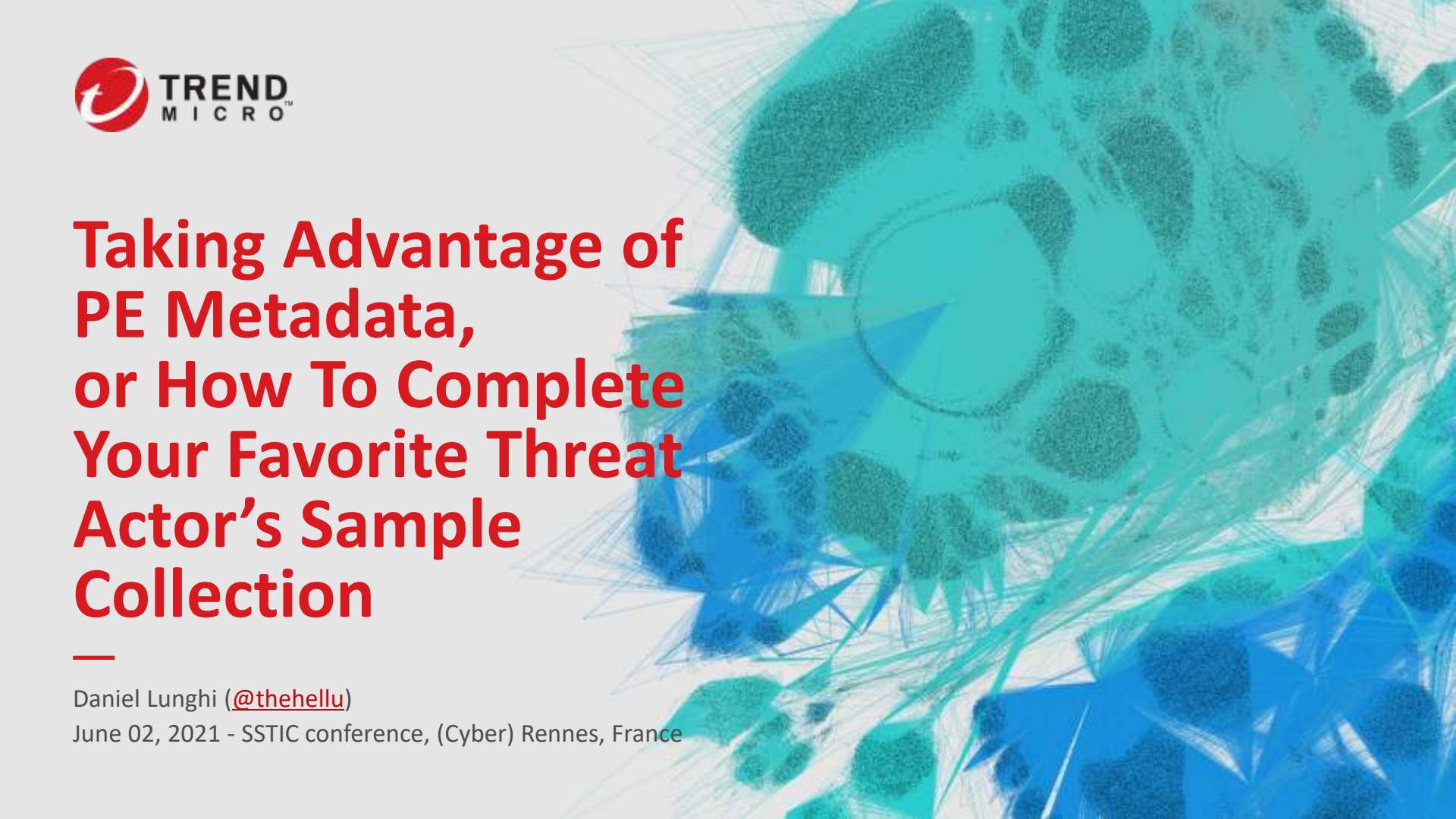


Taking Advantage of PE Metadata, or How To Complete Your Favorite Threat Actor's Sample Collection

Daniel Lunghi (@thehellu)

June 02, 2021 - SSTIC conference, (Cyber) Rennes, France

Outline

- Introduction
- Malware analysis and classification
- Pivoting
  - Filenames
  - Imphash
  - RICH header
  - Stolen certificates
  - TLSH
- Conclusion

© 2021 Trend Micro Inc.

Introduction

- This talk focuses on the methodology of sample pivoting

- Examples are based on a real case investigation published on April 09, 2021 in the Trend Micro blog

  Iron Tiger APT Updates Toolkit With Evolved SysUpdate Malware

- Goal:
  - Find more samples/IOCs of a particular malware family/threat actor

© 2021 Trend Micro Inc.

Introduction

- Investigation started in December 2020, after Talent-Jump technologies brought an unknown sample to us
- Sample was found in the same gambling company that was targeted during Operation DRBControl
- At the time, we found links to 3 different threat actors

© 2021 Trend Micro Inc.

Malware analysis and classification

© 2021 Trend Micro Inc.

Malware analysis and classification

- 4 files:
  - dlpumgr32.exe: legitimate signed file, part of the DESlock+ product
  - DLPPREM32.DLL: malicious side-loaded DLL file loading DLPPREM32.bin
  - DLPPREM32.bin: shellcode decompressing and loading a “launcher”
  - data.res: encrypted file containing the final payload, decoded by the “launcher”

After analysis, a fifth file is involved, config.res. It contains the C&C

© 2021 Trend Micro Inc.

Malware analysis and classification

- The unpacked code can be dumped from memory

- We look for patterns to identify the malware family
  - Uncommon strings/constants
  - Noteworthy encryption/obfuscation algorithm

⇒ There is a hardcoded user-agent which is listed in a Dell Secureworks blogpost

© 2021 Trend Micro Inc.

Malware analysis and classification

- The blogpost mentions multiple tools from the BRONZE UNION (Iron Tiger) threat actor

- **SysUpdate** is mentioned, and as far as we know, exclusive to the Iron Tiger threat actor

- We found a detailed description of **SysUpdate** in a NCC group blogpost that matches the behavior of the “launcher”

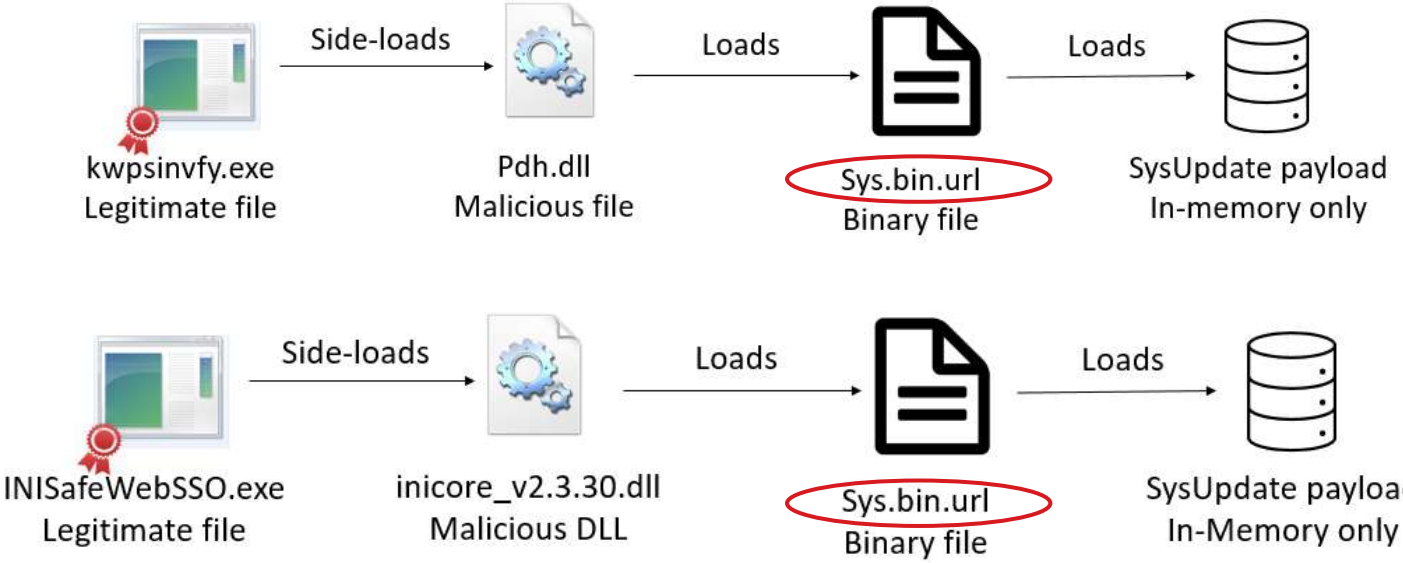
© 2021 Trend Micro Inc.

Pivoting

© 2021 Trend Micro Inc.

Pivoting – filenames

- Two loading scenarios found in previous blogs



© 2021 Trend Micro Inc.

Pivoting – filenames

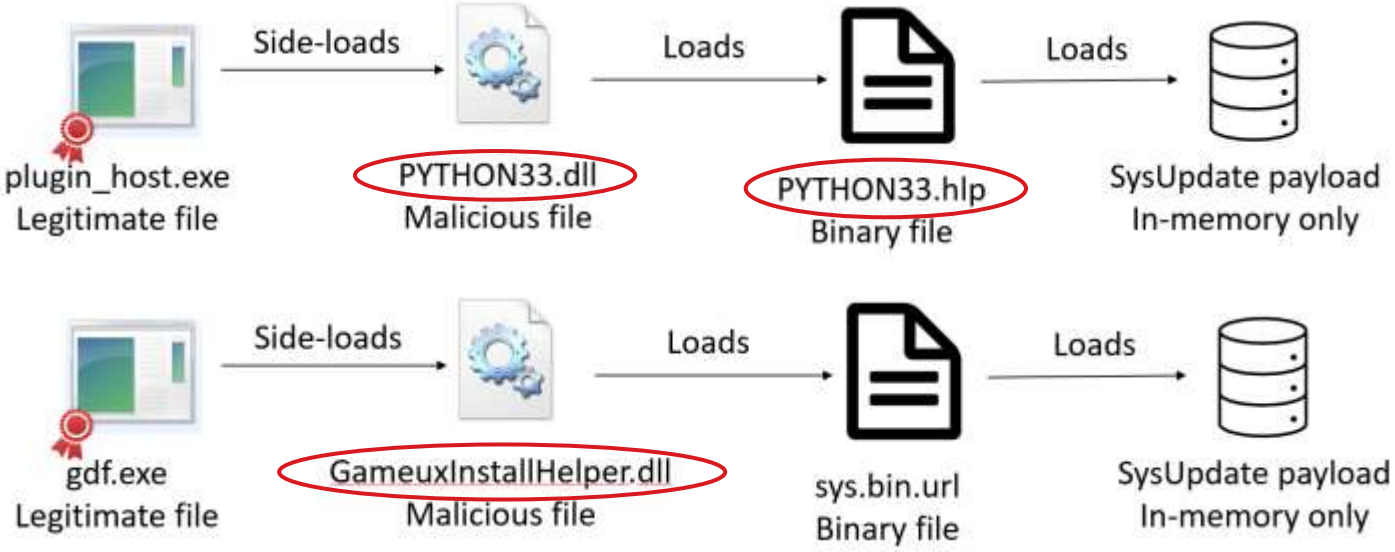
- Search engines
  - Few sandbox results, but the hashes were already known
- Malware repositories (Virus Total and internal)
  - 8 results, of which 7 were not listed in the two mentioned reports
- Searching those new samples lead to two additional reports:
  - One published by AE.CERT on June 13th, 2019
  - One published by Iranian private company on March 2020

  ⇒ History of previous targets (Iran, UAE)

© 2021 Trend Micro Inc.

Pivoting – filenames

- New loading scenarios/filenames in those reports



© 2021 Trend Micro Inc.

Pivoting – filenames

- Pivoting on DLL filenames is trickier
  - Filenames are used by legitimate files
  - The same legitimate executables can be abused by multiple threat actors
- Filtering on metadata such as file size reduces the number of results
  - “name:PYTHON33.DLL”: 129 results
  - “name:PYTHON33.dll size:100Kb-”: 6 results (3 FP)

© 2021 Trend Micro Inc.

Pivoting – filenames

- New filenames lead to additional reports from multiple companies or even researchers

THREAT ANALYSIS

A Peek into BRONZE UNION's Toolbox

WEDNESDAY, FEBRUARY 27, 2019
BY: COUNTER THREAT UNIT RESEARCH TEAM

Emissary Panda – A potential new malicious tool

Nikolaos Pantazopoulos Reverse Engineer May 18, 2018
6 Minutes

Advanced Notification of Cyber Threats against Family of Malware Giving Remote Access to Computers

CERT

Security Advisory	ADV-19-27	Criticality	High
Advisory Released On	13 June 2019		

in Norfolk

nd Malware Analysis

CT ME PRETZELS PRESENTATIONS

Emissary Panda DLL Backdoor

JULY 21, 2019 NORFOLK

Emissary Panda Attacks Middle East Government SharePoint Servers

58,523 people reacted 5 13 min. read

SHARE

By Robert Falcone and Tom Lancaster
May 28, 2019 at 6:00 AM
Category: Unit 42
Tags: APT27, Bronze Union, China Chopper, CVE-2019-0604, DLL Sideloading, Emissary Panda, ETERNALBLUE, HyperBro, Lucky Mouse, MS17-010, TG-3390, webshell

© 2021 Trend Micro Inc

Pivoting – imphash

- “Import hashing”, or imphash, is a method disclosed by Mandiant/FireEye in 2014
- It relies on the Import Address Table (IAT), which is built by the linker at compilation time
- The IAT will be different depending on
  - The order in which the functions are called in the source code
  - The order in which the source files are parsed by the linker
- The output of the imphash algorithm is an MD5 hash

© 2021 Trend Micro Inc.

Pivoting – imphash

- Virus Total and Malware Bazaar provide a search keyword:
  - imphash: <imphash value>
- Yara has a function to calculate it in the “pe” module:
  - pe.imphash() == <imphash value>
- There is a stand-alone Python implementation

© 2021 Trend Micro Inc.

Pivoting – imphash

- PYTHON33.DLL file from Iranian report has imphash 509a33520280773673 21fbf20f39f6d9

- Virus Total returns 3 files with such imphash
  - 2 files are named “GameuxInstallHelper.dll”

- There may be false positives, especially for small files

© 2021 Trend Micro Inc.

Pivoting – RICH header

- Metadata inserted in PE files by Microsoft compilers, first documented in 2010
- Contains information on the building environment (Product ID, version, count)
- XORed with a key which is a checksum of some headers

© 2021 Trend Micro Inc.

Pivoting – RICH header

- Two files with a similar RICH header may be generated in the same build environment
- By searching for similar RICH headers, we might find additional samples from the same threat actor
- Simplest approach for pivoting is to calculate a MD5 hash of the unxored RICH header

© 2021 Trend Micro Inc.

Pivoting – RICH header

- Virus Total has a search modifier for this
  - rich_pe_header_hash:<RICH header's MD5>
- For other platforms, a Yara rule can be used for this
  - hash.md5(pe.rich_signature.clear_data) == <RICH header's MD5>
- Or you can use a stand-alone Python implementation

© 2021 Trend Micro Inc.

Pivoting – RICH header

- inicore_v2.3.30.dll from Palo Alto's blogpost has RICH header's hash 5503d2d1e505a487cbc37b6ed423081f

- Virus Total returns 3 results for this hash
  - 2 files are named "GameuxInstallHelper.dll"

© 2021 Trend Micro Inc.

Pivoting – RICH header

- The RICH header is not needed for proper code execution
  - It can be removed, modified, copied, forged…

- Famous example of false flag involving RICH header in 2018
  - The RICH header from a sample attributed to Lazarus group was copied to a sample from the Olympic Destroyer campaign

© 2021 Trend Micro Inc.

Pivoting – Stolen certificates

- PE files can be signed via the Authenticode technology
- It identifies the publisher of the file, and guarantee that the code has not been tampered
- It relies on certificates, managed by certification authorities

© 2021 Trend Micro Inc.

Pivoting – Stolen certificates

- Private keys are sometimes stolen, allowing threat actors to sign malicious code
- Certification authorities revoke the certificate once notified
- Searching for all executables signed by a stolen certificate is a good pivot
  - Keep in mind that all results are not malicious

© 2021 Trend Micro Inc.

Pivoting – Stolen certificates

- Virus Total has a search keyword:
  - signature: <any metadata in the certificate, thumbprint, serial, CN field…>
- Malware Bazaar has a two search keywords:
  - serial_number: <certificate' serial number>
  - issuer_cn: <certificate's issuer>

© 2021 Trend Micro Inc.

Pivoting – Stolen certificates

- Yara can parse certificates in the “pe” module:

```
for any i in (0 .. pe.number_of_signatures): (
        pe.signatures[i].serial == <certificate’s serial number in low case>
        or pe.signatures[i].thumbprint == <certificate’s thumbprint in low case>
 )
```

© 2021 Trend Micro Inc.

Pivoting – Stolen certificates

- inicore_v2.3.30.dll from Palo Alto's blogpost is signed by a "Kepware Technologies" certificate

- Virus Total returns 9 results with this serial number
  - All are related to Iron Tiger

© 2021 Trend Micro Inc.

Pivoting – TLSH

- TLSH is a “fuzzy hashing” algorithm
  - Split the input in blocks of variable length and makes a hash out of it
- Output is a 72-character long hash
- Mixed results, although better than with other fuzzy hashing algorithms

© 2021 Trend Micro Inc.

Pivoting – TLSH

- Virus Total and Malware Bazaar provide a search keyword:
  - tlsh: <TLSH value>

- Yara does not have a way to calculate this hash

- The code is open source and can be applied to a local malware repository

© 2021 Trend Micro Inc.

Pivoting – TLSH

- Wsocks32.dll from Dell SecureWorks blogpost has TLSH
  T112F21A0172A28477E1AE2A3424B592725D7F7C416AF040CB3F9916FA9FB16D0DA3C367
  - More than 200 results, some of them are related, most are not

- PYTHON33.dll from Palo Alto blogpost has TLSH
  T17A634B327C97D8B7E1D97AB858A2DA12152F250059F588C9BF7043E70F2A6509E37F0E
  - 3 related results in Virus Total, one named “GameuxInstallHelper.dll”

© 2021 Trend Micro Inc.

Conclusion

© 2021 Trend Micro Inc.

Conclusion – Results

- Started from one sample found in 2020…
- …ended with 38 unpacked SysUpdate samples

- The oldest one has a compilation timestamp of March 2015, some of them were uploaded in 2016

© 2021 Trend Micro Inc.

Conclusion – Takeaways

- Many techniques enable malware sample correlation
- These techniques have flaws (collisions, based on forgeable fields), but are still useful
- Threat actors make mistakes, they improve, and so does the threat intelligence field

© 2021 Trend Micro Inc.

Conclusion – Takeaways

- Confrontation with other sources (infrastructure, TTPs, political agenda) is mandatory to avoid false flags
  - Everyone does mistakes. Acknowledge and fix them and you will be fine

- Sharing is caring, public research reports are useful if they contain enough actionable information

© 2021 Trend Micro Inc.


TREND MICRO
THE ART OF CYBERSECURITY
Automated hybrid cloud workload protection via calls to Trend Micro APIs. **Created with real data by Trend Micro threat researcher and artist Jindrich Karasek.**