Google

A World Where 0-day is Hard

Maddie Stone (@maddiestone)
AusCERT 2021

Google hacker

All News Images Books Videos More Settings Tools Collections SafeSearch

computer stock logo cyber minecraft background laptop roblox kid symbol cool hoodie ultra hd


How do hackers pick their targets ...
pandasecurity.com


Defining the modern hacker | The McGill ...
mcgilltribune.com


cybersecurity: Hackers are a busy lot ...
m.economictimes.com


Hacker group 'Anonymous' back in actio...
economictimes.indiatimes.com


How Do Hackers Hack? - Fresh Security ...
freshsec.com


How Can Hackers Compromise Your Mobile...
completecontroller.com

8 Common Hacking Techniques That Every...
oceanpointins.com


The Time Hacker Method | Hacker Noon
hackernoon.com


Who Is Hacking Me? The Surprising ...
iconicit.com


Ethical Hacker Earns Over $1 Million by ...
mytechdecisions.com

What hackers do: their motivations and ...
csoonline.com


Covid Crimes: Espionage, Hackers And ...
forbes.com


Russian hackers 'traded s...
theguardian.com


steal COVID-19 vaccine research ...
fiercepharma.com


Most famous hackers in history -...
pandasecurity.com


Bitcoin Hacker Who Breache...
hacked.com


Hacking 101
globalsign.com


Hacking Laws and Punishments - FindLaw
findlaw.com


What is Hacking? | Hacking Definition ...
avast.com

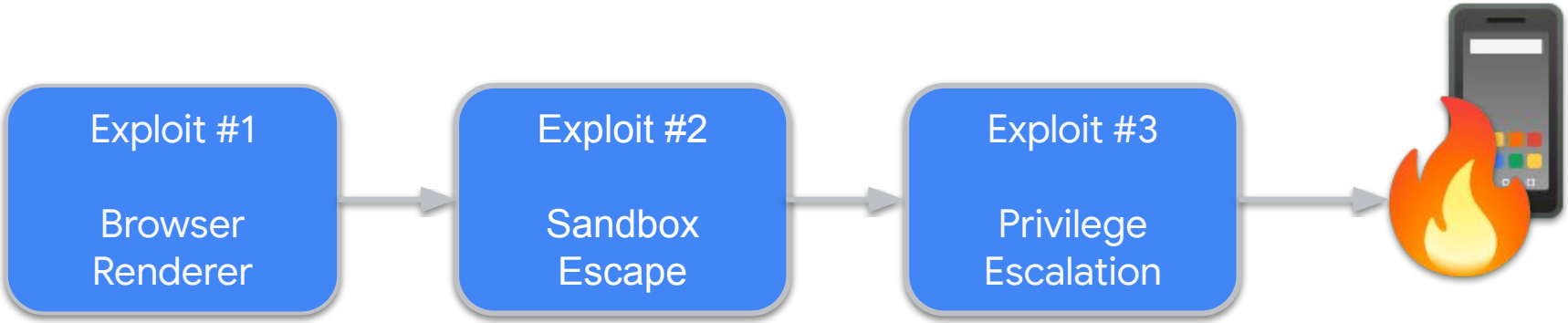

How Hackers Are Harvesting PI and Ho...
hstoday.us


Sneakers' and other hacker movies wi...
news.microsoft.com

Google

0-day exploit:

an exploit targeting a vulnerability that defenders don’t yet know about


Exploit #1
Browser Renderer
Exploit #2
Sandbox Escape
Exploit #3
Privilege Escalation

An Elite Spy Group Used 5 Zero-Days to Hack North Koreans

Zero-click iMessage zero-day used to hack the iPhones of 36 journalists

More Attackers Have Begun Using Zero-Day Exploits

This Map Shows the Global Spread of Zero-Day Hacking Techniques

The collection of countries using those secret hacking techniques has expanded far beyond the usual suspects.

Google fixes two more Chrome zero-days that were under active exploit

Microsoft patches 3 Windows 0-days under active exploit

Learn from 0-days exploited in the wild to make 0-day hard.

Make 0-day hard.

Make 0-day hard.

1. Increase cost per exploit.

2. Increase number of exploits required.

Make 0-day hard.

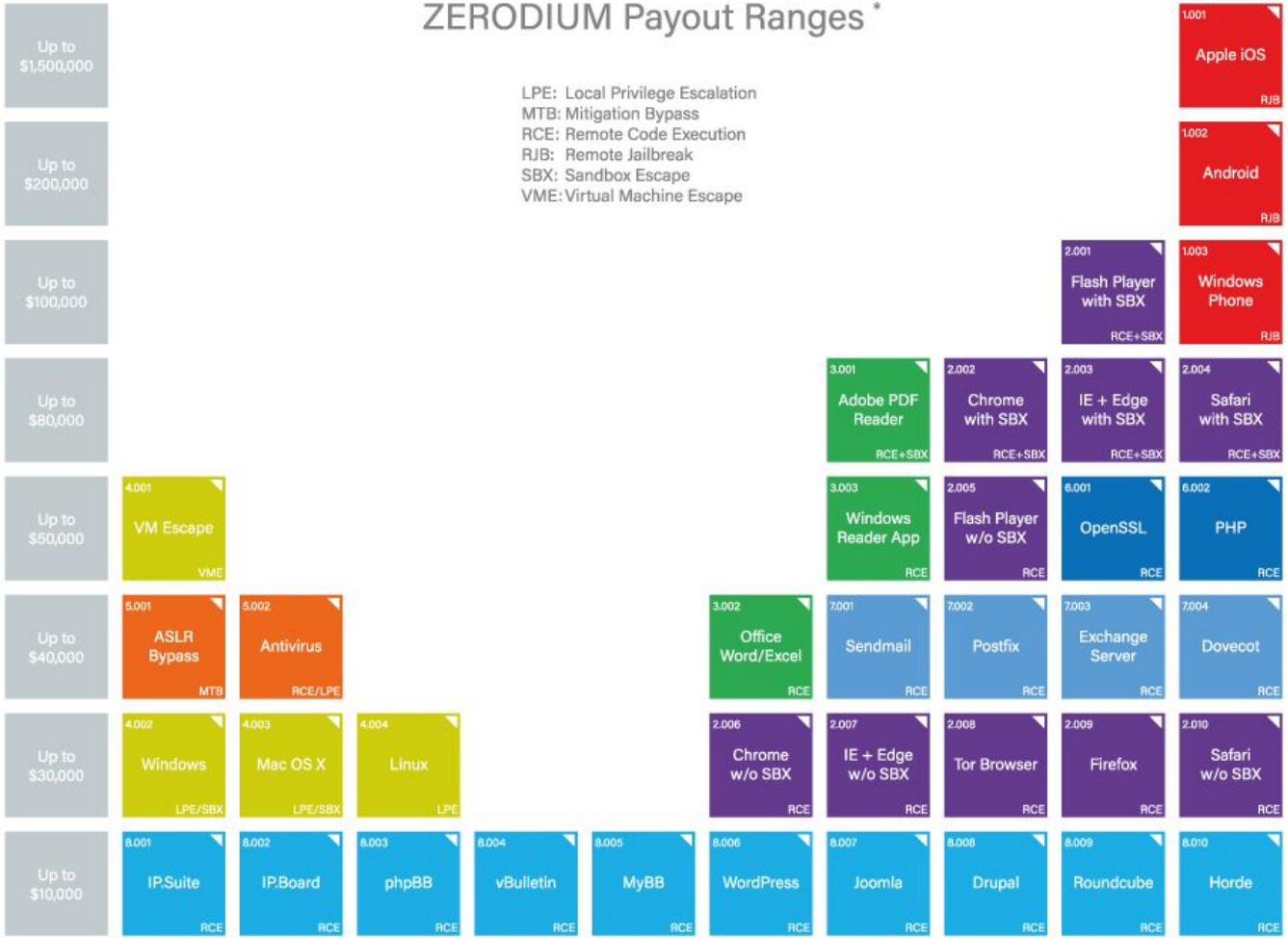
Money | Time | Expertise

1. Increase cost per exploit.

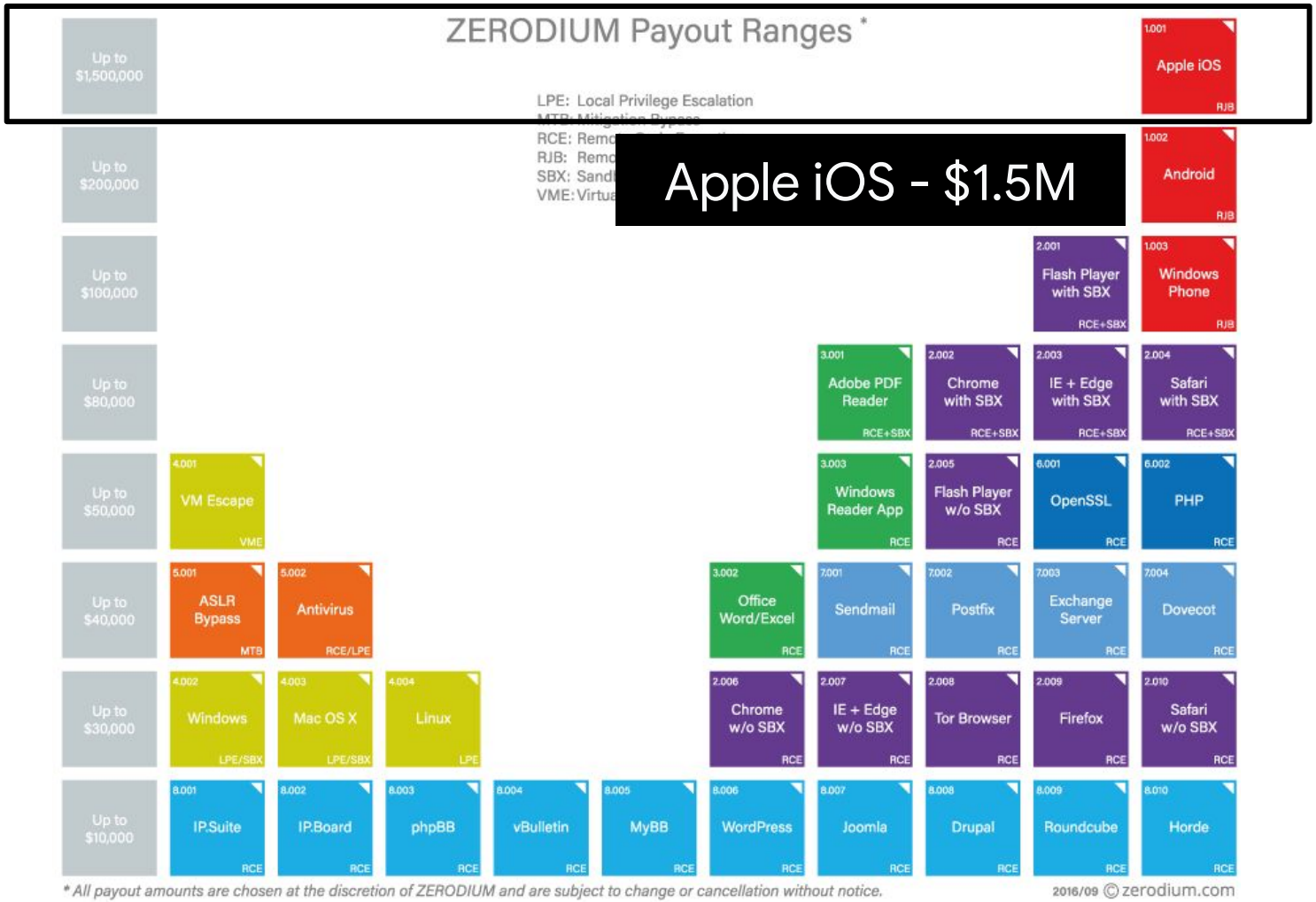
2. Increase number of exploits required.

Costs more for a less useful 0-day.

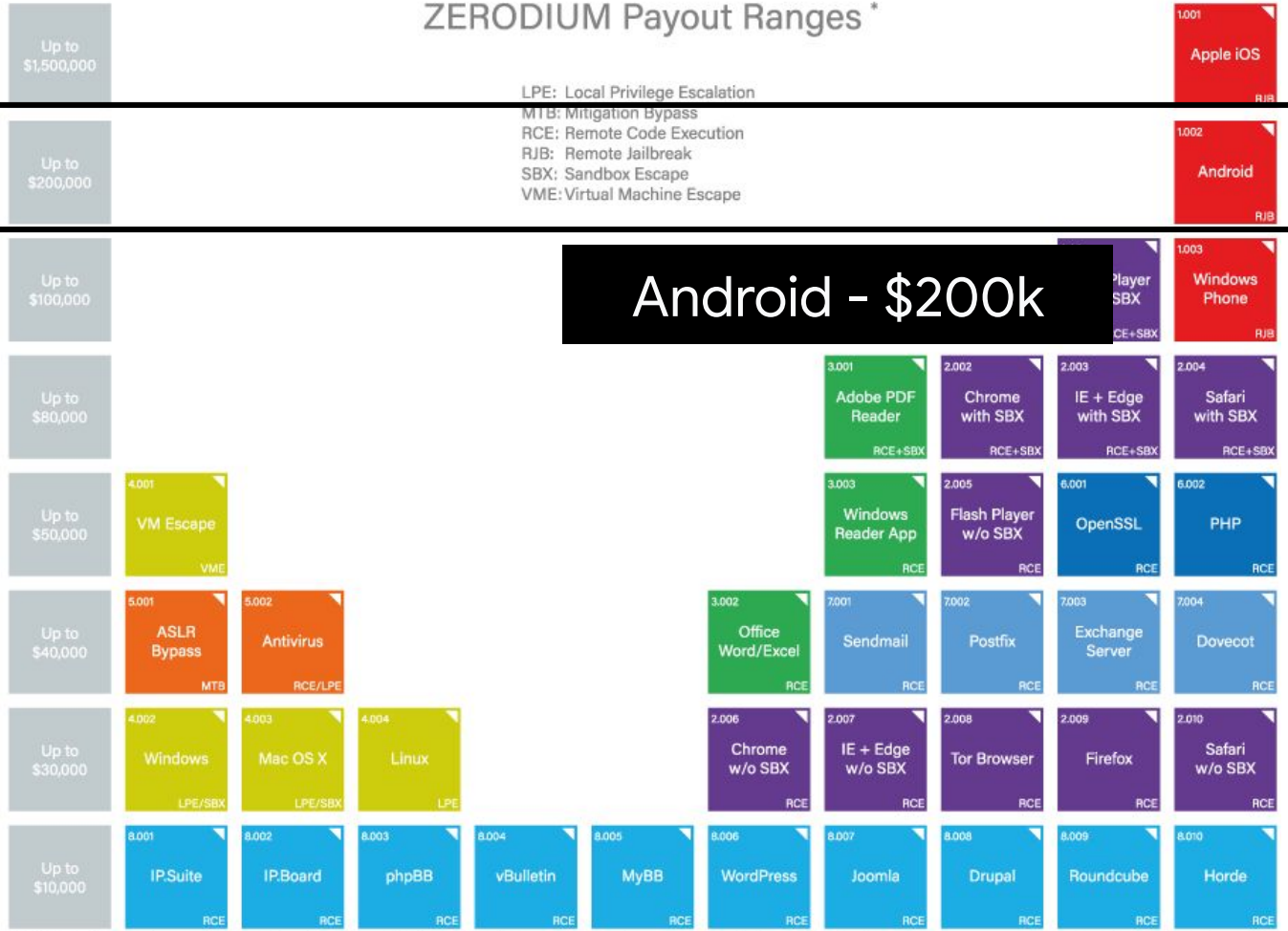
2016


ZERODIUM Payout Ranges *
LPE: Local Privilege Escalation
MTB: Mitigation Bypass
RCE: Remote Code Execution
RJB: Remote Jailbreak
SBX: Sandbox Escape
VME: Virtual Machine Escape
Up to $1,500,000
Up to $200,000
Up to $100,000
Up to $80,000
Up to $50,000
Up to $40,000
Up to $30,000
Up to $10,000
1.001 Apple iOS RJB
1.002 Android RJB
2.001 Flash Player with SBX RCE+SBX
1.003 Windows Phone RJB
3.001 Adobe PDF Reader RCE+SBX
2.002 Chrome with SBX RCE+SBX
2.003 IE + Edge with SBX RCE+SBX
2.004 Safari with SBX RCE+SBX
4.001 VM Escape VME
3.003 Windows Reader App RCE
2.005 Flash Player w/o SBX RCE
6.001 OpenSSL RCE
6.002 PHP RCE
5.001 ASLR Bypass MTB
5.002 Antivirus RCE/LPE
3.002 Office Word/Excel RCE
7.001 Sendmail RCE
7.002 Postfix RCE
7.003 Exchange Server RCE
7.004 Dovecot RCE
4.002 Windows LPE/SBX
4.003 Mac OS X LPE/SBX
4.004 Linux LPE
2.006 Chrome w/o SBX RCE
2.007 IE + Edge w/o SBX RCE
2.008 Tor Browser RCE
2.009 Firefox RCE
2.010 Safari w/o SBX RCE
8.001 IP.Suite RCE
8.002 IP.Board RCE
8.003 phpBB RCE
8.004 vBulletin RCE
8.005 MyBB RCE
8.006 WordPress RCE
8.007 Joomla RCE
8.008 Drupal RCE
8.009 Roundcube RCE
8.010 Horde RCE
* All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.
2016/09 © zerodium.com

2016


ZERODIUM Payout Ranges *
LPE: Local Privilege Escalation
RCE: Remo
RJB: Remo
SBX: Sandl
VME: Virtua
Apple iOS - $1.5M
Up to $1,500,000
1.001 Apple iOS RJB
Up to $200,000
1.002 Android RJB
Up to $100,000
2.001 Flash Player with SBX RCE+SBX
1.003 Windows Phone RJB
Up to $80,000
3.001 Adobe PDF Reader RCE+SBX
2.002 Chrome with SBX RCE+SBX
2.003 IE + Edge with SBX RCE+SBX
2.004 Safari with SBX RCE+SBX
Up to $50,000
4.001 VM Escape VME
3.003 Windows Reader App RCE
2.005 Flash Player w/o SBX RCE
6.001 OpenSSL RCE
6.002 PHP RCE
Up to $40,000
5.001 ASLR Bypass MTB
5.002 Antivirus RCE/LPE
3.002 Office Word/Excel RCE
7.001 Sendmail RCE
7.002 Postfix RCE
7.003 Exchange Server RCE
7.004 Dovecot RCE
Up to $30,000
4.002 Windows LPE/SBX
4.003 Mac OS X LPE/SBX
4.004 Linux LPE
2.006 Chrome w/o SBX RCE
2.007 IE + Edge w/o SBX RCE
2.008 Tor Browser RCE
2.009 Firefox RCE
2.010 Safari w/o SBX RCE
Up to $10,000
8.001 IP.Suite RCE
8.002 IP.Board RCE
8.003 phpBB RCE
8.004 vBulletin RCE
8.005 MyBB RCE
8.006 WordPress RCE
8.007 Joomla RCE
8.008 Drupal RCE
8.009 Roundcube RCE
8.010 Horde RCE
* All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.
2016/09 © zerodium.com

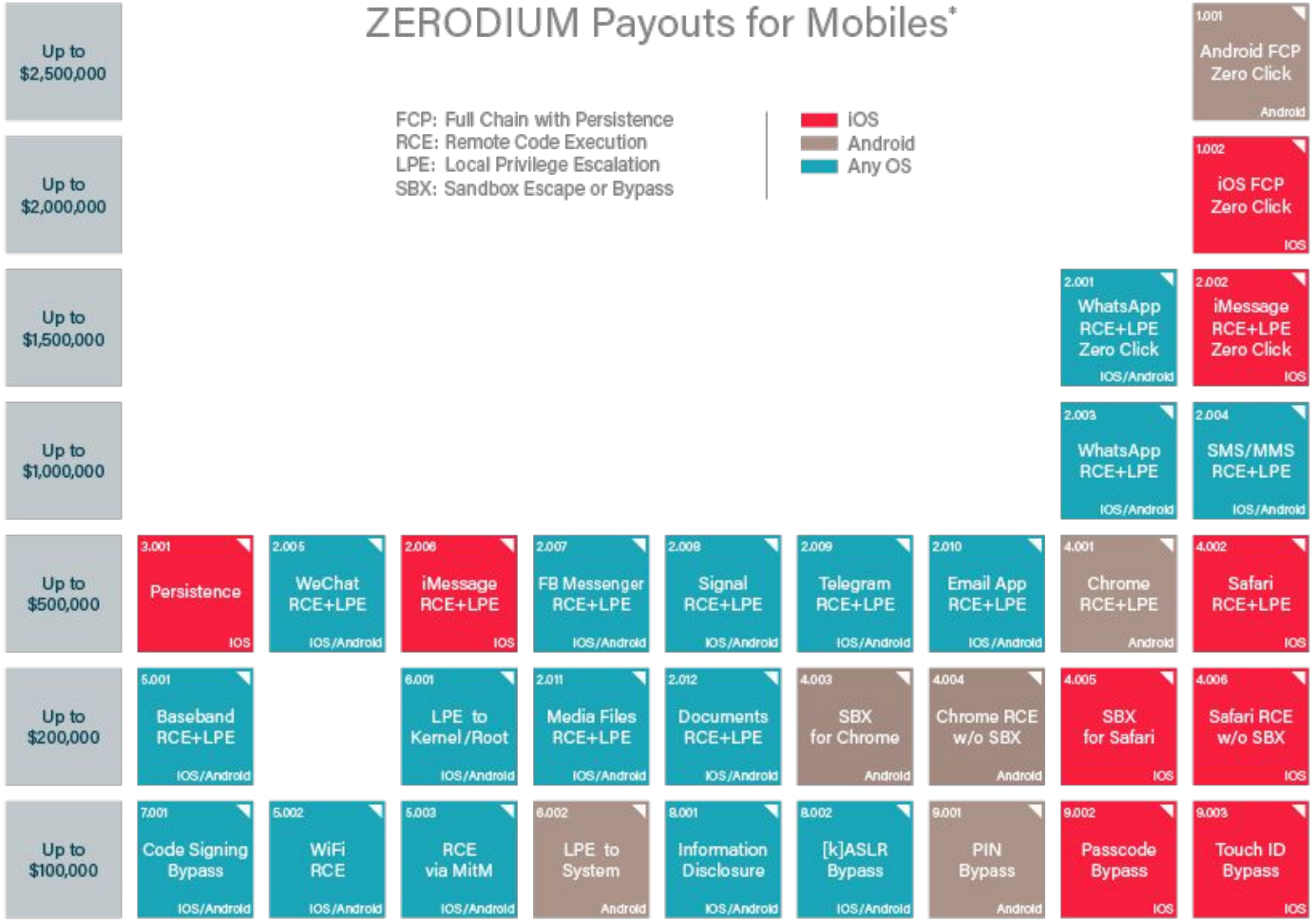
2016



Android - $200k

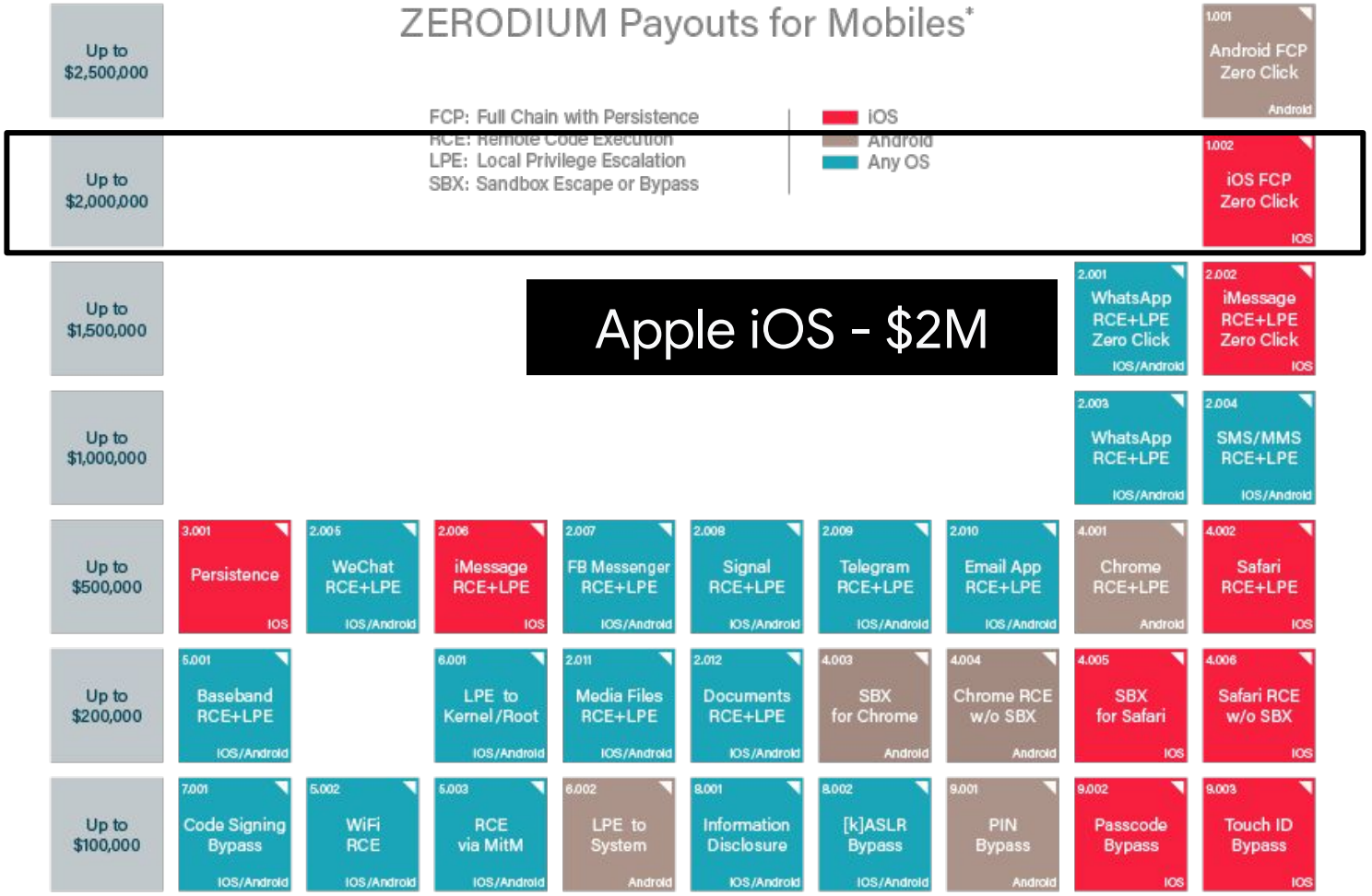
Google

2019



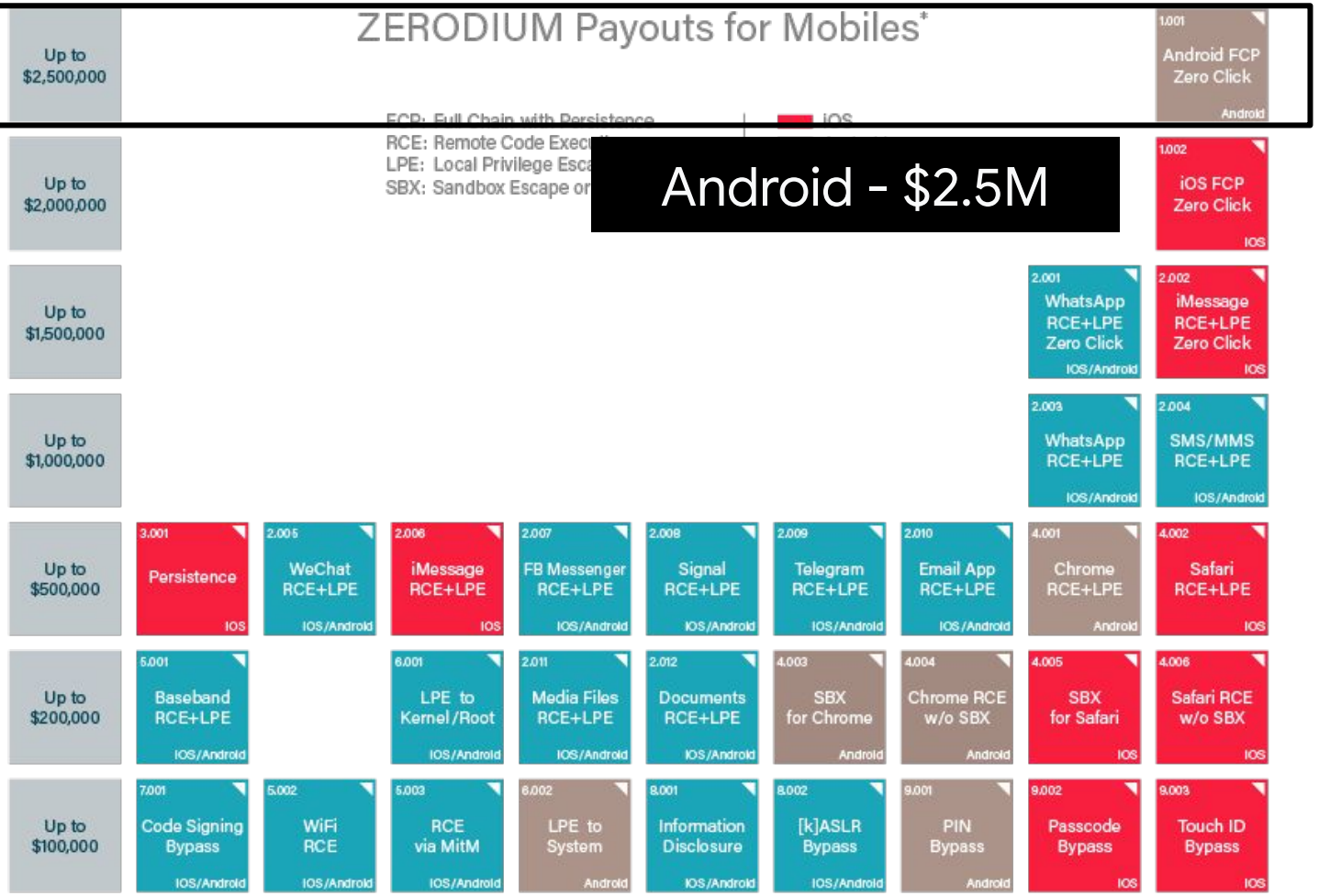
** All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*

2019



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

2019


ZERODIUM Payouts for Mobiles*
Up to $2,500,000
1.001 Android FCP Zero Click Android
FCP: Full Chain with Persistence
RCE: Remote Code Exec
LPE: Local Privilege Esc
SBX: Sandbox Escape or
iOS
Android - $2.5M
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

The price of an Android exploit chain increased 1150%.

- Regular security updates with advisories
- Application sandbox
- Exploit mitigations
- More mature software development lifecycle

The pri exploit
0%.

CAVEAT: The price of an exploit is not always equal to the cost of an exploit.

Measuring “hard”.

With better patching practices,

25% of 0-days exploited in 2020 could have been prevented.

Transparency.

iOS 14.5.1 and iPadOS 14.5.1

Released May 3, 2021

WebKit

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

Description: A memory corruption issue was addressed with improved state management.

CVE-2021-30665: yangkang (@dnpushme)&zerokeeper&bianliang of 360 ATA

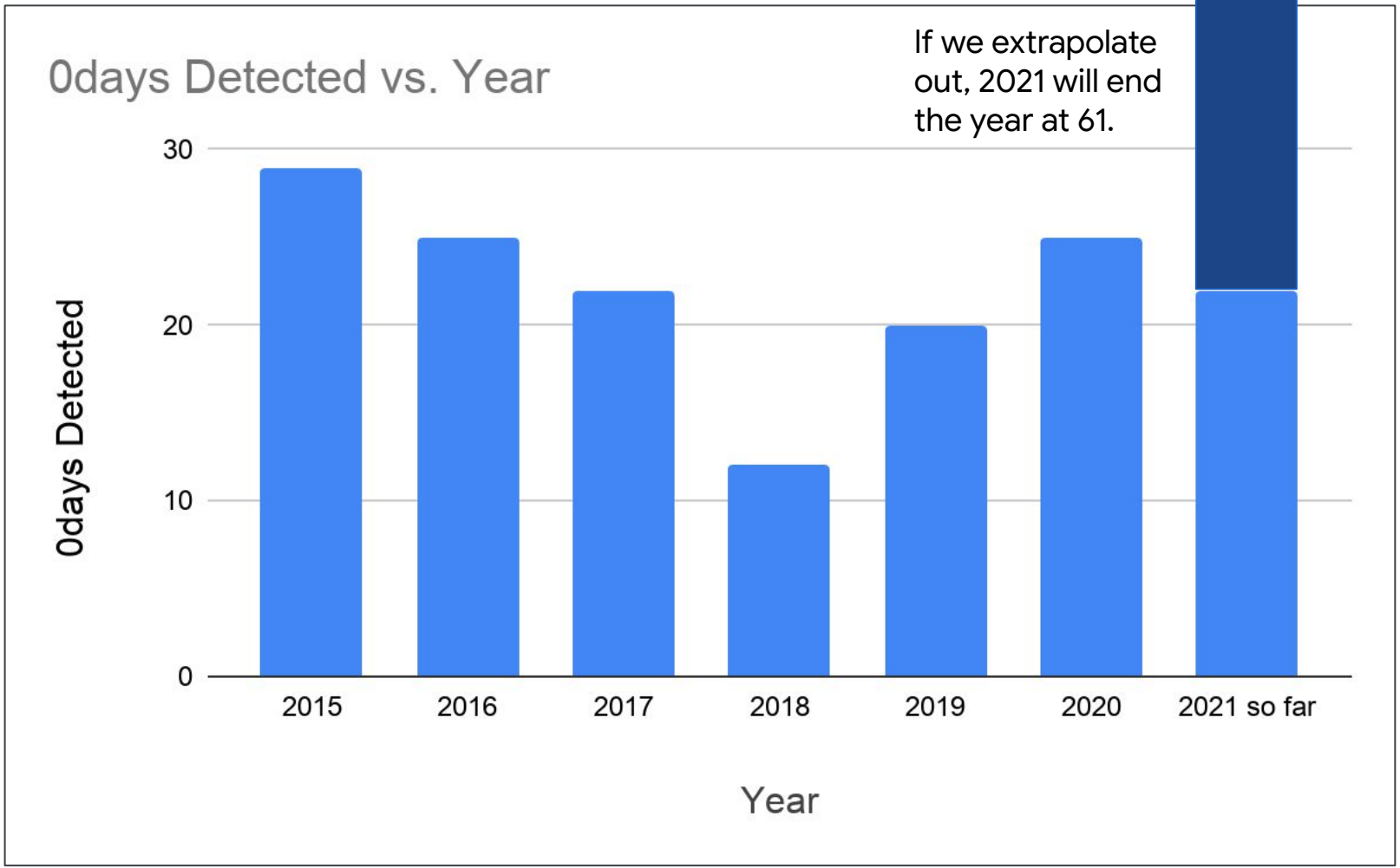
WebKit

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

Description: An integer overflow was addressed with improved input validation.

CVE-2021-30663: an anonymous researcher


0days Detected vs. Year
If we extrapolate out, 2021 will end the year at 61.
30
20
10
0
0days Detected
2015
2016
2017
2018
2019
2020
2021 so far
Year

CVE-2021-1647: Windows Defender mpengine remote code execution

Maddie Stone, Project Zero

The Basics

Disclosure or Patch Date: 12 January 2021

Product: Microsoft Windows Defender

Advisory: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1647

Affected Versions: Version 1.1.17600.5 and previous

First Patched Version: Version 1.1.17700.4

Issue/Bug Report: N/A

Patch CL: N/A

Bug-Introducing CL: N/A

Reporter(s): Anonymous

The Code

Proof-of-concept:

Exploit sample: 6e1e9fa0334d8f1f5d0e3a160ba65441f0656d1f1c99f8a9f1ae4b1b1bf7d788

Did you have access to the exploit sample when doing the analysis? Yes

The Vulnerability

Bug class: Heap buffer overflow

Vulnerability details:

There is a heap buffer overflow when Windows Defender (`mpengine.dll`) processes the section table when unpacking an ASProtect packed executable. Each section entry has two values: the virtual address and the size of the section. The code in `CAsprotectDLLAndVersion::RetrieveVersionInfoAndCreateObjects` only checks if the next section entry's address is lower than the previous one, not if they are equal. This means that if you have a section table such as the one used in this exploit sample: `[ (0,0), (0,0), (0x2000,0), (0x2000,0x3000) ]` , 0 bytes are allocated for the section at address 0x2000, but when it sees the next entry at 0x2000, it simply skips over it without exiting nor updating the size of the section. 0x3000 bytes will then be copied to that section during the decompression, leading to the heap buffer overflow.

Mitigating vulnerabilities faster.

Zero-day vulnerability in Desktop Window Manager (CV 28310) used in the wild

RESEARCH 13 APR 2021 8 minute read

We reported this new exploit to Microsoft in **February** and after confirmation that it is indeed a zero-day, it received the designation CVE-2021-28310. Microsoft released a patch to this vulnerability as a part of its **April** security updates.

// AUTHORS

Expert BORIS LARIN  COSTIN RAIU Expert BRIAN BARTHOLOMEW

While analyzing the CVE-2021-1732 exploit originally discovered by the DBAPPSecurity Threat Intelligence Center and used by the BITTER APT group, we discovered another zero-day exploit we believe is linked to the same actor. We reported this new exploit to Microsoft in February and after confirmation that it is indeed a zero-day, it received the designation CVE-2021-28310. Microsoft released a patch to this vulnerability as a part of its April security updates.

FROM THE SAME

Op 20

Int Wi use

GR IDA

Ma evo

Lo Co

Google

Memory safe languages could potentially have prevented **64%** of 0-days so far in 2021.

We can make 0-day hard.

THANK YOU!

@maddiestone
0day-in-the-wild <at> google.com

Google

References

- 2020 Year in Review blog post discussing how 25% of the 0-days detected in 2020 are closely related to previously publicly disclosed vulnerabilities.
  - Enigma 2021 video
- 2019 Year in Review blog post about struggles in 0-day detection.
- Project Zero 0-day tracking sheet
- 0-day in-the-wild root cause analyses

Sources for Headlines on Slide #6

- “More Attackers Have Begun Using Zero-Day Exploits”: https://www.darkreading.com/attacks-breaches/more-attackers-have-begun-using-zero-day-exploits-/d/d-id/1337493
- “An Elite Spy Group Used 5 Zero-Days to Hack North Koreans”: https://www.wired.com/story/north-korea-hacking-zero-days-google/
- “This Map Shows the Global Spread of Zero-Day Hacking Techniques”: https://www.wired.com/story/zero-day-hacking-map-countries/
- “Zero-click iMessage zero-day used to hack the iPhones of 36 journalists”: https://arstechnica.com/information-technology/2020/12/zero-click-imessage-zeroday-used-to-hack-the-iphones-of-36-journalists/
- “Microsoft patches 3 Windows 0-days under active exploit”: https://arstechnica.com/information-technology/2020/04/4-windows-0days-under-active-exploit-get-fixes-in-this-months-update-tuesday/
- “Google fixes two more Chrome zero-days that were under active exploit”: https://arstechnica.com/information-technology/2020/11/google-fixes-two-more-chrome-zerodays-that-were-under-active-exploit/