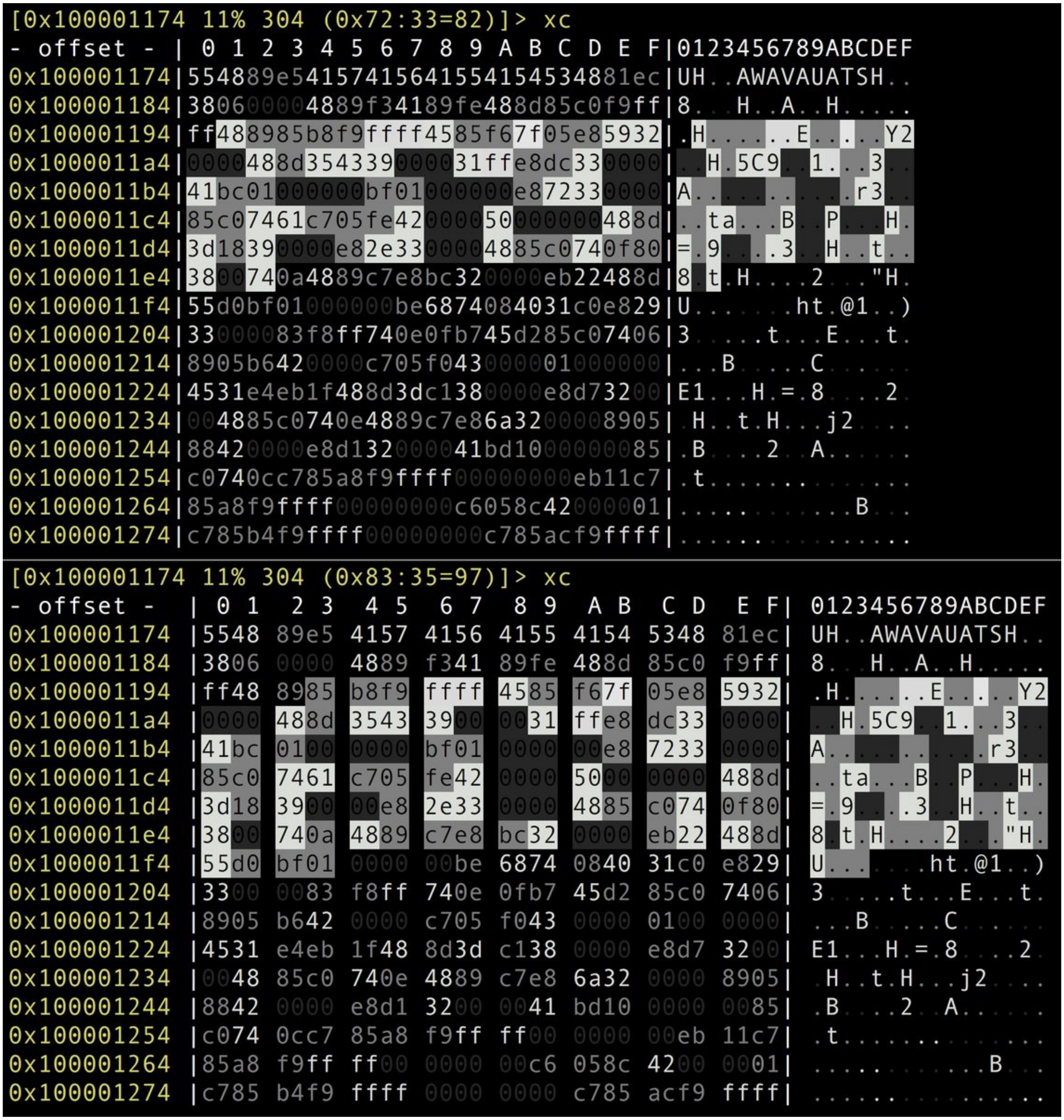
Digital Steganography as an Advanced Malware Detection Evasion Technique

z3roTrust Follow
Aug 30, 2018 · 55 min read ★

A Masters Thesis



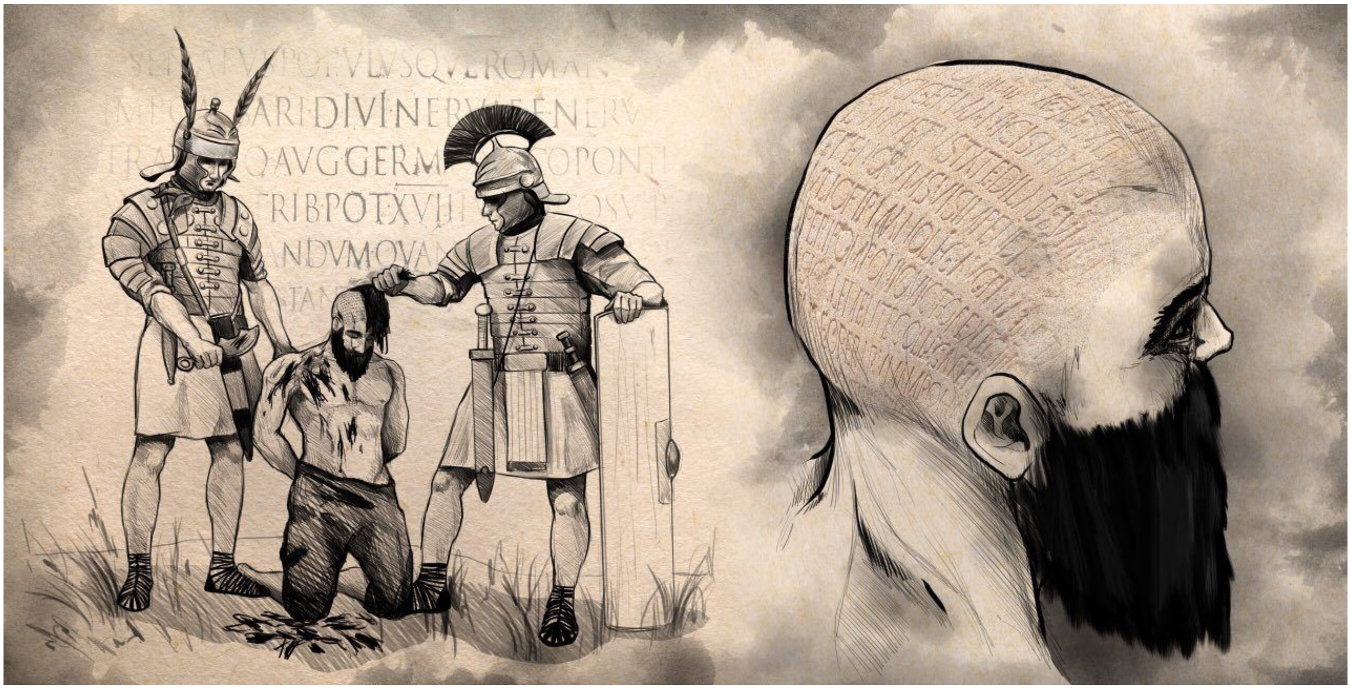
```
[0x100001174 11% 304 (0x72:33=82)]> xc
- offset - | 0 1 2 3 4 5 6 7 8 9 A B C D E F|0123456789ABCDEF
0x100001174|554889e541574156415541545348 81ec|UH..AWAVAUATSH..
0x100001184|380600004889f34189fe488d85c0f9ff|8...H..A..H.....
0x100001194|ff488985b8f9ffff4585f67f05e85932|.H......E.....Y2
0x1000011a4|0000488d354339000031ffe8dc330000|..H.5C9..1...3..
0x1000011b4|41bc01000000bf01000000e872330000|A...........r3..
0x1000011c4|85c07461c705fe420000500000000488d|..ta...B..P...H.
0x1000011d4|3d1839000 0e82e3300004885c0740f80|=.9....3..H..t..
0x1000011e4|3800740a4889c7e8bc320000eb22488d|8.t.H....2..."H.
0x1000011f4|55d0bf01000000be6874084031c0e829|U.......ht.@1..)
0x100001204|33000083f8ff740e0fb745d285c07406|3.....t...E...t.
0x100001214|8905b6420000c705f043000001000000|...B....C.......
0x100001224|4531e4eb1f488d3dc1380000e8d73200|E1...H.=.8....2.
0x100001234|004885c0740e4889c7e86a3200008905|.H..t.H...j2....
0x100001244|88420000e8d1320000 41bd1000000085|.B....2..A......
0x100001254|c0740cc785a8f9ffff00000000eb11c7|.t..............
0x100001264|85a8f9ffff00000000c6058c42000001|............B...
0x100001274|c785b4f9ffff00000000c785acf9ffff|................
```

```
[0x100001174 11% 304 (0x83:35=97)]> xc
- offset -   | 0 1  2 3  4 5  6 7  8 9  A B  C D  E F| 0123456789ABCDEF
0x100001174 |5548 89e5 4157 4156 4155 4154 5348 81ec| UH..AWAVAUATSH..
0x100001184 |3806 0000 4889 f341 89fe 488d 85c0 f9ff| 8...H..A..H.....
0x100001194 |ff48 8985 b8f9 ffff 4585 f67f 05e8 5932| .H......E.....Y2
0x1000011a4 |0000 488d 3543 3900 0031 ffe8 dc33 0000| ..H.5C9..1...3..
0x1000011b4 |41bc 0100 0000 bf01 0000 00e8 7233 0000| A...........r3..
0x1000011c4 |85c0 7461 c705 fe42 0000 5000 0000 488d| ..ta...B..P...H.
0x1000011d4 |3d18 3900 00e8 2e33 0000 4885 c074 0f80| =.9....3..H..t..
0x1000011e4 |3800 740a 4889 c7e8 bc32 0000 eb22 488d| 8.t.H....2..."H.
0x1000011f4 |55d0 bf01 0000 00be 6874 0840 31c0 e829| U.......ht.@1..)
0x100001204 |3300 0083 f8ff 740e 0fb7 45d2 85c0 7406| 3.....t...E...t.
0x100001214 |8905 b642 0000 c705 f043 0000 0100 0000| ...B....C.......
0x100001224 |4531 e4eb 1f48 8d3d c138 0000 e8d7 3200| E1...H.=.8....2.
0x100001234 |0048 85c0 740e 4889 c7e8 6a32 0000 8905| .H..t.H...j2....
0x100001244 |8842 0000 e8d1 3200 0041 bd10 0000 0085| .B....2..A......
0x100001254 |c074 0cc7 85a8 f9ff ff00 0000 00eb 11c7| .t..............
0x100001264 |85a8 f9ff ff00 0000 00c6 058c 4200 0001| ............B...
0x100001274 |c785 b4f9 ffff 0000 0000 c785 acf9 ffff| ................
```

Digital Steganography as an Advanced Malware Detection Evasion Technique

Introduction

The twenty-first century has systematically evolved into the Age of the Internet. Programming code includes the firmware of electronic devices, computer operating systems, and software applications virtually run the developed world. Over time, the economic pressures and demands for rapid software development have resulted in a situation where security is an afterthought. Traditionally, these ‘afterthoughts’ have been remedied by issuing software patches released by software vendors that users have the option of downloading automatically or selectively on their system. In reality, however, often these software patches are never applied for whatever reason, leaving countless numbers of computers vulnerable to previously patched exploits. This perpetual cycle of band-aid software security has presented a limitless well of opportunities for cybercriminals including Nation-state Advanced Persistent Threat (APT) cyber attacks expressly designed to steal data instead of damage networks by exploiting software code vulnerabilities with custom-crafted malicious software better known as malware. Malware used by Nation-state APT groups can take many different forms. However, never before has there been a single piece of malware as devastatingly effective as the Stuxnet virus. First


POPVLVSQVEROMA
ARI·DIVI·NER
AVG·GERM
OPONT
TRIB·POT·XVII
ANDVM·OVA

It is essential to approach steganography from its root origins to gain an appreciation for how it functions and how it has been cleverly applied throughout history before being able to fully comprehend how digital steganography in the twenty-first century is being used as an advanced malware detection evasion technique. The word steganography is derived from the ancient Greek language in which “steganos” translates as hidden and “graphy” translates as writing or drawing in, together the two ancient words mean “covered” or “hidden” writing (Warkentin, Schmidt, & Bekkering, 2008, p. 17). In ancient Greece, primitive applications of steganography were employed that included tattooing a message on people’s scalps and allowing the hair to grow back and completely cover the message prior to dispatching the messenger to the intended recipient (Yugala & Rao, 2013, p. 1629). The ancient Romans invented a different type of primitive steganography that involved writing secret messages in between the lines of scrolls using common substances such as fruit juice, urine, and milk as invisible inks that when heated would darken and become legible (Yugala & Rao, 2013, p. 1629). The preponderance of documented historical cases of steganography appears to demonstrate that the vast majority of steganography users were antagonists rather than protagonists. While this linkage may, in fact, illustrate a connection between secretive communications and nefarious intent, it could also demonstrate the unquenchable fascination society has for the spy novel thriller that many people suspect but that is seldom ever confirmed. These suspicions are