PRODAFT

AUTHOR PROFILING AND LINGUISTIC EVIDENCE: THE LOCKBITSUPP EXAMPLE

In the aftermath of Operation Cronos, the LOCKBIT leader LockBitSupp shared his response on how the whole situation unfolded. In an almost 3,000-word response letter, he was not holding back his thoughts on how the disruption occurred and what were his expectations for the future of LOCKBIT's operations.

This document presented a perfect opportunity for employing the AUCH project. This project, dubbed "Author Profiling & Linguistic Evidence" is a joint initiative by PRODAFT and the University of Zurich. AUCH is used to identify important characteristics of cybercriminals based on their use of language. Given that LockBitSupp's response contained a lot of information, we had plenty of examples to analyze. Moreover, we also correlated the response with the forum posts of the same user and concluded that we're talking about the same author.

At first glance, his adept use of idiomatic expressions and cultural references further indicates a high level of English proficiency. However, the presence of cross-linguistic influence in the writing strongly points to English not being their native language, indicating that it might be Russian instead.

Punctuation and Independent Clauses: *The influence of punctuation from a speaker's first language (L1) can significantly impact their use of a second language (L2), as exemplified by the sentence structure in the given examples, which aligns with Russian linguistic norms.*

Example:

1

EN: "On February 19, 2024 penetration testing of two of my servers took place, at 06:39 UTC I found an error on the site 502 Bad Gateway, restarted nginx - nothing changed, restarted mysql - nothing changed, restarted PHP - the site worked."

Russian syntax permits the crafting of extended, intricate sentences with fewer conjunctions or interruptions than English typically demands. In Russian, it is common practice to employ commas to delineate independent clauses without the use of conjunctions, and dashes are frequently utilized to insert supplementary details or signal a change in narrative direction. These punctuation patterns can be clearly seen throughout the official response he issued.

Example:

2

EN: Very simple [,] that I need to attack the .gov sector more often and more.
RU: Очень просто [,] что мне нужно больше атаковать.

Example:

3

EN: I didn't pay much attention to it [,] because...
RU: Я не обращал на это особого внимания [,] потому...

Examples 2 and 3 show that the author does not employ typical English syntax at the beginning of new clauses, which [in English] do not require a comma. In most of the text, the author's punctuation habits correspond to their Russian counterparts.

Direct Translations: *Direct translations from a person's native language into a second language can often result in calques, which are expressions or idioms translated literally and may not fully align with the idiomatic or syntactic norms of the target language.*

Example:

4

EN: The password did not fit.
RU: Пароль не подошел.

The direct translation results in a physical or spatial connotation of "fitting".

Example:

5

EN: It brings me joy from life.
RU: это приносит мне радость от жизни.

The direct translation produces a non-idiomatic expression that is not used in English in such a format.

Grammatical Influence: *In addition to direct translations and lexical choices, the author's writing exhibits grammatical peculiarities and syntactic structures indicative of a native Russian speaker. One notable feature is the use of double negatives, a construction that is grammatically correct and commonly used in Russian but often considered incorrect or stylistically problematic in standard English.*

Example:

6

EN: ...there is no guarantee that you have [not] been hardened on the server.

The author employs a double negative ("no" and "not") to convey a negative proposition. This sentence tries to highlight the point that there is no guarantee of server-side protection.

Example:

7

EN: Let's blame the hundreds of other people who use publicly available exchanges on Evil Corp.

The author uses the phrase blame [something] on [someone] incorrectly. In Russian, the verb "обвинить в" (to blame) is typically followed by a preposition that translates to "in" necessitating a different syntactic arrangement compared to English.

Example:

8

EN: Because I had to edit the source code for the latest version of PHP as there was [an] incompatibility.

The sentence presents an article mistake typical of native speakers of languages that do not have a direct equivalent to English articles, especially from Slavic backgrounds.

All the abovementioned examples present an exciting opportunity to dive deeper into the adversarial mindset and understand more about the threat actors and their backgrounds. If you want to stay up to date with our lastest research, projects and initiatives, visit www.prodaft.com for more information!