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 (?)
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
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
In the past 5 years the 0-day market has transformed drastically. The increase in the 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 / PWNoRAMA / 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
Vulnerability researchers – overview (bugcrowd)

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.
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

<table>
<thead>
<tr>
<th>End-product</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vector</strong></td>
<td><strong>Dedicated research</strong></td>
</tr>
<tr>
<td>• RCE + LPE + Persistence</td>
<td>• Freelancing</td>
</tr>
<tr>
<td><strong>Vulnerabilities</strong></td>
<td><strong>Workshops</strong></td>
</tr>
<tr>
<td>• RCE</td>
<td>LPE</td>
</tr>
<tr>
<td><strong>Component (parts in a chain)</strong></td>
<td><strong>Consulting</strong></td>
</tr>
<tr>
<td>• Info leak</td>
<td>• Validate other researchers vulnerabilities</td>
</tr>
<tr>
<td>• Mitigation bypass</td>
<td><strong>Support</strong></td>
</tr>
<tr>
<td></td>
<td>• Exploit new versions</td>
</tr>
</tbody>
</table>
Companies vs Governments

Offensive security companies

Knowledge (vulnerabilities)
Product (license)

Governments

Capable countries
Incapable countries

Internal research
How are they getting them 0-days?
Researchers by groups

Researchers

High-End

Working in Offensive Sec

Willing to sell
The researcher journey

Published 1-2 high-end vulnerabilities

Hired by an offensive security company

Opened own research company

Redirect
The researcher sells vulnerabilities and have a day-to-day job

Research team in cyber defense company

Pentest

Etc.
The Process of Selling 0-days
The sales process - overview

A researcher finds a vulnerability

Contacts a potential client

Provides an overview about the vulnerability

Negotiation

Signing a contract

Validation of the vulnerability by the client (Q&A)

Payment
Payouts

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

There is no single pricelist
• Competitions (pwn2own / PWNoRAMA)
• 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*

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

*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

WhatsApp / Signal / iMessage
0 clicks
~1.5M$

iOS / Android PE
~400-600k$

Windows PE
(Redstone 6)
~250-500k$

Linux PE
~150-400k$

Chrome RCE
(without sandbox escape)
~300-400k$

FF RCE
~200-400k$

Edge RCE
~100-300k$

*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.
A researcher finds a vulnerability
Contacts a potential client
Provides an overview about the vulnerability
Negotiation
Signing a contract
Validation of the vulnerability by the client (Q&A)
Payment
IMPORTANT

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

IANAL: I Am Not A Lawyer
SOFTWARE ACQUISITION AGREEMENT

This Agreement describes how the Seller, will provide the Software and any related services to the Buyer, which is to be used as specified in this Agreement.

DEFINITIONS

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 Specifications.
1.3 “Documentation” means the manuals, user instructions, and other related materials supplied to the Buyer by the Seller (whether in written or electronic form) for use with the Software, including any part or copy of it.
1.4 “Equipment” means any hardware equipment compatible with the Software.
1.5 “Fees” means the fee specified in clause 5.
1.6 “Materials” means the Software and the Documentation.
1.7 “Software” means the computer programs as described in the Specifications.
1.8 “Specifications” 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.

2. Sale of Software

2.1 Subject to the terms of this Agreement and in consideration of the payment to the Seller by the Buyer, the Seller shall sell and deliver to the Buyer the Software and the 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.

3. Delivery and Installation

3.1 The Seller will deliver one copy of the Software, as both object code and source code, to the Buyer as specified in 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.
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.
LEGAL - CONTRACTS

Spec

Exclusive / Nonexclusive

Delivery date

Validation period

Fees & payment

Propriety rights

Confidentiality

Support

Governing law

Export liability

SOFTWARE ACQUISITION AGREEMENT

This Agreement describes how the "Seller", will provide the "Software" and any of its affiliated components (including the "Hardware") with software and documentation, which are detailed below, and how the Buyer is allowed to use the same.

1. Definitions:

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 using 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 5.


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.

2. Sale of Software

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 the relevant export or import laws and regulations.

3. Delivery and Installation

3.1. The Seller will deliver one copy of the Software, as both object code and source code, and the Documentation by electronic means to the Buyer, within five (5) business days 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.
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

Propriety rights

Confidentiality

Support

Governing law

Export liability

SOFTWARE ACQUISITION AGREEMENT

This Agreement describes how the Seller, will provide specific software and documentation, which are detailed below, and how the Buyer is allowed to use the same.

1. Definitions:
   a. “Acceptance Date” means the date on which the Software is accepted or deemed to be accepted by the Buyer pursuant to clause 4.
   b. “Agreement” means these terms and conditions which shall include the Specifications.
   c. “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 using the Software, including any part or copy of it.
   d. “Equipment” means any hardware equipment compatible with the Software.
   e. “Fees” means the fees specified in clause 5.
   g. “Software” means the computer programs as described in the Specifications.
   h. “Specifications” means the specification document describing the functions of the Software provided by the Seller to the Buyer.
   i. “Release” means any improved version of the Software.
   j. “use the Software” means to sell or distribute the Software, or load the Software onto and store, run and display the Software in accordance with the terms of this Agreement.

2. Sale of Software
   a. Subject to the terms of this Agreement and in consideration of the payment to the Seller by the Buyer, the Seller shall sell and deliver to the Buyer the Software and Documentation.
   b. If and when applicable, each party will be responsible for its own expenses for complying with all relevant export or import laws and regulations.

3. Delivery and Installation
   a. The Seller will deliver one copy of the Software, as both object code and source code, and the Documentation by electronic means to the Buyer, within five (5) business days of the execution of this Agreement.
   b. The Buyer shall install the Software and the Documentation in accordance with the Specifications. The Buyer is responsible for installing the Software and the Documentation in the Equipment.
   c. The Seller will use all reasonable endeavors to achieve delivery by any specified or requested date.
6. Fee & Payment Terms

6.1. The Buyer shall pay to the Seller a total sum of __________ US dollars (USD __________) 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 __________ (USD __________) to be paid after successful acceptance tests within seven (7) days of the Acceptance Date (the “First Installment”).

6.1.2. __________ equal monthly installments of __________ US dollars (USD __________) 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.

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
SOFTWARE ACQUISITION AGREEMENT

This Agreement describes how the "Seller", will provide the software and documentation, which are detailed below, and how the Buyer is allowed to use the same.

1. Definitions
   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 Specifications.
   1.3 "Documentation" means the operating manuals, user instructions, and other related materials supplied to the Buyer schedules therein.
   1.4 "Equipment" means any hardware equipment compatible with the Software.
   1.5 "Fee" means the fee specified in clause 5.
   1.6 "Materials" means the Software and its Documentation.
   1.7 "Software" means the computer programs as described in the Specifications.
   1.8 "Specifications" means the specification document describing the functions of the Software produced 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.

2. Sale of Software
   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 for its own expenses for complying with its relevant export or import laws and regulations.

3. Delivery and Installation
   3.1 The Seller will deliver one copy of the Software, as both object code and source code, to the Buyer.
   3.2 The Seller 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**

<table>
<thead>
<tr>
<th>Exclusive</th>
<th>Nonexclusive*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buyer acquires any and all title, copyright, or other proprietary rights</td>
<td>The researcher sells a license</td>
</tr>
<tr>
<td>Researchers - make sure you add to the contract the ability to use your vulnerability for internal research</td>
<td>Can be sold multiple times</td>
</tr>
</tbody>
</table>

*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

Propriety rights
Confidentiality
Support
Governing law
Export liability

SOFTWARE ACQUISITION AGREEMENT
This Agreement describes how the “Seller”, will provide software and documentation, which are detailed below, and how the Buyer is allowed to use the same.

1. Definitions:
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 the terms and conditions which shall include the Specifications.
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 using the Software, including any part or copy of it.
1.4. “Equipment” means any hardware equipment compatible with the Software.
1.5. “Fees” means the fees specified in clause 8.
1.7. “Software” means the computer programs as described in the Specifications.
1.8. “Specifications” means the specification document describing the functions of the Software provided by the Seller to the Buyer.
1.9. “Release” means any updated 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.

2. Sale of Software
2.1. Subject to the terms of this Agreement and in consideration of the payment to the Seller by the Buyer of the Fees, the Seller shall sell and deliver to the Buyer the Software and Documentation.
2.2. If not otherwise applicable, each party will be responsible and in its own expense for complying with relevant export or import laws and regulations.

3. Delivery and Installation
3.1. The Seller will deliver one copy of the Software, as both object code and source code, and the Documentation by electronic means to the Buyer, within five (5) business days 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.
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

Propriety rights

Confidentiality

Support

Governing law

Export liability

SOFTWARE ACQUISITION AGREEMENT

This Agreement describes how the “Seller”, will provide and any of its affiliated companies (collectively the “Buyer”) with software and documentation, which are detailed below, and here the Buyer is agreed to use the same.

1. Definitions:

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 Specifications.

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 using 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 “Fees” means the fees 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.

2. Sale of Software

2.1 Subject to the terms of this Agreement and in consideration of the payment to the Seller by the Buyer of the Fees, the Seller shall sell and deliver to the Buyer the Software and Documentation.

2.2 If and when applicable, each party will be responsible for its own expenses for complying with its relevant export or import laws and regulations.

3. Delivery and Installation

3.1 The Seller will deliver one copy of the Software, as 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.
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.
SOFTWARE ACQUISITION AGREEMENT

This Agreement describes how the Seller, will provide the software and any related services to the Buyer. The terms and conditions of this Agreement are as follows:

1. Definitions:
   1.1 "Software" means the software and any related services.
   1.2 "License" means the right to use the Software.
   1.3 "Documentation" means the documentation associated with the Software.
   1.4 "Support" means any technical assistance provided by the Seller.

2. License:
   2.1 The Seller grants to the Buyer a non-exclusive, non-transferable license to use the Software.
   2.2 The Buyer may not copy, distribute, or sublicense the Software.

3. Restrictions:
   3.1 The Buyer may not reverse engineer, decompile, or disassemble the Software.
   3.2 The Buyer may not make any modifications to the Software.

4. Support:
   4.1 The Seller will provide technical support to the Buyer.
   4.2 The Buyer may contact the Seller for support.

5. Termination:
   5.1 Either party may terminate this Agreement at any time upon written notice.
   5.2 Termination will not affect any accrued rights or obligations.

6. Governing Law:
   6.1 This Agreement will be governed by the laws of the jurisdiction.

7. Export:
   7.1 The Buyer will comply with all export laws and regulations.
   7.2 The Buyer will not export the Software.

8. Proprietary Rights:
   8.1 The Seller retains all proprietary rights in the Software.

9. Confidentiality:
   9.1 The Buyer will keep the Software confidential.
   9.2 The Buyer will not disclose the Software to any third party.

10. Governing Law:
    10.1 This Agreement will be governed by the laws of the jurisdiction.
    10.2 Any dispute arising from this Agreement will be resolved in the jurisdiction.

11. Export:
    11.1 The Buyer will comply with all export laws and regulations.
    11.2 The Buyer will not export the Software.

12. Termination:
    12.1 Either party may terminate this Agreement at any time upon written notice.
    12.2 Termination will not affect any accrued rights or obligations.

Legal - Contracts
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.
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.
Export liability - **Wassenaar**

- Report to vendor
- No problem

- Exporting (End-product / Research Service)
- Special Marketing License
- Special Selling License

Ministry Of **Defense** (MOD)
Finding the Customers
The sales process - overview

A researcher finds a vulnerability

Contacts a potential client

Provides an overview about the vulnerability

Negotiation

Signing a contract

Validation of the vulnerability by the client (Q&A)

Payment
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

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>The researcher knows who the client is</td>
<td>The client (usually) knows the researcher identity</td>
</tr>
<tr>
<td>Updated in real time on the status of the deal</td>
<td>Limited number of potential clients (~5)</td>
</tr>
<tr>
<td>Legal (licensing)</td>
<td>Legal (licensing)</td>
</tr>
<tr>
<td></td>
<td>The researcher might get underpaid</td>
</tr>
<tr>
<td></td>
<td>Bad Contract (The client can add limiting terms before buying)</td>
</tr>
<tr>
<td></td>
<td>Multiple POCs Simultaneously - Time consuming</td>
</tr>
</tbody>
</table>
Selling Vulnerabilities to Govs / Companies

- Official point of contact
- Vulnerability brokers

Personal connections (govs / companies)
## Personal connections

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

PSSST

WANT TO BUY SOME 0-DAYS
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
- Negotiation
- Market Landscape
- Legal
- Close and intimate relationship with clients
- 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 sable

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

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

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

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 be the better offer if your 0day goes to 0$.

- **Always listen to feedback.** If you 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