IcedID Botnet Distributors Abuse Google PPC to Distribute Malware

trendmicro.com/en_ie/research/22/l/icedid-botnet-distributors-abuse-google-ppc-to-distribute-malware.html

23 December 2022

Content added to Folio

Malware

We analyze the latest changes in IcedID botnet from a campaign that abuses Google pay per click (PPC) ads to distribute IcedID via malvertising attacks.

By: Ian Kenefick December 23, 2022 Read time: (words)

After closely tracking the activities of the IcedID botnet, we have discovered some significant changes in its distribution methods. Since December 2022, we observed the abuse of Google pay per click (PPC) ads to distribute IcedID via malvertising attacks. This IcedID variant is detected by Trend Micro as TrojanSpy.Win64.ICEDID.SMYXCLGZ.

Advertising platforms like Google Ads enable businesses to display advertisements to target audiences for the purpose of boosting traffic and increasing sales. Malware distributors abuse the same functionality in a technique known as malvertising, wherein chosen keywords are hijacked to display malicious ads that lure unsuspecting search engine users to downloading malware.

In our investigation, malicious actors used malvertising to distribute the IcedID malware via cloned webpages of legitimate organizations and well-known applications. Recently, the Federal Bureau of Investigation (FBI) published a warning pertaining to how cybercriminals abuse search engine advertisement services to imitate legitimate brands and direct users to malicious sites for financial gain.

Our blog entry provides the technical details of IcedID botnet's new distribution method and the new loader it uses.

Technical analysis

Organic search results are those generated by the Google PageRank algorithm, whereas Google Ads appear in more prominent locations above, beside, below, or with the organic search results. When these ads are hijacked by malicious actors via malvertising, they can lead users to malicious websites.

Targeted brands and applications

In our investigation, we discovered that IcedID distributors hijacked the keywords used by these brands and applications to display malicious ads:

1. Adobe – A computer software company
2. AnyDesk - A remote control application
3. Brave Browser - A web browser
4. Chase Bank - A banking application
5. Discord - An instant messenger service
6. Fortinet - A security company
7. GoTo - A remote control application
8. Libre Office - An open-source alternative to Microsoft Office
9. OBS Project - A streaming application
10. Ring - A home CCTV (closed-circuit) manufacturer
11. Sandboxie - A virtualization/sandbox application
12. Slack - An instant messaging application
13. Teamviewer - A remote control application
14. Thunderbird - An email client
15. US Internal Revenue Service (IRS) – A US federal government body

The malicious websites where victims are directed are made to look like their legitimate counterparts. Figure 1 shows a legitimate-looking malicious Slack webpage used by IcedID distributors to lure victims into downloading malware.

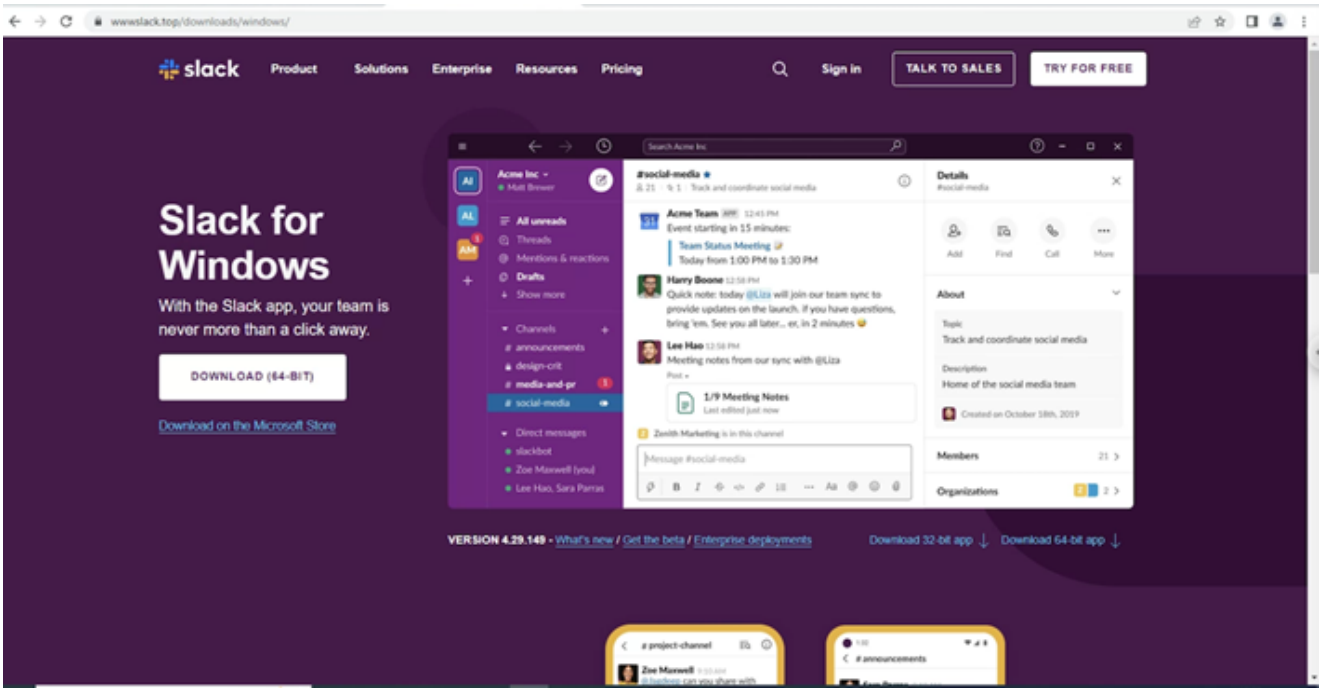


Figure 1. A legitimate-looking malicious Slack webpage used by IcedID distributors
Infection chain

The overall infection flow involves delivering the initial loader, fetching the bot core, and ultimately, dropping the payload. The payload is typically a backdoor.

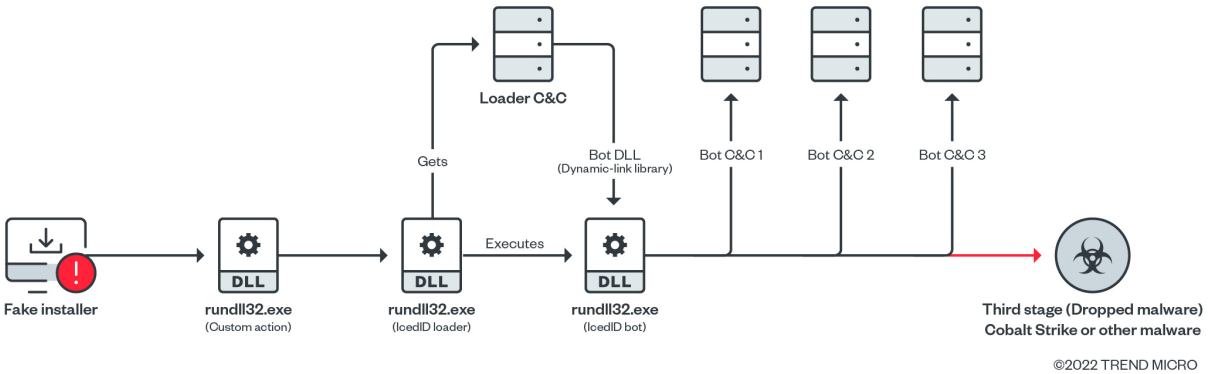
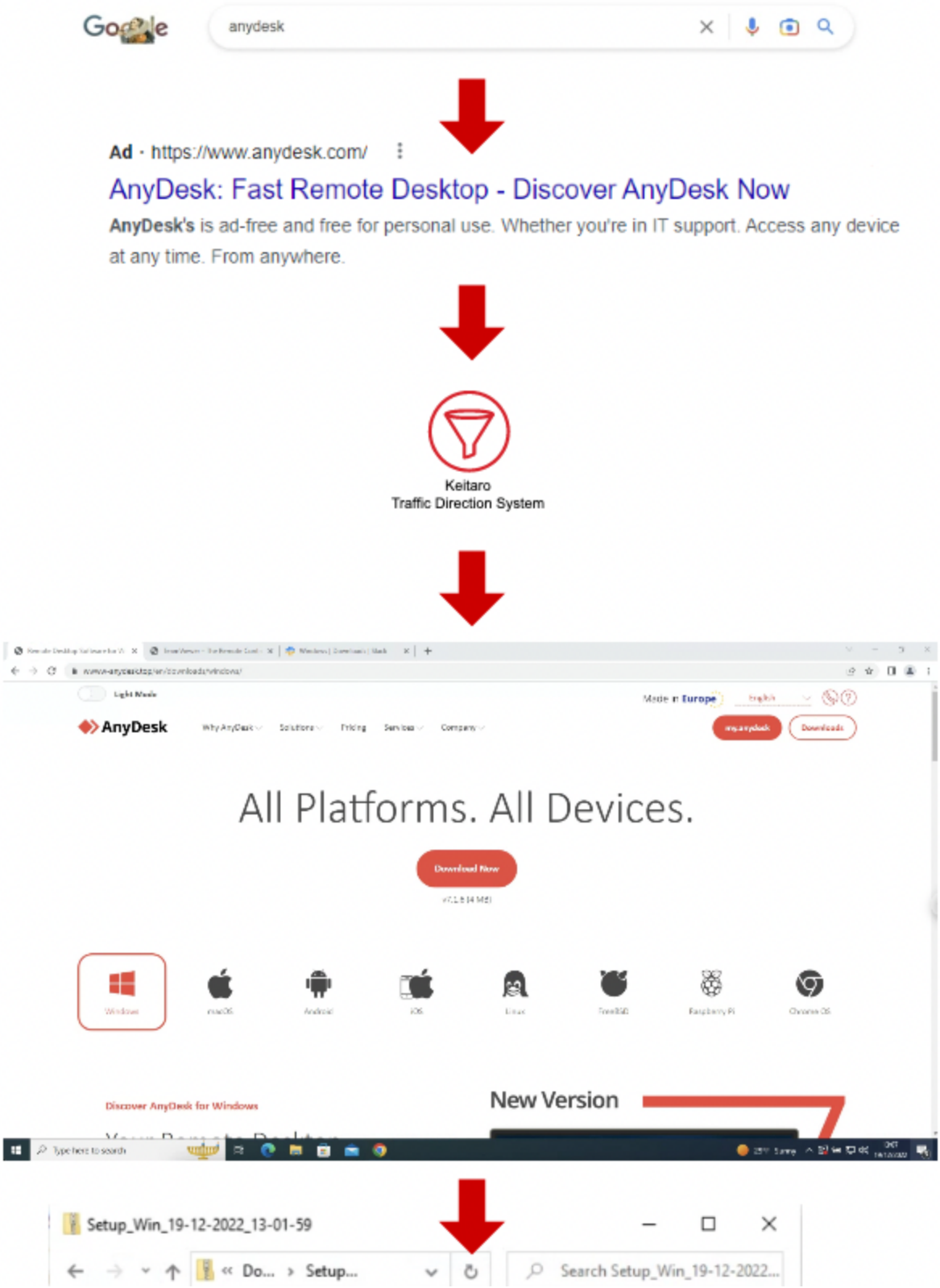


Figure 2. IcedID botnet malware infection chain

Infection via malvertising

1. A user searches for an application by entering a search term on Google. In this particular example, the user wants to download the AnyDesk application and enters the search term “AnyDesk” on the Google search bar.
2. A malicious ad for the AnyDesk application that leads to a malicious website is displayed above the organic search results.

3. IcedID actors abuse the legitimate Keitaro Traffic Direction System (TDS), to filter researcher and sandbox traffic. The victim is then redirected to a malicious website.
4. Once the user selects the “Download” button, it downloads a malicious Microsoft Software Installer (MSI) or Windows Installer file inside a ZIP file in the user’s system.



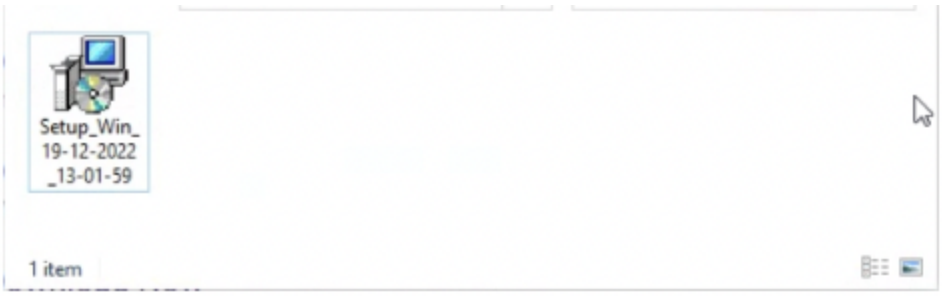


Figure 3. IcedID botnet malvertising infection chain

The new IcedID botnet loader

In this campaign, the loader is dropped via an MSI file, which is atypical for IcedID.

The installer drops several files and invokes the “init” export function via rundll32.exe, which then executes the malicious loader routine.

This “loader” DLL has the following characteristics:

- The authors have taken a legitimate DLL and replaced a single legitimate function with the malicious loader function using the “init” export function name at the last ordinal.
- The first character of each legitimate export function in the IcedID loader is replaced with the letter “h.”
- The reference to the malicious function is a patched legitimate function.

The resulting malicious file is almost identical to the legitimate version. This can prove to be challenging for machine learning (ML) detection solutions.

On the surface, the malicious IcedID and legitimate sqlite3.dll files look almost identical. Figure 4 shows a side-by-side comparison of these files using the PortEx Analyzer tool, which was developed by security researcher Karsten Hahn. The tool allows us to quickly visualize the structure of the portable executable (PE) files, and, in this case, assess the similarity of files.

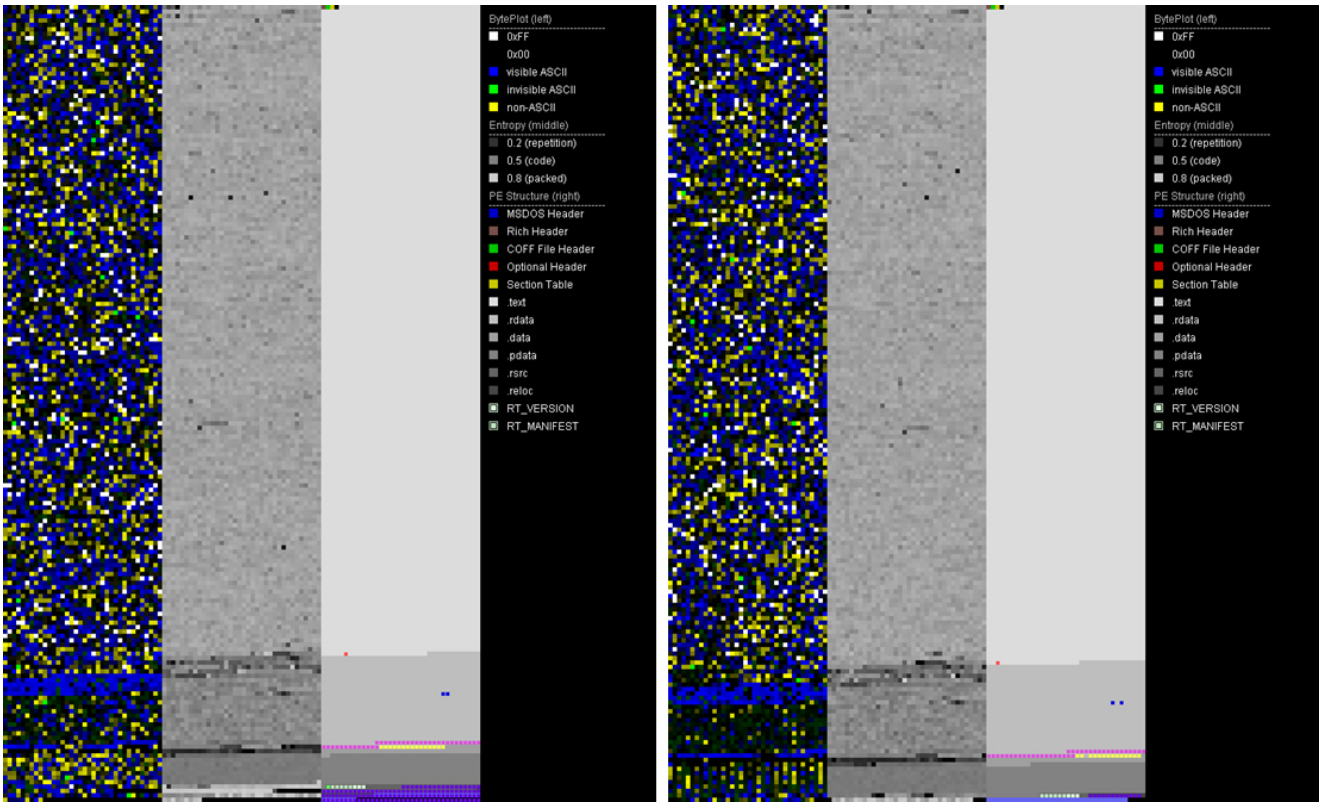


Figure 4. A visual representation of the malicious IcedID (left) and legitimate PE (right) files (using Karsten Hahn's PortEx Analyzer tool)

For this reason, we hypothesize that this is an attack on two types of malware detection technologies:

- Machine learning detection engines
- Whitelisting systems

Tampered DLL files functioning as IcedID loaders

We have observed that some of the files that have been modified to act as IcedID loaders are well-known and widely used libraries.

Table 1. Files that have been modified to act as IcedID loaders

DLL name	Description
tcl86.dll	A library component of ActiveState's TCL (Tool Command Language) Programming Language Interpreter
sqlite3.dll	A library component of SQLite database
ConEmuTh.x64.dll	A plugin for Far Manager
libcurl.dll	A CURL library

In sqlite3.dll, we observed that the function at ordinal 270 “sqlite3_win32_write_debug” has been replaced with the malicious “init” function in the IcedID loader.

This is the case across the modified DLL files listed above: The export function at the last ordinal is replaced with the malicious “init” function.

Name	Address	Ordinal
hqlite3_value_numeric_type	000000018003EBA0	257
hqlite3_value_pointer	000000018003A560	238
hqlite3_value_subtype	000000018003A550	239
hqlite3_value_text	000000018003A5B0	240
hqlite3_value_text16	000000018003A5F0	241
hqlite3_value_text16be	000000018003A630	242
hqlite3_value_text16le	000000018003A670	243
hqlite3_value_type	000000018003A6B0	244
hqlite3_version	0000000180134788	245
hqlite3_vfs_find	0000000180004B80	246
hqlite3_vfs_register	0000000180004C90	247
hqlite3_vfs_unregister	0000000180004D70	248
hqlite3_vmprintf	0000000180008DD0	249
hqlite3_vsnprintf	0000000180008EE0	250
hqlite3_vtab_collation	00000001800B2370	251
hqlite3_vtab_config	00000001800A4D30	252
hqlite3_vtab_nochange	000000018003C0D0	253
hqlite3_vtab_on_conflict	00000001800A4D10	254
hqlite3_wal_autocheckpoint	00000001800C6E70	255
hqlite3_wal_checkpoint	00000001800C70A0	256
hqlite3_wal_checkpoint_v2	00000001800C6F70	257
hqlite3_wal_hook	00000001800C6F00	258
hqlite3_win32_is_nt	000000018000C720	259
hqlite3_win32_mbcs_to_utf8	000000018000CD00	260
hqlite3_win32_mbcs_to_utf8_v2	000000018000CD30	261
hqlite3_win32_set_directory	000000018000CFD0	262
hqlite3_win32_set_directory16	000000018000CEF0	263
hqlite3_win32_set_directory8	000000018000CDE0	264
hqlite3_win32_sleep	**000000018000C6D0**	**265**
hqlite3_win32_unicode_to_utf8	000000018000CCD0	266
hqlite3_win32_utf8_to_mbcs	000000018000CD70	267
hqlite3_win32_utf8_to_mbcs_v2	000000018000CDA0	268
hqlite3_win32_utf8_to_unicode	000000018000CCA0	269
init	000000018012AB40	270
DllEntryPoint	**000000018012C134**	**[main entry]**

Name	Address	Ordinal
sqlite3_value_numeric_type	000000018003EBA0	257
sqlite3_value_pointer	000000018003A560	238
sqlite3_value_subtype	000000018003A550	239
sqlite3_value_text	000000018003A5B0	240
sqlite3_value_text16	000000018003A5F0	241
sqlite3_value_text16be	000000018003A630	242
sqlite3_value_text16le	000000018003A670	243
sqlite3_value_type	000000018003A6B0	244
sqlite3_version	0000000180134788	245
sqlite3_vfs_find	0000000180004B80	246
sqlite3_vfs_register	0000000180004C90	247
sqlite3_vfs_unregister	0000000180004D70	248
sqlite3_vmprintf	0000000180008DD0	249
sqlite3_vsnprintf	0000000180008EE0	250
sqlite3_vtab_collation	00000001800B2370	251
sqlite3_vtab_config	00000001800A4D30	252
sqlite3_vtab_nochange	000000018003C0D0	253
sqlite3_vtab_on_conflict	00000001800A4D10	254
sqlite3_wal_autocheckpoint	00000001800C6E70	255
sqlite3_wal_checkpoint	00000001800C70A0	256
sqlite3_wal_checkpoint_v2	00000001800C6F70	257
sqlite3_wal_hook	00000001800C6F00	258
sqlite3_win32_is_nt	000000018000C720	259
sqlite3_win32_mbcs_to_utf8	000000018000CD00	260
sqlite3_win32_mbcs_to_utf8_v2	000000018000CD30	261
sqlite3_win32_set_directory	000000018000CFD0	262
sqlite3_win32_set_directory16	000000018000CEF0	263
sqlite3_win32_set_directory8	000000018000CDE0	264
sqlite3_win32_sleep	**000000018000C6D0**	**265**
sqlite3_win32_unicode_to_utf8	000000018000CCD0	266
sqlite3_win32_utf8_to_mbcs	000000018000CD70	267
sqlite3_win32_utf8_to_mbcs_v2	000000018000CDA0	268
sqlite3_win32_utf8_to_unicode	000000018000CCA0	269
sqlite3_win32_write_debug	000000018000C640	270
DllEntryPoint	**000000018012C134**	**[main entry]**

Figure 5. A comparison of IcedID-modified (left) and normal (right) files, wherein the former’s export function at the last ordinal is replaced with the malicious “init” function

Further investigation shows that the structure of the file is identical.

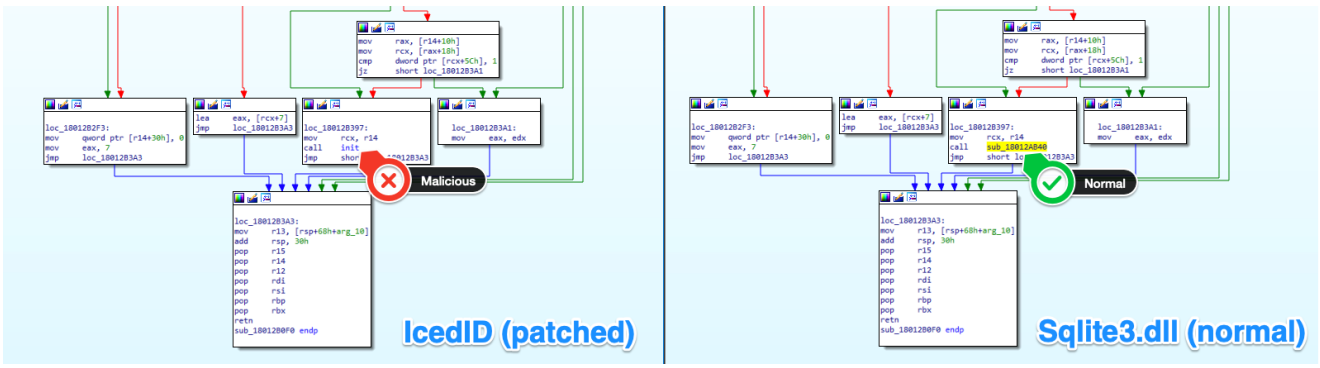


Figure 6. A comparison of IcedID-modified and normal files wherein both files show an identical structure

Execution

1. “MsiExec.exe” executes (parent process) (MITRE ID T1218.007 - System Binary Proxy Execution: msiexec)
2. “rundll32.exe” is spawned (MITRE ID T1218.011 - System Binary Proxy Execution: rundll32.exe)

3. “rundll32.exe” runs the custom action “Z3z1Z” via “zzzzInvokeManagedCustomActionOutOfProc” (MITRE ID T1218.011 - System Binary Proxy Execution: rundll32.exe)
4. The custom action spawns a second “rundll32.exe” to run the IcedID loader “MSI3480c3c1.msi” with the “init” export function (MITRE IDs T1027.009 - Embedded Payloads and T1218.011 - System Binary Proxy Execution: rundll32.exe)

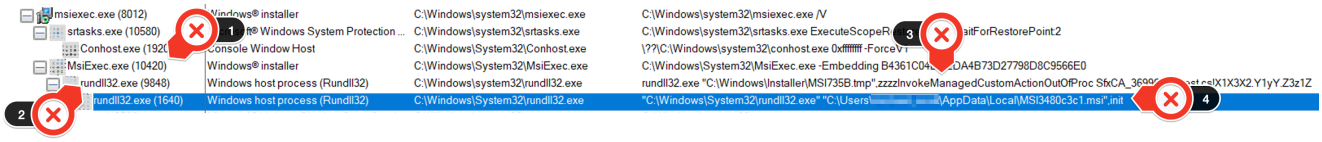


Figure 7. IcedID loader execution chain

Tables	Action	Type	Source	Target
AdminExecuteSequence	Z3z1Z	65	Z3z1Z_File	Z3z1Z
AdminUISequence				
AdvtExecuteSequence				
Binary				
Component				
CreateFolder				
CustomAction				

Figure 8. MSI custom action

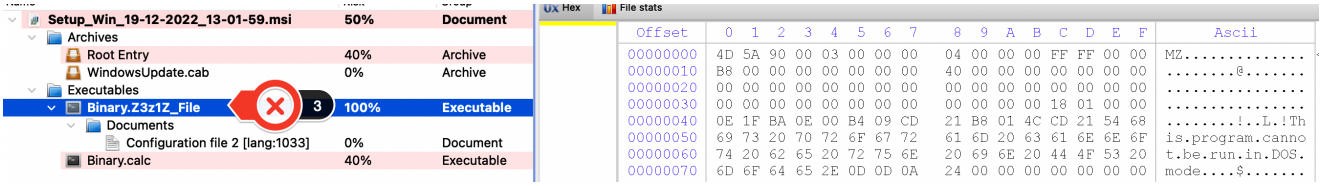


Figure 9. MSI structure that contains the custom action

Conclusion

IcedID is a noteworthy malware family that is capable of delivering other payloads, including Cobalt Strike and other malware. IcedID enables attackers to perform highly impactful follow through attacks that lead to total system compromise, such as data theft and crippling ransomware. The use of malvertising and an evasive loader is a reminder of why it’s important for businesses to deploy layered security solutions that include custom sandboxing, predictive machine learning, behavior monitoring and file and web reputation detection capabilities. Users can also consider the use of ad blockers to help thwart malveritising attacks.

Indicators Of Compromise (IOCs)

The indicators of compromise can be accessed via this text file.

Mitre ATT&CK

ID	Name	Description
T1218.007	System Binary Proxy Execution msiexec	IcedID is delivered via an MSIEXEC package which execute a malicious custom action to deploy the IceID Loader
T1218.011	System Binary Proxy Execution rundll32.exe	The malicious custom action invokes rundll32.exe to execute the IceID Loader
T1027.009	Embedded Payloads	Attackers embed a malicious function in an otherwise benign DLL in order to thwart detection technologies

sXpIBdPeKzl9PC2p0SWMpUSM2NSxWzPyXTMLlbXmYa0R20xk