TellYouThePass Ransomware Analysis Reveals a Modern Reinterpretation Using Golang

Anmol Maurya

- TellYouThePass ransomware, discovered in 2019, recently re-emerged compiled using Golang
- Golang's popularity among malware developers makes cross-platform development more accessible
- TellYouThePass ransomware was recently associated with Log4Shell post-exploitation, targeting Windows and Linux
- The CrowdStrike Falcon® platform protects customers from Golang-written TellYouThePass ransomware using the power of machine learning and behavior-based detection

The TellYouThePass ransomware family was recently reported as a post-exploitation malicious payload used in conjunction with a remote code execution vulnerability in Apache Log4j library, dubbed Log4Shell.

TellYouThePass was first reported in early 2019 as a financially motivated ransomware designed to encrypt files and demand payment for restoring them. Targeting both Windows and Linux

systems, TellYouThePass ransomware re-emerged in mid-December 2021 along with other ransomware like Khonsari. This lesser-known ransomware family came back into the spotlight as a post-exploitation payload associated with the Log4Shell. The remote code execution vulnerability is estimated to expose affected organizations to a wave of cybersecurity risks.

Previously known TellYouThePass ransomware samples were written in traditional programming languages like Java or .Net., but two new recent samples reported in public repositories have been rewritten and compiled in Golang.

Golang's popularity among malware developers has steadily increased over the past years. It allows them to use the same codebase and compile it for all major operating systems, making cross-platform development work more accessible.

What follows is a deeper dive into the new Golang-written TellYouThePass ransomware samples for Windows and Linux and how the CrowdStrike Falcon platform protects against them.

Setting Up the Analysis

We first check the binary for the "Go build id" string to identify the Golang build used for compiling it. In recent campaigns of Go-written malware, especially in ransomware cases, attackers patch the binary to remove this string, making it difficult for researchers to use string-based signatures to detect the binary as Go.

Going through the two samples —

`460b096aaf535b0b8f0224da0f04c7f7997c62bf715839a8012c1e1154a38984` (Windows)

`5c8710638fad8eeac382b0323461892a3e1a8865da3625403769a4378622077e` (Linux)

— we noticed that more than 85% of code in the Windows and Linux versions are almost the same:

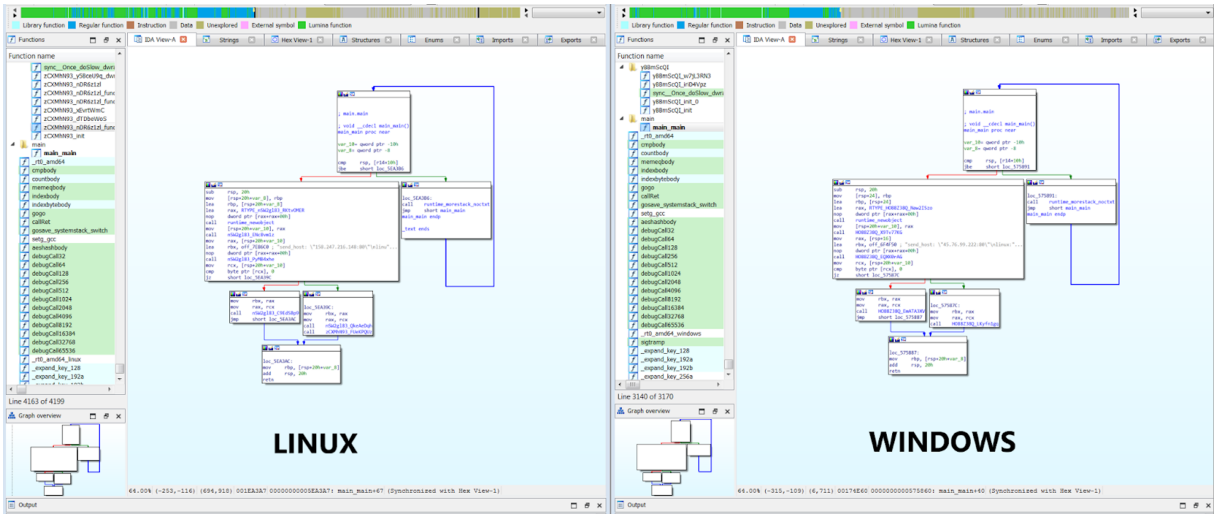


Figure 1. The "main." functions for both Windows and Linux samples are almost identical (Click to enlarge)

A deeper dive into the some of the ransomware's functions:

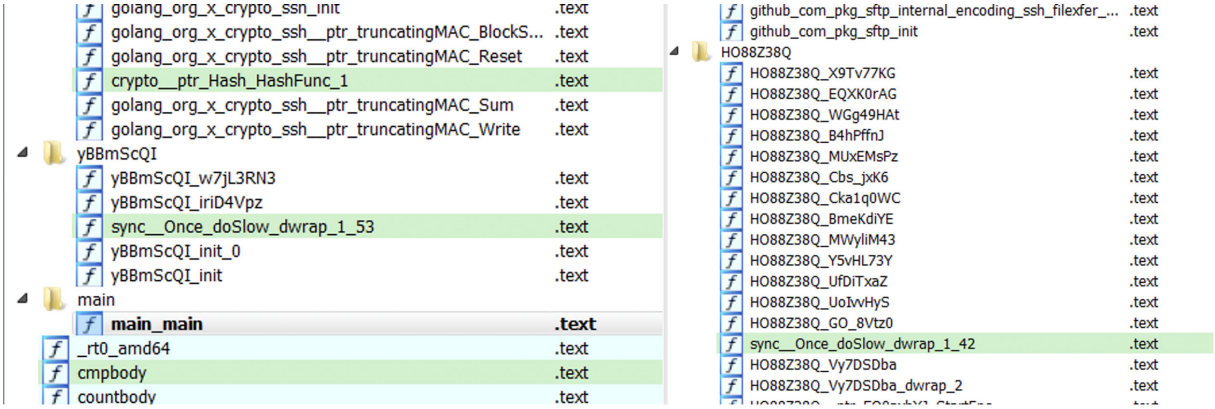


Figure 2. TellYouThePass ransomware functions for the Windows sample in IDA Pro (Click to enlarge)

As we have previously discussed, we start by focusing on the "main." functions in Golang. We notice in this case that the malware authors have left only one main function and changed the other functions to random names, making analysis difficult.

The sample checks the existence of the files "`showkey.txt`" and "`public.txt`" with the help of OS.Getenv, using "`ALLUSERSPROFILE`" and "`HOMEDRIVE`" as keys in Windows and `Home` and `/tmp/` in Linux. If it is present, it means encryption occurred, and it exists using `runtime_gopanic`; otherwise, it creates them.

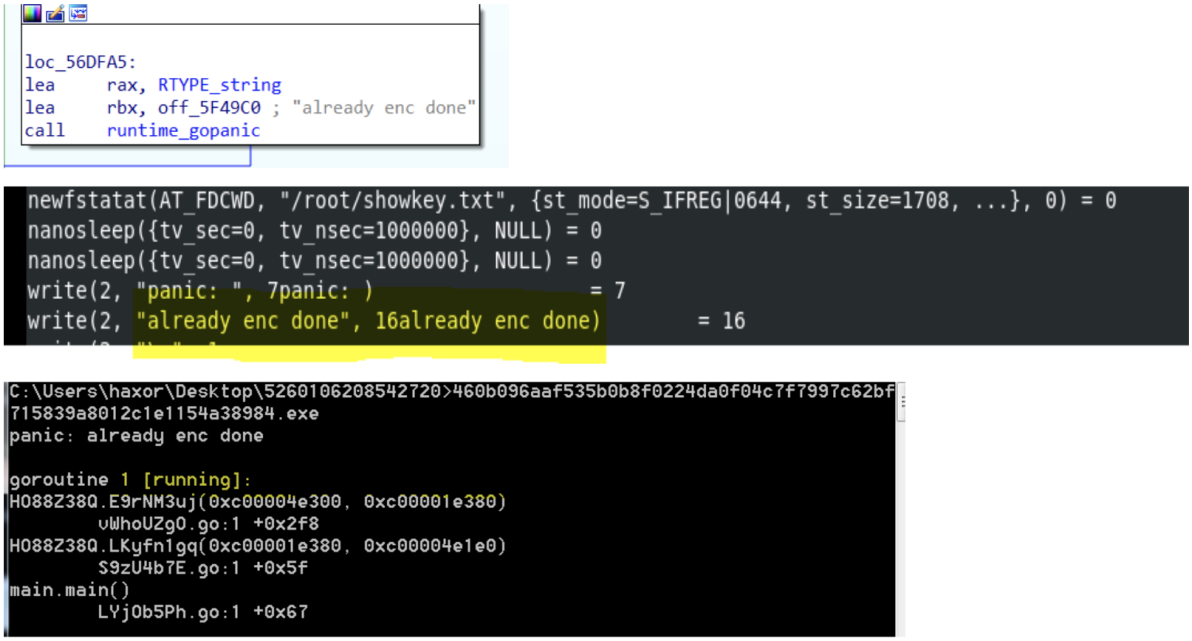


Figure 3. Encryption function followed by successful encryption for both Linux and Windows (Click to enlarge)

For Windows, the return is "`C:\\ProgramData`" and `/root/` directory in Linux.
Using `path.join` to join "`showkey.txt`" and "`public.txt`" with the directories results in:

Windows	Linux
○ "`C:\\ProgramData/showkey.txt`"	○ "`/root/showkey.txt`"

○ “C:\\ProgramData/public.txt”	○ “/root/public.txt”

Table 1. Directories for saving showkey.txt and public.txt

The sample uses the Golang Crypto Packages for RSA key — some of them are crypto_x509_MarshalPKCS1PublicKey, crypto_x509_MarshalPKCS1PrivateKey, encoding_pem_EncodeToMemory and crypto_rsa_GenerateMultiPrimeKey.

As seen in Figure 4, `crypto_x509_ MarshalPKCS1PrivateKey` converts the RSA private key to PKCS #1, ASN.1 DER form. Then, the encoding_pem_EncodeToMemory returns the PEM (Privacy Enhanced Mail) encoding, and after that, `runtime_slicebytetostring` converts bytes to string, resulting in the conversion of bytes to string (see Figure 5).

```
sub     rsp, 50h
mov     [rsp+50h+var_8], rbp
lea     rbp, [rsp+50h+var_8]
call    crypto_x509_MarshalPKCS1PrivateKey
lea     rdx, [rsp+50h+var_38]
movups  xmmword ptr [rdx], xmm15
lea     rsi, [rsp+50h+var_28]
movups  xmmword ptr [rsi], xmm15
lea     rsi, [rsp+50h+var_18]
movups  xmmword ptr [rsi], xmm15
lea     rsi, aRsaPrivateKey ; "RSA PRIVATE KEY"
mov     [rsp+50h+var_38], rsi
mov     [rsp+50h+var_30], 0Fh
mov     [rsp+50h+var_20], rax
mov     [rsp+50h+var_18], rbx
mov     [rsp+50h+var_10], rcx
mov     rax, rdx
nop     dword ptr [rax+rax+00h]
call    encoding_pem_EncodeToMemory
mov     rcx, rbx
mov     rbx, rax
xor     eax, eax
call    runtime_slicebytetostring
mov     rbp, [rsp+50h+var_8]
add     rsp, 50h
retn
```

Figure 4. Function that generates the RSA private key

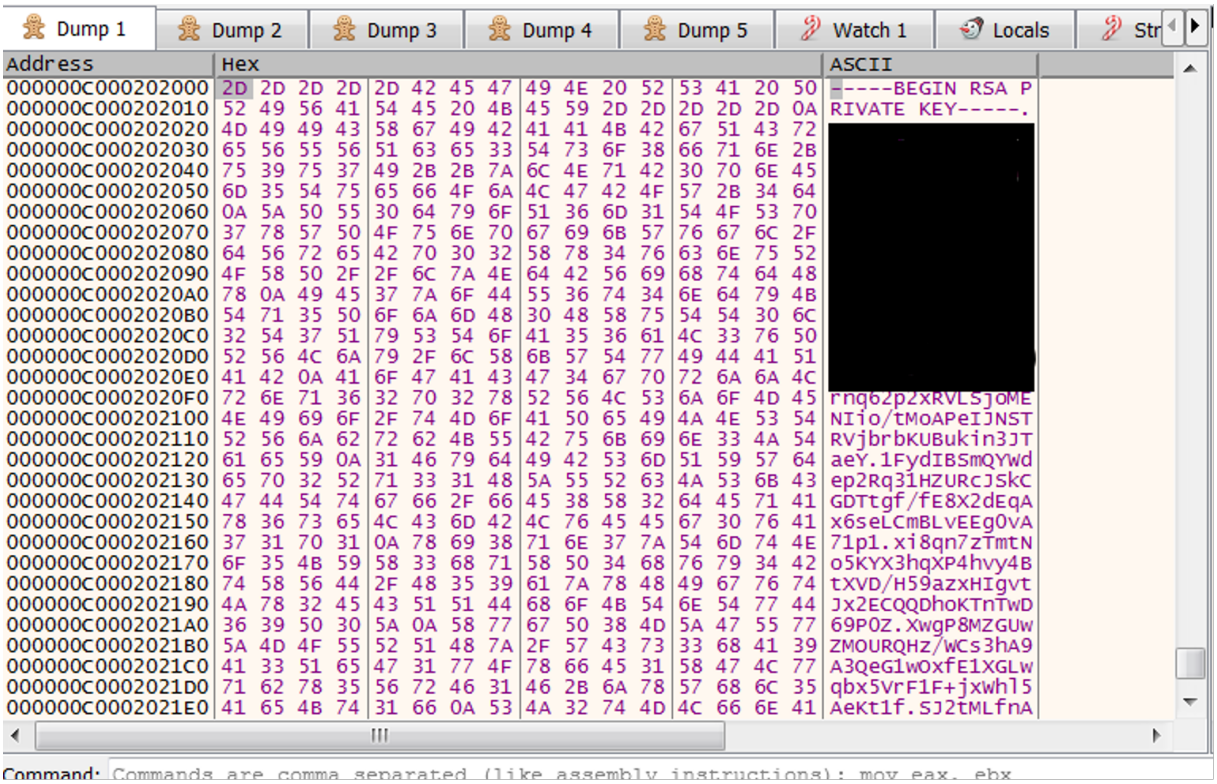
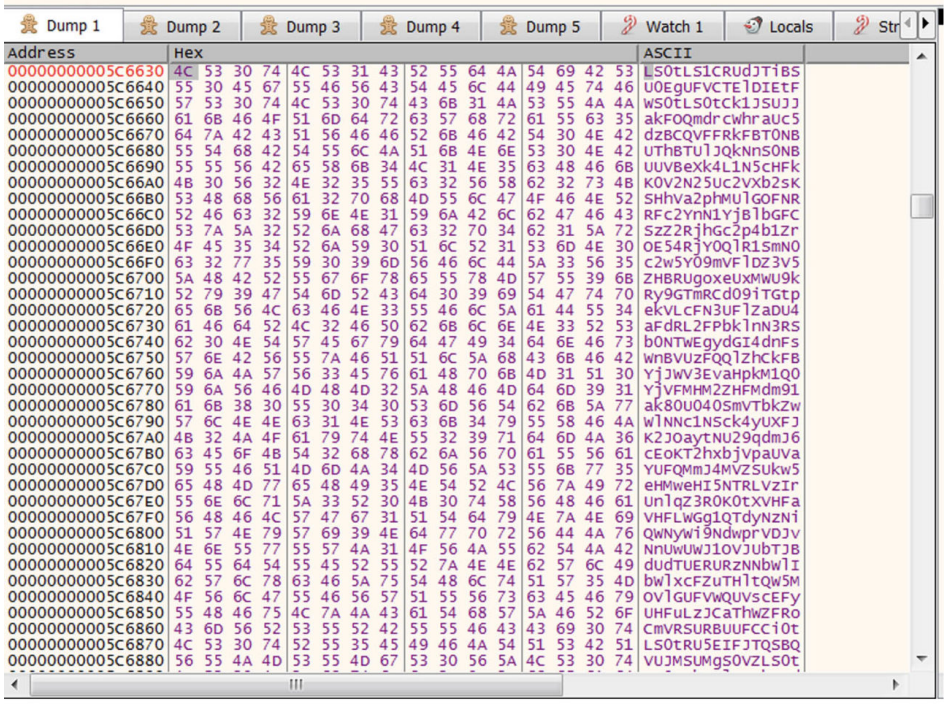
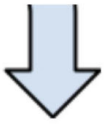


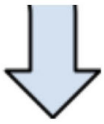
Figure 5. The generated RSA key (Click to enlarge)

The RSA public key is generated using the `encoding_base64_ptr_Encoding_DecodeString` and `encoding_pem_encode` packages from Golang, as shown in Figure 6.





```
call    encoding_base64__ptr_Encoding_DecodeString
call    encoding_pem_Decode
```



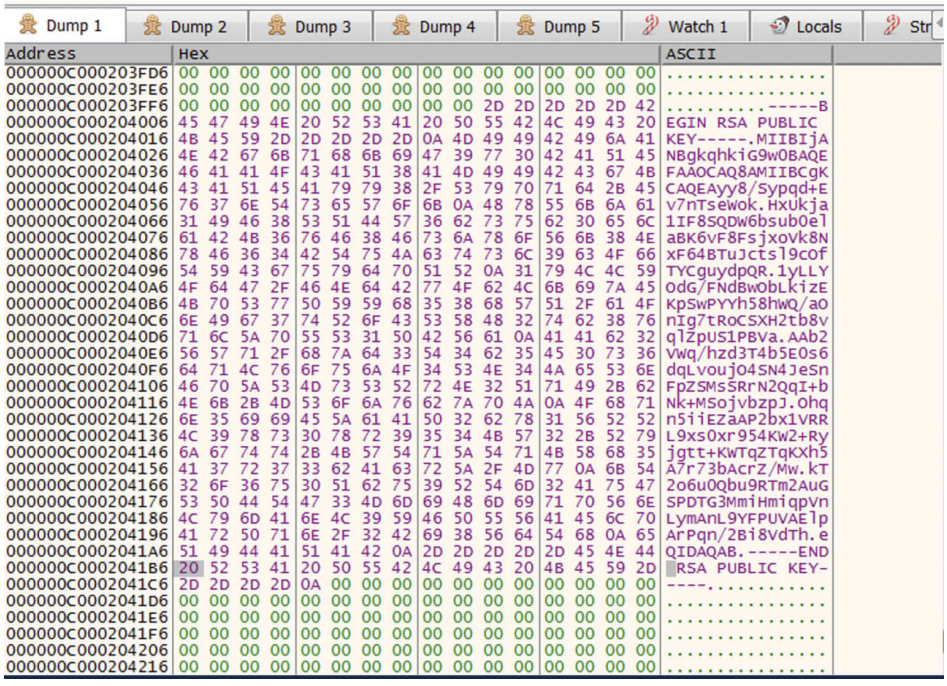


Figure 6. Base64 decoding (Click to enlarge)

After that, the PERSON_ID stores the encoding generated by "encoding_base64__ptr_Encoding_EncodeToString" (in this case:

"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"

as array for Base64 std encoding) every time the sample runs, saving it into "showkey.txt".

Afterward, another key is generated using the function below (Figure 7), also saving it into "public.txt":

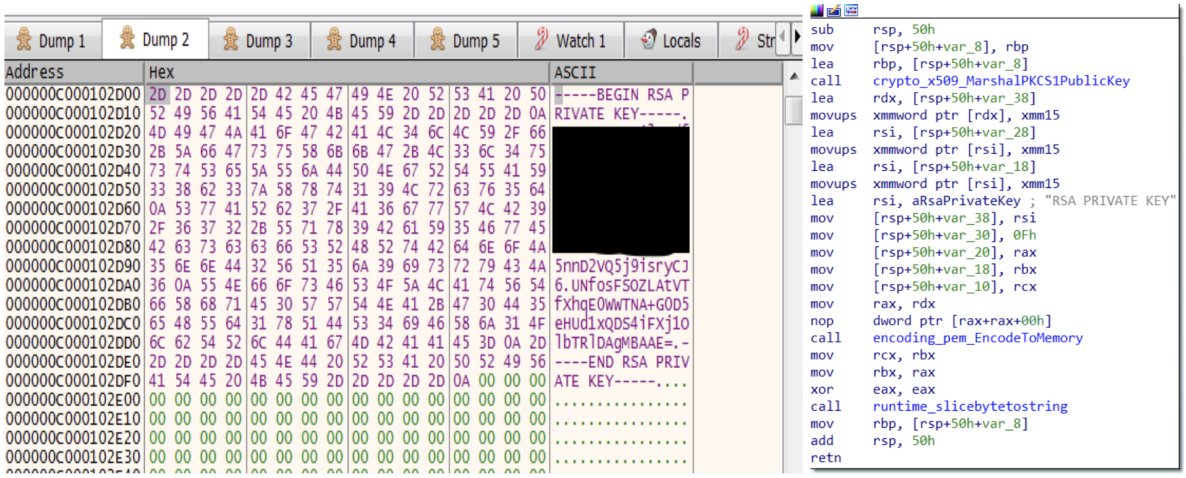


Figure 7. Key generation function (Click to enlarge)

Ransomware Behavior Prior to Encryption

TellYouThePass ransomware tries to kill some tasks and services before initiating the encryption routine, as shown in Table 2 below. However, in Linux, it requires root privilege to do that. Targeted applications include various email clients, database applications, web servers and document editors.

It runs various commands using `cmd.exe` to kill tasks in Windows, and in Linux, it takes the os_exec_command Go package to execute different commands using `/bin/bash/`:

Windows	Linux
○ "taskkill /f /im msftesql.exe " ○ "schtasks /delete /tn WM /F " ○ "taskkill /f /im sqlagent.exe " ○ "taskkill /f /im sqlbrowser.exe " ○ "taskkill /f /im sqlservr.exe " ○ "taskkill /f /im sqlwriter.exe " ○ "taskkill /f /im oracle.exe " ○ "taskkill /f /im ocssd.exe " ○ "taskkill /f /im dbsnmp.exe " ○ "taskkill /f /im synctime.exe " ○ "taskkill /f /im mydesktopqos.exe "	○ "service mysql stop" ○ "/etc/init.d/mysqld stop" ○ "service oracle stop" ○ "systemctl disable \"postgresql*\"" ○ "systemctl disable \"mysql*\"" ○ "systemctl disable \"oracle*\""

○ “taskkill /f /im agntsvc.exeisqlplussvc.” ○ “taskkill /f /im xfssvccon.exe “ ○ “taskkill /f /im mydesktopservice.exe “ ○ “taskkill /f /im ocautoupds.exe “ ○ “taskkill /f /im agntsvc.exeagntsvc.exe “ ○ “taskkill /f /im agntsvc.exeencsvc.exe “ ○ “taskkill /f /im firefoxconfig.exe “ ○ “taskkill /f /im tbirdconfig.exe “ ○ “taskkill /f /im ocomm.exe “ ○ “taskkill /f /im mysqld.exe “ ○ “taskkill /f /im mysqld-nt.exe “ ○ “taskkill /f /im mysqld-opt.exe “ ○ “taskkill /f /im dbeng50.exe “ ○ “taskkill /f /im sqbcoreservice.exe “ ○ “taskkill /f /im excel.exe “ ○ “taskkill /f /im infopath.exe “ ○ “taskkill /f /im msaccess.exe “ ○ “taskkill /f /im mspub.exe “ ○ “taskkill /f /im onenote.exe “ ○ “taskkill /f /im outlook.exe “ ○ “taskkill /f /im powerpnt.exe “ ○ “taskkill /f /im steam.exe “ ○ “taskkill /f /im sqlservr.exe “ ○ “taskkill /f /im thebat.exe “ ○ “taskkill /f /im thebat64.exe “ ○ “taskkill /f /im thunderbird.exe “ ○ “taskkill /f /im visio.exe “ ○ “taskkill /f /im winword.exe “ ○ “taskkill /f /im wordpad.exe” ○ “taskkill /f /im tnslsnr.exe”	

Table 2. TellYouThePass commands that try to terminate some tasks and services before initiating the encryption routine

After that, it iterates through all directories from **A to Z** and encrypts the files.

```
loc_56A857:
mov     [rsp+64], rcx
lea     rdx, aAbcdefghijklmn ; "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
movzx   ebx, byte ptr [rdx+rcx]
```

Both the Windows and the Linux versions have a list of directory exclusions for encryption, shown in Table 3.

Windows	Linux
○ EFI.Boot ○ EFI.Microsoft ○ Windows ○ Program Files	○ /bin ○ /boot ○ /sbin ○ /tmp

○ All Users ○ Boot ○ IEidcache ○ ProgramData ○ desktop.ini ○ autorun.inf ○ netuser.dat ○ iconcache.db ○ thumbs.db ○ Local Settings ○ bootfont.bin ○ System Volume Information ○ AppData ○ Recycle.Bin ○ Recovery	○ /etc ○ /lib ○ /proc ○ /dev ○ /sys ○ /usr/include ○ /usr/java

Table 3. TellYouThePass directory exclusions for encryption

The TellYouThePass ransomware focuses on encrypting popular media and file extensions, saving their paths in the "`encfile.txt`" text file, located in the same folder as "`public.txt`" and "`showkey.txt`".

Below is the full list of targeted extensions for encryption:

1cd, 3dm, 3ds, 3fr, 3g2, 3gp, 3pr, 602, 7z, ps1, 7zip, aac, ab4, accdb, accde, accdr, accdt, ach, acr, act, adb, adp, ads, aes, agdl, ai, aiff, ait, al, aoi, apj, arc, arw, asc, asf, asm, asp, aspx, asx, avi, awg, back, backup, backupdb, bak, bank, bat, bay, bdb, bgt, bik, bin, bkp, blend, bmp, bpw, brd, c, cdf, cdr, cdr3, cdr4, cdr5, cdr6, cdrw, cdx, ce1, ce2, cer, cfg, cgm, cib, class, cls, cmd, cmt, conf, config, contact, cpi, cpp, cr2, craw, crt, crw, cs, csh, csl, csr, css, csv, dac, dat, db, db3, db_journal, dbf, dbx, dc2, dch, dcr, dcs, ddd, ddoc, ddrw, dds, der, des, design, dgc, dif, dip, dit, djv, djvu, dng, doc, docb, docm, docx, dot, dotm, dotx, drf, drw, dtd, dwg, dxb, dxf, dxg, edb, eml, eps, erbsql, erf, exf, fdb, ffd, fff, fh, fhd, fla, flac, flf, flv, flvv, fpx, frm, fxg, gif, gpg, gray, grey, groups, gry, gz, h, hbk, hdd, hpp, html, hwp, ibank, ibd, ibz, idx, iif, iiq, incpas, indd, jar, java, jnt, jpe, jpeg, jpg, jsp, jspx, ashx, js, kc2, kdbx, kdc, key, kpdx, kwm, laccdb, lay, lay6, ldf, lit, log, lua, m, m2ts, m3u, m4p, m4u, m4v, mapimail, max, mbx, md, mdb, mdc, mdf, mef, mfw, mid, mkv, mlb, mml, mmw, mny, moneywell, mos, mov, mp3, mp4, mpeg, mpg, mrw, ms11, msg, myd, myi, nd, ndd, ndf, nef, nk2, nop, nrw, ns2, ns3, ns4, nsd, nsf, nsg, nsh, nvram, nwb, nx2, nxl, nyf, oab, obj, odb, odc, odf, odg, odm, odp, ods, odt, ogg, oil, orf, ost, otg, oth, otp, ots, ott, p12, p7b, p7c, pab, pages, paq, pas, pat, pcd, pct, pdb, pdd, pdf, pef, pem, pfx, php, pif, pl, plc, plus_muhd, png, pot, potm, potx, ppam, pps, ppsm, ppsx, ppt, pptm, pptx, prf, ps, psafe3, psd, pspimage, pst, ptx, pwm, py, qba, qbb, qbm, qbr, qbw, qbx, qby, qcow, qcow2, qed, r3d, raf, rar, rat, raw, rb, rdb, rm, rtf, rvt, rw2, rwl, rwz, s3db, safe, sas7bdat, sav, save, say, sch, sd0, sda, sdf, sh, sldm, sldx, slk, sql, sqlite, sqlite3, sqlitedb, sr2, srf, srt, srw, st4, st5, st6, st7, so, st8, stc, std, sti, stm, stw, stx, svg, swf, sxc, sxd, sxg, sxi, sxm, sxw, tar, tar.bz2, tbk, tex, tga, tgz, thm, tif, tiff, tlg, txt, uop, uot, vb, vbox, vbs, vdi, vhd, vhdx, vmdk, vmsd, vmx, vmxf, vob, wab, wad, wallet, war, wav, wb2, wk1, wks, wma, wmv, wpd, wps, x11, x3f, xis, xla, xlam, xlc, xlk, xlm, xlr, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw, xml, ycbcra, yuv, zip.

Finally, the ransom note contains information about the encryption algorithm used to encrypt the files, specifically RSA-1024 and AES-256. It also includes the personid, used for identifying the victim. Following 0.05 bitcoin transfer into a designated and hardcoded wallet, attackers promise to provide victims with the decryption tool to recover all files.

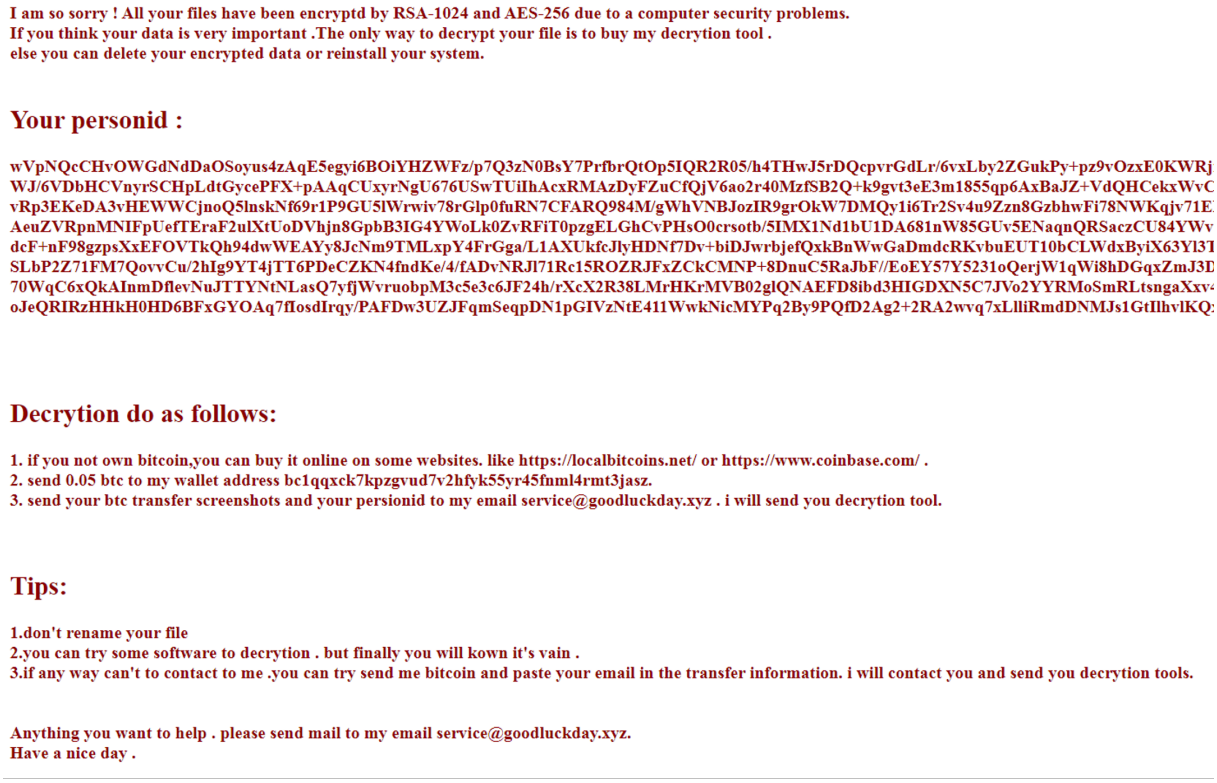


Figure 9. TellYouThePass ransom note (Click to enlarge)

CrowdStrike Falcon Protection

The Falcon platform automatically detects and protects against this type of Golang-written malware using the power of the cloud, on-sensor and in-the-cloud machine learning, and indicators of attack (IOAs) to detect the threat. As Figure 10 shows, Falcon's cloud-based machine learning detects both Golang-written ransomware samples for TellYouThePass, immediately protecting Windows and Linux environments.

CrowdStrike Falcon leverages machine learning to identify known and unknown malware or threats by understanding malicious intent. Both on-sensor and cloud-based machine learning can detect and prevent post-exploitation threats leveraging exploits such as Log4Shell to protect against malware, including the new Golang-written TellYouThePass ransomware.

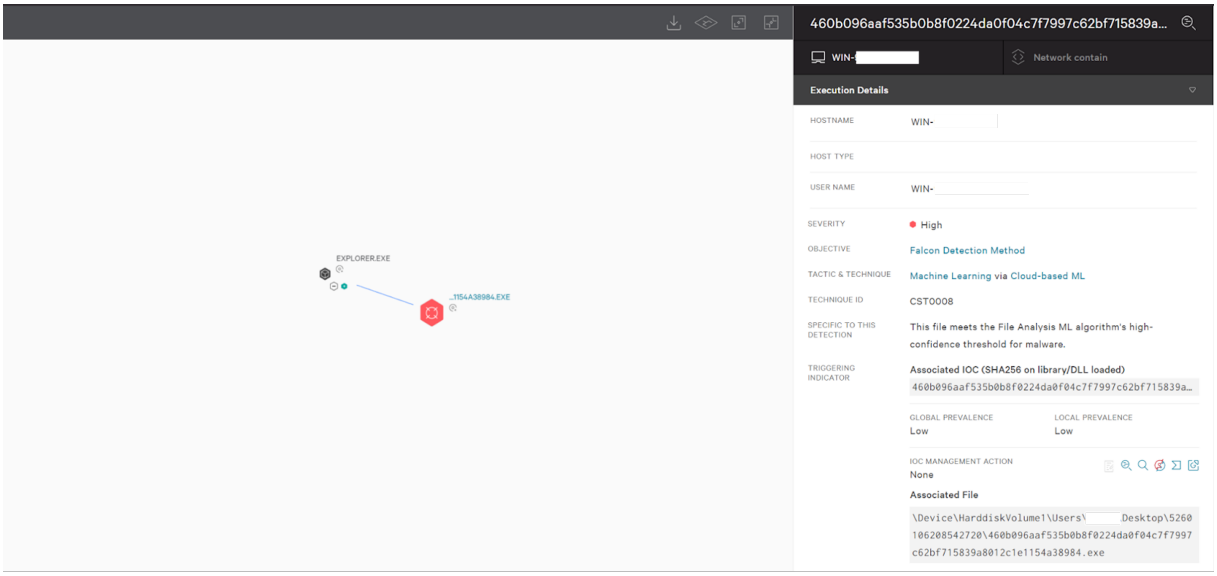


Figure 10. Falcon detection of Golang-written Windows TellYouThePass ransomware sample (Click to enlarge)

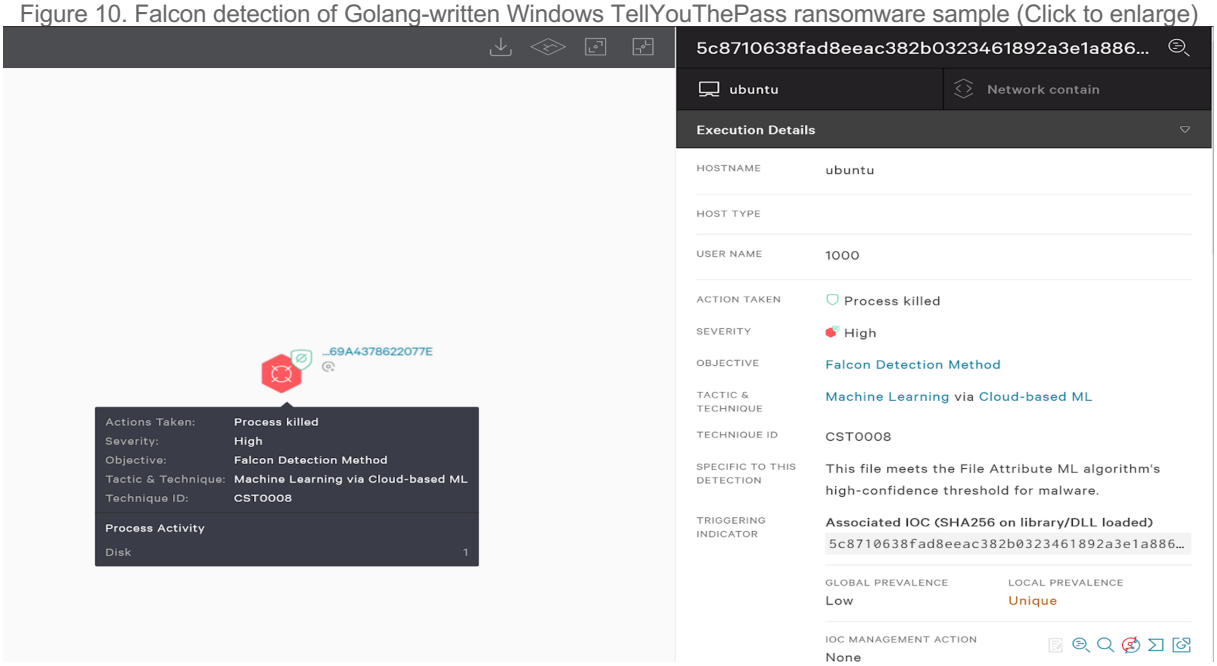


Figure 11. Falcon detection of Golang-written Linux TellYouThePass ransomware sample (Click to enlarge)

The CrowdStrike Falcon platform provides protection against threats and visibility for all hosts in Windows, Linux and macOS, regardless of their location. The Falcon sensor can detect and prevent threats ranging from ransomware, cryptocurrency miners, trojans and botnets to stop today's most sophisticated threats.

Indicators of Compromise (IOCs)

File/Host	sha256
Windows	460b096aaf535b0b8f0224da0f04c7f7997c62bf715839a8012c1e1154a38984

Linux	5c8710638fad8eeac382b0323461892a3e1a8865da3625403769a4378622077e
Windows host	45[.]76[.]99[.]222[:]80
Linux Host	158[.]247[.]216[.]148[:]80

MITRE ATT&CK® Framework Mapping

Attack Id	Tactic	Description
T1059	Execution	Command and Scripting Interpreter
T1053	Execution Persistence Privilege Escalation	Scheduled Task/Job
T1027	Defense Evasion	Obfuscated Files or Information
T1140	Defense Evasion	Deobfuscate/Decode Files or Information
T1083	Discovery	File and Directory Discovery
T1057	Discovery	Process Discovery
T1560	Collection	Archive Collected Data
T1486	Impact	Data Encrypted for Impact

Additional Resources

- *Read more about Golang malware in this blog: Golang Malware Is More than a Fad: Financial Motivation Drives Adoption*
- *Learn about another ransomware variant that uses a Golang packer: New Ransomware Variant Uses Golang Packer*
- *Visit the product website to learn how the powerful CrowdStrike Falcon platform provides comprehensive protection across your organization, workers and data, wherever they are located.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ and see how true next-gen AV performs against today's most sophisticated threats.*