Vidar Stealer Evasion Arsenal

blog.minerva-labs.com/vidar-stealer-evasion-arsenal

- Tweet
-

Vidar Stealer is not new to our world. It is known for stealing sensitive information such as banking details, IP addresses, saved passwords, browser history, login credentials, and recently, known crypto wallets. Being MAAS (Malware As A Service) gives it the ability to constantly develop. We spotted one of the new Variant's hashes on RedBeard's twitter page.

Following our research on the sample we have got, there is probably a code error. However, we have been able to detect several evasion techniques. There were two technique categories; anti-debugging and anti–emulation.

Anti-debugging techniques are usually used to evade analysis of the file and make the analysis process more difficult. In most cases, anti-debugging techniques will not prevent an analysis but might slow it down significantly. The anti-debugging techniques used in our sample are:

1. The use of IsDebuggerPresent API call – read more here .
2. IsDebbugerPresent re-check inside a code by moving a "large fs:30" (a PEB block) to EAX register and checking a second byte.
3. The sample is packed – which is also a well-known anti-debugging technique.

Anti–emulation techniques are also used to prevent analysis, but an analysis by security products. Security products might be sandboxes or anti-virus emulators. In code emulation, the emulator scans files' behavior, by executing the file in a virtual environment. The emulator is similar to sandboxes, but it is not a full-featured sandbox. Our sample uses two anti-emulation techniques:

1. Check if the username is "JohnDoe" - a user name associated with Windows Defender Emulator.

```
.text:004049AA push    offset aJohndoe ; "JohnDoe"
.text:004049AF push    eax
.text:004049B0 call    check_user_name
```

1. Check if the computer name “HAL9TH” - a computer name associated with Windows Defender Emulator.

```
.text:004049E9 loc_4049E9:
.text:004049E9 push    offset aHal9th  ; "HAL9TH"
.text:004049EE push    eax
.text:004049EF call    check_user_name_or_computer_name
```

Threat Actors are always finding a way of evading detection which is why it's crucial for you to have an anti-evasion product protecting your environment. Minerva is a pioneer and a world leader in preventing evasive malware. To learn more about how we can help protect your business from malware, click below.

Request a Meeting

Resources:

https://www.internetsecurity.tips/the-vidar-stealer-trojan-prevention-and-protection-tips/

https://www.kaspersky.com/enterprise-security/wiki-section/products/emulator