

Computer and Network Security

Lecture 13: Malware and Common Attacks pt2

COMP-5370/6370
Fall 2025





Malware Distribution



Malware is distributed via almost every imaginable technique and vector.

- Installed via Exploitation

Control Flow Hijacking

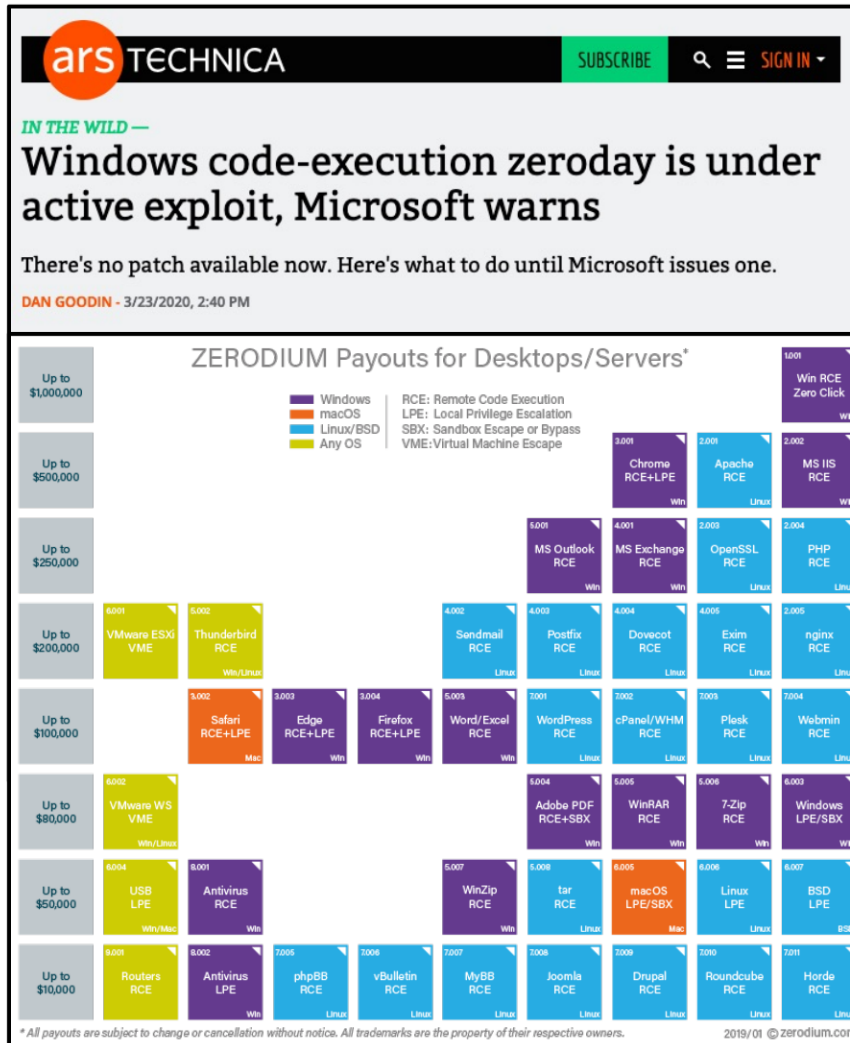


Control flow hijacking is when the attack gains the ability to maliciously influence the program's execution path.

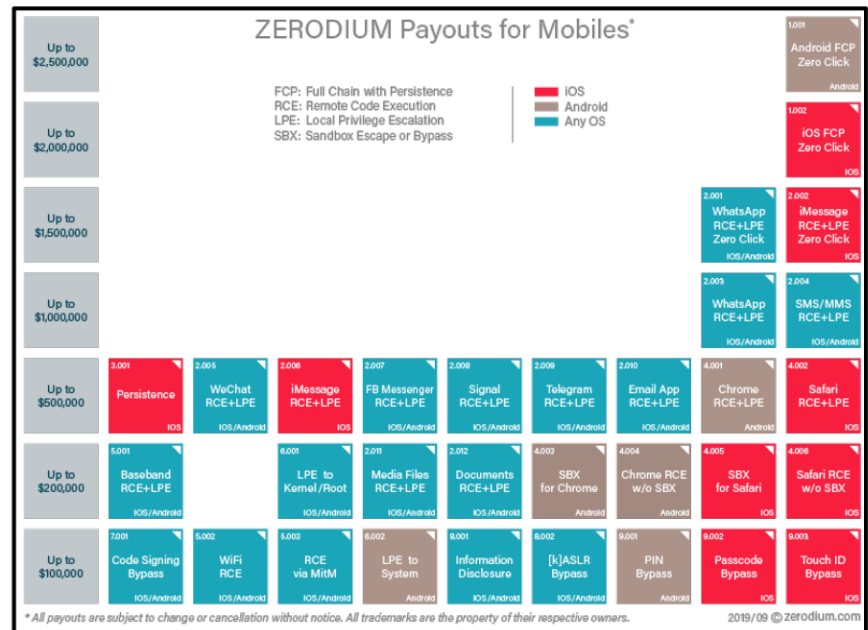
- End-goal of most binary exploitation attacks and technique

If you control EIP, you control the world.

Install via Exploitation

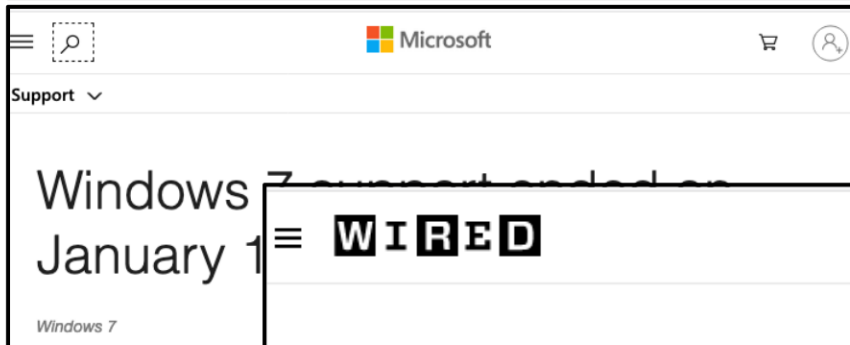


- 0-Day Vulnerability
 - Brand-new to vendor, defenders, and users
 - Find, exploit, & install



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

Install via Exploitation



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

Install via Exploitation



GitHub repository page for **danielmiessler / SecLists**. The repository has 1.7k watches, 27.4k stars, and 13.5k forks. The main branch is **Code**, with 13 issues, 16 pull requests, and 0 actions.

CYBERPUNK

Password Cracker THC Hydra

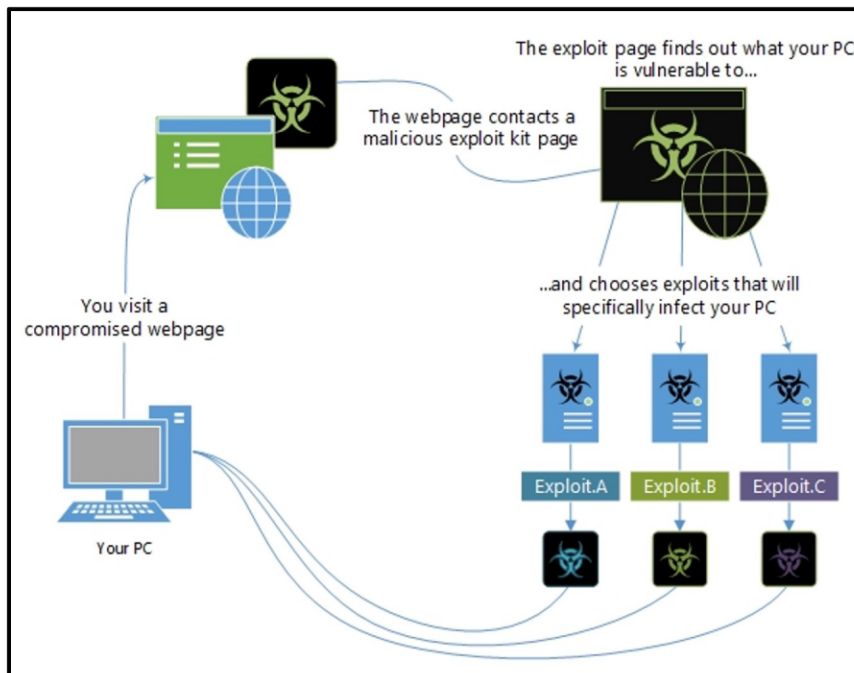
CyberPunk » Password Attacks



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



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

Installed via Third-Party



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



Installed via Third-Party



The image shows two overlapping screenshots. The top screenshot is a SourceForge blog post titled "Today We Offer DevShare (Beta), A Sustainable Way To Fund Open Source Software" by rgaloppini, dated July 1st, 2013. The post mentions that SourceForge is excited to launch DevShare, a new opt-in, revenue-sharing program aimed at giving developers a better and sustainable way. The bottom screenshot is a Google AdMob revenue calculator interface. It shows a form where the user's app location and content category are set as North America, Games, and Android. The Monthly Active Users are set at 50,000. The potential annual revenue is calculated as \$2,570. A "Get started" button is visible at the bottom.

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

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

A screenshot of a Wired article titled "A Mysterious Hacker Group Is On a Supply Chain Hijacking Spree" by Andy Greenberg, dated 05.03.2019. The article mentions that a group of likely Chinese hackers has poisoned software for at least six companies in the past three years.
A screenshot of an Ars Technica article titled "SourceForge grabs GIMP for Windows' account, wraps installer in bundle-pushing adware [Updated]". The article is categorized under "BIZ & IT".
A screenshot of a SourceForge blog post titled "GIMP-Win project wasn't hijacked, just abandoned" by the Community Team, dated May 27th, 2015. The post includes an update from June 22nd, 2015, stating that the two-day offers test was completed and further action on the mirroring program was taken on June 18th. A link to the update is provided: <http://sourceforge.net/blog/project-mirroring-policies-will-be-revisited-with-our-community-panel-existing-mirrors-removed/>.

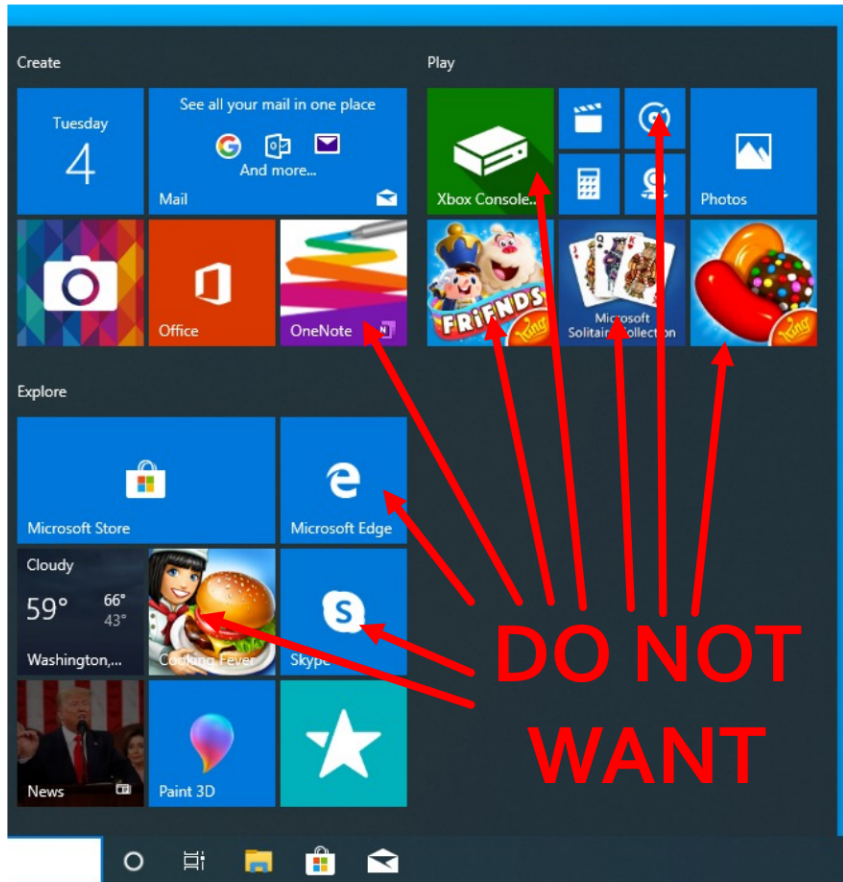
- Added to benign SW by developer
- Added by attacker via supply-chain access
 - Unknown to developer
 - External dependencies
 - Distribution mechanism

Installed via Third-Party



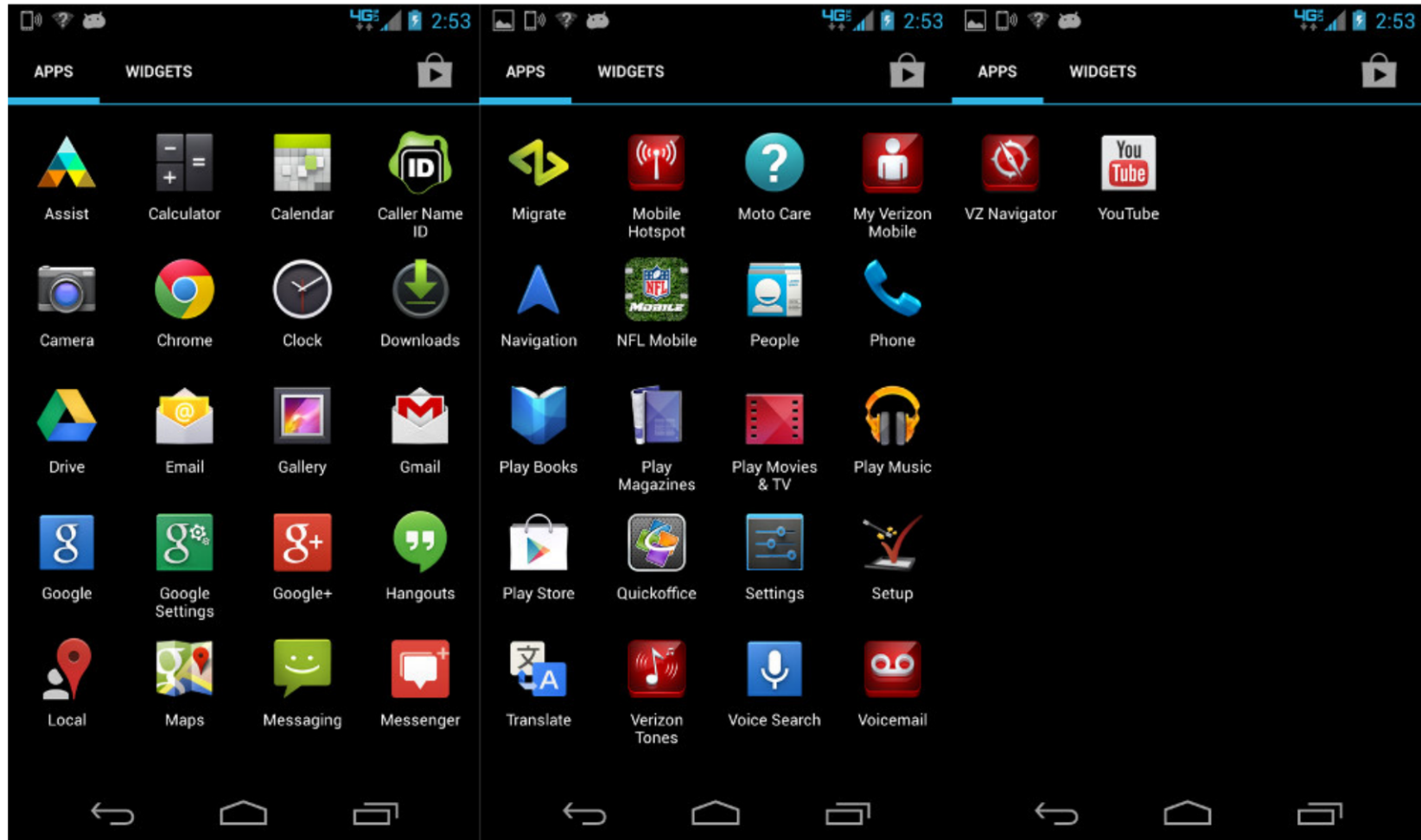
- Added to benign SW by developer
- Added by attacker via supply-chain access
- “Owner” adds for compliance/policy
 - Bossware, mobile device management (MDM)

Installed via Third-Party

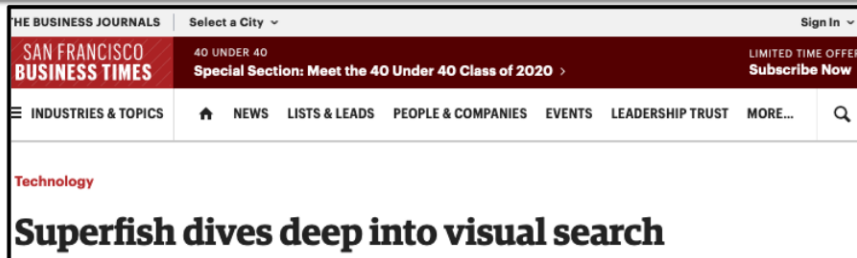


- Added to benign SW by developer
- Added by attacker via supply-chain access
- “Owner” adds for compliance/policy
- Preinstalled
 - May not be obvious
 - May be force-installed

Pre-Installed Malware



The Story of Superfish



- 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**

The Story of Superfish



The Hacker News

Home

Newsletter

Webinars

Lenovo Caught Using Rootkit to Secretly Install Unremovable Software

Aug 13, 2015 Swati Khandelwal

Lenovo Caught Red-Handed Again



Using Rootkit to Secretly Install Unremovable Software

Two years ago Chinese firm [Lenovo](#) got banned from supplying equipment for networks of the intelligence and defence services various countries due to hacking and

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

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

THE BUSINESS JOURNALS Select a City ▾

SAN FRANCISCO BUSINESS TIMES 40 UNDER 40 Special Section: Meet the

INDUSTRIES & TOPICS NEWS LISTS & LEAD

Technology

Superfish dives deep

WIRED

If you buy something using link

Technology

Lenovo faces huge

ars TECHNICA

BIZ & IT —

Lenovo PCs ship with malware that breaks Windows [Updated]

ars TECHNICA

BIZ & IT —

How to remove Superfish from your PC What Lenovo

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

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

installed
laptops
supported
with startup
M traffic
ion
t CA
VATE KEY
SINGLE

Malware Distribution



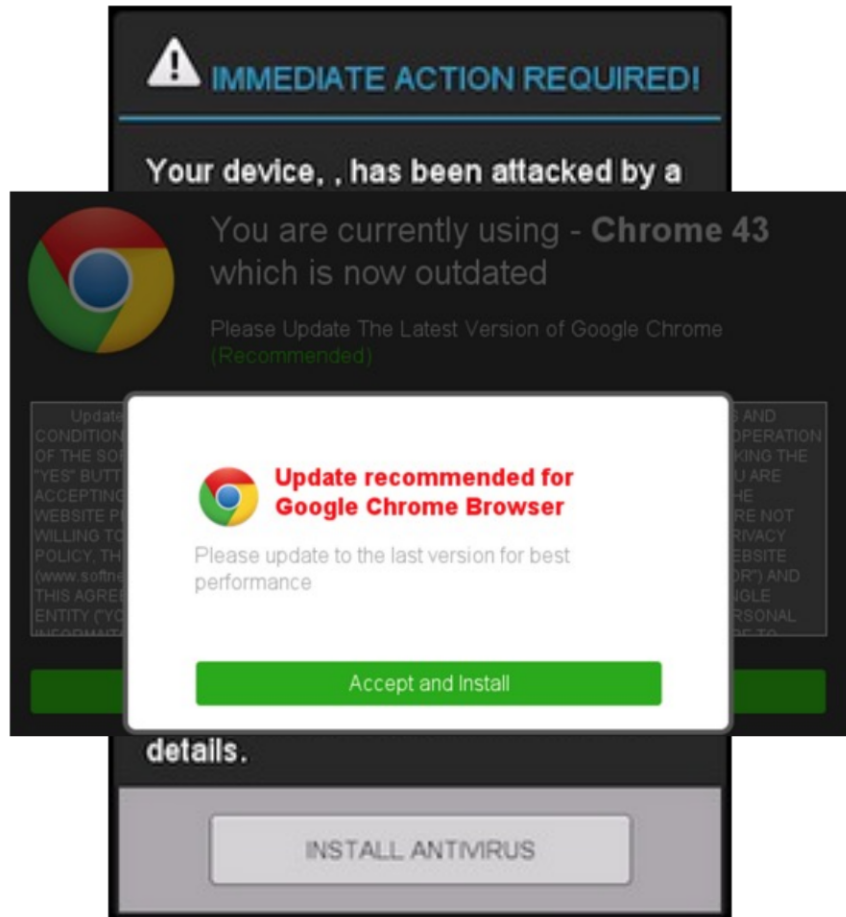
Malware is distributed via almost every imaginable technique and vector.

- 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

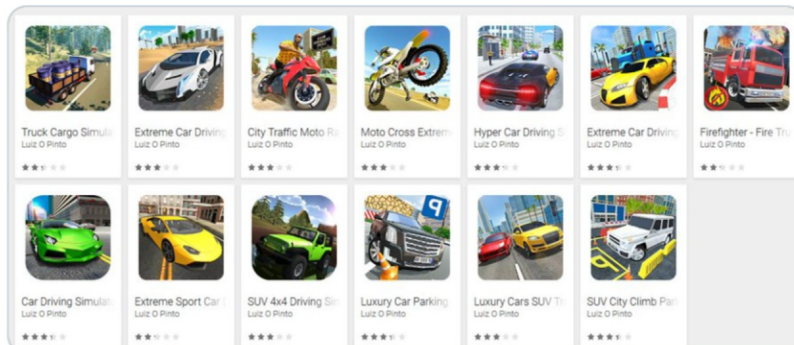


Lukas Stefanko
@LukasStefanko

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



- 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 a news article from The Guardian. The header includes the site's name and navigation links. The article title is "Fortnite players using Android phones at risk of malware infections". A yellow banner above the title states "This article is more than 2 years old".
A screenshot of a news article from WIRED. The header includes the site's name and navigation links. The article title is "Impostor Fortnite Android Apps Are Already Spreading Malware". The author is Brian Barrett, dated 08.16.2018.
A screenshot of a news article from Ars Technica. The header includes the site's name and navigation links. The article title is "Malicious warez hosted on Bitbucket get more than 500,000 downloads". A green banner above the title states "FREE AIN'T FREE". The article mentions an ongoing campaign installing credential stealers, RATs, ransomware, and cryptominers. The author is Dan Goodin, dated 2/5/2020.

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

Changes Coming to Android Side-Loading



Android Developers Blog

25 August 2025

A new layer of security for certified Android devices

Share

Posted by Suzanne Frey – VP, Product, Trust & Growth for Android



You shouldn't have to choose between open and secure. By engineering security into the core part of the OS, Android has proven that you can have both, and we continue taking new steps in that direction.

ars TECHNICA SIGN IN

PAPERS, PLEASE

Google will block sideloading of unverified Android apps starting next year

Google says it's no different than checking IDs at the airport.

RYAN WHITWAM – AUG 25, 2025 3:52 PM | 375



→ Credit: Ryan Whitwam

TEXT SETTINGS

Android's open nature set it apart from the iPhone as the era of touchscreen smartphones began nearly two decades ago. Little by little, Google has traded some of that openness for security, and its next security initiative could make the biggest concessions yet in the name of blocking bad apps. Google has announced plans to

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

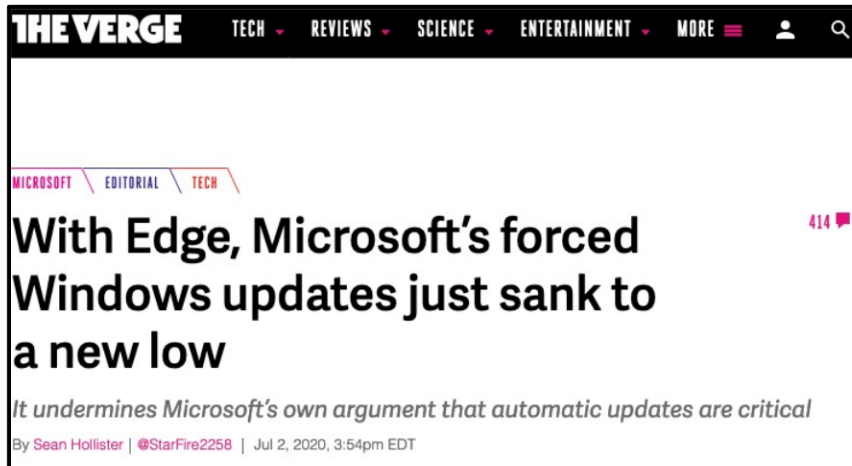
20 Software Cracks: A Great Way to Infect Your PC

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 free-version of paid software
 - Often actually are “key-hacked” version
 - WaReZ, Torrents, P2P

Installed via User



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

Malware Distribution



Malware is distributed via almost every imaginable technique and vector.

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



Computer and Network Security

Lecture 13: OS Security & Isolation

COMP-5370/6370
Fall 2025

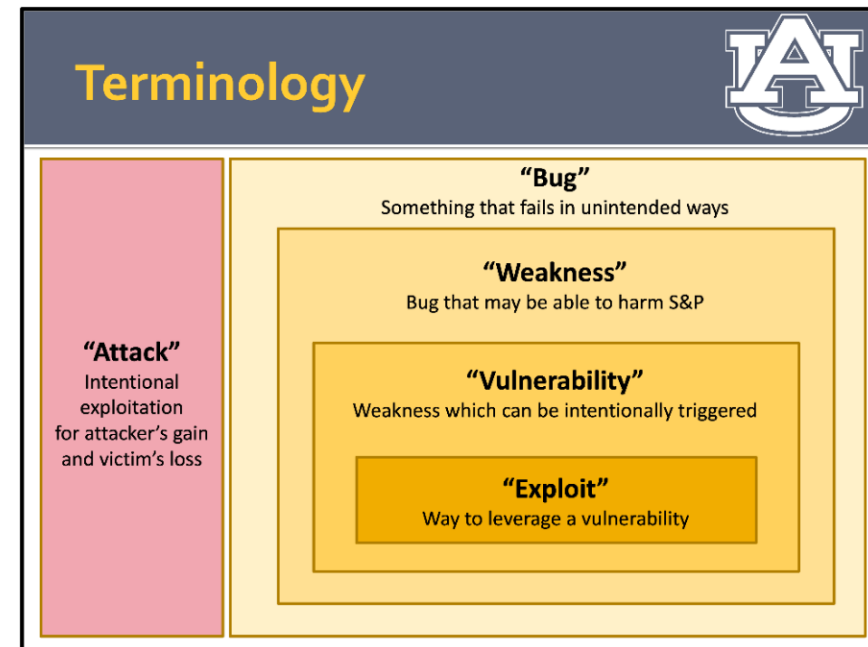




Software Facts of Life



- 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



Do you trust other people's code?



- Linux kernel: 27.8M lines of C
 - Pointer math, raw byte buffers, etc.
 - C99 compliant code lacks features like “smart pointers”, threads, implicit bounds-checking,...
 - Written, reviewed, and tested by those strange and mythical people known as “kernel devs”

Do you trust other people's code?



- Do you use an HP computer?
- Android OS or Google's Android Apps?
- Google services (GMail, Docs, Calendar, etc)?



Finster Professor



Shady Professor

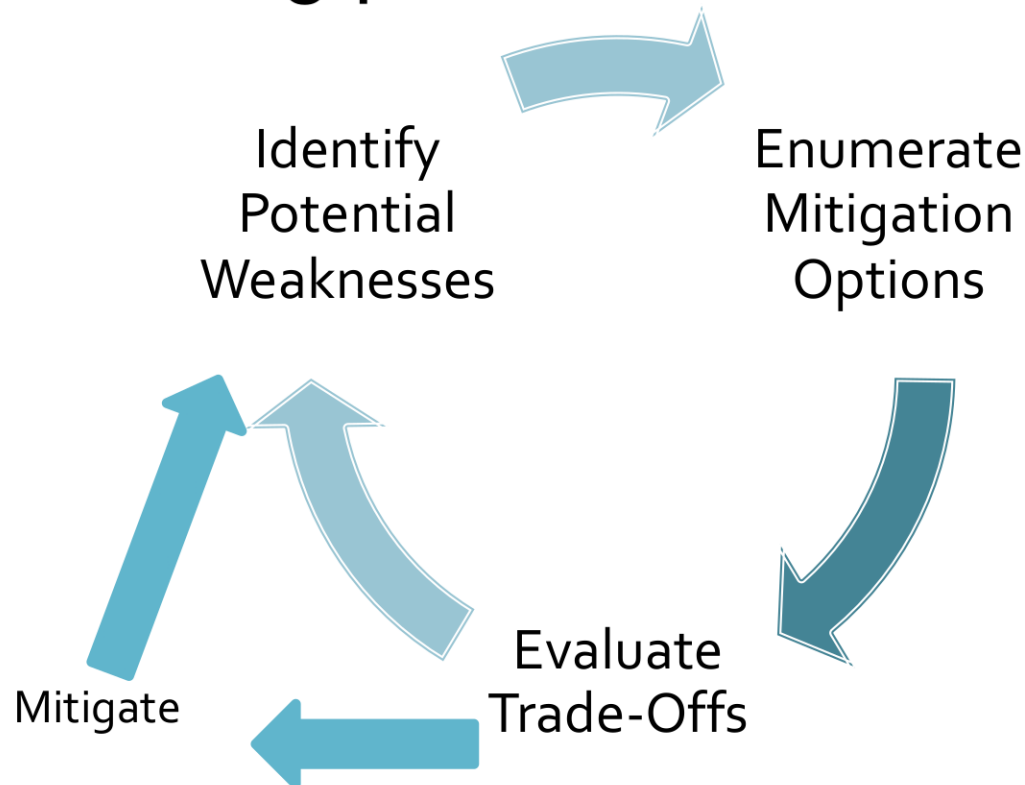


Profesor Turbio

Threat Modeling



A systematic approach to analyzing and understanding potential weaknesses.



Principle of Least Privilege



The **Principle of Least Privilege** is that access to data & resources is limited those who need for routine, authorized purposes.

- “Specific users can only run specific apps”
- “Normal users aren’t root-users”
- “routine” means **ROUTINE**
 - Having continuous ability to do something that is only needed every 3 years is ... less-than-ideal

Principle of Complete Mediation



The **Principle of Complete Mediation** is having a trusted entity validate any privilege use to ensure its validity.

- OS validates user X can run app Y
- OS validates that app Y is allowed to access resource Z

Applying Principles



- **Security Model** – An abstraction to *subjects*, *permissions*, and *objects* to allow reasoning about S&P properties.
- **Security Policy** – The mapping of *subjects*, *permissions*, and *objects* to implement the security model.
- **Security Mechanism** – The technical measure that enforces the security policy.

Access Control Model



Formal Models

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Role-based Access Control (RBAC)
- Bell-LaPadula
- <many, many more>

The real-world is a mixture of all.

Filesystem Example

Subjects

Users
Groups

Permissions

Read
Write
Execute

Objects

“Files”(data, binary, device)
Hierarchies (multiple files)

Access Control Policy



Create a logical representation of who has access to what file.

- Enumerate users
- Enumerate files
- Give specific users specific access to specific files
- Default: no-access

		Objects			
		File 1	File 2	File 3	File 4
Subjects	Alice	read	read/ write	no access	no access
	Bob	read	read/ write	no access	no access
	Carol	read	write	read/ write	read/ write
	Wendy	read/ write	read/ write	read	read

During Planning



- Create a system that is defensible



Subject Tracking Mechanism



Implement the policy in the real-world.

- Users assigned **user id**
- Users can **masquerade** as other users
- Users assigned to groups for simplicity (logic/mgmt)
- Groups are **meta-users** in some but not all aspects

```
user@desktop:~$ whoami; id -u
user
1000
```

```
user@desktop:~$ sudo whoami
[sudo] password for user:
root
```

```
user@desktop:~$ groups
user adm faculty
```

```
user@desktop:~$ $ sudo -u adm bash -c 'hi'
Sorry, user adm is not allowed to execute '/usr/bin/bash'
user@desktop:~$ $ sudo -u root bash -c 'hi'
hi
```

User Permission Tracking



- 3 permission bits per object (RWX)

<code>rwX</code>	<code>rwX</code>	<code>rwX</code>
Owner	Group	Others

```
user@desktop:~$ ls -l
d rwX rwX --- 1 user user      4096 Apr  2 15:56 go
- rw- rw- r-- 1 user user          0 Apr 11 04:15 test.py
d rwX rwX --- 1 user faculty 4096 Dec 28 21:09 courses
```

Permissions

Owner

Group

Object

- Each object has an “owner” and a group
- Only owner can change the permissions or group

```
user@desktop:~$ ls -l
- rw- r-- --- 1 user faculty 302 Apr 11 04:15 main.py
user@desktop:~$ chmod 751 main.py
user@desktop:~$ chgrp adm main.py
user@desktop:~$ ls -l
- rwX r-x r-x 1 user adm      302 Apr 11 04:15 main.py
```

OS Mediation of File Access



- Who is trying to act?

```
user@desktop:~$ whoami; id -u  
user  
1000
```

- What are they trying to act on?

```
user@desktop:~$ ls -l  
d rwx rwx --- 1 user user 4096 Apr 2 15:56 go  
- rw- rw- r-- 1 user user 0 Apr 11 04:15 test.py  
d rwx rwx --- 1 user faculty 4096 Dec 28 21:09 courses
```

- What are they trying to do?

- Allow action or not?

rwx	rwx	rwx
Owner	Group	Others

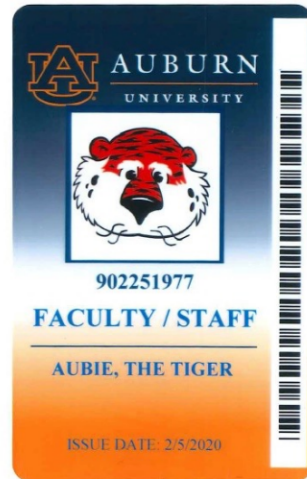
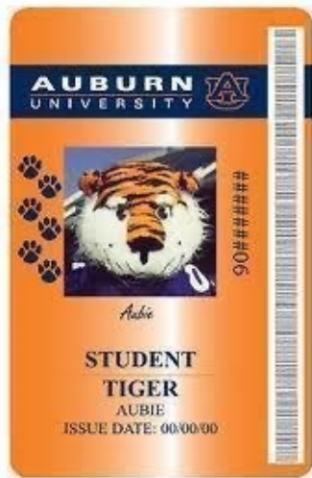


Processes as Subjects

Processes permissions are **logically identical** but slightly different in details.

- Process inherits user permissions (default)
 - Effective User ID (EUID)
 - Effective Group ID (GUID)
- EUID/GUID can be set manually:
 - `sudo, setuid, sg, ...`
 - Requires root user

During Operation



- Create a system that is defensible
- Maintain the mechanisms for defending it

Do you trust other people's code?



- Do you use an HP computer?
 - Android OS or Google's Android Apps?
 - Google services (GMail, Docs, Calendar, etc)?



Finster Professor



Shady Professor



Profesor Turbio

Computer and Network Security

Lecture 13: OS Security & Isolation

COMP-5370/6370
Fall 2025



Course Notes



- Project 1A
 - Grades posted tonight
 - Remember that 1A is **HALF** of Project 1
- Project 1B
 - Finishing-up this week, expect Friday
- Exam 1
 - Grades & Scans posted tonight
- Midterm
 - On Tuesday, 07Oct2025 (1 week from today)