Shaping the future 0-day market

CROWDFENSE

VULNERABILITY RESEARCH HUB

Agenda

1) Introduction

- What is Crowdfense?

2) The 0-day market today

- Definition
- Main issues
- Our approach

3) "Hacking the 0-day market"

- Crowdfense Bug Bounty program
- Vulnerability Research Hub (VRH)
- Acquisition and testing process

4) Ok so… does it work?

- Risk analysis evaluation (per tool, target, end-user)
- Statistics (success rates, reliability rates, assets longevity, ROI)

5) Shaping the future 0-day market

- What’s next?

What is Crowdfense?

- Crowdfense is a **UAE** based, **independent**, world-class **offensive security** R&D hub, engineered from the ground up to serve both institutional Customers and cyber-security Researchers.
- Researchers, Partners and Customers can benefit from our **professionalism** and **technical know-how**, our deep understanding of **CNE operations** and from our undisputed **reliability**.
- We support **a few selected institutional Customers**, either directly or through trusted **Partners**.
- With a growing portfolio of **highly actionable cyber capabilities**, which includes intelligence-grade 0-day exploits, specialized offensive and defensive tools, we deliver **turnkey solutions** that are innovative, expertly engineered, reliable, economically sustainable and efficient.

2. The 0-day Market Today

The 0-day Market Today – Definition

The **market for "zero-day" exploits** refers to the commercial activity that happens around the development and sale of software **exploits** that are based on **software "bugs"** which are **unknown to the vendors of the affected technologies**. The term "zero-day" refers to the **time since the discovery of the bug**, which in this case is zero.

Zero-day exploits can be used to **remotely (or locally) compromise a target device**, to control it and/or to install specific software on it in order **to collect and exfiltrate data** ("agents, "implants") or **to sabotage/damage it** ("cyber-weapons").

This type of exploit is **extremely powerful** for institutional purposes because the targets are **unaware of their existence** and cannot **properly defend** against them.

For this reason, a **small subset** of zero-day exploits (those which are stealth, silent, don't generate artifacts and are very reliable) is **highly valuable** (in the range of hundreds of thousand / millions of USD each).

The 0-day Market Today – Main issues

Historically, it's unsafe, chaotic and inefficient from a business pov.

This hampers the (now strategic) ability of law enforcement and intelligence agencies to fight crime / terrorism / hostile geopolitical actors in the cyber domain.

Researchers are often underpaid for their exponentially complicated efforts.

There is a talent vacuum as underpaid researchers seek more lucrative fields / do research as a second job.

From the **demand** side, Customers have **no guarantees**, must rely on middle-men and intermediaries which usually don't bring any added value, and the **risk** of scams, of quality issues and of financial losses is quite high.

Our mission is to **manage these risks** and create a better environment for performing cyber offensive operations, for **all the parties involved** (customers, researchers, integrators/partners).

3. “Hacking the 0-day Market”

Our Approach

The speed of the evolution in this field is astonishing.

The variables involved are so complex (from a geopolitical, strategic, technical, legal, financial, ethical and organizational point of view) that what was "true" and understood in 2015 is now pre-history. We strive to anticipate this evolution and to define it.

To combat the inefficiencies in the current 0-day market, we set the goal to "normalize", professionalize and streamline this business, by changing its rules:

- Protecting researchers with fair contracts and offering them higher pay-outs
- Efficiently allocating economic resources while minimizing legal, operative and reputational risks
- Reducing unnecessary middle men by building trust with researchers and customers
- Develop, adopt and spread new best practices, standards and methodologies

Crowdfense Bug Bounty Program

In early 2018 we launched our first **10M USD** Public Bug Bounty program, which offered the highest bounties ever paid for these classes of exploits.

In 2019 we added more bounties (**15M USD**) and included more classes of exploits in our program.

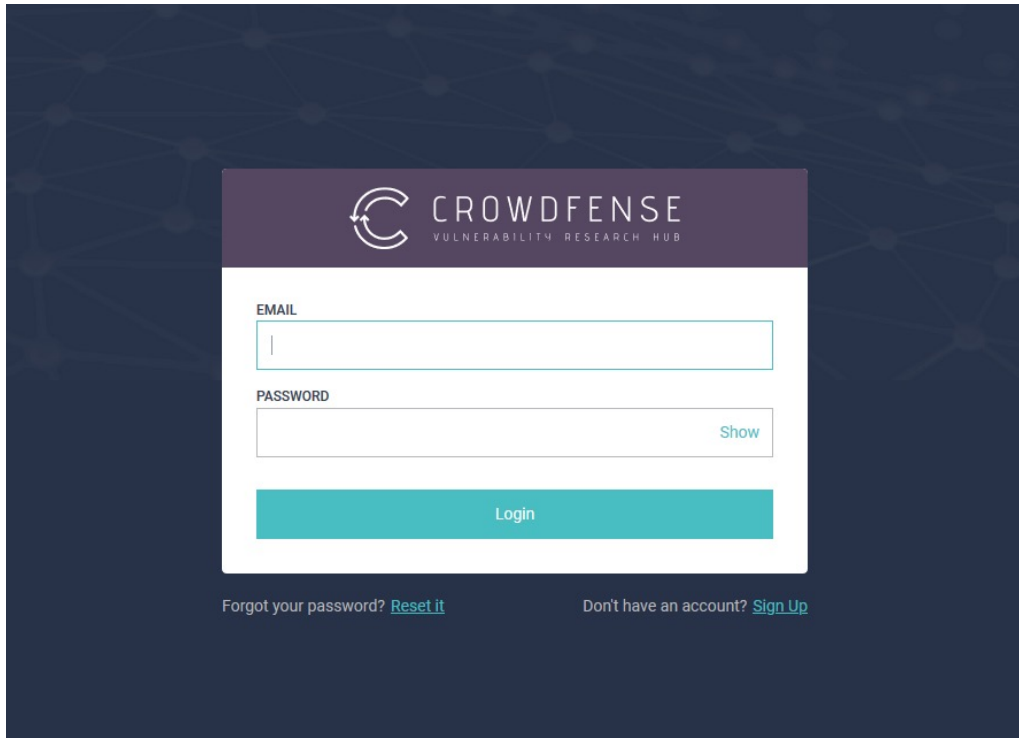
In 2020, we confirmed the same **15M USD** program.

Thanks to this program, we were able to purchase top quality capabilities, and are in the process of buying more.

By the end of 2020 we invested **40M USD in less than 3 years** on our Public Bug Bounty program.

OS	Chain components		Persistence	Partial or Full chain Payouts
Windows	Chrome RCE →	Sandbox Escape		1 click - Up to 1,5M USD
MacOS	Safari RCE →	Sandbox Escape		1 click - Up to 500k USD
iOS	Safari RCE →	iOS PE →	✓	1 click - Up to 1.5M - 2.5M USD
	Zero-interaction RCE →	iOS PE →	✓	0 click - Up to 1.5M - 3M USD
Android	Chrome RCE →	Android PE →	✓	1 click - Up to 1.5M - 2M USD
	Zero-interaction RCE →	Android PE →	✓	0 click - Up to 1.5M - 3M USD
Various	Instant Messengers or SMS/MMS RCE →		✓	0 click up to 1.5M USD 1 click up to 1M USD
	Routers RCE →			up to 100k USD
	WiFi / Baseband RCE →	LPE →		up to 500k USD

The Vulnerability Research Hub (VRH)



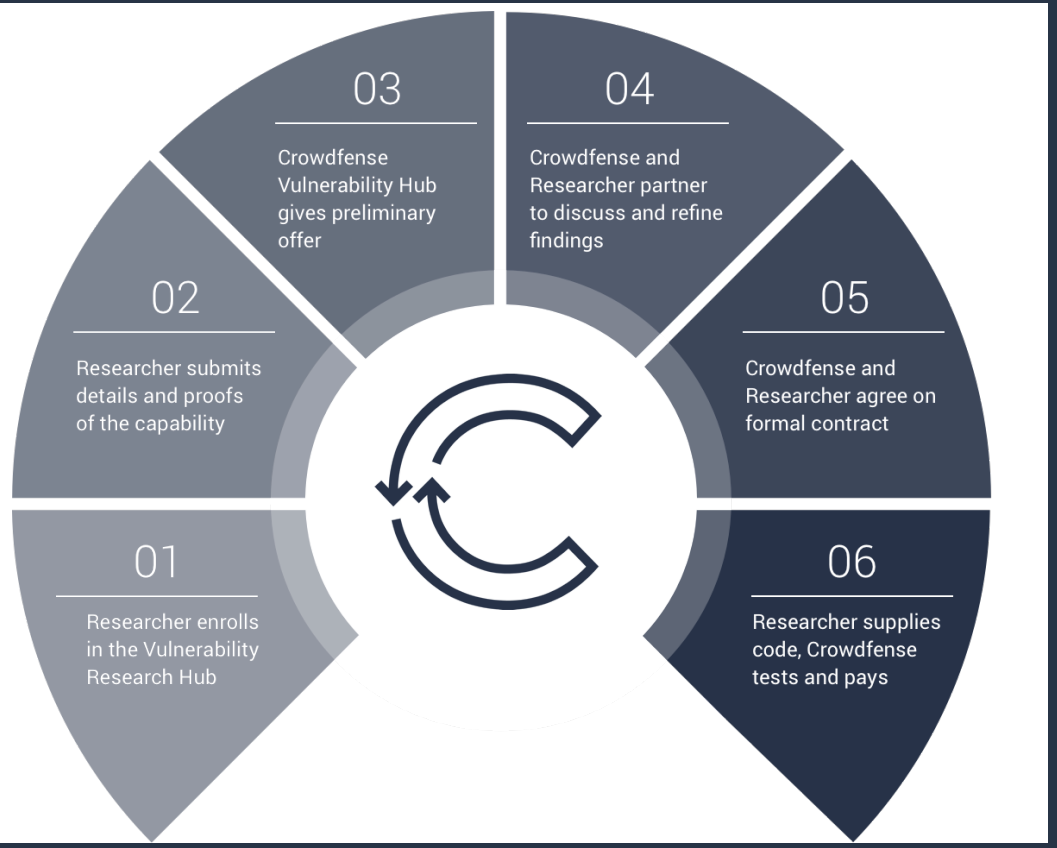
Step by step, user friendly workflows manage submission, discussion, testing, evaluation, contracting and payment.

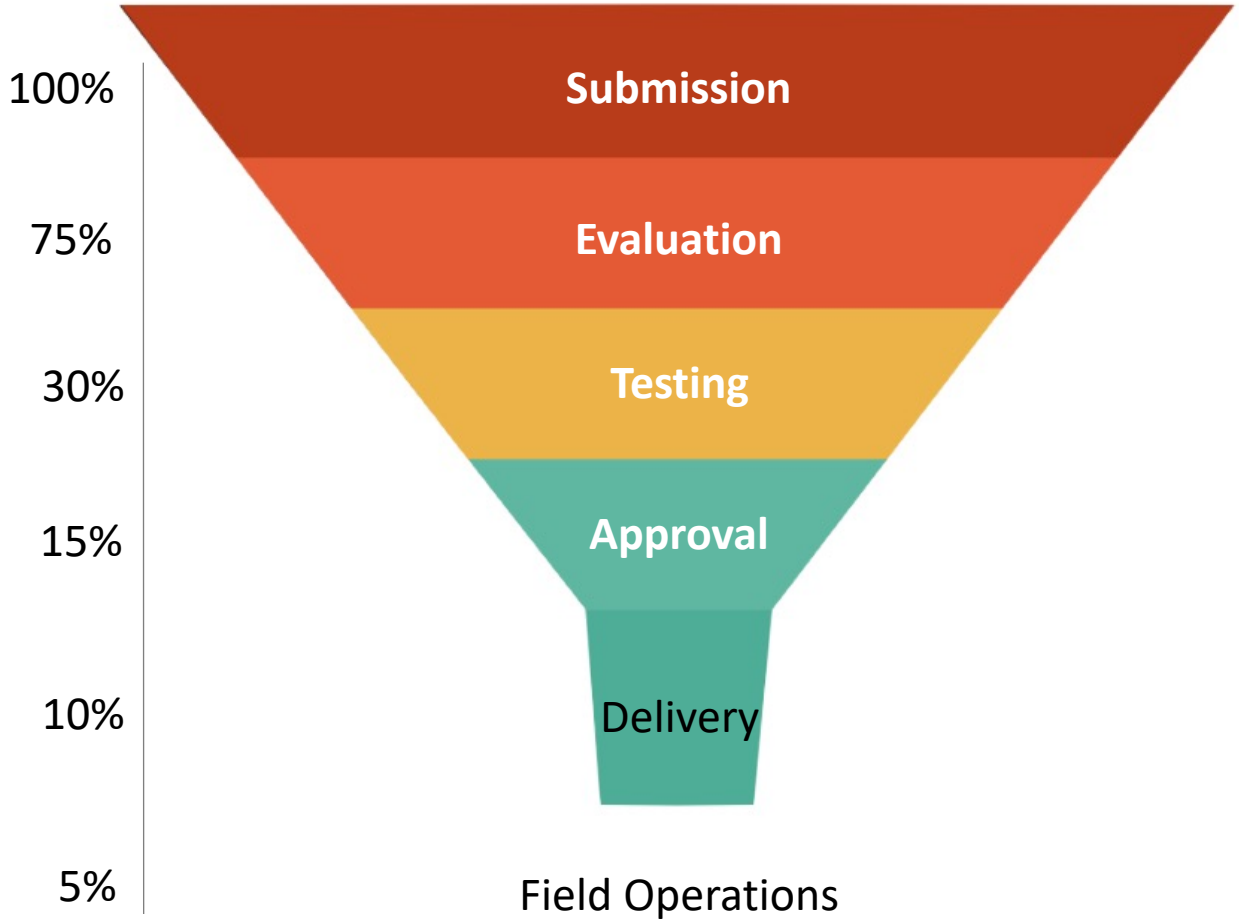
Findings can be both within the scope of the Bug Bounty Program or freely proposed by researchers (within our Code of Conduct).

Based on a zero-trust model with maximum OpSec for all participants.

Acquisition and testing process

Only a few 0-days are «good enough» for our Customers.
The intelligence-grade 0-days «funnel» is very steep.
Out of 100 submissions, no more than 5 can be deployed on the field.

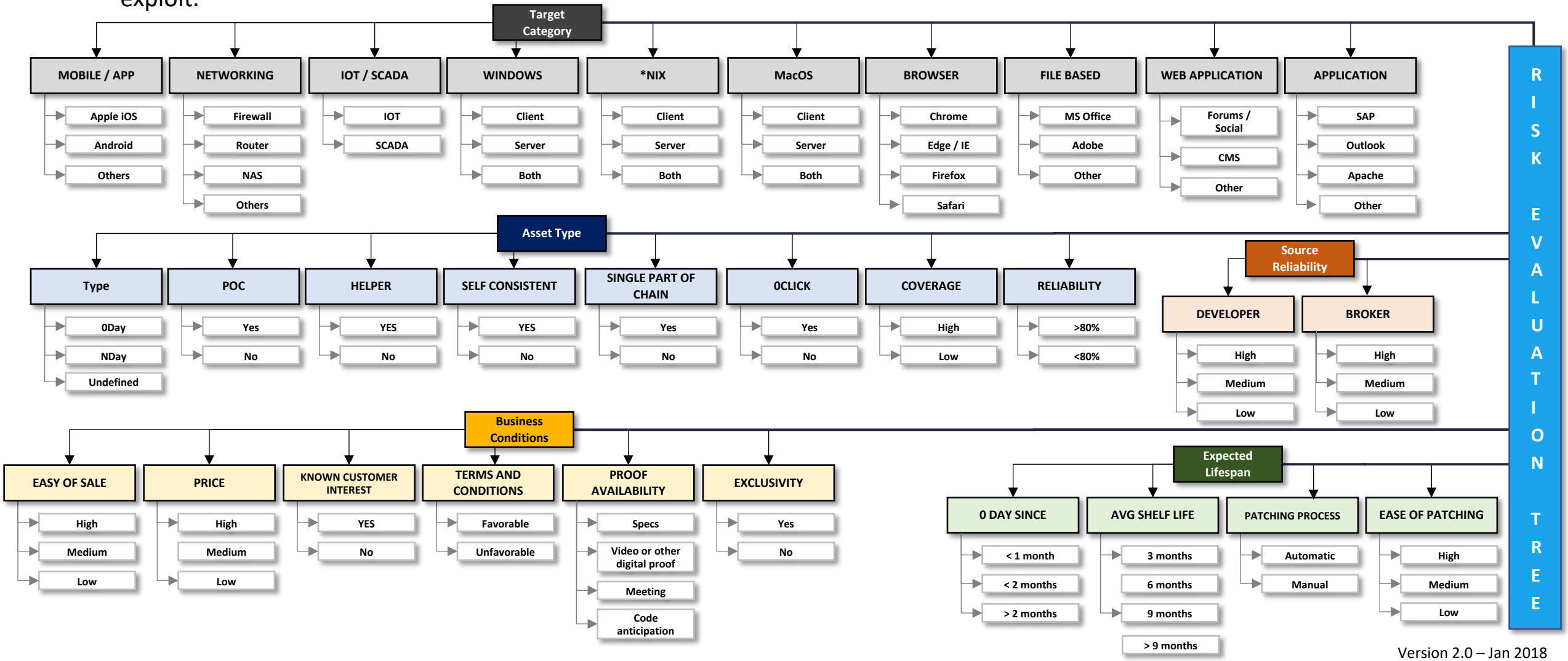




4. Ok so… does it work?

Risk analysis evaluation – 1

We developed a unique, proprietary methodology to assess (under different angles) the risks associated with each 0-day exploit.

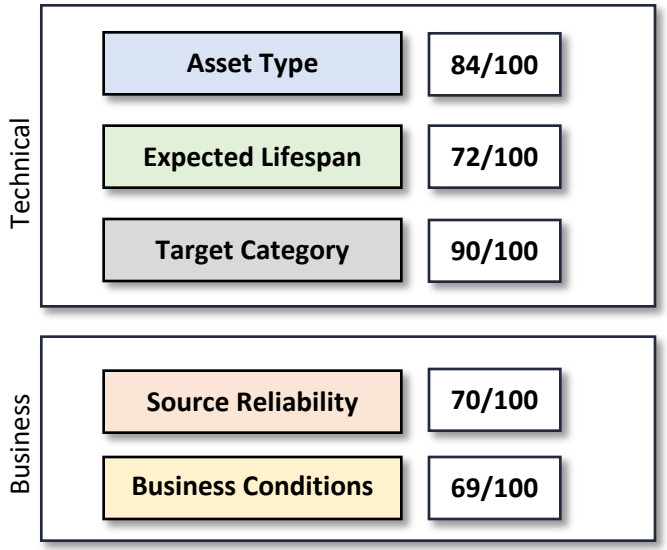


Version 2.0 – Jan 2018

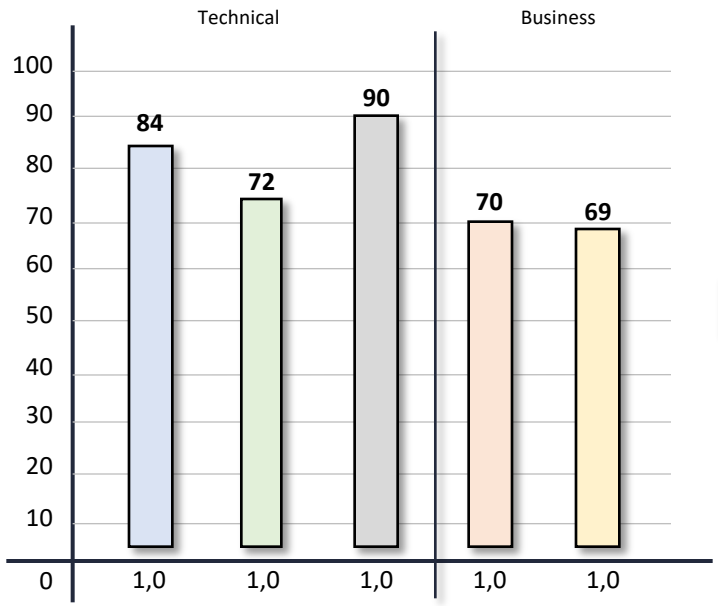
Risk analysis evaluation – 2

The result is a set of risk indexes, based on the specific features of the exploit, the use-cases and the customer posture.
This is an example of the summary of an exploit-related KRI (Key Risk Index).

According to our evaluation model, these are the initial results for asset **XX-XXX**. Higher values indicate a lower risk.



Asset risk evaluation results

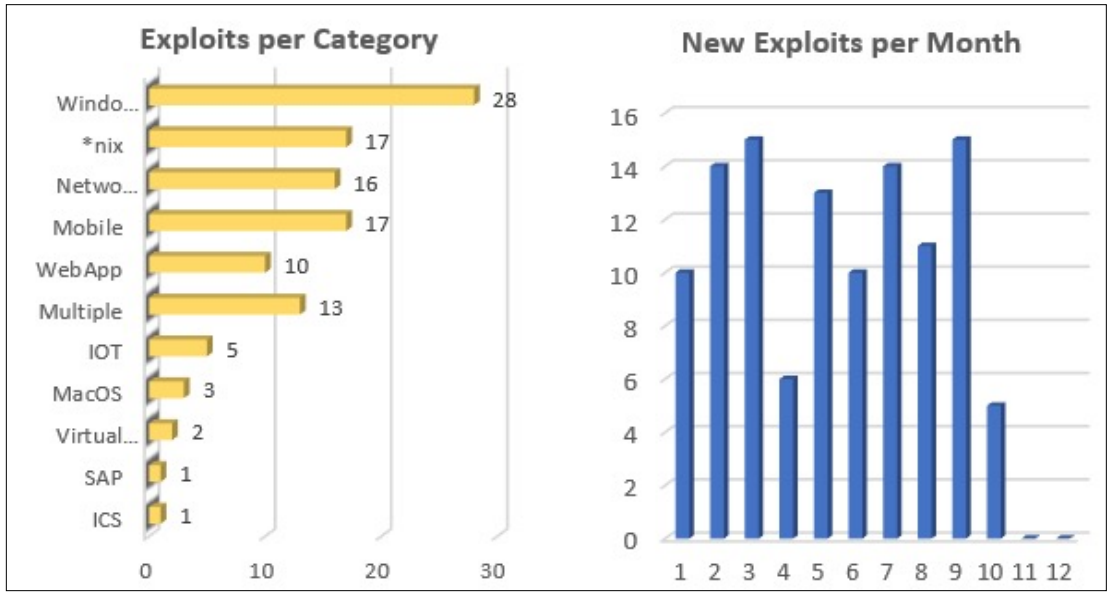


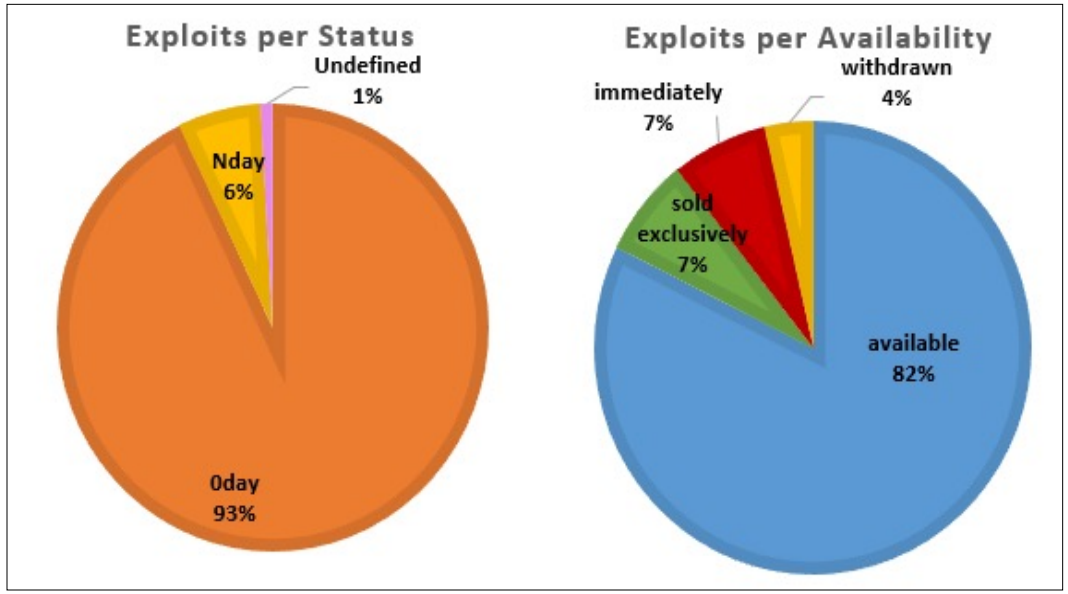
Weighted values (if any)

Some VRH statistics – 1

After 10 months, 93% of the 125 intelligence-grade exploits that we managed in 2019 were still 0-day and 89% were still available for sale. This result is very important, as (on average) the life span of a 0-day exploit is around 12+ months for networking devices, 9 months for desktop products, with a lower range of 3-6 months for important classes of mobile targets (Android and iOS).

This longer than average shelf-life improves the ROI of these exploits by 75-200%, depending on the situation and on their application model. The average reliability of these exploits is in the 90-100% range. The detectability is almost zero, due to the efforts we put in their testing, re-engineering and maintenance.





5 – The future

Shaping the future 0-day market

There are at least 3 trends that we are monitoring, and trying to anticipate in order to optimize them:

- the age of the “lone wolves” is almost finished. For certain classes of targets, finding valuable bugs, exploiting them in a reliable, actionable way is getting harder and harder for individual researchers (even if individual talents are still fundamental in this field). Research efforts must be handled by large groups (as is already happening in some places, with very good results). But these groups must be managed in a professional way, and someone with dedicated know-how and experience must take care of all the non-technical issues (legal, organizational, financial, project management, QA, etc). So, we will offer our expertise-as-a-services to these groups, by partnering with them.

- There is a clear trend towards the convergence of offensive and defensive security activities. Many people still think that these 2 areas should be separated and avoid contact as much as possible (except for red teaming activities and vanilla bug bounty programs, to a certain degree), but in our opinion this is a waste of resources and opportunities. For this reason we already created defensive products that embed all our offensive know-how, and vice-versa. We will push more towards this convergence in the next months and years.

- In this field there are still no proper risk management processes in place. People are trading highly dangerous goods without assessing their related risks, liabilities and potential adverse impacts on society as a whole (and no, a CVSS score is not what we are talking about). We will try to support the definition of a new market standard for assessing these risks in a systematic, comprehensive way, by collaborating with researchers, integrators, end-users and the public.

CROWDFENSE

VULNERABILITY RESEARCH HUB

Thanks!