APPENDIX B

Yara signatures

Zeus Yara signature

```
rule zeus_config
{
    meta:
      author = "RicoVZ"
      description = "Zeus config URL finder"

    strings:
      $s1 = "config.bin"
      $s2 = "sys.bin"
      $s3 = "c0nf19.bin"
      $s4 = "cfg.bin"
      $s5 = "konfig.bin"
      $s6 = "bsd.bin"
      $s7 = "ztres.bin"
      $s8 = "forum.php"
      $s9 = "hamilton.bin"
      $s10 = "config/index.php"
      $s11 = "pics.bin"
      $s12 = "40647494/test.rtf"
      $s13 = "O.bin"
      $s14 = "data.bin"
      $s15 = "static.htmls"
      $s16 = "gate.php?action=cfg"
      $s17 = "mysql.bin"
      $s18 = "new/stats.php"

    condition:
      any of ($s*)
}
```

Vawtrak Yara signature

```
rule vawtrak_config_url
{
    meta:
      author = "RicoVZ"
      description = "Vawtrak config data finder"

    strings:
      $s1 = "gate.php"
      $s2 = "index.php"
      $s3 = "components/com_contact"
      $s4 = "web.exe"
      $s5 = "/calc.exe"
      $s6 = "/tc.exe"
      $s7 = "/m1.exe"
      $s8 = "/s1.exe"
      $s9 = "/adverts.php"
      $s10 = "/file.exe"
      $s11 = "/llfrty.php"

    condition:
      any of ($s*)
}
```

Locky Yara signature

```
// Copyright (C) 2016 Cuckoo Foundation.
// This file is part of Cuckoo Sandbox - http://www.cuckoosandbox.org
// See the file 'docs/LICENSE' for copying permission.

rule locky_config
{
    meta:
      author = "jbremer"
      description = "Locky configuration identified"

    strings:
      // RSA1 hex
      $s1 = { 02 00 00 00 a4 00 00 52 53 41 31 }
      //Part of instruction file
      $s2 = { 5F 00 4C 00 6F 00 63 00 6B 00 79 00 5F }
      $s3 = "IMPORTANT INFORMATION"
      $s4 = "Tor Browser"
      $s5 = "&act=getkey&affid="

    condition:
      any of ($s*)
}
```

Teslacrypt Yara signature

```
rule teslacrypt_config
{
    meta:
      author = "RicoVZ"
      description = "Teslacrypt config"

    strings:
      //Part of config data hard coded post fields
      $s1 = { 53 75 62 3D [0-40] 64 68 3D [0-40] 61 64 64 72 3D [0-40] 73 69 7A 65 3D }
      $s2 = ".onion"
      $s3 = "IMPORTANT"
    condition:
      any of ($s*)
}
```