IEEE Taggant System

Mark Kennedy, Igor Muttik

Who we are

- Representing IEEE Industry Connections Security Group (ICSG)
- *Mark Kennedy* – Chair of ICSG Malware Working Group, Symantec
- *Igor Muttik* – Vice-Chair of ICSG Malware Working Group, McAfee/Intel
- IEEE ICSG membership includes:

AV vendors
- Ahn Labs
- AVG
- Eset
- F-Secure
- K7 Computing
- Kaspersky Labs
- Marvell
- Microsoft
- Palo Alto Networks
- Panda Software
- Sophos
- Trend Micro

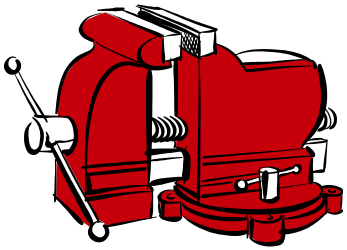
Packer vendors
- Bitsum (PECompact)
- EISST
- Enigma
- Obsidium
- Oreans (Themida)
- Safenet Inc.
- Sofpro (PCGuard)
- VMPSoft (VMProtect)

Agenda

- The problem
- The solution – Taggant System
- The players
- Benefits
  - For the Users (2 types)
  - For the Vendors (2 types)

- Taggants vs authenticode
- How the system works
- The lifecycle
- Current project status

The Packer Problem



- Packer Software takes an executable and “packs” it

- This packing changes the executable by:
  - Compressing (packed file is smaller than the original)
  - Anti-Debugging (packed file is obfuscated to make reverse-engineering difficult or impossible)
  - Using p-code virtualization (code executes under an interpreter)
  - Combination of above methods

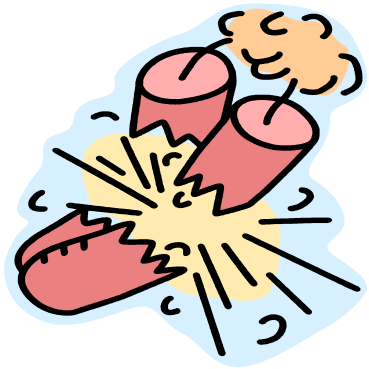
- Each of these changes have certain options

- By varying these options, one can make a near limitless number of variants from a single executable

- This becomes extremely cheap Server Side Polymorphism

Definitions

- **Packed File (Obfuscated Software or Malware)** – A result of applying Packer Software to a program file. This output file may or may not have a taggant associated with it.
- **Packed File User** – The end user, an individual who runs it.
- **Packer User** – An individual or organization that purchases or obtains Packer Software from a Software Packer Vendor.
- **Packer Software** – The tool used by Packer Users to create Packed Files.
- **Software Packer Vendor** – Develops, sells and markets the Packer Software to Packer Users.
- **Security Vendors** – Provide software to inspect files (Packed Files and other files which may or may not include a taggant).

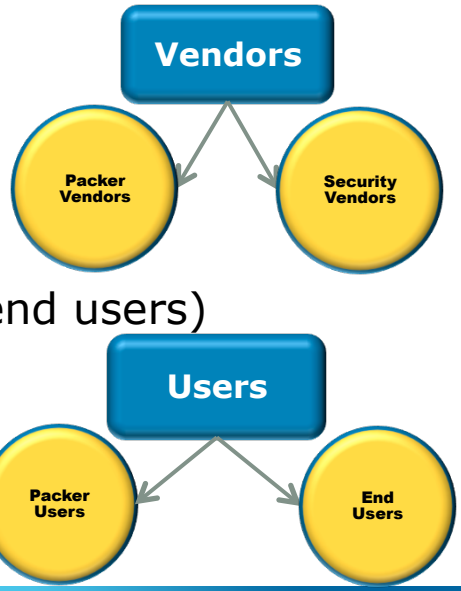


"A **taggant** is a chemical or physical marker added to materials to allow various forms of testing. Taggants allow testing marked items for qualities such as lot number and concentration (to test for dilution, for example). In particular, taggants are known to be widely used in plastic, sheet and flexible explosives."

http://en.wikipedia.org/wiki/Taggant

The IEEE Solution – Software Taggant

- The IEEE Software Taggant System will allow the "tagging" of the output of Packer Software with a cryptographically secure signature that enables positive origin identification and integrity of a Packed File using standard PKI techniques.
  - It is a portable C library
  - For packer vendors to write a taggant
  - For AV companies to read and verify it
- This will effectively "de-anonymize" code created by packers.
- Packing of files creates problems for all the players:
  - For security companies (AV)
  - For Software Packer Vendors (producers of packers)
  - For the users of packers (who pack software for the end users)
  - For the end users
- Our solution: Software Taggant System



Benefits for Everyone!

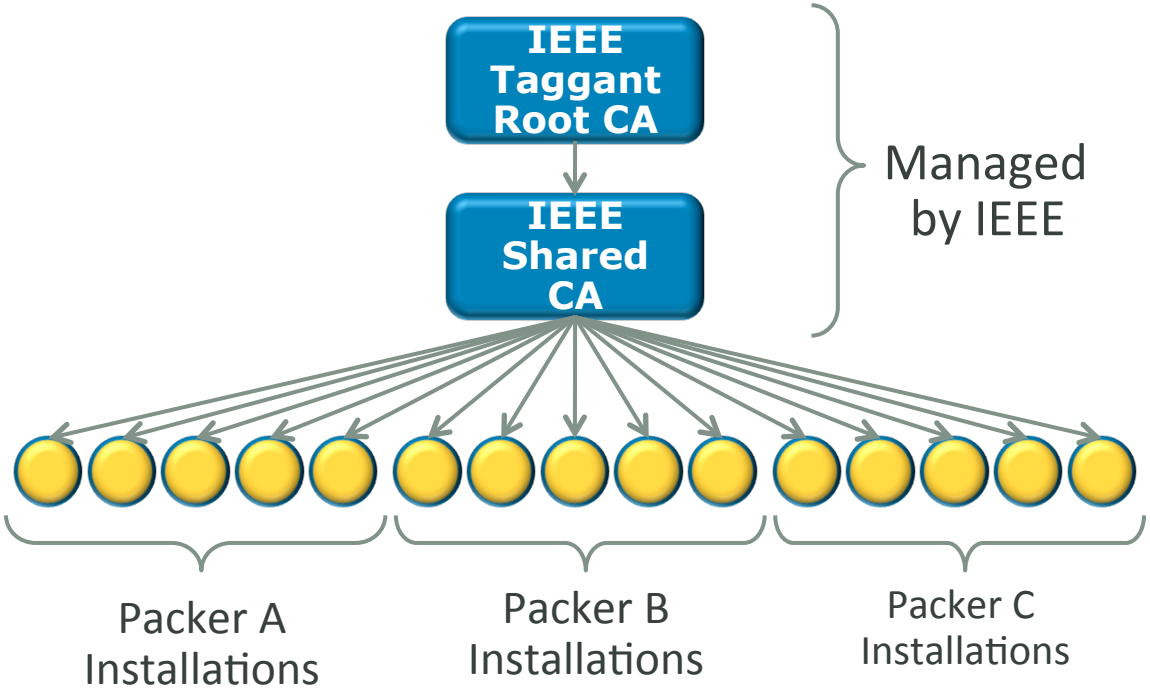
- Security Vendors
  - More proactive protection
  - Less false positives and slowdowns
  - Less resources wasted
- Software Packer Vendors
  - Less false positives
  - Enforcing of licensing, less piracy, higher returns
  - One point of contact with security industry
  - SPV are now part of the solution
  - Competitive benefits
  - It is free
- Packer Users and End-Users
  - Less false positives and slowdowns
  - It is transparent and free (unlike digital signatures)
- We are hoping to solve the problem of packed malware in ~2-3 years

Taggant vs authenticode

- Taggant contains a "performant" hash (SHA256 by default)
  - Covers only vital executable areas
- Taggant allows a fall-back on to a "default" hash
  - It covers the whole file (almost whole)
  - Will be used if the performant hash is broken
- Creating and using files with taggants is **free**
  - Included by the packing software automatically
  - The PKI infrastructure will be sponsored by AV companies
- Taggants are compatible with authenticode
  - Digital signature can be applied after a packer included a taggant

How the System Works

- Simple 3-level PKI system
- IEEE at the root of trust
- Authorizes packer vendors
- They manage certificates for Packer Users
  - Issue, revoke, etc.
- Each installation embeds its license into the taggant
- AV products can then block packed malware by recognizing bad sources



The lifecycle

Step 1 – packer vendor

- New packer vendor contacts IEEE
- IEEE verifies the vendor
- IEEE creates a vendor login
- Vendor asks for a URL for a user
- URL is embedded into the license for each user's packer setup
- Packer user gets the packer setup

Step 2 – packer software setup

- The setup logs into a unique URL
- IEEE creates a key pair
- Setup gets a certificate back

Step 3 – packer obfuscates a file

- Packer is executed to pack a file
- Taggant is created with 3 hashes
- Timestamp is included
- Setup/user certificate is included
- Taggant is part of the packed file
- Packed file is distributed

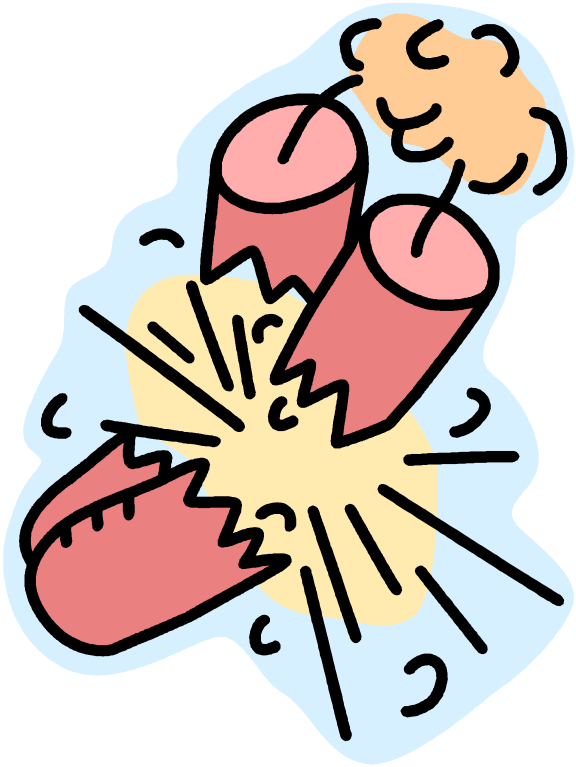
Step 4 – packed file executes

- End user runs a packed file
- AV checks the source (the setup certificate & maybe a timestamp)
- AV blocks if bad

Status of the project

- Documentation is ready
- **IEEE issued RFP** with the deadline on 07 September 2011
  - Write library code in C
- Implementation to be ready in November 2011

Questions



http://standards.ieee.org/develop/indconn/icsg