Pricing Software Vulnerabilities: Public, Private, and Black Markets

Bryce Downing

What is a Software Vulnerability?

First step in the chain of exploit development

- Vulnerability -> Payload -> Distribution Mechanism

Can be within Software or Hardware

Allows for unintended access to data, user commands, or root

Why Pay for Vulnerabilities?

To Develop Exploits

- To either use or sell

To patch your software and remove the vulnerability

- Explicitly done to prevent those who would develop exploits from doing so

To Resell

- To someone who will do one of the aforementioned two actions with it

Pricing for Private Sector

Motivation

- Reselling
  - Opaque market for vulnerabilities
- Patching Vulnerabilities
  - Prevent theft of company resources
  - Prevent liability in case of theft of customer resources

Analogs

- Insurance
  - Unlike insurance however, it is often difficult to determine how likely a vulnerability is to be found and exploited

Complicating factors

- Lack of legal precedent surrounding standards of care regarding consumer data
- Costs of not storing consumer data

Google Bug Bounties

Category	Examples	Applications that permit taking over a Google account [1]	Other highly sensitive applications [2]	Normal Google applications	Non-integrated acquisitions and other sandboxed or lower priority applications [3]
Vulnerabilities giving direct access to Google servers					
Remote code execution	*Command injection, deserialization bugs, sandbox escapes*	$31,337	$31,337	$31,337	$1,337 - $5,000
Unrestricted file system or database access	*Unsandboxed XXE, SQL injection*	$13,337	$13,337	$13,337	$1,337 - $5,000
Logic flaw bugs leaking or bypassing significant security controls	*Direct object reference, remote user impersonation*	$13,337	$7,500	$5,000	$500
Vulnerabilities giving access to client or authenticated session of the logged-in victim					
Execute code on the client	Web: *Cross-site scripting* Mobile / Hardware: *Code execution*	$7,500	$5,000	$3,133.7	$100
Other valid security vulnerabilities	Web: *CSRF, Clickjacking* Mobile / Hardware: *Information leak, privilege escalation*	$500 - $7,500	$500 - $5,000	$500 - $3,133.7	$100

Pricing for Black Market

Motivation

- Developing Exploits

Analogs

- Traditional Economics of Crime
  - Traditional costs of business
  - Lack of traditional legal protections
  - Potential for legal punishment

Complications

- Developer vs Deployer attribution problems
- State/Criminal Attribution problems

Black Market Zero Day Pricings

Zero-Day Prices Over Time

Service	Price	Year
"Some exploits"	$200,000–$250,000	2007
"Weaponized exploit"	$20,000–$30,000	2007
A "real good" exploit	$100,000	2007
Microsoft Excel	> $1,200	2007
Mozilla	$500	2007
Vista exploit	$50,000	2007
WMF exploit	$4,000	2007
ZDI, iDefense Purchases	$2,000–$10,000	2007
Adobe Reader	$5,000–$30,000	2012
Android	$30,000–$60,000	2012
Chrome or Internet Explorer	$80,000–$200,000	2012
Firefox or Safari	$60,000–$150,000	2012
Flash or Java Browser Plug-ins	$40,000–$100,000	2012
iOS	$100,000–$250,000	2012
Mac OSX	$20,000–$50,000	2012
Microsoft Word	$50,000–$100,000	2012
Windows	$60,000–$120,000	2012

Pricing for Public Sector

Motivation

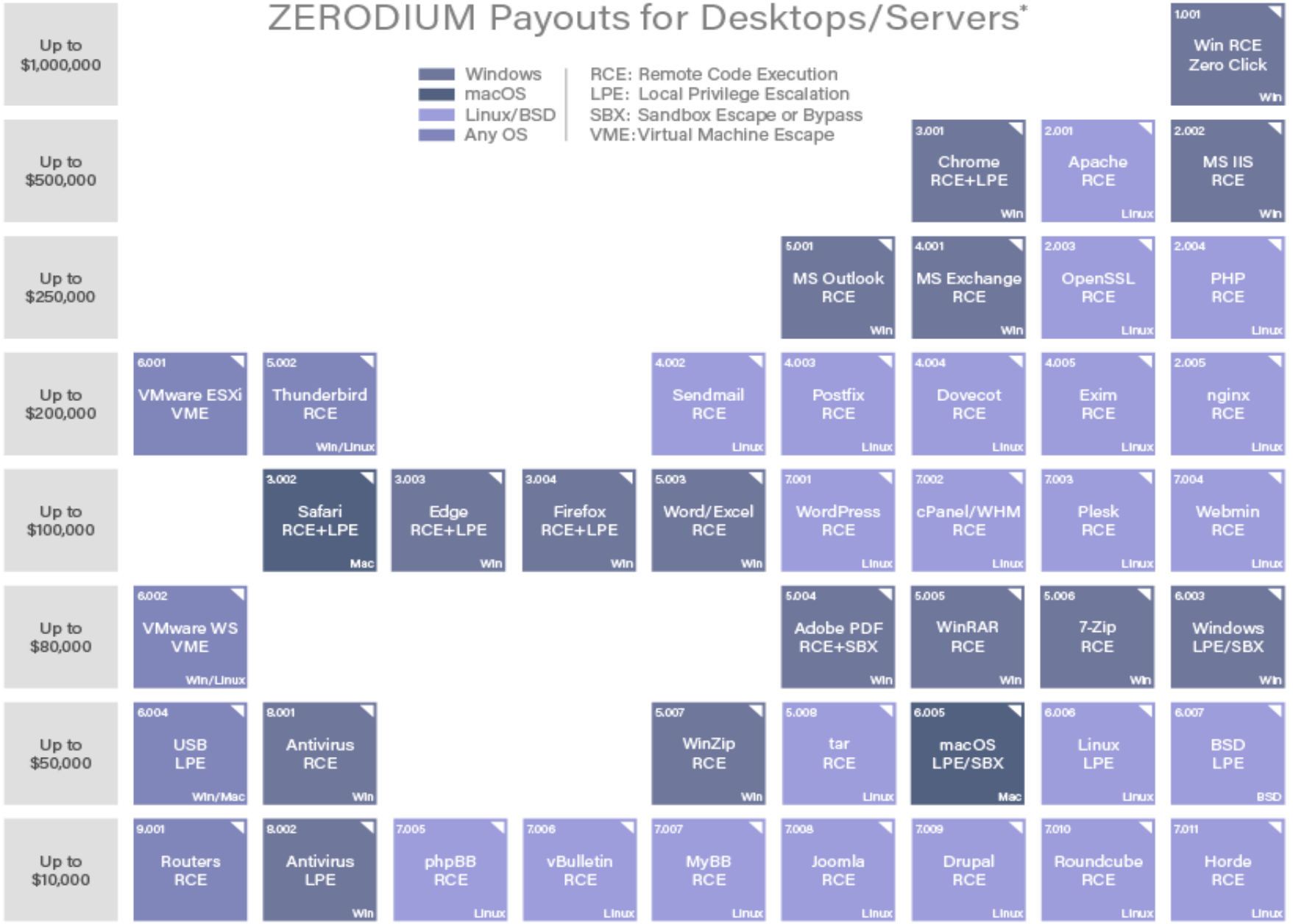
- Patching Vulnerabilities
- “NOBUS”

Analogs

- Undercover Law Enforcement Officers
- Arms Control Agreements

Complications

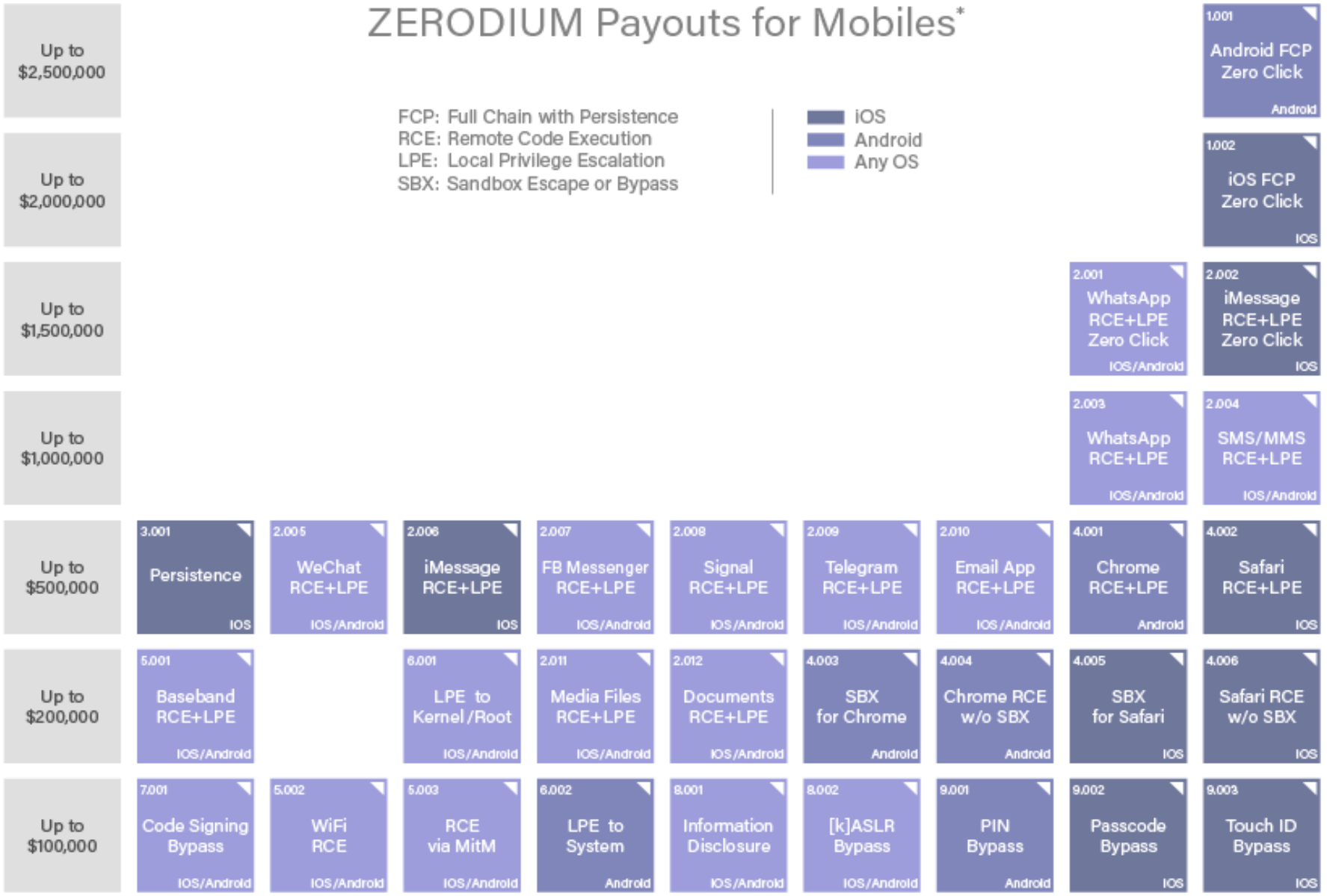
- No good analogs
- Tradeoffs between security and developing exploits
  - If critical systems can be insulated without patching the exploit, these tradeoffs can sometimes be negated


ZERODIUM Payouts for Desktops/Servers*
Windows
macOS
Linux/BSD
Any OS
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape
Up to $1,000,000
1.001 Win RCE Zero Click Win
Up to $500,000
3.001 Chrome RCE+LPE Win
2.001 Apache RCE Linux
2.002 MS IIS RCE Win
Up to $250,000
5.001 MS Outlook RCE Win
4.001 MS Exchange RCE Win
2.003 OpenSSL RCE Linux
2.004 PHP RCE Linux
Up to $200,000
6.001 VMware ESXi VME
5.002 Thunderbird RCE Win/Linux
4.002 Sendmail RCE Linux
4.003 Postfix RCE Linux
4.004 Dovecot RCE Linux
4.005 Exim RCE Linux
2.005 nginx RCE Linux
Up to $100,000
3.002 Safari RCE+LPE Mac
3.003 Edge RCE+LPE Win
3.004 Firefox RCE+LPE Win
5.003 Word/Excel RCE Win
7.001 WordPress RCE Linux
7.002 cPanel/WHM RCE Linux
7.003 Plesk RCE Linux
7.004 Webmin RCE Linux
Up to $80,000
6.002 VMware WS VME Win/Linux
5.004 Adobe PDF RCE+SBX Win
5.005 WinRAR RCE Win
5.006 7-Zip RCE Win
6.003 Windows LPE/SBX Win
Up to $50,000
6.004 USB LPE Win/Mac
8.001 Antivirus RCE Win
5.007 WinZip RCE Win
5.008 tar RCE Linux
6.005 macOS LPE/SBX Mac
6.006 Linux LPE Linux
6.007 BSD LPE BSD
Up to $10,000
9.001 Routers RCE
8.002 Antivirus LPE Win
7.005 phpBB RCE Linux
7.006 vBulletin RCE Linux
7.007 MyBB RCE Linux
7.008 Joomla RCE Linux
7.009 Drupal RCE Linux
7.010 Roundcube RCE Linux
7.011 Horde RCE Linux
* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.
2019/01 © zerodium.com

ZERODIUM Payouts for Mobiles*

FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

iOS
Android
Any OS



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

Competition Between Buyers

Price

- Should also remember that unlike in public and private sector bug bounty programs, exploits can be sold multiple times on the black market

Legal Punishment

- Difficult to accurately price in given short lifespan of black markets for exploits and the obfuscating effects of the exploit development chain

Use Preference

- Hackers have a history of fairly unique use preferences (e.g. open source software)

Ease of payment

- While illicit activities have additional transaction costs and risk due to their illegal nature public and private bug bounty programs often have fairly lengthy verification processes and opaque pricing schemes that can delay and reduce payment

Potential Frameworks for Competition Among Buyers

Traditional Auctions

- Most actors in Auctions don't derive their utility exclusively from depriving another actor of the object
- Still potentially useful to help with pricing

Bribes/Ransom Insurance

- While you can't ensure that that vulnerabilities won't be found and exploited you can pre-pay to reduce your exposure to potential threats by paying more than nefarious actors
- Doesn't account for dual use for public sector buyers

Future Investigation

Obtain more current data on black market and public sector zero day sales

Specifically identify both monetary and non-monetary changes to improve competitiveness of public and private bug bounty programs

Identify additional potential frameworks for the combined market for zero days

Test various frameworks on updated data

Use results from these tests in conjunction with monetary and non-monetary levers identified earlier to inform others

Sources

https://zerodium.com/program.html

Ablon, Lillian, Martin C. Libicki, and Andrea M. Abler, Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. Santa Monica, CA: RAND Corporation, 2014. https://www.rand.org/pubs/research_reports/RR610.html. Also available in print form.

https://www.google.com/about/appsecurity/reward-program/

Putting Auction Theory to Work – Paul Milgrom 2004

The economics of crime – Gary Becker 1995