Magniber ransomware actors used a variant of Microsoft SmartScreen bypass

blog.google/threat-analysis-group/magniber-ransomware-actors-used-a-variant-of-microsoft-smartscreen-bypass/

Benoit Sevens March 14, 2023

Threat Analysis Group

Google's Threat Analysis Group (TAG) recently discovered usage of an unpatched security bypass in Microsoft's SmartScreen security feature, which financially motivated actors are using to deliver the Magniber ransomware without any security warnings. The attackers are delivering MSI files signed with an invalid but specially crafted Authenticode signature. The malformed signature causes SmartScreen to return an error that results in bypassing the security warning dialog displayed to users when an untrusted file contains a Mark-of-the-Web (MotW), which indicates a potentially malicious file has been downloaded from the internet.

TAG reported its findings to Microsoft on February 15, 2023. The security bypass was patched today as CVE-2023-24880 in Microsoft's Patch Tuesday release.

TAG has observed over 100,000 downloads of the malicious MSI files since January 2023, with over 80% to users in Europe — a notable divergence from Magniber's typical targeting, which usually focuses on South Korea and Taiwan. Google Safe Browsing displayed user warnings for over 90% of these downloads.

The Previous SmartScreen Bypass: CVE-2022-44698

In September 2022, Magniber ransomware was delivered using JScript files. In October, HP Threat Research blogged about these Magniber campaigns, upon which a security researcher noticed a bug in SmartScreen that allowed an attacker to use a malformed Authenticode signature to bypass SmartScreen security warnings. On October 28, 0patch published additional research and patch recommendations.

In mid-November, other threat actors adopted the same bypass to spread the Qakbot malware. The Authenticode signatures in the November 2022 Qakbot campaigns were strikingly similar to those used by Magniber, suggesting the two operators either purchased the bypasses from the same provider, or copied each others' technique. Microsoft patched the security bypass in December 2022 as CVE-2022-44698.

Similar to the bypass occurring now, Magniber ransomware actors used CVE-2022-44698 before a patch was made available. However, the Magniber actors used JScript files during the previous campaigns, whereas in the current campaign they are using MSI files with a

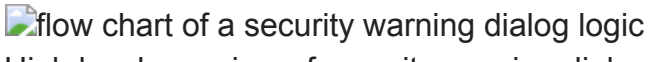
different type of malformed signature.

Security Bypass Details

CVE-2022-44698

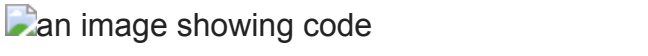
Root cause analysis

As described in 0patch's blog, when the explorer.exe process runs a file, the shdocvw.dll module will perform a request to the AppReputationService interface implemented in smartscreen.exe to get a verdict.



High level overview of security warning dialog logic

By default, shdocvw.dll's DoSafeOpenPromptForShellExec will not display a security warning, and if the smartscreen.exe request returns an error for whatever reason, DoSafeOpenPromptForShellExec proceeds with using the default option and runs the file without displaying any security warnings to the user.



shdocvw.dll's DoSafeOpenPromptForShellExec pseudocode

In CVE-2022-44698's case, a JScript file with a malformed signature was used to force the SmartScreen request to return an error, triggering the behavior described above to bypass the security warning. The error was raised while parsing the file's signature in the function windows::security::signature_info::retrieve of smartscreen.exe.

smartscreen.exe's windows::security::signature_info::retrieve pseudocode

Specifically, this function will first call WTGetSignatureInfo in wintrust.dll to retrieve a CERT_CONTEXT structure pointer cert_context and a HANDLE wvt_state_data. The cert_context, for a well formed signature, will point to the signer certificate, which is the first certificate in the certificate chain.

Next, the function calls WTHelperProvDataFromStateData on wvt_state_data, which returns a CRYPT_PROVIDER_DATA structure pointer crypt_provider_data. Now, if crypt_provider_data and its member hMsg are non-NULL, but cert_context is NULL, an E_INVALIDARG error is raised.

Bypass

Authenticode signatures are encoded in PKCS #7 SignedData structures. A SignedData structure contains amongst other things a list of certificates that are required to validate the signature and a SignerInfo structure. The SignerInfo structure in its turn contains the issuer and serial number of the signer certificate, which can then be looked up in the SignedData certificates.

In practice, the attackers achieved a NULL cert_context by providing an Authenticode signature where the SignerInfo certificate serial number can not be found among the SignedData certificates. This leads to wintrust.dll not being able to find the certificate for the signer, in which case WTGetSignatureInfo will return a NULL value for cert_context.


Magniber used CVE-2022-44698 by providing a signer certificate serial number that is not present in the signature certificates.

It's noteworthy that the signatures in the November 2022 Qakbot campaigns are highly similar to the Magniber signatures, except for a few randomized fields.


Comparison between the certificates included in a Magniber and Qakbot signature

CVE-2023-24880

Root cause analysis

Microsoft patched CVE-2022-44698 in smartscreen.exe, by not raising an error in this specific case, but rather taking an alternative path.


CVE-2022-44698 patch of windows::security::signature_info::retrieve

The problem with this patch is that THROW_HR is called from many other places in smartscreen.exe when different errors are encountered. Every one of these is a potential opportunity for an attacker to return an error to shdocvw.dll, which will fail open and not display a security warning.

This is exactly the route the attackers took with the new bypass. The signature in this case leads to a valid cert_context, so the CVE-2022-44698 patch is not applicable. Further on windows::security::signature_info::retrieve calls windows::security::authenticode_information::create. This function checks if crypt_provider_data->pPDSip->psIndirectData is non-NULL. If not, it calls THROW_HR which will again return an error to shdocvw.dll.


smartscreen.exe's windows::security::authenticode_information::create pseudocode

Bypass

To obtain a NULL crypt_provider_data->pPDSip->psIndirectData, the attackers corrupted the ASN1 numerical identifier (NID) of the SPC_INDIRECT_DATA_OBJID, a Authenticode specific Object Identifier (OID) which contains, for example, the message digest of the signed file.

 image of code
Magniber corrupted the SPC_INDIRECT_DATA_OBJID NID, which leads to crypt_provider_data->pPDSip->psIndirectData being NULL and an error being raised.

Conclusion

This security bypass is an example of a larger trend Project Zero has highlighted previously: vendors often release narrow patches, creating an opportunity for attackers to iterate and discover new variants. When patching a security issue, there is tension between a localized, reliable fix, and a potentially harder fix of the underlying root cause issue. Because the root cause behind the SmartScreen security bypass was not addressed, the attackers were able to quickly identify a different variant of the original bug. Project Zero has written and presented extensively on this trend, and recommends several practices to ensure bugs are correctly and comprehensively fixed.

Indicators of compromise (IoCs)

- ad89fb8819f98e38cddf6135004e1d93e8c8e4cba681ba16d408c4d69317eb47 (CVE-2022-44698, Magniber)
- 77e3a3bc905f9a172e95ba70bf01c3236e6c6423f537fa728b1bda5a40a77fe3 (CVE-2022-44698, Qakbot)
- 8efb4e8bc17486b816088679d8b10f8985a31bc93488c4b65116f56872c1ff16 (CVE-2023-24880, Magniber)

POSTED IN:
Threat Analysis Group

Related stories

- Threat Analysis Group
  TAG Bulletin: Q1 2023

  Threat Analysis Group shares their Q1 2023 bulletin.

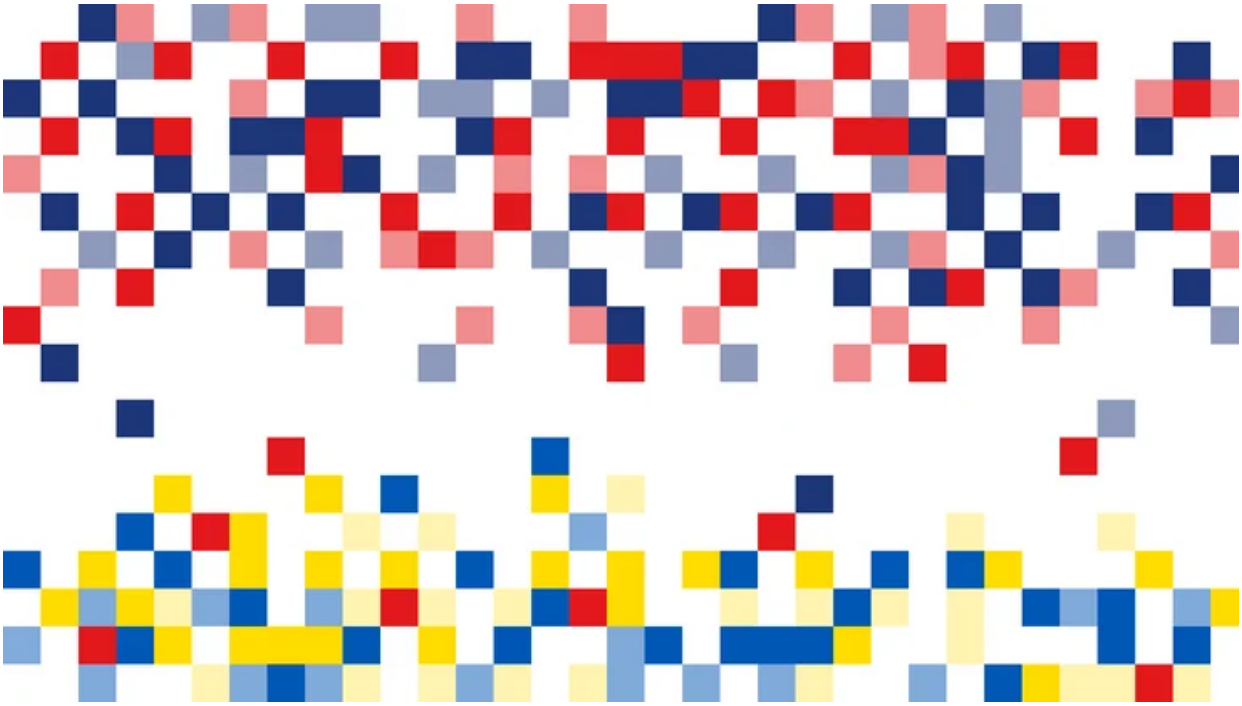
  By Shane Huntley

  Mar 30, 2023

- Threat Analysis Group
  Spyware vendors use 0-days and n-days against popular platforms

  Google's Threat Analysis Group (TAG) tracks actors involved in information operations (IO), government backed attacks and financially motivated abuse. For years, TAG has…

  By Clement Lecigne

  Mar 29, 2023
- 

  Threat Analysis Group
  Fog of war: how the Ukraine conflict transformed the cyber threat landscape

  By Shane Huntley

  Feb 16, 2023
- Threat Analysis Group
  Over 50,000 instances of DRAGONBRIDGE activity disrupted in 2022

  An update on TAG's work to disrupt the information operation network DRAGONBRIDGE.

  By Zak Butler Jonas Taege

  Jan 26, 2023

- Threat Analysis Group
  TAG Bulletin: Q4 2022

  Threat Analysis Group shares their Q4 bulletin.

  By Shane Huntley

  Jan 25, 2023
- Threat Analysis Group
  Internet Explorer 0-day exploited by North Korean actor APT37

  Google's Threat Analysis Group describes a new 0-day vulnerability attributed to North Korean government-backed actors known as APT37.

  By Clement Lecigne Benoit Sevens

  Dec 07, 2022
- .