenges & Possible Solutions

Vulnerabilities to side channel attacks*

Bet on the low probability that a side channel attack has been set-up to target a ransomware attack….

*“How SGX Fails in Practice”, https://sgaxe.com/files/SGAxe.pdf

Conclusion

CROWDSTRIKE

Conclusion

> From an offensive perspective...
- One of the ideal ways to manage cryptographic keys
- Still, lots of challenges to overcome

> From a defense perspective...
- Keep in mind that enclaves are not malicious on their own
- The use of enclaves won't bypass EDR detections capabilities

CROWDSTRIKE

Thank you for your attention!

Any questions?