Washington DC – Feb 2013

A 0-day’s life

“Offense as Defense”

Panel Discussion – Offensive Markets for Vulnerability Research – Pros and Cons

Donato Ferrante

@dntbug

[Re]Vuln

Suits & Spooks
WASHINGTON DC | FEBRUARY 8-9, 2013

Who?

- Donato Ferrante
  - donato@revuln.com
  - twitter.com/dntbug
- Co-Founder and Principal Security Researcher at ReVuln
  - revuln.com

Who?

- ReVuln Ltd.
  - 0-day and 1-day vulnerability feeds
  - SCADA/HMI security
  - Penetration testing
  - Training
  - Consulting

revuln.com

info@revuln.com

twitter.com/revuln

[Re]Vuln

What do you do?

- As ReVuln
  - We sell 0-days
  - We sell 1-days
  - We don’t buy vulnerabilities. We find them.
  - And.. **we are not evil :]**

Agenda

- **Introduction**
- Where does a 0-day come from?
- What does a 0-day do?
- How does a 0-day die?
- Conclusion

Introduction I

- When we use / We mean
  - **Bug** = a software/hardware issue
  - **0-day** = a private/non-public bug
  - **1-day** = a bug usually coming from patch analysis
  - **Exploit** = a way to use bugs

Introduction II

- A quick tour through the life of a 0-day
- We will cover just some aspects of 0-days and exploits
- We will discuss a way to use offense as defense
- **Goal**: generate a discussion (and questions)

Agenda

- Introduction
- **Where does a 0-day come from?**
- What does a 0-day do?
- How does a 0-day die?
- Conclusion

Where does a 0-day come from?

- Vulnerability research
  - **Fuzzing**, easy way but they tend to die sooner
    - Everybody is fuzzing..
    - *(Usually) Not a good investment*
  - **Code review**, medium way
    - *(Usually) A good investment*
  - **Reversing**, hard way but they usually last longer
    - *(Usually) A good investment*

Where does a 0-day come from?

- Malware analysis
  - Not actually 0-days, let’s call them **0.5-days**
    - *They usually tend to die quickly*
    - *You shouldn’t invest on 0-day coming from malware analysis*
  - There are several examples of such 0-days found in the wild
    - *Mila* of *Contagiodump* found several of them in the wild
    - Exploits kits are good examples of **0.5**-day / **1**-day collections

Where does a 0-day come from?

- Exploits kits' CVE recap:
  - *2006-2009*, just a few
  - *2010-2011*, more
  - *2012*, more and more
- Exploits kits' targets:
  - Mainly *PDF*, *Flash* and *JAVA*
  - But even some *Office*..

Agenda

- Introduction
- Where did a 0-day come from?
- **What does a 0-day do?**
- How does a 0-day die?
- Conclusion

What does a 0-day do?

- Nothing per-se
- It can be used to write code
- It can be used to write patch

What does a 0-day do?

- Please be aware of an important point
- **0-day** and **exploit** are two different entities
  - 0-days refer to unpatched and undisclosed bugs
  - Exploits refer to a way of using/abusing bugs
- We should reformulate the question..
  - **What does an exploit do?**

What does an exploit do?

- It depends
- It can be a simple proof-of-concept
- It can be something more complex
- … it depends on the "user"
- **From now on, exploits are not meant as proof-of-concepts**

What does an exploit do?

- Several usages
- Testing
  - *As proof-of-concept*
- Attack
  - *Well known*
- Defense
  - **Wait!**

What does an exploit do?

- **Question**: should you use **exploits** for defense?

What does an exploit do?

- **Question**: should you use **0-days** for defense?

What does an exploit do?

- **Concept**: using exploits for defense (*signatures*)

What does an exploit do?

- **Concept**: using exploits for defense (*signatures*)
- Why is this sentence wrong?

What does an exploit do?

- **Concept**: using exploits for defense (*signatures*)
- To write signatures for *AV/IDS/IPS/etc.* you don't actually need a fully working *ASLR-DEP-bypass* exploit
- You **just** need a simple **proof-of-concept**

What does an exploit do?

- **Concept**: using exploits for defense (*signatures*)
- What happens if you write your detections on the "**techniques**" used instead of the actual problem?
  - Let's reason on this question..

What does an exploit do?

- *1* bug = *n* exploits
- Given *2* exploits (E_1, E_2) for the same bug
  - E_1 does *ROP*, E_2 doesn't
  - E_1 uses a *local* payload, E_2 uses a *remote* payload
- They are obviously different exploits
- But they do exploit the same bug

What does an exploit do?

- ~~**Concept**: using exploits for defense (*signatures*)~~
- If a Company works on defense-solutions (*IPS/AV/etc*):
  - It doesn't usually need the exploit (*DEP-ASLR-bypass one..*)
  - It needs the 0-day
    - Info
    - Proof-of-concept
- **Concept**: using 0-days for defense (*signatures*)

What does an exploit do?

- Is there any way to use exploits for “**offensive**” defense?
  - Any ideas?

What does an exploit do?

- Is there any way to use exploits for "**offensive**" defense?
  - Any ideas?
    - **HINT**: don't think about penetration-testing

What does an exploit do?

- Is there any way to use exploits for “**offensive**” defense?
  - **Yes. Data exfiltration / Attribution.**

What does an exploit do?

- **Data exfiltration** (exfil)
  - Data exfiltration, also called data extrusion, is the unauthorized transfer of data from a computer.
  - **Key points:**
    - Privacy
    - Confidentiality
    - Intellectual Property
    - Etc..

What does an exploit do?

- **Attribution**
  - Attribution, detecting an enemy’s fingerprints on a cyber-attack
  - **Key points:**
    - Counter-intelligence
    - Fingerprints
    - Etc..

What does an exploit do?

- **Problem**, case of study **assumptions**
  - Target data: big files (*i.e. .doc / .xls / .pdf*)
  - Computer compromised
    - Smart way, so no trivial hooks on APIs etc
    - Let's say in a smart and professional way
  - Network compromised
    - Not sure if the traffic you see is the real one

What does an exploit do?

- **Problem**, case of study **goals**
  - Be able to spot exfil events
  - Be able to (*reasonably*) detect the attacker’s identity

What does an exploit do?

- **Exfil/Attribution problems**, possible solution
  - Any ideas?

What does an exploit do?

- **Exfil/Attribution problems**, possible solution
  - Write a "*call-back-home*" exploit, able to..
    - Gather *fingerprints* (*locations, docs, etc.*)
  - Deploy the exploit in **your** sensitive documents
    - Don't need to use fake documents, they recognize them
    - Welcome **Exploit-based "watermarking"**
  - Wait for a "*call*"..

What does an exploit do?

- **Exploit-based watermarking**
  - Use **exploits** as a sort of "watermark", **for your defense**
  - A way to *counter-attack* or better…
  - If you prefer ***Counter-intelligence***

What does an exploit do?

- **Exploit-based watermarking** considerations
  - It can be *expensive*, if you use *0-days*
  - It can be *cheaper*, if you use *1-days*
  - But, money-wise you are very likely to get your return…

What does an exploit do?

- **Exploit-based watermarking** considerations
    - At some point the exfil'ed document will be opened in a wrong place
        - *i.e.* not inside a VM without network connections..
    - **Why? Attackers are humans too, at some point they will fail**
    - And especially …

What does an exploit do?

- **Exploit-based watermarking** considerations
  - Technical people “**can’t read**” the documents they get
  - So a **non-technical** person will have to access the documents
    - i.e. a person **knowledgeable in the topic** of the exfil’ed documents
  - Non-technical person ~ 99% fail rate
    - Using non-updated software versions
    - Using “popular” software
    - Having almost no knowledge about security
    - Etc.

Agenda

- Introduction
- Where does a 0-day come from?
- What does a 0-day do?
- **How does a 0-day die?**
- Conclusion

How does a 0-day die?

- 0-days don’t like to go public
  - Mailing lists
  - Mail to vendors
  - Etc.
- 0-days tend to approach death
  - *Because of possible detections, when used in*
    - Exploits
    - Malware

How does a 0-day die?

- Why do people like killing bugs?
  - They don't like animals
  - They work for vendors
  - Fame
  - Fun
  - **Money?**

How does a 0-day die?

- Money?
  - This is an interesting point
  - Vendors usually pay for 0-days via bug-bounty programs
    - (*Usually*) A way to “underpay” researchers **valuable work**
    - **A bug reported to the vendor is a dead bug**
    - A 1-time only sale
    - The points above should be kept in consideration while defining the rewards for bug-bounty programs

Agenda

- Introduction
- Where does a 0-day come from?
- What does a 0-day do?
- How does a 0-day die?
- Conclusion

Conclusion

- **Exploits** are for offense
  - You don’t need exploits for defense
  - As long as defense doesn’t mean “offensive” defense
- **0-days** are for both: defense and offense
  - They give you ways to detect possible exploits
  - They give you the info to write exploits
- Think at least **100** times before killing a bug **:]**

Thanks! Questions?

- Donato Ferrante
- donato@revuln.com
- twitter.com/dntbug

Invincibility lies in the defense,
the possibility of victory in the attack.

[Re]Vuln

revuln.com
info@revuln.com twitter.com/revuln