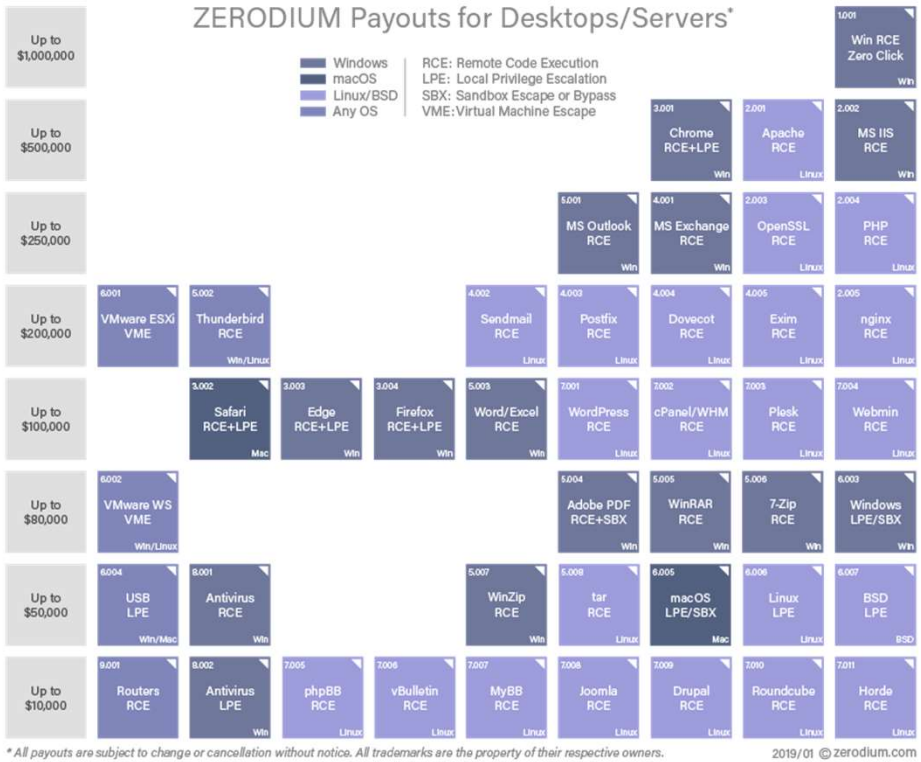
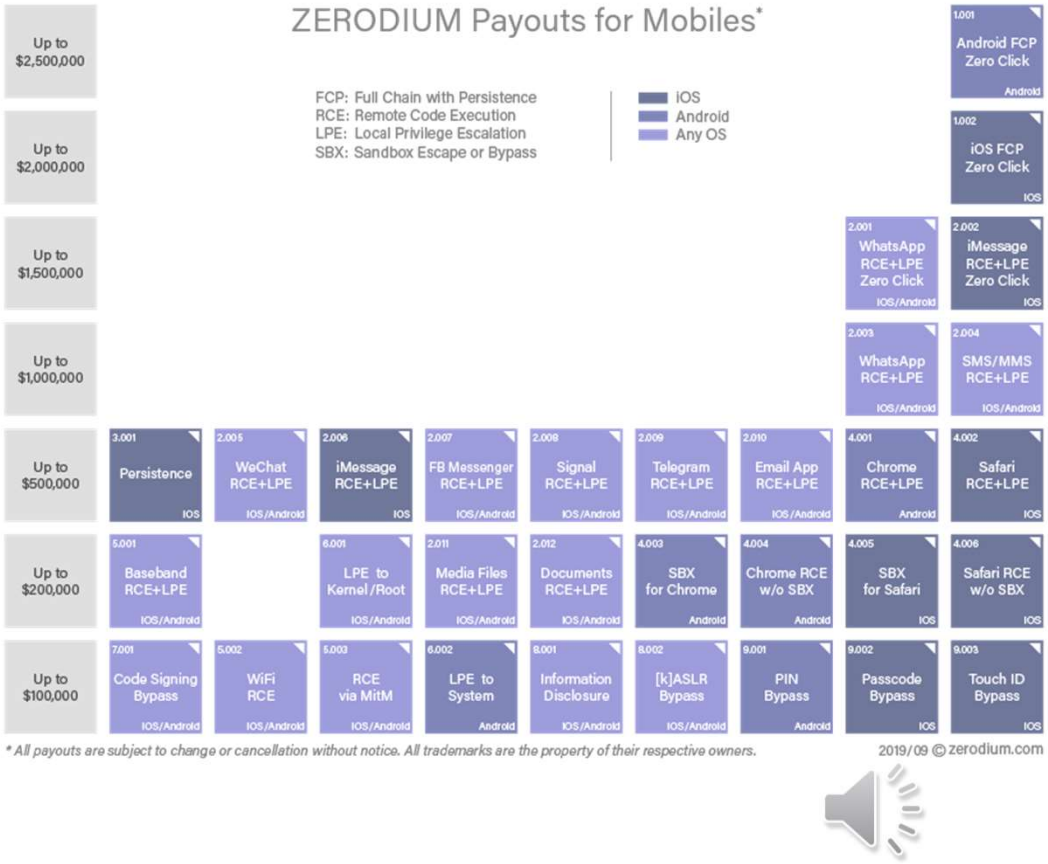
Hacking in the 21st Century

Sidhardh Burre


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
Up to $500,000
Up to $250,000
Up to $200,000
Up to $100,000
Up to $80,000
Up to $50,000
Up to $10,000
1.001 Win RCE Zero Click Win
3.001 Chrome RCE+LPE Win
2.001 Apache RCE Linux
2.002 MS IIS RCE Win
5.001 MS Outlook RCE Win
4.001 MS Exchange RCE Win
2.003 OpenSSL RCE Linux
2.004 PHP RCE Linux
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
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
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
6.004 USB LPE Win/Mac
6.001 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
8.001 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

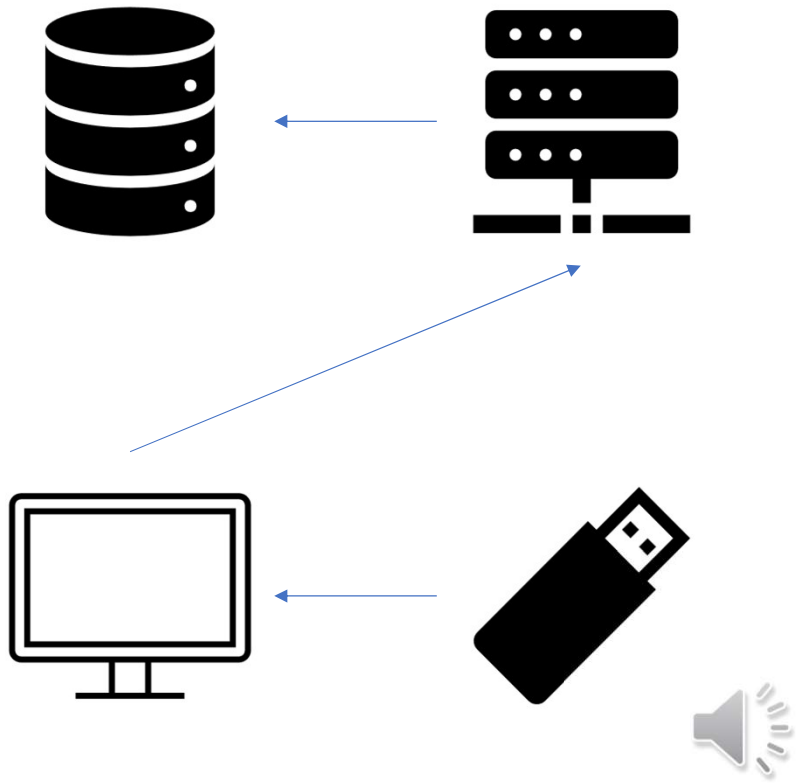

ZERODIUM Payouts for Mobiles*
FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
iOS
Android
Any OS
Up to $2,500,000
Up to $2,000,000
Up to $1,500,000
Up to $1,000,000
Up to $500,000
Up to $200,000
Up to $100,000
1.001 Android FCP Zero Click Android
1.002 iOS FCP Zero Click iOS
2.001 WhatsApp RCE+LPE Zero Click IOS/Android
2.002 iMessage RCE+LPE Zero Click IOS
2.003 WhatsApp RCE+LPE IOS/Android
2.004 SMS/MMS RCE+LPE IOS/Android
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
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
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

Secondary Market for Exploits

- Exploits are essentially “hacks”
- Private companies purchase them
- Government agencies (and others) buy them second hand
  - for 10-100x the original price
  - have little to no traceability

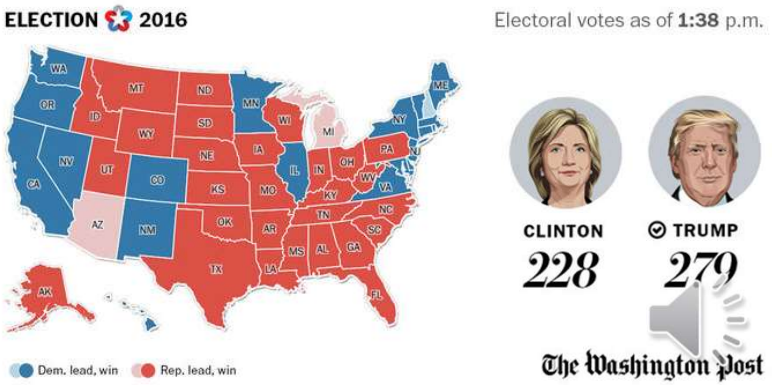
Stuxnet

- Used four exploits
  1. .LNK exploit
  2. 2. Remote code exploit for network printers
  3. Escalation of privilege zero day 1
  4. Escalation of privilege zero day 2
  - Zero-day flaw in Siemens PLC
  - Conficker attack hole
- What was it designed to do?



What does this mean for war?

- War has completely changed
  - Hyper-efficient
  - Anonymous
  - Little to no oversight
- Cyberwarfare capabilities
  - espionage
  - sabotage
  - propaganda
  - economic disruption
  - etc.



"…Napoleon won his victories because the Grand Army could outmarch the enemy. It is the same to-day. War never changes. Only weapons are new. Yet it is not always the weapons, but the men who handle them, who win victories."

-"The Days Work of a Soldier" from *The World's work; Second War Manual; The Conduct of War (1914)*

What does this mean for us?

- Our capabilities for destruction have outstripped our abilities to understand them
  - Specify and follow rules of engagement
  - Apply intense scrutiny to companies/organizations/people that develop/research/disseminate enabling technologies
  - Contain civilian fallout