

 BRIEF

STRELA STEALER

ZEROFOX INTELLIGENCE

B-2022-11-29a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Malware

November 29, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 5:00 PM (EST) on November 25, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Strela Stealer

Executive Summary

In November 2022, ZeroFox Intelligence analyzed a new information stealer known as Strela Stealer. While most current information stealers target a wide variety of applications and cryptocurrencies, Strela Stealer instead focuses on credentials obtained from Microsoft Outlook and Mozilla Thunderbird. Publicly available samples are known to spread via ISO files containing Windows Shortcut (.lnk) files. An ISO file is a type of container file—similar to ZIP files without compression—that is most commonly used in connection with optical media such as a CD-ROM or DVD. Clicking on the included shortcut file in this instance uses Windows' built-in rundll32.exe to open x.html, a polyglot file that is a valid HTML file and Windows dynamic link library (DLL).

Capabilities

Exfiltrates to Command and Control (C2)

Strela Stealer targets account credentials stored in Microsoft Outlook and Mozilla Thunderbird, sending stolen credentials to an actor-controlled C2 server.

Runs Once

Strela Stealer attempts to create a mutex when it starts to ensure that only one instance is running at a time on the victim's machine.

Protects Strings

Strings in the recovered samples are protected by a hardcoded XOR key.

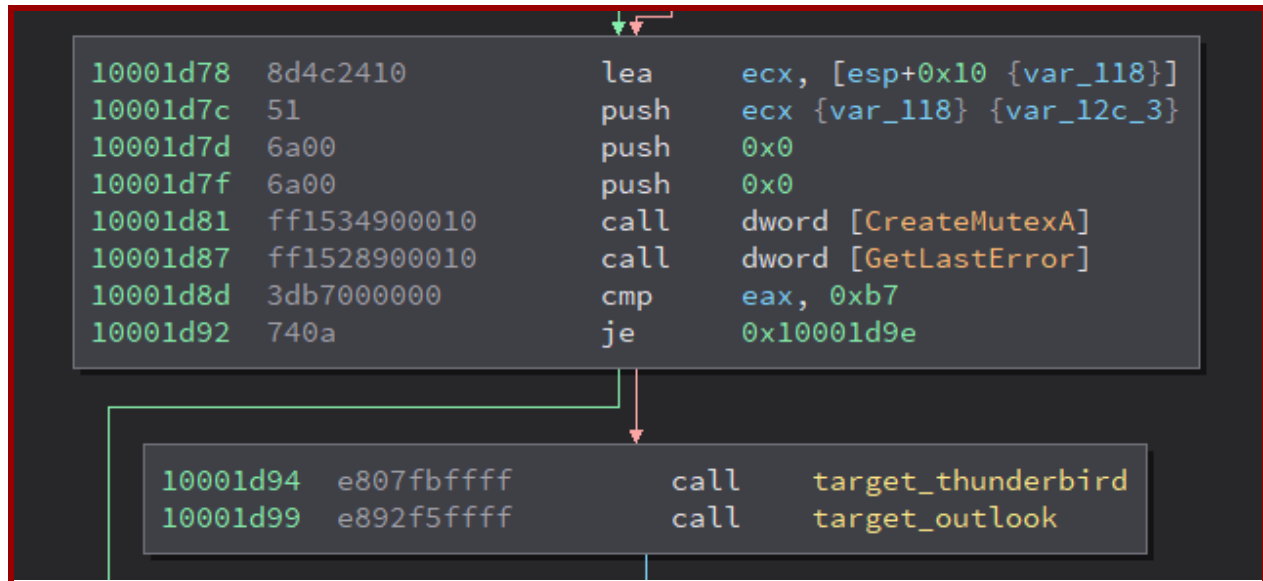


Figure 1. Strela Stealer creates a mutex before targeting Thunderbird and Microsoft Outlook

Source: ZeroFox Intelligence

Recommendations

ISO files are a highly unusual email attachment to send or receive. Threat actors are increasingly turning towards ISOs containing shortcut files as an alternative to Excel and Word documents with macros for initial infection. ZeroFox Intelligence recommends that email administrators block unnecessary attachment types like these when possible. All employees should exercise caution when receiving an ISO file as an email attachment. While these files do not “execute” as a typical application would, Windows 10 includes native support for mounting them as a disc. Attacks utilizing ISO files require the victim to mount the ISO and interact with the contents in some way. When in doubt, do not open the email attachment.



Appendix 1: Indicators of Compromise (IOCs)

SHA256 Hashes

- fal295c746e268a3520485e94d1cecc77e98655a6f85d42879a3aeb401e5cf15
- f6c9532e1f4b66be96f0f56bd7c3a3c1997ea8066b91bfcc984e41f072c347ba
- 8b0d8651e035fcc91c39b3260c871342d1652c97b37c86f07a561828b652e907

URLs

- hXXp://193.106.191[.]166/server.php



Appendix 2: YARA Rules

```
rule StrelaStealer : stealer
{
  meta:
    author   = "@_FirehaK <yara@firehak.com>"
    date     = "2022-11-18"
    description = "Detects Strela Stealer"
    modified  = "2022-11-18"
    reference =
      "https://medium.com/@DCSO_CyTec/shortandmalicious-strelastealer-aims-for-mail-credentials-a4c3e78c8abc"
    tlp      = "CLEAR"

  strings:
    $s1 = "StrelaDLLCompile" ascii

    $x1 = { 8d4c24?? 51 6a00 6a00 ff15????0010 ff15????0010 3db7000000 74?? e8????ffff e8????ffff
8b8c24????0000 5f 5e 5b 33cc 33c0 e8???????? 8be5 5d c3 }
    $xor_string = { (33d2 8bc?|8bc? 33d2) f7f? 4? 8a(82|92)???????? 30(44|54)??ff (3b|83??)?? 72 }

  condition:
    uint16(0) == 0x5a4d
    and any of them
}
```



Appendix 3: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.