Sample submission guide

Steef | ESET Nederland - 2022-02-03 - Reacties (0) - Diagnostics

Issue:

Throughout the years of dealing with technical issues and sample submissions, We have realized the number of improper submissions has not dropped substantially which led us to prepare this guide and summarize how submissions should be handled properly, enabling researches and engineers to process them quickly and eventually providing you with accurate and timely response.

Sample submissions:

1. Always submit files in a rar or zip archives protected with the password “infected”. Do not use custom passwords; otherwise the system will not be able to unpack and pre-process files. If a user has used a non-standard password for encryption, extract files from the archive and re-pack them using the standard password “infected”.
2. Submit only one file per email. More files should be submitted only if there’s a correlation between the files, e.g. if you are submitting a downloader/dropper and the payload or if files come from the same infected system.
3. Files (archives) smaller than 10 MB should be always submitted by email. For larger files ESET support will provide a sharing link to submit the sample.
4. In urgent matters commence the subject with a magic keyword “[URGENT]”. Do not misuse it for ordinary cases, otherwise all tickets will be treated with standard priority.

New malware and suspicious files

If you are submitting an undetected suspicious file from an infected machine, also enclose logs gathered by ELC. Run ELC in normal mode and with the machine connected to the Internet, if possible.

False positives on files

1. Commence the subject with “FP” followed by the detection name and application name. Example of the subject of an urgent FP report: [URGENT] FP Win64/Packed.Themida Synergy
2. In the email body, provide:
   - The name of the application maker.
   - Official product page and download page, if available.
   - The purpose of the application if no page with a product description exists.
   - If more versions of the application are detected, provide them as well.

Antispam

Please provide the original e-mail message in .msg or .eml format in a password protected zip file with password: "infected"

Undetected spam

Please provide the original e-mail message in .msg or .eml format in a password protected zip file with password: "infected"

False positives - IP address found on cloud blacklist

Please provide the ip address that is listed on the blacklist. To illustrate you could provide the screenshot of the detection.

Always submit a new ticket with above information so we can follow-up quickly!