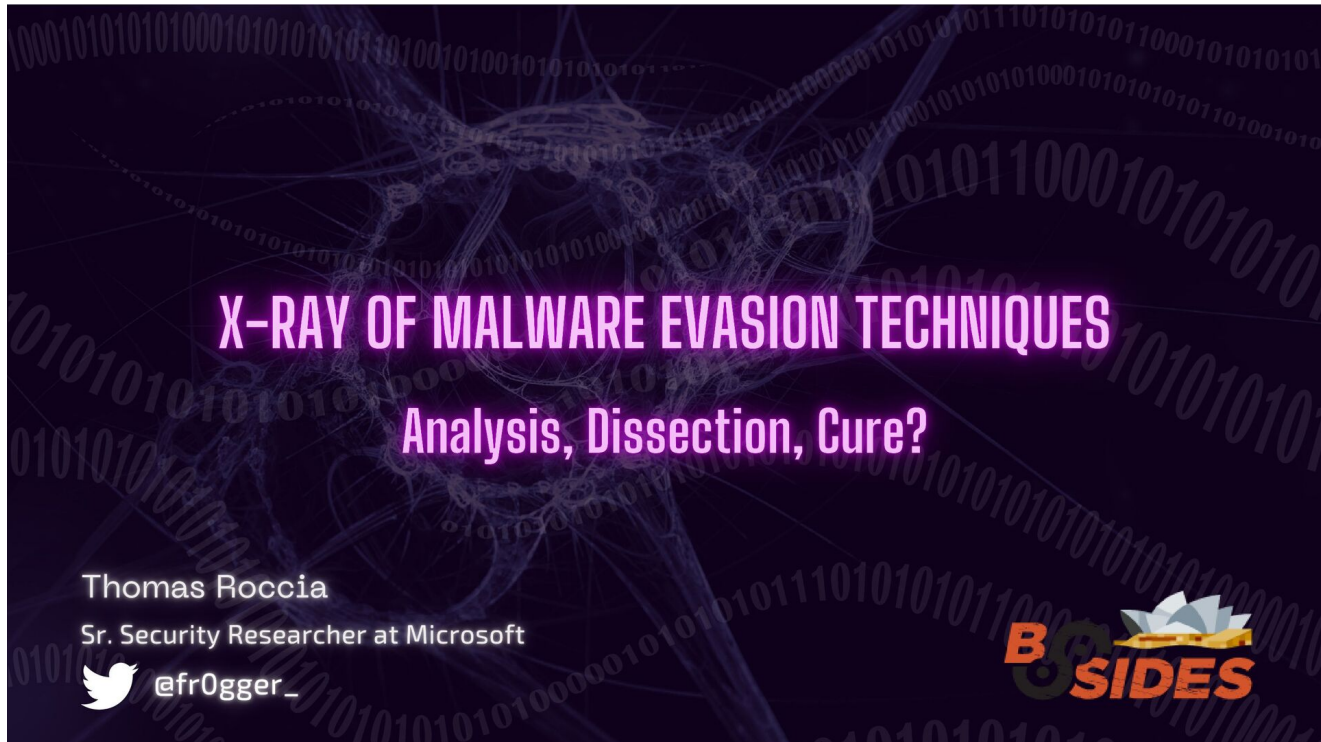


X-Ray of Malware Evasion Techniques: Analysis, Dissection, Cure?

 speakerdeck.com/fr0gger/x-ray-of-malware-evasion-techniques-analysis-dissection-cure



This presentation has been presented at Bsidess Sydney (<https://bsidessydney.org/>)

Malware evasion consists of techniques used by malware to bypass security in place, circumvent automated and static analysis as well as avoiding detection and harden reverse engineering. There is a broad specter of techniques that can be used. In this talk we will review the history of malware evasion techniques, understand the latest trends currently used by threat actors and bolster your security analysis skills by getting more knowledge about evasion mechanisms.


More Decks by Thomas Roccia

[See All by Thomas Roccia](#)

Other Decks in Technology

[See All in Technology.](#)

API連携に伴う規制と対応 / Regulations and responses to API linkage

 moneyforward

0

150


ユーザーテストガイドライン VERSION 2.0

 kouzoukaikaku

0

880

プログラミング支援AI GitHub Copilot すごい話

 moyashi

0

290

ROS_Japan_UG_#49_LT

 maeharakeisuke

0

210

FlexScan HD2452Wの後継を探して

 tring

0

6k

【NGK2023S】ノードエディタ形式の画像処理ツール「Image-Processing-Node-Edi...

 kazuhitotakahashi

0

250

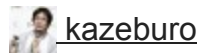
OPENLOGI Company Profile



0

12k

DNS権威サーバのクラウドサービス向けに行われた攻撃および対策 / DNS Pseudo-R...



5

1.2k

Stripe / Okta Customer Identity Cloud(旧Auth0)の採用に至った理由 ～モリサワの S...



0

120


エアドロップ for オープンソースプロジェクト

 epicsdao

0

350

オンプレk8sとEKSの並行運用の実際

 ch1aki

0

220

SPA・SSGでSSRのようなOGP対応！

 simo123

2

150

Featured

[See All Featured](#)

[Put a Button on it: Removing Barriers to Going Fast.](#)



[kastner](#)

56

2.5k

[Building Your Own Lightsaber](#)



[phodgson](#)

96

4.9k

Fontdeck: Realign not Redesign

 paulrobertilloyd

74

4.3k

Fight the Zombie Pattern Library - RWD Summit 2016

 marcelosomers

227

16k

RailsConf & Balkan Ruby 2019: The Past, Present, and Future of Rails at GitHub

 eileencodes

120

29k

Designing the Hi-DPI Web

 ddemaree

273

32k


Building Adaptive Systems

 keathley

27

1.3k

We Have a Design System, Now What?

 morganepeng

37

5.9k

The Power of CSS Pseudo Elements

 geoffreycrofte

52

4.3k

Building a Scalable Design System with Sketch

 lauravandoore

451

31k

Cheating the UX When There Is Nothing More to Optimize - PixelPioneers

 stephaniewalter

270

12k

Java REST API Framework Comparison - PWX 2021

 mraible

PRO

13

5.4k

Transcript

1. None

2. None

3. None

4. **What are Evasion Techniques? Practical examples and current trends**
How

can you step up on that topic? The power of information sharing

5. **All the techniques used by a a software to avoid**

static, dynamic, automatic and human analysis in order to understand its behavior All the techniques used by malware to avoid and evade security solutions, security configuration as well as human detection to perform malicious action the longer on the infected computer.

6. **In Mitre ATT&CK, the Defense Evasion section is the most**

dominant tactic For attackers, the longer the malware remains undetected the longer they can perform actions For defenders, the sooner the malware is detected the less damage it will cause

7. *None*

8. **Anti Security techniques Anti Sandboxing techniques Anti Analyst techniques**

9. **Infection Vectors Malware Delivery Malware Behavior Actions on Objectives**

10. **Malicious Doc Obfuscated Macro Powershell Base64 encoded Dropping Emotet**

11. **Binded with legit Software Fake Metadata**

12. **Fake Operations to harden reverse engineering and delay sandbox Anti-disassembly**

with Code Spaghetti

13. **Encrypted data related to host sent to multiple C2 Multiple**

Network Connections not available in the binary

14. **2015 2016 2017 2019 2020 2021 2022 Creation of Unprotect**

Project First public release at Botconf Creation of the Unprotect POC BlackHat ASIA @DarkCoderSc joined the project Redesign, includes detection rules and code snippets API Engine, statistics

15. **Community centric open project dedicated to cataloguing malware evasion techniques**

Includes detection rules (Yara, Sigma, Capa) and code snippets Extends the Mitre ATTT&CK Defense Evasion Section Share and improve knowledge about evasion mechanisms Propose a detailed classification

16. *None*

17. *None*

18. *None*

19. *None*

20. **Malware Evasion Techniques are used by malware to avoid detection**

and analysis These techniques are highly regarded by threat actors. The Unprotect Project is a database dedicated to it and provide the broadest knowledge about evasion techniques.

21. *None*