



# **Selling 0-days to governments and offensive security companies**

Maor Shwartz



---

## About Me

Working as a vulnerability broker (~4 years)

- Q-recon
- Beyond Security

Cyber Security / Threat Intel researcher in Insurance industry

Hobbies

- Hiking
- E-games



@malltos92



Maor@qrecon.com

---

# Agenda

- Who is this talk for?
- My Story
- Overview
- Who is selling 0-days to governments / offensive security companies?
- The process of selling 0-days
- How to sell 0-days?
- Tips for beginners



# Is this talk for you?

This is not a technical talk, this also not a deep drill down in to the brokerage world

This is meant to help researchers who are new or interested in the transactional process

Share some of my experiences and a few tricks to help you along the way



# My story – **The Beginning**

Founded a vulnerability brokerage company called Q-recon

Had quite a few researchers working with me

Attained some major clients

After a few successful moves started to get attention

- Sold 0-days
- Found jobs for a few researchers



Got on a major player's radar (will not reveal the name).  
Effectively threatened in a broad daylight at a café.  
Not worth the risk, closed Q-recon

---

My Story – **The End (?)**

A grayscale background image of a business meeting. A person in a suit is seated at a desk, gesturing with their right hand. On the desk are a laptop, a glass of water, and some papers. The image is framed by two vertical blue bars on the left and right sides.

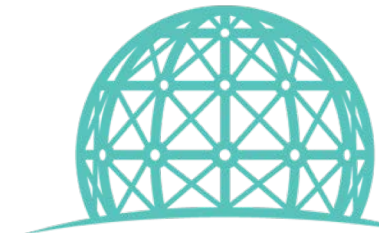
# Overview

---

# Regular Development issues

In traditional software companies:

- The problem is linear
- When the company encounters a technology problem – they hire an army of developers in order to solve that problem



# The uniqueness of vulnerabilities research

Finding vulnerabilities is an art, not a science  
(Most of the time) That's why it's a multi million  
dollars industry

You can hire a lot of vulnerability researchers,  
spend millions and find nothing



# History

In the past 5 years the 0-day market has transformed drastically

Increase in number of:

Brokerage companies

Offensive security companies

Conferences

Competitions

Bug bounty programs

Budgets

Stepping out of the shadows

(No more whispering in dark alleyways)

# Who is interested in 0-days?



Cyber security  
companies  
(defense)

Bug bounty  
programs

Bug bounty  
platform



Vulnerability  
brokers

Competitions  
Pwn2Own /  
PWNoRAMA /  
Hack2Win /  
Zer0Fest



Offensive  
Security  
Companies

Government

Criminals



**Who is buying  
what?**

# The community



Cyber security  
companies  
(defense) - PR

Bug bounty  
programs

Bug bounty  
platform



Vulnerability  
brokers

Competitions  
Pwn2Own /  
PWN0RAMA /  
Hack2Win /  
Zer0Fest



Offensive  
Security  
Companies

Government

# Vulnerability researchers – overview (HackerOne)

HackerOne  
166,000  
Registered Hackers

72,000 vulnerabilities  
submitted



70% of the reported  
vulnerabilities are focused  
on web

*What is Your Favorite Kind of Platform  
or Product to Hack?*

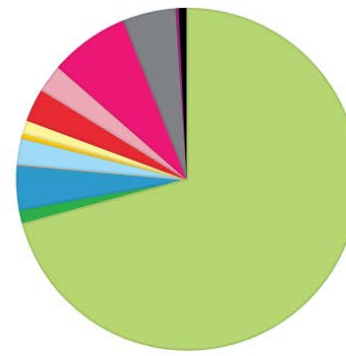
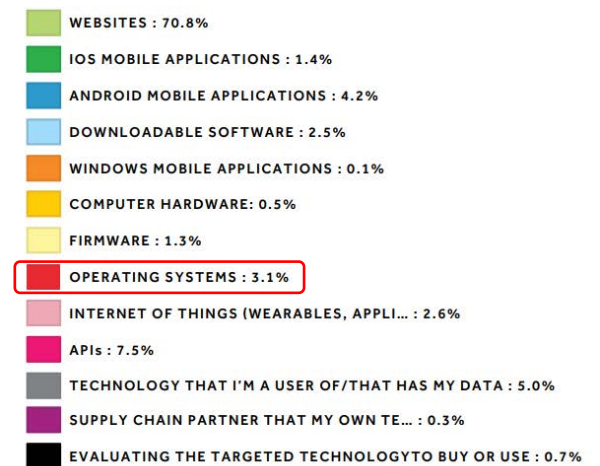
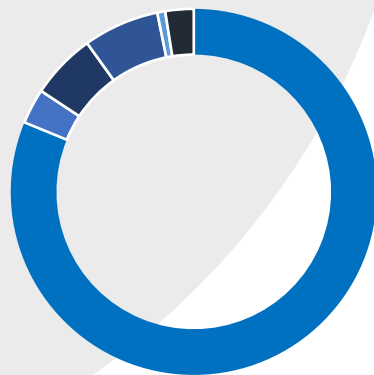


Figure 11

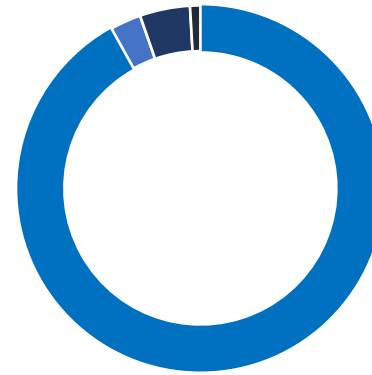


# Vulnerability researchers – overview (bugcrowd)

AMOUNT PAID BY TARGET



SUBMISSIONS PAID BY TARGET



■ WEBSITE ■ ANDROID ■ API ■ HARDWARE ■ IOS ■ IOT ■ WEBSITE ■ ANDROID ■ API ■ ■ IOT



**Cross-Site Scripting (XSS) Reflected (P3)**, was the **top vulnerability submitted this year** via the Crowdcontrol™ platform.



The majority, **13% of all submissions paid out** last year were for vulnerabilities classified as **Cross-Site Scripting (XSS) Stored**.

# There are also high-end researchers that contribute to the community

## iOS 12

Released September 17, 2018

### Accounts

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: A local app may be able to read a persistent account identifier

Description: This issue was addressed with improved entitlements.

CVE-2018-4322: Min (Spark) Zheng, Xiaolong Bai of Alibaba Inc.

### Auto Unlock

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: A malicious application may be able to access local users AppleIDs

Description: A validation issue existed in the entitlement verification. This issue was addressed with improved validation of the process entitlement.

CVE-2018-4321: Min (Spark) Zheng, Xiaolong Bai of Alibaba Inc.

Entry added September 24, 2018



P0

# Whitehats

**There are a lot of  
“vulnerability researchers”**

**Most are focused on low-  
hanging fruit**  
Quick and easy money  
Bug bounties

## **The high-end researchers:**

- (Sometimes) Ideologically motivated
- Working in Cyber security companies / research teams (PR motivated)

# Who is interested in 0-days?



Cyber security  
companies  
(defense)- PR

Bug bounty  
programs

Bug bounty  
platform



Vulnerability  
brokers

Competitions  
Pwn2Own /  
PWNoRAMA /  
Hack2Win /  
Zer0Fest

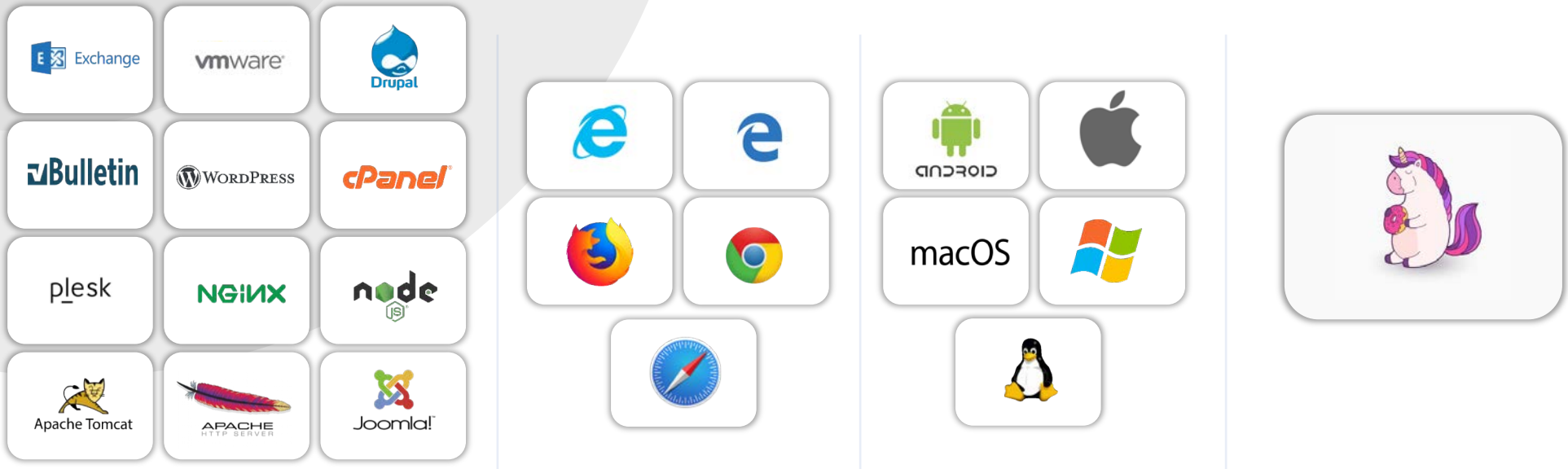


Offensive  
Security  
Companies

Government

Criminals

# The High-End Market



\*No user interaction pre-auth RCE or LPE

# The High-Rollers Table

## End-product

### Vector

- RCE + LPE + Persistence

### Vulnerabilities

- RCE | LPE | Persistence

### Component (parts in a chain)

- Info leak
- Mitigation bypass

## Services

### Dedicated research

- Freelancing

### Workshops

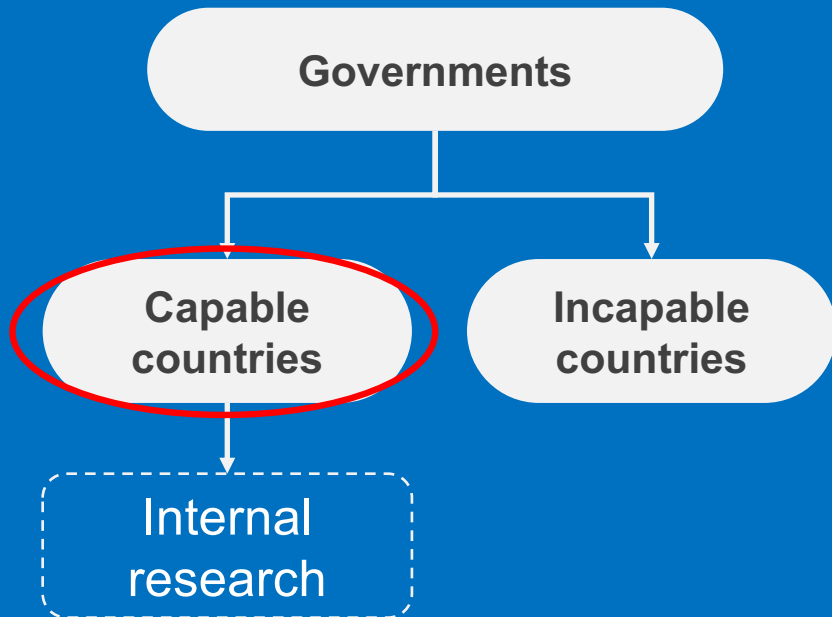
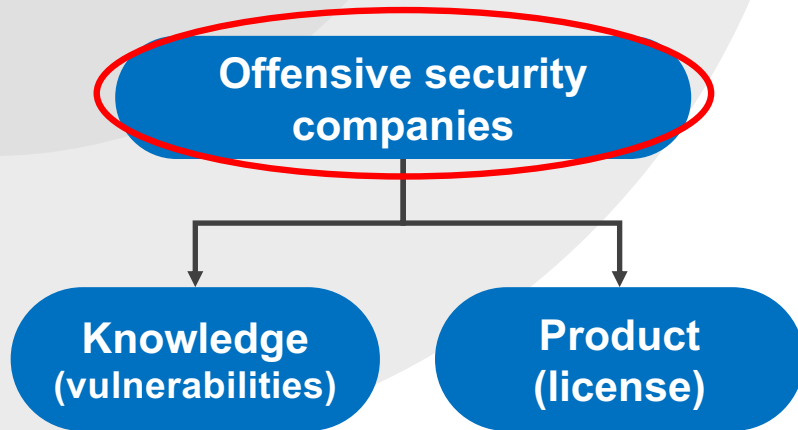
### Consulting

- Validate other researchers vulnerabilities

### Support

- Exploit new versions

# Companies vs Governments



How are they  
getting **them**  
**0-days**

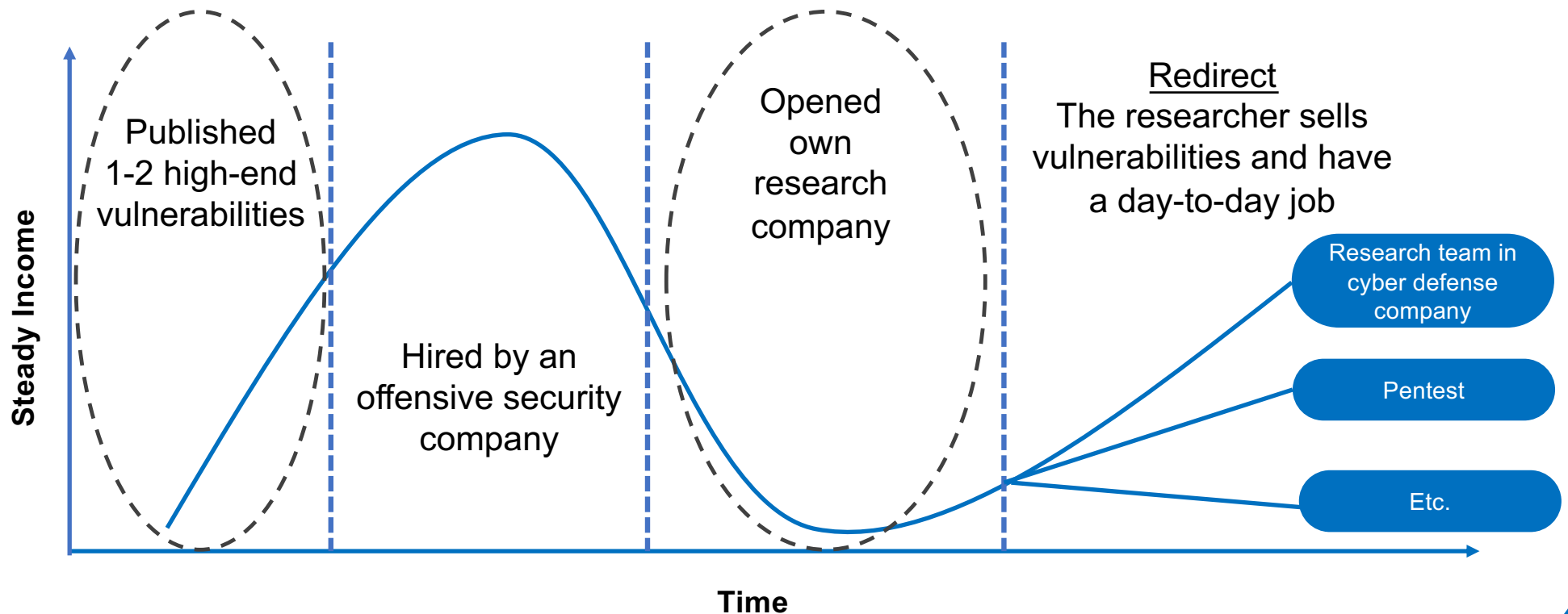


---

# Researchers by **groups**



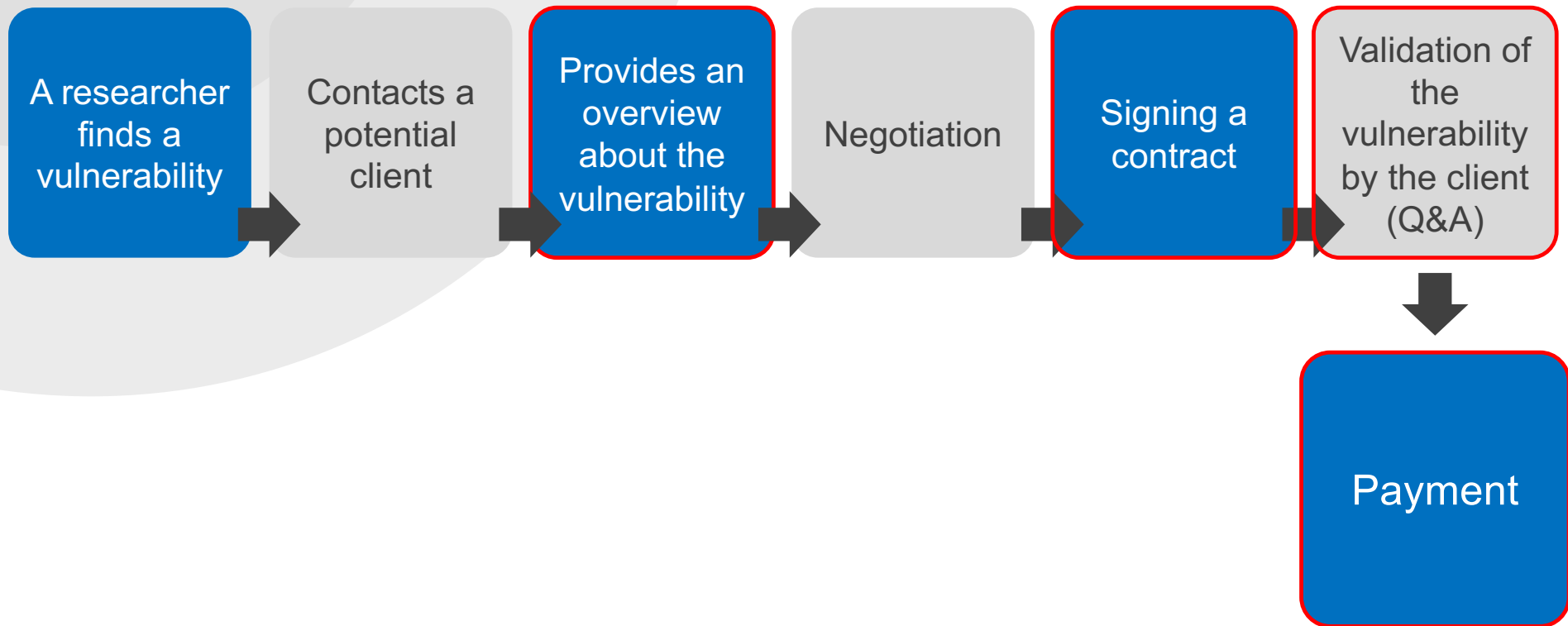
# The researcher journey





# The Process of Selling 0-days

# The sales process - overview



# Payouts

As a researcher you expect to get paid more than the vendor bug bounty program

There is no single pricelist

- Competitions (pwn2own / PWN0RAMA)
- Rumors – other researchers that sold
- Hacking Team like incidents

Zerodium transformed the optics for 0day acquisition, devil is in the details.

## ZERODIUM Payouts for Mobiles\*

ZERODIUM Payouts for Mobiles\*

RJB: Remote Jailbreak with Persistence  
RCE: Remote Code Execution  
LPE: Local Privilege Escalation  
SBX: Sandbox Escape or Bypass

IOS  
Android  
Any OS

Up to \$1,500,000											1.001 iPhone RJB Zero Click IOS
Up to \$1,000,000											1.002 iPhone RJB IOS
Up to \$500,000	2.001 WeChat RCE+LPE IOS/Android	2.002 Viber RCE+LPE IOS/Android	2.003 FB Messenger RCE+LPE IOS/Android	2.004 Signal RCE+LPE IOS/Android	2.005 Telegram RCE+LPE IOS/Android	2.006 WhatsApp RCE+LPE IOS/Android	2.007 iMessage RCE+LPE IOS	2.008 SMS/MMS RCE+LPE IOS/Android	2.009 Email App RCE+LPE IOS/Android		
Up to \$200,000	3.001 Baseband RCE+LPE IOS/Android							4.001 Chrome RCE+SBX Android	4.002 Safari RCE+SBX IOS		
Up to \$100,000	5.001 Code Signing Bypass IOS	3.002 WiFi RCE+LPE IOS/Android	2.010 Media Files RCE IOS/Android	2.011 Documents RCE IOS/Android	6.001 LPE to Kernel IOS/Android	4.003 SBX for Chrome Android	4.004 Chrome RCE w/o SBX Android	4.005 SBX for Safari IOS	4.006 Safari RCE w/o SBX IOS		
Up to \$50,000	5.002 Code Signing Bypass Android	5.003 Secure Boot IOS	3.003 RCE via MitM IOS/Android				6.002 LPE to Root IOS/Android	4.007 Chrome UXSS/SOP IOS/Android	4.008 Safari UXSS/SOP IOS		
Up to \$25,000	5.004 TrustZone Android	5.005 Verified Boot Android		6.003 LPE to System Android	7.001 ASLR Bypass IOS/Android	7.002 kASLR Bypass IOS/Android	7.003 Seccomp Bypass Android	7.004 RKP Bypass Android	7.005 Knox Bypass Android		
Up to \$15,000	8.001 Information Disclosure IOS/Android						8.001 Passcode Bypass IOS	8.002 Touch ID Bypass IOS	8.003 PIN Bypass Android		

RJB: Remote Jailbreak with Persistence  
RCE: Remote Code Execution  
LPE: Local Privilege Escalation  
SBX: Sandbox Escape or Bypass

Red: iOS  
Brown: Android  
Teal: Any OS

\*All payouts are subject to change or cancellation without notice, at the discretion of ZERODIUM. All trademarks are the property of their respective owners.

2018/09 © zerodium.com

# Payouts – behind the scenes

Different entities will offer different payouts for the same vulnerability

Warranty and Seller model matters

Complexity of  
the system

Mitigations

Supply and  
demand

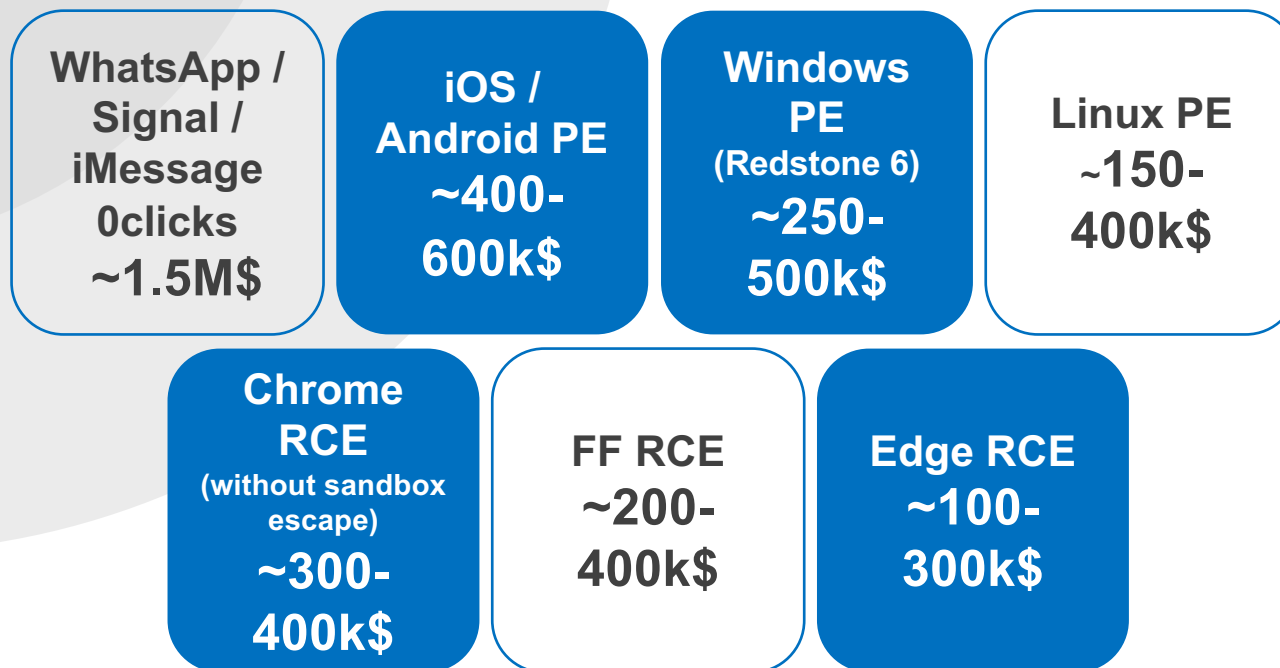
Who is the  
researcher

Deliverables

Generic

Exclusive /  
Nonexclusive

# Payouts – behind the scenes



\*Assuming high end products with ~95% reliable, ~3 seconds execution time and generic



# NOTE

---

Just because your item is worth this amount, doesn't mean there is an active or captive buyer willing to pay for it

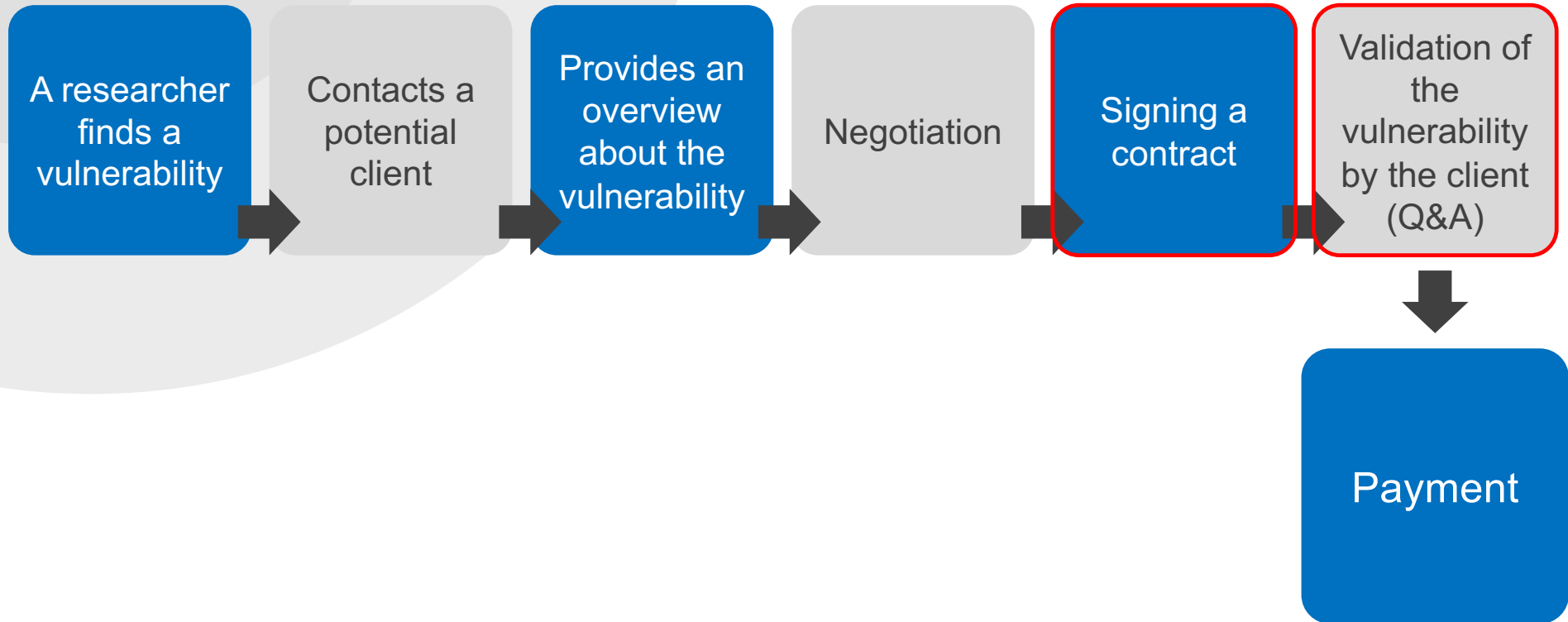
---

Market demand changes regularly

---

But the “High end vulnerabilities” are generally in “regular” demand

# The sales process - overview



The background of the slide is a solid blue color. Overlaid on this blue background is a faint, semi-transparent image of two hands shaking over a document, with a pen resting on the document. This image is positioned behind the text.

# IMPORTANT

*I DO NOT PROVIDE LEGAL  
ADVICE AND DO NOT  
CREATE AN ATTORNEY-  
CLIENT RELATIONSHIP.*

IANAL: I Am Not A Lawyer

# Legal - Contracts

Spec

Exclusive / Nonexclusive

Delivery date

Validation period

Fees & payment

SOFTWARE ACQUISITION AGREEMENT	
This Agreement describes how [redacted] (the "Seller"), will provide [redacted] and any of its affiliated companies (collectively the "Buyer") with software and documentation, which are detailed below, and how the Buyer is allowed to use the same.	
<b>1. Definitions</b>	
In this Agreement, unless inconsistent with the context or otherwise specified, the following definitions will apply:	
1.1. "Acceptance Date"	means the date on which the Software is accepted or deemed to be accepted by the Buyer pursuant to clause 4.
1.2. "Agreement"	means these terms and conditions which shall include the Specification.
1.3. "Documentation"	means the operating manuals, user instructions, and other related materials supplied to the Buyer by the Seller (whether physically or by electronic means) for aiding the use of the Software, including any part or copy of it.
1.4. "Equipment"	means any hardware equipment compatible with the Software.
1.5. "Fee"	means the fee specified in clause 6.
1.6. "Materials"	means the Software and the Documentation.
1.7. "Software"	means the computer programs as described in the Specification.
1.8. "Specification"	means the specification document describing the functions of the Software provided by the Seller to the Buyer.
1.9. "Release"	means any improved version of the Software.
1.10. "use the Software"	means to sell or distribute the Software, or load the Software into and store, run and display the Software in accordance with the terms of this Agreement.
<b>2. Sale of Software</b>	
2.1.	Subject to the terms of this Agreement and in consideration of the payment to the Seller by the Buyer of the Fee, the Seller shall sell and deliver to the Buyer the Software and Documentation.
2.2.	If and when applicable, each party will be responsible at its own expense for complying with its relevant export or import laws and regulations.
<b>3. Delivery and Installation</b>	
3.1.	The Seller will deliver one copy of the Software, in both object code and source code, and the Documentation by electronic means to the Buyer, within five (5) business days as of the execution of this Agreement.
3.2.	The Buyer is responsible for ensuring that the Equipment is installed and fully operational prior to the scheduled date for delivery of the Software.
3.3.	The Buyer is responsible for installation of the Software on the Equipment.
3.4.	The Seller will use all reasonable endeavors to achieve delivery by any specified or requested date.

Propriety rights

Confidentiality

Support

Governing law

Export liability

# Spec

Bug type

Exploit result

Vector

Affected  
architecture

Reliability

Execution time

Mitigations bypass

Supported  
versions

Product  
configuration

Deliverables

As a researcher, you guarantee the  
end result of the vulnerability on a  
pre-defined configuration

There is some acceptable variance  
with your estimates (+/- 5%)



Never claim it is more reliable or  
capable than it is, it will end badly.

## Specification

Title:

Bug type:

Exploit result:

Vecotr:

Affected architecture:

Exploit result:

Reliability:

Execution time:

Mitigation bypass:

Supported versions:

- The exploit works on the following versions:
- The vulnerability is open but not exploited on the following versions:

Process continuation:

Product configuration:

Deliverables:

# Legal - Contracts

Spec

Exclusive / Nonexclusive

Delivery date

Validation period

Fees & payment

SOFTWARE ACQUISITION AGREEMENT	
This Agreement describes how [redacted] (the "Seller"), will provide [redacted] and any of its affiliated companies (collectively the "Buyer") with software and documentation, which are detailed below, and how the Buyer is allowed to use the same.	
<b>1. Definitions</b>	
In this Agreement, unless inconsistent with the context or otherwise specified, the following definitions will apply:	
1.1. "Acceptance Date"	means the date on which the Software is accepted or deemed to be accepted by the Buyer pursuant to clause 4.
1.2. "Agreement"	means these terms and conditions which shall include the Specification.
1.3. "Documentation"	means the operating manuals, user instructions, and other related materials supplied to the Buyer by the Seller (whether physically or by electronic means) for aiding the use of the Software, including any part or copy of it.
1.4. "Equipment"	means any hardware equipment compatible with the Software.
1.5. "Fee"	means the fee specified in clause 6.
1.6. "Materials"	means the Software and the Documentation.
1.7. "Software"	means the computer programs as described in the Specification.
1.8. "Specification"	means the specification document describing the functions of the Software provided by the Seller to the Buyer.
1.9. "Release"	means any improved version of the Software.
1.10. "use the Software"	means to sell or distribute the Software, or load the Software into and store, run and display the Software in accordance with the terms of this Agreement.
<b>2. Sale of Software</b>	
2.1.	Subject to the terms of this Agreement and in consideration of the payment to the Seller by the Buyer of the Fee, the Seller shall sell and deliver to the Buyer the Software and Documentation.
2.2.	If and when applicable, each party will be responsible at its own expense for complying with its relevant export or import laws and regulations.
<b>3. Delivery and Installation</b>	
3.1.	The Seller will deliver one copy of the Software, in both object code and source code, and the Documentation by electronic means to the Buyer, within five (5) business days as of the execution of this Agreement.
3.2.	The Buyer is responsible for ensuring that the Equipment is installed and fully operational prior to the scheduled date for delivery of the Software.
3.3.	The Buyer is responsible for installation of the Software on the Equipment.
3.4.	The Seller will use all reasonable endeavors to achieve delivery by any specified or requested date.

Propriety rights

Confidentiality

Support

Governing law

Export liability

# Validation Period

## 4. Acceptance

- 4.1. Buyer shall conduct acceptance tests of the Materials within fourteen (14) days following the delivery of the Software (the "**Acceptance Date**"). If before the expiration of the acceptance period the Buyer finds that the Materials do not conform to their Specification, Buyer may reject the Software by providing written notice with a description of the nonconformity to the Seller. In which case, the Seller, at its sole cost, will update the Materials to fix its failure to conform to the Specification and deliver revised Materials. Buyer will then be granted with additional seven (7) days to conduct additional acceptance tests.
- 4.2. If the Buyer uses the Software before acceptance under this clause, except for testing purposes in accordance with the acceptance tests, then the Software will be deemed to have been accepted on the date of such first use.
- 4.3. If the Buyer rejects the Software after the acceptance tests the Buyer agrees to cease all use of the Software and Materials and will promptly destroy all copies of the Software and Materials in its possession or control.

Make sure you get access to the client test environment

Where possible, consider having a VM image ready in case you need to ship the working state PoC

Ensure buyer is prepared to test the item before sending – avoid anxiety

Usually 14 days

If the client has questions  
– there is an extension of  
up to 7 days  
(Total of 21 days)

During the validation  
period, the client can  
decline the vulnerability if  
it doesn't comply to the  
Spec

# Legal - Contracts

Spec

Exclusive / Nonexclusive

Delivery date

Validation period

Fees & payment

SOFTWARE ACQUISITION AGREEMENT	
This Agreement describes how [redacted] (the "Seller"), will provide [redacted] and any of its affiliated companies (collectively the "Buyer") with software and documentation, which are detailed below, and how the Buyer is allowed to use the same.	
<b>1. Definitions</b>	
In this Agreement, unless inconsistent with the context or otherwise specified, the following definitions will apply:	
1.1. "Acceptance Date"	means the date on which the Software is accepted or deemed to be accepted by the Buyer pursuant to clause 4.
1.2. "Agreement"	means these terms and conditions which shall include the Specification.
1.3. "Documentation"	means the operating manuals, user instructions, and other related materials supplied to the Buyer by the Seller (whether physically or by electronic means) for aiding the use of the Software, including any part or copy of it.
1.4. "Equipment"	means any hardware equipment compatible with the Software.
1.5. "Fee"	means the fee specified in clause 6.
1.6. "Materials"	means the Software and the Documentation.
1.7. "Software"	means the computer programs as described in the Specification.
1.8. "Specification"	means the specification document describing the functions of the Software provided by the Seller to the Buyer.
1.9. "Release"	means any improved version of the Software.
1.10. "use the Software"	means to sell or distribute the Software, or load the Software into and store, run and display the Software in accordance with the terms of this Agreement.
<b>2. Sale of Software</b>	
2.1.	Subject to the terms of this Agreement and in consideration of the payment to the Seller by the Buyer of the Fee, the Seller shall sell and deliver to the Buyer the Software and Documentation.
2.2.	If and when applicable, each party will be responsible at its own expense for complying with its relevant export or import laws and regulations.
<b>3. Delivery and Installation</b>	
3.1.	The Seller will deliver one copy of the Software, in both object code and source code, and the Documentation by electronic means to the Buyer, within five (5) business days as of the execution of this Agreement.
3.2.	The Buyer is responsible for ensuring that the Equipment is installed and fully operational prior to the scheduled date for delivery of the Software.
3.3.	The Buyer is responsible for installation of the Software on the Equipment.
3.4.	The Seller will use all reasonable endeavors to achieve delivery by any specified or requested date.

Propriety rights

Confidentiality

Support

Governing law

Export liability

#### 4 6. Fee & Payment Terms

- 6.1. The Buyer shall pay to the Seller a total sum of [REDACTED] US dollars (USD [REDACTED]), plus VAT if applicable, as a fixed compensation for the Materials to be provided as part of this Agreement. The Fee shall be payable as follows:
- 6.1.1. an amount of [REDACTED] (USD [REDACTED]) to be paid after successful acceptance tests within seven (7) days of the Acceptance Date (the “**First Installment**”).
- 6.1.2. [REDACTED] equal monthly installments of [REDACTED] US dollars (USD [REDACTED]) each, following the date of First Installment.
- 6.2. For the avoidance of doubt, in the event where the Software becomes either (i) part of the "public domain" due to any reason other than infringement by the Buyer of its obligations under this Agreement or misuse by Buyer's customers, or (ii) inefficient due to modifications made in the relevant software, and were implemented in a subsequent release or (iii) otherwise compromised or not functional, in whole or in part, then any remaining payment obligations of the Buyer hereunder at such time, shall be cancelled and no longer due to the Seller unless the Seller updates the Materials to fix its failure to conform to the Specification and delivers revised Materials.
- 6.3. The Buyer will pay to the Seller the Fee which fall due under this Agreement in the amounts and at the times specified in clause 6, against a duly issued invoice. The Buyer will deduct any withholding taxes as required by law unless Seller will present an exemption from such withholding taxes.

# Fees & Payment

## THERE IS NO SUCH THING AS ADVANCED PAYMENT

- Split the risk approach
- 100% on validation usually below 100k
- VAT (if applicable)
- Cryptocurrency VS Fiat
- Remember - if the transaction will be in USD (standard pricing), you should have a USD account

# Legal - Contracts

Spec

Exclusive / Nonexclusive

Delivery date

Validation period

Fees & payment

SOFTWARE ACQUISITION AGREEMENT	
This Agreement describes how [redacted] (the "Seller"), will provide [redacted] and any of its affiliated companies (collectively the "Buyer") with software and documentation, which are detailed below, and how the Buyer is allowed to use the same.	
<b>1. Definitions</b>	
In this Agreement, unless inconsistent with the context or otherwise specified, the following definitions will apply:	
1.1. "Acceptance Date"	means the date on which the Software is accepted or deemed to be accepted by the Buyer pursuant to clause 4.
1.2. "Agreement"	means these terms and conditions which shall include the Specification.
1.3. "Documentation"	means the operating manuals, user instructions, and other related materials supplied to the Buyer by the Seller (whether physically or by electronic means) for aiding the use of the Software, including any part or copy of it.
1.4. "Equipment"	means any hardware equipment compatible with the Software.
1.5. "Fee"	means the fee specified in clause 6.
1.6. "Materials"	means the Software and the Documentation.
1.7. "Software"	means the computer programs as described in the Specification.
1.8. "Specification"	means the specification document describing the functions of the Software provided by the Seller to the Buyer.
1.9. "Release"	means any improved version of the Software.
1.10. "use the Software"	means to sell or distribute the Software, or load the Software into and store, run and display the Software in accordance with the terms of this Agreement.
<b>2. Sale of Software</b>	
2.1.	Subject to the terms of this Agreement and in consideration of the payment to the Seller by the Buyer of the Fee, the Seller shall sell and deliver to the Buyer the Software and Documentation.
2.2.	If and when applicable, each party will be responsible at its own expense for complying with its relevant export or import laws and regulations.
<b>3. Delivery and Installation</b>	
3.1.	The Seller will deliver one copy of the Software, in both object code and source code, and the Documentation by electronic means to the Buyer, within five (5) business days as of the execution of this Agreement.
3.2.	The Buyer is responsible for ensuring that the Equipment is installed and fully operational prior to the scheduled date for delivery of the Software.
3.3.	The Buyer is responsible for installation of the Software on the Equipment.
3.4.	The Seller will use all reasonable endeavors to achieve delivery by any specified or requested date.

Propriety rights

Confidentiality

Support

Governing law

Export liability

# Propriety Rights

## Exclusive

Buyer acquires any and all title, copyright, or other proprietary rights

Researchers - make sure you add to the contract the ability to use your vulnerability for internal research

## Nonexclusive\*

The researcher sells a license

Can be sold multiple times

\*Non exclusive isn't as good as you may think strategically, many times its worst

# Legal - Contracts

Spec

Exclusive / Nonexclusive

Delivery date

Validation period

Fees & payment

SOFTWARE ACQUISITION AGREEMENT	
This Agreement describes how [redacted] (the "Seller"), will provide [redacted] and any of its affiliated companies (collectively the "Buyer") with software and documentation, which are detailed below, and how the Buyer is allowed to use the same.	
<b>1. Definitions</b>	
In this Agreement, unless inconsistent with the context or otherwise specified, the following definitions will apply:	
1.1. "Acceptance Date"	means the date on which the Software is accepted or deemed to be accepted by the Buyer pursuant to clause 4.
1.2. "Agreement"	means these terms and conditions which shall include the Specification.
1.3. "Documentation"	means the operating manuals, user instructions, and other related materials supplied to the Buyer by the Seller (whether physically or by electronic means) for aiding the use of the Software, including any part or copy of it.
1.4. "Equipment"	means any hardware equipment compatible with the Software.
1.5. "Fee"	means the fee specified in clause 6.
1.6. "Materials"	means the Software and the Documentation.
1.7. "Software"	means the computer programs as described in the Specification.
1.8. "Specification"	means the specification document describing the functions of the Software provided by the Seller to the Buyer.
1.9. "Release"	means any improved version of the Software.
1.10. "use the Software"	means to sell or distribute the Software, or load the Software into and store, run and display the Software in accordance with the terms of this Agreement.
<b>2. Sale of Software</b>	
2.1.	Subject to the terms of this Agreement and in consideration of the payment to the Seller by the Buyer of the Fee, the Seller shall sell and deliver to the Buyer the Software and Documentation.
2.2.	If and when applicable, each party will be responsible at its own expense for complying with its relevant export or import laws and regulations.
<b>3. Delivery and Installation</b>	
3.1.	The Seller will deliver one copy of the Software, in both object code and source code, and the Documentation by electronic means to the Buyer, within five (5) business days as of the execution of this Agreement.
3.2.	The Buyer is responsible for ensuring that the Equipment is installed and fully operational prior to the scheduled date for delivery of the Software.
3.3.	The Buyer is responsible for installation of the Software on the Equipment.
3.4.	The Seller will use all reasonable endeavors to achieve delivery by any specified or requested date.

Propriety rights

Confidentiality

Support

Governing law

Export liability




# Support

Support can take many forms:

- Exploit adjustments to:  
Product new / older versions  
New vectors
- If the vulnerability is patched, the researcher may need to provide a different vulnerability
- Provide a workshop about the vulnerability to the client

**Don't Forget – Support is worth money**

if you are going to provide technical support for your sale, make sure you get paid for it



# Legal - Contracts

Spec

Exclusive / Nonexclusive

Delivery date

Validation period

Fees & payment

SOFTWARE ACQUISITION AGREEMENT	
This Agreement describes how [redacted] (the "Seller"), will provide [redacted] and any of its affiliated companies (collectively the "Buyer") with software and documentation, which are detailed below, and how the Buyer is allowed to use the same.	
<b>1. Definitions</b>	
In this Agreement, unless inconsistent with the context or otherwise specified, the following definitions will apply:	
1.1. "Acceptance Date"	means the date on which the Software is accepted or deemed to be accepted by the Buyer pursuant to clause 4.
1.2. "Agreement"	means these terms and conditions which shall include the Specification.
1.3. "Documentation"	means the operating manuals, user instructions, and other related materials supplied to the Buyer by the Seller (whether physically or by electronic means) for aiding the use of the Software, including any part or copy of it.
1.4. "Equipment"	means any hardware equipment compatible with the Software.
1.5. "Fee"	means the fee specified in clause 6.
1.6. "Materials"	means the Software and the Documentation.
1.7. "Software"	means the computer programs as described in the Specification.
1.8. "Specification"	means the specification document describing the functions of the Software provided by the Seller to the Buyer.
1.9. "Release"	means any improved version of the Software.
1.10. "use the Software"	means to sell or distribute the Software, or load the Software into and store, run and display the Software in accordance with the terms of this Agreement.
<b>2. Sale of Software</b>	
2.1.	Subject to the terms of this Agreement and in consideration of the payment to the Seller by the Buyer of the Fee, the Seller shall sell and deliver to the Buyer the Software and Documentation.
2.2.	If and when applicable, each party will be responsible at its own expense for complying with its relevant export or import laws and regulations.
<b>3. Delivery and Installation</b>	
3.1.	The Seller will deliver one copy of the Software, in both object code and source code, and the Documentation by electronic means to the Buyer, within five (5) business days as of the execution of this Agreement.
3.2.	The Buyer is responsible for ensuring that the Equipment is installed and fully operational prior to the scheduled date for delivery of the Software.
3.3.	The Buyer is responsible for installation of the Software on the Equipment.
3.4.	The Seller will use all reasonable endeavors to achieve delivery by any specified or requested date.

Propriety rights

Confidentiality

Support

Governing law

Export liability

---

## Governing law

Be mindful of where legal disputes are handled.

Make sure you have all the licenses if something goes terribly wrong.

Are there grounds for a suit?

Work with reputable buyers, they have no incentive to take bad deals that lead to legal action. Reputation matters for both sides.

# Legal - Contracts

Spec

Exclusive / Nonexclusive

Delivery date

Validation period

Fees & payment

SOFTWARE ACQUISITION AGREEMENT	
This Agreement describes how [redacted] (the "Seller"), will provide [redacted] and any of its affiliated companies (collectively the "Buyer") with software and documentation, which are detailed below, and how the Buyer is allowed to use the same.	
<b>1. Definitions</b>	
In this Agreement, unless inconsistent with the context or otherwise specified, the following definitions will apply:	
1.1. "Acceptance Date"	means the date on which the Software is accepted or deemed to be accepted by the Buyer pursuant to clause 4.
1.2. "Agreement"	means these terms and conditions which shall include the Specification.
1.3. "Documentation"	means the operating manuals, user instructions, and other related materials supplied to the Buyer by the Seller (whether physically or by electronic means) for aiding the use of the Software, including any part or copy of it.
1.4. "Equipment"	means any hardware equipment compatible with the Software.
1.5. "Fee"	means the fee specified in clause 6.
1.6. "Materials"	means the Software and the Documentation.
1.7. "Software"	means the computer programs as described in the Specification.
1.8. "Specification"	means the specification document describing the functions of the Software provided by the Seller to the Buyer.
1.9. "Release"	means any improved version of the Software.
1.10. "use the Software"	means to sell or distribute the Software, or load the Software into and store, run and display the Software in accordance with the terms of this Agreement.
<b>2. Sale of Software</b>	
2.1.	Subject to the terms of this Agreement and in consideration of the payment to the Seller by the Buyer of the Fee, the Seller shall sell and deliver to the Buyer the Software and Documentation.
2.2.	If and when applicable, each party will be responsible at its own expense for complying with its relevant export or import laws and regulations.
<b>3. Delivery and Installation</b>	
3.1.	The Seller will deliver one copy of the Software, in both object code and source code, and the Documentation by electronic means to the Buyer, within five (5) business days as of the execution of this Agreement.
3.2.	The Buyer is responsible for ensuring that the Equipment is installed and fully operational prior to the scheduled date for delivery of the Software.
3.3.	The Buyer is responsible for installation of the Software on the Equipment.
3.4.	The Seller will use all reasonable endeavors to achieve delivery by any specified or requested date.

Propriety rights

Confidentiality

Support

Governing law

Export liability

---

# Wassenaar agreement

The **Wassenaar** agreement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a multilateral export control regime.

In simple words – In **some** countries you need an export license.

Each state legislates laws that represent the Wassenaar agreement differently.

Agreement



Law



# Wassenaar agreement

'Vulnerability disclosure' means the process of identifying, reporting, or communicating a vulnerability to, or analyzing a vulnerability with, individuals or organizations responsible for conducting or coordinating remediation for the purpose of resolving the vulnerability.

## 4. E. TECHNOLOGY

### 4. E. 1. "Technology" as follows:

- a. "Technology" according to the General Technology Note, for the "development", "production" or "use" of equipment or "software" specified by 4.A. or 4.D.
- b. "Technology" according to the General Technology Note, other than that specified by 4.E.1.a., for the "development" or "production" of equipment as follows:
  1. "Digital computers" having an 'Adjusted Peak Performance' ('APP') exceeding 15 Weighted TeraFLOPS (WT);
  2. "Electronic assemblies" specially designed or modified for enhancing performance by aggregation of processors so that the 'APP' of the aggregation exceeds the limit in 4.E.1.b.1.
- c. "Technology" for the "development" of "intrusion software".

Note 1 4.E.1.a. and 4.E.1.c. do not apply to 'vulnerability disclosure' or 'cyber incident response'.

Note 2 Note 1 does not diminish national authorities' rights to ascertain compliance with 4.E.1.a. and 4.E.1.c.

#### Technical Notes

1. 'Vulnerability disclosure' means the process of identifying, reporting, or communicating a vulnerability to, or analysing a vulnerability with, individuals or organizations responsible for conducting or coordinating remediation for the purpose of resolving the vulnerability.
2. 'Cyber incident response' means the process of exchanging necessary information on a cyber security incident with individuals or organizations responsible for conducting or coordinating remediation to address the cyber security incident.

# Export liability - Wassenaar

Report to vendor

No problem

Exporting  
(End-product / Research  
Service)

Special Marketing License

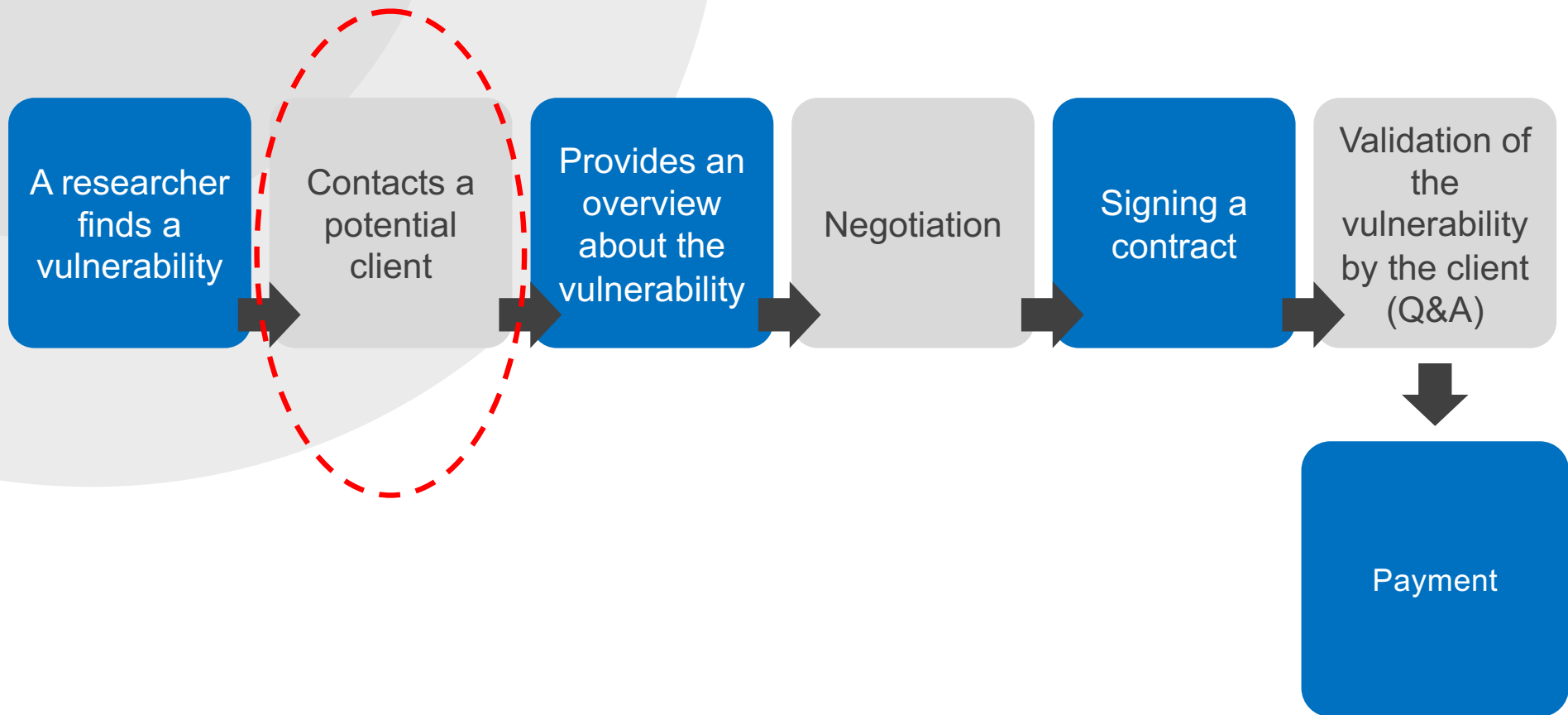
Special Selling License

Ministry Of **Defense** (MOD)

A blurred office scene. In the foreground, a man with grey hair, wearing a grey suit, is seen from the back, sitting at a wooden desk. On the desk is a laptop and a white coffee cup on a saucer. In the background, several other people are visible, some standing and some sitting, in a bright, modern office environment. The image has a semi-transparent grey overlay and is framed by two vertical blue bars on the left and right sides.

# Finding the **Customers**

# The sales process - overview



# Selling Vulnerabilities to Govs / Companies

Official point of  
contact

Vulnerability  
brokers

Personal connections  
(govs / companies)



# Official point of contact

Some governments and offensive security companies publish “official” point of contact

Conferences (business cards / emails / flyers etc.)

Direct approach (“cold email”)

As a researcher, you can email companies you think will be interested (They will probably reply)

Governments direct can be extremely time consuming



don't expect amazing terms or a timely schedule for decision making or payment



Some may be willing to engage directly unsolicited (expect significant competition)

some may be impossible to reach and need a direct relationship or introduction

# Official point of contact

Pros	Cons
The researcher knows who the client is	The client (usually) knows the researcher identity
Updated in real time on the status of the deal	Limited number of potential clients (~5)
Legal (licensing)	Legal (licensing)
	The researcher might get underpaid
	Bad Contract (The client can add limiting terms before buying)
	Multiple POCs Simultaneously - Time consuming

# Selling Vulnerabilities to Govs / Companies

Official point of  
contact

Vulnerability  
brokers

Personal connections  
(govs / companies)



# Personal connections

Pros	Cons
The researcher knows who the client is	The client (usually) knows the researcher identity
Updated in real time on the status of the deal	Limited number of potential clients (~5)
Legal (licensing)	Legal (licensing)
Full payment without worries*	The researcher might get underpaid
Trust	Bad Contract (The client can add limiting terms before buying)
	Multiple POCs Simultaneously - Time consuming

Vulnerability  
broker

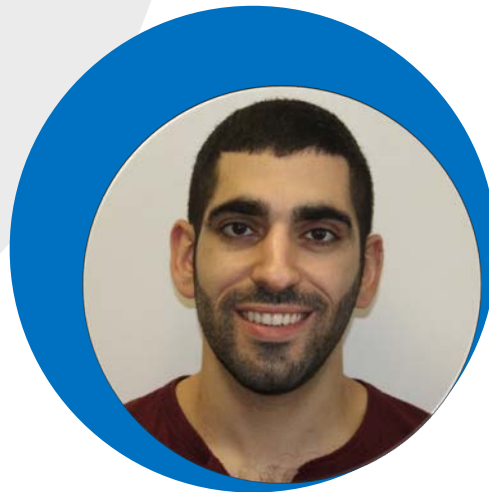


# The 0-day broker – My experiences

**Workshops**

**HR services  
(Full / part time jobs)**

**On demand projects  
(freelancers)**



**Selling end-product  
(vulnerabilities / exploits)**

**Working with other  
brokers**

**Helping clients to create  
their own ability to buy  
and sell 0-days**



# Benefits of working with brokers

Anonymity

Market  
Landscape

Close and  
intimate  
relationship with  
clients

Negotiation

Legal

Manage the  
process



# How does a broker make his money?

The broker charge the client for his services  
There are couple of models:

Broker Fee - %  
on top of the  
initial price.

Q-recon fees  
were:

- 17% from companies
- 15% from governments

Reseller - The  
broker buys the  
vulnerability from  
the researcher  
and sells it to  
couple of clients

Subscription -  
yearly or monthly  
subscription fee.

# Selling 0-days – In a nutshell

**Don't waste too much time** in the high-end market if your vulnerability isn't high quality

**Ensure** your PoC is stable and mature and always works on the latest stable

Just because your iOS Safari RCE/LPE is worth XXXX **doesn't mean there is a buyer for it**

**NEVER** oversell a vulnerability hoping it will lead to a successful transaction, **IT WILL NOT**, find better bugs

# Selling 0-days – In a nutshell

Exclusive has its pros.  
Juggling non-exclusive to  
multiple parties is both  
stressful and can easily fall  
apart



If you sell non exclusive, limit  
the expose to a few trusted  
clients

DO explain if the vulnerability  
is stable and deterministic, but  
your exploit is just sh\*t and  
can be improved  
(can save a deal)

NEVER tweet or be overt  
about a transaction, it can  
breach the contract  
confidentiality and relationship  
trust

# Selling 0-days – In a nutshell

**0days lately burn a lot faster due to p0 and such .**

Your lower offer might in fact to be the better offer if your 0day goes to 0\$

**Always listen to feedback.** If your are skilled at Edge Chakra and your broker tells you to focus on V8 you should probably consider the buyer feedback

**Sometimes transactions just don't work out, but when they do work out – it's definitely worth it**

# Selling 0-days – In a nutshell

The going rate for any vulnerability is based purely on Demand. If the market is flooded with a capability, it doesn't matter what its worth if everyone is redundant

Exclusive might seem easy to work around or later "convert" to non exclusive. DON'T, most buyers/brokers are in the same network/circles, with real deal buyer its even a smaller world. Trust is everything in this market

# Some Tips for Beginners



Don't eat yellow snow

---

# Get Some Street Cred

Play CTFs

Go to Conferences – meet researchers and potential clients

Publish 1-2 vulnerabilities (high-end)

Get help when in doubt

Know your s\*\*\* (Never “Fake it till you make it”).

Don't worry about imposter syndrome or if you're good enough, you never know until you try



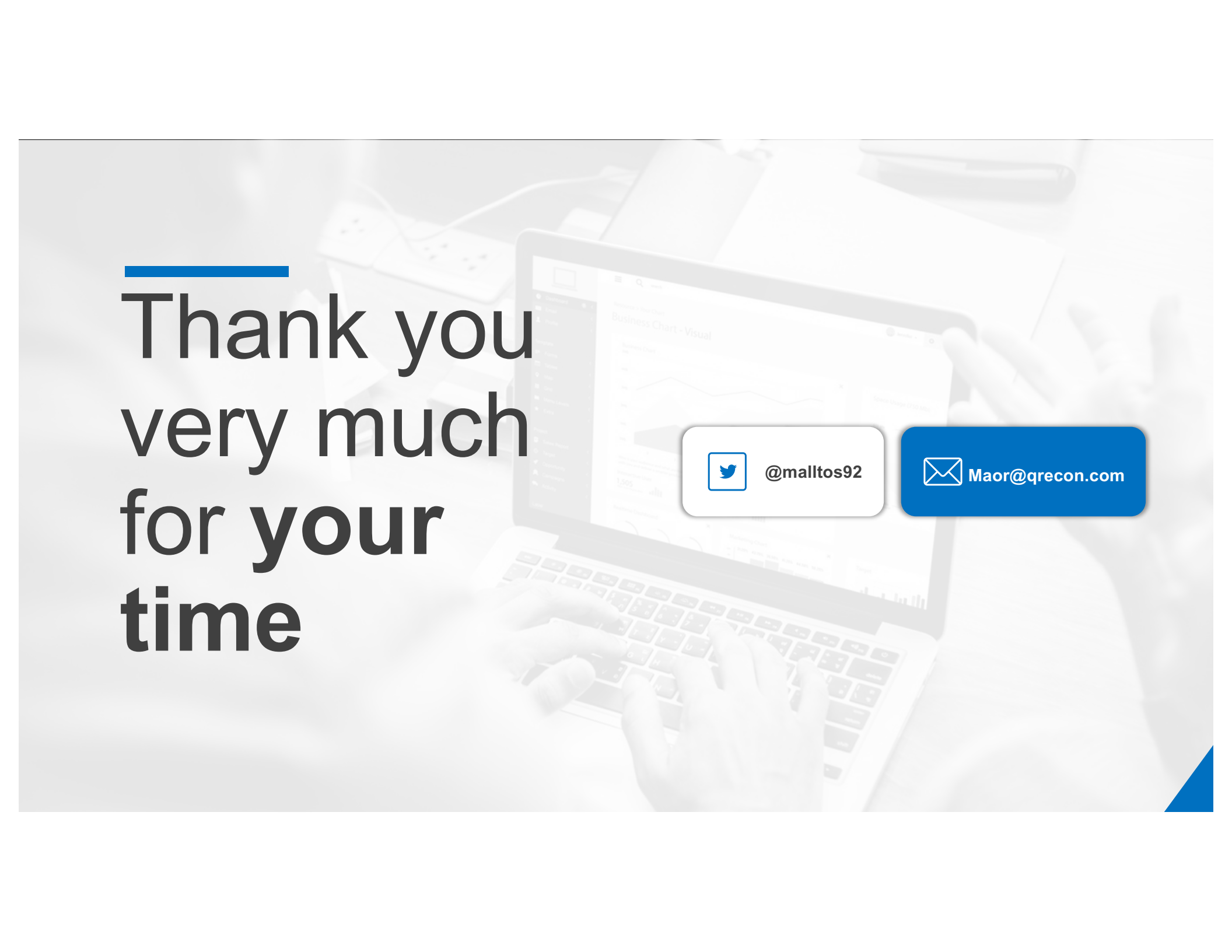


# How Can I Help You on Your Journey

I closed my company, but I still want to help.  
ATM, I offer my services for free, no strings attached.



Questions?



Thank you  
very much  
for **your**  
**time**



@malltos92



Maor@qrecon.com