SANS ISC: How the "Contact Forms" campaign tricks people - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training SANS ISC InfoSec Forums

isc.sans.edu/forums/diary/How+the+Contact+Forms+campaign+tricks+people/28142/

How the "Contact Forms" campaign tricks people

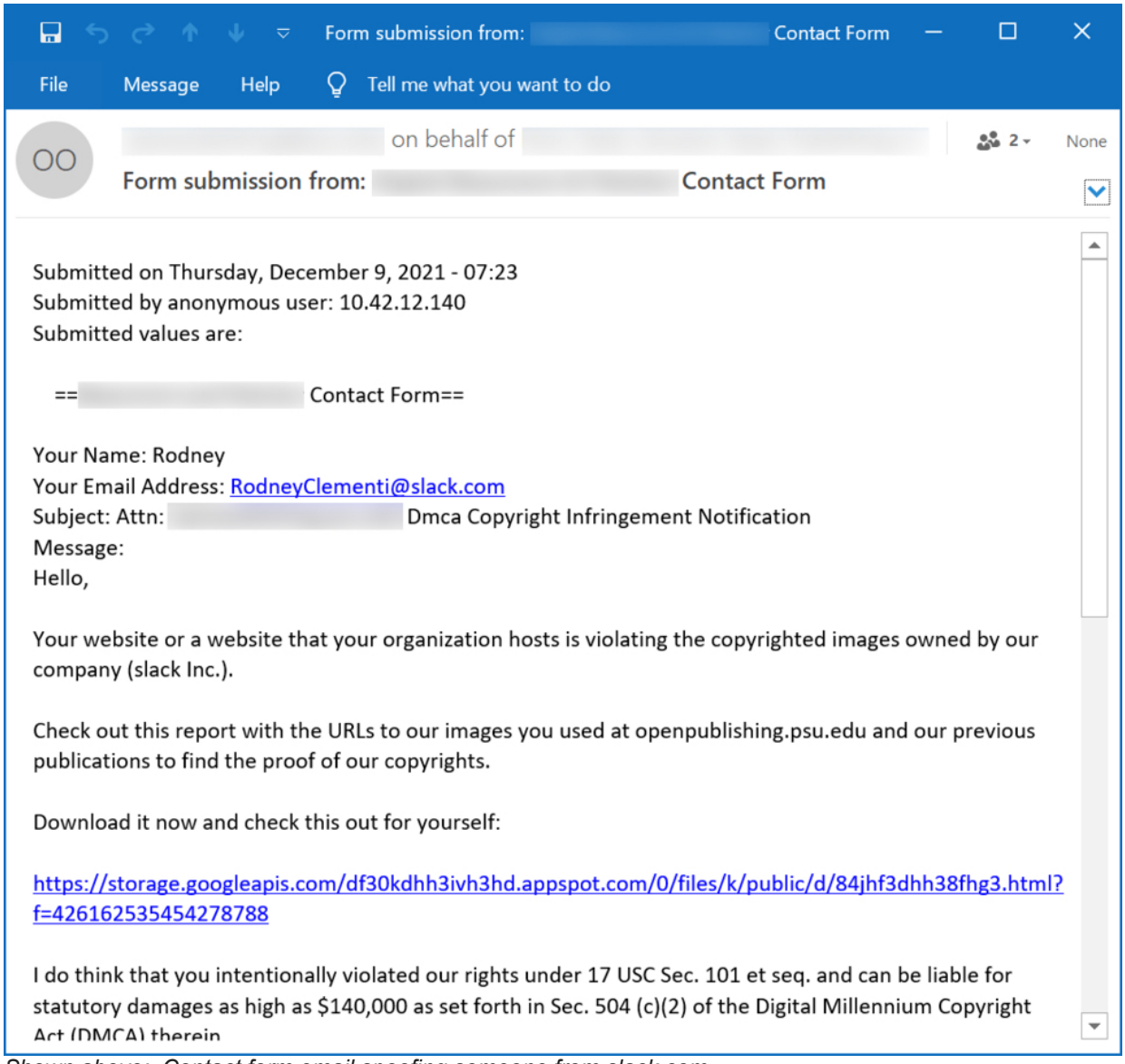
Brad

433 Posts
ISC Handler
Dec 16th 2021

Introduction

This diary is based on an infection I started on Monday 2021-12-13 at 21:45 UTC that ran until Tuesday 2021-12-14 at 17:17 UTC. The infection generated traffic for IcedID (Bokbot), DarkVNC, and Cobalt Strike. A pcap of the network traffic and the associated malware samples are available here.

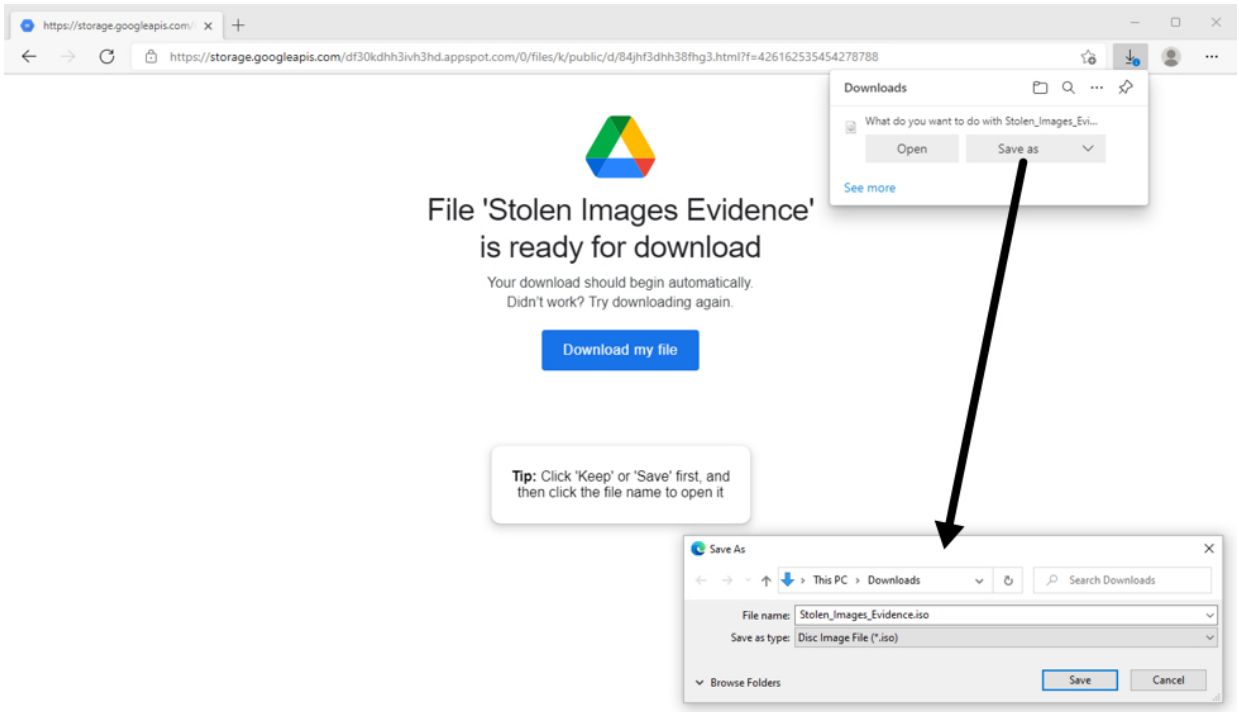
"Contact Forms" is a campaign that uses a web site's contact form to email malicious links disguised as some sort of legal complaint. We've seen this campaign push BazarLoader malware and distribute Sliver, but recently it's been pushing IcedID (Bokbot). Most of the time, the Contact Forms campaign uses a "Stolen Images Evidence" theme, with emails stating a supposed violation of the Digital Millennium Copyright Act (DMCA). Below is an example seen on December 9th, 2021.



Shown above: Contact form email spoofing someone from slack.com.

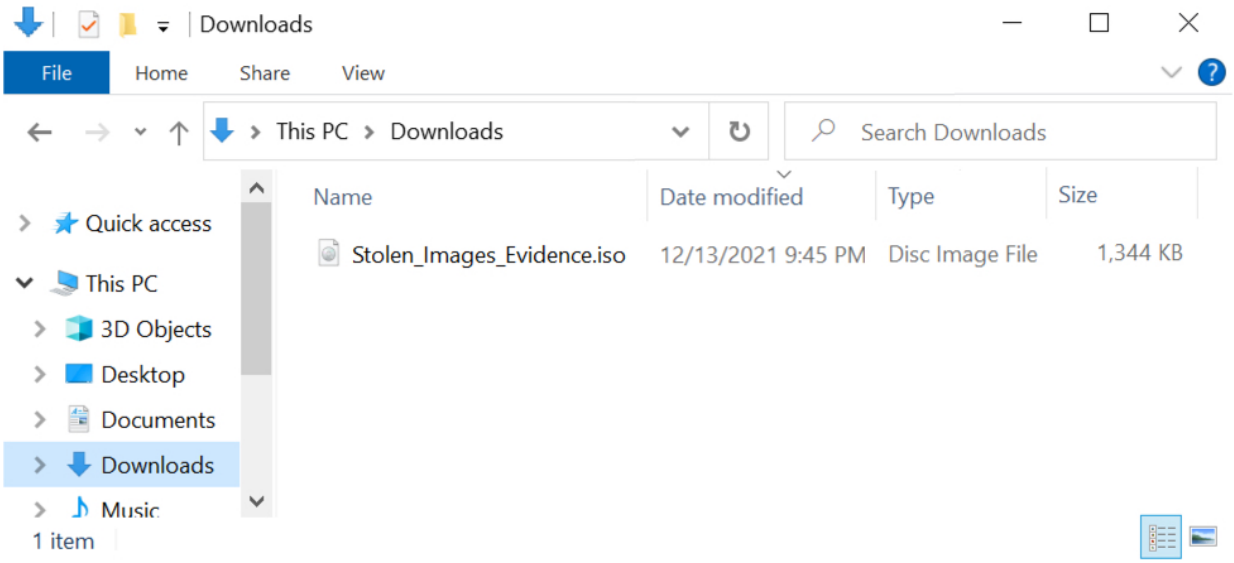
A website's contact form is easy method for cyber criminals to reach an organization. They can enter any name, email, and message text in these forms to deliver. With anonymous browsing methods like tor or VPN, criminals can hide their true location when filling out these forms.

In this case, the link is a googleapis URL that abuses Google services to distribute malware. I checked the link in a web browser, and it was a "Stolen Images Evidence" themed web page. The page automatically presented an ISO file named ***Stolen_Images_Evidence.iso***.



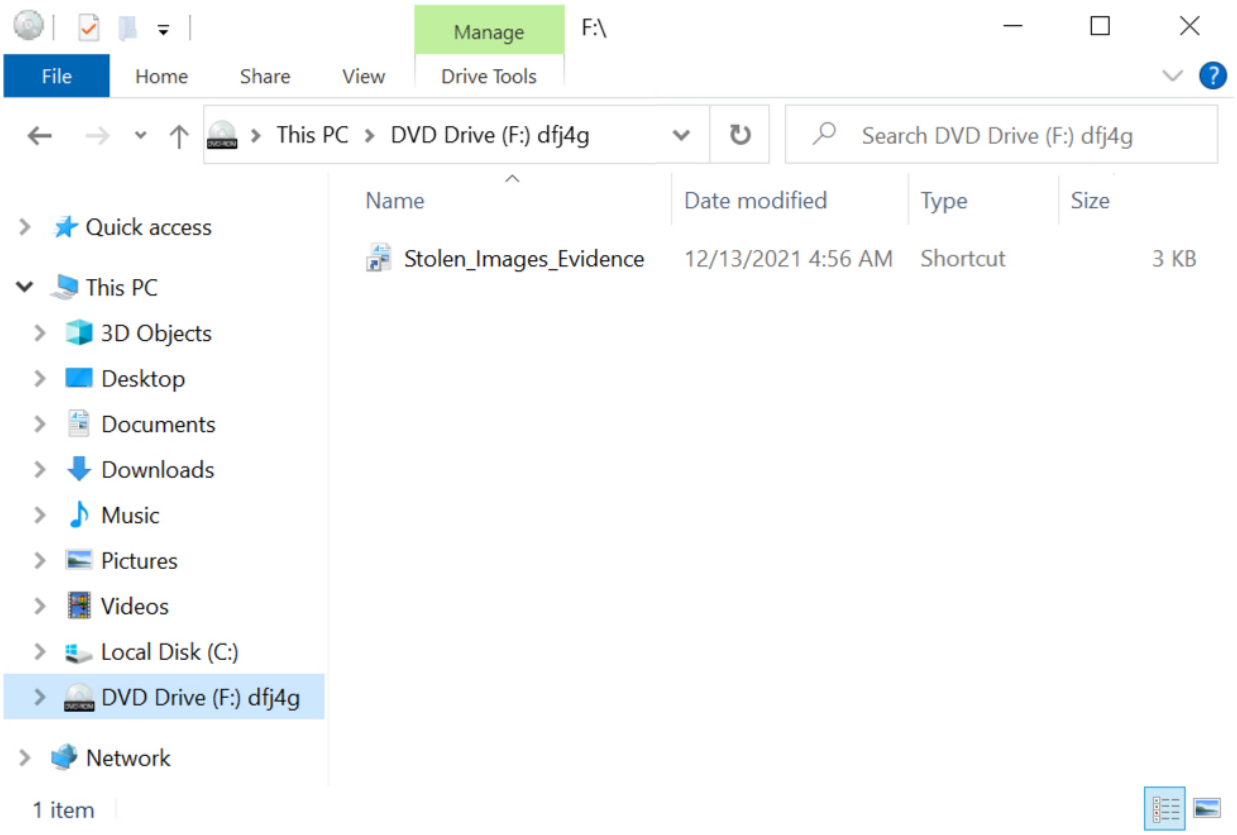
Shown above: "Stolen Images Evidence" page sending an ISO file.

ISO files have been used by cyber criminals for years, and the Contact Forms campaign started consistently delivering ISO files from these pages as early as November 30th, 2021. Prior to that, this campaign almost always sent zip archives.



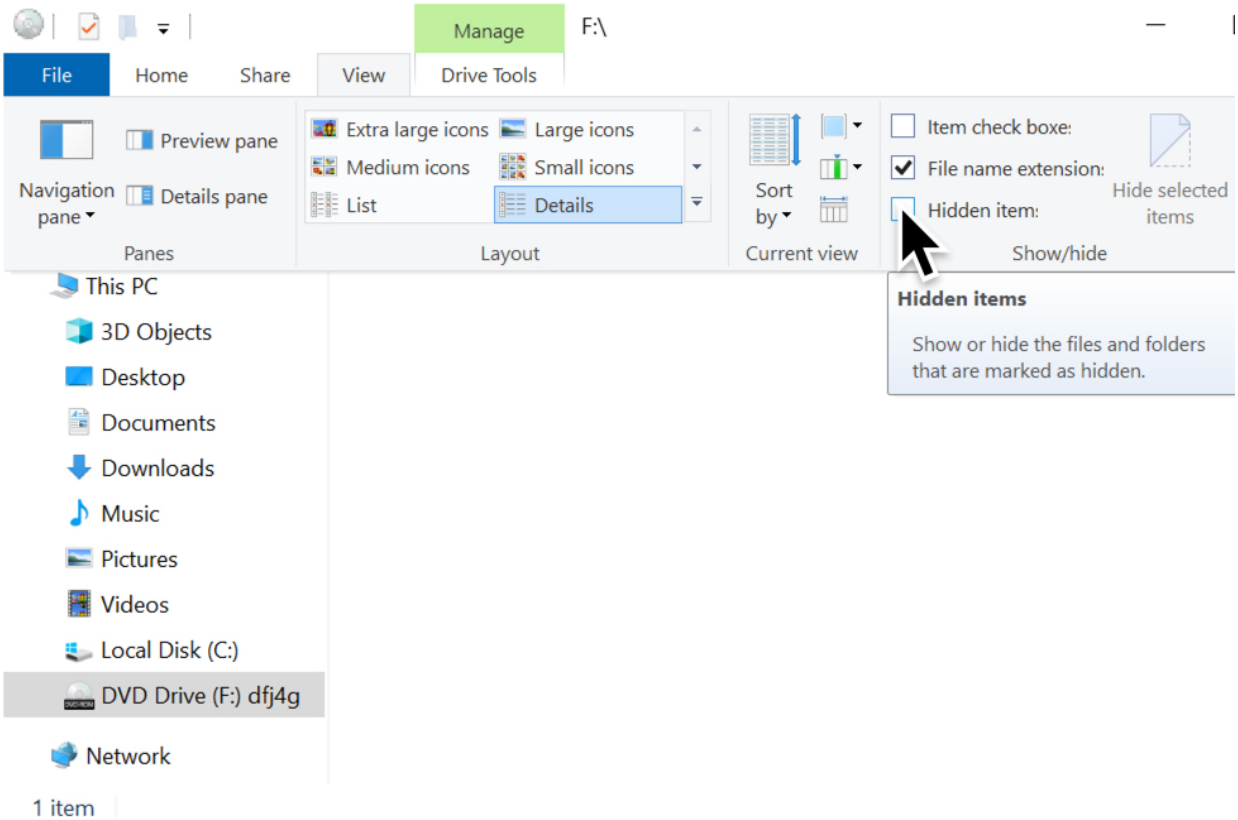
Shown above: Stolen_Images_Evidence.iso downloaded on 2021-12-13.

Double-clicking an ISO file on a Windows host will mount the file as a drive, then it will open Windows Explorer to view its contents. In this example, the double-clicked ISO file appears at ***F:*** as a DVD drive, and it contains a Windows shortcut.



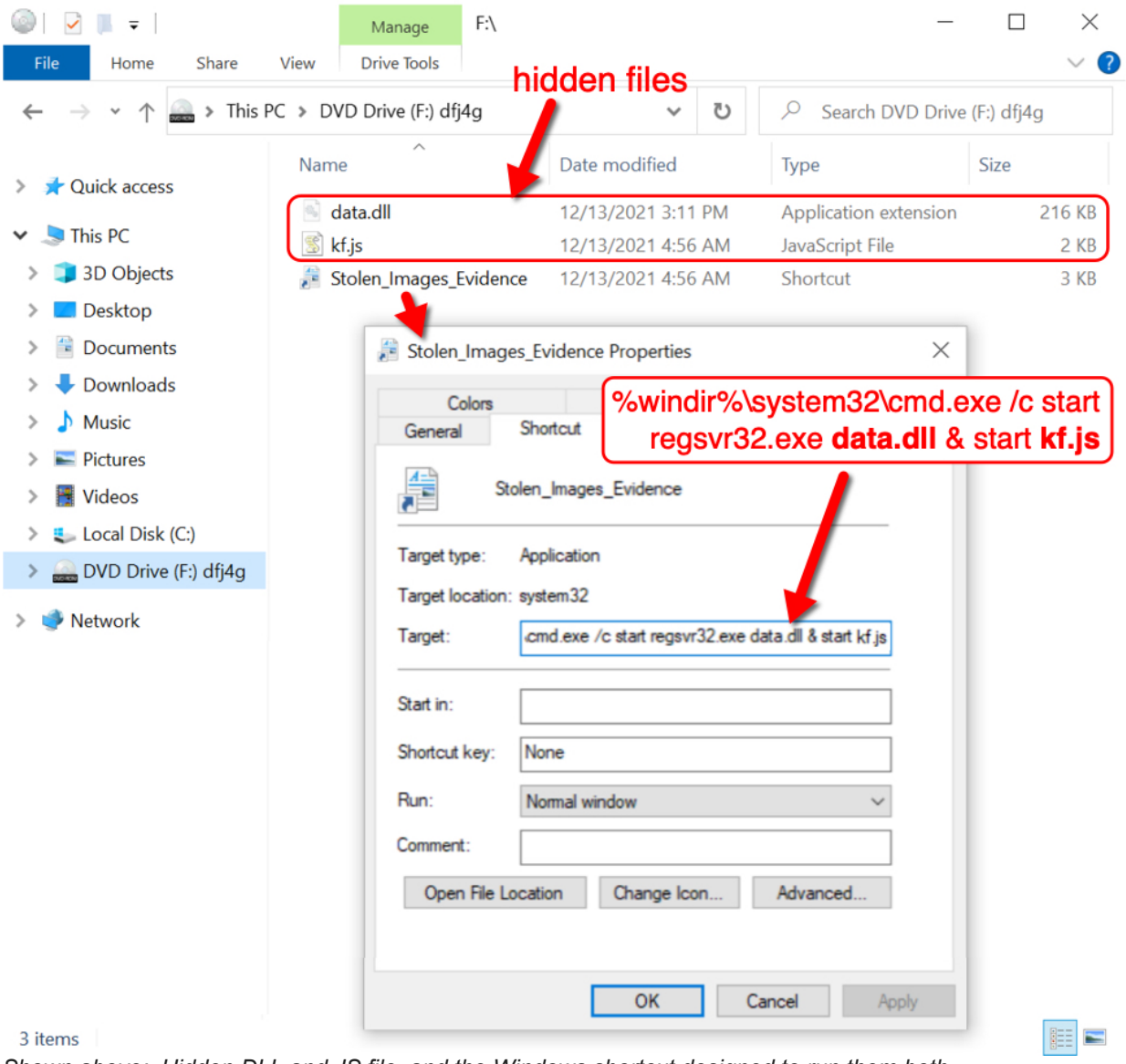
Shown above: Windows Explorer shows the ISO file mounted as a DVD drive at F:\.

By default, Windows Explorer does not show hidden files, so we should reveal hidden files from the Explorer menu.



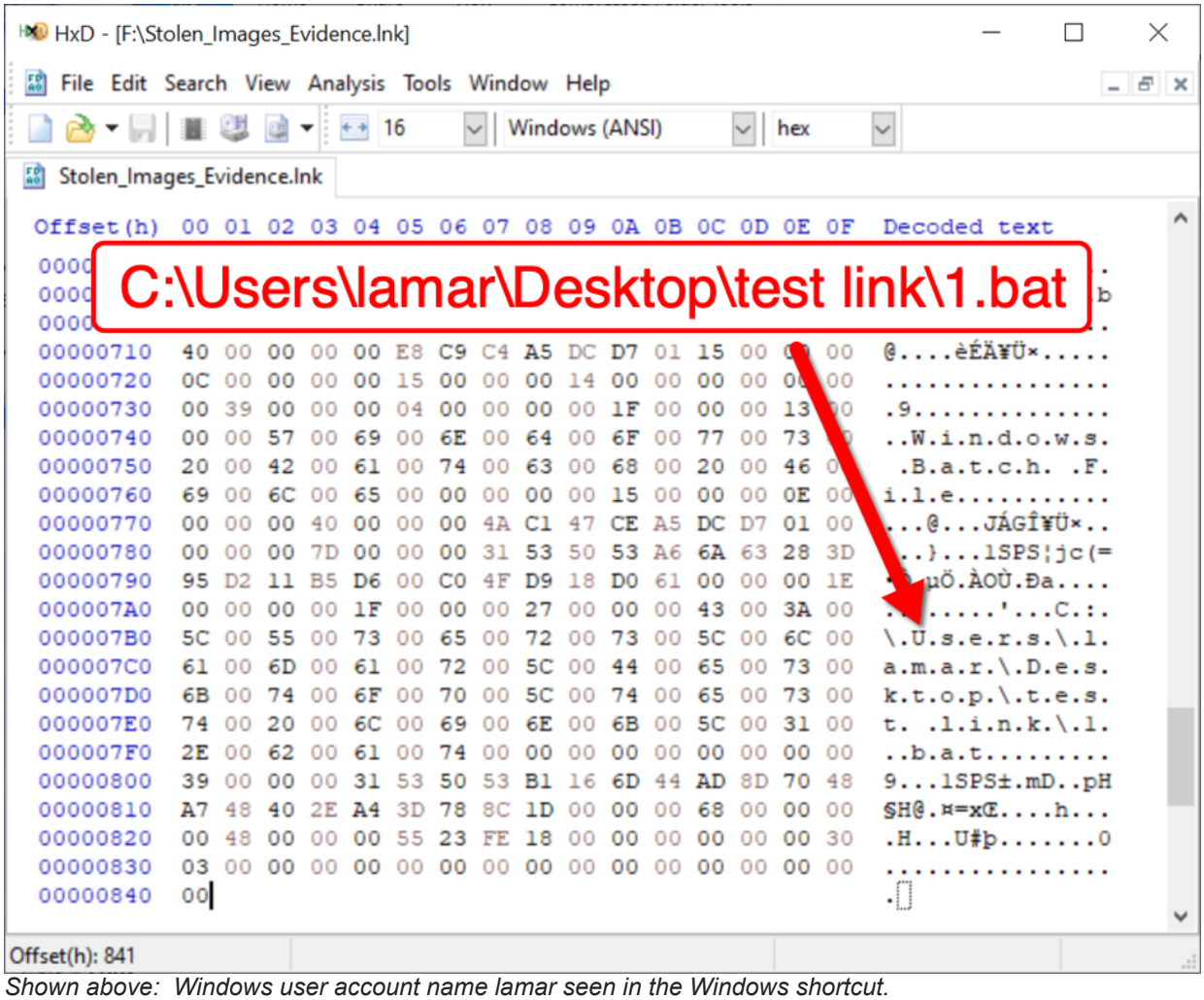
Shown above: Revealing hidden items in Windows Explorer.

Revealing hidden files, we find a DLL and a JavaScript (.js) file hiding in the ISO. The Windows shortcut runs both files. It runs the DLL using ***regsvr32.exe***, and it also runs the ***.js*** file separately.



Shown above: Hidden DLL and JS file, and the Windows shortcut designed to run them both.

Examining the Windows shortcut in a hex editor, we find a Windows user account named ***lamar*** that may have been used when creating the shortcut.



Shown above: Windows user account name lamar seen in the Windows shortcut.

The account name ***lamar*** has been consistent in each shortcut I've examined from these ISO files since they started appearing from the Contact Forms campaign on 2021-11-30.

Indicators of Compromise (IOCs)

The following are IOCs are from an infection run I started on Monday 2021-12-13 at 21:45 UTC that ran until Tuesday 2021-12-14 at 17:17 UTC.

URL for the "Stolen Images Evidence" page:

> hxxps://storage.googleapis[.]com/d03uhg49h1m5na.appspot.com/0/files/st/public/d/0390vfh478gj4.html?d=958418188474764759

Domain called by above googleapis page:

> 172.67.195[.]237 port 443 - ***maruadix[.]top*** - HTTPS traffic

Traffic generated after double clicking Windows shortcut in downloaded ISO file:

Caused by the .js file:

> 104.21.68[.]138 port 80 - ***maruadix[.]top*** - GET /stis1.php

Caused by the DLL (an installer for IcedID):

- port 443 - ***aws.amazon.com*** - HTTPS traffic (not inherently malicious)
- 192.236.177[.]53 port 80 - ***hdgravity[.]com*** - GET /

IcedID (Bokbot) post-infection traffic:

194.180.174[.]136 port 443 - ***asrspoe[.]com*** - HTTPS traffic

DarkVNC activity starting on 2021-12-13 at 23:33 UTC:

88.119.161[.]88 port 8080 - encoded/encrypted TCP traffic

Cobalt Strike activity starting on 2021-12-14 at 06:30 UTC and ending at 11:55 UTC:

- 149.91.89[.]17 port 80 - ***149.91.89[.]17*** - GET /soft/musicbee.dll
- 104.41.145[.]218 port 443 - ***api.musicbee.getlist.destinycraftpe[.]com*** - HTTPS traffic

Cobalt Strike activity starting on 2021-12-14 at 15:33 UTC and continued through the end of the pcap at 17:17 UTC:

- 192.34.109[.]104 port 80 - ***192.34.109[.]104*** - GET /download/HI1FA3OB3N7D9.dll
- 192.34.109[.]104 port 443 - ***bqtconsulting[.]com*** - HTTPS traffic

SHA256 hash: 0e1fa8cc5697d60664e9bf5fb4ef6af14d63d7f31f0b1565e0ff0e7ce86af735

- File size: 1,376,256 bytes
- File name: Stolen_Images_Evidence.iso
- File description: ISO file downloaded from googleapis page.

SHA256 hash: 5b2751fa6c0c93f8f625375a87c8f235d7b61eb9941633f59cf2ec18352f915a

- File size: 2,113 bytes
- File name: Stolen_Images_Evidence.lnk
- File description: Windows shortcut contained in ISO

SHA256 hash: c7d3cabf68151b9207d6262f3fd739f70f18a736a5a8d04479150f08448bd7bf

- File size: 1,164 bytes
- File name: kf.js
- File description: JS file contained in ISO
- Analysis: https://tria.ge/211216-ecnb5sbbe2

SHA256 hash: b71f914f40d146462cafac5f360f816d59366be377268b33d0d4688917950223

- File size: 221,184 bytes
- File name: data.dll
- File description: installer DLL for IcedID contained in ISO
- Run method: regsvr32.exe *[filename]*
- Analysis: https://tria.ge/211216-ebwbcsbbd7

SHA256 hash: 0cc2afa847096e322c014f04f54b405902ce2613c555fb6b36fc4f93d53ba2a5

- File size: 497,278 bytes
- File location: hxxp://hdgravity[.]com/
- File description: binary of gzip compressed data retrieved by IcedID installer DLL
- File type: gzip compressed data, was "Artwork.txt", from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 2063440

SHA256 hash: cfc202b44509f2f607d365858a8218dfdc6b26f8087efcc5e46f4fef9ab53705

- File size: 341,898 bytes
- File location: C:\Users*[username]*\AppData\Roaming\TrueLend\license.dat
- File description: data binary used to run persistent IcedID DLL

SHA256 hash: 4fbf01e80561ac1528b50e3a49b7b7bf8139decf62c3653672a545cfec7deee5

- File size: 154,624 bytes
- File location: C:\Users*[username]*\AppData\Local\ukudhe3\ojfepp.dll
- File description: IcedID DLL persistent through scheduled task
- Run method: rundll32.exe *[filename]*,DllMain --fi="*[path to license.dat]*"
- Analysis: https://tria.ge/211216-d9t1hsbhcm

SHA256 hash: fba9dd0ebb8d838fa394cda10dca50450d8c0fc6158deff38904072140d64507

- File size: 154,624 bytes
- File location: hxxp://149.91.89[.]17/soft/musicbee.dll
- File location: C:\Users*[username]*\AppData\Local\Temp\oben32.dll
- File description: 64-bit DLL for Cobalt Strike retrieved by IcedID-infected host
- Run method: regsvr32.exe *[filename]*
- Analysis: https://tria.ge/211214-q5xl3afgf6

SHA256 hash: f9c4a119234df78e1ad71b10fb0bf18622fd5245b72b93e5b71992f20cb9fd2e

- File size: 413,696 bytes
- File location: hxxp://192.34.109[.]104/download/HI1FA3OB3N7D9.dll
- File location: C:\Users*[username]*\AppData\Local\Temp\Ihopot2.dll
- File description: another 64-bit DLL for Cobalt Strike retrieved by IcedID-infected host
- Run method: rundll32.exe *[filename],[unknown entry point]*
- Analysis: https://tria.ge/211214-vw9mgsgbe3

Final words

This and similar IcedID infections have led to Cobalt Strike, which can lead to other malicious activity like ransomware as reported in this real-world example.

A pcap of the network traffic and the associated malware from this infection are available here.

Brad Duncan
brad [at] malware-traffic-analysis.net