



PRESENTATION BY MARK DOWD (@MDOWD)

Inside The Zero Day Market

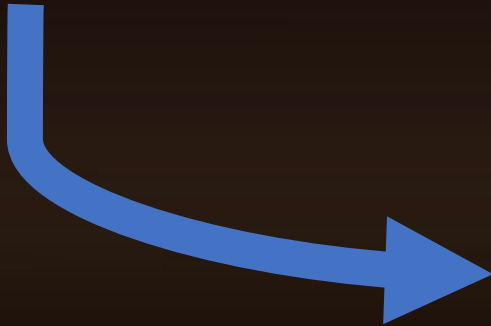
Context: Who Am I?

- ◇ Early career as a vulnerability researcher for ISS (now IBM)
- ◇ Wrote a book on vulnerability research (The Art of Software Security Assessment)
- ◇ Founded Azimuth security, specializing in offensive research
- ◇ Acquired after 10 years by US defense contractor (L3Harris)
- ◇ Founded Vigilant Labs in 2022
 - ◇ Retirement wasn't working out
- ◇ **Worked in offensive market for the past 15 years**

Evolution (Market Landscape)

EARLY DAYS (2000 – 2010)

- ◆ Taboo, very opaque
- ◆ Few customers, mostly intelligence agencies
- ◆ Often denied existence of the market at all
- ◆ Defense contractors well-positioned as primary sellers



PARADIGM SHIFT (2010 – 2020)

- ◆ Budgets started ballooning
- ◆ Customer set expanded dramatically
 - ▶ LE/MIL other specialty agencies
 - ▶ More countries got involved
- ◆ More efficient commercial entities emerge as new leaders
- ◆ Cost of exploits significantly increased

The Market: Present Day

- ◆ It's 2023 and the 0-day market is largely destigmatized, and semi-public
- ◆ Experienced significant growth
- ◆ Many players don't hide their participation
 - ◆ Sponsor conferences, advertise jobs for exploit devs
- ◆ Exploit prices (and in turn, cost of researchers is through the roof)
 - ◆ SAS2017 prediction realized

The Market: Present Day



The Future

- **Prediction 5: Full chains will mostly be possible, but extremely high cost**
 - Full chains likely unattainable for most organizations for lengthy periods of time
 - Full chain cost estimate: 1 year

Evolution (Technology)

EARLY DAYS (2000 – 2010)

- ◇ Mostly Windows-based, client side
- ◇ Server-side highly prized
- ◇ Bugs typically sold individually
- ◇ Bugs plentiful, and reliably exploitable

PARADIGM SHIFT (2010 – 2020)

- ◇ Focus started to be on mobile devices
- ◇ Chains became more common
- ◇ Development time: 3-6 months
- ◇ Uptime: close to 100%
- ◇ Exclusivity disappeared as difficulty increased
- ◇ Windows client-side demand dropped
- ◇ Server-side still interesting

MODERN DAY (2020+)

- ◇ Focus is still largely on mobile devices
- ◇ Typically, they achieve limited
- ◇ Chain development: 6-12 months
- ◇ Uptime: ~9 months?
- ◇ Current state predicted in SAS2017

A Secretive Market

- ◇ Participants rarely comment publicly
- ◇ Misconception (Implication by media): must be nefarious
- ◇ Real reasons:
 - ◇ Don't want to make you or yourself a target for espionage
 - ◇ Commercial advantage
 - ◇ Automatic negative portrayal or association by media
 - ◇ Generally looked down upon by community

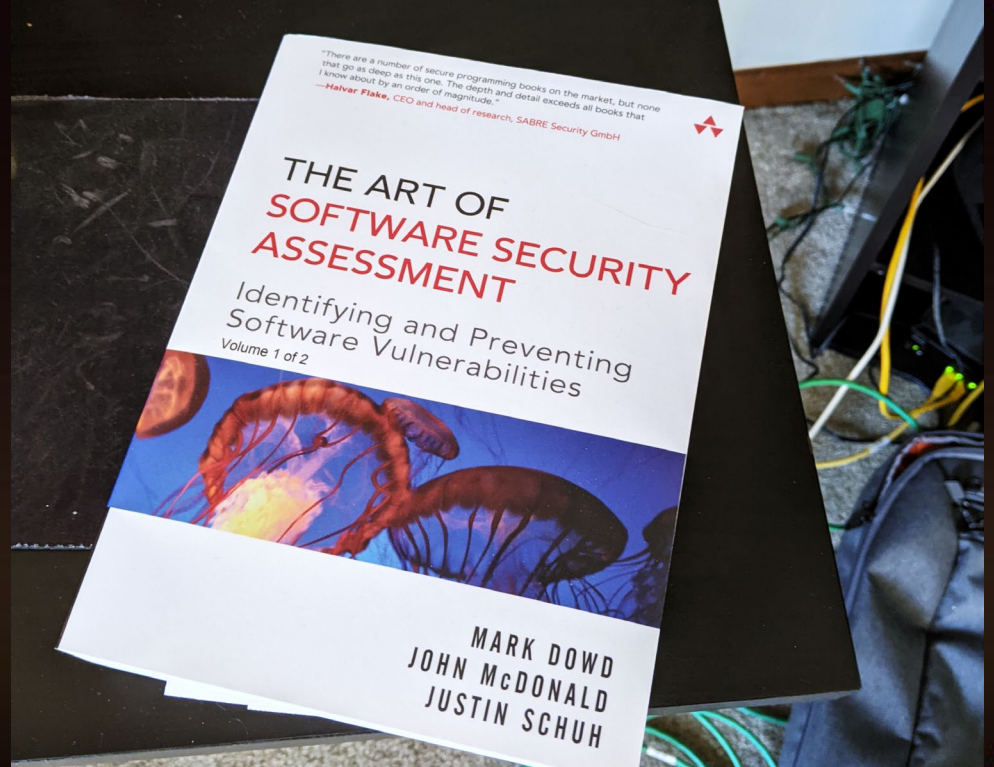
A Secretive Market

- ◇ Why Am I speaking about it?

- ◇ I was asked to!
- ◇ Give outsiders some insight in to how the market really works
- ◇ Help to dispel some myths associated with the market

Scope

- ◆ The product
- ◆ The market
- ◆ Pricing and market forces
- ◆ Note: I will only be talking about the licit government market and vendor market, not the criminal market



PRODUCT



BlueHat IL

Definition

0-day exploit:

**Code that exploits an unpatched exploitable vulnerability
that is unknown to the vendor**

Exploit Development Cost

- ◆ Discovery Cost

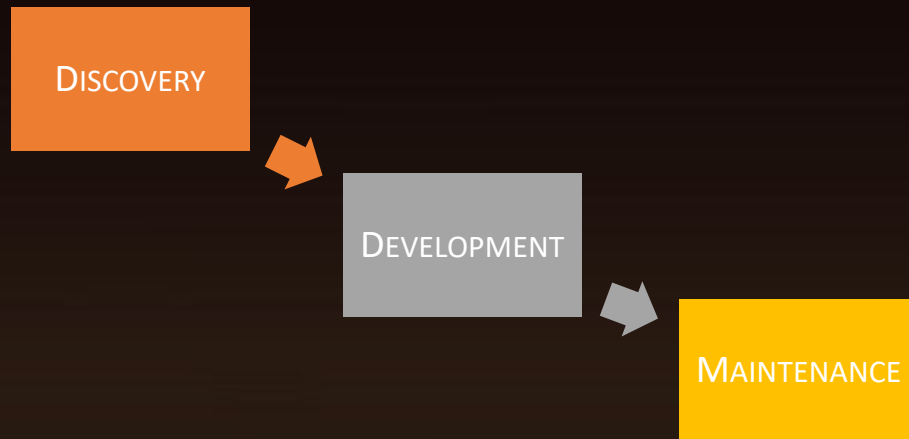
- ◆ Time to discover flaw

- ◆ Development cost

- ◆ Implement reliable exploit

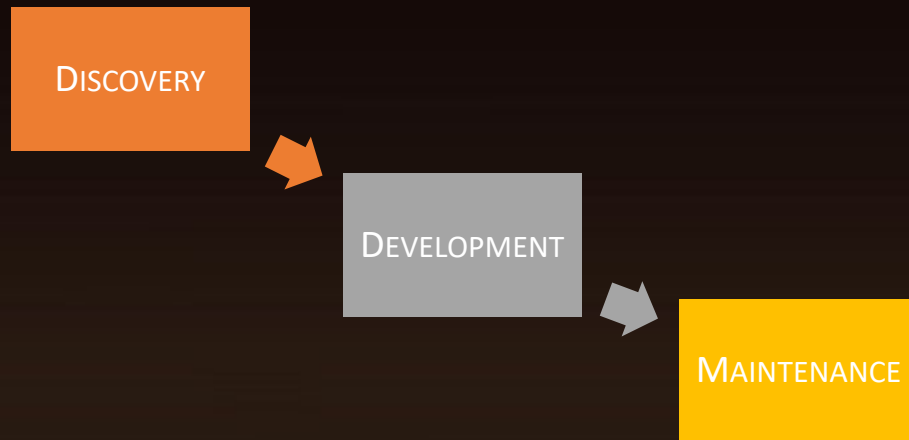
- ◆ Maintenance Cost

- ◆ Keeping exploit operational




Exploit Development Cost

- ◆ These costs are generally non-linear
- ◆ Large startup cost to attain knowledge / bug pattern identification
 - ◆ Find multiple instances of similar bugs in similar places
 - ◆ Reuse exploit techniques



Exploit Lifespan

- ◇ Exploit lifespan is shrinking
 - ◇ Defense is more effectively finding/preventing them
- ◇ Discovery/Development cost is rising
- ◇ I discuss these in depth here:
<https://github.com/mdowd79/presentations/blob/main/hitb-dowd-final.pdf>



**Exploits are temporal:
They will be rendered
obsolete**

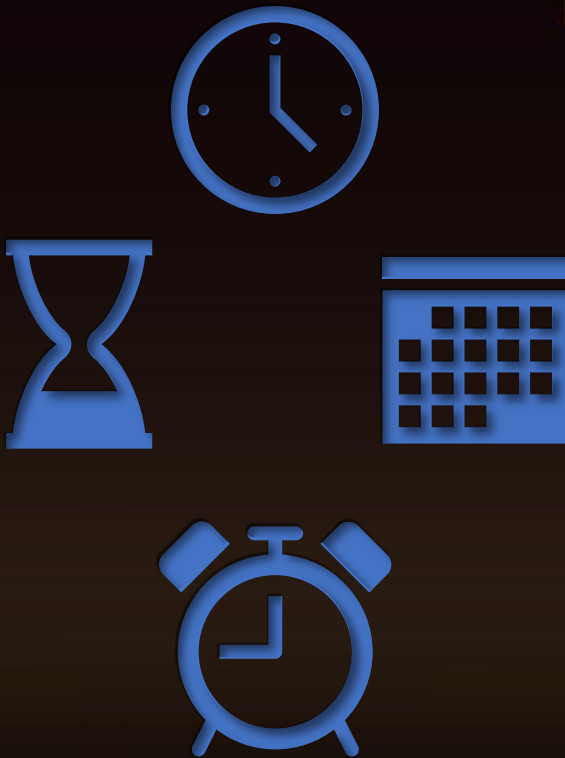
Exploit Lifespan

♦ In my experience:

- ♦ Browser bugs: ~6-12 months
- ♦ Other remote bugs: ~12-24 months
- ♦ Privilege escalations: ~12-24 months

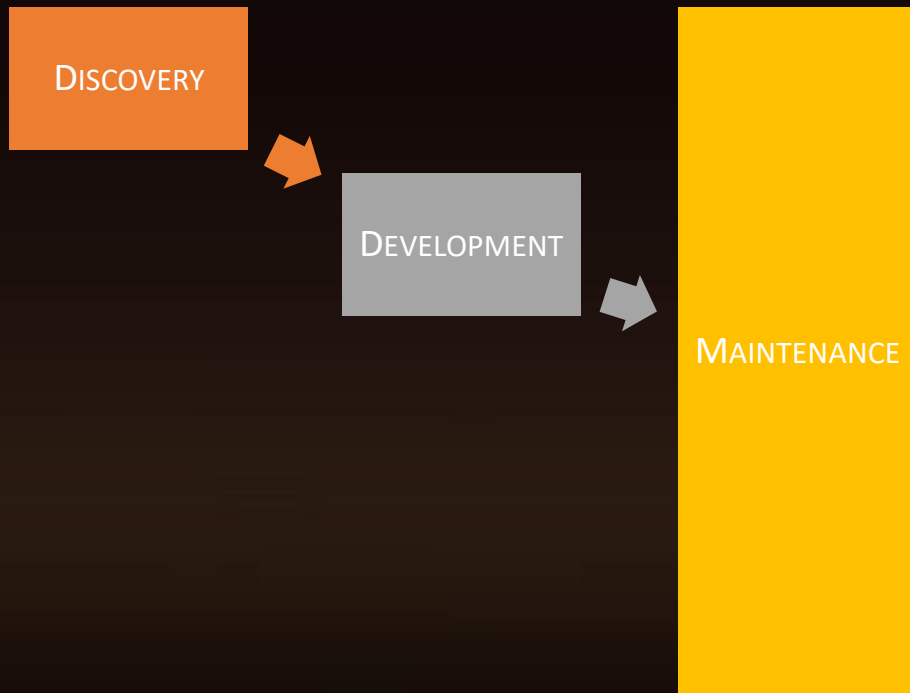
♦ Observations

- ♦ If the attack surface is publicized, all the bugs in that area tend to go quickly
- ♦ Patching a technique can impact all bugs at once



The Hoarding Myth

- ◇ It's expensive to buy multiple copies of the same thing when you don't need it
- ◇ HUGE maintenance burden (maintaining 5-10 exploits is a nightmare)
 - ◇ Most of that effort is wasted
- ◇ Often capabilities disappear at same time
 - ◇ Using common techniques
 - ◇ Subsystem is deprecated etc



Market vs Public Research

How do 0-day market products compare with public security research?

Public Research vs Market: Motivation

Defensive research is fuelled by **interest** (personal or commercial)

Offensive research is fuelled by **necessity**

Public Research vs Market: Focus

- ◆ Offensive tools have rigid requirements
- ◆ It has to work, and work reliably
 - ◆ Should work in the face of adverse conditions
- ◆ No noticeable side effects*
 - ◆ Locking up device, visual artifacts, etc
- ◆ Execution needs to continue as if nothing happened
- ◆ It (might) have to safely abort on failure

“Offensive tools are an outlier in the security product industry: They reliably do what they advertise they do” – Thomas Dullien

Public Research vs Market: Focus

- ◆ A lot of public research doesn't satisfy the criteria for the offensive market
 - ◆ Target is not interesting to customers
 - ◆ A lot of customers have a limited appetite for hacking Nest's
 - ◆ Too theoretical / impractical / academic
 - ◆ eg. Many of the side channel attacks
 - ◆ Other example: impractical requirements
 - ◆ Can't generate a reliable exploit
 - ◆ eg. Stagefright (2015)

PoC vs Commercial-Grade Exploit

- ◆ Most public exploits released are in Proof of Concept (PoC) form
 - ◆ Bug trigger
 - ◆ Exploit a particular OS version/device (semi-) reliably
 - ◆ Might omit significant challenges (ie. Write to file -> code execution)

Most PoC's you see released by researchers are not in a saleable condition

PoC vs Commercial-Grade Exploit

- ◇ 50+% of the effort improving reliability from 75% -> 95%
- ◇ Sometimes you need to completely rework solution
- ◇ Deployment concerns can be significant
 - ◇ Version detection & back-off
 - ◇ Generating logs
 - ◇ Other footprints



Going from PoC to exploit is most of the work!

Public Research vs Market: Who is ahead?

- ◇ In areas of common interest, market is typically 1-2 years ahead
 - ◇ Again, this is due to necessity
 - ◇ Also direct feedback loop: market researchers know first-hand what will work and what won't work in the wild
 - ◇ By comparison: Many of the ITW samples you see have been in existence for some significant period of time
- ◇ Every now and then, this is inverted when a public researcher reveals a new attack surface or exploit technique
 - ◇ Market researchers borrow good ideas and strategies
 - ◇ In some cases, public research sets off a wave of similar products

What about 3rd Party security Products?

- ◇ Less relevant than in the past
- ◇ Early market was Windows client-side
 - ◇ many ran McAfee, Kaspersky, etc
 - ◇ Some advanced post-exploitation detection techniques
- ◇ Main target now is mobile
 - ◇ Not much in the way of endpoint security products
 - ◇ Some enterprise security products but they're limited
- ◇ Larger threat now is detection by vendors (TAG, etc)

Capabilities

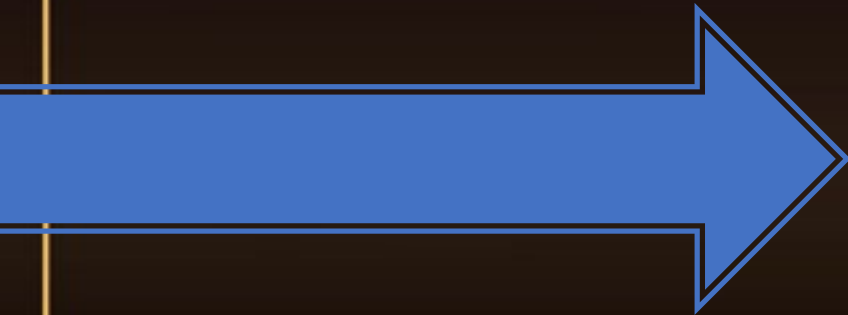
- ◆ Productization involves some or all of these steps:
 - ◆ Integration of all components
 - ◆ End-to-end testing
 - ◆ Payload, or front-end for customer to insert payload
 - ◆ Documentation
 - ◆ (Support)

Capabilities

- ◆ For less sophisticated customers, capabilities are the only option
 - ◆ Don't have the expertise to develop and integrate individual components
 - ◆ Need a “black box” essentially
- ◆ Not having a full chain can significantly decrease your potential customer market

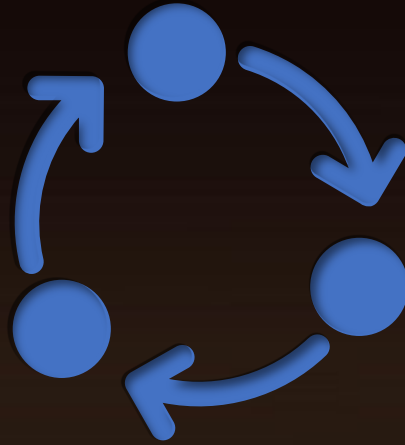
Exploit Lifespan

◆ Chains are much more complicated to maintain...



**If any of the components
stop working, the whole
chain is useless**

THE MARKET




The 0-Day Market

- ◆ It is a market much like any other, except you're working on partial information
- ◆ There are some significant inefficiencies
- ◆ Goods are highly time-sensitive
- ◆ It is high-risk, high-reward



Market Composition

♦ A common misconception is that the market is monolithic and/or regular



♦ Reality: Series of distinct markets that sometimes overlap

♦ Broken down by nation and/or geopolitical region (eg 5EYES, NATO)

- ♦ Each market is a microcosm
- ♦ Broken down by function (Intel, Military, Law Enforcement)
- ♦ Budgets, missions, and sophistication differ
- ♦ Different products are required although underlying tech is similar
- ♦ Pricing is also dramatically different for different markets

Market Composition

- ◆ A common misconception is that the market is monolithic and/or regular



◆ Result:

- ◆ Less sophisticated customers need a “point-and-click” black box, and cheap
- ◆ More sophisticated customers can deal with individual components or full capabilities, can deal with more complicated deployment scenarios, have their own payloads, etc
- ◆ All customers are at the mercy of the researchers who supply the product and also hold veto power over it, in perpetuity

The Players

Buyers

Government Agency

Vendor

Other
(crime, vigilantism)

First-tier Sellers

Productizer
(Defense contractor, VR
firm, some brokers)

Reseller (Broker)

Freelance Researchers

Second-tier Sellers

Some companies

Freelance Researchers

The Players

Buyers

Government Agency

Vendor

Other
(crime, vigilantism)

First-tier Sellers

Productizer
(Defense contractor, VR
firm, some brokers)

Reseller (Broker)

Freelance Researchers

Second-tier Sellers

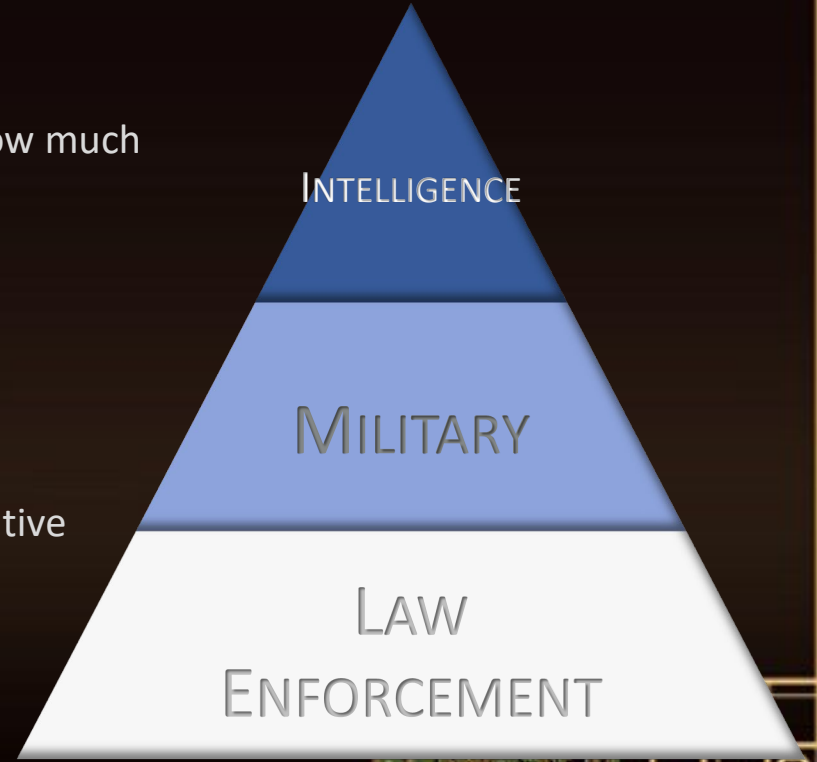
Some companies

Freelance Researchers

Buyers

Different markets are different sizes, inverse to how much of their mandate is accessing information

- ◇ Biggest market is government:
- ◇ Small number of intelligence purchasers
- ◇ Medium number of military purchasers
- ◇ Large number of law enforcement and investigative agencies



Buyers

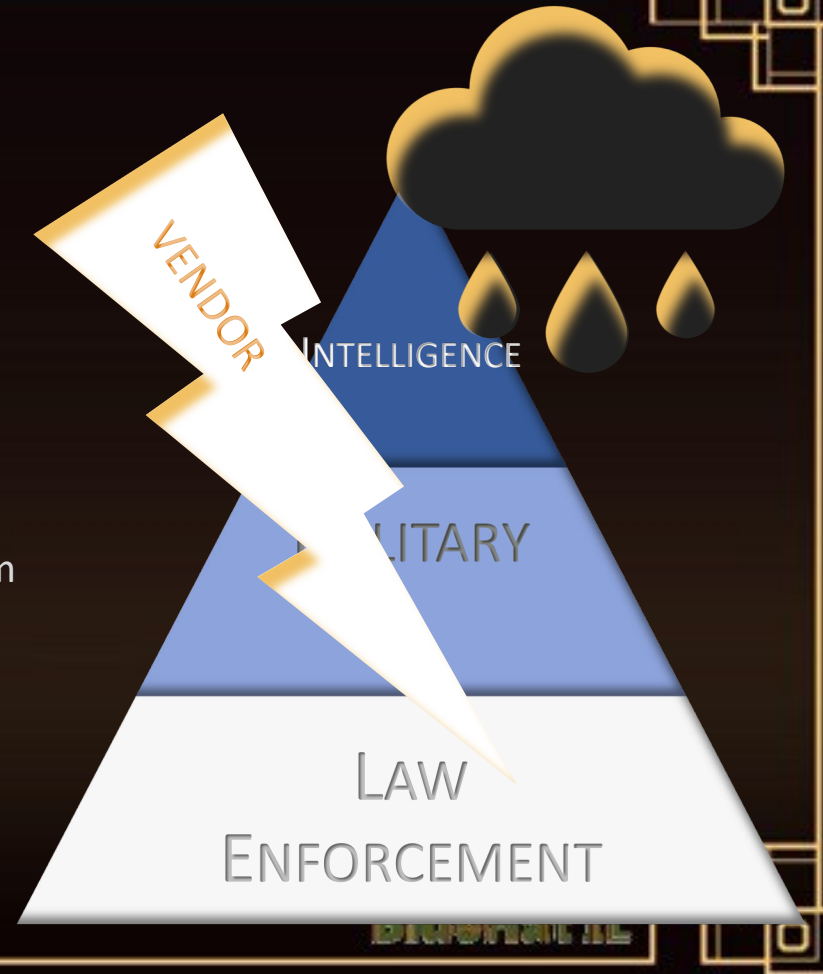
However their budget is proportionate to the size of their information mandate



Buyers

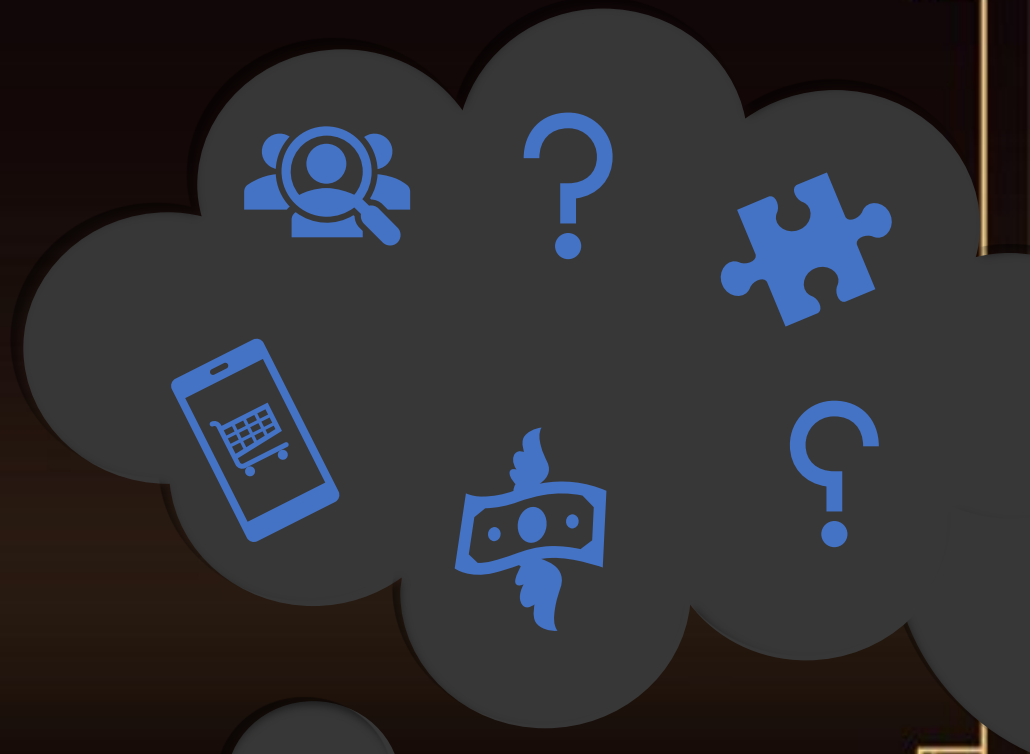
WILDCARD - VENDOR

- ♦ Vendors can remove the product anytime they discover it
 - ♦ Even accidentally
 - ♦ Without paying for it
- ♦ Also vendors can entice researchers to sell to them instead of alternatives
- ♦ This makes them part of the market



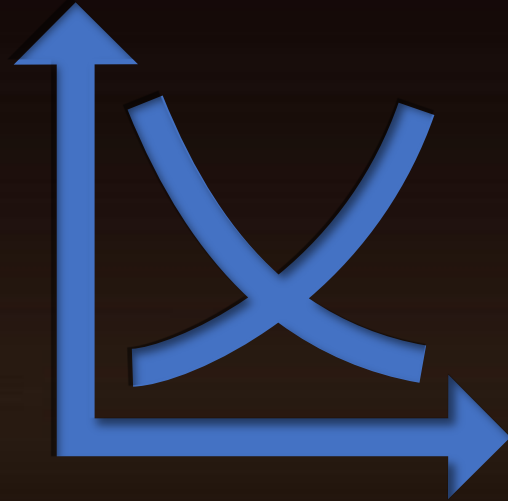
Market Composition

- ◆ The market(s) are opaque
 - ◆ Exact number of sellers is unknown
 - ◆ Reasonable estimates of buyers can be known
 - ◆ Budgets are (in some cases) not known



Market Size

- ◆ Some numbers for the US
 - ◆ 18 intelligence agencies
 - ◆ 45 doing intelligence with military and law enforcement
 - ◆ 17,985 law enforcement agencies (65 federal)
- ◆ But these are then split again
 - ◆ Intelligence: high price point, low volume
 - ◆ Law Enforcement: low price point, volume



Market Size

- ◇ Opaque, but in the billions of dollars
 - ◇ Defense dept cyber operations: \$4.4B FBI: \$123M

(<https://www.politico.com/newsletters/weekly-cybersecurity/2022/03/28/cybers-big-budget-week-00020739#:~:text=As%20for%20offensive%20tools%20and,total%20budget%20to%20%24123%20million>)

Market Size: Sellers

We did not know how many competitors we had

♦ In a compilation of 180 vendors:

- ♦ Doesn't include freelance researchers
- ♦ Includes now defunct companies
- ♦ Includes some companies more than once (eg. Azimuth and Trenchant)
- ♦ Not all of these are competitors (there are multiple markets)
- ♦ Overall it is not up to date or complete

<https://xorl.wordpress.com/offensive-security-private-companies-inventory/>

Market Size: Sellers

- ◆ My estimate:
 - ◆ ~2015: 10-20, including defense contractors
 - ◆ Now: 30-40
- ◆ Most vendors aren't premium providers

The Players

Buyers

Government Agency

Vendor

Other
(crime, vigilantism)

First-tier Sellers

Productizer
(Defense contractor, VR
firm, some brokers)

Reseller (Broker)

Freelance Researchers

Second-tier Sellers

Some companies

Freelance Researchers

The Players

Buyers

Government Agency

Vendor

Other
(crime, vigilantism)

First-tier Sellers

Productizer
(Defense contractor, VR
firm, some brokers)

Reseller (Broker)

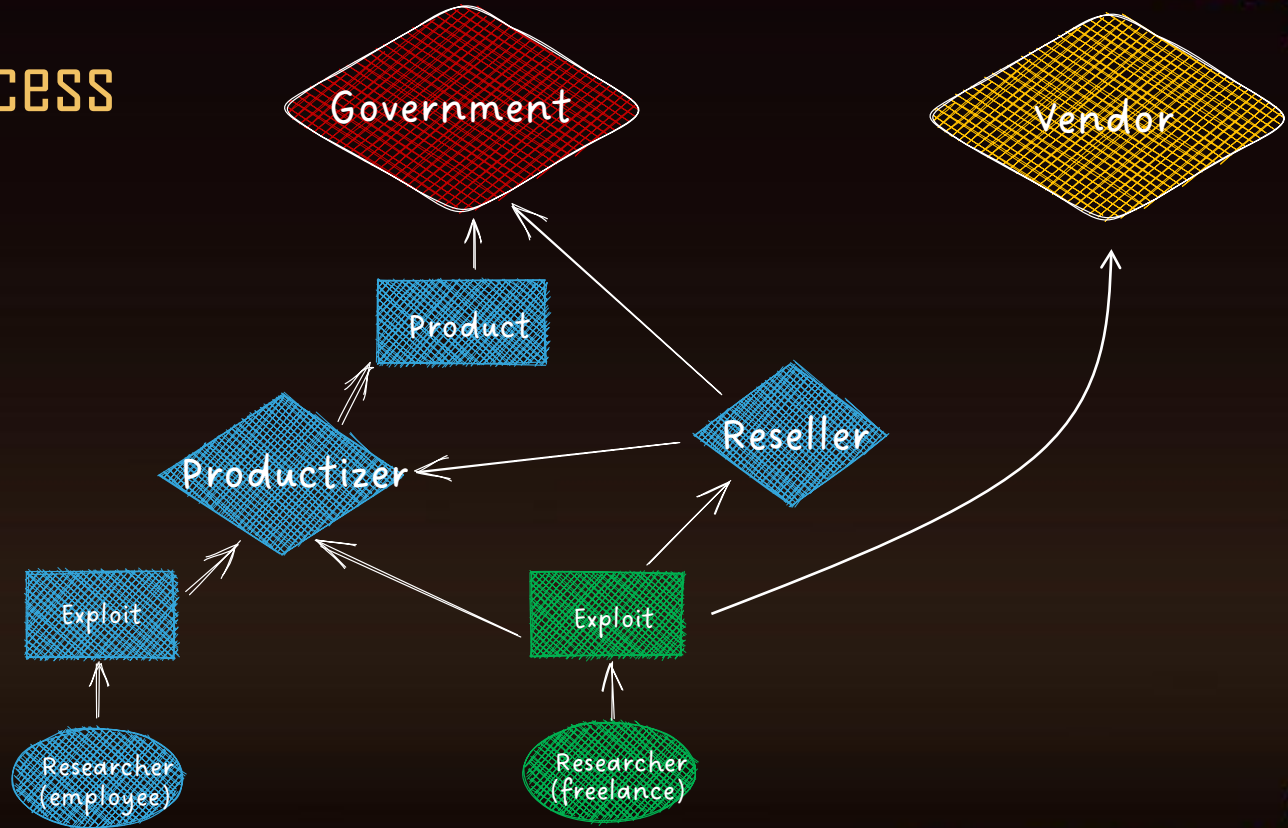
Freelance Researchers

Second-tier Sellers

Some companies

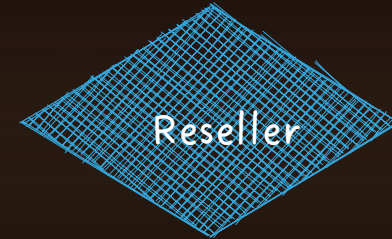
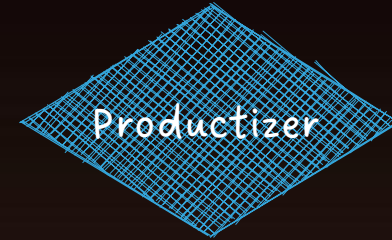
Freelance Researchers

The Sale Process



First Tier Suppliers - Intermediaries

- ◆ Comprised of companies whose primary purpose is the exploit market
- ◆ Can be broken in to roughly two classes of entities:
 - ◆ Productizers (create products, or buy products and value-add)
 - ◆ Reseller (buy products and resell them)



First Tier Suppliers - Intermediaries

◆ Productizers:

- ◆ Typically buy an exploit outright with an exclusive license
- ◆ Testing, integration (perhaps), reformat
- ◆ Sell to multiple customers or one customer at a markup

◆ Reseller:

- ◆ Typically list an exploit on behalf of a seller with sellers desired terms
- ◆ When a customer wants it, buy it and then immediately resell
- ◆ Take a small commission

First Tier Suppliers – Productizer and Reseller

IN COMMON

- ◆ Direct customer relationships
- ◆ Know exactly where their tools are going
- ◆ Verifies exploit exists
- ◆ Usually require clearance or to be mediated via clearance
- ◆ More flexibility in contract terms

DIFFERENCES

- ◆ Productizers generate their own exploits and incorporate additional work to produce a product
- ◆ Resellers do not do their own research or add code
- ◆ Productizers provide support and maintenance

First Tier Suppliers – Productizer

- ◆ Productizers deliver consistent quality and deliverable format
- ◆ Sources external exploits on spec (takes risk on purchase)
- ◆ Creates additional value by improving reliability or integrating into existing frameworks
- ◆ Verifies product with extensive testing
- ◆ Attempts to control the dissemination of the product by managing sales
- ◆ Typically stands to gain (or lose) more for a given transaction

The Players – Reseller

- ◇ Can only source exploits from the second tier sellers
- ◇ Typically does not buy the product with any exclusivity agreement
- ◇ Typically lacks testing infrastructure
- ◇ If a customer is interested they buy the product and immediately resell
- ◇ This involves little risk

Inconsistent quality
Product not extensively tested
Lower profit



The Players

Buyers

Government Agency

Vendor

Other
(crime, vigilantism)

First-tier Sellers

Productizer
(Defense contractor, VR
firm, some brokers)

Reseller (Broker)

Freelance Researchers

Second-tier Sellers

Some companies

Freelance Researchers

Suppliers - Researchers

Nearly all researchers come from the general research community. Whether their work becomes commercialized depends on a few factors:

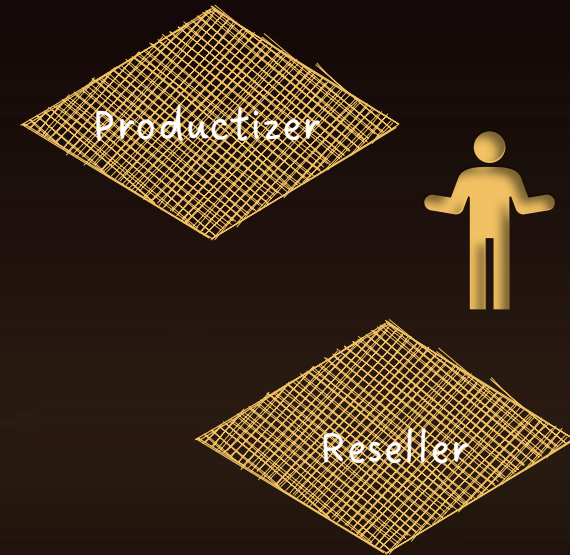
- ♦ Public research is largely powered by interest. So:
 - ♦ Their areas of interest may not be relevant to most customers
 - ♦ They may create solutions that are not practical in the wild
 - ♦ Cannot develop a reliable product
- ♦ Academic research is typically open by its very nature
- ♦ And vendor research is in-depth but narrowly targeted



This leaves a very small pool of potential suppliers because they are the only ones whose work is: relevant, reliable, and discreet.

Suppliers - Researchers

- ◆ Comprised of individual researchers (and some small partnerships)
- ◆ If not selling to the vendor, they:
 - ◆ Usually sell to productizer or reseller intermediary
 - ◆ Have less insight into where tools are going
 - ◆ Have less ability to capitalize because they are usually “answers looking for a question”



Suppliers - Researchers

- ◆ Why use intermediaries?
- ◆ Significant barriers to enter the market directly:
 - ◆ Customers opaque – difficult to get direct access to
 - ◆ Constraints on who they deal with – clearances, citizenships, etc
 - ◆ Monetary risk (products are volatile, deals are slow)
 - ◆ Business side is time consuming

Suppliers - Researchers

♦ Why sell to the vendor?

- ♦ Bug bounties are (now) a substantial market force
- ♦ Transaction expected to be quick and easy
- ♦ No minimum complexity hurdle – a bug is a bug
- ♦ Free feedback
- ♦ Ability for publicity, self-promotion, or glory
- ♦ No moral or legal ambiguity



(Plenty of Oday market participants also dabble in bounties)

The Sale Process – Researcher



The Sale Process: Problems

- ◆ Once code is submitted, the researcher risks being cheated or threatened
 - ◆ Not a huge risk unless working with unsavoury outfits
 - ◆ Motivation for the intermediary to do this is low: lose the researcher's faith and they can burn the exploit by selling to the vendor or otherwise publicly revealing it
 - ◆ The vendor can threaten legal or criminal consequences. But this is unlikely now that the market has matured and there is a set cultural expectation for behaviour and dialogue.
- ◆ What about duplicates?
 - ◆ Non-fatal in this market
 - ◆ Sometimes people buy duplicates to keep the bugs out of circulation
 - ◆ Happens pretty infrequently

PRICING



Market Forces

Product is unusual because of its opaqueness:

- ◆ It may or may not exist elsewhere
- ◆ It can be exclusive but doesn't have to be
- ◆ It could or could not exist tomorrow – and those who know about it always have the ability to burn it

HOWEVER

the normal rules of business and economics still apply

Power of the Researcher

The Researchers:

◆ Have huge power:

- ◆ Exceptionally rare skill
- ◆ Requiring certain motivations and personality
- ◆ Very hard to replace or switch

◆ Possible to motivate and entice with various motivators:

- ◆ Money
- ◆ Fame and glory
- ◆ Mission and morality
- ◆ Lifestyle

When insufficient in one, the motivators can sometimes be compensated by the others

Power of the Researcher

There are choices if they don't want to work for a productizer:

Full-time tech employment


- ◆ Prestige for future career progress
- ◆ Good salary and some reliability
- ◆ Ability to have a public profile
- ◆ Variety of opportunity

Life of crime

- ◆ Don't know this market
- ◆ Possibly lucrative, but your family has to visit you in non-extradition countries

Working in the public sector

- ◆ Sense of purpose
- ◆ Interesting work
- ◆ No public profile – stay under the radar
- ◆ Near guaranteed results somehow, somewhere, for some things, sometimes



You guys
are here!

Competitors to the Intermediaries

- ◇ Unusual expression of competitive rivalry:
 - ◇ All sellers operate in an black box market – both buyers and sellers are not supposed to reveal any information about the products
 - ◇ Occasional leaks of information provide glimpses
 - ◇ Reaction of buyers reveals some information about pricing
- ◇ Overall sellers are unable to make decisions based on the movements of competitors, except intermittently

market equilibrium is reached without price signaling

Competitors to the Intermediaries

- ◆ Vendor's bug bounties also compete with the intermediaries
- ◆ Researchers could make more in Oday market, but there is decent money with pwn2own etc
 - ◆ Excellent for public profile
 - ◆ Plenty of Oday market participants also dabble in bounties
 - ◆ The payouts are generally lower, but the requirements are significantly less

Economics

From the perspective of the 0-day market productizer:

- ◇ The strength of the customer in the market is balanced by the desirability of the products and their rarity.
 - ◇ If the product is good, the productizer or relister has a lot of power.
- ◇ The suppliers (researchers) have extraordinary power in this market.
 - ◇ They are rare, difficult to replace, and infeasible to train. Their salaries almost entirely set both the cost of doing business and the price of the products.
- ◇ There is little threat of new competitors.
 - ◇ The cost of the suppliers sets the bar exceptionally high. There remains a small risk of an instant overnight competitor sprouting from a colossal moonshot investment or a cluster of prodigy geniuses banding together.

Economics

From the perspective of the 0-day market productizer:

- ◇ There is a constant threat of the customer seeking substitute products.
 - ◇ But this stems primarily from the ever-present risk that a product breaks without notice. The customer is then compelled to find a substitute. However, this substitute may or may not immediately exist.
- ◇ There may be many competitors in the market, but it is mostly opaque to the productizers and relisters.
 - ◇ So any competition in the market is set by an implicitly negotiated equilibrium between the intermediaries and the customer.

**“HOW MUCH IS A AN
EXPLOIT FOR XYZ
WORTH?”**

- EVERYONE

Common Question



Answer: To whom?

Common Question

- ♦ Media conflates seller price and buyer price
- ♦ The most complex exploits are confused for basic ones
- ♦ Misunderstanding of the price levers

0-Day Pricing Movers

- ◇ Desirability
- ◇ Quality
- ◇ Terms
- ◇ Scarcity



HIGH VARIANCE

Pricing: Desirability

- ◇ How necessary is it in order to complete the customer's goals?
- ◇ How useful is an exploit of a given type?
- ◇ How difficult is it to deploy?

Vendor is generally unmoved by this lever



Pricing: Necessity

- ◆ If a buyer needs something, the seller can charge more than a “nice to have”
- ◆ The more urgent the necessity, the more the seller can charge (assuming no substitutes)

Pricing: Usefulness

- ◇ Different buyers have different products that are of value to them
- ◇ An exploit for a phone predominately used in another country might be of value to intelligence, but not law enforcement
- ◇ Different attack vectors have greater use to different customers
 - ◇ A browser chain might be of high value to Intelligence, but less so to a local police force

Pricing: Deployment

Source:
<https://zerodium.com/program.html>

ZERODIUM Payouts for Mobiles*											
Up to \$2,500,000											
Up to \$2,000,000											
Up to \$1,500,000											
Up to \$1,000,000											
Up to \$500,000	3.001 Persistence IOS	2.005 WeChat RCE+LPE IOS / Android	2.006 iMessage RCE+LPE IOS	2.007 FB Messenger RCE+LPE IOS / Android	2.008 Signal RCE+LPE IOS / Android	2.009 Telegram RCE+LPE IOS / Android	2.010 Email App RCE+LPE IOS / Android	4.001 Chrome RCE+LPE Android	4.002 Safari RCE+LPE IOS	1.001 Android FCP Zero Click Android	1.002 iOS FCP Zero Click IOS
Up to \$200,000	5.001 Baseband RCE+LPE IOS / Android		6.001 LPE to Kernel/Root IOS / Android	2.011 Media Files RCE+LPE IOS / Android	2.012 Documents RCE+LPE 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	2.001 WhatsApp RCE+LPE Zero Click IOS / Android	2.002 iMessage RCE+LPE Zero Click IOS
Up to \$100,000	7.001 Code Signing Bypass IOS / Android	5.002 WiFi RCE IOS / Android	5.003 RCE via MitM IOS / Android	6.002 LPE to System Android	8.001 Information Disclosure IOS / Android	8.002 [k]ASLR Bypass IOS / Android	9.001 PIN Bypass Android	9.002 Passcode Bypass IOS	9.003 Touch ID Bypass IOS		

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/09 © zerodium.com

Pricing: Deployment

Baseband RCE + LPE can be done two ways:

- ◆ Rogue base station

- ◆ Requires physical proximity
- ◆ Often downgrade to 2G
- ◆ Integrate exploit with base station product

- ◆ Via the carrier

- ◆ With carrier assistance (only useful for in-country agencies)
- ◆ Without carrier assistance (requires hacking a telco)
- ◆ Lots of integration issues – each carrier is unique

Pricing: Deployment

OR...

- ◆ iMessage RCE deployment
 - ◆ Point and click, works everywhere

PRICE DIFFERENCE: \$300K – \$1.3M

Pricing: Quality

- ◆ Reliability and guarantees
- ◆ Product Features

**Exploits are not
all created equal**



Pricing: Quality

- ◆ Affected device/OS range
- ◆ Reliability
- ◆ Side effects
- ◆ Deployment complications
 - ◆ Fingerprinting
 - ◆ Encryption
- ◆ Lifetime expectation
- ◆ Maintenance burden

Pricing: Product Features

- ◆ Zerodium chart
 - ◆ Android FCP example: “You will make UP TO \$2.5M”
- ◆ “UP TO” is doing a lot of work here

Pricing: Product Features

- ◇ Example: “I have a remote zero-click Android exploit”
 - ◇ Which android? (Samsung flagships? Exynos or QC? Pixel? etc)
 - ◇ How reliable is it? What happens when it fails?
 - ◇ Can you fingerprint the target? What happens if you deploy it against a non-vulnerable target?
 - ◇ Does it require MITM of some kind for deployment?
 - ◇ How easy is it for the vendor to catch?
 - ◇ Does it produce side effects (lock up device, prompt, etc)?
- ◇ Price could range from \$0 -> \$2.5M!

Pricing: Terms

- ◇ Exclusivity vs non-exclusivity
 - ◇ Customers would all prefer exclusive sales
- ◇ Most sales to end customers are semi-exclusive
 - ◇ Most common: anyone within 5-eyes/NATO
 - ◇ Sometimes limited to a single country
 - ◇ Sometimes specific to branch (intel vs law enforcement etc)

Pricing: Terms

- ◆ Non-exclusive sales: potential higher profit, but higher risk
 - ◆ Usually sell at about half price, profit after 2 or 3 sales
 - ◆ Much higher income potential, but might get patched before passing break-even point
 - ◆ Some customers might be less inclined to buy it depending on who else you sell it to

Pricing: Terms

- ◆ Maintenance negotiation is also part of pricing
 - ◆ Often some agreement for fixed-term maintenance (while exploit is still viable)
 - ◆ Maybe an additional ongoing fee for maintenance
- ◆ Payment can also be on a schedule (relatively common)
 - ◆ Eg. 50% up front, 25% a month later, 25% two months later
 - ◆ If exploit dies in that time, further payments are terminated
 - ◆ Risk mitigation for acquirer, possibly higher total potential price for seller

Pricing: Scarcity

- ◆ The more rare a (desirable) capability, the more it's worth
 - ◆ Inverse rule the same, can even go to 0
- ◆ Something required urgently also can command a higher price
 - ◆ Time-sensitive operation in need of a solution
- ◆ Scarcity changes frequently and suddenly
 - ◆ Particularly true when a major shared capability/attack surface is burned

Pricing: Scarcity

- ◆ Scarcity can be due to a dearth of sellers too
 - ◆ The less options the buyer has, the more they are at the mercy of sellers aggressive pricing
 - ◆ Example: Saudi Arabia reportedly paid significantly more for Pegasus than other countries

Pricing: Myth Busting

- ◇ Myth: You can always sell a bug
- ◇ Reality:
 - ◇ Significant number of developed exploits fail to ever sell
- ◇ Reasons for failure to sell:
 - ◇ Customers already have it (scarcity is low)
 - ◇ Patched / rendered unexploitable before sale
 - ◇ Features / deployment issues make it undesirable to customers
 - ◇ Other (eg. Budget depleted)

Pricing: Myth Busting

- ◇ Myth: “I found 5 bugs in Chrome, at 600k each, I will make \$3M!”
- ◇ Reality: You will likely sell only one or two of these
- ◇ Reasons:
 - ◇ Customer needs filled – customers do not hoard!
 - ◇ Reasons listed for previous myth

Pricing: Myth Busting

- ◆ Partial Myth: “Zerodium is buying X for \$1M, so the end buyer is buying it for more, maybe much more!”
- ◆ Reality: That is a possibility, or they might be making money on multiple sales of the same item

Pricing: Myth Busting

- ◇ Partial Myth: Oday exploit prices are a reliable barometer for how effective security mitigations are for a given product
- ◇ Reality:
 - ◇ Within a given category, this is somewhat true
 - ◇ Price also might be affected by:
 - a current scarcity
 - a particular mission
 - some market movement (“iPhones all now use Qualcomm basebands”)

Sales Examples

- ◇ Product: Chrome Oday RCE (no sandbox)
 - ◇ Assumptions: reliable and works on both Windows and Android
- ◇ Market
 - ◇ Relatively sophisticated customers (no chain, needs integration)
- ◇ Price
 - ◇ Depending on market, anywhere from \$200-\$800k
 - ◇ Usually around \$300k

Sales Examples

- ◆ Product: Exynos Baseband chain

- ◆ Assumptions: reliable and work on flagship Samsung devices

- ◆ Market

- ◆ Sophisticated (unless base station is supplied as all-in-one product)
 - ◆ Agencies operating in countries where Samsung use Exynos (Europe)

- ◆ Price

- ◆ Depending on market, anywhere from \$500k - \$1M
 - ◆ Usually around \$700k

Sales Examples

- ◆ Product: Graykey (iPhone USB-based unlocking device)

- ◆ Assumptions: reliable and work on flagship iOS-based devices

- ◆ Market

- ◆ Unsophisticated – point and click

- ◆ Targeted specifically at law enforcement with small budgets

- ◆ Price

- ◆ \$18k - \$40k*

The Future of the Market

- ◇ The market is currently dominated by memory corruption exploits
- ◇ Memory corruption exploits are in trouble
 - ◇ H/W + S/W mitigations are rendering many bugs unexploitable
 - ◇ Reliability is also often a significant issue
 - ◇ Difficulty is increasing while lifespan is shrinking
 - ◇ Level of compromise is also shrinking
- ◇ Result: Chains for high-value devices will become scarce

The Future of the Market

- ◆ **Prediction: Full or close to full compromises will go through the roof**

 - ◆ \$10M+

- ◆ **Prediction: Offensive companies will collaborate/merge**

 - ◆ Collaboration becomes more beneficial than competition

 - ◆ Smaller/less-skilled operations will likely exit, or pivot

- ◆ **Prediction: Customers will also pool resources**

 - ◆ Cost becomes prohibitive for minor players

The Future of the Market

- ◇ Re-examining the value of memory corruption bugs
 - ◇ Traditionally used because they yield the largest compromise
 - ◇ Is this still the case? By how much?
 - ◇ Even if so, is it worth the cost?
- ◇ Prediction: Buyers (particularly minor ones) will opt for lower-compromise / cheaper solutions
 - ◇ Target non memory corruption flaws that yield limited compromise
 - ◇ Web-style bugs, logic flaws, etc
 - ◇ Interest in lower-tier devices

The Future of the Market

- ♦ **Prediction: High demand for authentication bypasses/crypto weaknesses**
 - ♦ Potential to yield the highest level of compromise
 - ♦ Unsure how these will be priced – maintenance often isn't really required
- ♦ **Prediction: Huge interest in cloud-based compromises**
 - ♦ Accessing your google/Apple/WeChat account might be much more beneficial that targeting any one device
 - ♦ Caveat: Presents some sticky legal questions – might not be feasible

The Future of the Market: Biggest Unknowns

- ◆ Legal / Policy changes
 - ◆ Hacking cloud infrastructure – who can do this and when?
 - ◆ Probably largely illegal, but not for your adversaries!
 - ◆ Tightened export controls – who can sell to where?
 - ◆ Exacerbate talent shortage

The Future of the Market: Biggest Unknowns

- ♦ AI – Will offense/defense just be two ChatGPT's playing chess?
 - ♦ My guess: AI with human with in-depth domain knowledge will be a powerful combination
 - ♦ Dramatically cut down time for some tasks (RE, looking for specific patterns, coding tasks)
 - ♦ Still need talented researchers, but less of them

Summary

- ◆ Exploit market is complex
- ◆ High-risk, high reward
- ◆ It's about to get crazy
- ◆ Questions?

