

Computer and Network Security

Lecture 13: Malware & Common Attacks

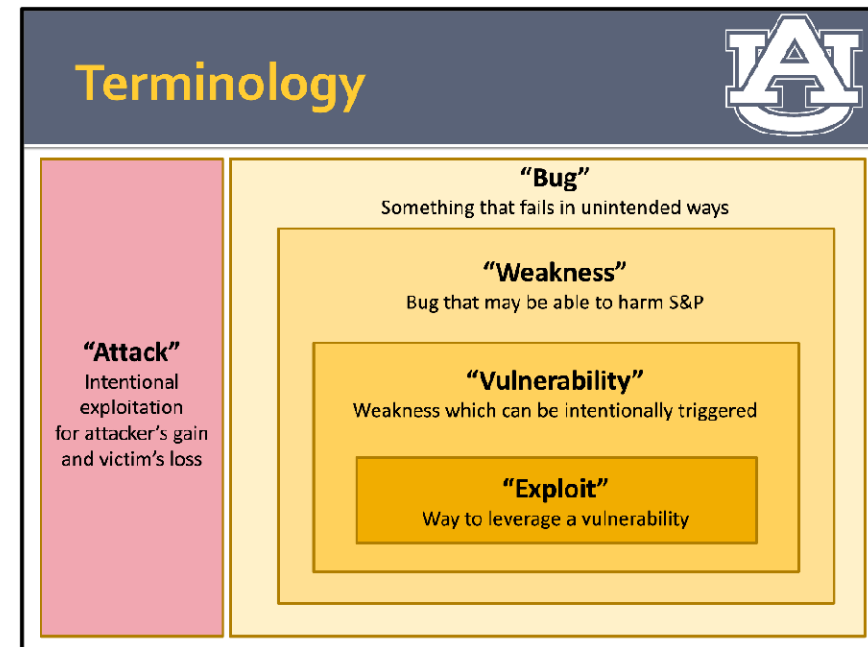
COMP-5370/6370
Fall 2024



Software Facts of Life



- Software has bugs
- Some bugs are weaknesses
- Some weaknesses are vulnerabilities
- Some vulnerabilities can be exploited
- Someone has an interest in exploiting others for gain
- Malware is a different breed of software



Malware



Malware is any software intentionally designed to:

- Operate for others' advantage
- Negatively affect the victim



Classification of Malware



- A given piece of malware can do multiple things from multiple classes
- Boundaries between classes are vague and ill-defined
- Our categorizations are just for partitioning and separation

Infection Type: Trojan Horse



A **trojan horse** is a type of malware that gains access to the device by hiding its true intent and impact to the victim.

- Social engineering attacks
- Fake anti-virus
- Re-packages apps

Lukas Stefanko
@LukasStefanko

Don't install these apps from Google Play - it's malware.

Details:
-13 apps
-all together 560,000+ installs
-after launch, hide itself icon
-downloads additional APK and makes user install it (unavailable now)
-2 apps are [#Trending](#)
-no legitimate functionality
-reported

A grid of 13 app icons from Google Play, arranged in two rows. The first row contains 7 icons and the second row contains 6 icons. Each icon is a small square with a colorful background and a white border. Below each icon is the app name and the number of installs. The apps are: Truck Cargo Simulator (100k+), Extreme Car Driving (100k+), City Traffic Moto Racer (100k+), Moto Cross Extreme (100k+), Hyper Car Driving (100k+), Extreme Car Driving (100k+), Firefighter - Fire Truck (100k+), Car Driving Simulator (100k+), Extreme Sport Car (100k+), SUV 4x4 Driving (100k+), Luxury Car Parking (100k+), Luxury Cars SUV (100k+), and SUV City Climber (100k+).

Infection Type: Virus



A **virus** is a type of malware that replicates itself on the host to stay on that host.

- Examples:
 - A single bad-app installs many bad-apps
 - Bad-behavior continues after uninstall
- Often “mutate” self to be harder to detect

Viruses Mutate for Stealth



Polymorphic

- Uses encryption or obfuscation to make instances unique
- Instance 1
 - `Encrypt(key1, ...)`
- Instance 2
 - `Encrypt(key2, ...)`

Metamorphic

- Modifies self w/ same functionality to make instances unique
- Instance 1
 - `if a > 0:...`
- Instance 2
 - `if !(a <= 0):...`

Infection Type: Worm



A **worm** is a virus that has the ability to spread itself to other devices automatically.

- Infection rate makes hard to stop
- Most commonly via vulnerable network services and network clients

The Morris Worm



- 1988: Robert Tappan Morris
 - Cornell grad-student
 - Released into the wild for ...reasons...
- Infected 10% of the Internet
- Repeatedly infected machine
- First CFAA prosecution



Infection Type: Worm



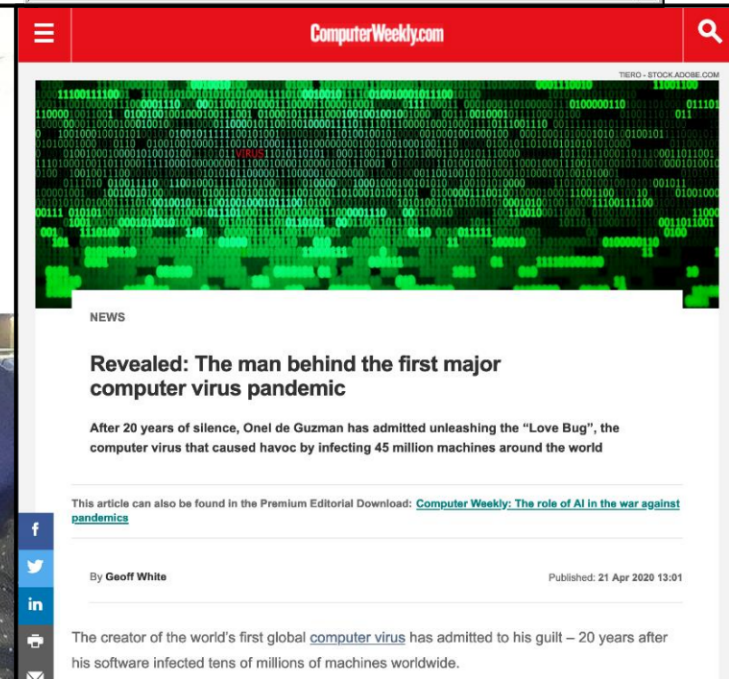
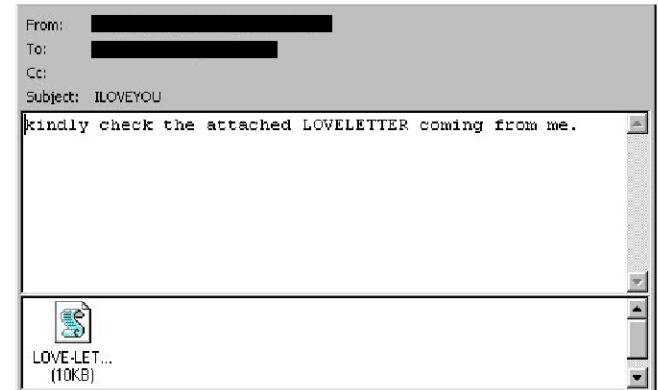
A **worm** is a virus that has the ability to spread itself to other devices automatically.

- Infection rate makes hard to stop
- Most commonly via vulnerable network services and network clients
- Technique can be re-used for other types of attacks and combined for more impact

ILOVEYOU Worm



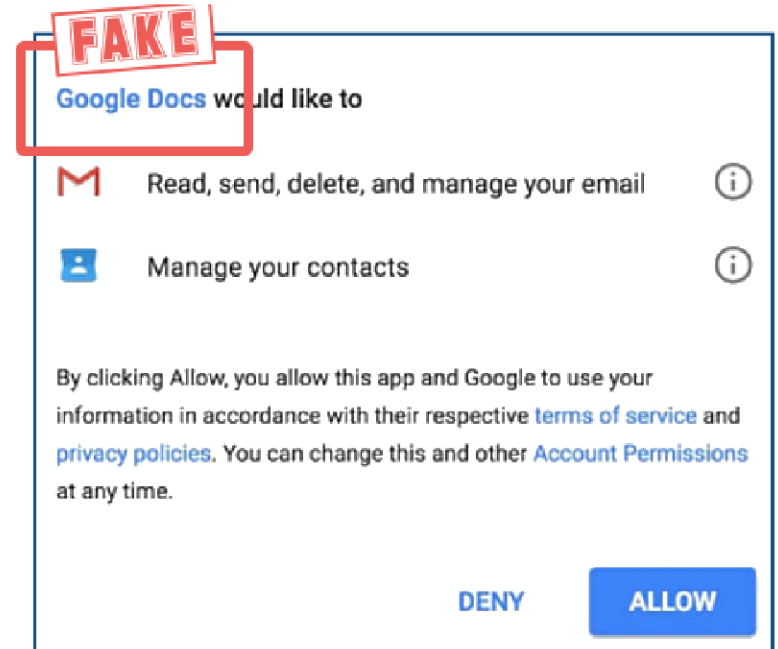
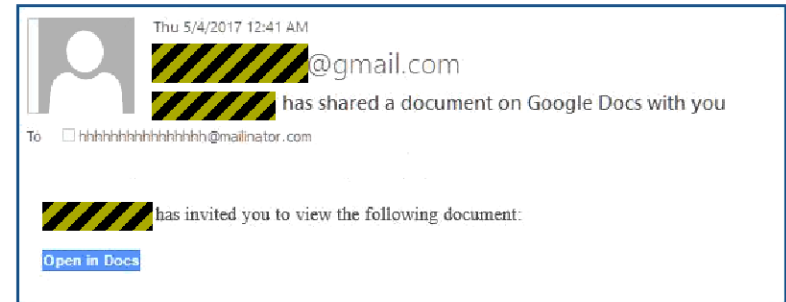
- 2000: Onel de Guzman
- Was geo-restricted... at first
- Infected 10% of Internet
- Was never prosecuted



2017 Google Phishing Worm



- A "wormed" phishing attack via misleading UI and poor validation
- Clicking link to you to the real Google Docs
- Granting permissions gave access to email



Malware



Malware is any software intentionally designed to:

- Operate for others' advantage
- Negatively affect the victim

In order to understand malware threats in the real-world, economics and incentives are often the keys.

Intent: Cryptojacking



Cryptojacking (sometimes referred to as “crypto-miners” with context) uses victim’s resources to generate direct revenue.

- Often injected via JS and run in browser
- Miner “pools” make it profitable even with limited computation

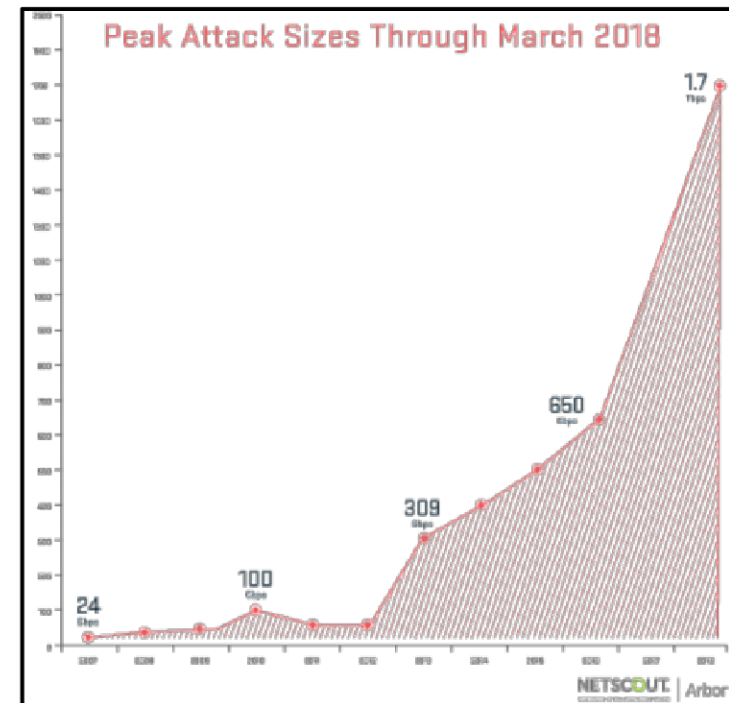
A screenshot of two news websites, Ars Technica and Wired, illustrating cryptojacking. The top portion shows the Ars Technica header with the 'ars TECHNICA' logo, a 'SUBSCRIBE' button, and a search icon. Below the header, a green sub-headline reads 'DON'T MINE ME, BRO —' followed by the main headline: 'Websites use your CPU to mine cryptocurrency even when you close your browser'. The bottom portion shows the Wired website header with the 'WIRED' logo, navigation links for 'LONG READS', 'BUSINESS', and 'CULTURE', and a search icon. Below the header, the author 'WATT BURGESS' and the date '12.02.2018 01:17 PM' are visible. The main headline reads: 'UK government websites were caught cryptomining. But it could have been a lot worse'. A sub-headline below it states: 'An accessibility plugin from Texthelp installed cryptomining code on more than 4,000 websites'.

Intent: Botnets



A **botnet** is a group of “zombie” device that has been infected with malware that causes it to participate in coordinated attacks.

- Contribute DDoS traffic
- Act as a “jump-box” for arbitrary maliciousness
- Whatever the owner wants to rent it for



Intent: Ransomware



Ransomware “encrypts” the victims files and then tries to sell the decryption key.

- Are usually untargeted attacks and any victim is acceptable to attacker
- The attacker will provide decryption key once the ransom is paid
- Payment does not always mean recovery



Intent: Ransomware



CNN politics

• LIVE TV



Colonial Pipeline did pay ransom to hackers, sources now say

By [Natasha Bertrand](#), [Evan Perez](#), [Zachary Cohen](#), [Geneva Sands](#) and [Josh Campbell](#), CNN

Updated 2300 GMT (0700 HKT) May 13, 2021

CNN politics

• LIVE TV



New details emerging about decision to shut pipeline

Meanwhile, new details are emerging about Colonial's decision to proactively shut down its pipeline last week, a move that has led to panic buying and massive lines at gas pumps.

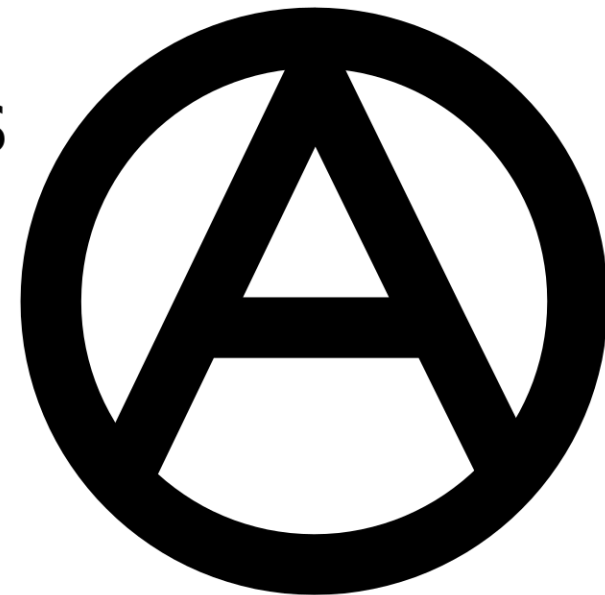
The company halted operations because its billing system was compromised, three people briefed on the matter told CNN, and they were concerned they wouldn't be able to figure out how much to bill customers for fuel they received.

Intent: Wiper



Wipers delete files en masse to deprive the victim of data and access.

- Use by activists and other ideological actors is not unheard of
- Use by criminal organizations is relatively rare
- Use by nation-state actors is widely believed



Intent: Adware



Adware is software that interferes with standard advertising models to generate revenue via third parties.



Adware – After-the-Fact



- Sometimes software becomes adware after it's widely used and installed
- Very rarely are users properly informed

A screenshot of a SourceForge blog post. The header shows the SourceForge logo and the text 'SOURCEFORGE'. Below the header, there is a navigation bar with links for 'Home / Blog / Today We Offer DevShare (Beta), A Sustainable Way To Fund Open Source Software'. The main content area features the title 'Today We Offer DevShare (Beta), A Sustainable Way To Fund Open Source Software' and the author 'By rgaloppini July 1st, 2013'. The text below the title reads: 'Today SourceForge it is excited to launch DevShare, a new opt-in, revenue-sharing aimed at giving developers a better way to monetize their projects in a transparent, and sustainable way.'

A screenshot of a Kaspersky Daily article. The header shows the Kaspersky Daily logo. Below the header, there is a navigation bar with links for 'extensions'. The main content area features the title 'Chrome extensions abuse millions with adware' and the author 'Marina Mash'. The text below the title reads: 'Too many ads on your computer lately? Malicious Chrome extensions might be to blame.'

Adware – Less-Obvious



A screenshot of a Yahoo search results page for the query 'antivirus'. The page shows search results for various antivirus products, including Kaspersky. A large, semi-transparent advertisement overlay is positioned in the center of the page. The ad has a red background on the left with a white shield containing a red 'M' and a pair of scissors cutting the shield. The right side of the ad has a green background with white and red text: 'McAfee 50% OFF HURRY UP EXPIRE SOON! Click Here'. The 'Click Here' text is underlined. The background search results are partially obscured by the ad.



COVID-19 BEST ▾ REVIEWS ▾ NEWS ▾ HOW TO ▾ CARS ▾ DEALS ▾

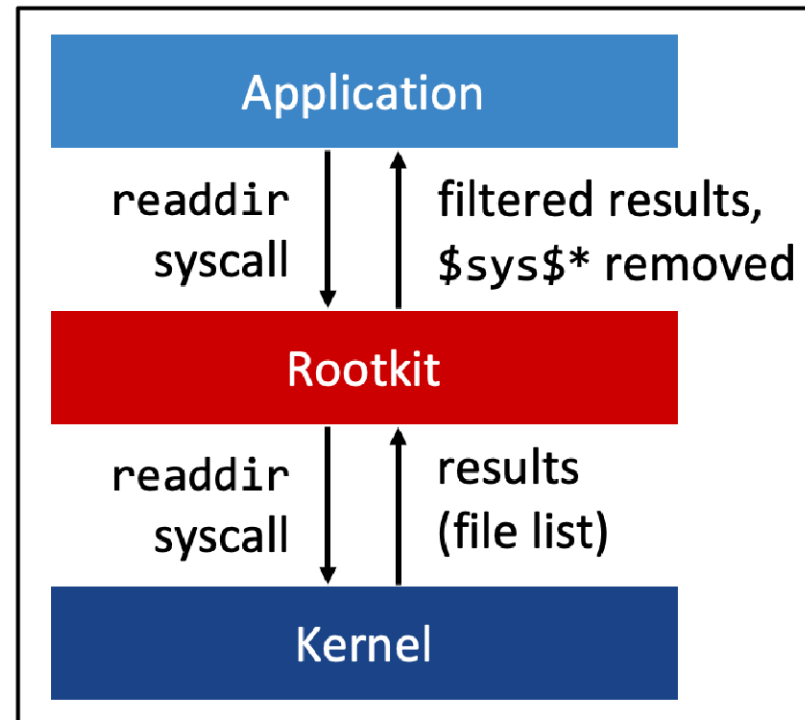
Lenovo's Superfish security snafu blows up in its face

Intent: Rootkit



Rootkits are a type of malware that strives to hide itself and other various components.

- Hook system calls to:
 - Remove certain results
 - Add certain results
- Persistence and stealth are the hallmarks



Intent: Spyware



Spyware is a type of malware that provides remote access to local data such as activity, sensors, and other information.








- Key loggers, screen captures, data exfiltration, GPS/microphone/camera data


Obvious Spyware



- Some examples are obvious based on their users and capabilities
 - Law Enforcement
 - Intelligence Orgs
 - *...the like...*
- Often sold openly
- Once sold, the buyer takes over

FinSpy / Target Features 31

- Full **Skype Monitoring** (Calls, Chats, File Transfers, Video, Contact List) 
- Recording of all **VoIP communication** 
- **Live Surveillance** through Webcam and Microphone 
- **Country Tracing** of Target 
- **Full File-Access:** Live File-Browsing, capturing of deleted/printed/opened Documents 
- **Process-based Keylogger** for faster analysis 
- Forensic Tools for **Live Remote Forensic** 
- **Enhanced Filtering** of data and recorded Information

© GAMMAGROUP 

Government Spyware



The Great iPwn

Journalists Hacked with Suspected iMessage 'Zero-Click' Exploit

By Bill Marczak, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, and Ron Deibert

December 20, 2020 [Arabic translation](#)

[Download this report](#)

Summary & Key Findings

- In July and August 2020, government operatives used a zero-click exploit to hack 36 personal phones belonging to journalists, primarily at *Al Jazeera*. The personal phone of a journalist at *Al Jazeera* was hacked.
- The phones were compromised using an exploit chain that appears to involve an invisible zero-click exploit in iMessage, a zero-day against at least iOS 13.5.1 and could have been used as early as December 2019.
- Based on logs from compromised phones, we believe the exploit was successfully deployed KISMET or a related zero-click exploit.

FORCEDENTRY

NSO Group iMessage Zero-Click Exploit Captured in the Wild

By Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ron Deibert

September 13, 2021

Summary

- While analyzing the phone of a Saudi activist infected with NSO Group's Pegasus spyware, we discovered a zero-day zero-click exploit against iMessage. The exploit, which we call **FORCEDENTRY**, targets Apple's image rendering library, and was effective against Apple iOS, MacOS and WatchOS devices.
- We determined that the mercenary spyware company NSO Group used the vulnerability to remotely exploit and infect the latest Apple devices with the Pegasus spyware. We believe that **FORCEDENTRY** has been in use since at least February 2021.
- The Citizen Lab disclosed the vulnerability and code to Apple, which has assigned the **FORCEDENTRY** vulnerability CVE-2021-30860 and describes the vulnerability as "processing a maliciously crafted PDF may lead to arbitrary code execution."

Intent: Spyware



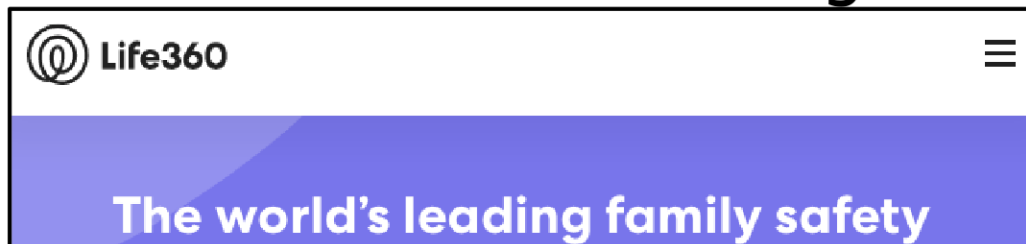
Spyware is a type of malware that provides remote access to local information such as activity, sensors, and other information.

- Key loggers, screen captures, data exfiltration, GPS/microphone/camera data
- **Does not have to be entirely hidden**

Less Obvious Spyware



- Some instances are significantly less obvious due to their branding



Johnson's Driving Summary

All Sarah Mom Dad Noah Rebec

254 Total Miles 76 mph Top Speed 40 Total Drives

Phone Usage 13

Real-time Speed Monitoring
Cruise under control.
Keep an eye on top speed while Circle members are en route — whether they're behind the wheel, on public transit, or riding with friends.

ZenScreen
A balanced digital diet.
Help your family create healthy screen habits with our partner ZenScreen. Learn about your usage, get advice from the digital assistant, and choose from a range of helpful tools, like: Smart Mornings, Daily Limit, Calm Nights, and Quiet Time.

[Get ZenScreen](#) →

The ZenScreen logo is a stylized white 'Z' inside a teal square.

See an ongoing timeline of your family's past trips, retrace your steps, and see stops you made along the way.

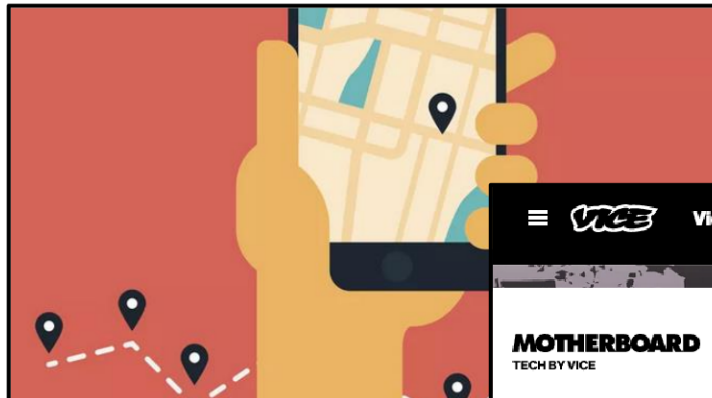
Rebecca
Last updated Now

Home
8:20 pm - 9:42 pm (1 hr, 22 min)

1 km Drive
8:16 pm - 8:20 pm (< 5 min)

A map showing a route starting from a home location, going to a location labeled '1 km Drive', and then returning. The map includes street names like 17th St NE, 15th St, and 14th St NE.

Really Sketchy Spyware



MOTHERBOARD
TECH BY VICE

Spyware Company Marketed to Domestic Abusers Gets Hacked

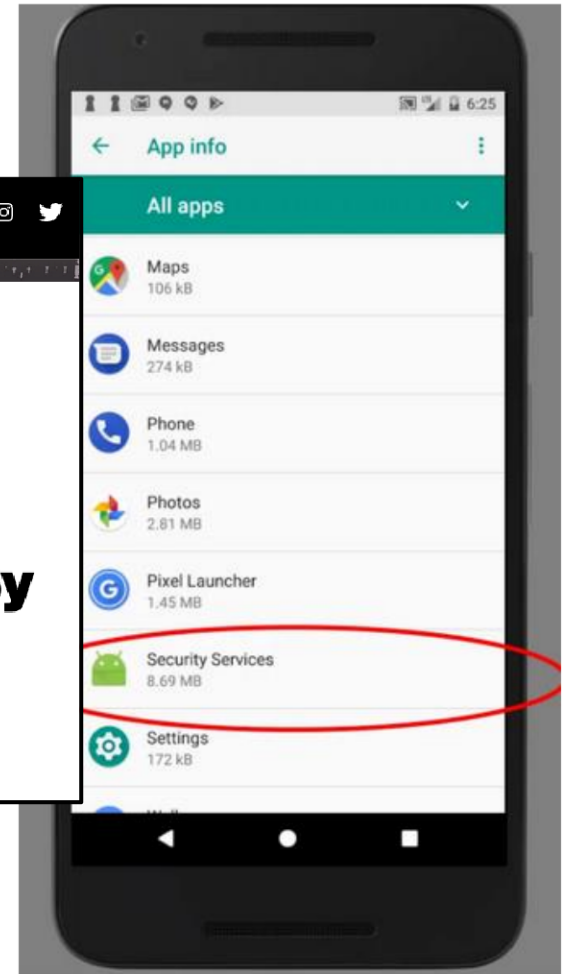
A hacker broke into the servers of TheTruthSpy, one of the most notorious stalkerware companies out there, and stole logins, audio recordings, pictures, and text messages, among other data.

By Lorenzo Franceschi-Bicchieri

MOTHERBOARD
TECH BY VICE





'I See You': A Domestic Violence Survivor Talks About Being Surveilled By Her Ex

pluspluspodcast dives into the horrifying world of smartphone spyware.









Is it Spyware?



 Location ^
For example: region, IP address, GPS coordinates, or information about things near the user's device
 Web history ^
The list of web pages a user has visited, as well as associated data such as page title and time of visit
 User activity ^
For example: network monitoring, clicks, mouse position, scroll, or keystroke logging
 Website content ^
For example: text, images, sounds, videos, or hyperlinks



 Personally identifiable information ^
For example: name, address, email address, age, or identification number
 Financial and payment information ^
For example: transactions, credit card numbers, credit ratings, financial statements, or payment history
 Authentication information ^
For example: passwords, credentials, security question, or personal identification number (PIN)
 Personal communications ^
For example: emails, texts, or chat messages
 Location ^
For example: region, IP address, GPS coordinates, or information about things near the user's device
 User activity ^
For example: network monitoring, clicks, mouse position, scroll, or keystroke logging

Is it Spyware?



Respondus[®]

Assessment Tools for Learning Systems

The screenshot shows a technical support page from Respondus. At the top, there are links for 'Submit a Ticket' and 'Sign in'. The main heading is 'LockDown Browser + Respondus Monitor'. Below this is a search bar and a breadcrumb trail: 'Respondus Support > LockDown Browser + Respondus Monitor > Student Support'. The article title is 'How do I install LockDown Browser?' and it is dated '7 months ago'. A video player is embedded, showing a Windows security warning dialog box for 'LOCKDOWN' with a 'Share' button. Below the video is a list of 6 numbered steps for installation, including logging in as an administrator, downloading the installer from a specific URL, and running the installer.

Respondus[®]
TECHNICAL SUPPORT [Submit a Ticket](#) [Sign in](#)

LockDown Browser + Respondus Monitor

How can we help you?

Respondus Support > LockDown Browser + Respondus Monitor > Student Support

How do I install LockDown Browser?

7 months ago

Windows computer

We have a helpful video that shows how to install LockDown Browser on a Windows computer:

Installing LockDown Browser to Windows [Share](#)

Watch on [YouTube](#)

1. Log in as a local administrator with full rights. (Windows Control Panel-User Accounts-"user account"-Change your account type-"Administrator").
2. Go to "https://download.respondus.com/ockdown/download.php?i=xxxxxxxx" where "xxxxxxxx" is your institution's unique 9-dgi. Institution ID. Do not use the web address with "xxxxxxxx". It must be the 9-digit number provided to your institution.)
3. Download the LockDown Browser installer package. It will be in the form of "LockDownBrowser-2.0-xxx.exe" where "xxx" is the current version number.
4. Locate the installer package in your Downloads folder and run it.
5. Accept all the default prompts to install LockDown Browser.
6. Most Learning Management Systems require that you first open a standard browser (Chrome, Firefox, etc.) log in to the LMS, and then use the "Launch LockDown Browser" button on the quiz summary page.

For Canvas "Classic" quizzes and Blackboard Learn quizzes, go to your desktop and double click on the "LockDown Browser" icon (A blue diamond with a gold padlock) to start LockDown Browser.

Is it Spyware?



Respondus[®]

Assessment Tools for Learning Systems

Terms of Use/End User License Agreement - LockDown Browser

Terms of Use/End User License Agreement - LockDown Browser

Last Updated: January 10, 2022

System Check. The System Check gathers certain information from your computing device, the networking environment, and the institution's Learning Management System.

Is it Spyware?



Respondus[®]

Assessment Tools for Learning Systems

[Respondus Support](#) > [LockDown Browser + Respondus Monitor](#) > [Student Support](#)

Permissions Dialog Appears

2 years ago

When you click on the "Launch LockDown Browser" button, whatever browser you are using will initially ask you permission to open the LockDown Browser application installed on your computer. The dialog will be slightly different, depending on the

in each case you must grant permission.

Open URL:Respondus LockDown Browser?

Remember my choice for URL:Respondus LockDown Browser links

Open URL:Respondus LockDown Browser

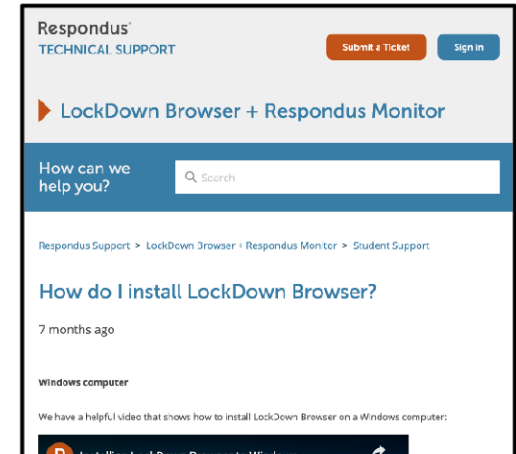
Don't open

Is it Spyware?

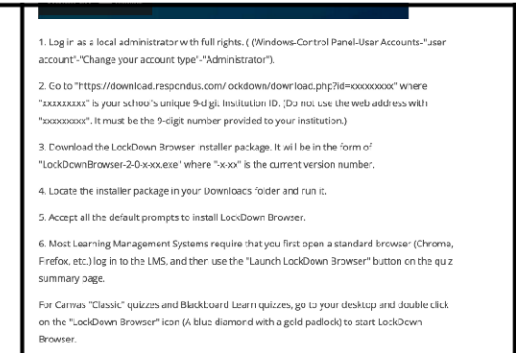


Respondus[®]

Assessment Tools for Learning Systems



1. Log in as a local administrator with full rights. ((Windows-Control Panel-User Accounts-"user account"- "Change your account type"- "Administrator").



EFF Thinks It Is



Most proctoring apps are effectively indistinguishable from spyware, which is malware that is commonly used to track unsuspecting users' actions on their devices and across the Internet.



Proctoring Apps Subject Students to Unnecessary Surveillance
With COVID-19 forcing millions of teachers and students to rethink in-person schooling, this moment is ripe for an innovation in learning. Unfortunately, ...
eff.org

4:13 PM · Oct 11, 2020 · TweetDeck

Classification of Malware



- A given piece of malware can do multiple things from multiple classes
- Boundaries between classes are vague and ill-defined
- Our categorizations are just for partitioning and separation



Malware Distribution



Malware is distributed via almost every imaginable technique and vector.

- Installed via Exploitation

Install via Exploitation



ars TECHNICA SUBSCRIBE SIGN IN

IN THE WILD —

Windows code-execution zeroday is under active exploit, Microsoft warns

There's no patch available now. Here's what to do until Microsoft issues one.

DAN GOODIN - 3/23/2020, 2:40 PM

ZERODIUM Payouts for Desktops/Servers*

Payout	OS	Exploit
Up to \$1,000,000	Win	Win RCE Zero Click
Up to \$500,000	Win	Chrome RCE+LPE
Up to \$250,000	Win	MS Outlook RCE
Up to \$200,000	Win	MS Exchange RCE
Up to \$200,000	Linux	Apache RCE
Up to \$200,000	Linux	OpenSSL RCE
Up to \$200,000	Linux	PHP RCE
Up to \$200,000	Win/Linux	VMware ESXi VME
Up to \$200,000	Win/Linux	Thunderbird RCE
Up to \$100,000	Linux	Sendmail RCE
Up to \$100,000	Linux	Postfix RCE
Up to \$100,000	Linux	Dovecot RCE
Up to \$100,000	Linux	Exim RCE
Up to \$100,000	Linux	nginx RCE
Up to \$100,000	Mac	Safari RCE+LPE
Up to \$100,000	Win	Edge RCE+LPE
Up to \$100,000	Win	Firefox RCE+LPE
Up to \$100,000	Win	Word/Excel RCE
Up to \$100,000	Linux	WordPress RCE
Up to \$100,000	Linux	cPanel/WHM RCE
Up to \$100,000	Linux	Plesk RCE
Up to \$100,000	Linux	Webmin RCE
Up to \$80,000	Win/Linux	VMware WS VME
Up to \$80,000	Win	Adobe PDF RCE+SBX
Up to \$80,000	Win	WinRAR RCE
Up to \$80,000	Win	7-Zip RCE
Up to \$80,000	Win	Windows LPE+SBX
Up to \$50,000	Win/Mac	USB LPE
Up to \$50,000	Win	Antivirus RCE
Up to \$50,000	Win	WinZip RCE
Up to \$50,000	Linux	tar RCE
Up to \$50,000	Mac	macOS LPE+SBX
Up to \$50,000	Linux	Linux LPE
Up to \$50,000	BSD	BSD LPE
Up to \$10,000	Win	Routers RCE
Up to \$10,000	Win	Antivirus LPE
Up to \$10,000	Win	phpBB RCE
Up to \$10,000	Linux	vBulletin RCE
Up to \$10,000	Linux	MyBB RCE
Up to \$10,000	Linux	Joomla RCE
Up to \$10,000	Linux	Drupal RCE
Up to \$10,000	Linux	Roundcube RCE
Up to \$10,000	Linux	Horde RCE

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners. 2019/01 © zerodium.com

- 0-Day Vulnerability
 - Brand-new to vendor, defenders, and users
 - Find, exploit, & install

ZERODIUM Payouts for Mobiles*

Payout	OS	Exploit
Up to \$2,500,000	Android	Android FCP Zero Click
Up to \$2,000,000	IOS	IOS FCP Zero Click
Up to \$1,500,000	IOS/Android	WhatsApp RCE+LPE Zero Click
Up to \$1,500,000	IOS	iMessage RCE+LPE Zero Click
Up to \$1,000,000	IOS/Android	WhatsApp RCE+LPE
Up to \$1,000,000	IOS/Android	SMS/MMS RCE+LPE
Up to \$500,000	IOS	Persistence
Up to \$500,000	IOS/Android	WeChat RCE+LPE
Up to \$500,000	IOS	iMessage RCE+LPE
Up to \$500,000	IOS/Android	FB Messenger RCE+LPE
Up to \$500,000	IOS/Android	Signal RCE+LPE
Up to \$500,000	IOS/Android	Telegram RCE+LPE
Up to \$500,000	IOS/Android	Email App RCE+LPE
Up to \$500,000	Android	Chrome RCE+LPE
Up to \$500,000	IOS	Safari RCE+LPE
Up to \$200,000	IOS/Android	Baseband RCE+LPE
Up to \$200,000	IOS/Android	LPE to Kernel/Root
Up to \$200,000	IOS/Android	Media Files RCE+LPE
Up to \$200,000	IOS/Android	Documents RCE+LPE
Up to \$200,000	Android	SBX for Chrome
Up to \$200,000	Android	Chrome RCE w/o SBX
Up to \$200,000	IOS	SBX for Safari
Up to \$200,000	IOS	Safari RCE w/o SBX
Up to \$100,000	IOS/Android	Code Signing Bypass
Up to \$100,000	IOS/Android	WiFi RCE
Up to \$100,000	IOS/Android	RCE via MITM
Up to \$100,000	Android	LPE to System
Up to \$100,000	IOS/Android	Information Disclosure
Up to \$100,000	IOS/Android	[k]ASLR Bypass
Up to \$100,000	Android	PIN Bypass
Up to \$100,000	IOS	Passcode Bypass
Up to \$100,000	IOS	Touch ID Bypass

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners. 2019/09 © zerodium.com

Install via Exploitation



The image shows two screenshots. The top screenshot is from the Exploit Database website, displaying search filters for 'Verified' and 'Has App', a search bar with 'chrome' entered, and sorting options. The bottom screenshot is from the Wana Decrypt0r 2.0 ransomware interface, showing a red warning message: 'Oops, your files have been encrypted!'. It includes a padlock icon, a countdown timer for payment (02:23:57:37), and instructions on how to recover files by paying in Bitcoin. A Bitcoin address is provided for payment, and buttons for 'Check Payment' and 'Decrypt' are visible at the bottom.

- 0-Day Vulnerability
- N-Day Vulnerability
 - Patch exists but is not applied to host
 - Old \neq Ineffective
 - Google, exploit, & install

Install via Exploitation



This block contains two overlapping screenshots. The top screenshot is from a Microsoft Support page, showing the title 'Windows 7 support ended on January 14, 2020' and the URL 'Windows 7'. The bottom screenshot is from an Ars Technica article, showing the site's navigation bar with 'ars TECHNICA', 'SUBSCRIBE', and 'SIGN IN' buttons. The article title is 'The XPocalypse is upon us: Windows XP support has...' and the author is 'PETER BRIGHT - 4/8/2014, 10:10 AM'.


- 0-Day Vulnerability
- N-Day Vulnerability
- Perma-Vuln (∞ -day)
 - Worse version of n-day
 - **Will never be patched**

This block contains a screenshot of a Wired article. The article title is 'Security News This Week: Windows XP Source Code Got Leaked All Over the Internet'. The author is 'BRIAN BARRETT' and the date is '09.26.2020 09:00 AM'. The Wired logo is visible at the top of the article snippet.

Install via Exploitation



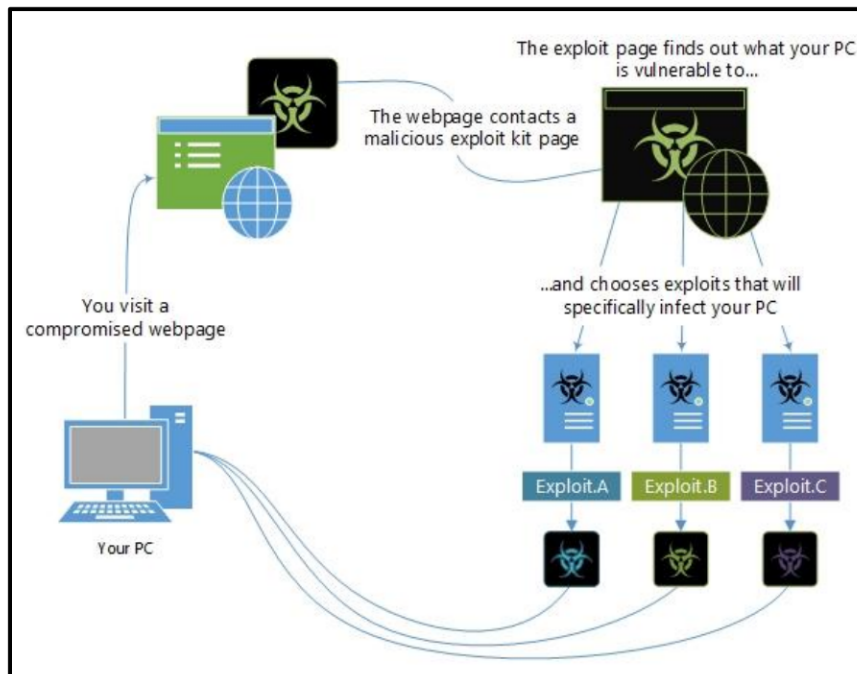
GitHub repository page for `danielmiessler / SecLists`. The repository is titled "CYBERPUNK" and contains a file named "Password Cracker THC Hydra". The file is located in the "CyberPunk » Password Attacks" directory.

The Hydra logo is a stylized, green and white dragon-like creature with multiple heads, set against a dark green background with a binary code pattern.

10	3COM	<BLANK>	PASSWORD
11	3COM	<BLANK>	admin
12	3COM	<BLANK>	comcomcom
13	3COM	<N/A>	<BLANK>
14	3COM	<N/A>	PASSWORD
15	3COM	<N/A>	admin

- 0-Day Vulnerability
- N-Day Vulnerability
- Perma-Vuln (∞ -day)
- Password Guessing
 - **Default creds are bad**
 - Repeatedly try until successful or blocked
 - Gain access & install

Install via Exploitation



- 0-Day Vulnerability
- N-Day Vulnerability
- Perma-Vuln (∞ -day)
- Password Guessing
- Drive-by-Download
 - Clients are largely not arbitrarily accessible
 - Get client to interact w/ attacker & hijack
 - Get interaction, profile, select, & install

Malware Distribution



Malware is distributed via almost every imaginable technique and vector.

- Installed via Exploitation
- Installed via Third-Party

Installed via Third-Party

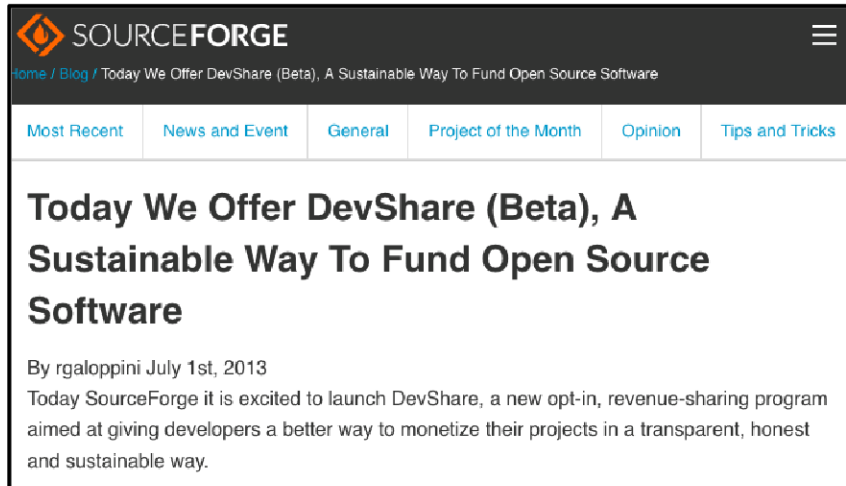


A screenshot of a webpage from ars TECHNICA. The header is black with the 'ars TECHNICA' logo on the left, a green 'SUBSCRIBE' button, and a search icon and 'SIGN IN' link on the right. Below the header, the text 'BIZ & IT' is in green. The main headline reads 'Adware vendors buy Chrome Extensions to send ad- and malware-filled updates'. A sub-headline states 'Once in control, they can silently push new ad-filled "updates" to those users.' The author is 'RON AMADEO' and the date is '1/17/2014, 5:10 PM'.

- Added to benign SW by developer
 - Leverage existing userbase & trust
 - Change of control

A screenshot of a webpage from The New York Times. The header is white with the 'The New York Times' logo in the center, a hamburger menu icon on the left, and a user profile icon on the right. Below the header, there are links for 'SUBSCRIBE NOW' and 'LOG IN'. The main headline reads 'Adblock Plus, Created to Protect Users From Ads, Instead Opens the Door'. The author is 'By Sapna Maheshwari' and the date is 'Sept. 18, 2016'. At the bottom, there are social media sharing icons for Facebook, Twitter, Email, Print, and Bookmark.

Installed via Third-Party



SOURCEFORGE

home / Blog / Today We Offer DevShare (Beta), A Sustainable Way To Fund Open Source Software

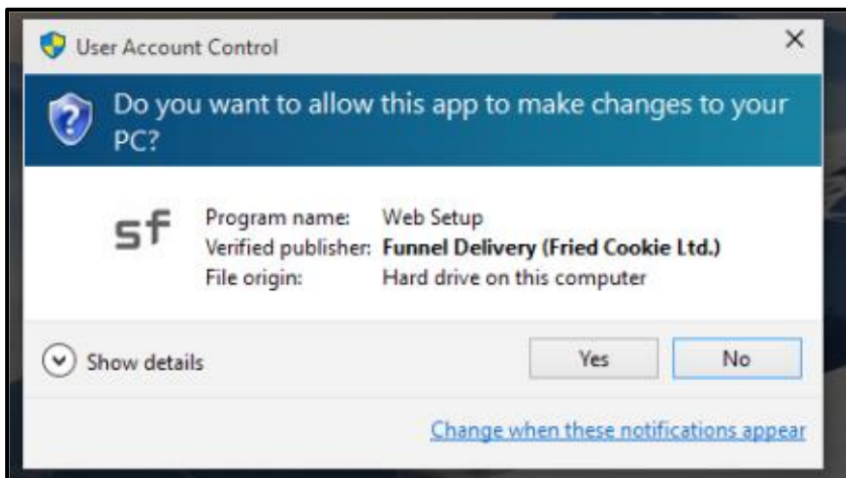
Most Recent | News and Event | General | Project of the Month | Opinion | Tips and Tricks

Today We Offer DevShare (Beta), A Sustainable Way To Fund Open Source Software

By rgaloppini July 1st, 2013

Today SourceForge it is excited to launch DevShare, a new opt-in, revenue-sharing program aimed at giving developers a better way to monetize their projects in a transparent, honest and sustainable way.

- Added to benign SW by developer
 - Leverage existing userbase & trust
 - Change of control
 - Explicitly for revenue



User Account Control

Do you want to allow this app to make changes to your PC?

sf Program name: Web Setup
Verified publisher: **Funnel Delivery (Fried Cookie Ltd.)**
File origin: Hard drive on this computer

Show details Yes No

[Change when these notifications appear](#)

Installed via Third-Party



- Added to benign SW by developer
- Added by attacker via supply-chain access
 - Unknown to developer
 - External dependencies

Installed via Third-Party



WIRED SIGN IN SUBSCRIBE

ANDY GREENBERG SECURITY 05.03.2015 07:00 AM

A Mysterious Hacker Group Is On a Supply Chain Hijacking Spree

A group of likely Chinese hackers has poisoned the software of at least six companies in just the past three years.

ars TECHNICA SUBSCRIBE SIGN IN

BIZ & IT

SourceForge grabs GIMP for Windows' account, wraps installer in bundle-pushing adware [Updated]

SOURCEFORGE

Home / Blog / GIMP-Win project wasn't hijacked, just abandoned

Most Recent News and Event General Project of the Month Opinion Tips and Tricks

GIMP-Win project wasn't hijacked, just abandoned

By Community Team May 27th, 2015

[Updated on 22th of June 2015 : Though the two-day offers test completed May 27th, we took further action on our project mirroring program on June 18th. See the update at <http://sourceforge.net/blog/project-mirroring-policies-will-be-revisited-with-our-community-panel-existing-mirrors-removed/>]

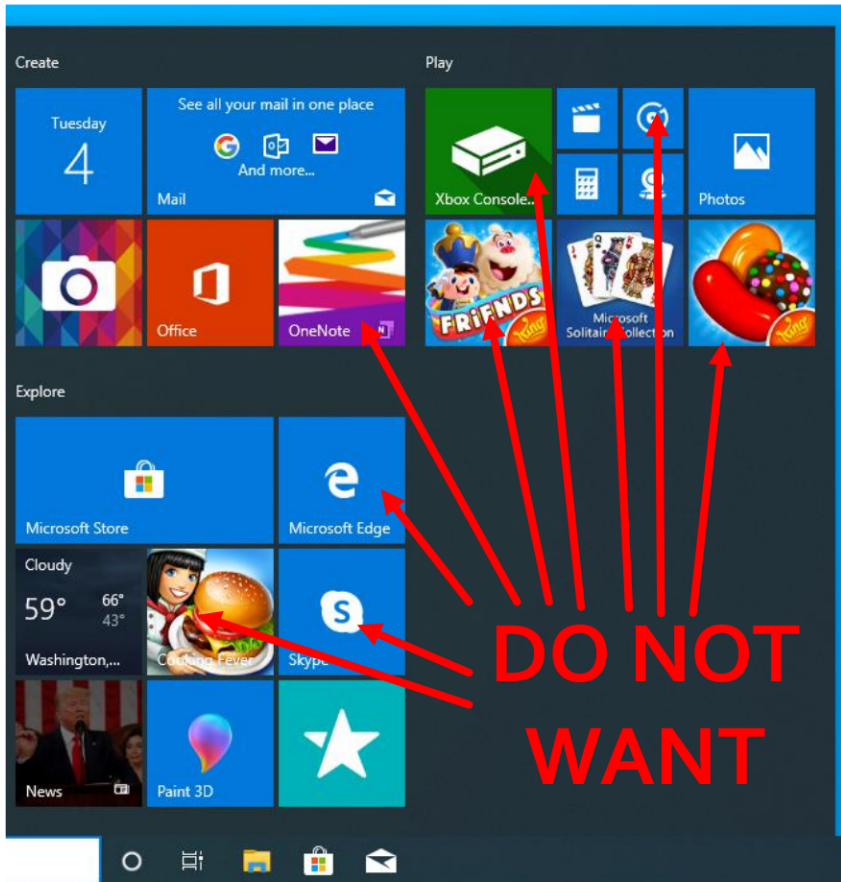
- Added to benign SW by developer
- Added by attacker via supply-chain access
 - Unknown to developer
 - External dependencies
 - Distribution mechanism

Installed via Third-Party



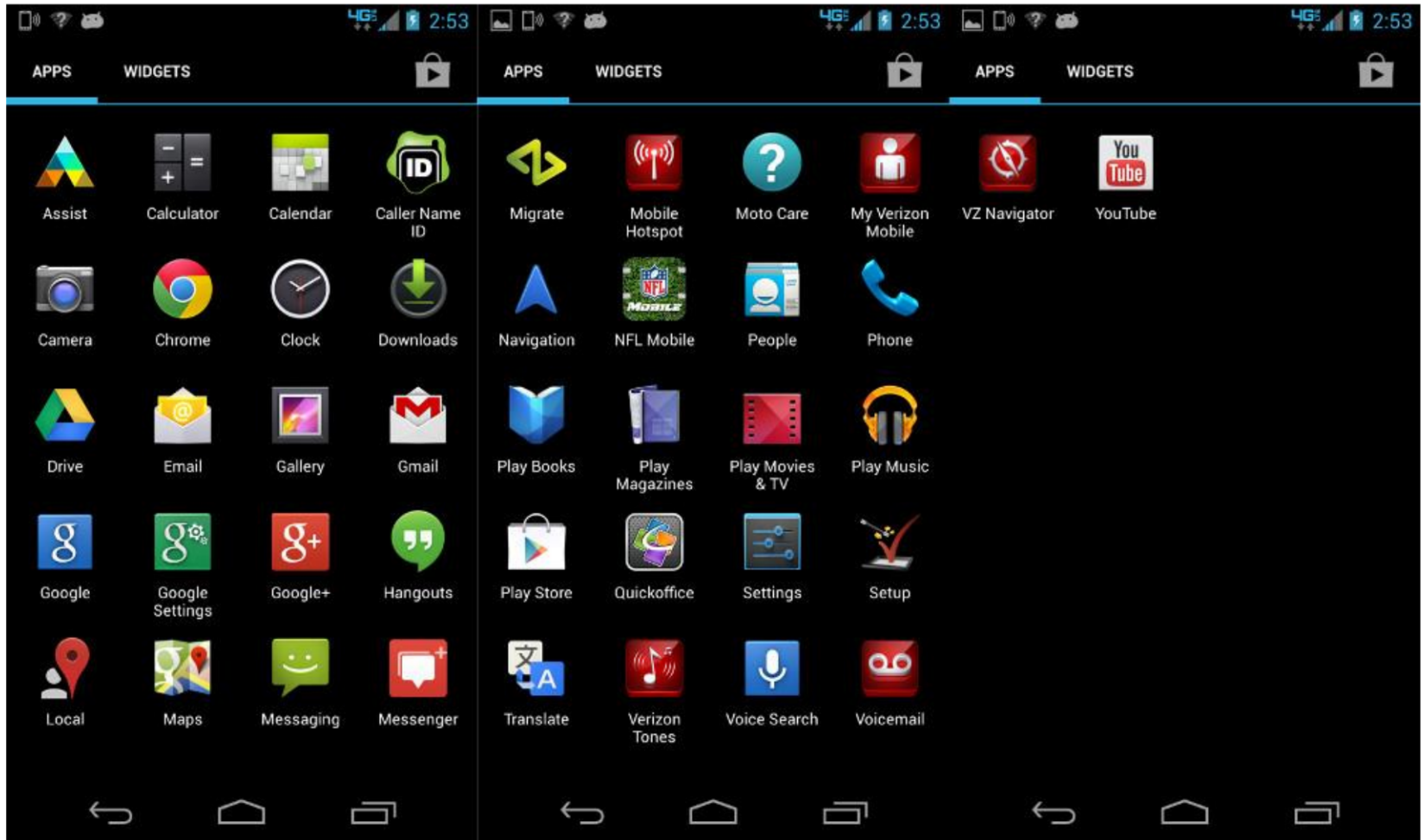
- Added to benign SW by developer
- Added by attacker via supply-chain access
- “Owner” adds for compliance/policy
 - Bossware, mobile device management (MDM)

Installed via Third-Party

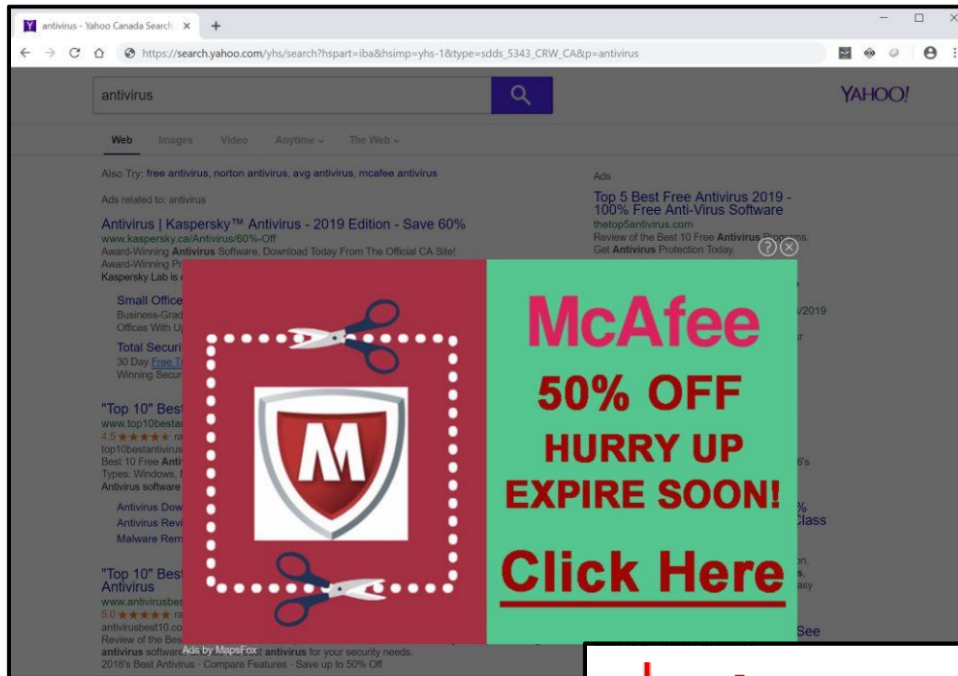


- Added to benign SW by developer
- Added by attacker via supply-chain access
- “Owner” adds for compliance/policy
- Preinstalled
 - May not be obvious
 - May be force-installed

Pre-Installed Malware



Adware – Less-Obvious



COVID-19 BEST ▾ REVIEWS ▾ NEWS ▾ HOW TO ▾ CARS ▾ DEALS ▾

Lenovo's Superfish security snafu blows up in its face

The Story of Superfish



THE BUSINESS JOURNALS Select a City Sign In

SAN FRANCISCO BUSINESS TIMES 40 UNDER 40 Special Section: Meet the 40 Under 40 Class of 2020 > LIMITED TIME OFFER Subscribe Now

INDUSTRIES & TOPICS NEWS LISTS & LEADS PEOPLE & COMPANIES EVENTS LEADERSHIP TRUST MORE... Q

Technology

Superfish dives deep into visual search

WIRED

If you buy something using links in our stories, we may earn a commission. [Learn more.](#)

Technology

Lenovo faces huge backlash over Superfish adware

ars TECHNICA SUBSCRIBE Q SIGN IN

BIZ & IT

Lenovo PCs ship with man-in-the-middle adware that breaks HTTPS connections [Updated]

ars TECHNICA SUBSCRIBE Q SIGN IN

BIZ & IT

How to remove the Superfish malware: What Lenovo doesn't tell you

Uninstalling the software doesn't undo the damage it does to your system.

PETER BRIGHT - 2/19/2015, 4:55 PM

- Came pre-installed on Lenovo laptops
- Was an ad-supported visual search startup
- Actively MitM traffic for ad injection
- Injected root CA
- **SAME PRIVATE KEY ON EVERY SINGLE INSTALL**

Malware Distribution



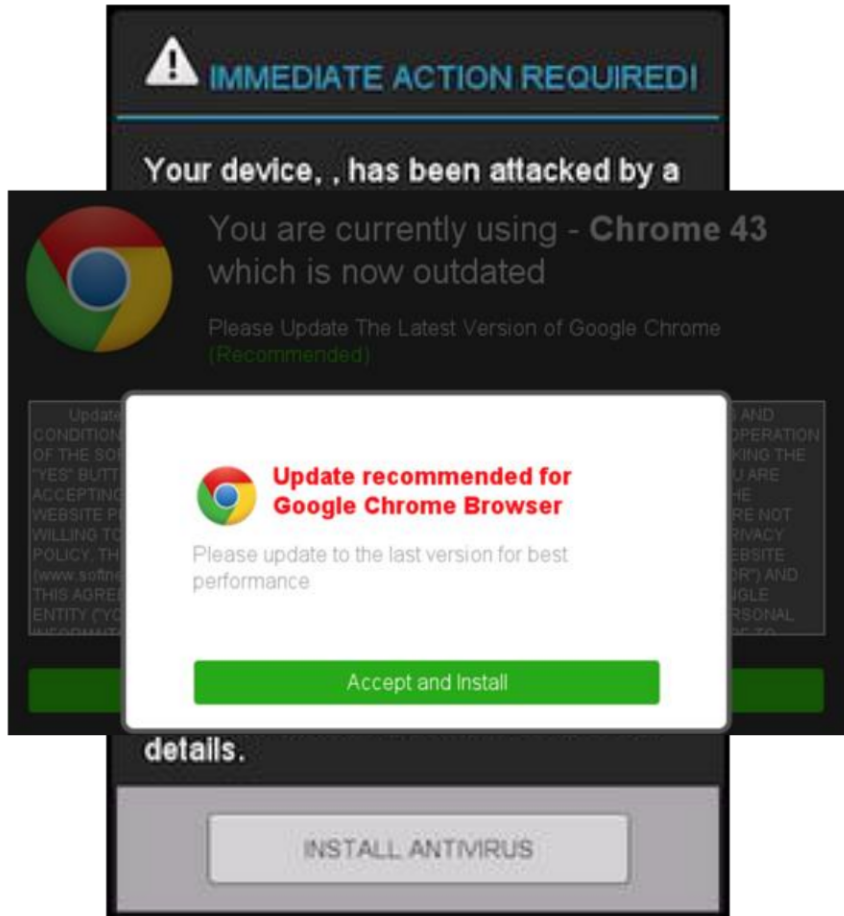
Malware is distributed via almost every imaginable technique and vector.

- Installed via Exploitation
- Installed via Third-Party
- Installed via User

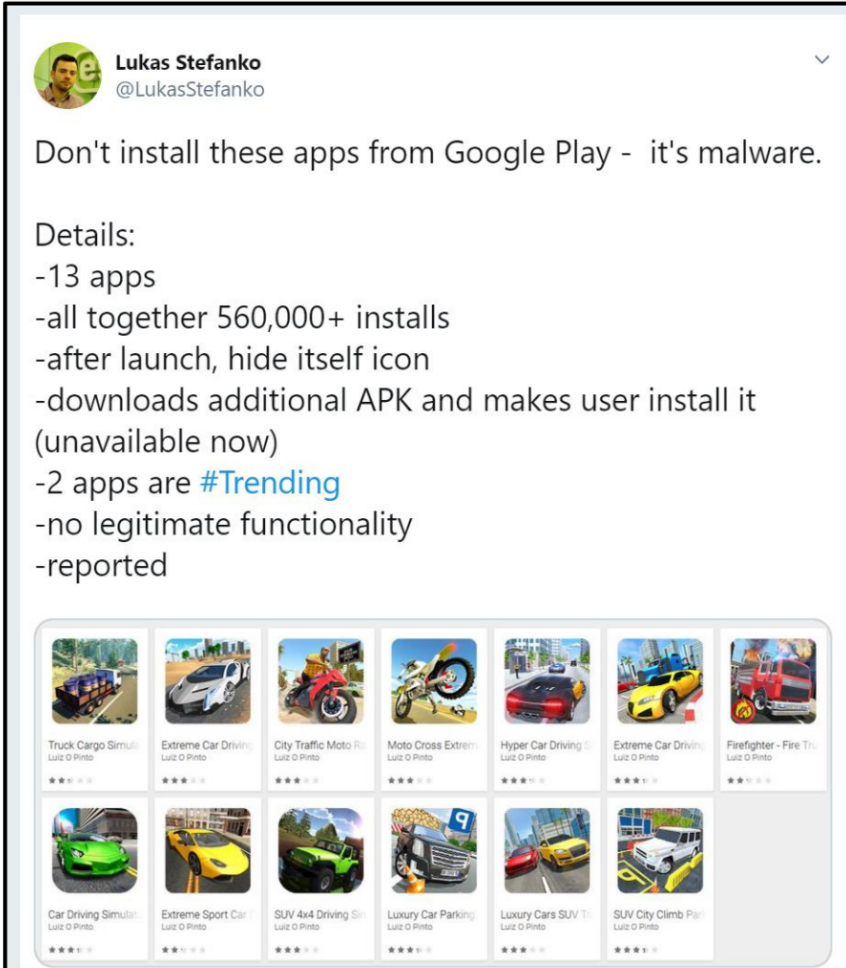
Installed via User



- Social Engineering
 - User is tricked into installing themselves
 - Can be last-resort of drive-by-download



Installed via User
















Lukas Stefanko
@LukasStefanko

Don't install these apps from Google Play - it's malware.

Details:

- 13 apps
- all together 560,000+ installs
- after launch, hide itself icon
- downloads additional APK and makes user install it (unavailable now)
- 2 apps are **#Trending**
- no legitimate functionality
- reported

 Truck Cargo Simulator Luz O Pinto ★ ★ ★ ★	 Extreme Car Driving Luz O Pinto ★ ★ ★ ★	 City Traffic Moto Racer Luz O Pinto ★ ★ ★ ★	 Moto Cross Extreme Luz O Pinto ★ ★ ★ ★	 Hyper Car Driving Luz O Pinto ★ ★ ★ ★	 Extreme Car Driving Luz O Pinto ★ ★ ★ ★	 Firefighter - Fire Truck Luz O Pinto ★ ★ ★ ★
 Car Driving Simulator Luz O Pinto ★ ★ ★ ★	 Extreme Sport Car Luz O Pinto ★ ★ ★ ★	 SUV 4x4 Driving Simulator Luz O Pinto ★ ★ ★ ★	 Luxury Car Parking Luz O Pinto ★ ★ ★ ★	 Luxury Cars SUV Luz O Pinto ★ ★ ★ ★	 SUV City Climb Luz O Pinto ★ ★ ★ ★	

- Social Engineering
- Freeware/Shareware
 - Cheap, low-effort applications as bait
 - Packed w/ arbitrary libs
 - *If you can't figure out what the product is... it's probably you.*

Installed via User



A screenshot of the The Guardian website. The header includes the text "Support The Guardian" and "Available for everyone, funded by readers". There are "Contribute" and "Subscribe" buttons. The main navigation bar lists "News", "Opinion", "Sport", "Culture", and "Lifestyle". Below this, there are links for "Film", "Books", "Music", "Art & design", "TV & radio", "Stage", "Classical", and "Games". The article title is "Fortnite" and a yellow banner indicates "This article is more than 2 years old". The main headline reads "Fortnite players using Android phones at risk of malware infections".

A screenshot of the WIRED website. The header includes the WIRED logo, "SIGN IN", and "SUBSCRIBE" buttons. The article is by "BRIAN BARRETT" in the "SECURITY" category, dated "08.16.2018 06:00 AM". The headline is "Impostor Fortnite Android Apps Are Already Spreading Malware".

A screenshot of the ars TECHNICA website. The header includes the ars TECHNICA logo, "SUBSCRIBE", a search icon, and "SIGN IN" buttons. A green banner reads "FREE AIN'T FREE —". The headline is "Malicious warez hosted on Bitbucket get more than 500,000 downloads". The sub-headline says "Ongoing campaign installs credential stealers, RATs, ransomware, and cryptominers." The author is "DAN GOODIN" and the date is "2/5/2020, 3:10 PM".

- Social Engineering
- Freeware/Shareware
- Untrusted sources
 - Even if it works 100% the same, it's most likely not
 - **SIDE-LOAD APKs are extremely dangerous**

Installed via User



ars TECHNICA SUBSCRIBE SEARCH SIGN IN

FREE AIN'T FREE —

Malicious warez hosted on Bitbucket get more than 500,000 downloads

Ongoing campaign installs credential stealers, RATs, ransomware, and cryptominers.

DAN GOODIN - 2/5/2020, 3:10 PM

KrebsonSecurity

In-depth security news and investigation

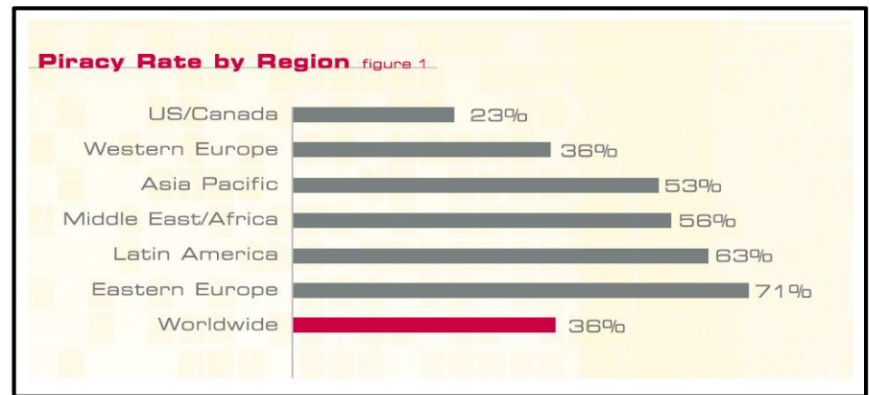
20 Software Cracks: A Great Way to Infect Your PC

JUN 11

I often get emails from people asking if it's safe to download executable programs from peer-to-peer filesharing networks. I always answer with an emphatic "NO!" and the warning that pirated software and cracks — programs designed to generate product keys or serial numbers for popular software and games — are almost always bundled with some kind of malware. But I seldom come across more than anecdotal data that backs this up.

- Social Engineering
- Freeware/Shareware
- Untrusted sources
- “Cracked” software
 - Promise of free-version of paid software
 - Often actually are “key-hacked” version
 - WaReZ, Torrents, P2P

Software Piracy



Office Home & Student 2019

Microsoft Corporation

For 1 PC or Mac For 1 person

- One-time purchase for 1 PC or Mac
- Classic 2019 versions of Word, Excel, and PowerPoint
- Microsoft support included for 60 days at no extra cost
- Licensed for home use

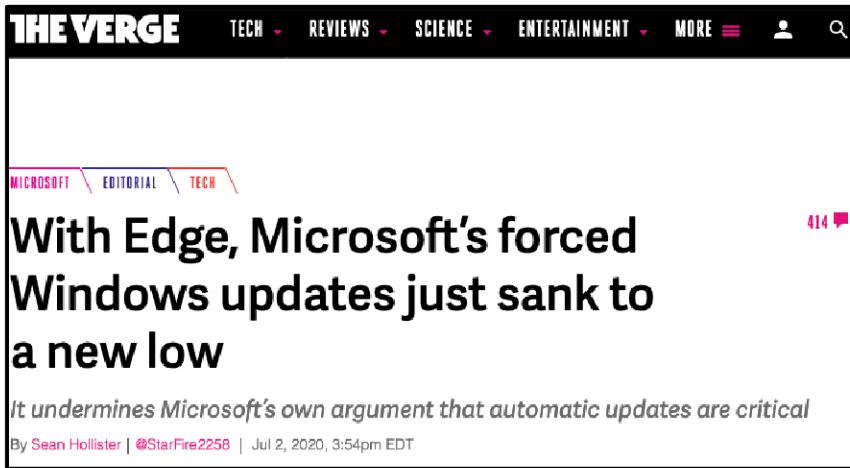
All languages included. Compatible with Windows 10 or macOS*

*Go to office.com/systemrequirements for compatible versions of Windows 10 and macOS and for other feature requirements.

\$149.99

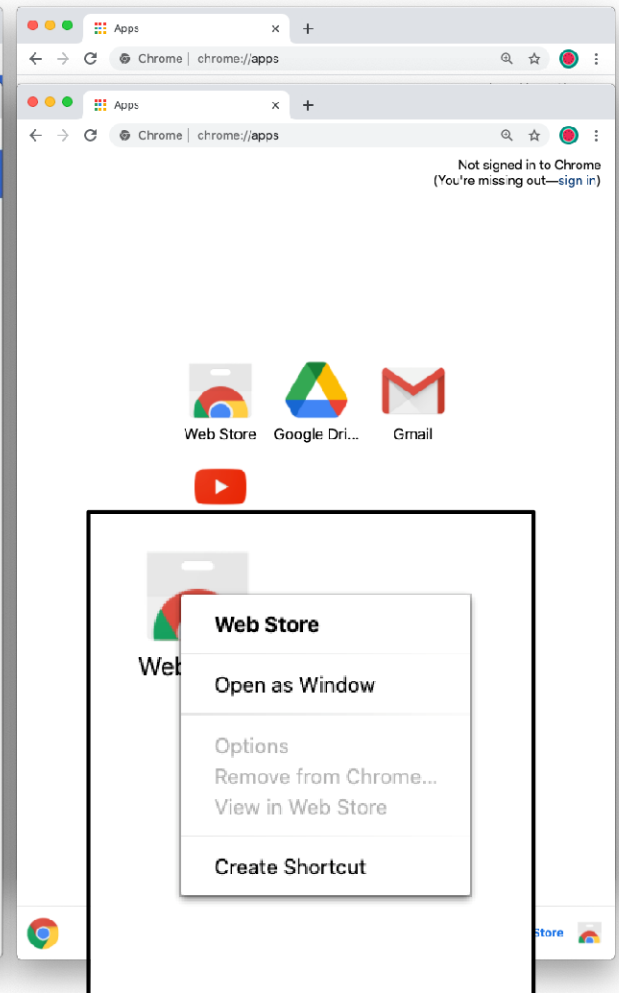
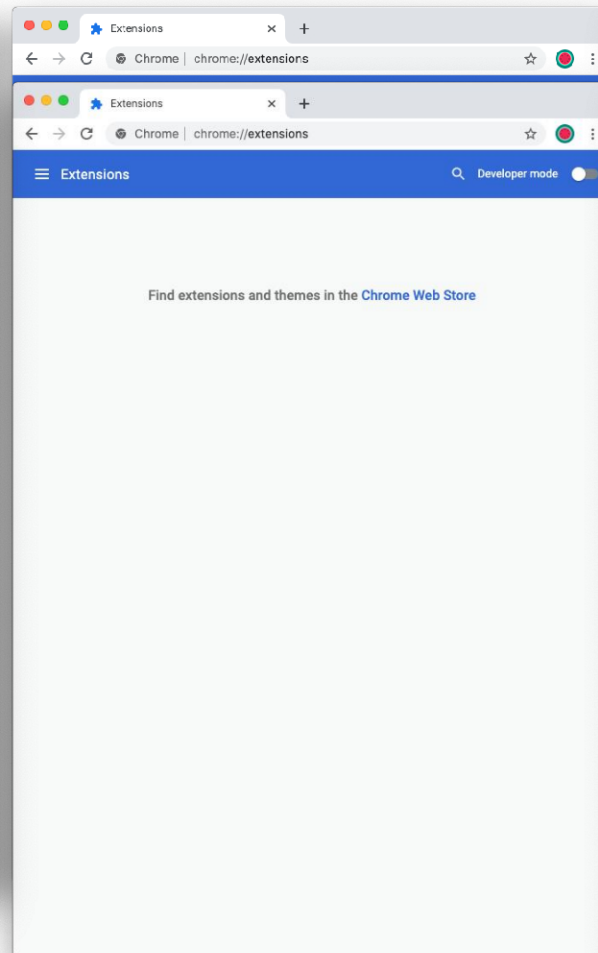
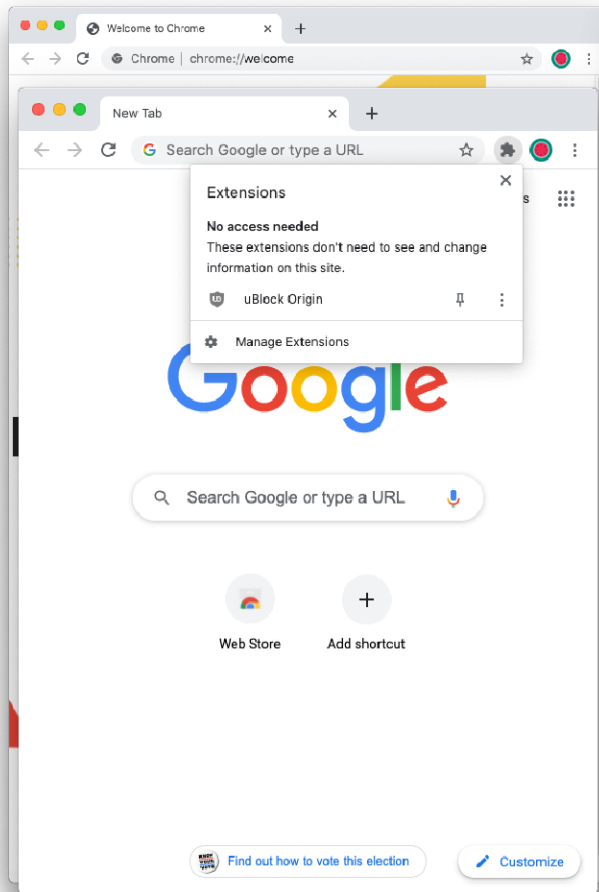
Buy now

Installed via User



- Social Engineering
- Freeware/Shareware
- Untrusted sources
- “Cracked” software
- “Bundled” software
 - Installs the software you want to install
 - Also install its friends

Bundled Malware



Malware Distribution



Malware is distributed via almost every imaginable technique and vector.

- Installed via Exploitation
- Installed via Third-Party
- Installed via User

Degrees of Malware



- Boundaries are vague and ill-defined
- Categorize for simplicity
- Many, many shades of grey and alternative ways to categorize
 - “Potentially Unwanted Apps”
 - “Potentially Harmful Apps”
 - ...

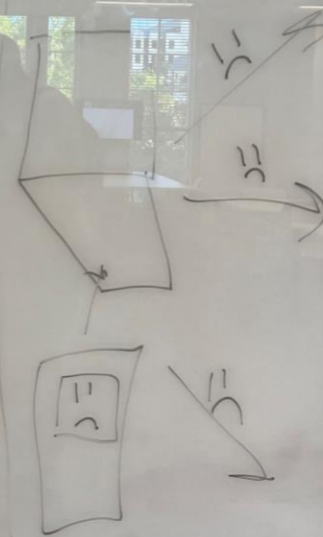
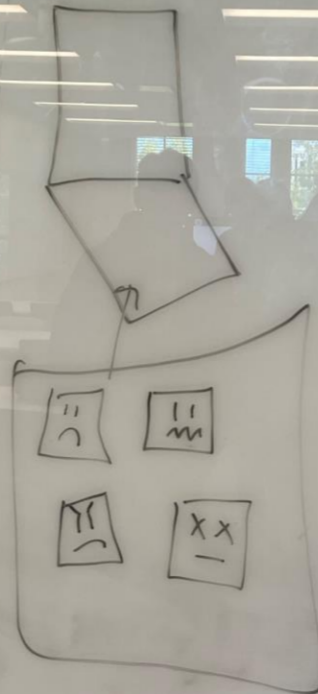




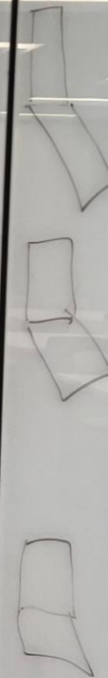
Trojan Horse



Virus / Worm



A gentle reminder: Please erase the whiteboard after your class.



Computer and Network Security

Lecture 13: Malware & Common Attacks

COMP-5370/6370
Fall 2024

