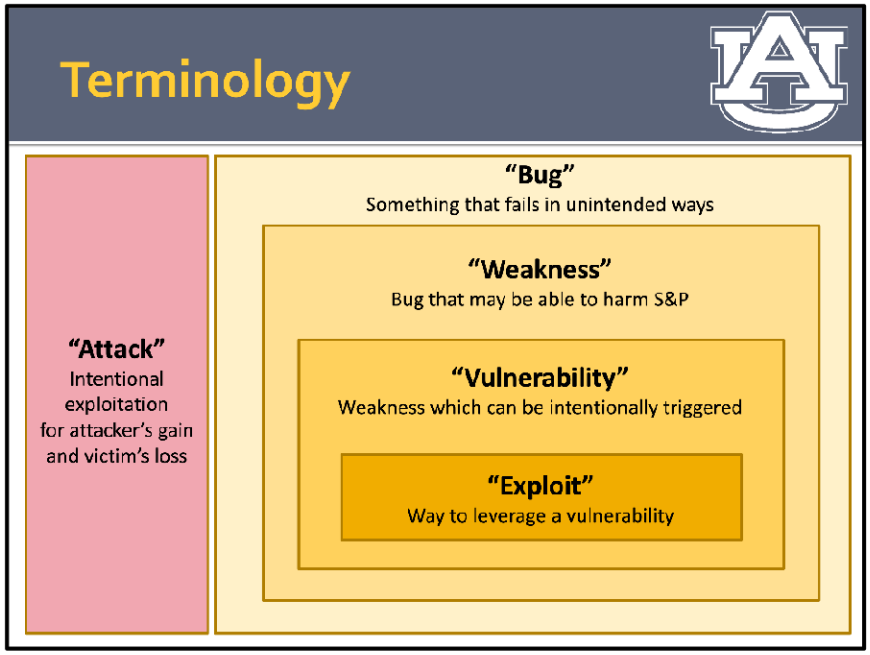
Computer and Network Security

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

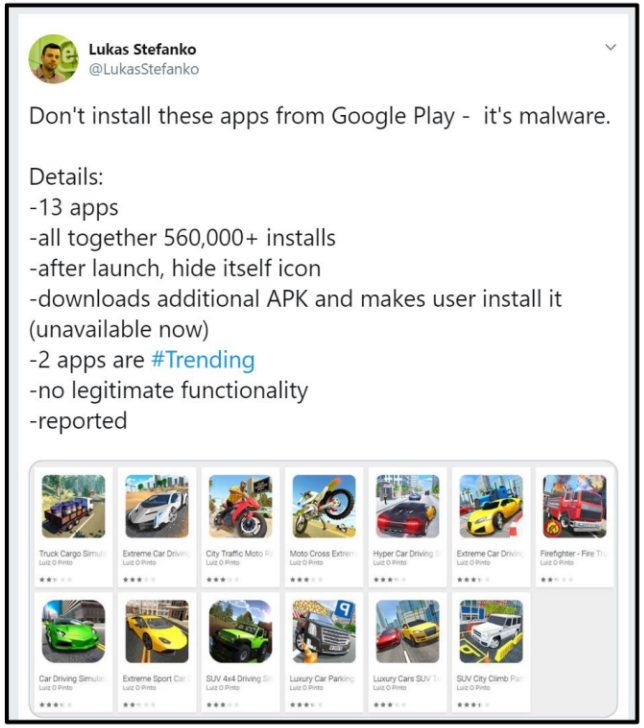
Classification of Malware

- 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



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(key`$_1$`, …)`
- Instance 2
  - `Encrypt(key`$_2$`, …)`

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

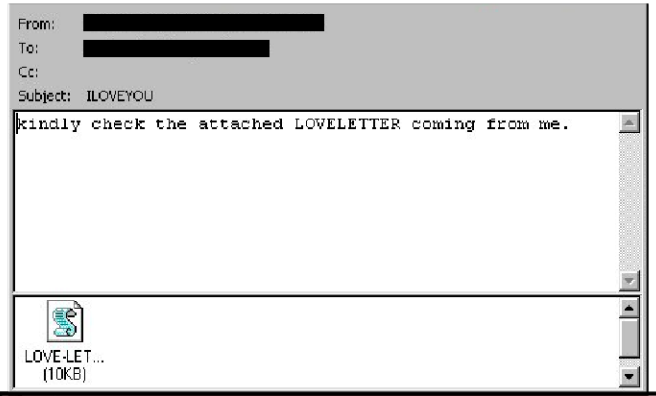
Infection Type: Worm

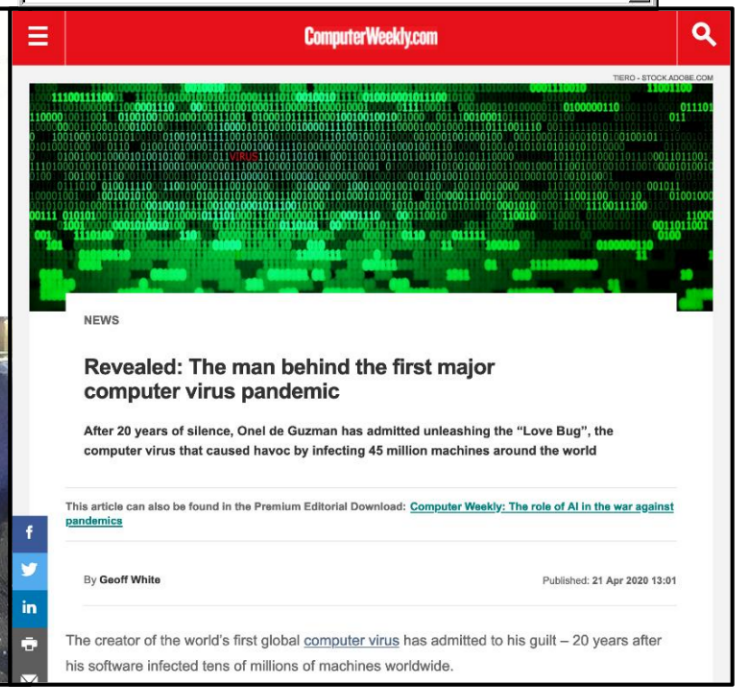
A **worm** is a virus that has the ability to spread itself to other devices automatically.

- 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

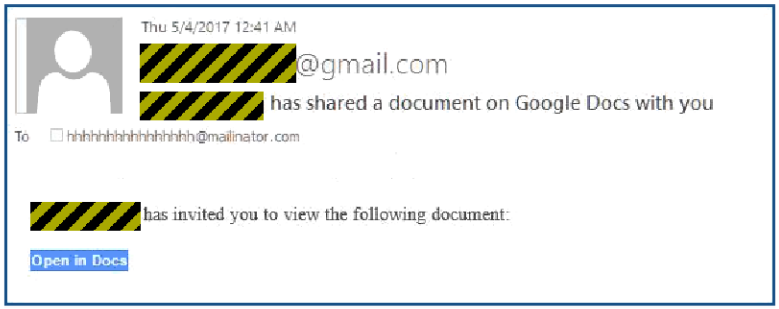
- 2000: Onel de Guzman
- Was geo-restricted… at first
- Infected 10% of Internet
- Was never prosecuted

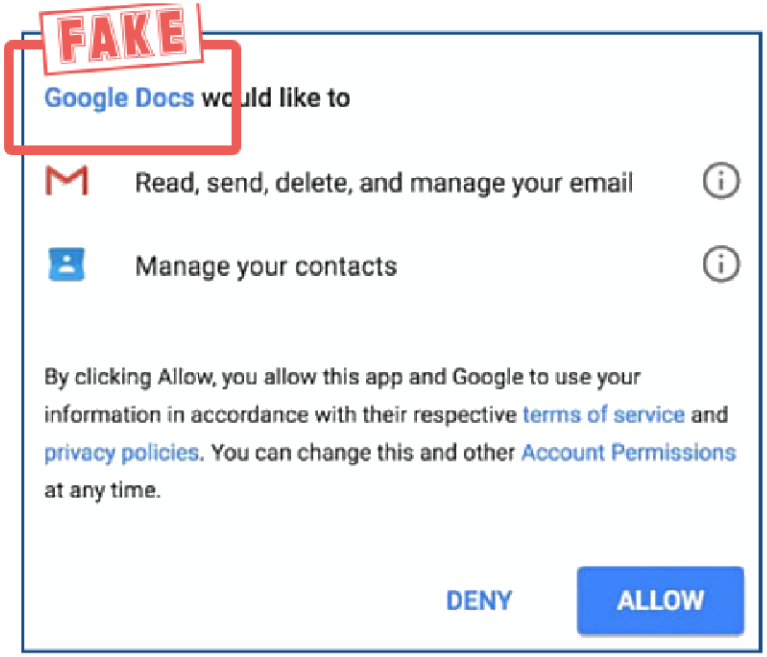




2017 Google Phishing Worm

- 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:

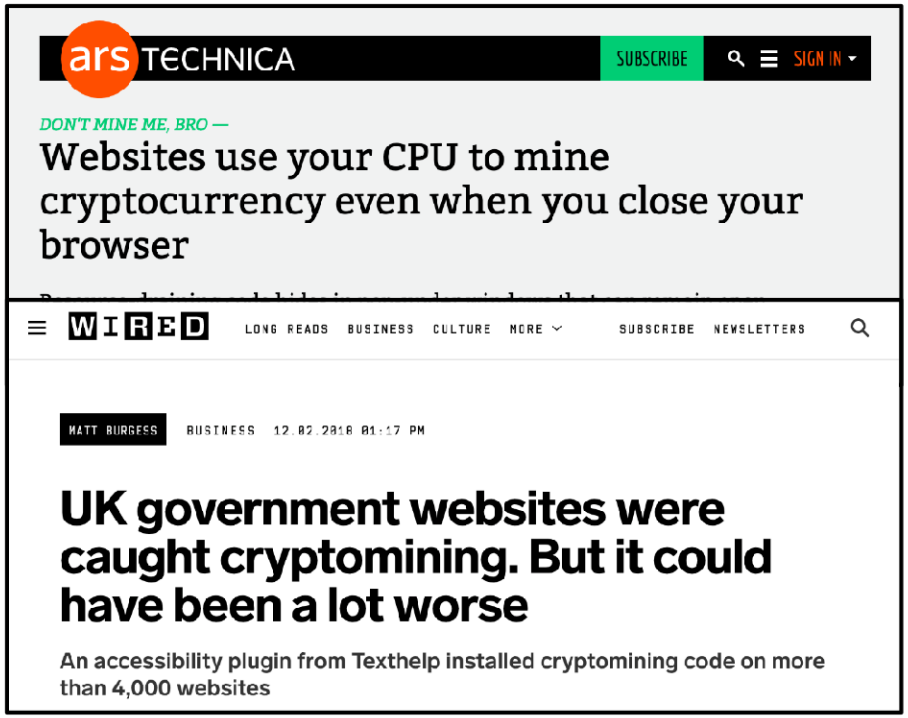
- Operate for others' advantage
- Negatively affect the victim

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.

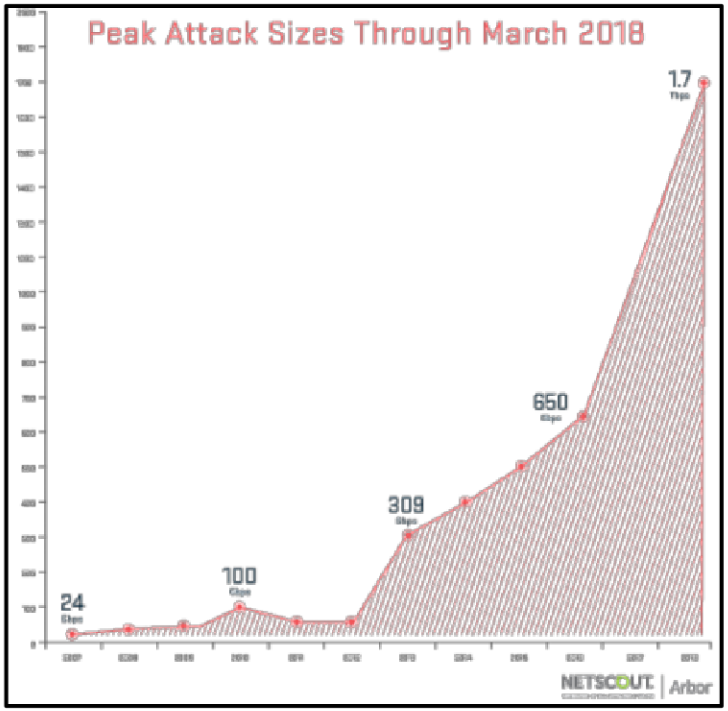
- Often injected via JS and run in browser
- Miner "pools" make it profitable even with limited computation



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

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

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
aimed at giving developers a better way to monetize their projects in a transparent,
and sustainable way.

kaspersky daily

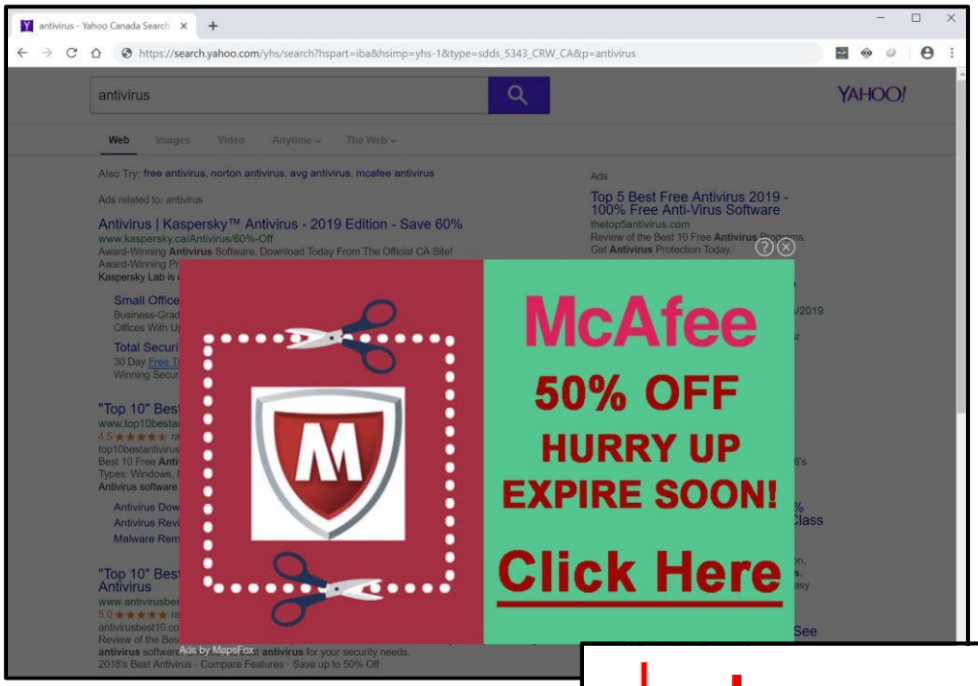
extensions

Chrome extensions abuse millions with adware

Too many ads on your computer lately? Malicious Chrome extensions might be to blame.

Marina Mash February 18, 2019

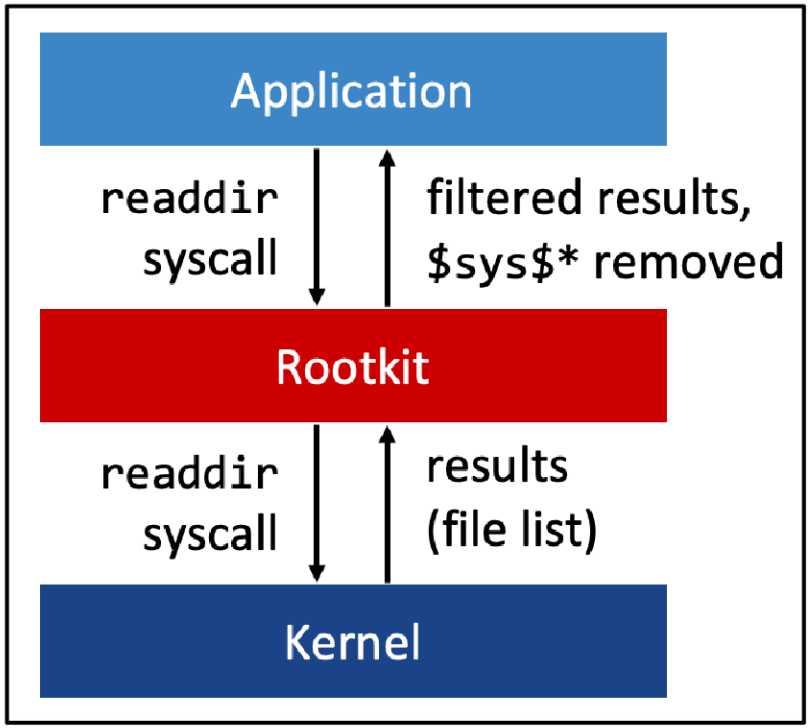
Adware – Less-Obvious



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

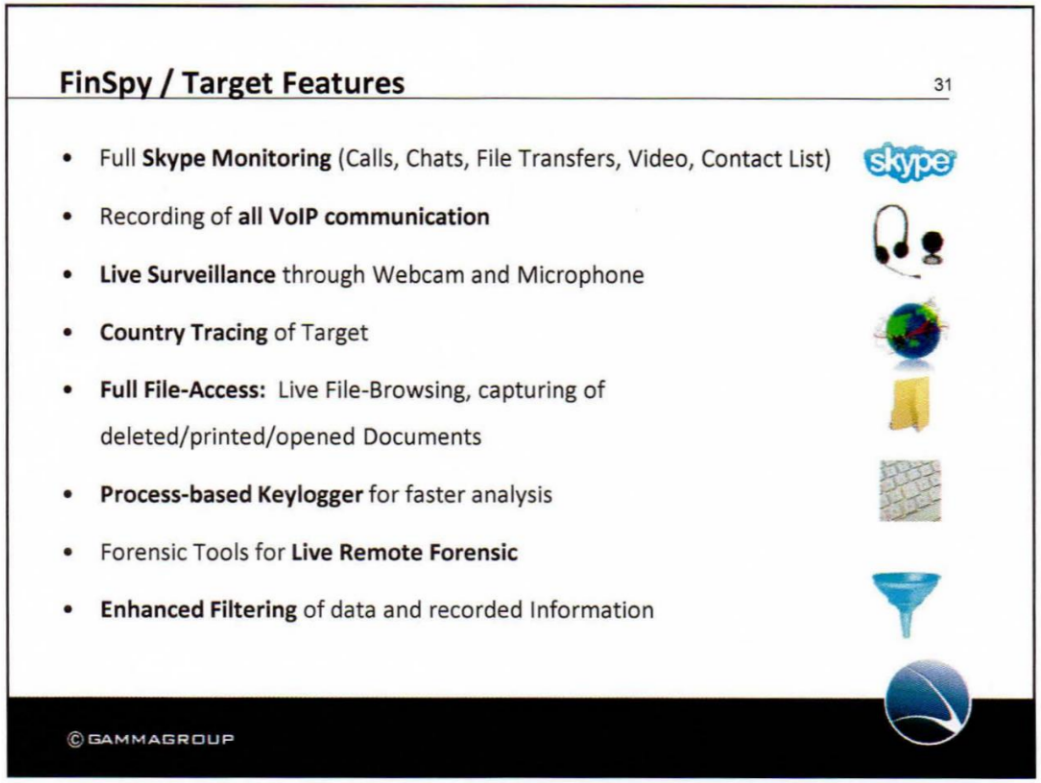
Spyware is a type of malware that provides remote access to local data such as activity, sensors, and other information.

- 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



Government Spyware

The Great iPwn

Journalists Hacked with Suspect iMessage 'Zero-Click' Exploit

By Bill Marczak, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, a

December 20, 2020 Arabic translation

Download this report

Summary & Key Findings

- In July and August 2020, government operatives use hack 36 personal phones belonging to journalists, pr at *Al Jazeera*. The personal phone of a journalist at L hacked.
- The phones were compromised using an exploit cha appears to involve an invisible zero-click exploit in iM a zero-day against at least iOS 13.5.1 and could hack
- Based on logs from compromised phones, we believ successfully deployed KISMET or a related zero-click and December 2019.

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."

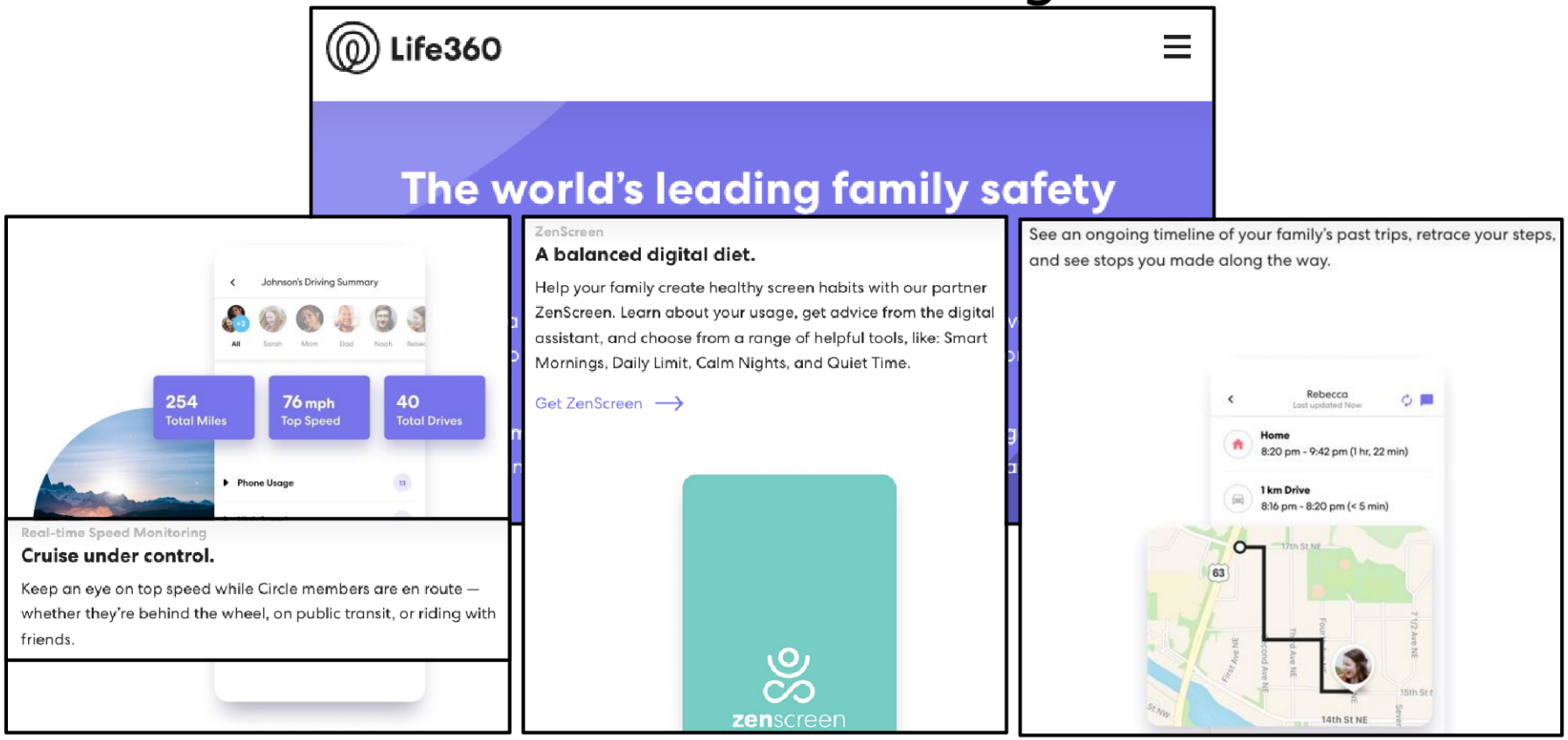
Intent: Spyware

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

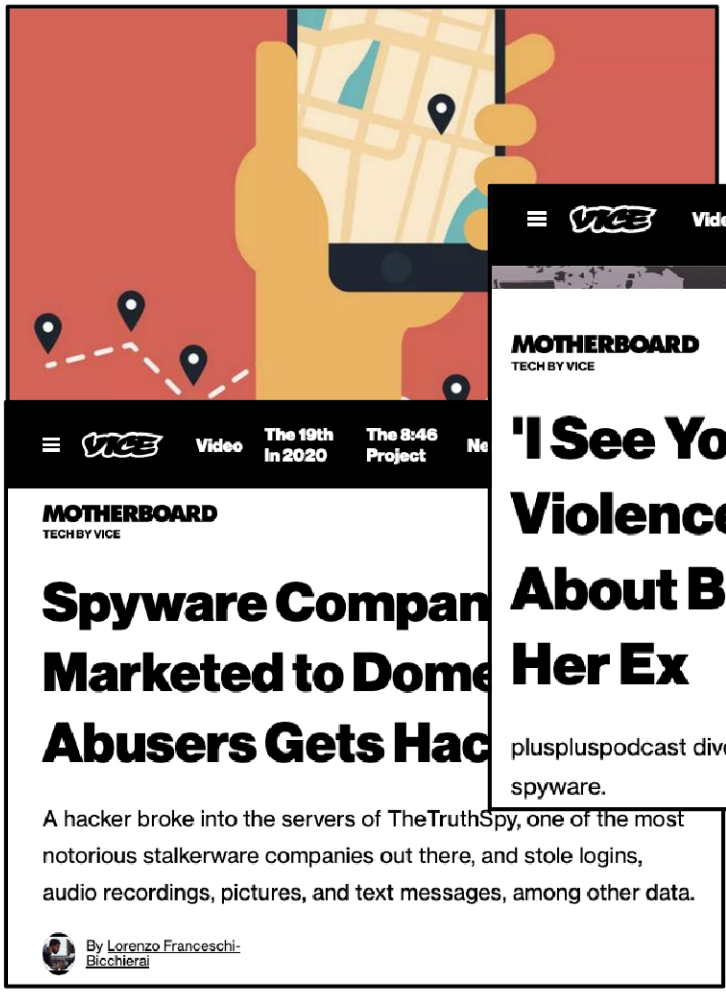
- Key loggers, screen captures, data exfiltration, GPS/microphone/camera data
- **Does not have to be entirely hidden**

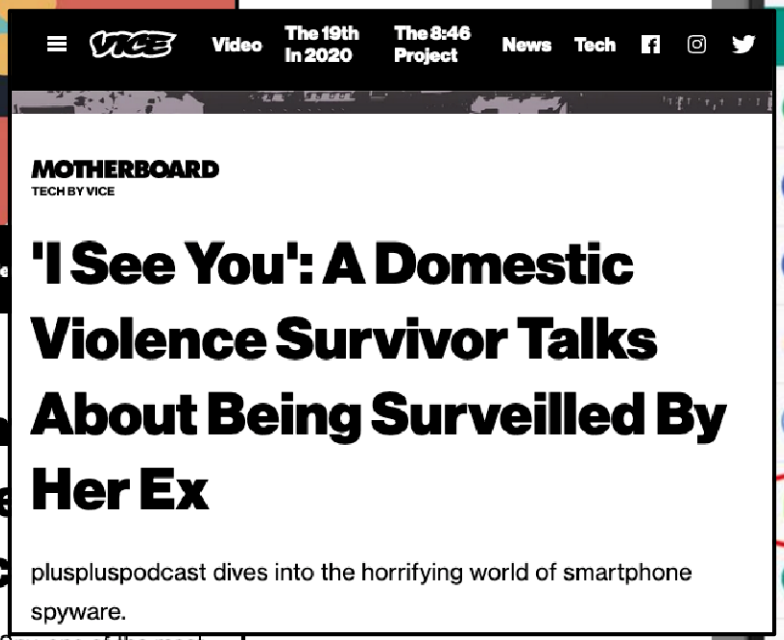
Less Obvious Spyware

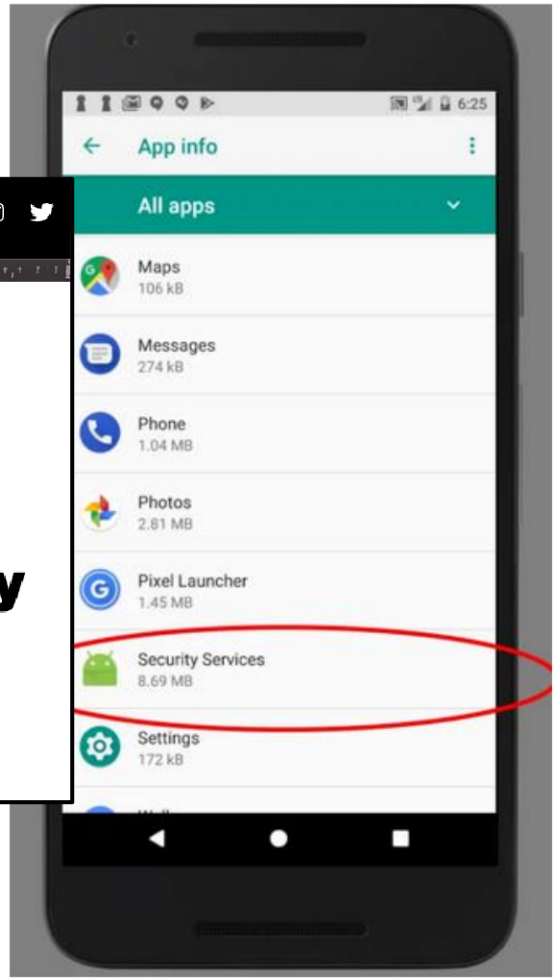
- Some instances are significantly less obvious due to their branding



Really Sketchy Spyware







Is it Spyware?

Honorlock®

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

MEASURE LEARNING proctorU

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

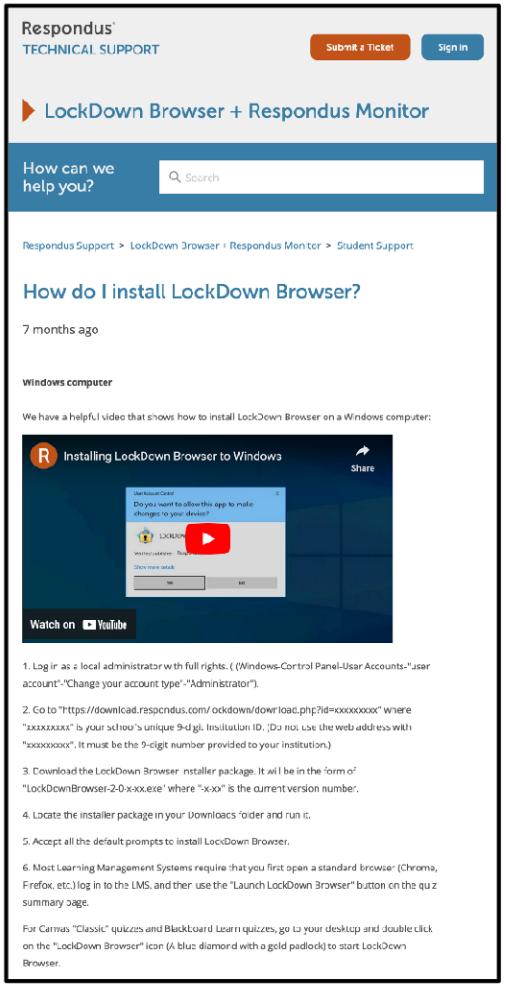
User activity

For example: network monitoring, clicks, mouse position, scroll, or keystroke logging

Is it Spyware?

Respondus®

Assessment Tools for Learning Systems



Respondus
TECHNICAL SUPPORT

Submit a Ticket | Sign in

LockDown Browser + Respondus Monitor

How can we help you?

Search

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/lockdown/download.php?id=xxxxxxxx" where "xxxxxxxx" is your school's unique 9-digit 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-x-xx.exe" where "-x-xx" 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

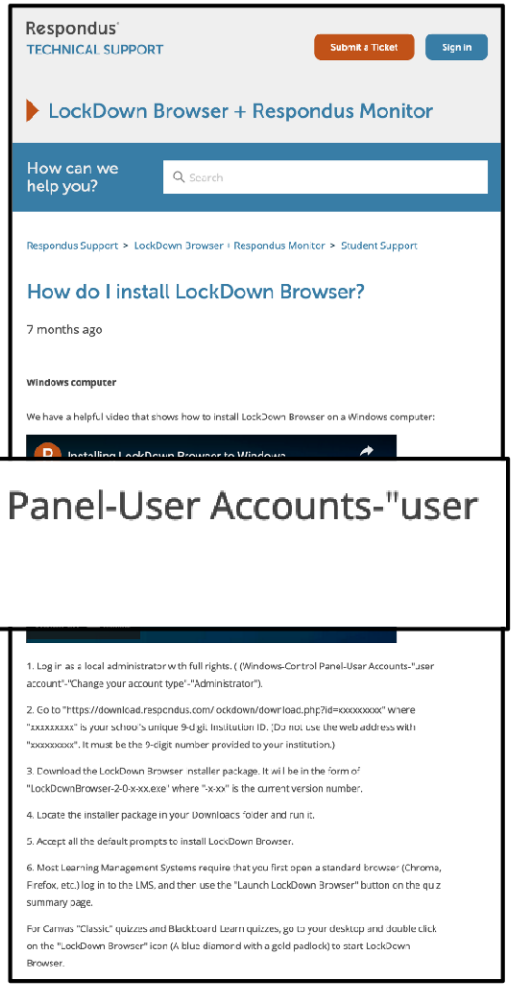
When you click on the "Launch LockDown Browser" button, whatever browser you are using will initially ask you permission to open the LockDown Browser application installed on your computer. The dialog will be slightly different, depending on the

in each case you must grant permission.

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

EFF
@EFF

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

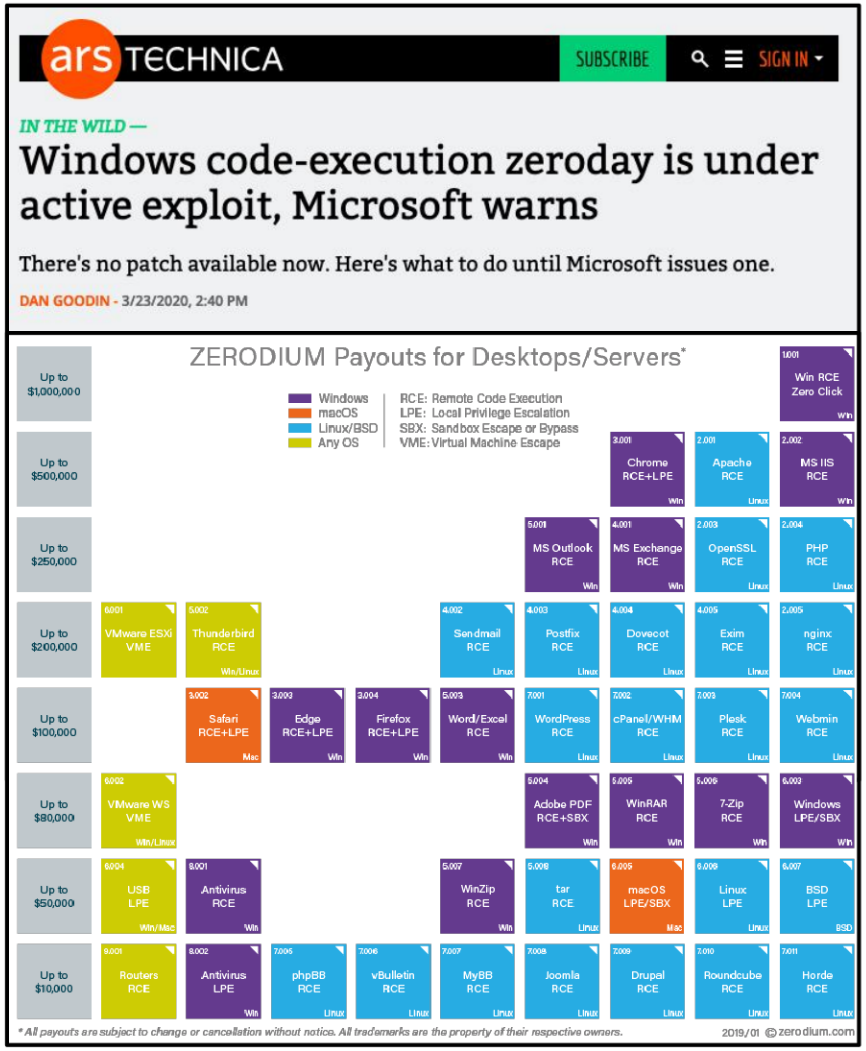

IF YOU DON'T WANT MALWARE
DON'T INSTALL MALWARE
imgflip.com

Malware Distribution

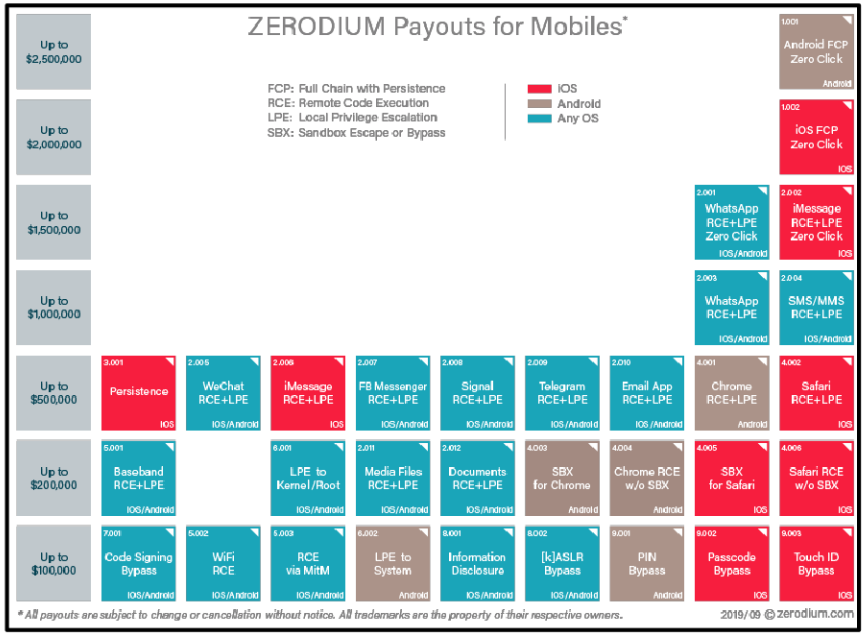
Malware is distributed via almost every imaginable technique and vector.

- Installed via Exploitation

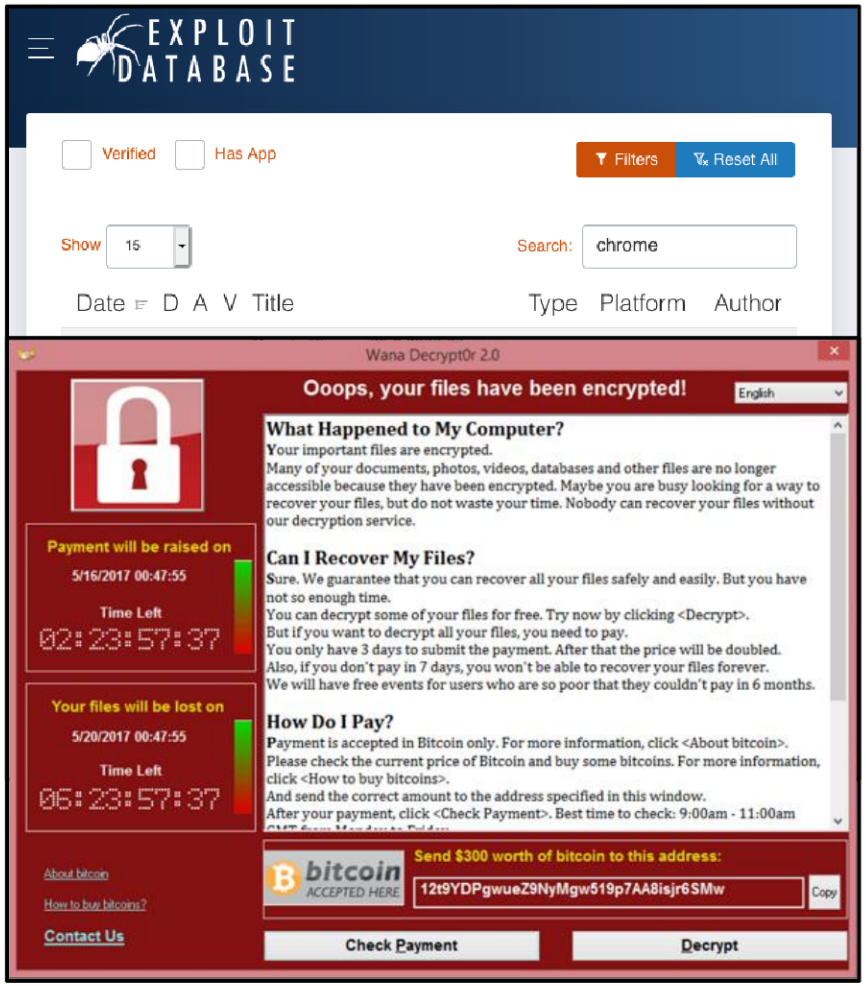
Install via Exploitation



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

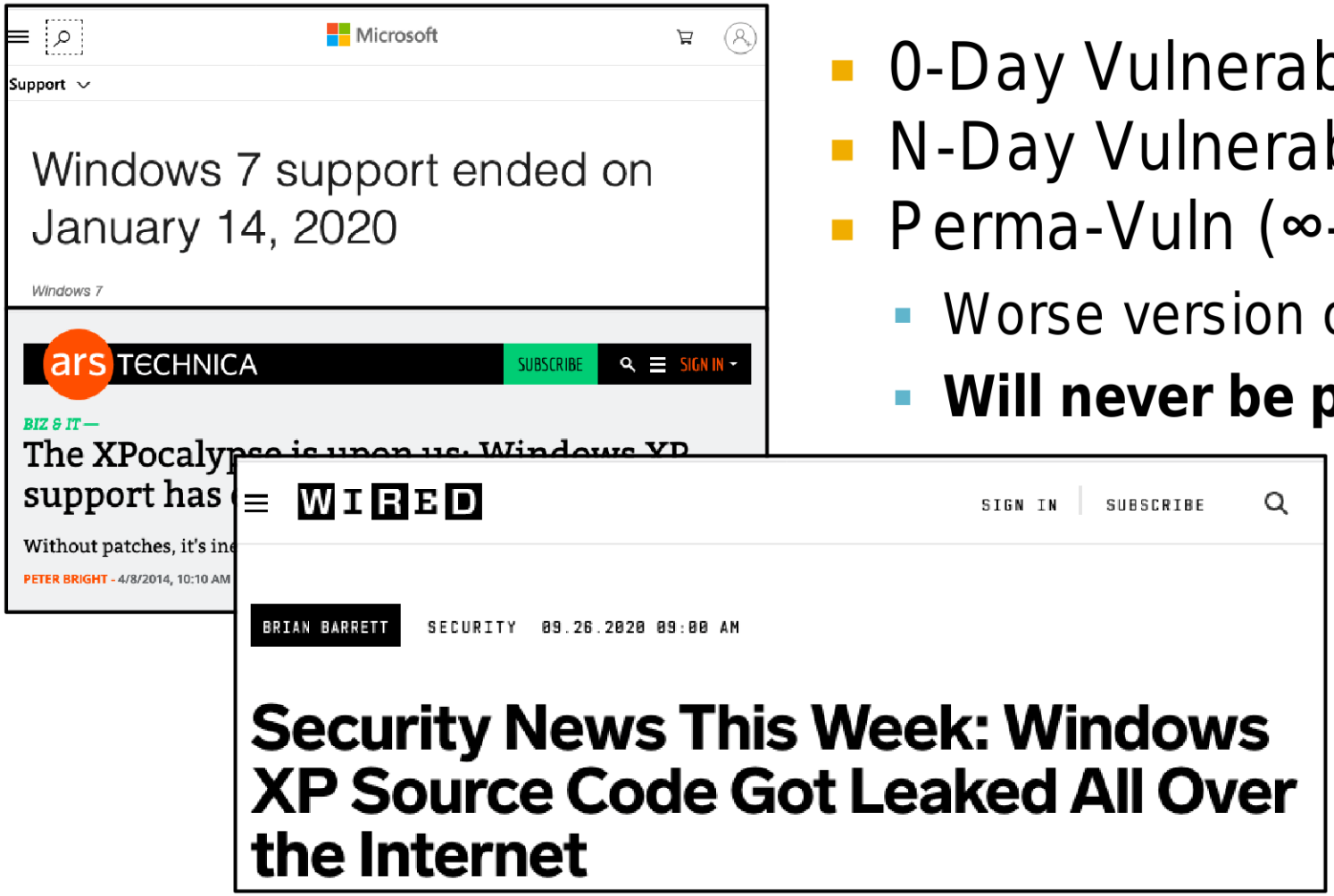


Install via Exploitation



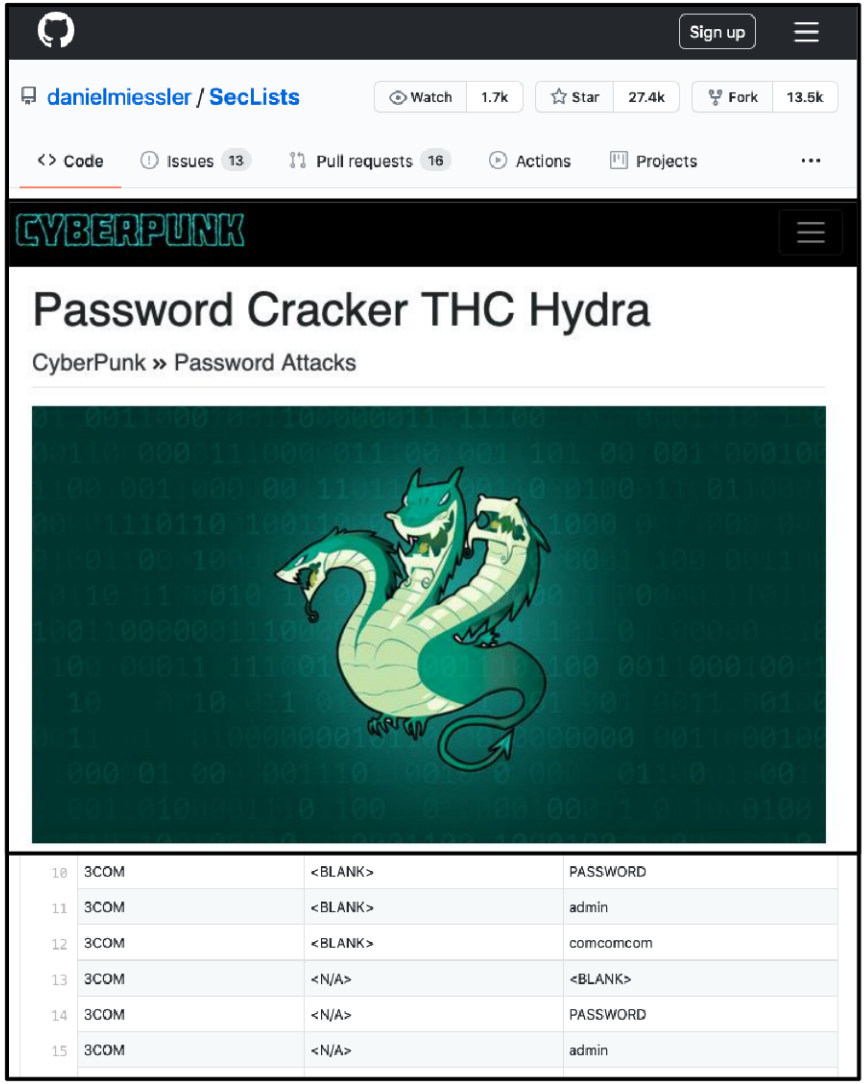
- 0-Day Vulnerability
- N-Day Vulnerability
  - Patch exists but is not applied to host
  - Old =!= Ineffective
  - Google, exploit, & install

Install via Exploitation



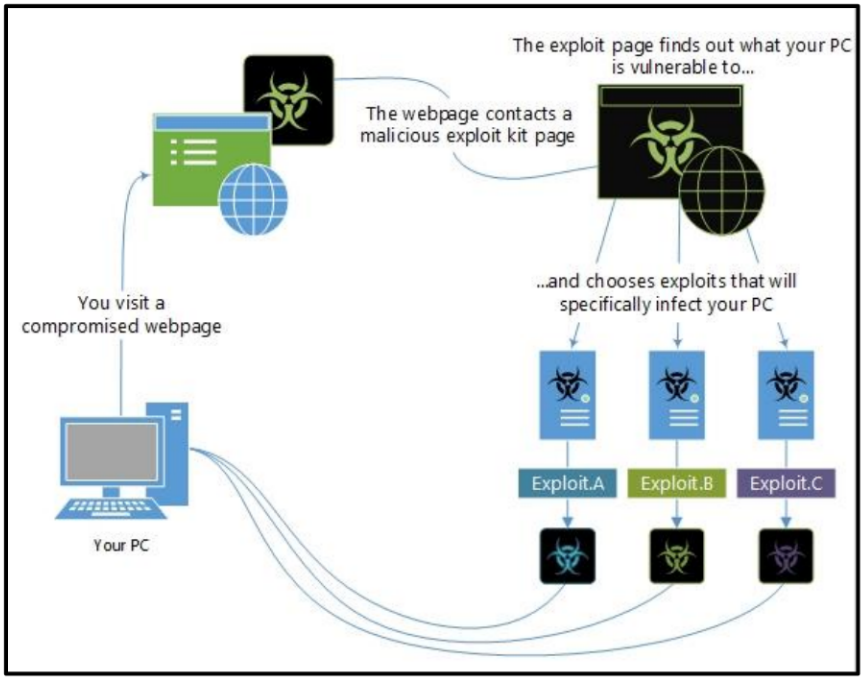
- 0-Day Vulnerability
- N-Day Vulnerability
- Perma-Vuln (∞-day)
  - Worse version of n-day
  - **Will never be patched**

Install via Exploitation



- 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

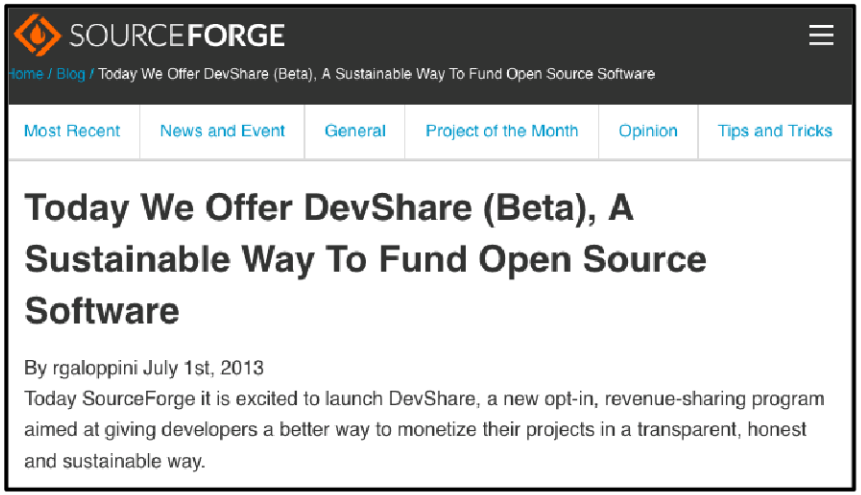
Malware is distributed via almost every imaginable technique and vector.

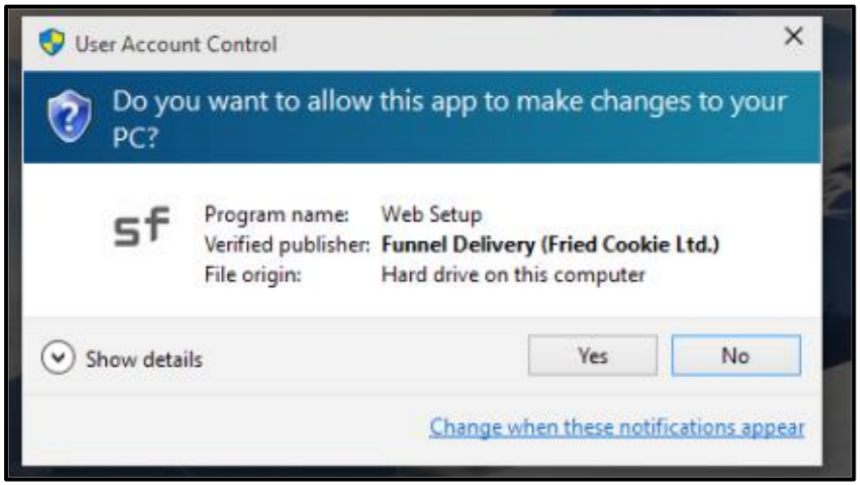
- Installed via Exploitation
- Installed via Third-Party

Installed via Third-Party

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

Installed via Third-Party





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

Installed via Third-Party


WIRED SIGN IN | SUBSCRIBE

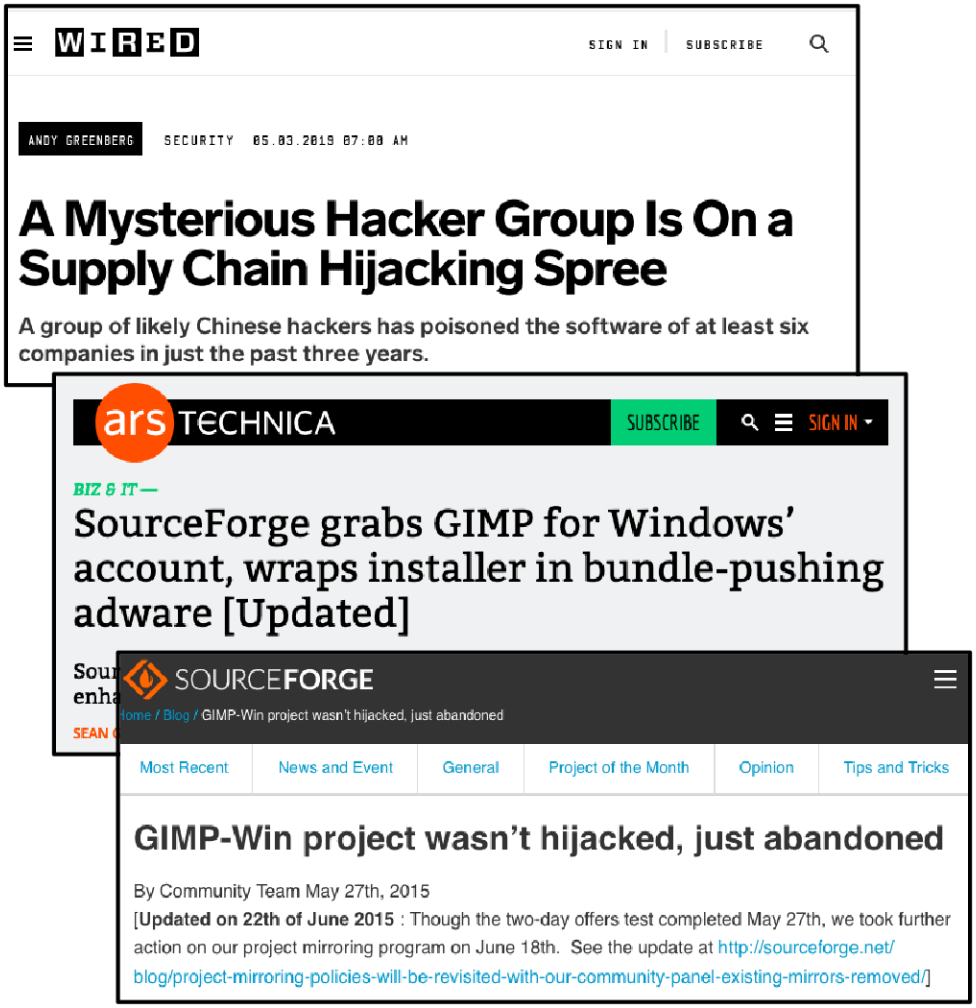
ANDY GREENBERG SECURITY 05.03.2019 07:00 AM

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.

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

Installed via Third-Party

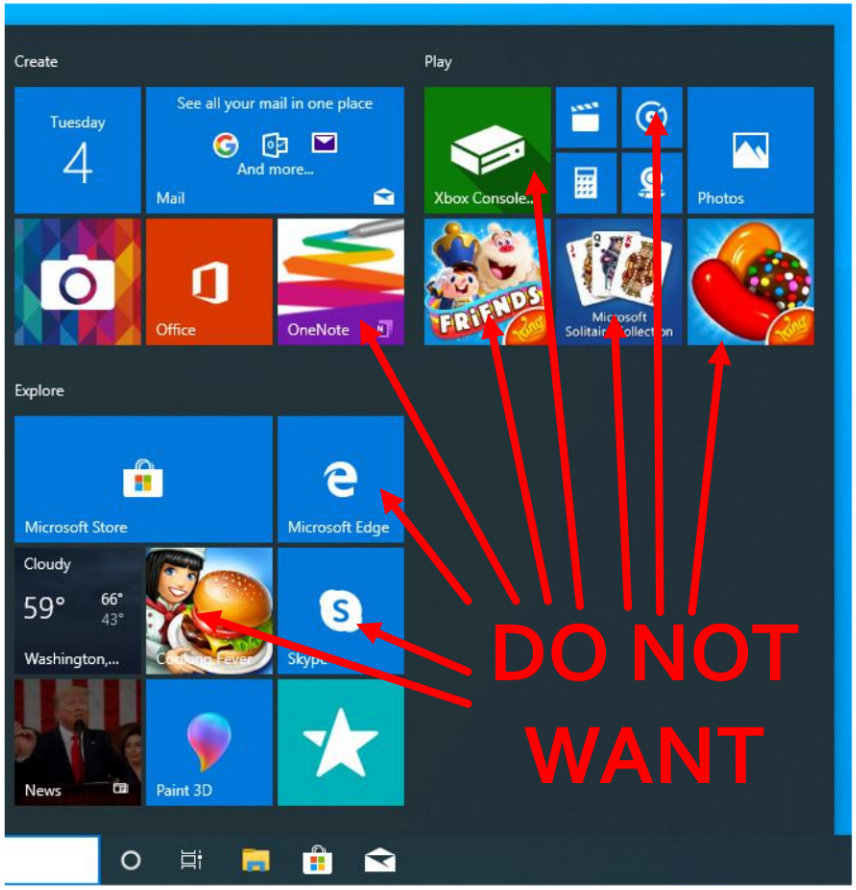


- Added to benign SW by developer
- Added by attacker via supply-chain access
  - Unknown to developer
  - External dependencies
  - Distribution mechanism

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)

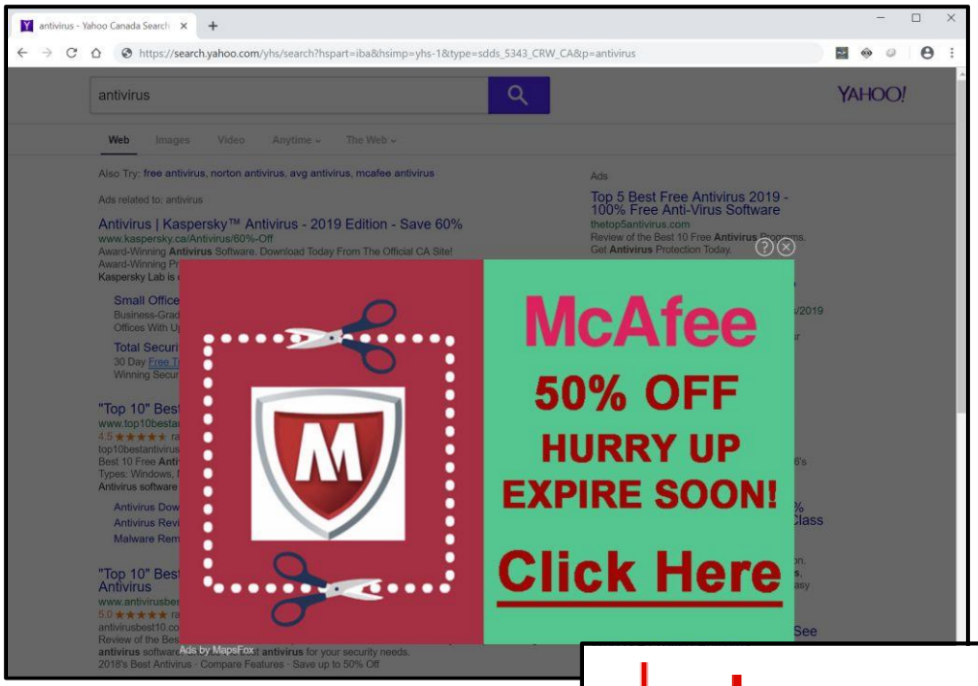
Installed via Third-Party



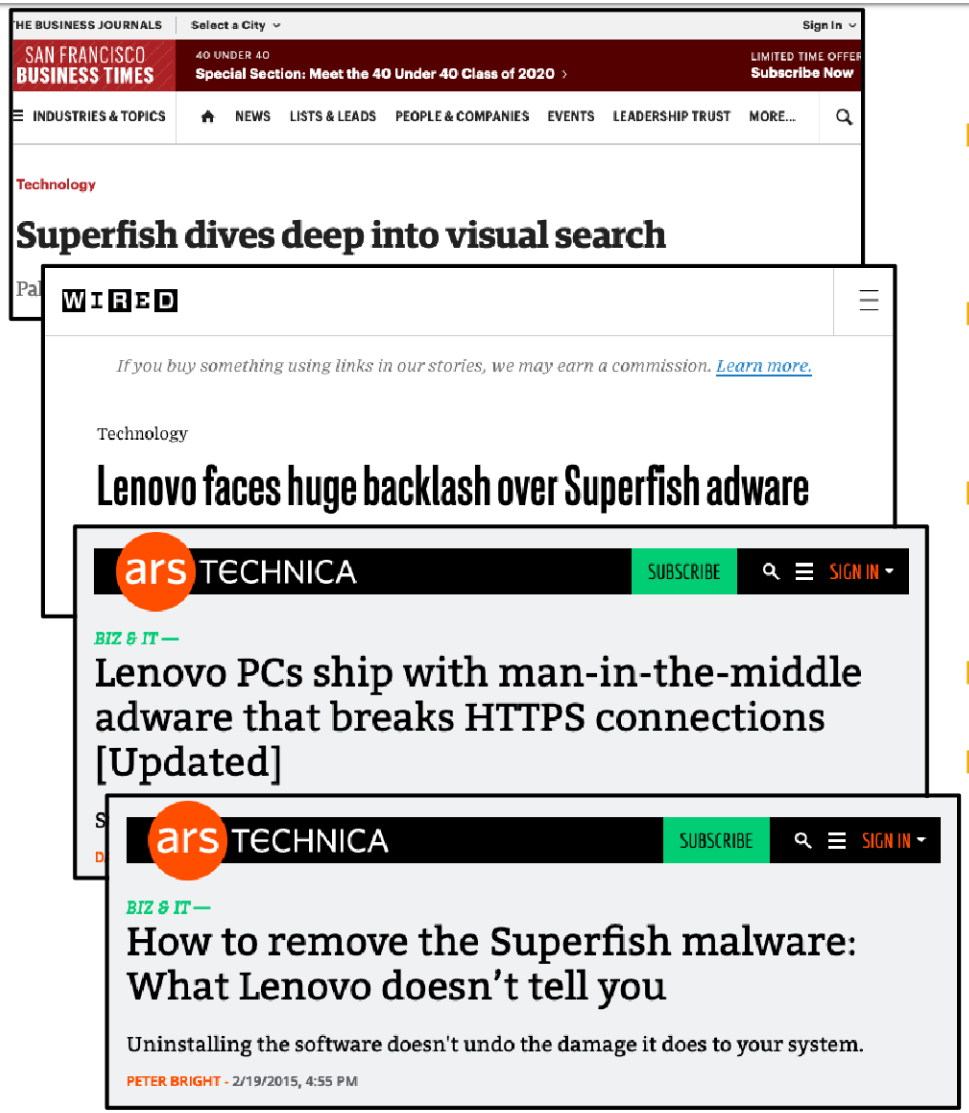
- Added to benign SW by developer
- Added by attacker via supply-chain access
- "Owner" adds for compliance/policy
- Preinstalled
  - May not be obvious
  - May be force-installed

Pre-Installed Malware

Adware – Less-Obvious



The Story of Superfish



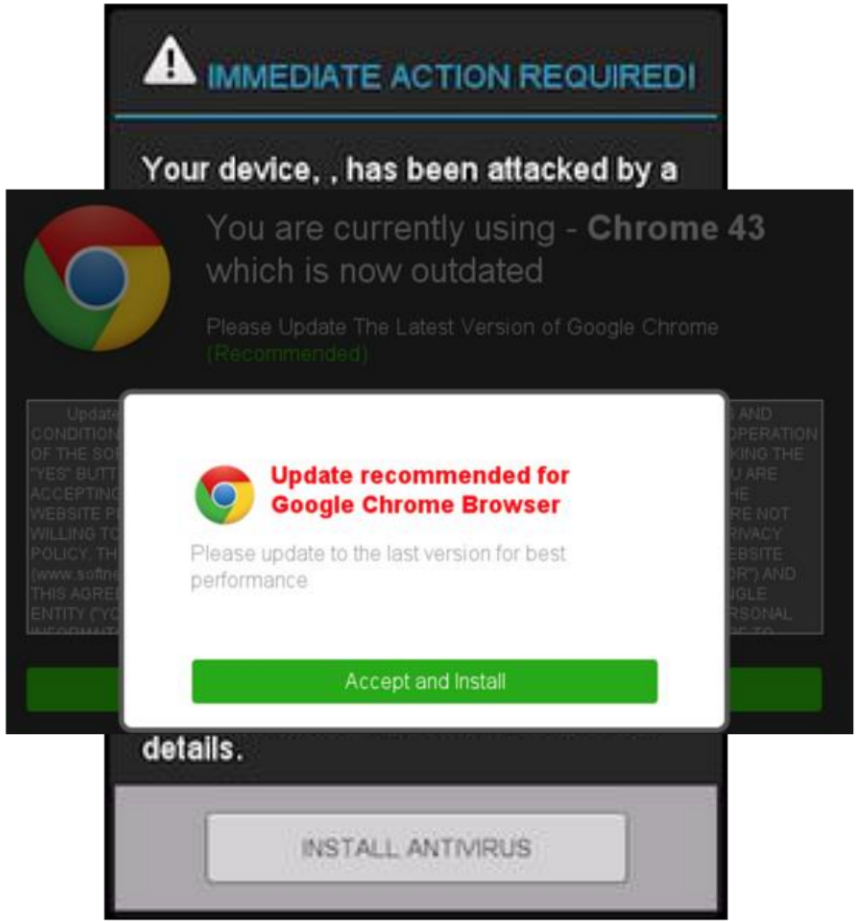
- Came pre-installed on Lenovo laptops
- Was an ad-supported visual search startup
- Actively MitM traffic for ad injection
- Injected root CA
- **SAME PRIVATE KEY ON EVERY SINGLE INSTALL**

Malware Distribution

Malware is distributed via almost every imaginable technique and vector.

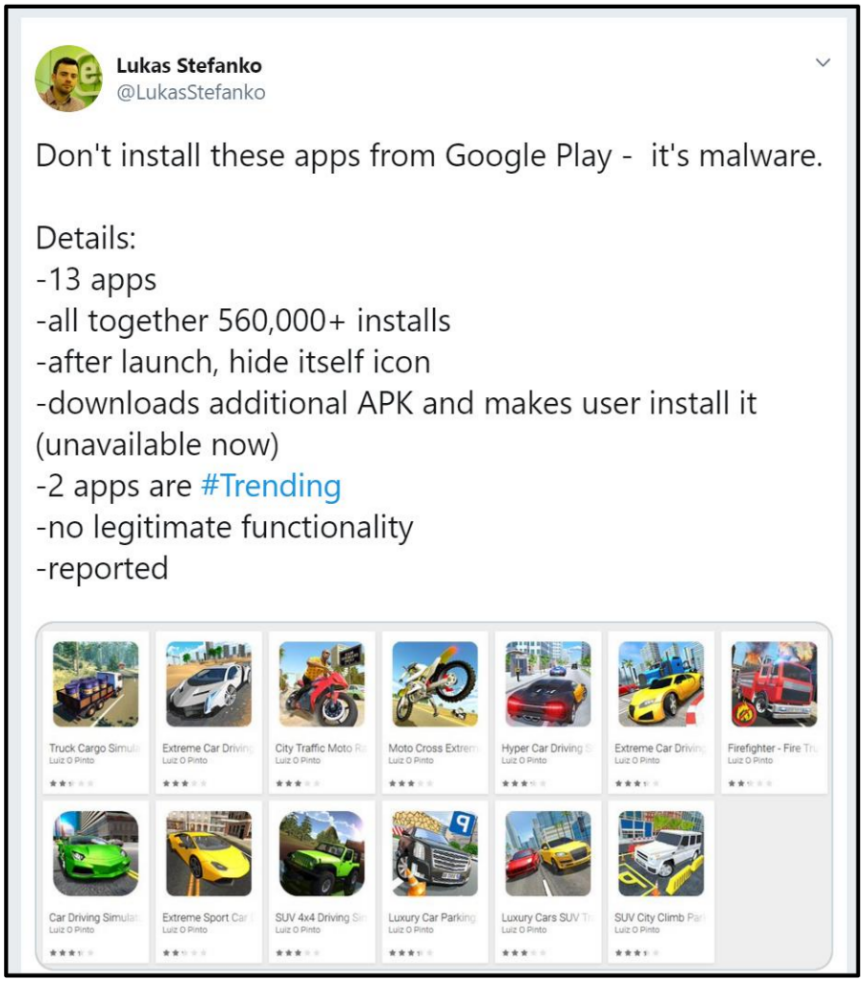
- Installed via Exploitation
- Installed via Third-Party
- Installed via User

Installed via User



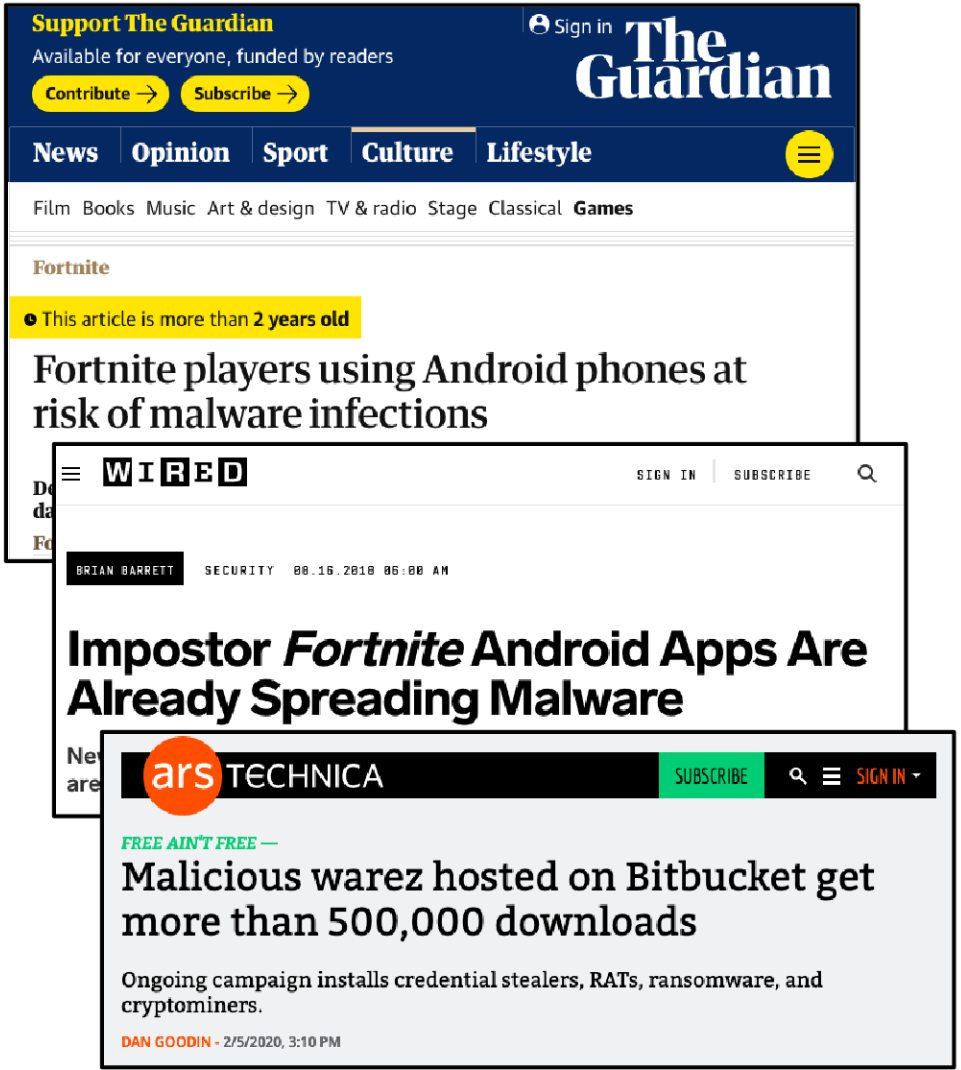
- Social Engineering
  - User is tricked into installing themselves
  - Can be last-resort of drive-by-download

Installed via User



- 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



- 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 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

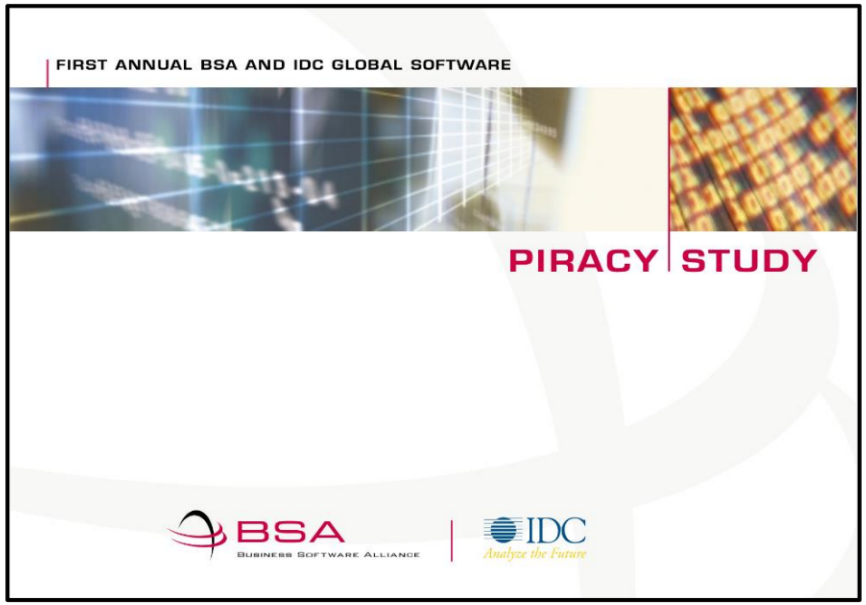
20 Software Cracks: A Great Way to Infect Your PC

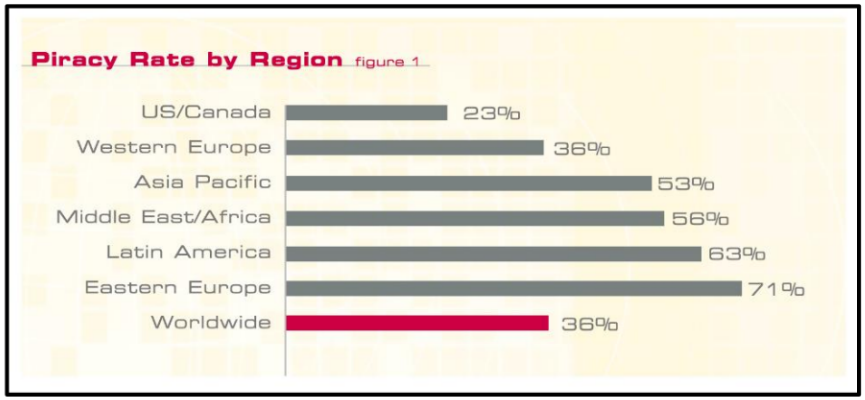
JUN 11

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

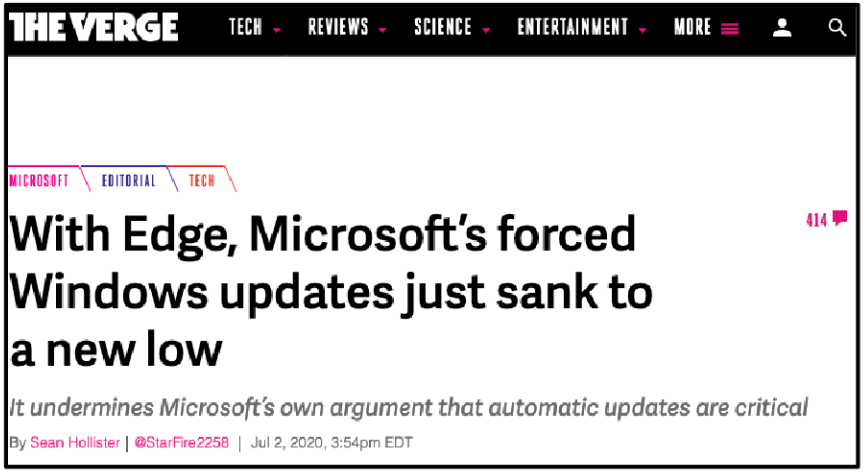
- One-time purchase for 1 PC or Mac
- Classic 2019 versions of Word, Excel, and PowerPoint
- Microsoft support included for 60 days at no extra cost
- Licensed for home use

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


THE VERGE TECH REVIEWS SCIENCE ENTERTAINMENT MORE

MICROSOFT EDITORIAL TECH

414

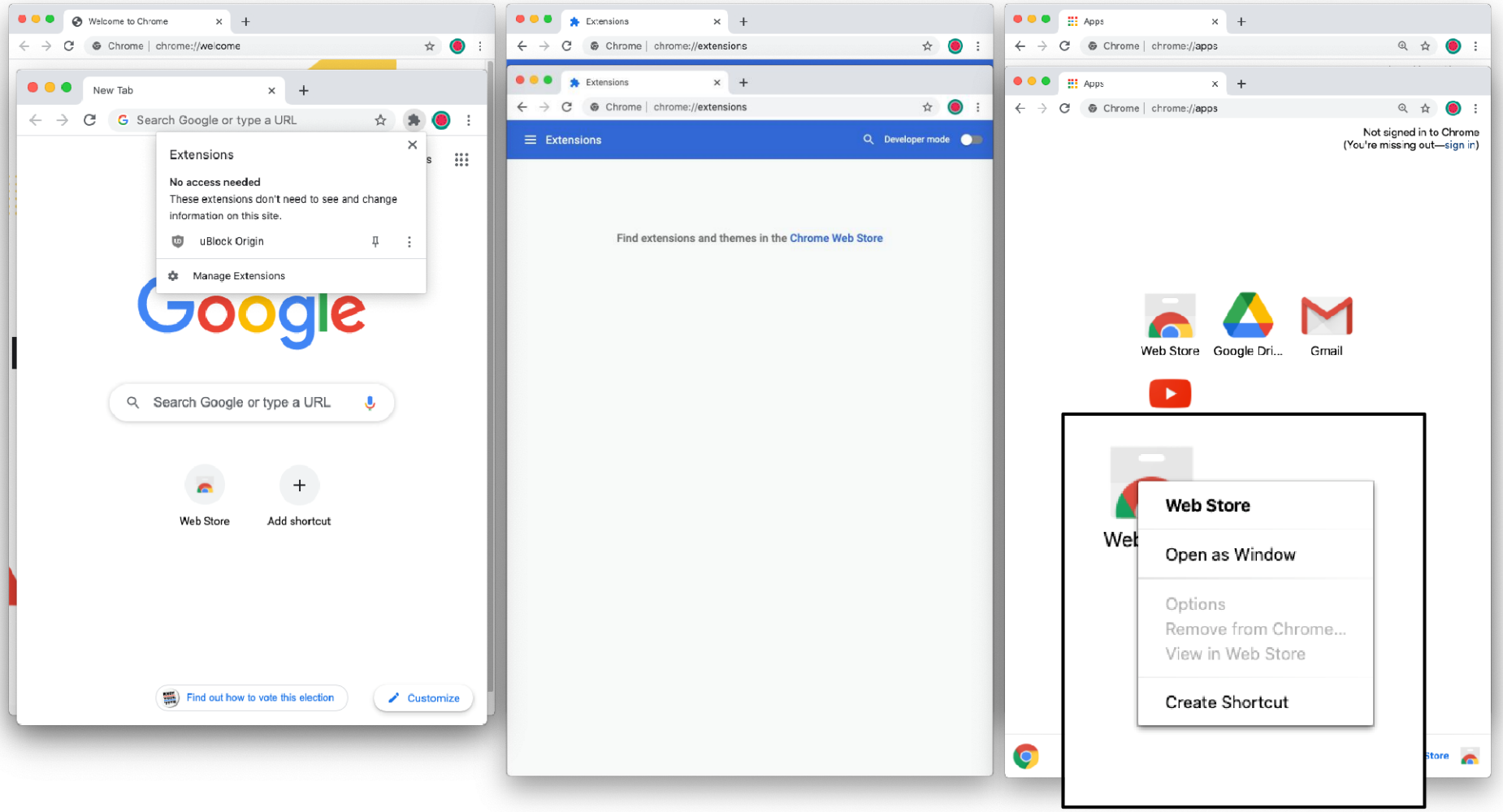
With Edge, Microsoft's forced Windows updates just sank to a new low

It undermines Microsoft's own argument that automatic updates are critical

By Sean Hollister | @StarFire2258 | Jul 2, 2020, 3:54pm EDT

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

Bundled Malware



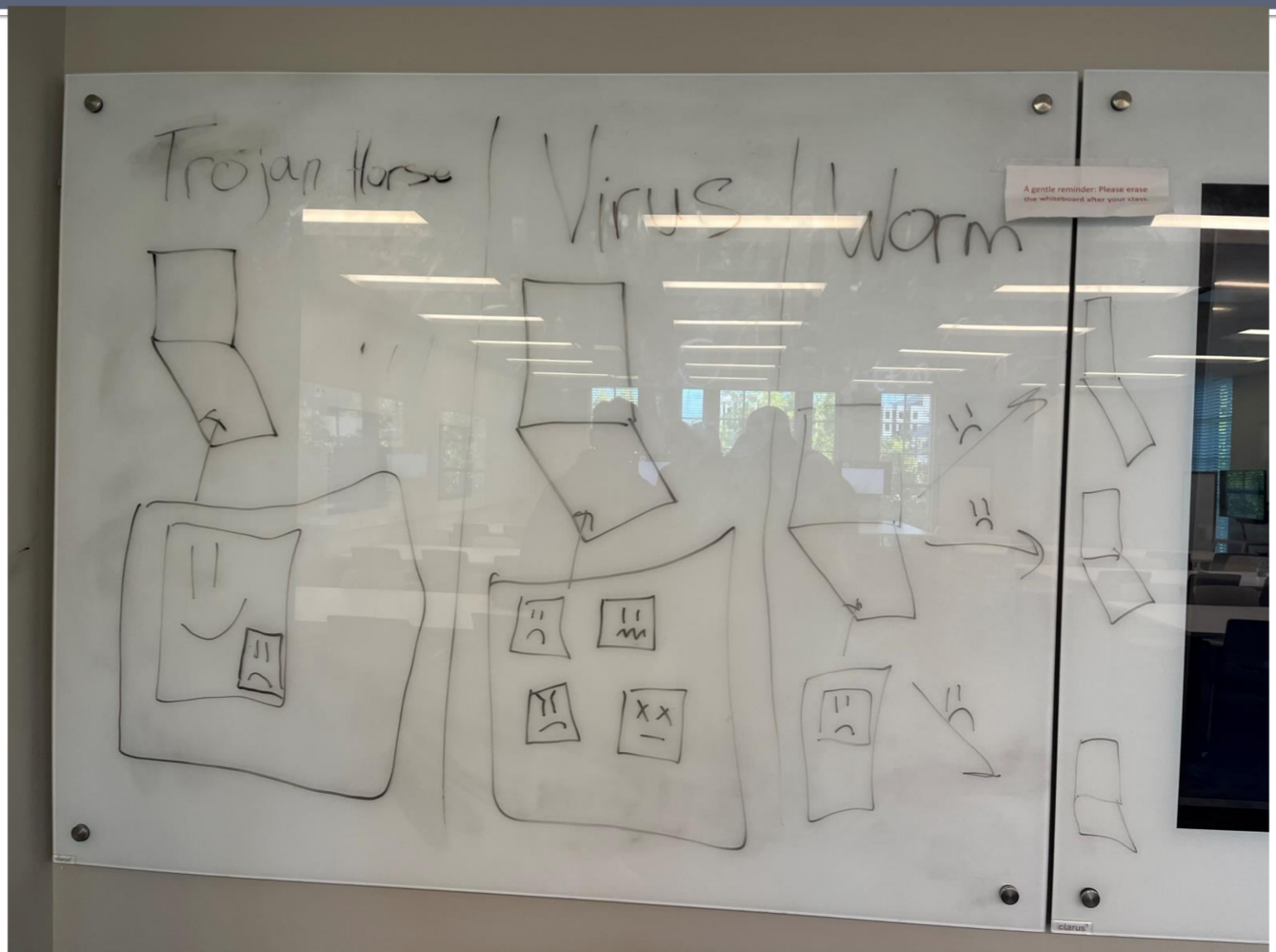
Malware Distribution

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