James Chad Ballay

Zodiac Killer's z340 Cipher

The running gag of referring to Ted Cruz as being the Zodiac Killer was a tongue in cheek exercise in absurdity. To reiterate, Ted Cruz was not alive during the beginning of the Zodiac Killer's start of his killings. However, an unintended benefit was that the renewed awareness has prompted people to revisit the ciphers that are attributed to the killer. Tom S Juzek[1] argues that the z340 cipher is likely a false one or at least not a simple substitution cipher. His arguments go much further than my current understanding. Much of his analysis hinges upon comparing the z340 cipher against the known and broken earlier z408 cipher. Then these are in turn compared against several other known ciphers from different authors as well as several selfmade false ciphers. His approach is to show that encrypted text from broken ciphers show common patterns of Ngrams and character frequency. The false ciphers do not show these same patterns. Comparing this behavior against the broken Zodiac Killer z408 cipher and then contrasting it with the behavior of the unbroken z340 cipher. His closing analysis put forward two hypotheses. The first hypothese is that this cipher is not a substitution cipher but a more complex one. This would be in response to the earlier z408 cipher being broken rather quickly. The other hypothesis is that the cipher is just a ruse and is not a valid one. Another possible reaction to his earlier z408 cipher being broken quickly.

Phishing Font and Substitution Cipher to Evade Automatic Detection

There is the analogy that you don't have to outrun a bear you just have to faster than the other guy also outrunning the bear has an inversion that applies to cybercrime. You don't have to be the smartest criminal, you just have to be different enough to break the normal automated detectors. Proofpoint reported that a novel usage of a substitution cipher and custom font pairing was recently discovered.[2] The novelty here comes in two forks. The first layer was to encode the text in the HTML source using a straightforward substitition cipher. (

Unencrypted: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Encrypted: MBCDTFGHRJXLANVUWIZEPOQKYS

So when the letter A was being displayed to the user, it was in the webpage source as the letter M. This obfuscation would bypass simple keyword detection scans of the HTML source. Normally, the decryption step would be done using some JavaScript function. They instead encoded that into the font file itself bypassing detection mechanism looking for the pattern of using JavaScript calls to render

---

[1] *TOM S JUZEK'S BLOG. (n.d.). Retrieved November 22, 2019, from http://tsjuzek.com/blog/z340.html*

[2] Phishing template uses fake fonts to decode content and evade detection: Proofpoint US. (2019, March 12). Retrieved from https://www.proofpoint.com/us/threat-insight/post/phishing-template-uses-fake-fonts-decode-content-and-evade-detection.

decrypted text. Neither of these items are technically complex to implement or detect. But the uncommon usage of those steps would mean that many automated detectors would not catch these phishing attempts.