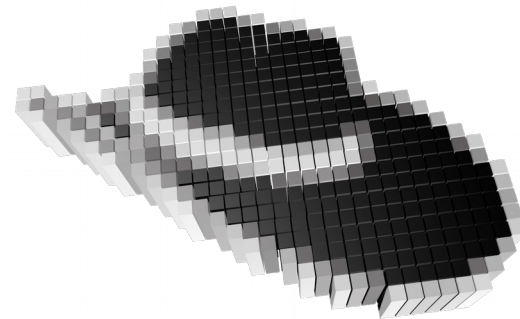


---

why today's security  
researchers cannot just  
publish vulnerabilities

---



# About me – Noam Rathaus

---

- I have been working in the security field since the age of 13 (yes I'm old...)
- Wrote 4 books on Penetration Testing and Fuzzing
- Found over 40 vulnerabilities in various types of software
- Wrote about a third of the code of Nessus
  - when it was still Open Source
  - wrote over 500 tests out of the 1000 tests it had back then



# About Beyond Security

---

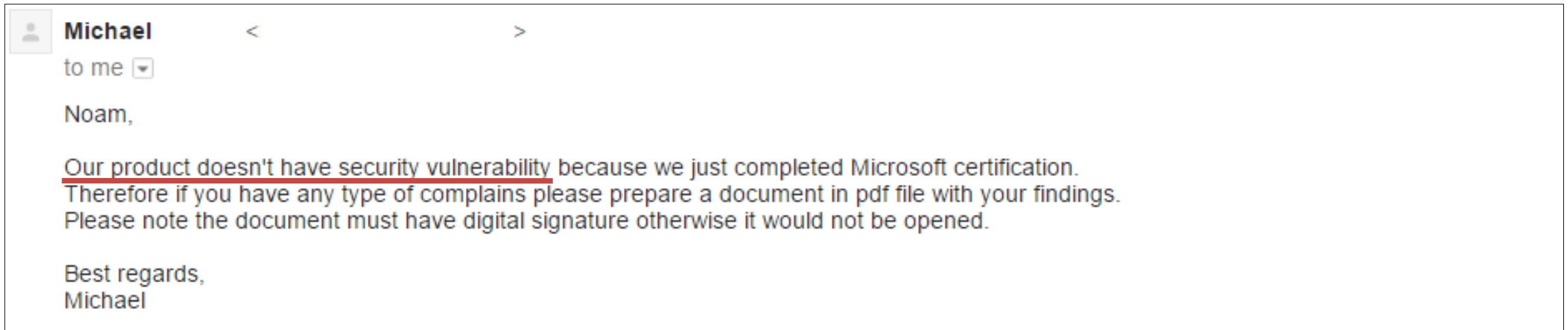
- I founded Beyond Security with my colleague Aviram Jenik
- The company today:
  - **SecuriTeam Secure Disclosure** - vulnerability acquisition program since 2007
  - **AVDS** - vulnerability management system
  - **beSTORM** - a commercial fuzzing tool



# Researcher needs to do research

---

- Researchers do not want to mess with the vendors / disclosure
  - too much hassle better things to do
- Research disclosure may backfire:





# Money



- Researcher wants to get paid for his effort
  - Days of hard work, will not lead to adequate compensation.  
A researcher wants to maximize the amount of money he gets paid for, and he needs to an expert to do this for him
- (Potential) Non-existing compensation
  - Unless you go through an agreed contract or paid research you may end up with not getting any payment

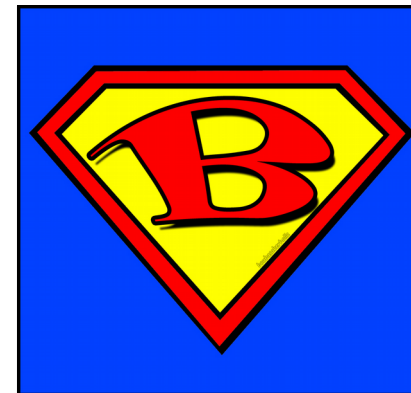
# So you found vulnerability! What should you do next?

---

- We believe you are a good person – so you probably want to disclosed it responsibly
- What are your options?



Bug bounty



Brokers



Do I need to  
say?



# Introduction

---

- There are 3 main routes to contact the vendor:
  - Email the contact information showed in the vendor website
  - Bug bounty program – if the vendor has one
  - Friends / colleagues / community
- Let's review the difficulties in the process of reporting vulnerabilities to the vendors



# Environmental factors (1)

---

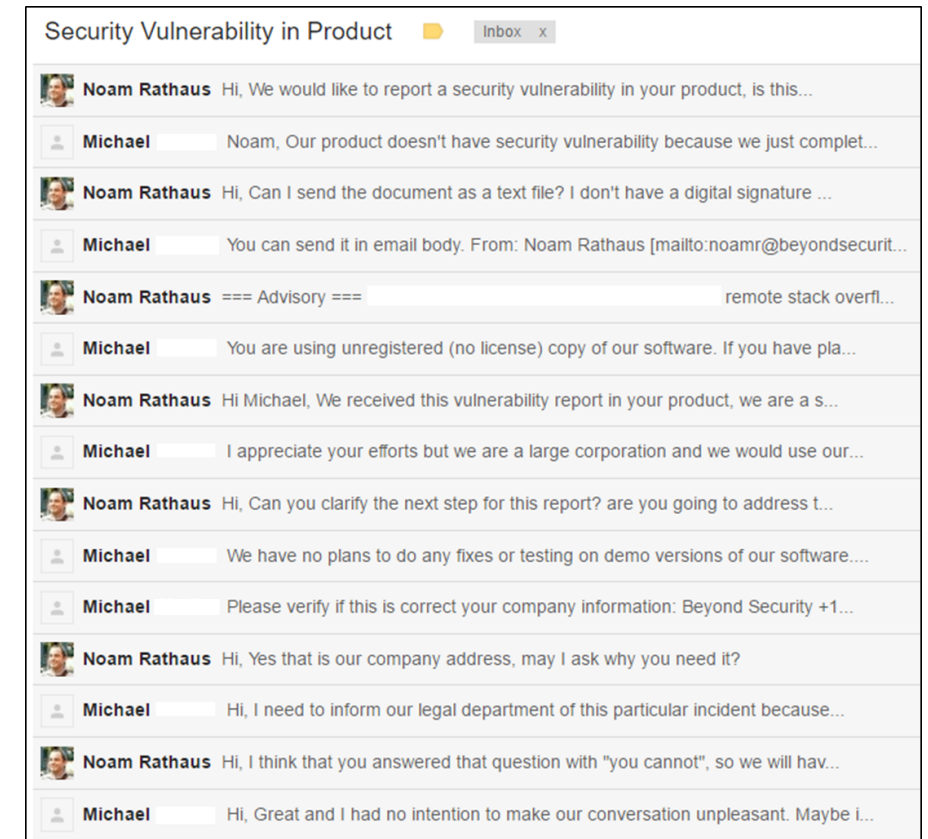


- Language is a barrier
  - Beside the obvious your language to some foreign language
  - Also Technical (researcher) to Sales (company) - in many places the sales team gets the “lead” on a new vulnerability
- Researcher may have a day job
  - It’s possible that the job would forbid him from doing this publicly, anonymity is important



# Environmental factors (2)

- Time is limited
  - You work hard on finding the vulnerabilities and you want to move on to the next item
  - Spending time talking and chasing the vendor, convincing him that he needs to fix the vulnerabilities, and waiting for him to fix them can take months



# Endless cycle (from discovery to patch)

Bug 1333618 - (CVE-2016-3737) CVE-2016-3737 JON: The agent/server communication deserializes data, and does not require authentication

Status: NEW

Aliases: CVE-2016-3737

Product: Security Response

Component: vulnerability (Show other bugs)

Version: unspecified

Hardware: All Linux

Priority urgent Severity urgent

Target Milestone: ---

Target Release: ---

Assigned To: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard: impact=critical,public=20160506,repor...

Keywords: Security

Depends On: 1333619 1333620

Reported: 2016-05-05 22:20 EDT by Jason Shepherd

Modified: 2016-08-25 00:31 EDT (History)

CC List: 6 users (show)

See Also:

Fixed In Version:

Doc Type: Bug Fix

Doc Text: It was discovered that sending specially crafted HTTP request to the JON server would allow deserialization of that message without authentication. An attacker could use this flaw to cause remote code execution.

Clone Of:

Environment:

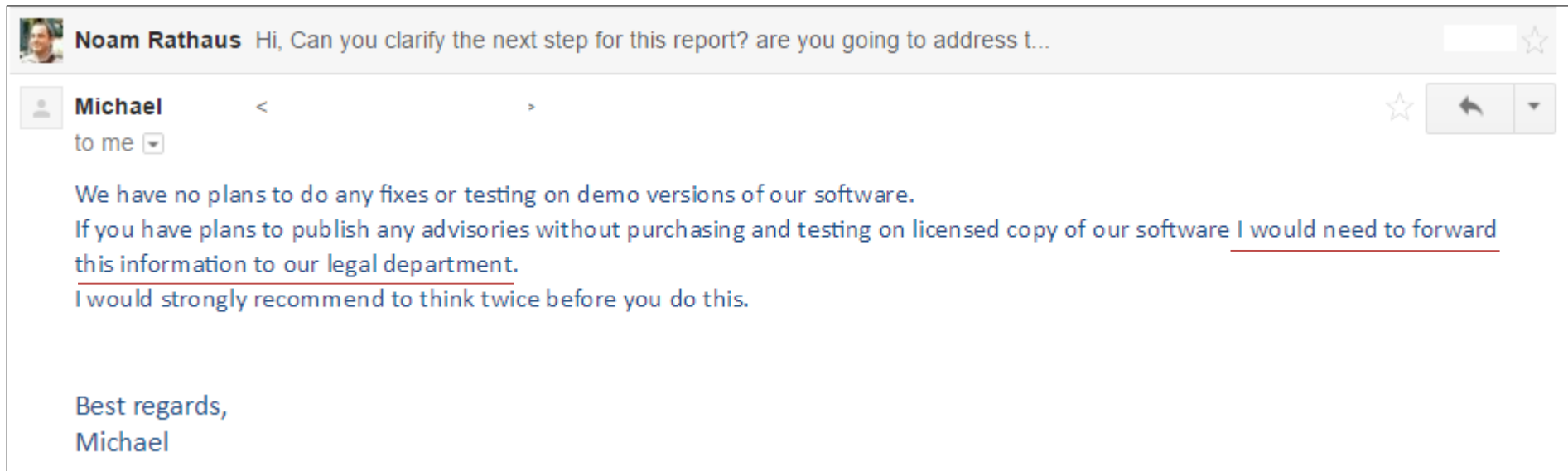
Last Closed:

3 Month from initial report to patch being released

# Bureaucracy (1)

---

- Hostile vendors
  - Want to sue you, not get the information from you





# Bureaucracy (2)

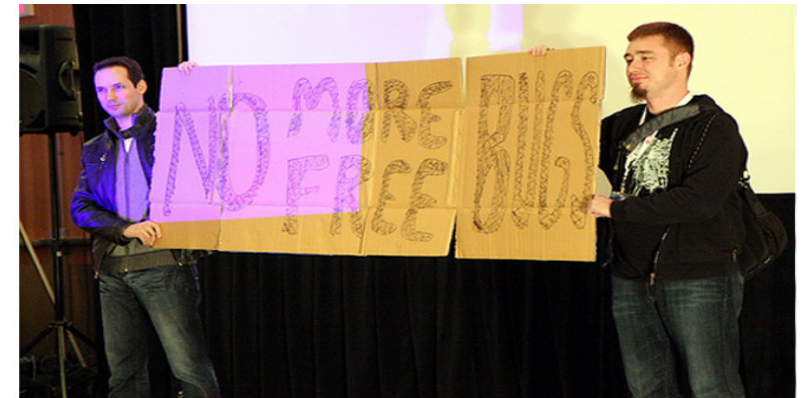
---

- Legislation
  - Privacy and computer laws may prevent the researcher from disclosing issues that affect “humans” (Real Name, Private profiles, etc)
  - Vulnerability disclosure and discovery may be illegal in the country where the researcher lives in

# Bug bounties (1)

---

- There are quite a few Bug bounty programs, however:
  - For **every company / product** - different rules and different compensation (shirt, gift card, etc)
  - You send in your discovery and hope for the best -
  - can't negotiate a price, cannot guarantee its acceptance, cannot report it to anyone else until its "rejected" (which may never happen)



# Bug bounties (2)

---

- May get unhandled or ignored – best case scenario you will get an explanation, usually nothing
- In many cases it's a “web site” not a person you are communicating with – there is no way to “escalate” it or move it forward in some way
- **In most cases you will be paid low sums of money or get a Free T-shirt!**



Francisco Alonso  
@revskills

Reported that there is now an use-after-free..  
They fixed and my reward is \$1000. (2/2)

# Conclusions

- A lot of work for a free T-shirt!
- You won't get your research published
- Time consuming



---

# Bug Bounty Platforms – evolution?



**BOUNTY  
FACTORY**.io

# Bug bounties

THURSDAY, 11 AUGUST 2016

## Reviewing bug bounties - a hacker's perspective

A prospective bug bounty hunter today has very little information on which to base his or her decision about which programs to participate in. There's a dramatic horror story every few months and that's about it. This is unfortunate because bounty hunting is founded on mutual trust; nobody wants to spend hours auditing a target only to find out that the client is disrespectful, incompetent, or likes to avoid paying out. I thought it might be helpful to write up reviews of the different bounty programs and platforms that I've dealt with.

# Introduction

---

- Bug bounty platforms try different approach to answer the problems shown above:
  - One place for the vendors to contact with the security researchers
  - “Bug bounty” program for small – medium companies (anyone can take a part)
  - Fast access for the security researcher to report the vulnerabilities
  - The security researcher can gain reputation



**KEEP  
CALM  
AND**

**PROBLEM  
SOLVE**

Is it?







bobrov posted a comment.

Hi, vulnerability is fixed

Jan 5th (2 years ago)



reidski posted a comment.

Thank you for your report, our security team has addressed the issue you raised.

Jan 7th (2 years ago)

I'd like to offer you a free t-shirt and an upgrade to Dropbox Pro account (100GB quota)! If you're interested, please email me your Dropbox login email address, phone number (for shipping), t-shirt size and mailing address.

Again, thanks!

Reid



Dropbox



evancf posted a comment.

The fix just got merged in to our staging branch. I'll let you know when it gets released.

We will probably kick off a project internally to revamp how we output that bootstrap section of the page, so I really appreciate the bug find.

We don't pay out money, but if you have an address I would love to get a tshirt sent to you, and we can upgrade your cloudflare account for a year I believe.



Aug 11th (3 months ago)

Bounty \$2,000

Collapse

SUMMARY BY SLACK



@secalert discovered an information disclosure on our server which took advantage of an authorization error that allowed the viewing of sensitive information on the server. We mitigated the issue and no longer expose such information, and performed an investigation to verify that no unauthorized access had occurred. Thank you @secalert!



---

## ManageEngine Asset Explorer Agent - Remote Code Execution as SYSTEM

---

So I'm annoyed with these guys, 6 months later and no fixes despite several product releases and updates, `aeagent.exe` has been changed, but it doesn't fix anything, the `ZohoMeeting.exe` hasn't been changed at all and has the same MD5 as before.

They have a Bug Bounty program, but only want to pay for XSS vulnerabilities, my name should be here: <https://www.zoho.com/security/hall-of-fame.html> - but I am no good with Burp and Firebug... maybe if I made this trigger XSS on one of their sites they'd do something about it.

### Usage

---

Ports 9000 and 10443 must be accessible on the target machine for the exploit to work. We provide an example shellcode which calls `ShellExecuteA` and then `exit()` and allows you to pass the command to execute as an argument to the script.

To launch Calculator on 192.168.203.100, use:



[ - ] [blufferoverthrow](#) [ S ] 2 points 13 hours ago\*

Author here, sorry about the shitty writeup.

Bug Bounties promote good intentions, they create a direct feedback loop between the project manager, software authors, the customer and the researcher. The problem comes when Bug Bounties are in name only, they are supposed to attribute cost to a software flaw and provide an impetus for correcting that.

But what happens when the system is broken, when the Bug Bounty is a marketing exercise, when companies do 'Teh Trendy Thing' and espouse an open security policy but don't put any weight behind it?

The worst I expect from a bug bounty program is for our labour to be ripped off, they take our time, use it to improve their products, and deny us the goods. The problem is when they take our time, don't improve their products, and deny themselves the goods... That's corporate dysfunction folks, welcome to the real-world.

After many months of prodding they finally got in touch with us via LinkedIn:

# Reality (1)

---

- The bug bounty platforms did some good things
  - The rules in each bug bounty program are published
  - You contact the security team directly
  - All the vendors in one place
  - You gain reputation (kindof...)



# Reality – The downside (1)

---

- There is no negotiation
  - you report your vulnerability and hope for the best
  - Most of the vendors don't pay – a free T-shirt / few hundreds dollars
  - The platform does not enforce the amount of money a vendor needs to pay for the researcher

# Reality – The downside (2)

---

Reputation - Most of the reported vulnerabilities do not get published

- through vendor advisory
- The researcher still needs to be in contact with the vendor
  - Time consuming
  - Miss understanding





# Conclusions

---

- Bug bounty programs are a step in the evolution but not the solution
- As long there is no third party reviewing the vulnerabilities and determined how much they worth – the bug bounty programs will remain “a nice thing to have”

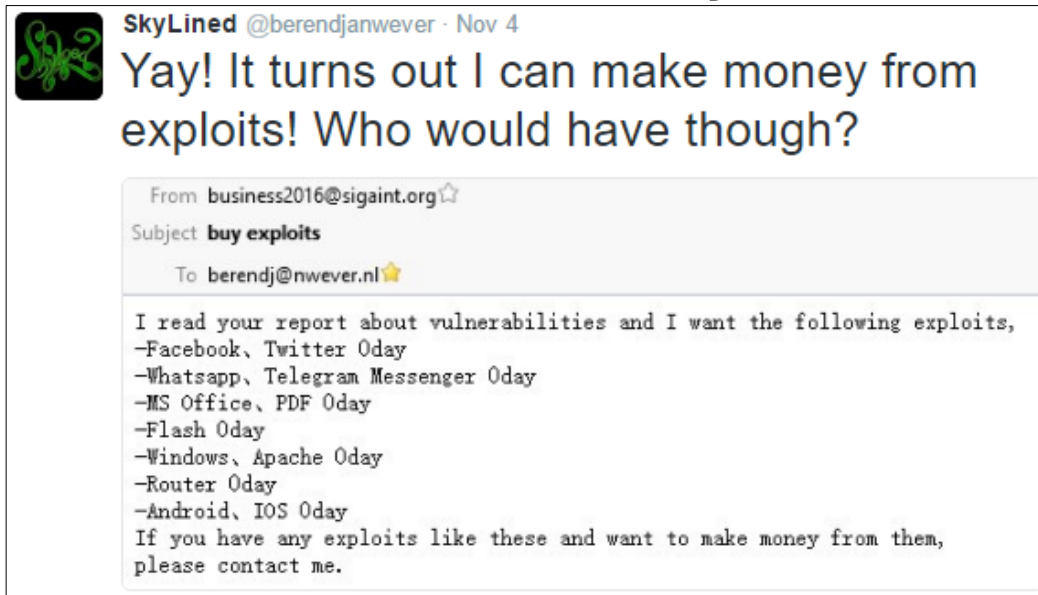
---

# The Dark Side



# Shady Business

- The business of paid vulnerability disclosure has become a hot subject over the years, this has brought much improvement but also a lot of shady stuff



**SkyLined** @berendjanwever · Nov 4

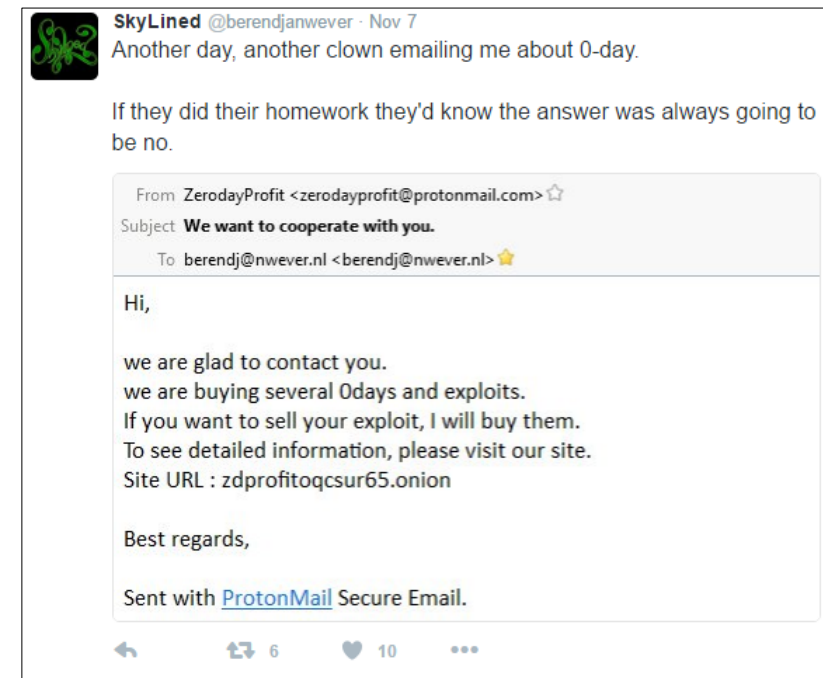
Yay! It turns out I can make money from exploits! Who would have though?

From [business2016@sigaint.org](mailto:business2016@sigaint.org) ☆

Subject **buy exploits**

To [berendj@nwever.nl](mailto:berendj@nwever.nl) 🌟

I read your report about vulnerabilities and I want the following exploits,  
-Facebook, Twitter Oday  
-Whatsapp, Telegram Messenger Oday  
-MS Office, PDF Oday  
-Flash Oday  
-Windows, Apache Oday  
-Router Oday  
-Android, IOS Oday  
If you have any exploits like these and want to make money from them, please contact me.



**SkyLined** @berendjanwever · Nov 7

Another day, another clown emailing me about 0-day.

If they did their homework they'd know the answer was always going to be no.

From [ZerodayProfit <zerodayprofit@protonmail.com>](mailto:ZerodayProfit <zerodayprofit@protonmail.com>) ☆

Subject **We want to cooperate with you.**

To [berendj@nwever.nl](mailto:berendj@nwever.nl) <[berendj@nwever.nl](mailto:berendj@nwever.nl)> 🌟

Hi,

we are glad to contact you.  
we are buying several Odays and exploits.  
If you want to sell your exploit, I will buy them.  
To see detailed information, please visit our site.  
Site URL : [zdprofitoqcsur65.onion](http://zdprofitoqcsur65.onion)

Best regards,

Sent with [ProtonMail](#) Secure Email.

🔄 6 ❤️ 10

---

# So what do we do?





(1)

---

- Guaranteed payment – escrow process
- Quick response (within 24 hours)
- A human person that can
  - Answer your questions and give you advise
  - Help you negotiate with on all aspects, price, details, scope, vulnerability type, etc **before** you send in your research material – giving you the control



(2)

- Different ways to get paid - Bitcoin, PayPal, Wire transfer and of course Victoria's Secret gift cards
- A system where you get more than "just" money
  - Free training and courses
  - Free conference access
  - Software and hardware to help you with your research or your next target



# Summary

---

- As you can see there are many problems and pitfalls in the path of disclosure and paid vulnerability researcher
- Use this presentation as a reference guide to what to expect, what to “fight” over, and most importantly on how to make the most out of it



# Or let us do this for you

---



**SSD – SecuriTeam Secure Disclosure**



**@SecuriTeam\_SSD**  
**@beyondsecurity**



**<http://www.beyondsecurity.com/ssd>**



**SSD@beyondsecurity.com**



**<http://www.securiteam.com/>**