Πολιτικές Ασφάλειας & Ιδιωτικότητας στο Διαδίκτυο

Ασφάλεια Δικτύων

Χριστόφορος Νταντογιάν

Malware

- A piece of malicious software
  - Botnet
  - Ransomware
  - Steal personal info
- Popular in Windows machines
- Mobile malware on the rise
  - Especially for Android

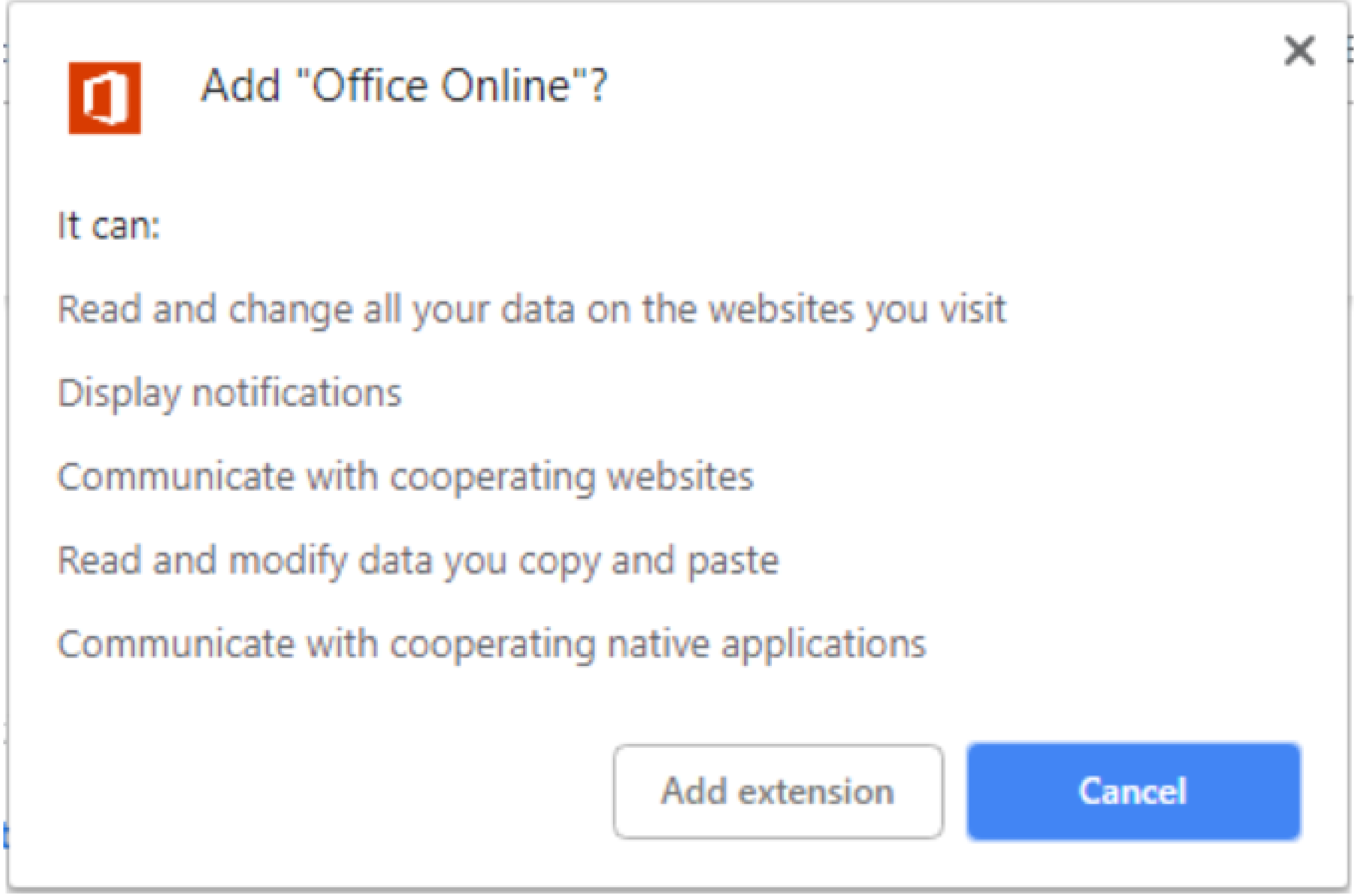
Malware motivation

- Initially the goals of a malware were disruption → Now is money

1. Blackmail based on ransomware
2. Blackmail based on DDOS by becoming part of a botnet
3. Steal personal information (e.g., from keyloggers to man in the browser)

Man-in-the-browser

- Man-in-the-browser attacks, a specialised breed of man-in-the-middle attack that manipulates browser content to steal sensitive user information or lure victims into malware-infected websites.



Add "Office Online"?

It can:

Read and change all your data on the websites you visit

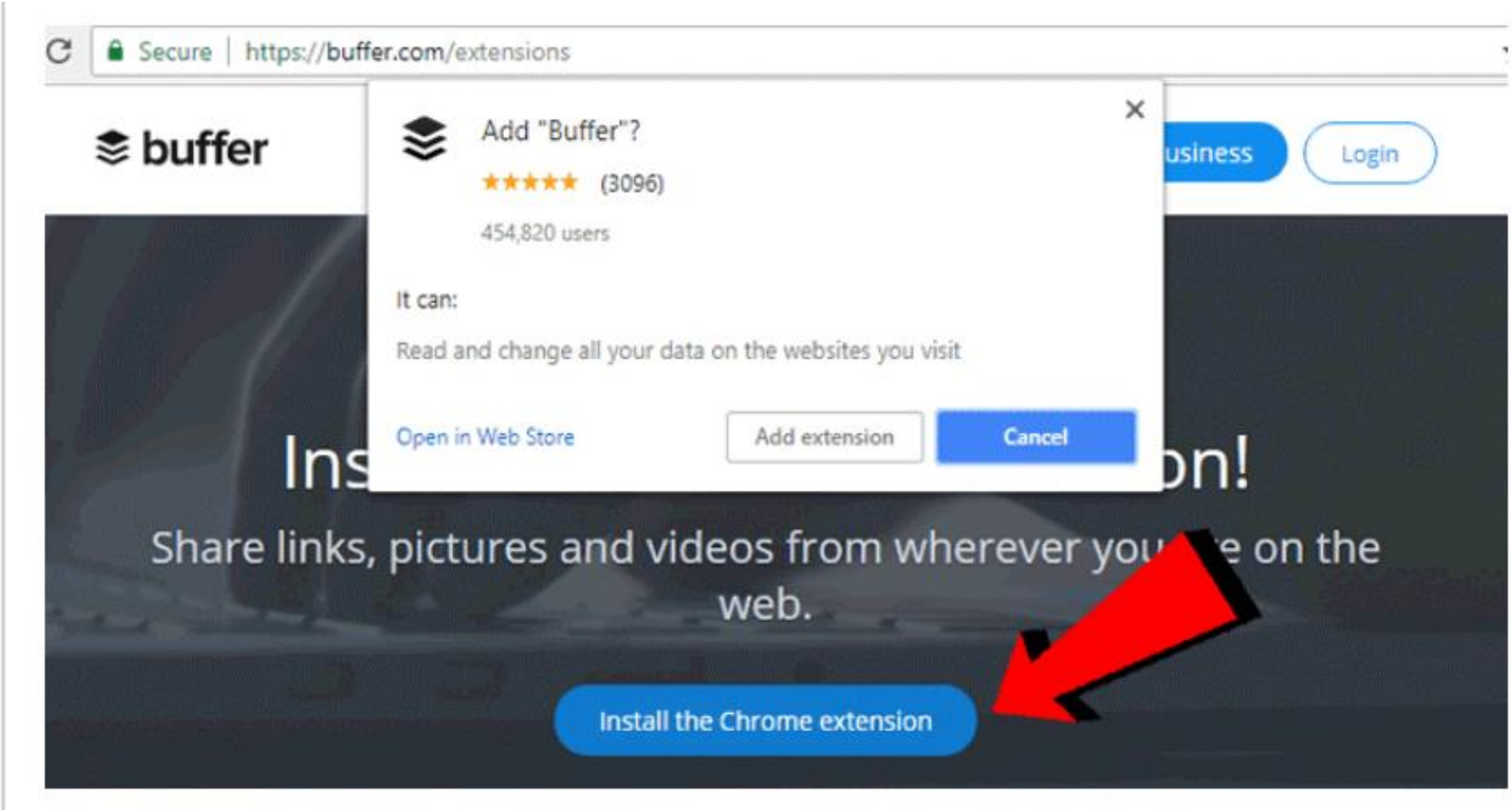
Display notifications

Communicate with cooperating websites

Read and modify data you copy and paste

Communicate with cooperating native applications

Inline install



Add "Buffer"?

★★★★★ (3096)

454,820 users

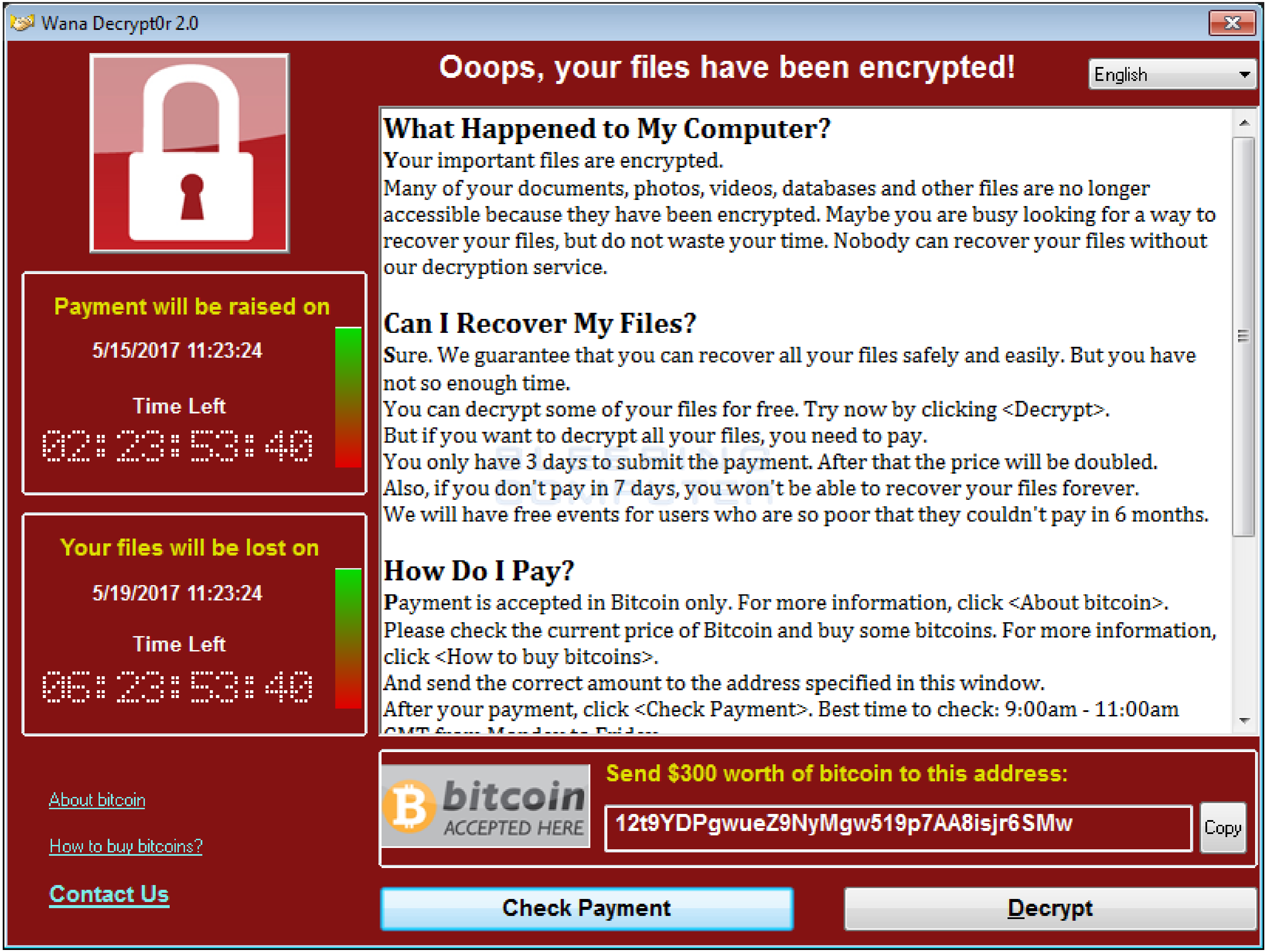
It can:

Read and change all your data on the websites you visit

Share links, pictures and videos from wherever you e on the web.

WannaCry ransomware

- The WannaCry ransomware attack was a May 2017 worldwide cyberattack, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.
- It propagated through EternalBlue, an exploit developed by the US National Security Agency (NSA) for older Windows systems
- The attack was estimated to have affected more than 200,000 computers across 150 countries,



Ooops, your files have been encrypted!

Payment will be raised on

5/15/2017 11:23:24

Time Left

02:23:53:40

Your files will be lost on

5/19/2017 11:23:24

Time Left

06:23:53:40

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

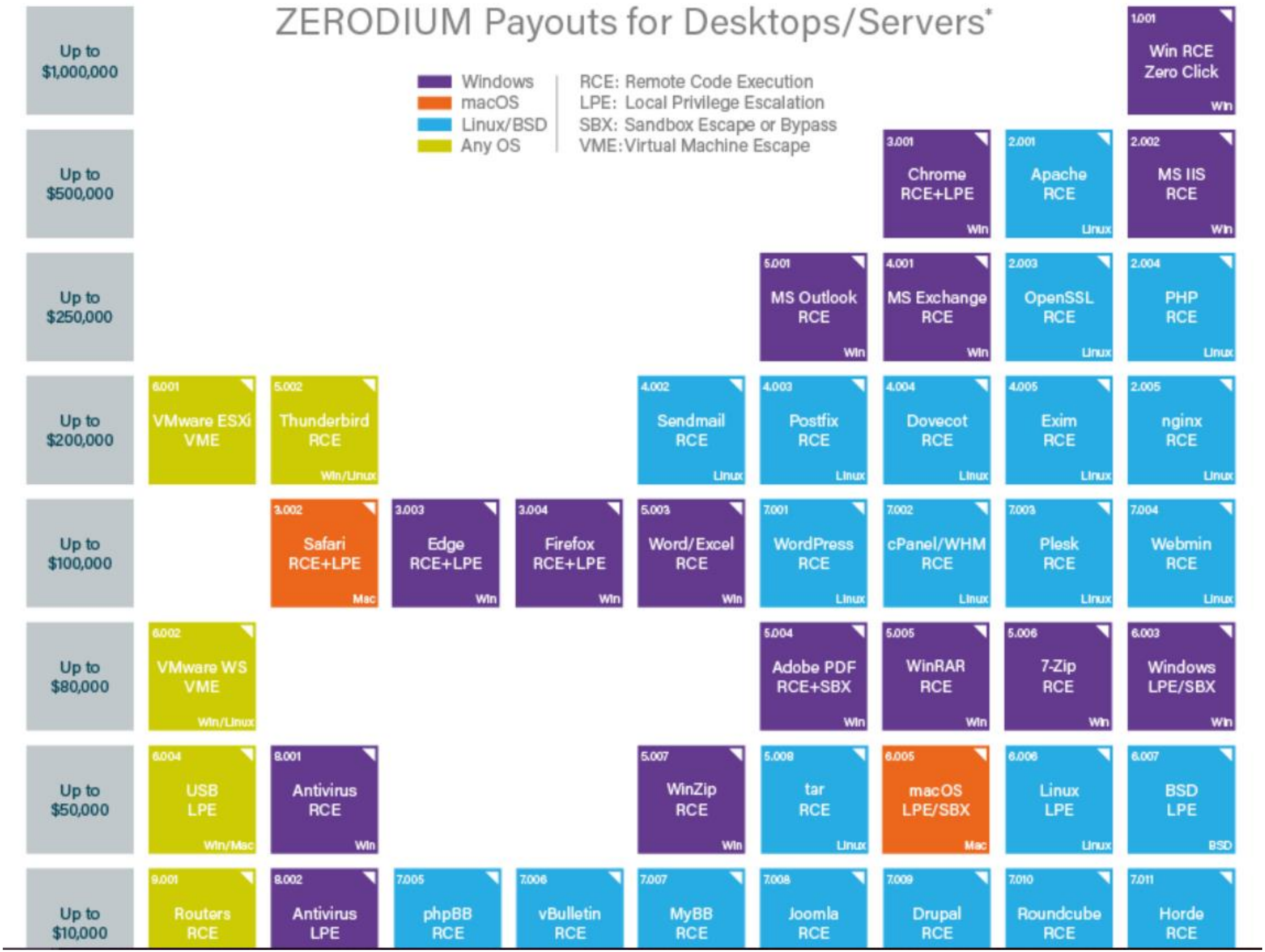
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

How organizations are attacked and infected?

- Old days through internet worms…(e.g., splasher)
- Spam email with malicious attachments
- Visiting malicious web sites
  - Malicious software as maltervisement
  - Scareware also known as Rogue AV or other malicious software
  - Drive by downloads
- Visiting compromised web sites → Drive by download attacks

Recon

- Information gathering using public data
  - emails,
  - Names and accounts,
  - Phone numbers
  - Job descriptions...
- Discover IP ranges, domains, servers

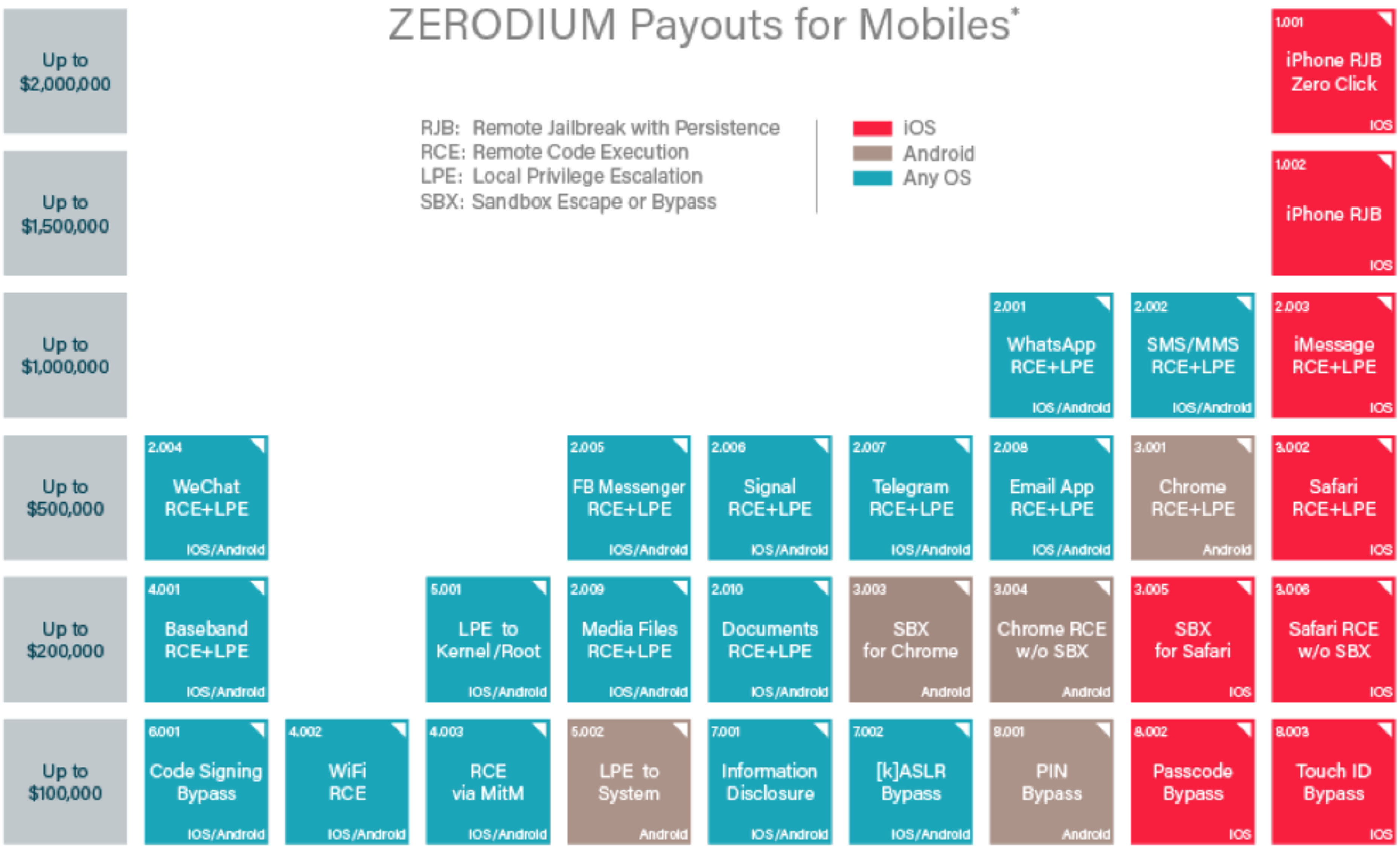


ZERODIUM Payouts for Desktops/Servers*

🟪 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	7.005 phpBB RCE	7.006 vBulletin RCE	7.007 MyBB RCE	7.008 Joomla RCE	7.009 Drupal RCE	7.010 Roundcube RCE	7.011 Horde RCE



ZERODIUM Payouts for Mobiles*

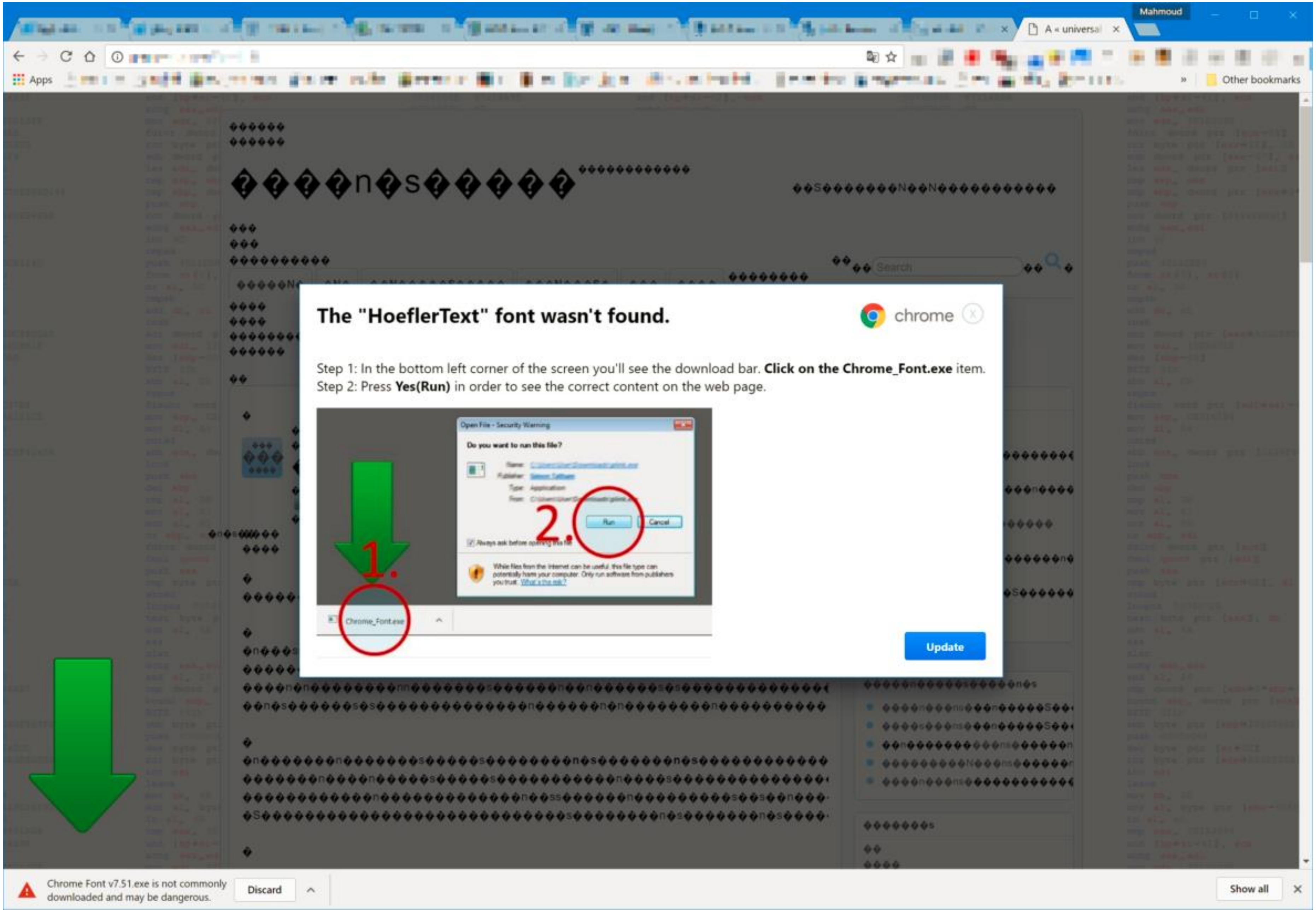
RJB: Remote Jailbreak with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

🟥 iOS
🟫 Android
🟦 Any OS

Up to $2,000,000									1.001 iPhone RJB Zero Click iOS
Up to $1,500,000									1.002 iPhone RJB iOS
Up to $1,000,000							2.001 WhatsApp RCE+LPE iOS/Android	2.002 SMS/MMS RCE+LPE iOS/Android	2.003 iMessage RCE+LPE iOS
Up to $500,000	2.004 WeChat RCE+LPE iOS/Android			2.005 FB Messenger RCE+LPE iOS/Android	2.006 Signal RCE+LPE iOS/Android	2.007 Telegram RCE+LPE iOS/Android	2.008 Email App RCE+LPE iOS/Android	3.001 Chrome RCE+LPE Android	3.002 Safari RCE+LPE iOS
Up to $200,000	4.001 Baseband RCE+LPE iOS/Android		5.001 LPE to Kernel/Root iOS/Android	2.009 Media Files RCE+LPE iOS/Android	2.010 Documents RCE+LPE iOS/Android	3.003 SBX for Chrome Android	3.004 Chrome RCE w/o SBX Android	3.005 SBX for Safari iOS	3.006 Safari RCE w/o SBX iOS
Up to $100,000	6.001 Code Signing Bypass iOS/Android	4.002 WiFi RCE iOS/Android	4.003 RCE via MitM iOS/Android	5.002 LPE to System Android	7.001 Information Disclosure iOS/Android	7.002 [k]ASLR Bypass iOS/Android	8.001 PIN Bypass Android	8.002 Passcode Bypass iOS	8.003 Touch ID Bypass iOS

Social Engineering

- Spoofed email!
  - Depends on the mail server of the organization
  - Buy a resembling domain (e.g., user@faceb00k.com)
  - Change the name of the email sender
- Using cc with familiar emails increases the chances.
- Nicknames
- Executables change the file format (e.g., cats.pdf.exe)
- Use zip files with passwords!



The "HoeflerText" font wasn't found.

Step 1: In the bottom left corner of the screen you'll see the download bar. **Click on the Chrome_Font.exe** item.

Step 2: Press **Yes(Run)** in order to see the correct content on the web page.

Open File - Security Warning

Do you want to run this file?

Name:

Publisher:

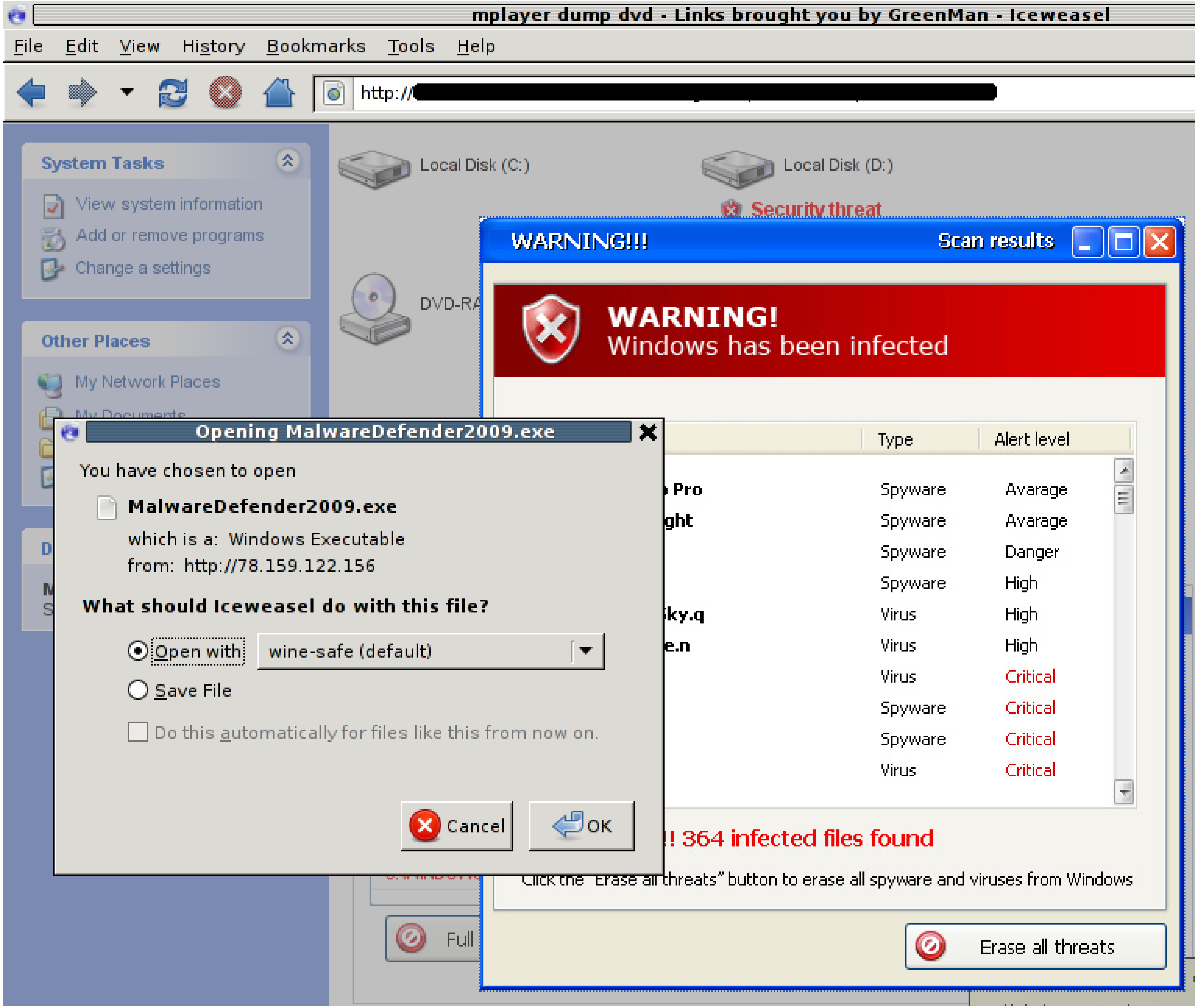
Type: Application

From:

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

Chrome Font v7.51.exe is not commonly downloaded and may be dangerous.



http://[redacted]

WARNING!!! Scan results

WARNING!
Windows has been infected

	Type	Alert level
Pro	Spyware	Avarage
ght	Spyware	Avarage
	Spyware	Danger
	Spyware	High
ky.q	Virus	High
e.n	Virus	High
	Virus	Critical
	Spyware	Critical
	Spyware	Critical
	Virus	Critical

!! 364 infected files found

Click the "Erase all threats" button to erase all spyware and viruses from Windows

Opening MalwareDefender2009.exe

You have chosen to open

MalwareDefender2009.exe

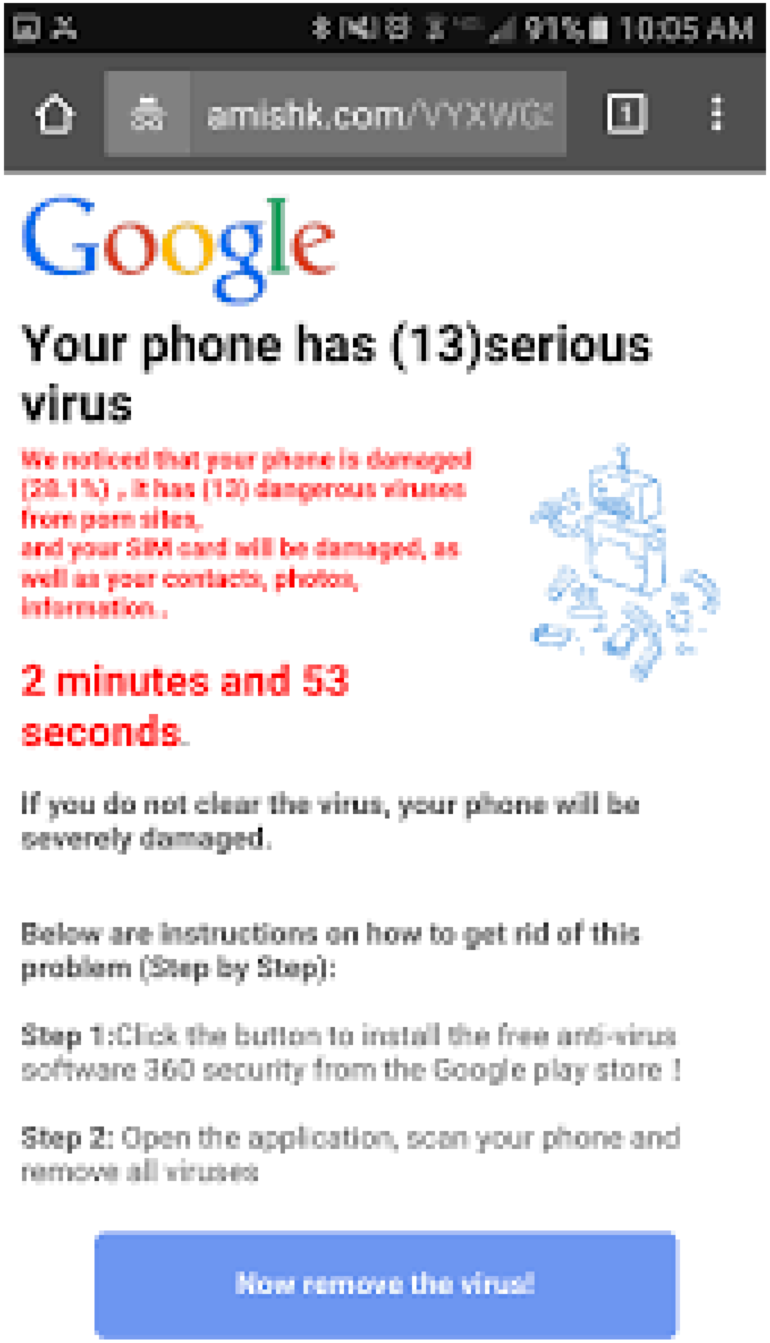
which is a: Windows Executable
from: http://78.159.122.156

What should Iceweasel do with this file?

● Open with wine-safe (default)

○ Save File

□ Do this automatically for files like this from now on.



Your phone has (13)serious virus

We noticed that your phone is damaged (28.1%) , it has (13) dangerous viruses from porn sites,
and your SIM card will be damaged, as well as your contacts, photos, information.,

2 minutes and 53 seconds.

If you do not clear the virus, your phone will be severely damaged.

Below are instructions on how to get rid of this problem (Step by Step):

Step 1: Click the button to install the free anti-virus software 360 security from the Google play store !

Step 2: Open the application, scan your phone and remove all viruses

Questions