Stealing secrets

The attackers view

Yaniv Miron, Security Researcher, IL Hack

July 2010

ISACA
Trust in, and value from, information systems
האיגוד הישראלי
לביקורת ואבטחת מערכות מידע

/ About Me

- Yaniv Miron aka Lament
- Security Researcher and Consultant
- Found security vulnerabilities in IBM, Oracle, Microsoft and Apache products as in other products.
- CISO Certified from the Technion
- Certified Locksmith

Agenda

- Steganography
- MetaData
- Trojans / Malwares
- Encryption
- Social Engineering
- Removable Devices / External X / Laptop

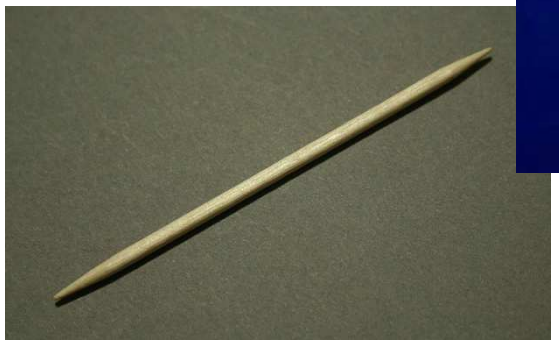
Steganography

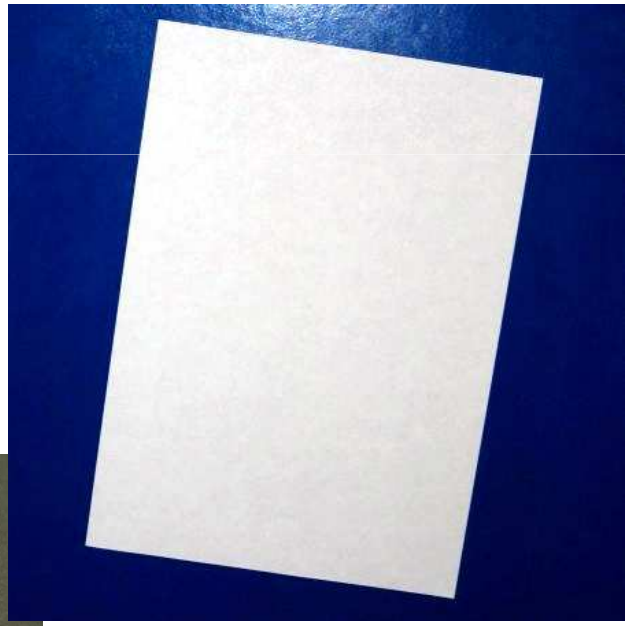
- Steganography
  - The word steganography is of Greek origin and means " ".

Steganography cont.

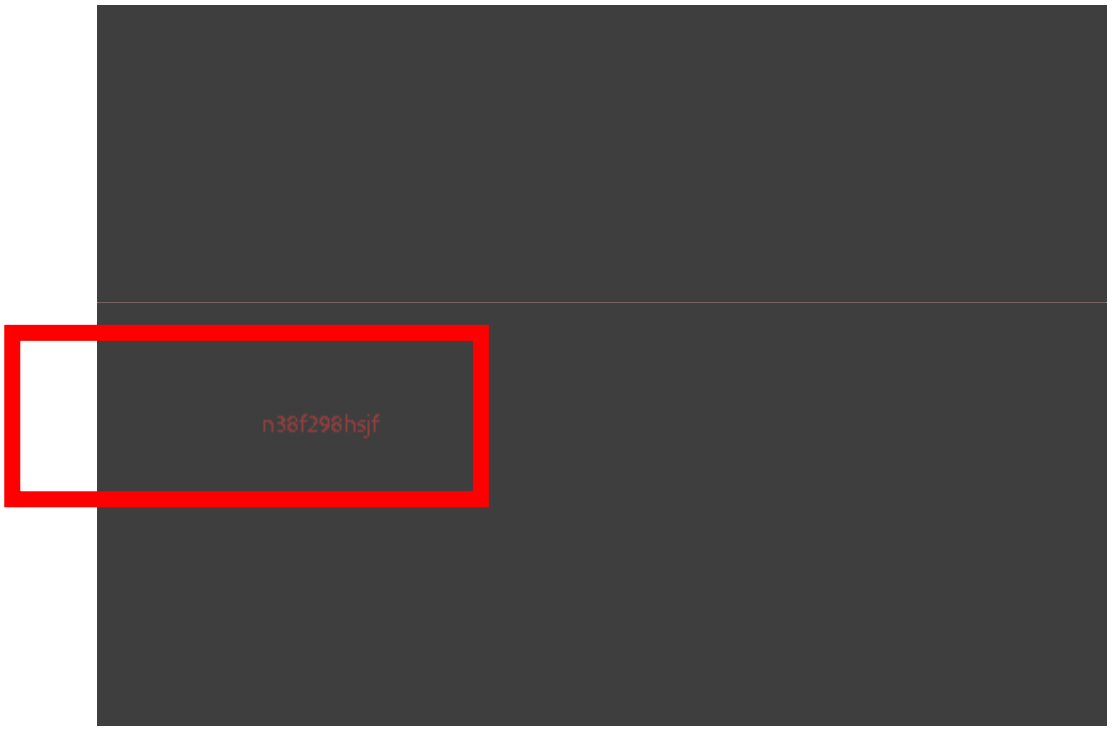
- Steganography
  - The word steganography is of Greek origin and means "concealed writing".

Steganography cont.





Steganography cont.



Steganography DEMO

- Image DEMO

Steganography DEMO

- Sound DEMO

MetaData

- MetaData
  - Data about data

MetaData, Example

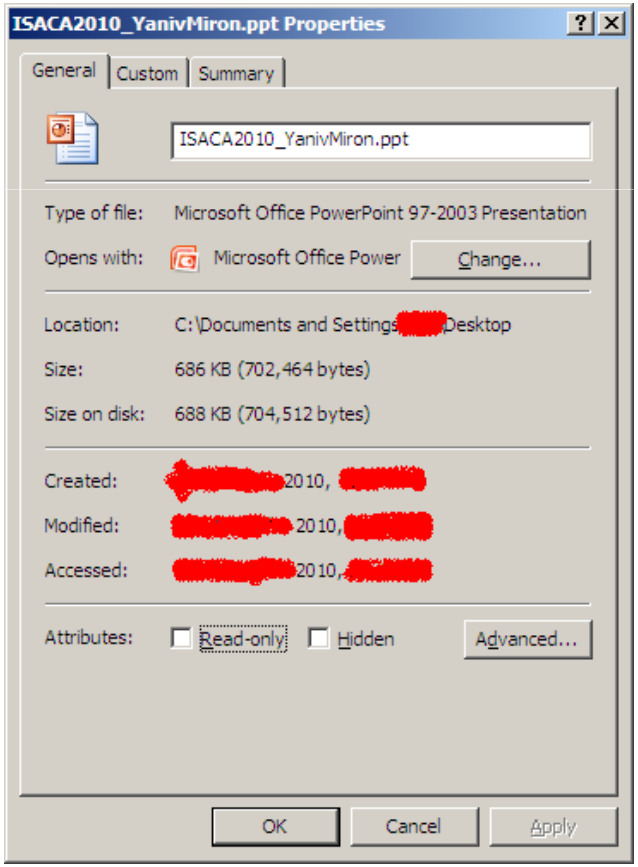
- *“Just Because You’re Paranoid Doesn’t Mean They Aren’t After You”*

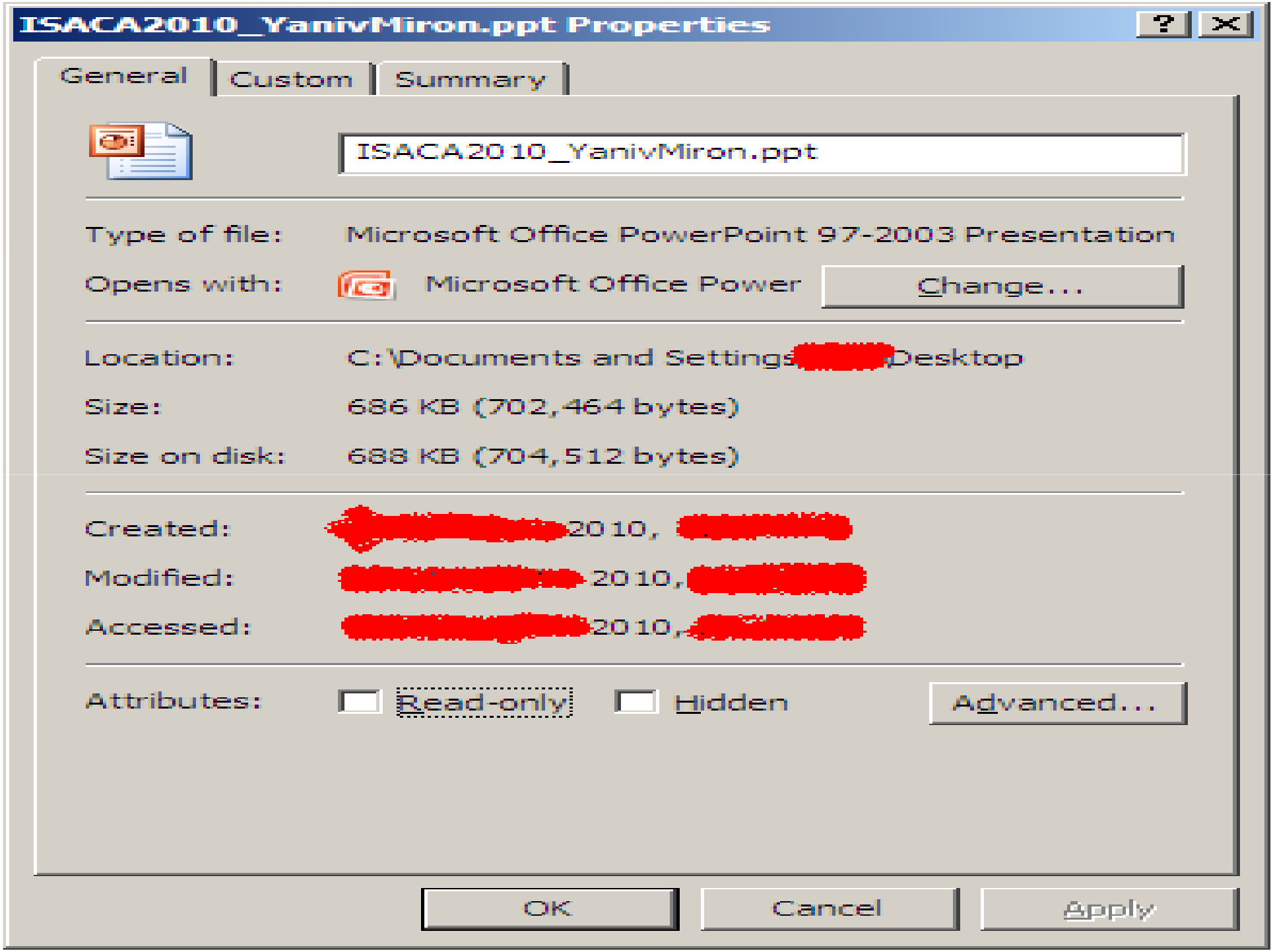
MetaData cont.

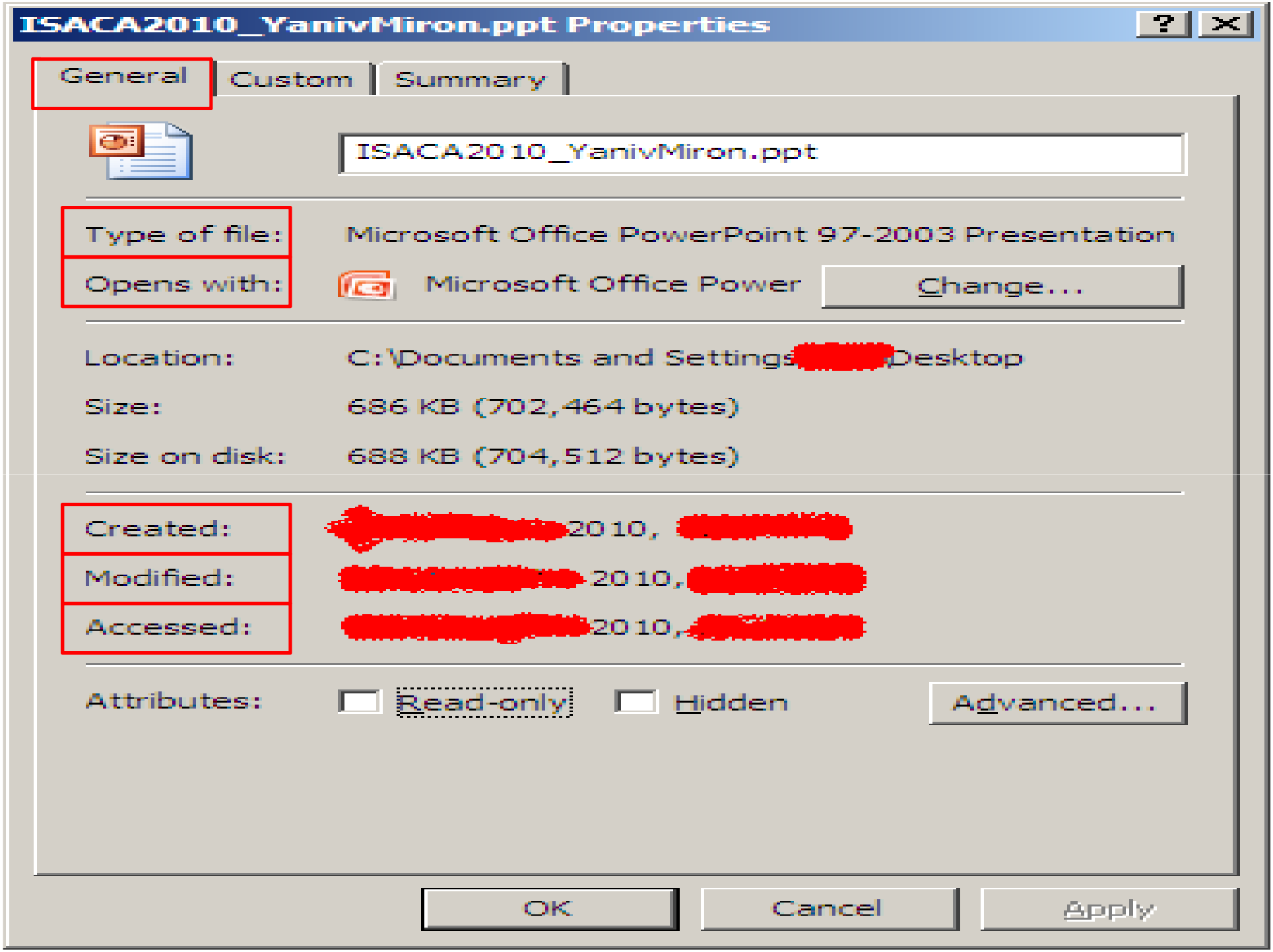
- I *__DON'T__* want you to know what I was doing, when, and if it was done me or my secretary.

MetaData cont.

- What a simple PPT file can do…

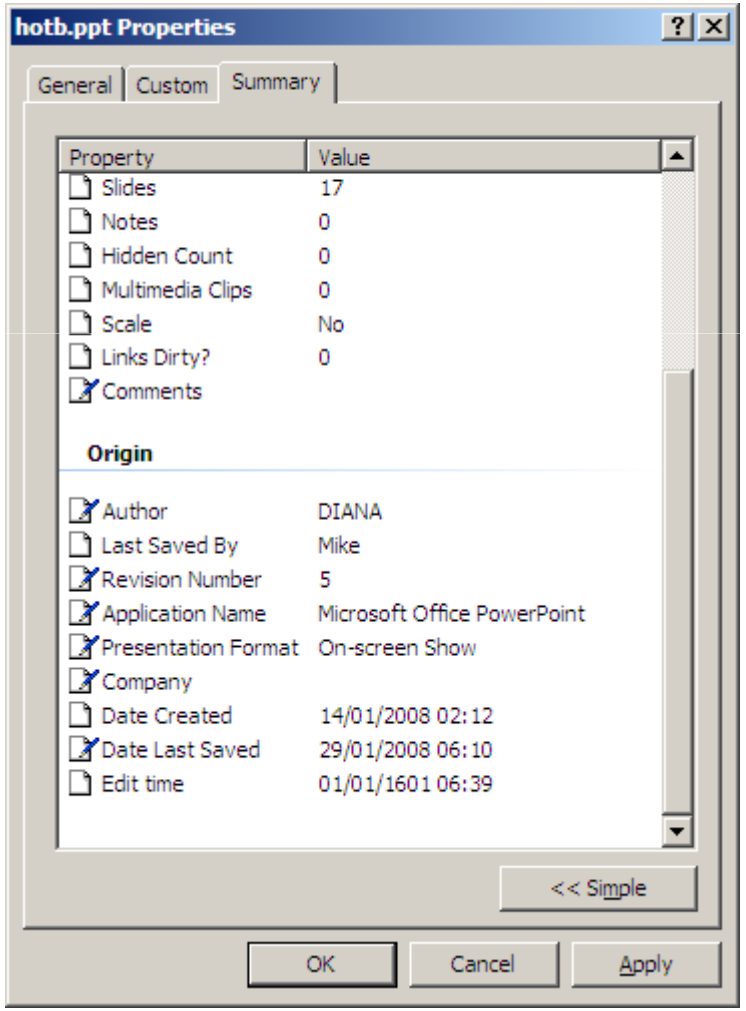


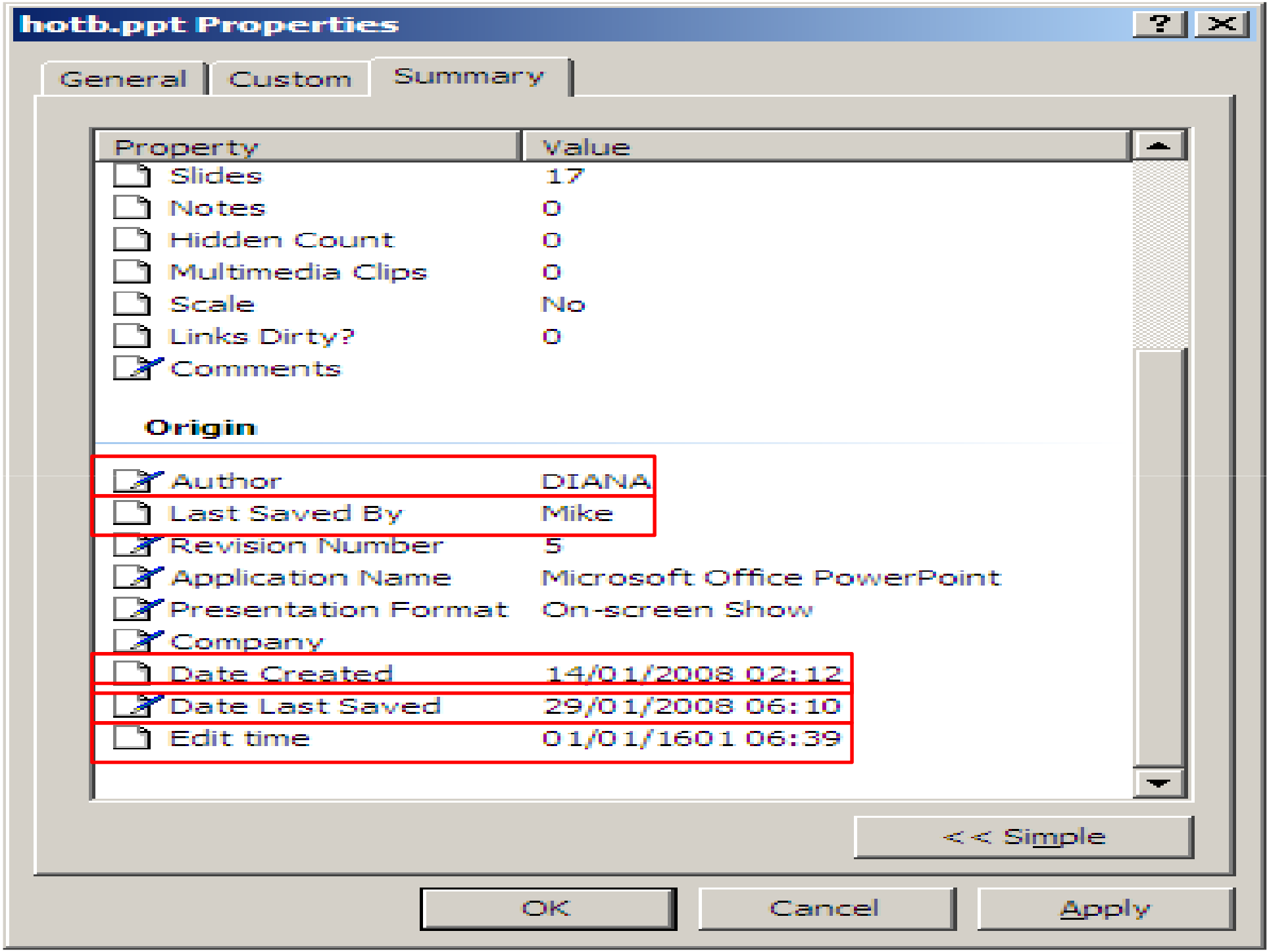

ISACA2010_YanivMiron.ppt Properties
General
Custom
Summary
ISACA2010_YanivMiron.ppt
Type of file: Microsoft Office PowerPoint 97-2003 Presentation
Opens with: Microsoft Office Power
Change...
Location: C:\Documents and Settings[redacted]\Desktop
Size: 686 KB (702,464 bytes)
Size on disk: 688 KB (704,512 bytes)
Created: [redacted] 2010, [redacted]
Modified: [redacted] 2010, [redacted]
Accessed: [redacted] 2010, [redacted]
Attributes: Read-only Hidden
Advanced...
OK
Cancel
Apply


ISACA2010_YanivMiron.ppt Properties
General
Custom
Summary
ISACA2010_YanivMiron.ppt
Type of file:
Microsoft Office PowerPoint 97-2003 Presentation
Opens with:
Microsoft Office Power
Change...
Location:
C:\Documents and Settings
Desktop
Size:
686 KB (702,464 bytes)
Size on disk:
688 KB (704,512 bytes)
Created:
2010,
Modified:
2010,
Accessed:
2010,
Attributes:
Read-only
Hidden
Advanced...
OK
Cancel
Apply

MetaData cont.

- But wait there's more…



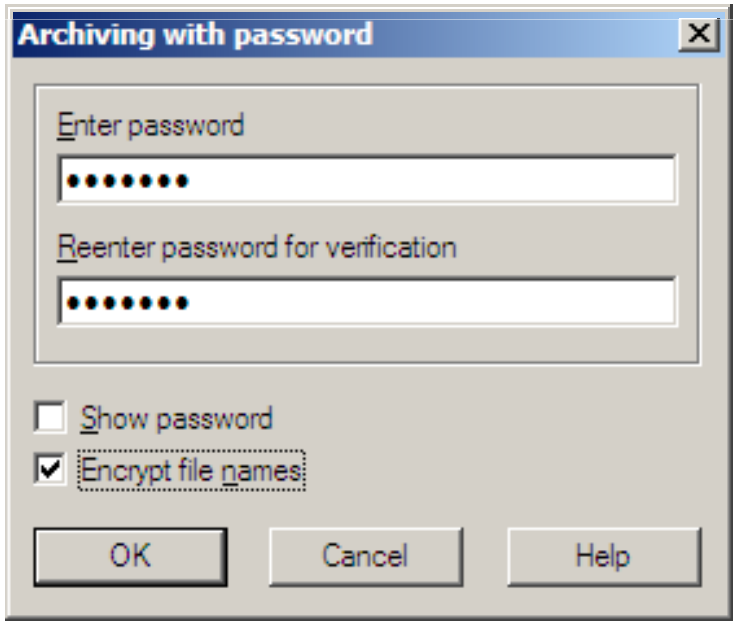

hotb.ppt Properties
General
Custom
Summary
Property
Value
Slides
17
Notes
0
Hidden Count
0
Multimedia Clips
0
Scale
No
Links Dirty?
0
Comments
Origin
Author
DIANA
Last Saved By
Mike
Revision Number
5
Application Name
Microsoft Office PowerPoint
Presentation Format
On-screen Show
Company
Date Created
14/01/2008 02:12
Date Last Saved
29/01/2008 06:10
Edit time
01/01/1601 06:39
<< Simple
OK
Cancel
Apply

Malware

- hxxp://2677.in/yahoo.js – DO NOT USE THIS LINK !!!

Encryption

- Simple RAR, ZIP
- Password protected



Social Engineering

- The files are ok, nothing to see there…
- Old fashion SE

Removable Devices / External X / Laptop

- CD
- USB
- HD
- Tokens (yes they can!)
- Laptop

E [0] F

Yaniv Miron

Security Researcher, IL Hack

lament@ilhack.org

In god we trust, all others we monitor.