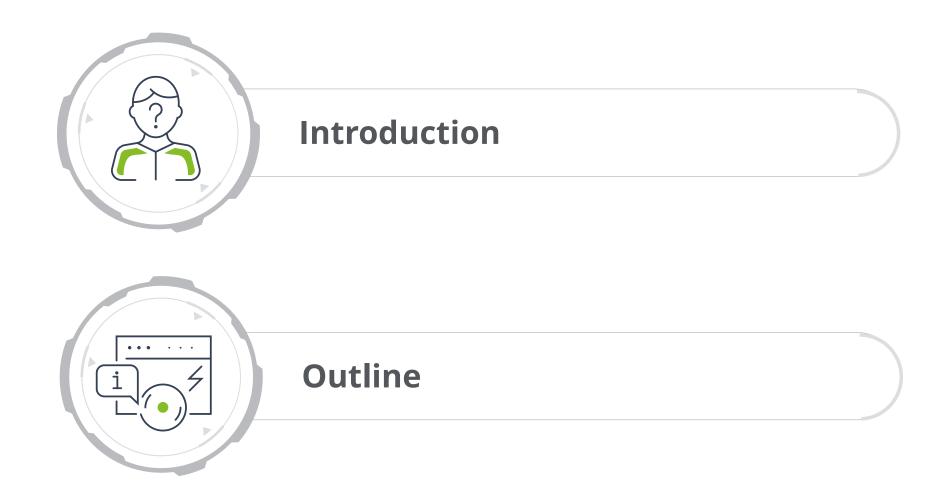
# Deloitte.

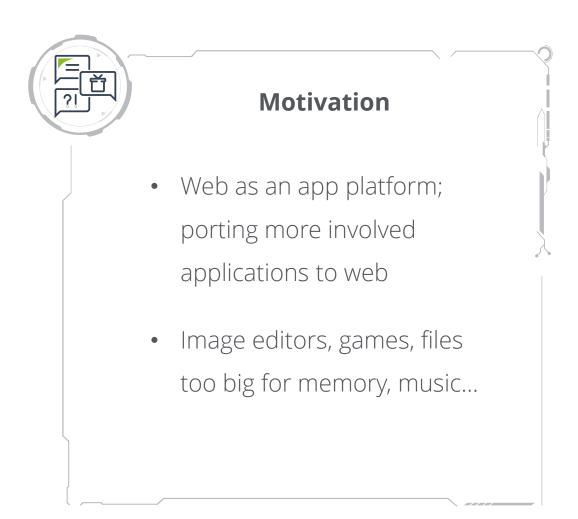


Internal affairs
Hacking file system access from the
Matt Weeks, Technology Fellow, Deloitte & Touche
LLP

### Welcome

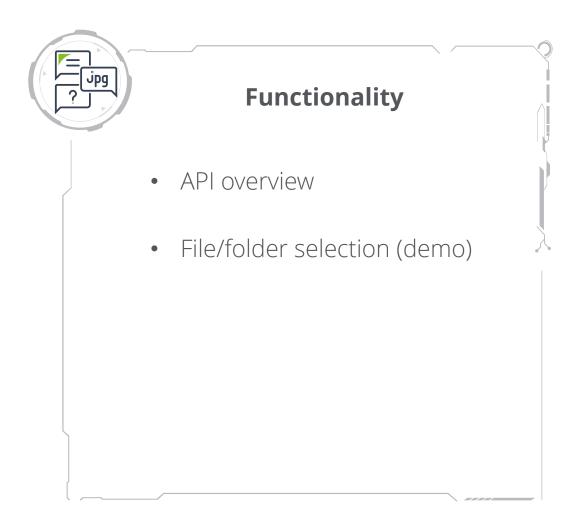


# File system access application programming interface (API) background





### File system access API current

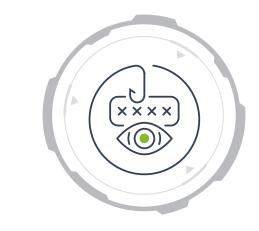




### **Security features**

- Mark-of-the-web, SmartScreen on Windows
- No full paths or separators
- Blocked file types
- Limits of arbitrary R/W

### Threat models



- Unintended reads
- Sensitive data exposure



- Unintended writes
- Corruption
- Denial of Service (DoS)



Code execution



### **Negative results—failed attacks**



Alternate data stream modification

- Attempts to remove MOTW
   Many different autoetc.
- Blocked

Directory traversal

 Path shenanigans effectively blocked Startup folder and profile attacks

- execute locations in user profiles
- Sharing of these folders disabled

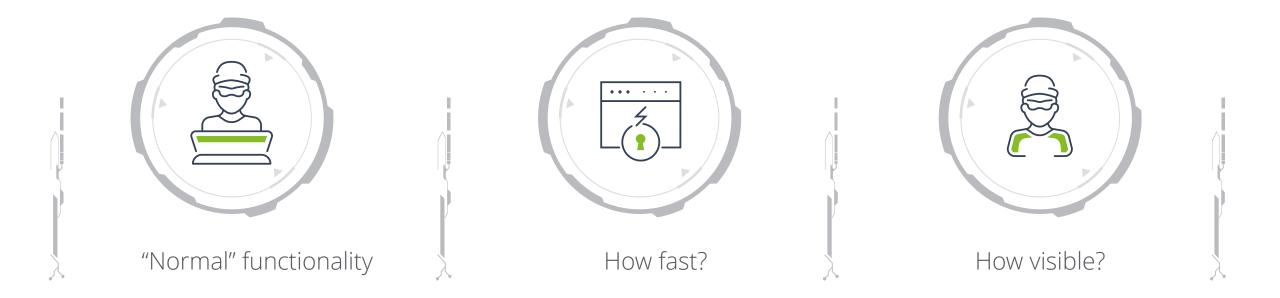
Shortcut based attacks

Blocked by type

High level folder access

 No sharing of C: drive root for example

### **Exfiltration demo**



### DoS



- Temporary file creation
  - In writable directories new files temporarily create a .crswap file
  - o If conflicting writes, multiple crswap files will be created, numbered
  - Numbers go up to 99 then failures occur
  - o This can be forced, or in certain circumstances can happen as the result of a bug

- Disk space usage
- These are worth noting but low severity

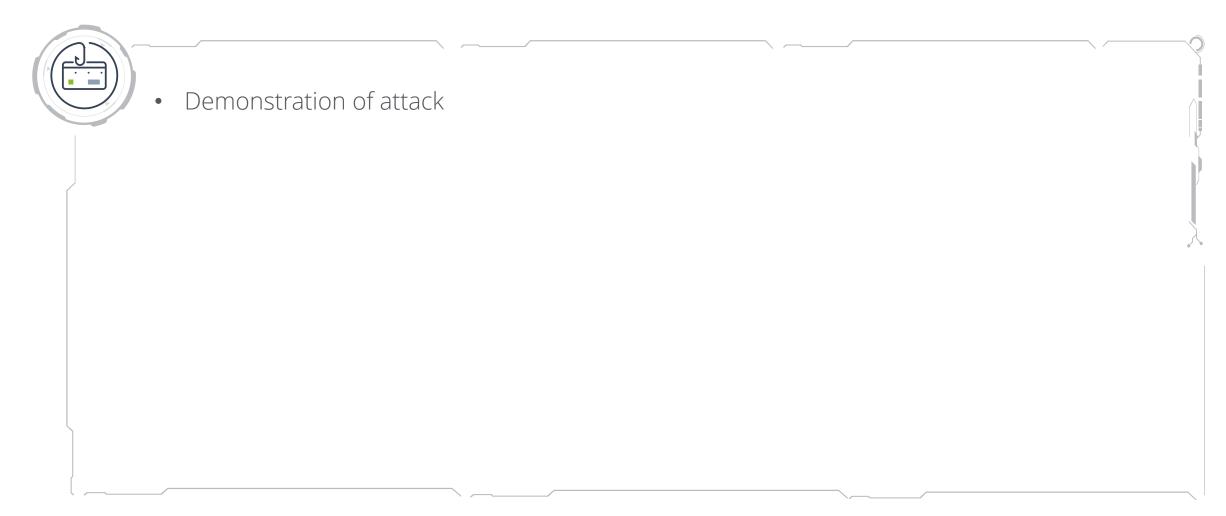
### Remote code execution (RCE)—binary planting



- Many applications load various libraries (dynamic link library's [DLL] on Windows) at startup
- DLL search path is a complicated topic dependent on various settings, but often includes the current directory
- If a DLL isn't a standard system DLL the current directory may be checked for it

- When a program is started by doubleclicking a file in explorer, current directory is the same as the file
- If a website has been granted folder write access via file access API, it can write a
- Many of these bugs were released in 2010, referencing file shares especially
- Same concept applies to other commands a program executes

# **RCE**—sleight of hand



### RCE—sleight of hand explanation



#### Normal download flow

- User opens site
- User clicks to download a small script to run
- Save prompt for file with name
- User examines file— SmartScreen checks
- User runs file



#### Attack

- Users opens site
- User clicks to download a small script to run
- Save prompt for file without name
- User examines file— SmartScreen checks
- User runs file
- Page edits file
- Modified commands run

## RCE—sleight of hand explanation



#### Normal download flow

- Site can only suggest extension
- Website only has write access once



#### Attack

- Site can force extension
- Website can re-access file
  - o Re-access requires whole file lock and replacement
  - o Execution types that maintain handles are generally not vulnerable

### **Forensic artifacts**



- Browser cache and other forensics
- Timelines
- Modification attack
  - o Watch for file creation/modification dates
  - o Deleted temporary file entries may still exist in MFT

### Mitigation suggestions



#### User level

- Understanding the new permissions
- Signs to look for—specifying full name
- Actions to avoid downloading without
- Close your tab before touching files



#### **Browser level**

- Blocking script files
- Lock file for entire duration of potential access
- Add user approval prompt for R/W access
- Visual indication for ongoing access, similar to camera/ microphone

# Deloitte.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Product names mentioned in this document are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Inclusion does not constitute an endorsement of the product and/or service.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see <a href="https://www.deloitte.com/us/about">www.deloitte.com/us/about</a> for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.