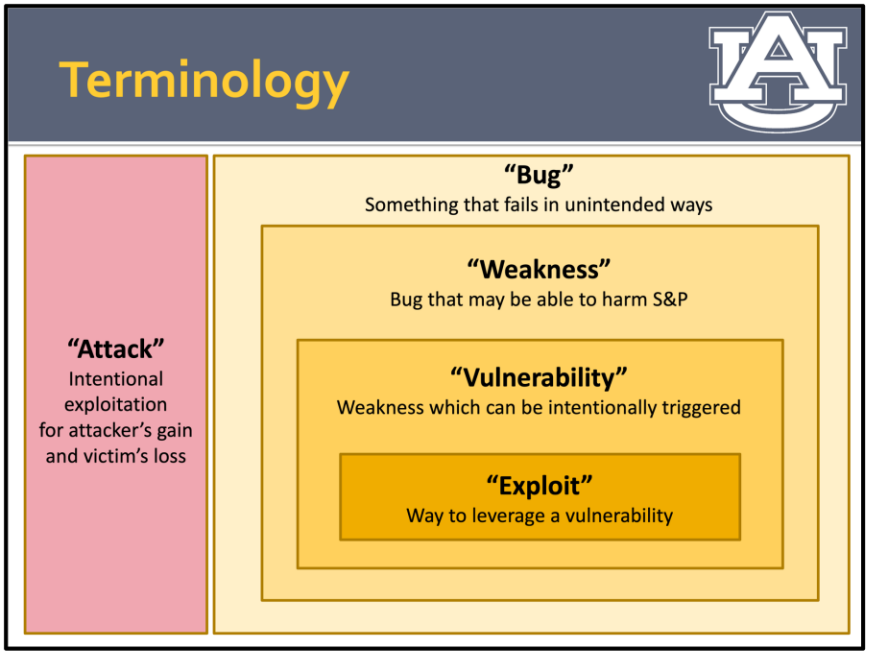
Computer and Network Security

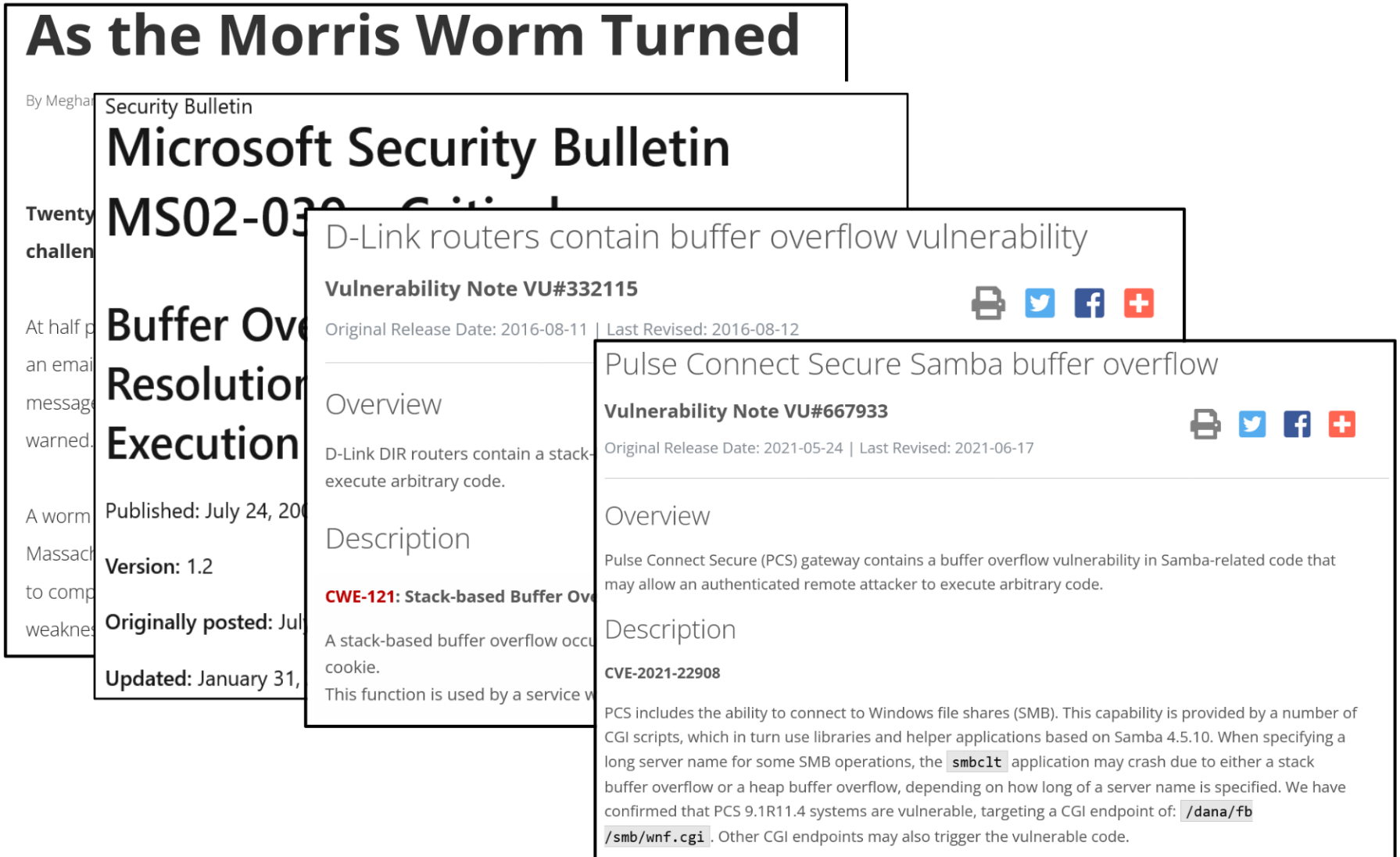
Lecture 12:
Malware & Common Attacks

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





As the Morris Worm Turned

By Megha

Twenty
challen

At half p
an emai
messag
warned.

A worm
Massach
to comp
weakne

Security Bulletin

Microsoft Security Bulletin MS02-03

Buffer Ov
Resolutio
Execution

Published: July 24, 20

Version: 1.2

Originally posted: Jul

Updated: January 31,

D-Link routers contain buffer overflow vulnerability

Vulnerability Note VU#332115

Original Release Date: 2016-08-11 | Last Revised: 2016-08-12

Overview

D-Link DIR routers contain a stack-
execute arbitrary code.

Description

CWE-121: Stack-based Buffer Ov

A stack-based buffer overflow occu
cookie.
This function is used by a service w

Pulse Connect Secure Samba buffer overflow

Vulnerability Note VU#667933

Original Release Date: 2021-05-24 | Last Revised: 2021-06-17

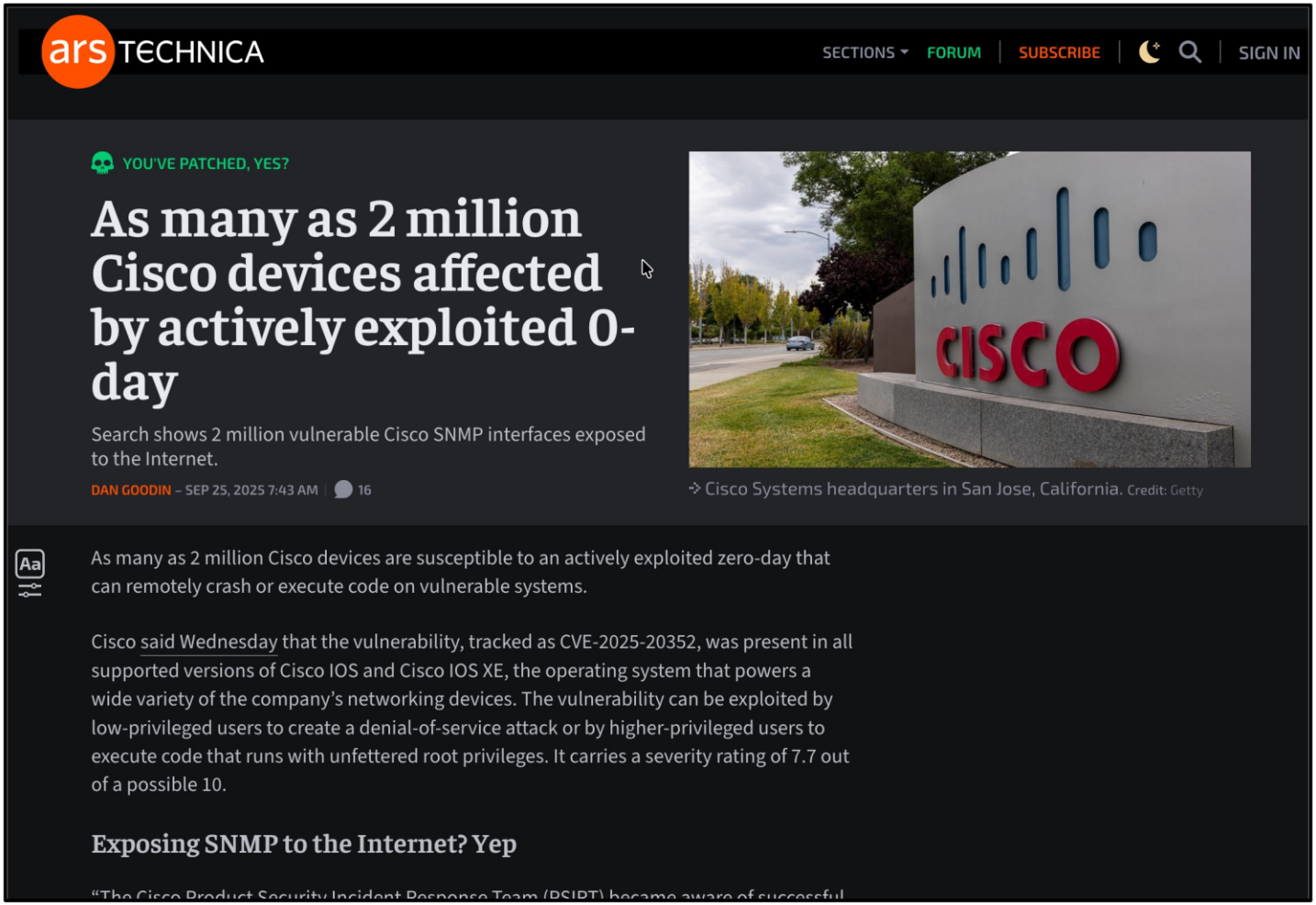
Overview

Pulse Connect Secure (PCS) gateway contains a buffer overflow vulnerability in Samba-related code that may allow an authenticated remote attacker to execute arbitrary code.

Description

CVE-2021-22908

PCS includes the ability to connect to Windows file shares (SMB). This capability is provided by a number of CGI scripts, which in turn use libraries and helper applications based on Samba 4.5.10. When specifying a long server name for some SMB operations, the `smbclt` application may crash due to either a stack buffer overflow or a heap buffer overflow, depending on how long of a server name is specified. We have confirmed that PCS 9.1R11.4 systems are vulnerable, targeting a CGI endpoint of: `/dana/fb` `/smb/wnf.cgi`. Other CGI endpoints may also trigger the vulnerable code.


ars TECHNICA
SECTIONS
FORUM
SUBSCRIBE
SIGN IN
YOU'VE PATCHED, YES?
As many as 2 million Cisco devices affected by actively exploited 0-day
Search shows 2 million vulnerable Cisco SNMP interfaces exposed to the Internet.
DAN GOODIN – SEP 25, 2025 7:43 AM
16
CISCO
Cisco Systems headquarters in San Jose, California. Credit: Getty
As many as 2 million Cisco devices are susceptible to an actively exploited zero-day that can remotely crash or execute code on vulnerable systems.
Cisco said Wednesday that the vulnerability, tracked as CVE-2025-20352, was present in all supported versions of Cisco IOS and Cisco IOS XE, the operating system that powers a wide variety of the company's networking devices. The vulnerability can be exploited by low-privileged users to create a denial-of-service attack or by higher-privileged users to execute code that runs with unfettered root privileges. It carries a severity rating of 7.7 out of a possible 10.
Exposing SNMP to the Internet? Yep

Network Input Buffer Overflow

```
int getField(int socket, char* field){
   int fieldLen = 0;
   read(socket, &fieldLen, 4);
   read(socket, field, fieldLen);
   return fieldLen;
}
```

```
python –c "print '\x00\x01\x00\x00' +
'a' * 65536" | nc <IP> <PORT>
```

Malware

Malware is any software intentionally designed to:

- Operate in and for others' advantage
- Negatively affect the victim

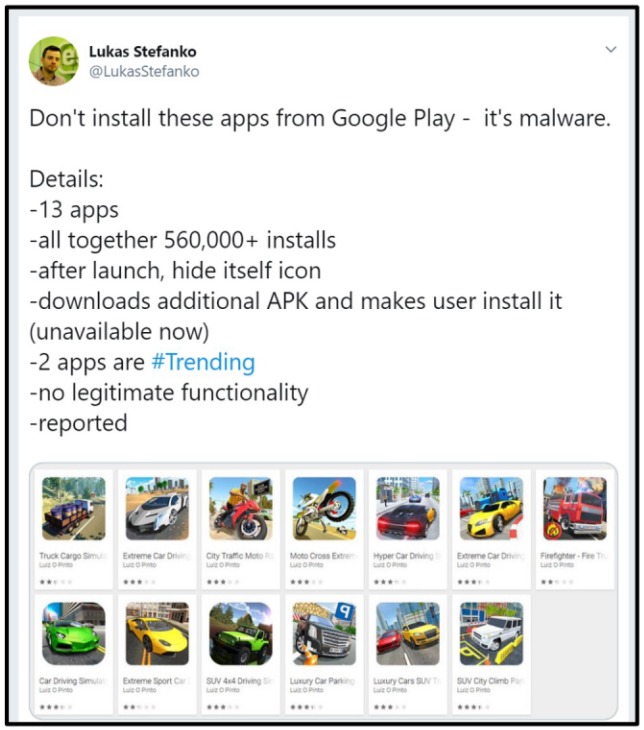
Classification of Malware

- 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

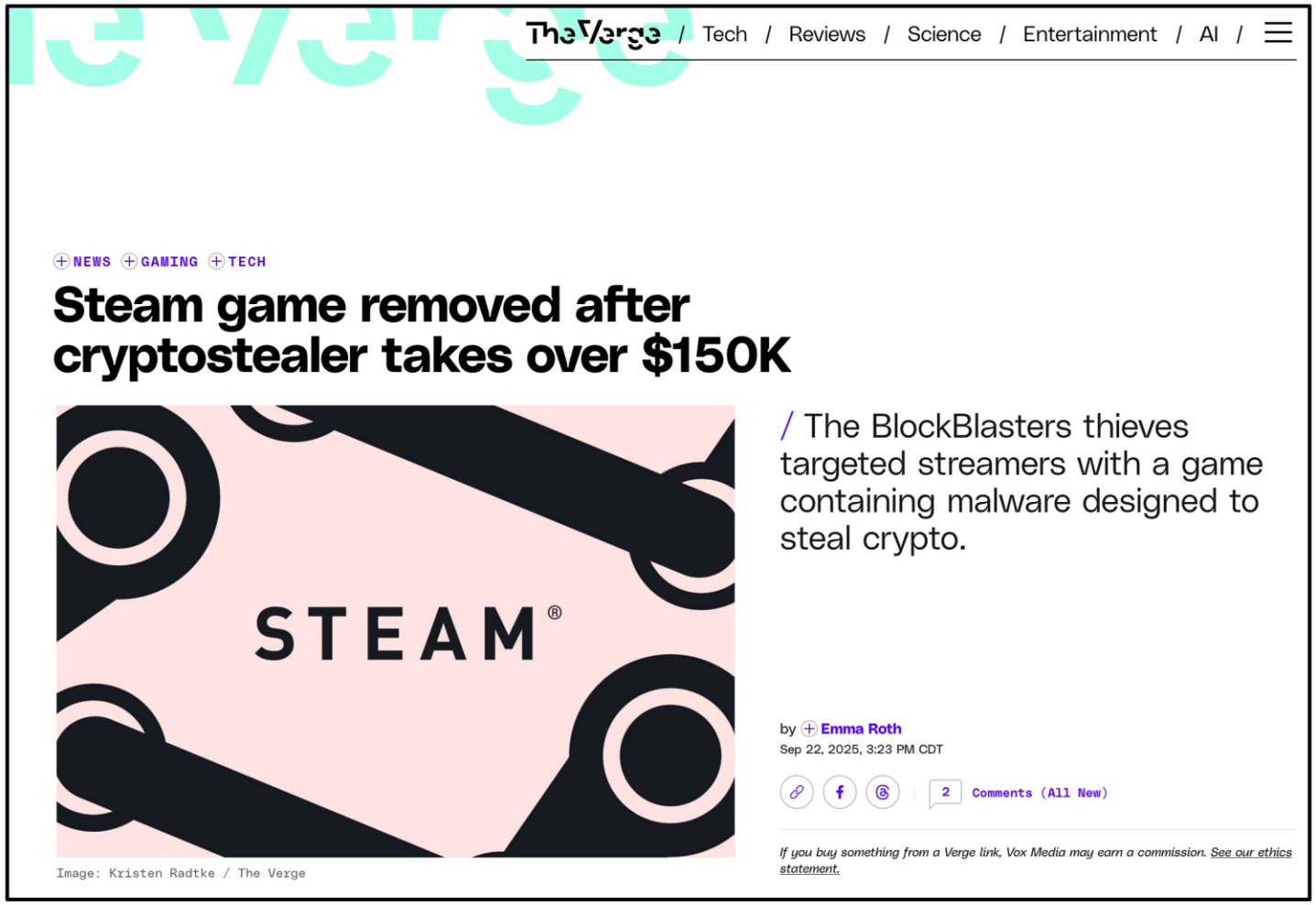
Infection Type: Trojan Horse

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

- Fake anti-virus
- Re-packages apps
- Low-effort apps



Infection Type: Trojan Horse



The Verge / Tech / Reviews / Science / Entertainment / AI /

NEWS GAMING TECH

Steam game removed after cryptostealer takes over $150K

Image: Kristen Radtke / The Verge

/ The BlockBlasters thieves targeted streamers with a game containing malware designed to steal crypto.

by Emma Roth
Sep 22, 2025, 3:23 PM CDT

2 Comments (All New)

If you buy something from a Verge link, Vox Media may earn a commission. See our ethics statement.

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

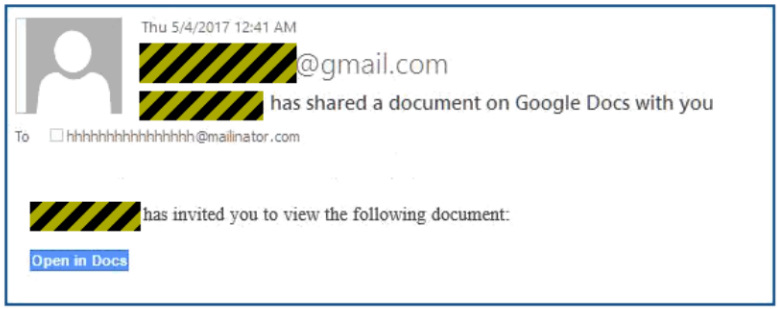
Infection Type: Worm

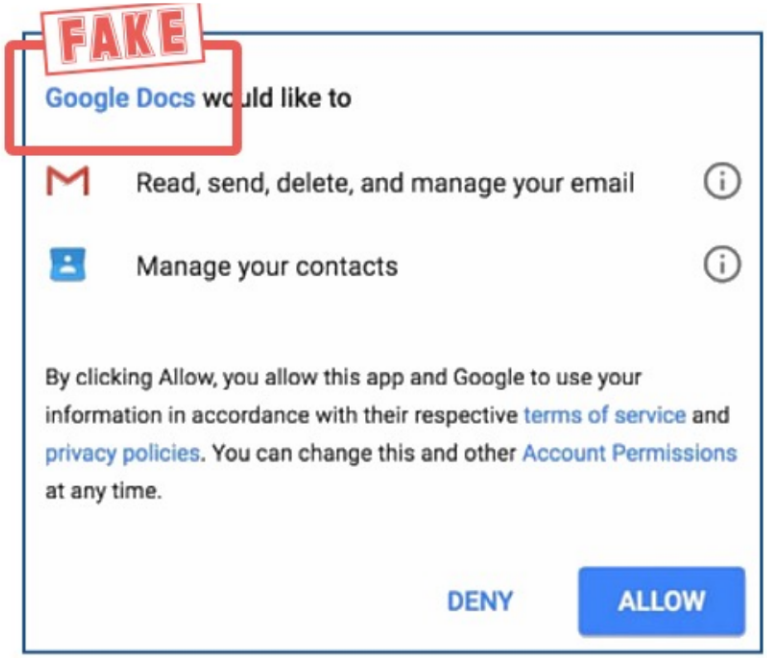
A **worm** is a virus that has the ability to spread itself to other devices automatically.

- 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

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:

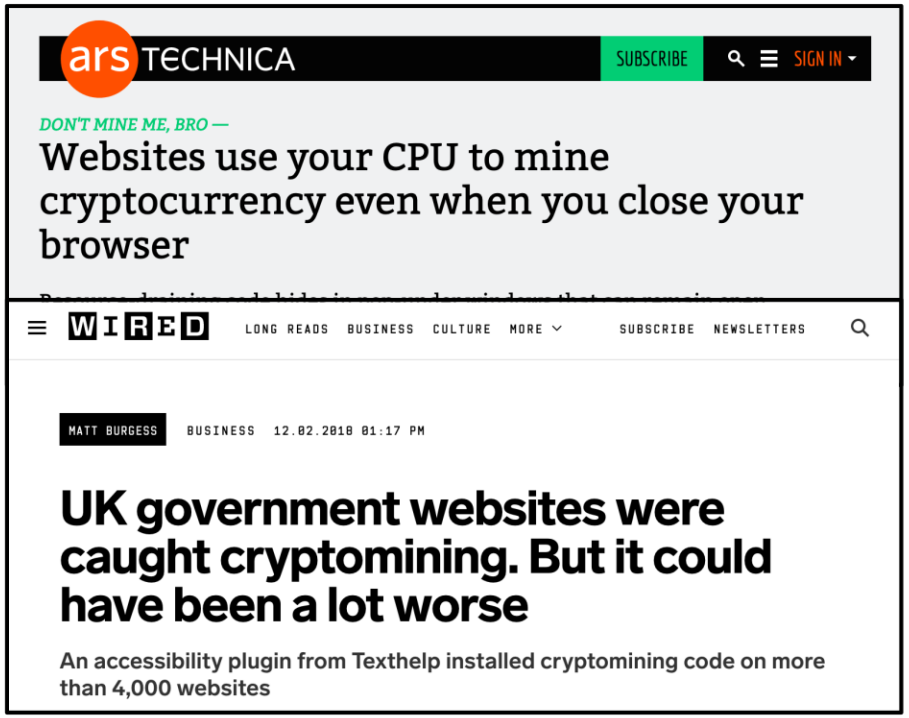
- Operate in and for others' advantage
- Negatively affect the victim

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.

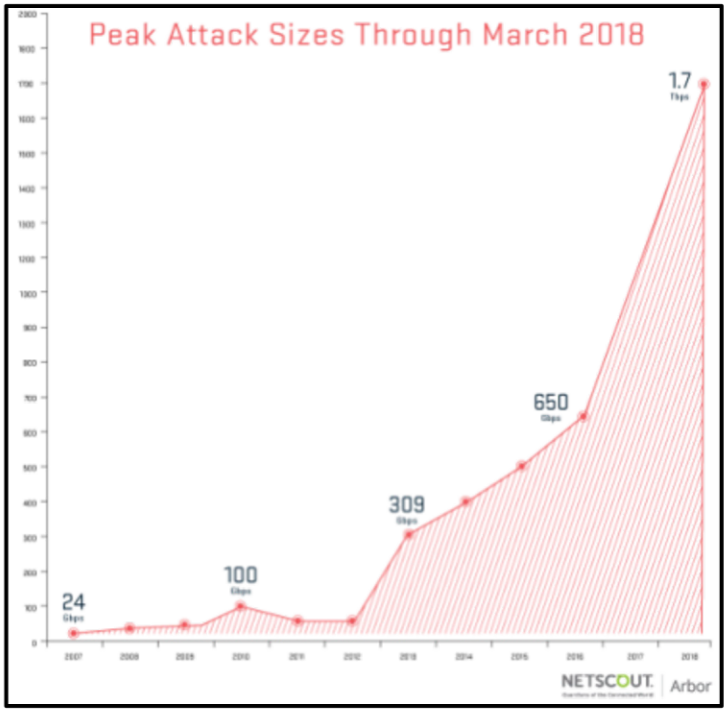
- Often injected via JS and run in browser
- Miner "pools" make it profitable even with limited computation



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*

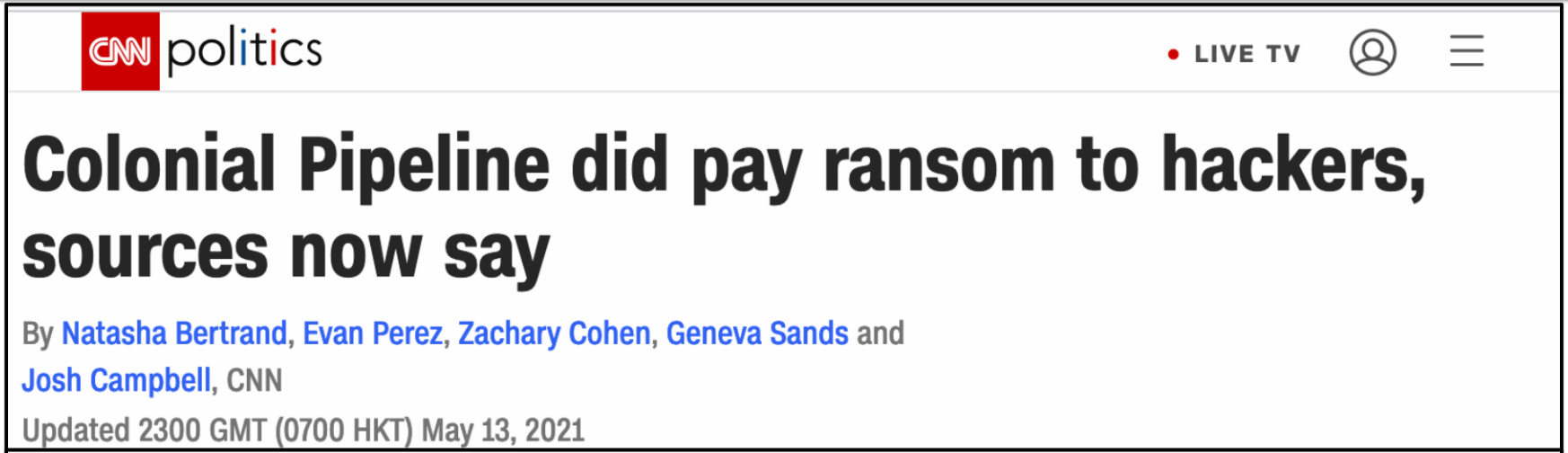


Intent: Ransomware

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

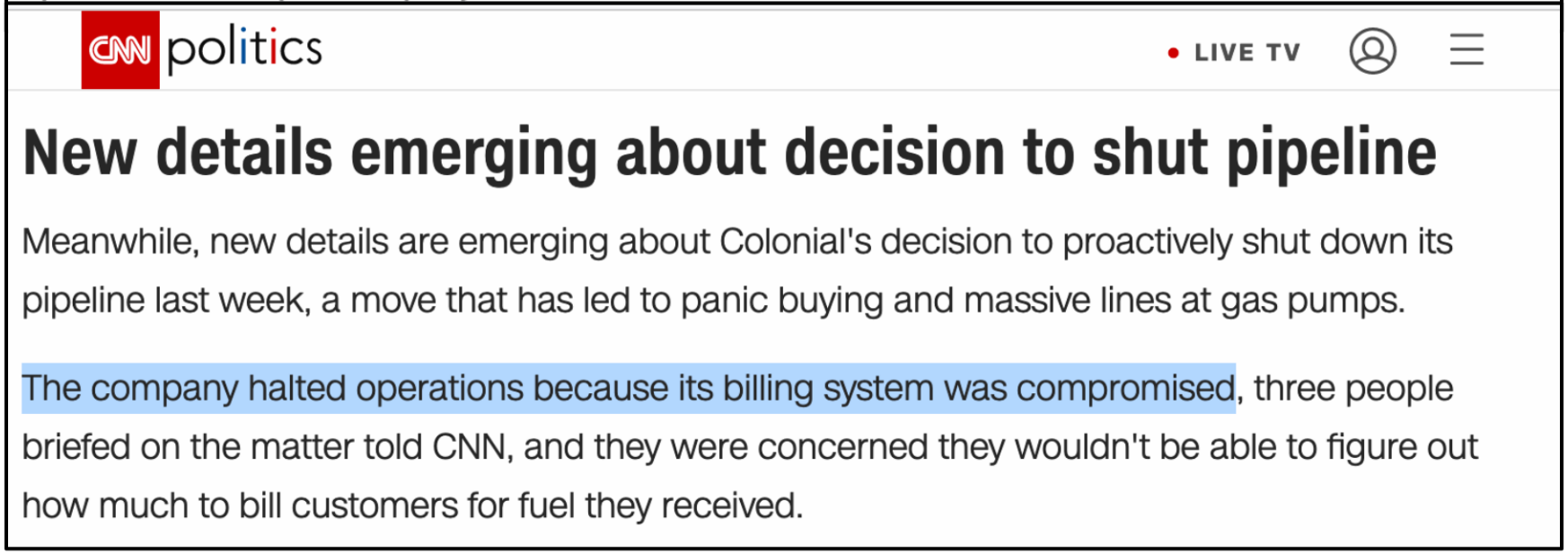


CNN politics • LIVE TV

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

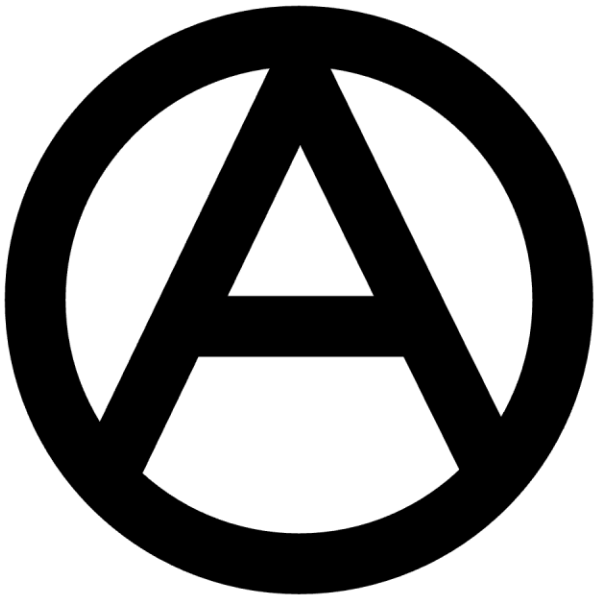
Meanwhile, new details are emerging about Colonial's decision to proactively shut down its pipeline last week, a move that has led to panic buying and massive lines at gas pumps.

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.

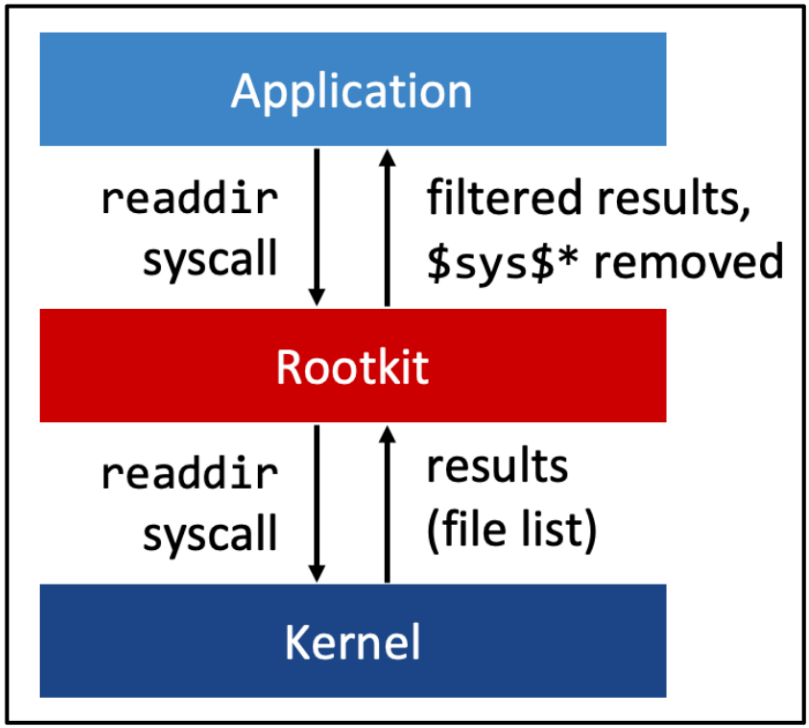
- Use by activists and other ideological actors is not unheard of
- Use by criminal organizations is relatively rare
- Use by nation-state actors is widely believed



Intent: 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



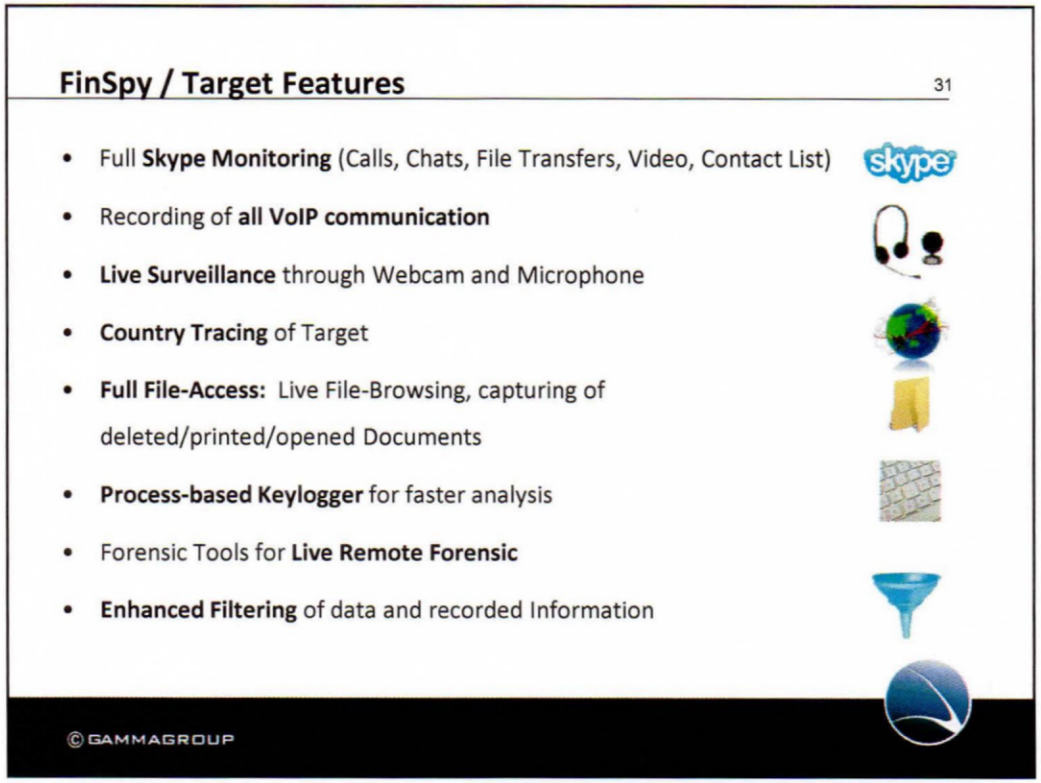
Intent: Spyware

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 base on their by 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."

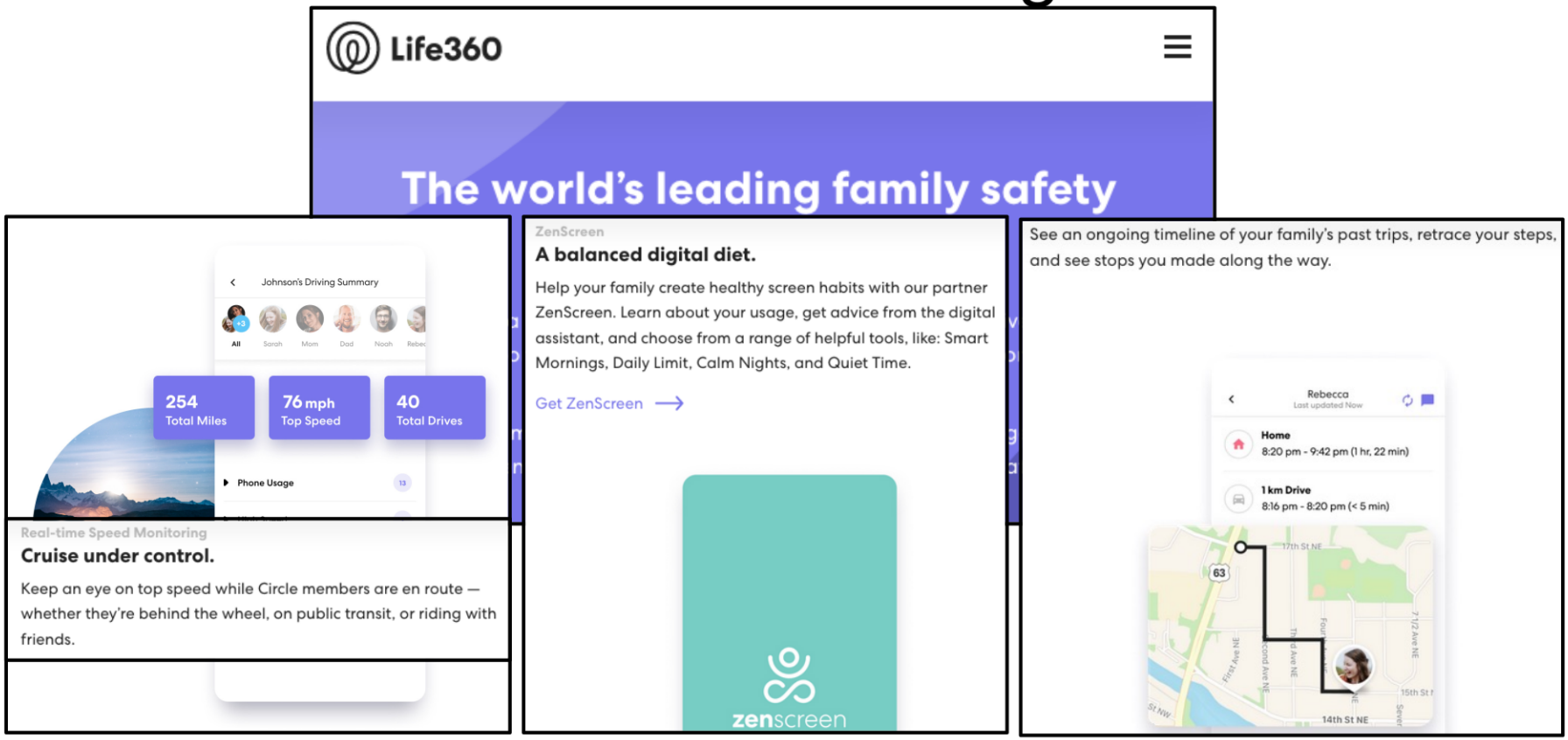
Intent: Spyware

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

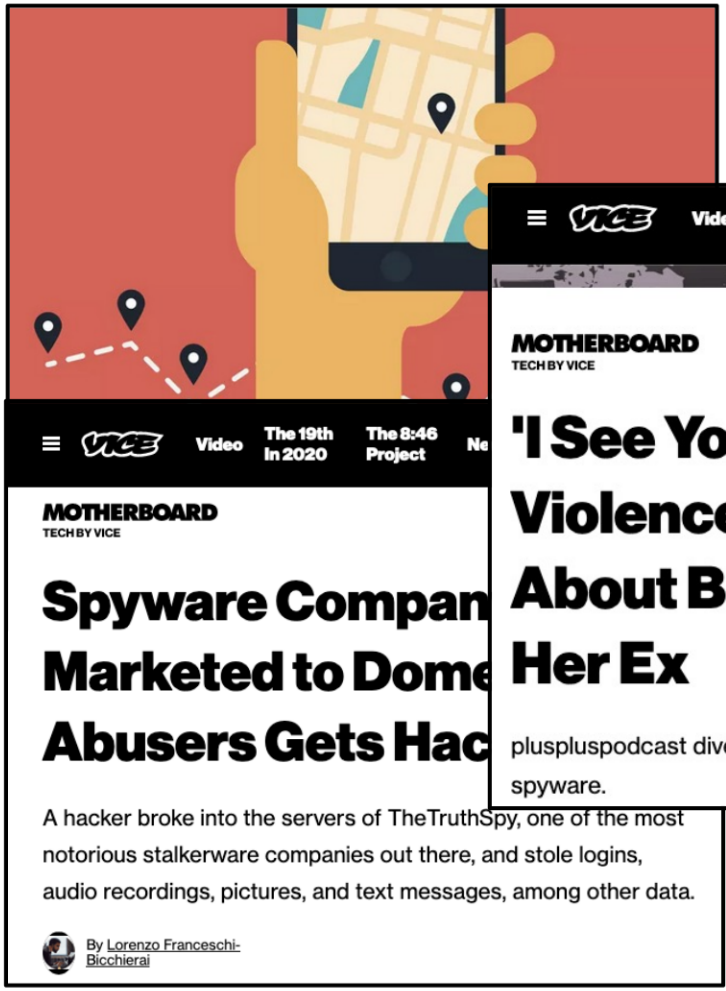
- Key loggers, screen captures, data exfiltration, GPS/microphone/camera data
- **Does not have to be hidden**

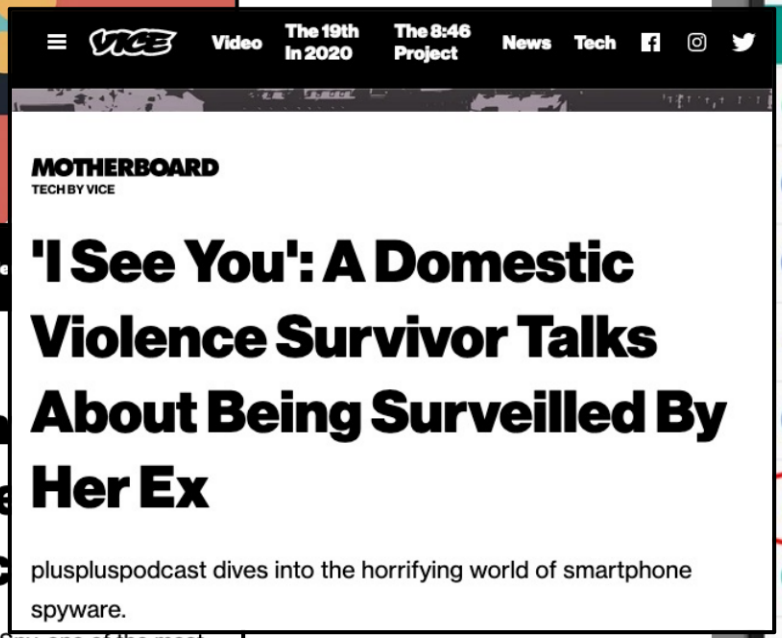
Less Obvious Spyware

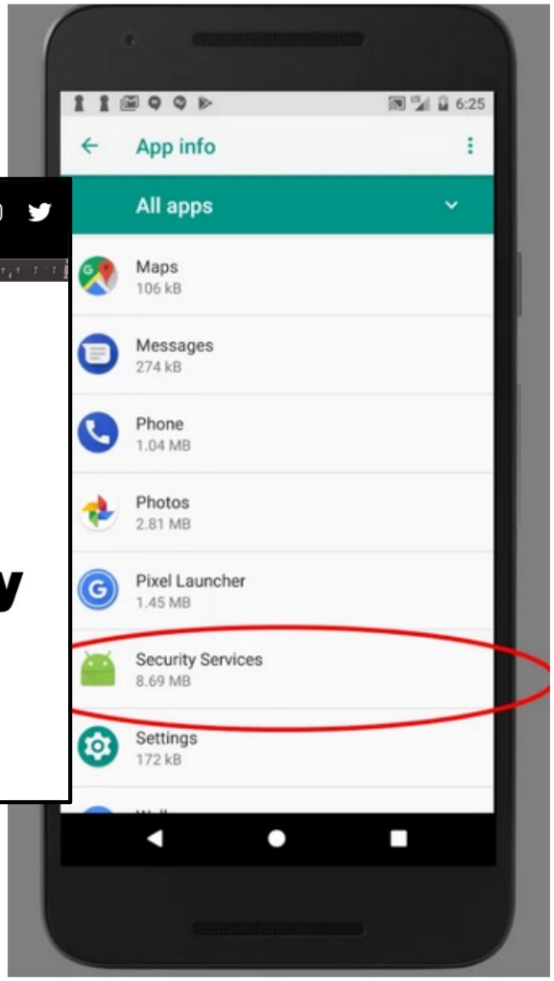
- Some instances are significantly less obvious due to their branding



Really Sketchy Spyware







Is it 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

MEAZURE 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

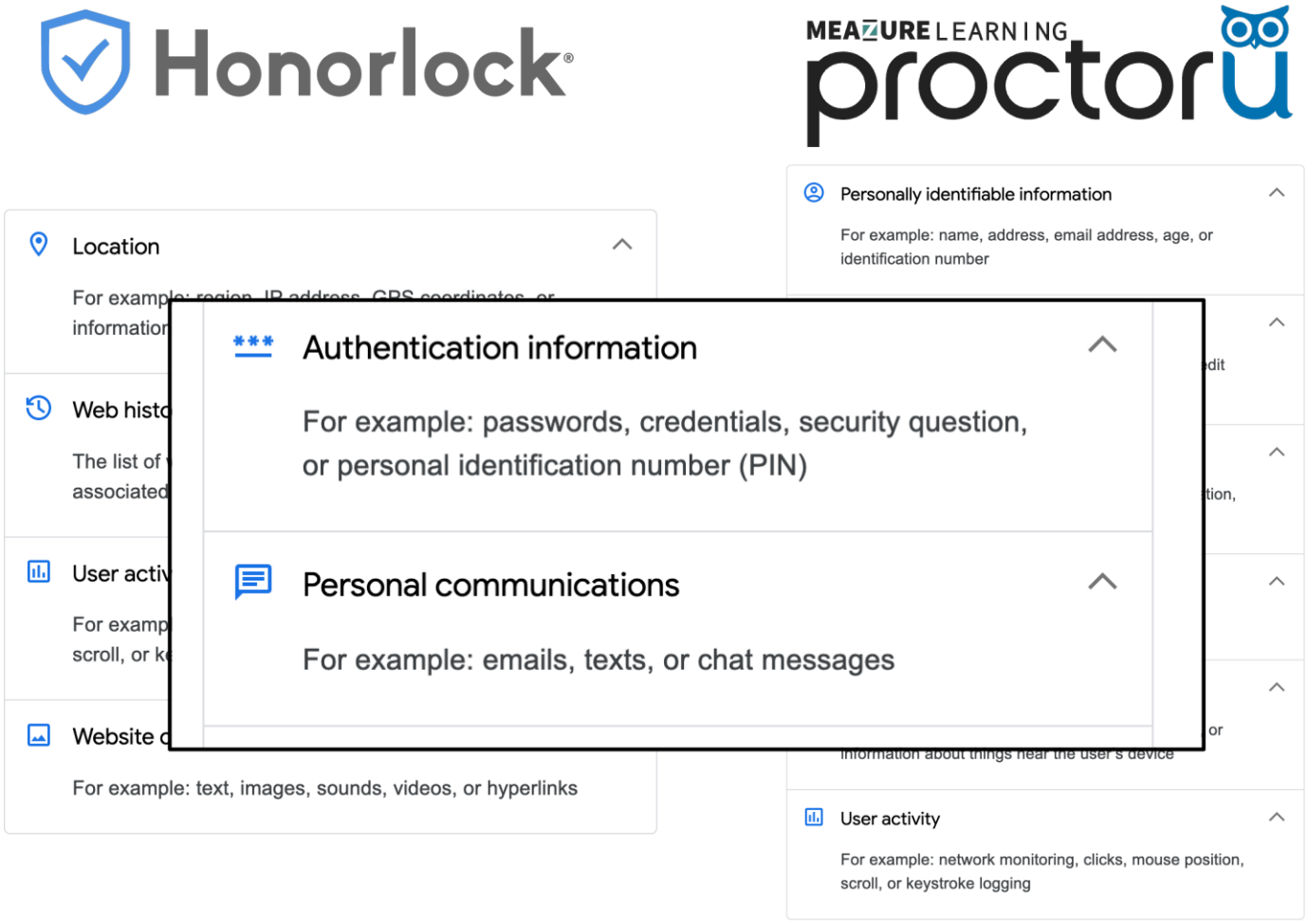
Location

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?



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.

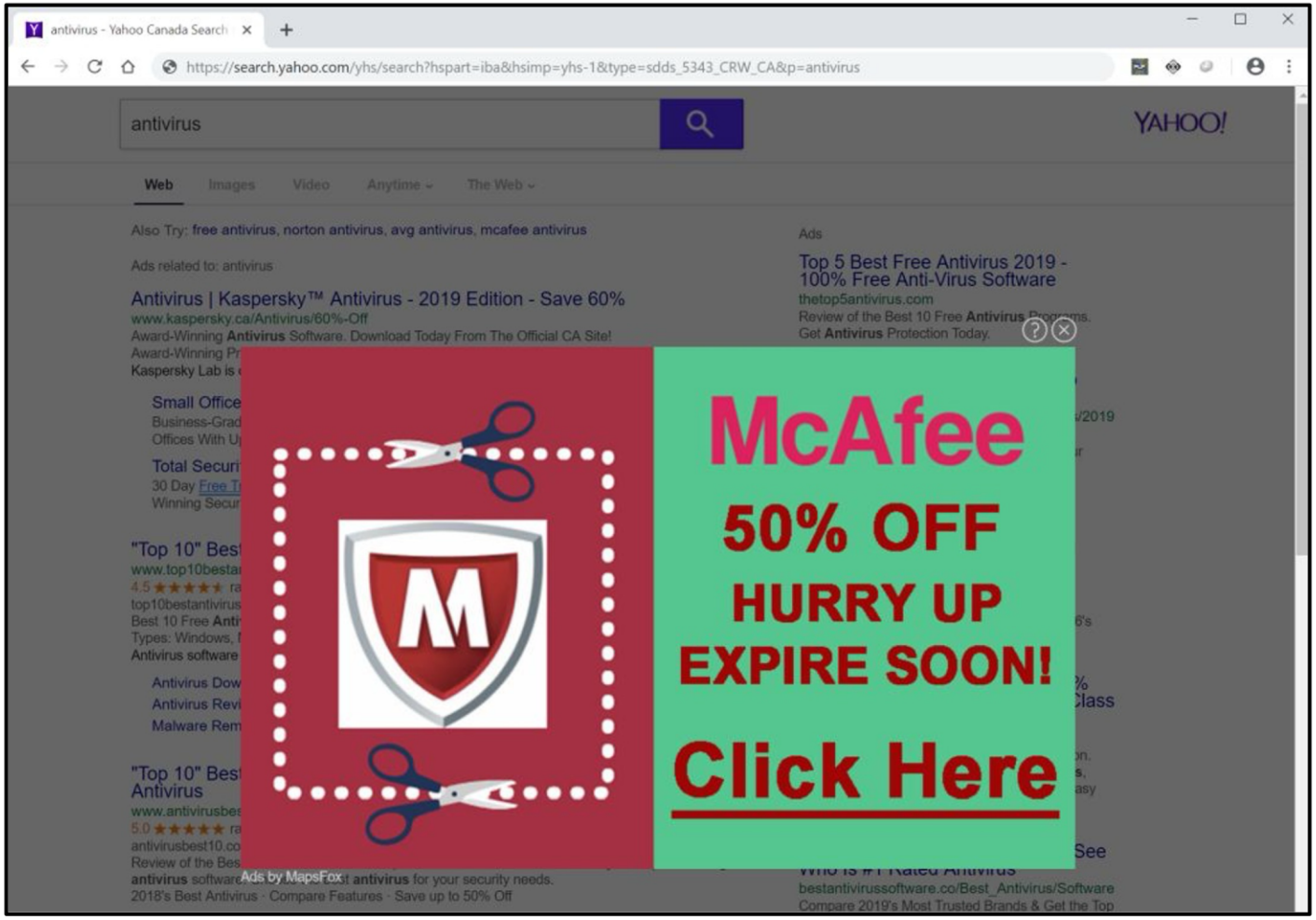
Proctoring Apps Subject Students to Unnecessary Surveillance
With COVID-19 forcing millions of teachers and students to rethink in-person schooling, this moment is ripe for an innovation in learning. Unfortunately, ...
eff.org

4:13 PM · Oct 11, 2020 · TweetDeck

Intent: Adware

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

Adware – Less-Obvious



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

Computer and Network Security

Lecture 12:
Malware & Common Attacks

COMP-5370/6370
Fall 2025