PoC 2024 Keynote

An insider perspective on the offensive industry

~qwertyoruiop, Seoul

Who am I

- Luca Todesco, aka qwertyoruiop
- Cofounder at Dataflow Security S.R.L.
- Have always been interested in the iOS jailbreaking scene since iPhoneOS 1.1
    - First tried to get in the scene around iOS 3, making Cydia Store tweaks as my very first income source
- Have been an independent researcher for several years before starting DFS
    - I'll talk a bit about my independent experience in the next few slides

Foreword

- This is going to be a talk about my own experience and insights of the offensive industry
  - My own biases and misunderstandings are quite hard to remove from the equation in such a non-technical talk
  - I have however incorporated takes from a lot of people I have discussed with over the years, and while these are my personal opinions they are a strong influence in how we approach this industry at Dataflow Security
- I don't claim to have a full understanding of the industry, and there are people who certainly disagree with my perspective
  - I'm more than happy to have discussions around this topic and willing to change my opinion and learn new perspectives!

Security research as hobby

- In early 2015 I wrote my first (really bad) exploit for a (really dumb) MacOS bug I found in IOHIDFamily (CVE-2015-1140)
    - https://github.com/kpwn/vpwn
- I kept going with my holy grail goal being a full iOS kernel privesc straight from the default ‘container’ app sandbox
    - After a few months I ended up finding a very nice iOS kernel use-after-free and managed to come up with a reliable exploit
        - My first hit of 0day dopamine, got hooked ever since

From hobby to career

- At the time I had recently turned 18, was still in high school and I had read about the existence of a zero-day market in the Hacking Team email leaks
  - Armed with my UaF I decided to ask around for any pointer towards brokers in the zero day market, and eventually a friend pointed me towards a broker
    - I managed to reach a deal and sold an exploit for the first time
    - I had no knowledge of the market at all at the time, but I figured one could reasonably trust a broker from being in a respectable jurisdiction alone
      - It however was a mistake, and I have since learned that brokers are very seldom trustworthy and will not be transparent about end users, exclusivity or deal pricing

Going all in into security research

- After ending high school I decided to skip college and focus on independent research, and I decided to relocate to a low cost of living country
    - Ended up living in Timisoara, Romania for 6 years
        - It was pretty good, and I got my very first gigabit FTTB connection after growing up on 7mbit DSL :)
- I set up a Romanian SRL (limited liability company) and started doing research full time
    - Initially focusing on iOS PE but later diversifying into WebKit RCE

Scaling up

- Eventually I got acquainted with several other independent researchers and we began working on group projects
    - Much better to share the pie with talented people, working on more items and being able to come up with full chains more regularly
- I also ended up meeting with a trusted advisor in my network who represented my interests on the sales side of the equation, and unlocked direct access to end users with full transparency every step of the way
    - I consider working with him one of the best choices I made, and he ended up as a fellow cofounder in Dataflow Security

Scaling up even further

- Due to the rising complexity of iOS exploitation, I decided to grow the independent operation into a larger research shop
  - This is how Dataflow Security started, and we have 90+ people involved these days!
  - **Adapting to change is a key skill required to be a successful attacker, and the avenues for change are not only technical but also entrepreneurial/strategic**
- I have since learned that my understanding of the industry as an independent researcher was very lacking compared to the perspective I have these days
  - One of the goals of this talk is to demystify some aspects of this fairly opaque industry, a la “things I wish I would have known from the beginning”

The offensive industry at a glance

- The ultimate “end-to-end product” is an interception system that operators at relevant governmental bodies can use in order to accomplish their national security, law enforcement and/or public safety missions
  - Operators (mostly) are abstracted from the details of how the sausage is made and how exploits and agents work in detail
- These products can either be developed in-house by end users directly or are purchased from private end-to-end product companies
  - Almost all governments have in-house expertise and capabilities, but this does not usually apply to mobile targets, which are significantly more hardened than desktops
    - Few end users have the budget, knowhow and need to go in-house for mobile due to fast changing complexity, market dynamics and limited availability of talent

The offensive supply chain

- There is usually an extensive supply chain involved, and private companies and government end users alike have supplier networks for exploits, agents and other components, but also sponsored external research and development for specific uncommon capabilities
  - Even highly vertical players with strong in-house skills will occasionally have a need to tap into the supply chain due to unforeseen circumstances
  - Some government end users will even purchase several equivalent offerings for backup or specific operational purposes
- Exploit providers are a key part of this supply chain, and are either independent researchers or are organized in larger “research shops”
  - Due to increasing difficulty in developing exploit chains independent researchers for the most complex targets have been disappearing, and purchasing exploits is becoming more and more relevant even to end users that were previously not part of the market

Private offensive suppliers: pros and cons

- For end-users a big drawback of private sector suppliers is that capability lifetime is dependent on the customer set
    - By developing stronger relationships with suppliers this can be minimized and controlled to an extent
    - When purchasing full end-to-end products it may create a link between operations of different end users, potentially resulting in misattribution by defense
        - Can pose reputational risks to responsible end users if the same end-to-end product is also used by less responsible governments, tying different operations together
        - It can conversely also be used strategically by less responsible governments as a reputational shield, shifting attribution to either the supplier or other end-users

Private offensive suppliers: pros and cons

- On the other hand, the ability to tap into an external supply chains has both economical and operational advantages
  - On the economic side it allows the R&D costs to be shared between multiple end users, and uptime risk can be split via contractual warranty provisions
  - Operationally it unlocks access to capabilities which require rare talent as well as the ability to have redundant suppliers to maximize uptime

Exploit sales 101

- Exploit sales are either exclusive or non exclusive
    - End users are mostly fine with non-exclusive on more liquid/available items, and exclusivity is usually more relevant for tailored or strategic capabilities
- Sponsored research and development is usually exclusive
    - Since the end-user is taking the research risk, IP is usually owned by the end-user directly
    - I have heard of some arrangements with limited non exclusivity for the resulting IP, usually with provisions to compensate the risk taken by the sponsor such as credits for future engagements
        - Usually these also have strong limits (eg veto power) on other potential customers

Exploit sales 101

- Some end users prefer exclusivity within a given ‘country club’
    - An example is Five Eyes, which tends to prefer FVEY-exclusive items
        - This can be a strong requirement, but it’s highly dependent on specific agency and operational needs
- Every end user will prefer locally sourced items if available (sovereign market), but if not available will have no problem with purchasing from foreign suppliers
    - Having operational capability and high uptime is the most important factor
    - In the past few years, given the complexity and talent shortage, even the most self-sustaining end users are looking to the outside

Exploit sales 101

- Some end users will not want to have overlap with capabilities that some other friendly government or end-to-end supplier already has
  - Usually because the capability will be used in some joint operation or as a backup for the end-to-end supplier’s own product rather than unofficial capability sharing
  - De-duping can be achieved commercially, but will not rule out natural collisions
    - Customers can provide salted hash pre-commitments ahead of delivery by sharing a list of hashes of specific descriptions of vulnerabilities already in their possession, and can demonstrate prior knowledge by revealing the preimage
      - If one wants to obscure the number of similar capabilities held, random hashes can be added to the list

Exploit sales: Customer risk

- Some end users see items from private companies as more disposable and may purchase them to specifically avoid risking proprietary capabilities and agents during operations with a higher chance of detection
    - Not as true for exploits due to integration cost and the need to combine them with end-user proprietary assets as it is for end-to-end solutions, where the economical and technical impact is shifted to the supplier and doesn’t endanger sovereign capabilities/agents
- **Selling exploits to private companies that develop end-to-end products can be significantly riskier than dealing with end users with in-house capabilities**
- A customer specific risk premium is usually baked into pricing and this entices companies with less regard for their reputation or long-term viability into selling to riskier customers for more profits

Legal & Compliance Aspects

- Companies involved in the offensive industry must align with their jurisdiction’s geopolitical stance, which translates into export control law and other regulations
    - On top of that, barely following the law is the lower bar, and ethical companies need to have self-imposed policies stricter than current legal restrictions
- Picking customers based on export control and ethical concerns alone is not a sound strategy
    - You need your customers to be competent technically and have a strong internal culture of avoiding misuse, otherwise they **WILL** fuck things up
        - Technical capability and good operational security has a correlation with their tendency to respect human rights and freedom

Ethical considerations on offense

- Many people shape their beliefs around the legitimacy and ethics of the offensive industry based on partial views strongly influenced by the very publicized abuse and misuse of intrusion software
    - It would be a lie to claim these don’t exist, and it would be a lie to claim every player involved is acting in good faith or operates with care for negative externalities and ethical concerns
- Positive effects of the offensive industry tend to not be publicized, but they are quite significant
    - Some significant positive outcomes have been talked about publicly, notably in Synaktiv’s foreword to the most recent Hexacon

Ethical considerations on offense

- Some believe the offensive industry is inherently unethical, and that the world would be better off without it, and sadly many in defense hold this belief
  - Might be possible to make such an argument in an utopic vacuum, but I am a firm believer that the lack of legally mandatory backdoors in widely deployed end-to-end encryption products is a direct result of the offensive industry's existence
    - Look no further than the telecom industry and mandatory lawful intercept in order to see what happens when wiretapping becomes a commodity product with near-zero per-interception cost and almost no ability for defense to detect abuse, mass-interception or impose risk to continued operational uptime to countries with little respect to human rights
- **Cooperation between offense and defense could be a strategic approach to limit risks while maximizing benefits**

Misuse/abuse as key risks

- Avoiding misuse and abuse should be the most important concern for anyone in this field
    - Misuse is not only a horrible outcome ethically but also bad for business, endangering reputation and capabilities lifetime (thus contractual warranty provisions)
- **Effective customer selection is the difference between success and failure in the long run**

Sanctioned entities as an emerging risk

- Ever since sanctions started hitting some of the more unscrupulous offensive end-to-end product companies, sanction evasion is a new key risk for players involved in the offensive supply chain
    - Sanctioned companies have been aggressively setting up shell companies and creating credible stories to convince suppliers into selling to them
        - Improved due diligence and cooperation between offensive companies and local governments/defense can significantly improve the effectiveness of sanctions & export control, and status quo is far for optimal

Customer selection: whitelist/blacklist

- Whitelist-based approaches should only be made in order to choose acceptable clients to try to begin conversations with
    - Due diligence must be performed at every step of the way, and you must assume you will not be able to determine wether a party can be fully trusted in advance
        - Strong relationships are built over time, and trust but verify is paramount even with the most (perceived to be) trustworthy customers
- Blacklist-only approaches do not work at all, and are the bare minimum
    - The proper usage of blacklists is to block customers that would otherwise seem acceptable on paper, but experience showed they cannot be trusted
- **Whitelist and blacklist approaches serve different purposes and should both be used**

Customer selection: beyond the flag

- Evaluating customers based on their flag alone is not enough
    - It is key to evaluate each and every customer at an entity level
        - This is not only true for private companies (where it may be more obvious) but also very important for government customers too
            - Governments are not monolithic and one agency may have a strong internal ethical/technical culture while another may play fast and loose or lack technical competency to handle sensitive items
- Things change over time, so it’s important to continuously assess and be very willing to blacklist problematic customers as early as possible

Customer selection

- Meaningful and enforceable contractual obligations are key to enforcing consequences and incident response for misuse/abuse cases
    - Burden of proof is on the customer, and it is important to adopt a zero-tolerance policy.
        - Losing a customer can hurt in the short term but getting rid of a problem customer always helps in the long run
- Some research shops have relied on single or few well paying customers
    - This tends to be a mistake, since it makes it very hard to cut ties in case of abuse or change for the worse in a country's democratic/ethical position
        - There are some cases where this is not as much of a concern, especially in companies that only serve local authorities

On Watermarking

- Watermarking every deliverable, specification and contract is essential to be able to attempt incident response, but it’s not a guarantee that you will know which customer is at fault in certain circumstances
    - Defense often withholds samples and they don’t seem to be willing to share them with offensive players all that much (*aligns incentive defense/offense)
- A more reliable but not always practical approach is to deliver chains with different specific components, and patch-diff
    - This gives very few bits of information, so potentially leaky customers need to be binary searched for, allowing misuse to persist over longer timeframes while action could be taken sooner

On Watermarking

- One idea that’s been floating around is to have exploits come with specific public-key markers inserted by suppliers
  - This is a very dumb idea, since it’s an easy to remove watermark for leaked items or malicious players, and will paradoxically end up only affecting operations of more reasonable actors
- Being more open with sharing samples of ITW operations among select offensive players requires a leap of faith, but it’s the only approach that will enable the supply chain to enforce contractual rights or at the very least make informed blacklist choices sooner rather than later
  - Prejudice against the industry and playing politics seems to cloud the judgment of some defensive orgs, and I think it’s a missed opportunity for all
  - Mechanisms to de-risk such an approach can be developed in order to allow parties that do not trust each other to cooperate in such cases, eg. trusted neutral parties with strong NDA acting as middleman

Rising complexity

- Vendor mitigations have been very effective in increasing the complexity of exploitation on top-tier platforms
  - Apple has a strong lead among the whole industry, and has been investing heavily in security engineering and it’s finally paying off for them
- Future hardware (eg MTE) and software (eg memory safe languages) changes will force a change in the strategies used by the offensive industry
  - Logic and design flaws will become more and more relevant, and memory-corruption style approaches will be reserved to much rarer compiler/hardware bugs
  - Products may become more bespoke, eg. Instead of a full chain to deploy a system level agent with wide capabilities, think specific bugs that directly result in a more limited but still operationally useful capability

Rising complexity

- In the short term rising complexity means that offensive research and development becomes more expensive and requires more talent
    - Prices have historically somewhat scaled with complexity, but there are limits to increases: this requires diversification of licensing models to fit customer budgetary & regulatory needs
- I predict this will create a stronger incentive to lock in better, more reliable customers to maximize capability lifetime and a stronger incentive to root out misuse
- Talent is becoming harder and harder to find, putting a strong upper bound to what can be realistically be achieved in a market with many players like today
        - We will see more and more cooperation between research shops, eventually resulting in strong incentives to consolidate via mergers and acquisitions

Takeaways

- The offensive industry is in an incredibly delicate and complex business, requiring a fine balancing act in order to operate smoothly
- Law & compliance, market dynamics and rising complexity tend to align offensive players in democratic countries that are looking to operate for the long run with common-good ethical goals
  - Thoughtful cooperation between offense and defense can improve outcomes for all, potentially posing limited downsides if carefully designed
- Novel mitigations are posing significant challenges to the industry
  - But the key trait of a successful attacker is the ability to adapt to change

Any questions?

Thanks!