CSC 405
Computer Security

Alexandros Kapravelos
akaprav@ncsu.edu

Why take a course in computer security?

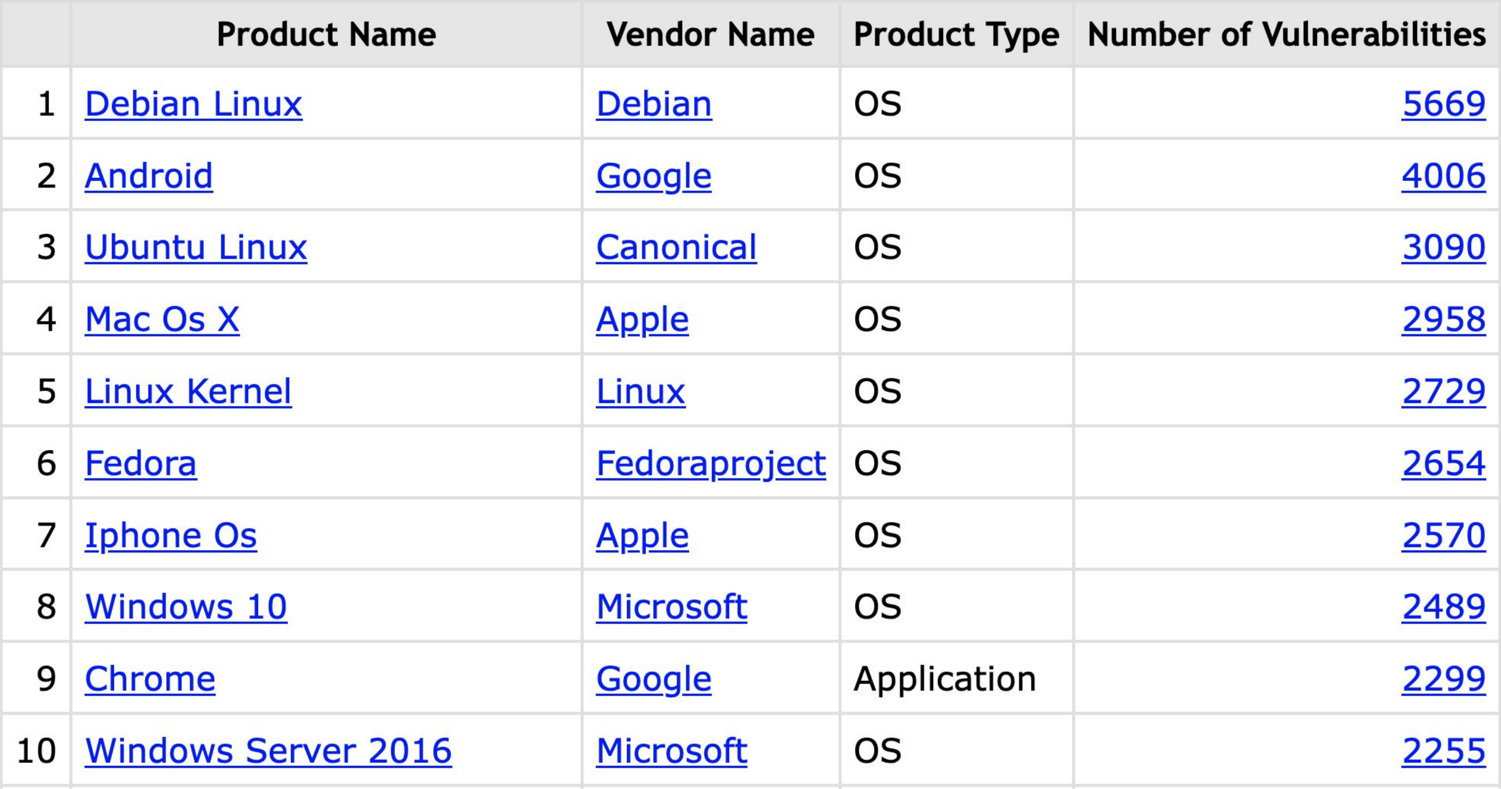
The computer security problem

- Security is everywhere (like the Matrix)
- Developers are not aware of security (we should fix this!)
  - Buggy software
  - Legacy software
  - Social engineering
- Vulnerabilities can be very damaging (and expensive)

Hacking used to be cool

But now everything is done for profit!

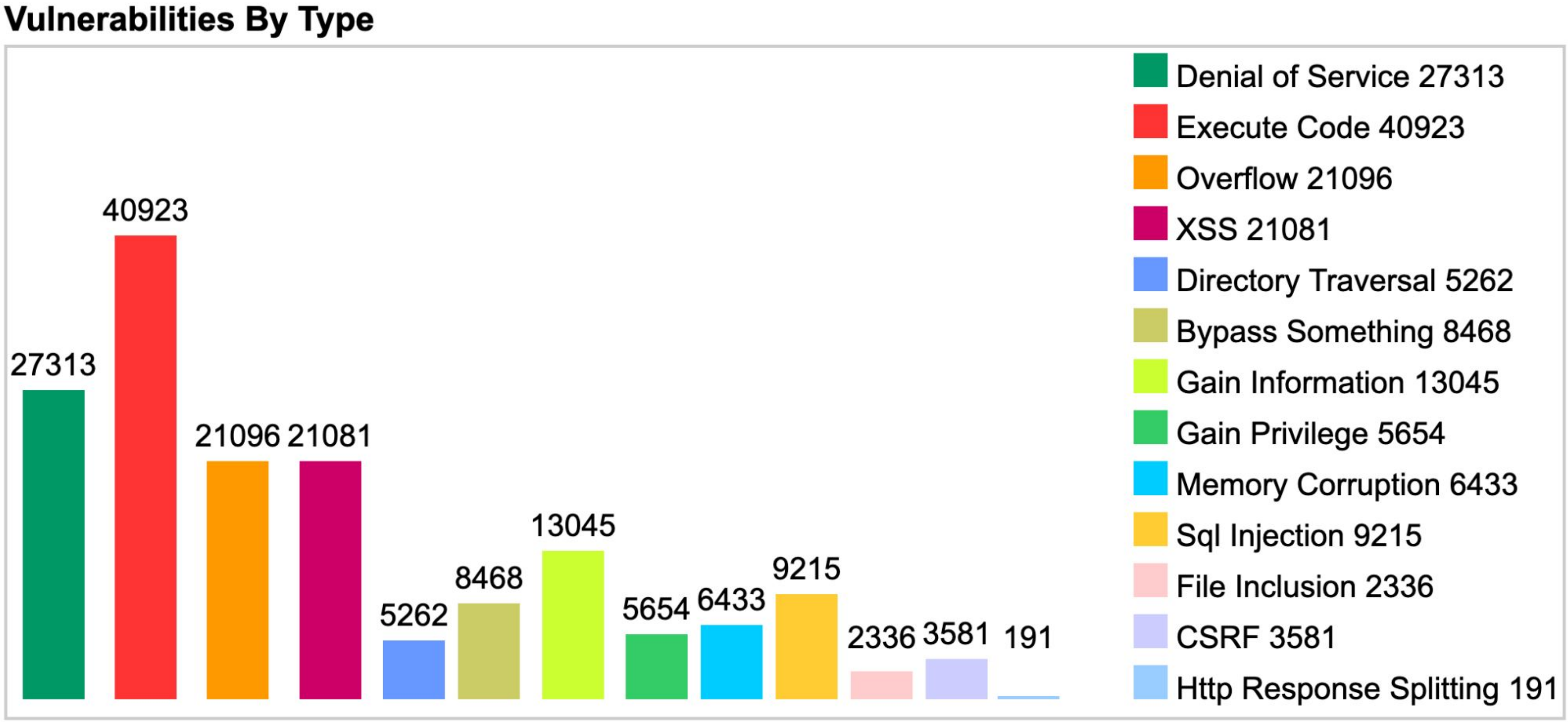
Vulnerabilities per product - 2021



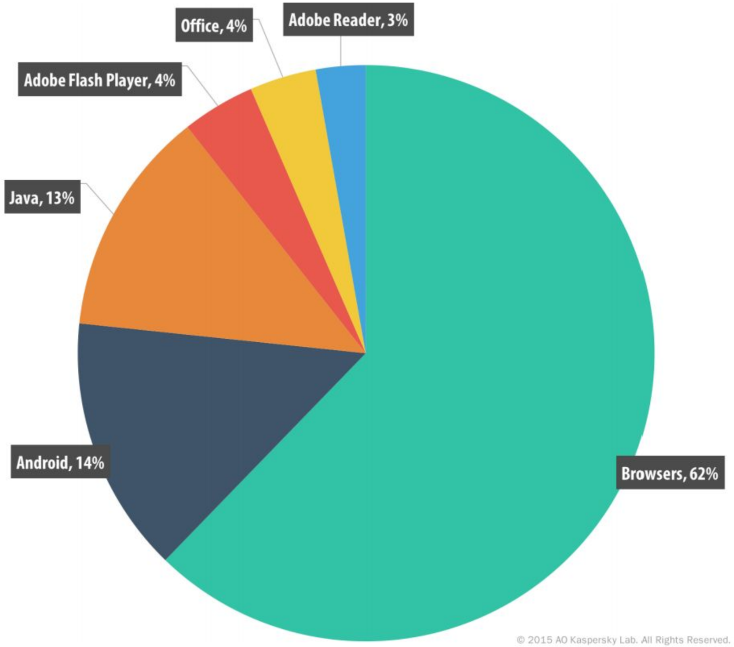
	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Debian Linux	Debian	OS	5669
2	Android	Google	OS	4006
3	Ubuntu Linux	Canonical	OS	3090
4	Mac Os X	Apple	OS	2958
5	Linux Kernel	Linux	OS	2729
6	Fedora	Fedoraproject	OS	2654
7	Iphone Os	Apple	OS	2570
8	Windows 10	Microsoft	OS	2489
9	Chrome	Google	Application	2299
10	Windows Server 2016	Microsoft	OS	2255

Source: https://www.cvedetails.com/top-50-products.php?year=2021

Vulnerabilities per type - 1999-2021

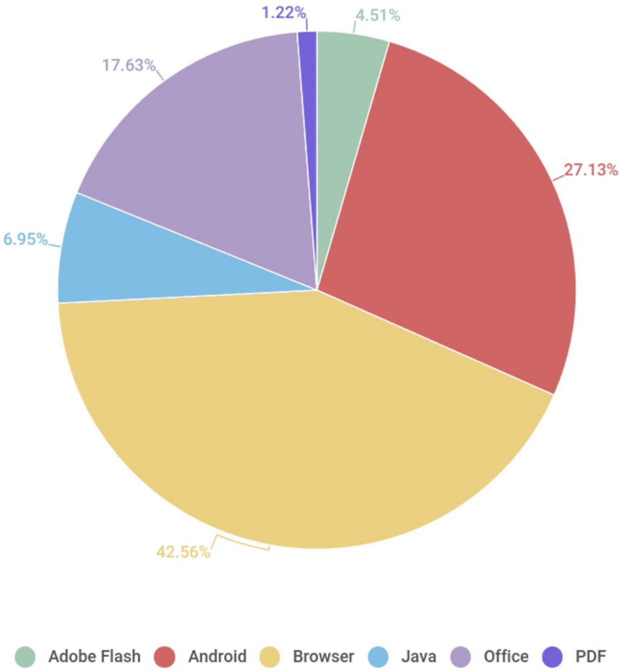


Distribution of exploits per application 2015



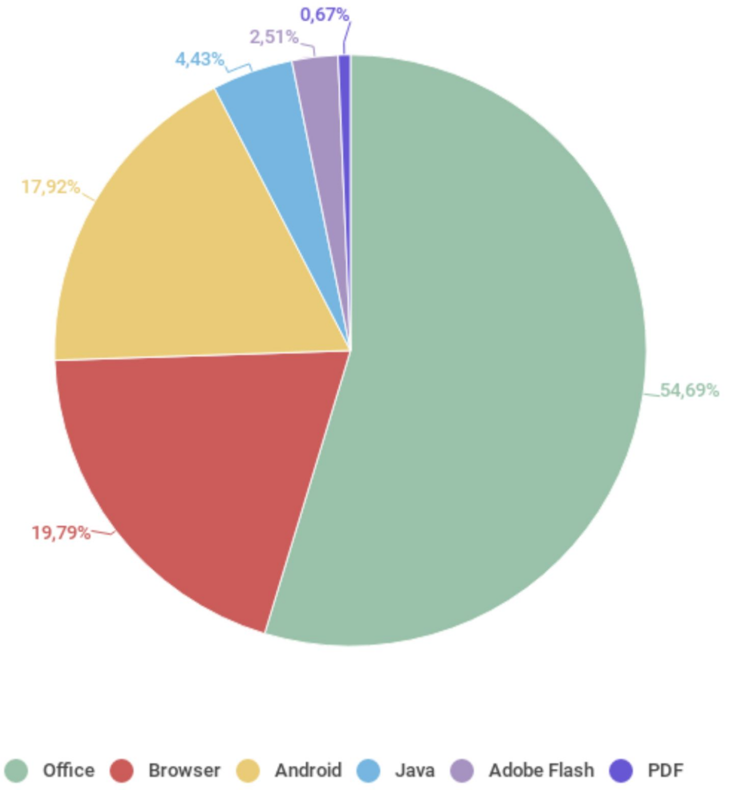
Source: Kaspersky Security Bulletin 2015

Distribution of exploits per application 2017



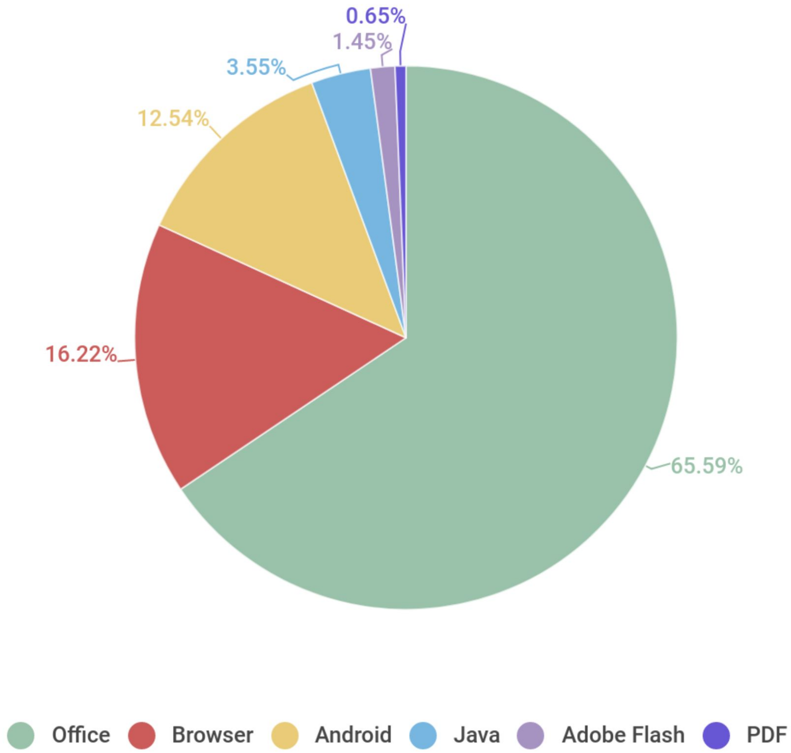
Source: Kaspersky Security Bulletin 2017

Distribution of exploits per application 2018



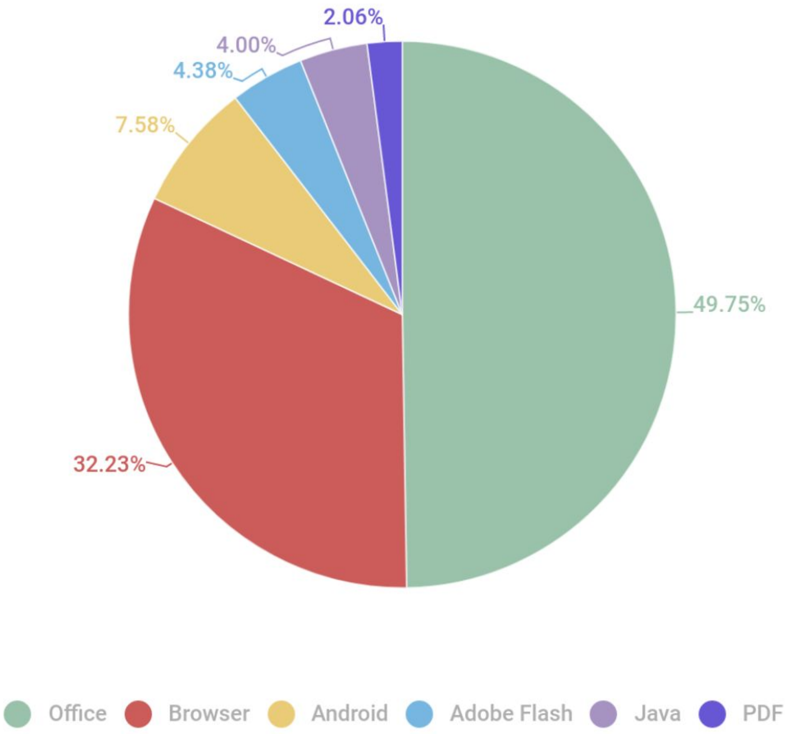
Source: Kaspersky Security Bulletin 2018

Distribution of exploits per application 2019



Source: Kaspersky Security Bulletin 2019

Distribution of exploits per application 2021



Source: Kaspersky Security Bulletin 2021

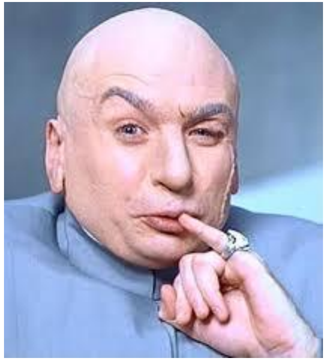
Bug bounty programs

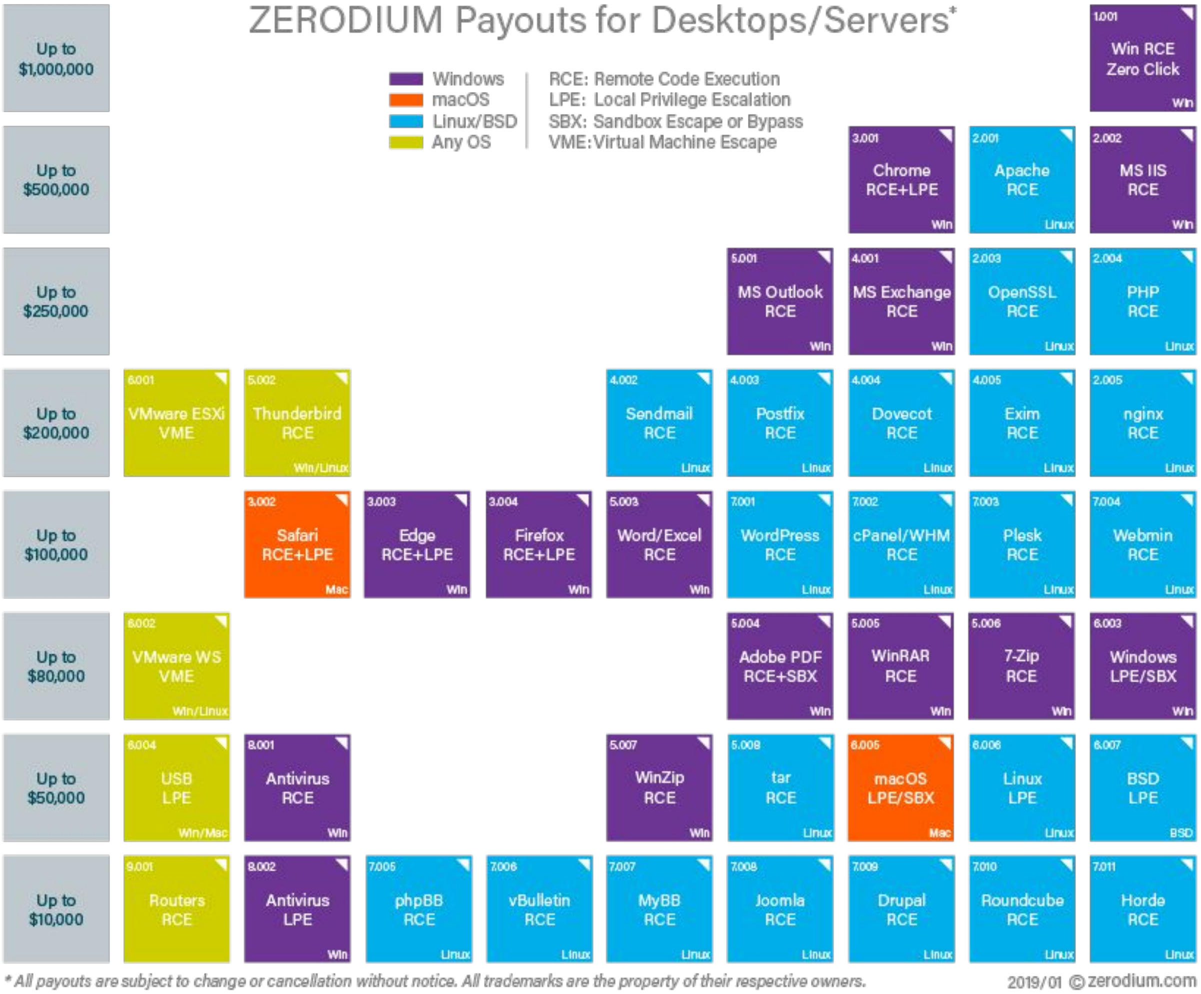
- Companies will pay you money to report vulnerabilities
- Certain conditions and rules per program
  - No Denial-of-service attacks
  - Spam
  - … (depends on the program)

Black market for exploits

Last iOS exploit was sold for

more than 1 million dollars





ZERODIUM Payouts for Desktops/Servers*

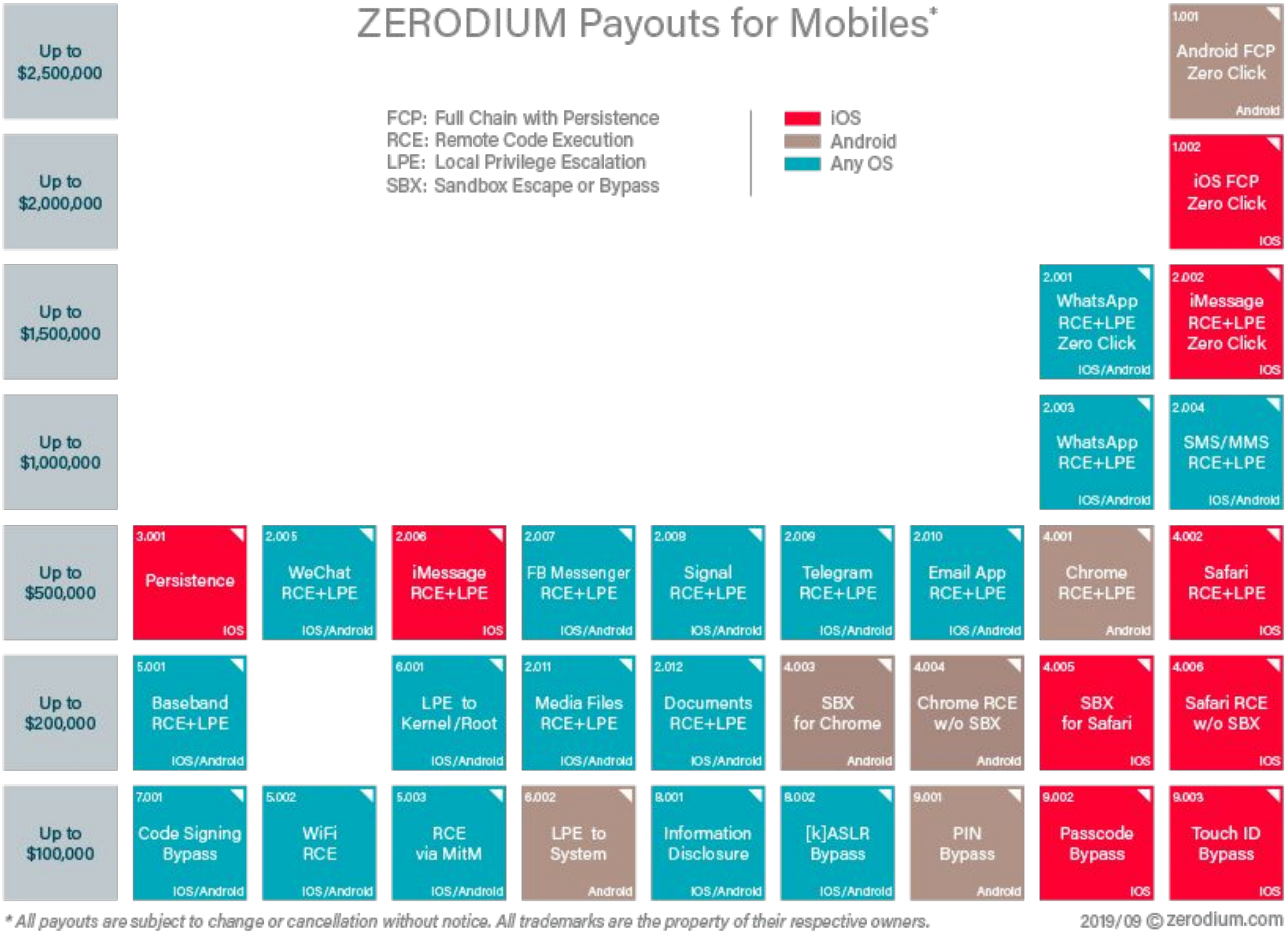
🟪 Windows
🟧 macOS
🟦 Linux/BSD
🟨 Any OS

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

Up to $2,500,000									1.001 Android FCP Zero Click Android
Up to $2,000,000									1.002 iOS FCP Zero Click iOS
Up to $1,500,000								2.001 WhatsApp RCE+LPE Zero Click iOS/Android	2.002 iMessage RCE+LPE Zero Click iOS
Up to $1,000,000								2.003 WhatsApp RCE+LPE iOS/Android	2.004 SMS/MMS RCE+LPE iOS/Android
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
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
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

Exploits for modern software are extremely difficult to write!

Chrome exploit

- Bug 1: run Native Client from any website
- Bug 2: integer underflow bug in the GPU command decoding -> ROP chain in GPU process
- Bug 3: impersonate the renderer from the GPU in the IPC channel
- Bug 4: allowed an unprivileged renderer to trigger a navigation to one of the privileged renderers -> launch the extension manager

Source: https://blog.chromium.org/2012/05/tale-of-two-pwnies-part-1.html

Chrome exploit

- Bug 5: specify a load path for an extension
- Bug 6: failure to prompt for confirmation prior to installing an unpacked NPAPI plug-in extension

Result: install and run a custom NPAPI plugin
that executes outside the sandbox at full user privilege

Next class

Refresh your assembly skills!