CTRL+ESC+HOST

Ezra Woods
https://www.linkedin.com/in/ezrawoods/

Mike Manrod
@CroodSolutions
https://www.linkedin.com/in/manrod/

Kiosks – Gotta Catch Em All!!

Who are we?

Ezra Woods

Mike Manrod

[BeaconatorC2]

[BYOEDR]

[Threat Intelligence Support Unit (TISU)]

[Arizona Cyber Threat Response Alliance (ACTRA)]

The views expressed are our own and do not represent the views of our employers or any affiliated organizations.

Do not attack or test malware / tactics against systems you do not either own or have permission to test on.

If we look younger in these photos, it is because this work has aged us both.

--- Acknowledgments ---
These project would not have been possible without the outstanding contributions of these key researchers, among several others:

- Jordan Mastel
- flawdC0de (Jim)
- Kitsune-Sec (Cameron)
- Mspisces8 (Komal)
- Alexander, Ken, David, John, and Thomas
- The Bingus Man
- TechSpence
- John Hammond

Agenda

- Introduction to Escape to Host flaws.
- A bit about hacking Kiosks and Presented Apps.
- Introduction to our new CTRL+ESC+HOST framework/project.
- Specific walkthroughs of our experiences hacking kiosks and escaping presented apps.

Kiosks and Presented Apps

- What is a Kiosk?
  - A computer terminal exposed in a somewhat public area, for users of lower trust levels to interact with, usually consuming and/or providing information to support some business process or use case.
- What is a Presented Application?
  - A Presented Application is a software program that runs on a remote server, but is delivered to the user as if it were a local app, with only the interface of that single application exposed.
- Other (Out of Scope) Escape Scenarios:
  - VDI, browser, VM, container, etc.

Why is this important?

- Sometimes it isn't.
  - A Kiosk that is fully isolated in every way, serving a use that is low risk and low priority.
  - Sometimes kiosk hacking is not important. It is REALY fun though.
- Other times it is wildly important:
  - A kiosk device is publicly facing in insecure areas, while also being on the same network or joined to a domain, as critical resources.
  - A presented app has lower trust users, but is running on a server, domain, and network zone that provides a fast track from outside to widespread compromise.

Escape to Host

Escape to Host refers to a situation where an application that is presented in a restricted or sandboxed environment, can be “escaped” to allow the user to execute code, commands, or take other actions on the host or backend infrastructure.

MITRE ATT&CK technique T1611 lists this under Privilege Escalation, which checks out, but it also can be so much more.
https://attack.mitre.org/techniques/T1611/

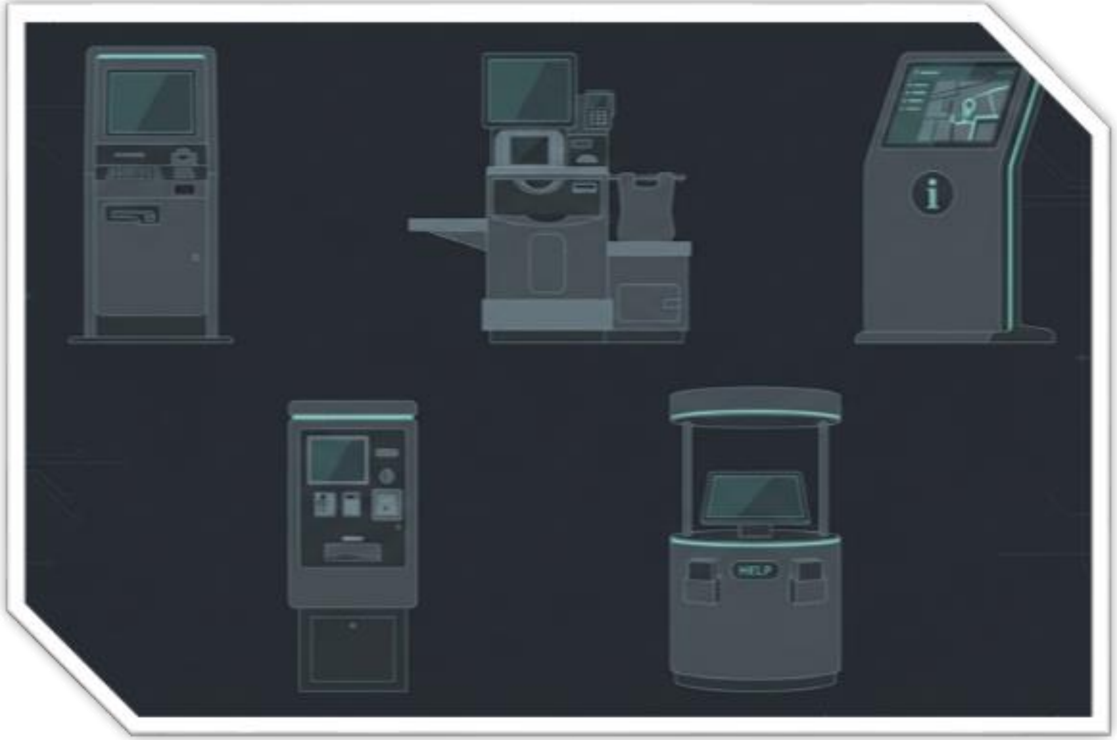
Introducing Ctrl+Esc+Host

- A framework.
- A series of stories from our own testing.
- Some tools that helped along the way

CTRL+ESC+HOST

The Methodology

Identify the Target



Kiosk or Presented App?

- Kiosk vs Presented App
- Citrix and VMware Horizon

What type of Kiosk?

- Windows
- ChromeOS
- Android
- Linux (other)
- Apple

Layers of Kiosk Attack Surface

- Application running on the kiosk
- Kiosk software itself (OS native vs. 3rd party)
- Physical factors:
    - Are there any exposed ports (such as USB)?
    - What input/output devices can you interact with?
    - Are there physical locks protecting the ports / are they effective?
    - Wireless attack surface to consider

Windows 11 Attended Access (Default Config)

- Windows 11 Attended Access is Microsoft's built-in single-app kiosk mode
- It locks the device to a single application (typically Edge), restricting the user from accessing the desktop, taskbar, Start menu, or other apps.
- Commonly deployed for public-facing kiosks, library terminals, digital signage, and shared-use workstations.
- The default configuration relies heavily on UI restrictions rather than actual secure configurations

USB: The Gift That Keeps on Giving

- Win11 Attended Access does not show USB drives in File Explorer or dialog boxes.
- However, typing an explicit path like `D:\msedge.exe` in a file dialog will access and launch from the USB.
- PowerShell can also interact with USB via `cd D:/` even though the drive is invisible in the GUI.
- `Set-Clipboard -Path 'D:\payload.exe'` stages a payload on the clipboard for pasting into a save dialog.
- Executables can be smuggled as `.txt` files to bypass file-type copy restrictions, then renamed back.

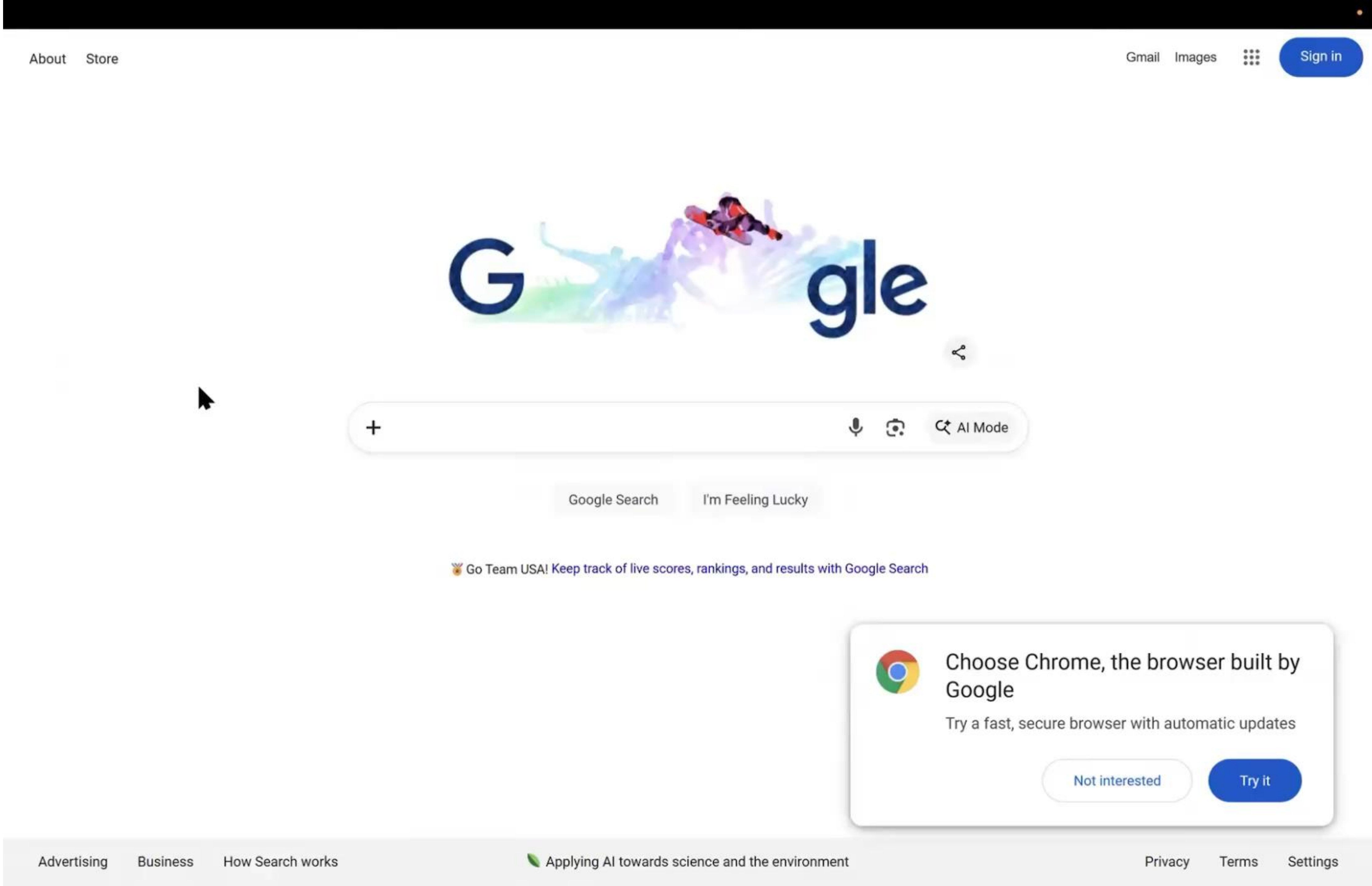
ftp.exe & LotL via the ! Command

- App control in Attended Access checks filenames, not binaries
- Stage ftp.exe on a USB, renamed to msedge.exe.
- Open a file dialog (Ctrl+O or Ctrl+S), type D:\msedge.exe to launch.
- Inside ftp.exe, the ! operator executes arbitrary shell commands:
  - `! powershell.exe` gives a full interactive shell.
- This bypasses CMD-level restrictions,
- AutoIT-compiled executables also run successfully when renamed to `msedge.exe`, so custom payloads are viable.
- Credit: @NotNordgaren for the ftp.exe suggestion; multiple additional LotL binaries confirmed to work.

Settings as an Attack Surface

- VPN configuration is available in Settings — a malicious VPN could redirect traffic for ingress or C2.
- Proxy / PAC file settings are writable, even with InTune policies applied.
- PAC file requests confirmed via RequestBin, WinHTTP sends actual HTTP requests to the configured URL despite network restrictions
- Windows PAC files are JavaScript, and sanitization strength is an open question worth further research.

Download and Run LotL via Edge from Local Host



Go Team USA! Keep track of live scores, rankings, and results with Google Search

Choose Chrome, the browser built by Google

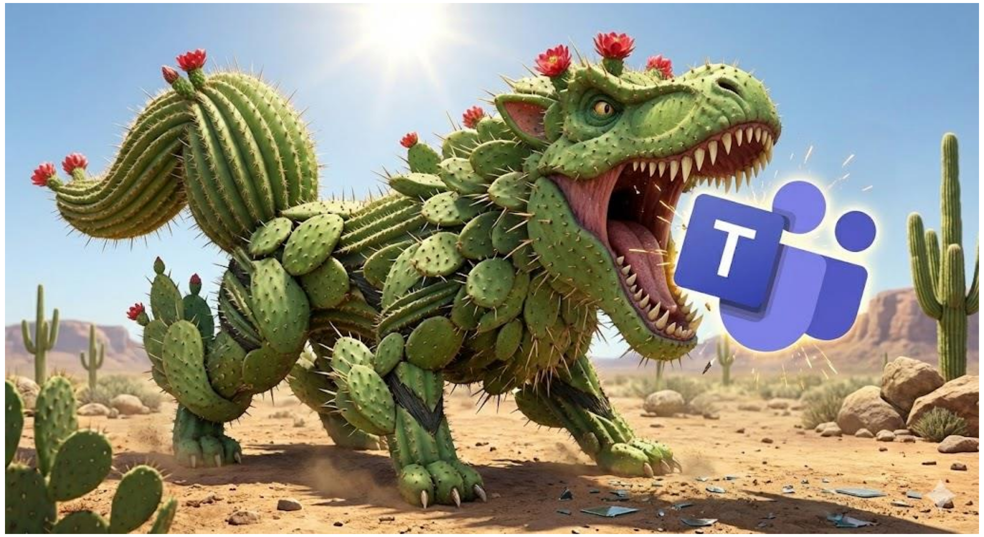
Try a fast, secure browser with automatic updates

Applying AI towards science and the environment

File Staging & Ingress Without a Download

- Upload a payload to an allowed internal platform (e.g., Teams, Slack, etc), then download via the kiosk browser.
- Ctrl+S saves a webpage as "Complete HTML," writing all dynamic content (CSS, JS, images) to a local folder.
- Stage executable content as text on an allowed web page, copy it, paste into a `.txt` file on the kiosk, then rename.
- MS Teams meetings can deliver files, zip extraction is blocked, but sending as `.txt` and renaming back works.
- PowerShell clipboard staging from USB (`Set-Clipboard -Path`) lets you paste payloads into save dialogs.

There's no I in MS Teams



Ctrl+Win+Shift+F11 launches Teams on Lenovo hardware after a fresh reboot (does not work on subsequent attempts without rebooting).

Teams' file dialog provides a less locked-down explorer view than the kiosk default, full "New" button, folder options, and rename are available.

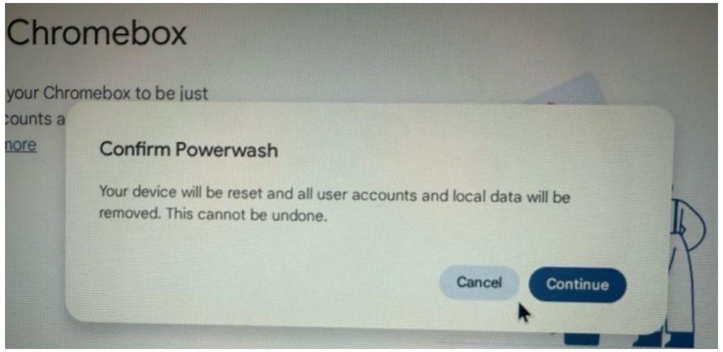
This enables renaming `.txt` files back to `.exe`, which is blocked in the normal kiosk explorer.

Files can be delivered remotely via a malicious Teams meeting, zip extraction is blocked, but text files get through and can be renamed.

The Teams launch is currently unreliable and hardware-specific, but the less-locked explorer view is the real value, if any other method triggers it, the same file operations become available.

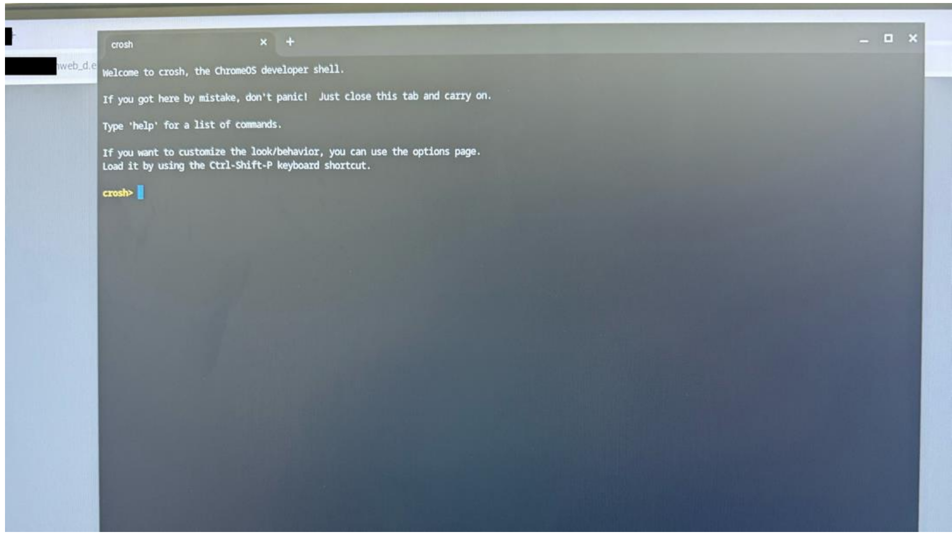
A misconfigured ChromeOS Enterprise Enrolled box.

- What we did:
  - Ctrl+Alt+Shift+M for AppSpace device menu
  - Ctrl+Alt+S
  - Ctrl+Alt+Shift+R to Powerwash
  - Ctrl+Alt+Shift+R again and Powerwash to reset
  - Click the Gear Icon
  - Restart
- Why it worked:
  - *This was not a ChromeOS flaw, but an implementation issue where there were multiple profiles for Enterprise Enrollment, and we were able to make it pick up a less secure default profile, which let us change this from a signage kiosk into a full system that would let us browse and interact with resources in that network zone.*



Confirm Powerwash

Your device will be reset and all user accounts and local data will be removed. This cannot be undone.



[redacted]

[redacted]web_d.e

```
Welcome to crosh, the ChromeOS developer shell.

If you got here by mistake, don't panic!  Just close this tab and carry on.

Type 'help' for a list of commands.

If you want to customize the look/behavior, you can use the options page.
Load it by using the Ctrl-Shift-P keyboard shortcut.

crosh>
```

Attacking the Application

Secondary escape within the SaaS application, did not actually require a full ChromeOS kiosk escape, hijack the signage kiosk and make it our own.

Key point: Sometimes there are many shades of kiosk escape, providing a wide range of capabilities.

An HP POS Kiosk on the wrong network

- Shift+Alt+NumLock to open the Mouse Keys dialog box.
- Click "Disable this keyboard shortcut..."
- Control Panel window loads, opening path to File Open.
- Typed C:\Windows\System32\cmd.exe and shell.

(flaw reported to HP last year / remediated where we found it)

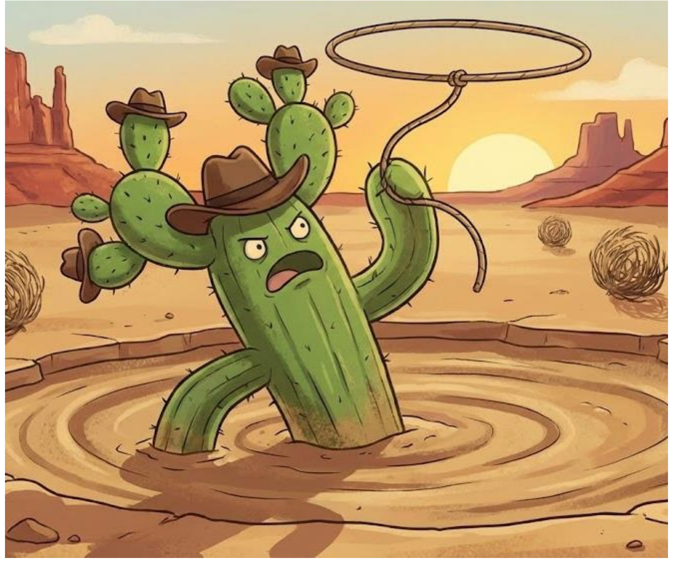
Escaping a Citrix Presented App as a datacenter foothold

- One problem with Citrix presented apps:
  - The Citrix Storefront server needs to be joined to the domain with the users who need to authenticate to the application, so escape the domain and you probably have the ability to interact with an important domain controller.
- Methods of escape to try that we have found to work:
  - Find a Save As or Open dialog box and launch applications (think LotL).
  - Launch a browser to explore vulnerable internal resources with a web interface.
  - Print will sometimes allow you to enumerate domain objects via Find Printer / Advanced.
  - See the repo for a full set of escapes to try.

EnvisionWare PC Reservation Software

- Pre-Authentication Escape
  - Sticky Keys (Shift x5).
  - Win+L, followed by immediately Win+K, holding both keys down a moment, and then screen cast comes up.
  - Then Win+TAB to expose desktop options.
  - Then click “+” add more desktops.
  - Then drag a desktop up onto the screen.
  - Search for something to run, such as Netsh.exe or custom payload off USB (RMM).
- Post-Authentication Escape
  - Super simple:
    - Open one of the allowed/approved apps.
    - File / Save As, and then just navigate to LotL binaries and launch.

Adventures with Win11 Kiosk Mode (Attended Access)



- Win11 Attended Access Single App Kiosk Mode is rather locked down.
- John Hammond did a great series of videos three years ago, and a bunch of stuff got fixed.
- However, a variety of pathways for partial escape still exist, and new ones arise from time to time (Win+C escaped via copilot, for a short time, until it was removed).
- An interesting one we found to escape with an admin password, if it is weak or known, is:
  - Windows Key and "+" to launch Magnifier, and click the gearbox for settings.
  - Then Network and Internet / Advanced, to Modify an Adapter.
  - UAC / enter password, then Configure / Events to launch Event Viewer.
  - From the Open menu option in Event Viewer, LotL binaries can be launched

Other Issues w/ Kiosks

- While we have focused on escape-to-host flaws, it is important to note that kiosks also may have other issues:
  - Weak or default credentials.
  - Unpatched vulnerabilities / flaws.
  - Misconfigurations, including direct NAT rules / making a kiosk internet-facing.
- Sometimes it is possible to just attack the kiosk directly via one of these other pathways, vs escape-to-host.

How does one get stated in Kiosk Hacking?

- Don’t:
  - Go hack random kiosks that are not yours.
  - It is not legal and you will get in trouble.
- Fortunately:
  - There are a lot of kiosk products you can setup for low/no cost, such as Win11 Attended Access or ChromeOS kiosk mode / Enterprise Enrollment.
  - Free trials are also a good option, or you can scrounge for after-market kiosks that are no longer in use, but fully functional.
  - Get permission to test live systems, from the security team in writing or as part of a scope for an assessment engagement or penetration test.

How to use CTRL+ESC+HOST

- Use the repo as a guide of things you can try, while kiosk hacking (ethically, only with permission or on systems you own).
- Follow the testing guides for each OS generically – and,
- Read our specific scenario walkthroughs for real life examples.
- Report flaws to vendors via Responsible Disclosure.
- Also, contribute to the project, to help the overall community more effectively look for these types of flaws.

- REPO Link:
  - https://github.com/CroodSolutions/CTRL-ESC-HOST

THANK YOU…

ANY QUESTIONS?