Ransomware Shield bypass mitigations

2020-01-22 - Steef | ESET Nederland - Comments (0) - Customer Advisories

ESET Customer Advisory 2020-0002
January 21, 2020
Severity: Medium

Summary

ESET was made aware of a possible bypass of its Ransomware Shield feature in the consumer, business, and server products for Windows. ESET identified the underlying method used to administer this attack and prepared updates, which the affected products download automatically.

Details and solution

ESET received a report with a proof-of-concept code attached stating that on a machine with an affected ESET product installed and Ransomware Shield turned on, it was possible for an attacker to misuse the standard Windows API EncryptFile function to maliciously encrypt user's files.

ESET remedied this by preparing an updated version of the HIPS module (1380.2 and later), which contains the Ransomware Shield feature, for version 13 of ESET consumer products, along with a detection engine update for all affected products that block the malicious files used to administer this attack. A separate update of the HIPS module for business, server, and previous versions of consumer products will be released to be able to address the changes in the entire product line.

Once released, the respective modules will be updated automatically, and no user intervention is required. In the meantime, users may perform one of the following two actions to protect their systems from this bypass:

1. Create a HIPS rule to ask for permission every time a process wants to make any change in `%PROGRAMDATA%\Microsoft\Crypto\RSA\MachineKeys*`.

2. Render the bypass non-functional by disabling the Encrypting File System feature in Windows (recommended if not actively using the feature). To disable this feature, run `fsutil behavior set disableencryption 1` from an elevated command prompt, or navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem` in Registry Editor and change the value of `NtfsDisableEncryption` to 1.

Affected programs and versions

- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security and ESET Smart Security Premium 10 and later
- ESET Endpoint Antivirus and ESET Endpoint Security 7 and later
- ESET server security products 7 and later

Feedback & Support

If you have any feedback or questions about this issue, please contact us using the ESET Security Forum, or via local ESET Technical Support.

Acknowledgment

ESET values the principles of responsible disclosure within the security industry and would like to express our thanks to SafeBreach, who reported this issue.