TellYouThePass Ransomware Analysis Reveals Modern Reinterpretation Using Golang

crowdstrike.com/blog/tellyouthepass-ransomware-analysis-reveals-modern-reinterpretation-using-golang/

Anmol Maurya January 11, 2022

- 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:

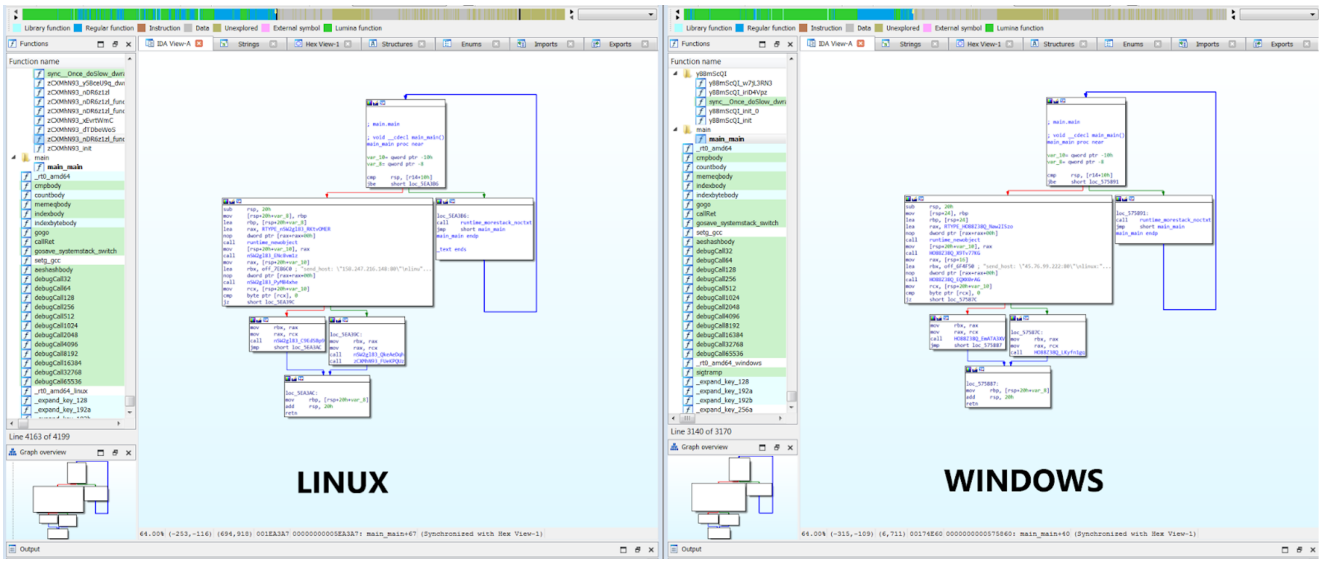


Figure 1. The “main.” functions for both Windows and Linux samples are almost identical (Click to enlarge)

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

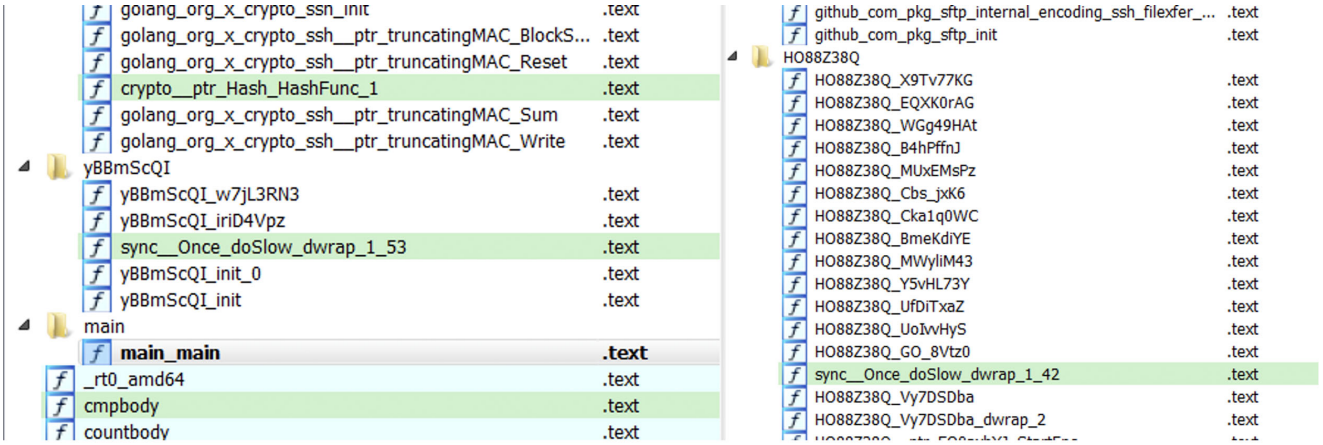


Figure 2. TellYouThePass ransomware functions for the Windows sample in IDA Pro (Click to enlarge)

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.

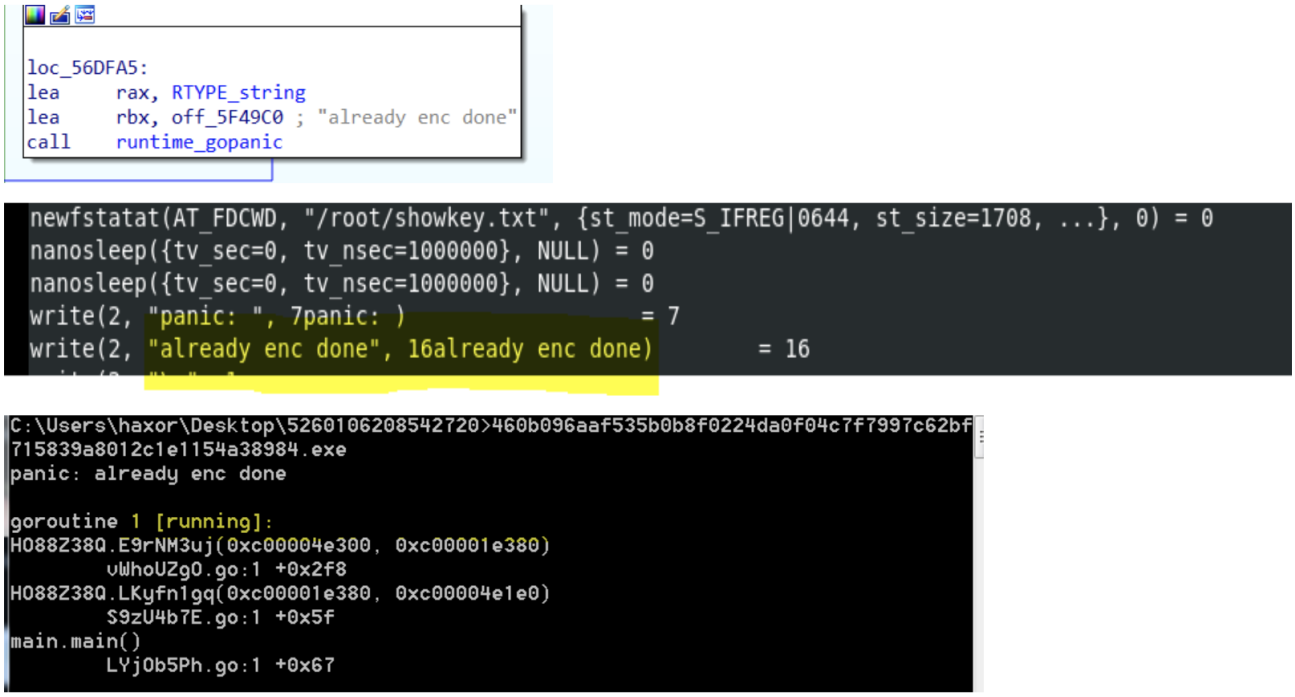


Figure 3. Encryption function followed by successful encryption for both Linux and Windows (Click to enlarge)

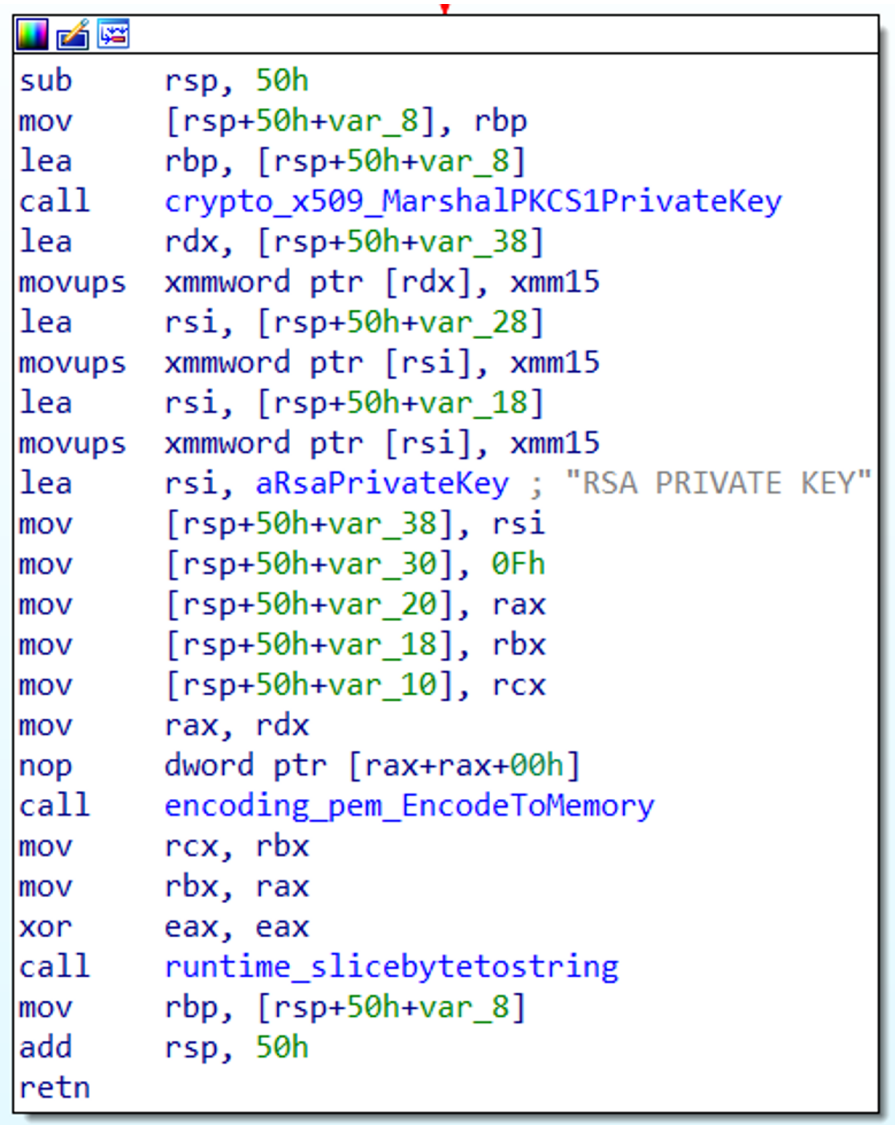
For Windows, the return is " `C:\\ProgramData` " and `/root/` directory in Linux. Using `path.join` to join " `showkey.txt` " and " `public.txt` " with the directories results in:

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

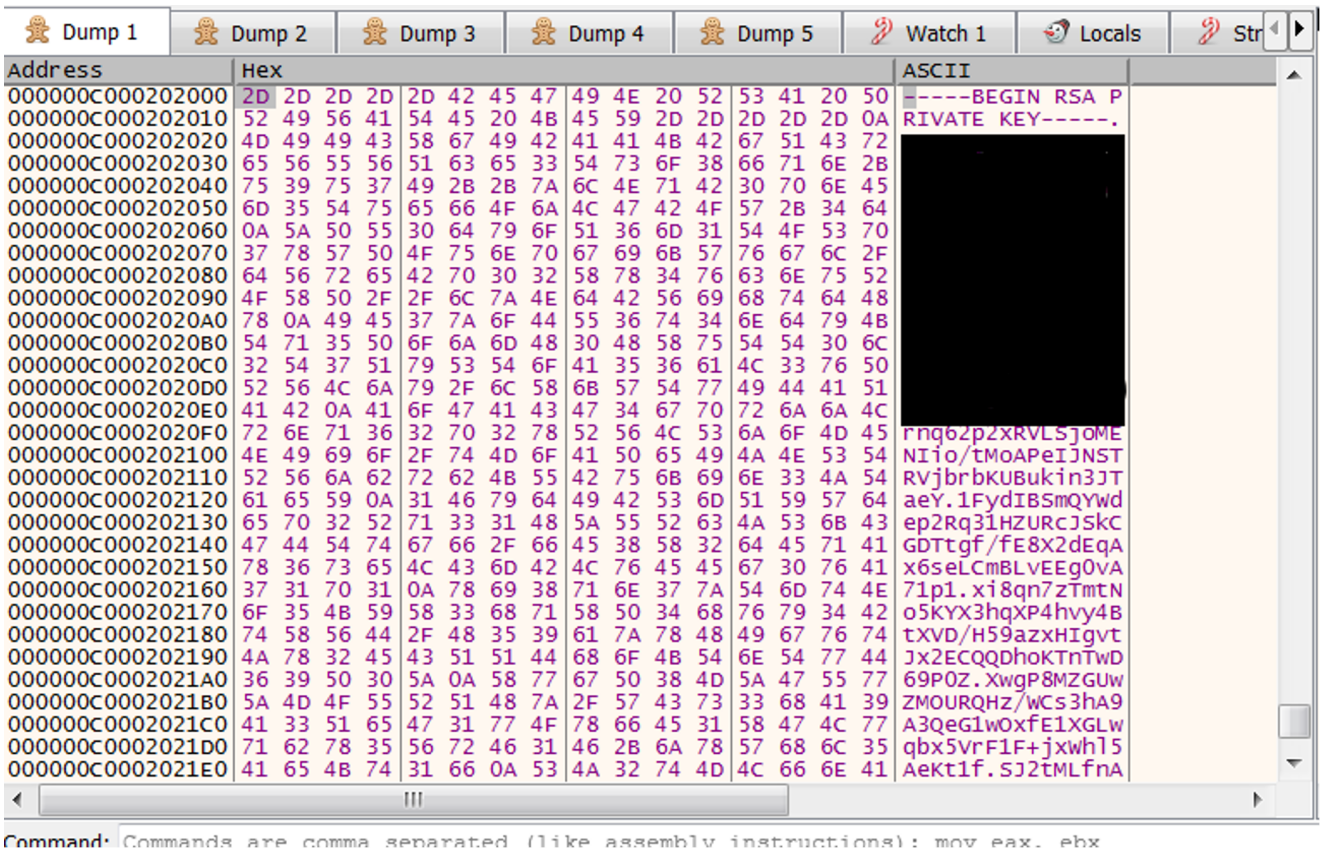
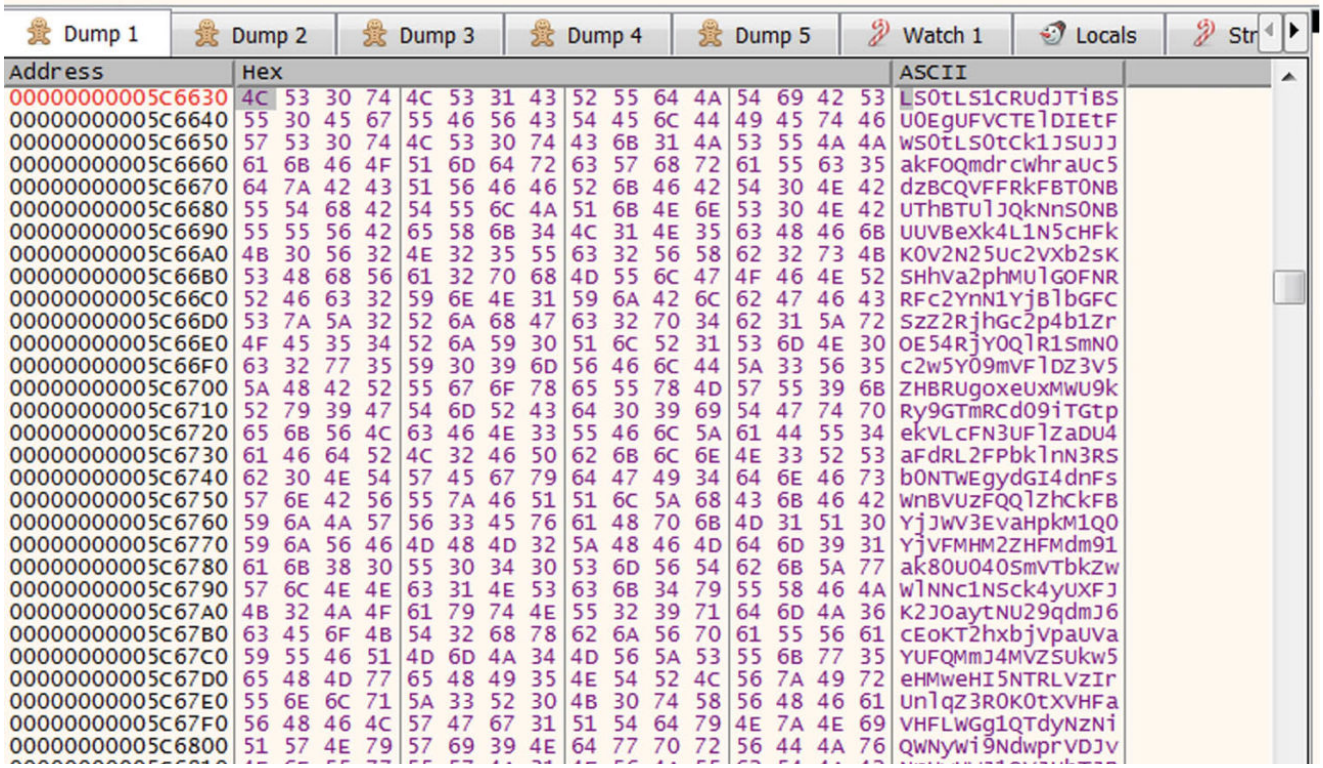
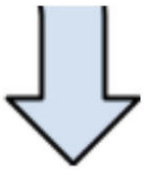


Figure 5. The generated RSA key (Click to enlarge)

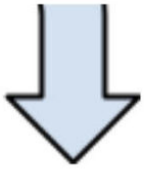
The RSA public key is generated using the `encoding_base64_ptr_Encoding_DecodeString` and `encoding_pem_encode` packages from Golang, as shown in Figure 6.



```
000000000005C6810 4E 6E 55 77 55 57 4A 31 4F 56 4A 55 62 54 4A 42 NnUwUWJ1OVJUbTJB
000000000005C6820 64 55 64 54 55 45 52 55 52 7A 4E 4E 62 57 6C 49 dUdTUERURzNNbWlI
000000000005C6830 62 57 6C 78 63 46 5A 75 54 48 6C 74 51 57 35 4D bWlxcFZuTHltQW5M
000000000005C6840 4F 56 6C 47 55 46 56 57 51 55 56 73 63 45 46 79 OVlGUFVWQUVscEFy
000000000005C6850 55 48 46 75 4C 7A 4A 43 61 54 68 57 5A 46 52 6F UHFuLzJCaThWZFRo
000000000005C6860 43 6D 56 52 53 55 52 42 55 55 46 43 43 69 30 74 CmVRSURBUUFCCi0t
000000000005C6870 4C 53 30 74 52 55 35 45 49 46 4A 54 51 53 42 51 LS0tRU5EIFJTQSBQ
000000000005C6880 56 55 4A 4D 53 55 4D 67 53 30 56 5A 4C 53 30 74 VUJMSUMgS0VZLS0t
```



```
call    encoding_base64__ptr_Encoding_DecodeString
call    encoding_pem_Decode
```



Dump 1 | Dump 2 | Dump 3 | Dump 4 | Dump 5 | Watch 1 | Locals | Str

Address	Hex	ASCII
000000C000203FD6	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
000000C000203FE6	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
000000C000203FF6	00 00 00 00 00 00 00 00 00 00 2D 2D 2D 2D 2D 42	..........-----B
000000C000204006	45 47 49 4E 20 52 53 41 20 50 55 42 4C 49 43 20	EGIN RSA PUBLIC
000000C000204016	4B 45 59 2D 2D 2D 2D 2D 0A 4D 49 49 42 49 6A 41	KEY-----.MIIBIjA
000000C000204026	4E 42 67 6B 71 68 6B 69 47 39 77 30 42 41 51 45	NBgkqhkiG9w0BAQE
000000C000204036	46 41 41 4F 43 41 51 38 41 4D 49 49 42 43 67 4B	FAAOCAQ8AMIIBCgK
000000C000204046	43 41 51 45 41 79 79 38 2F 53 79 70 71 64 2B 45	CAQEAyy8/Sypqd+E
000000C000204056	76 37 6E 54 73 65 57 6F 6B 0A 48 78 55 6B 6A 61	v7nTseWok.HxUkja
000000C000204066	31 49 46 38 53 51 44 57 36 62 73 75 62 30 65 6C	1IF8SQDW6bsub0el
000000C000204076	61 42 4B 36 76 46 38 46 73 6A 78 6F 56 6B 38 4E	aBK6vF8FsjxoVk8N
000000C000204086	78 46 36 34 42 54 75 4A 63 74 73 6C 39 63 4F 66	xF64BTuJctsl9cOf
000000C000204096	54 59 43 67 75 79 64 70 51 52 0A 31 79 4C 4C 59	TYCguydpQR.1yLLY
000000C0002040A6	4F 64 47 2F 46 4E 64 42 77 4F 62 4C 6B 69 7A 45	OdG/FNdBwObLkizE
000000C0002040B6	4B 70 53 77 50 59 59 68 35 38 68 57 51 2F 61 4F	KpSwPYYh58hWQ/aO
000000C0002040C6	6E 49 67 37 74 52 6F 43 53 58 48 32 74 62 38 76	nIg7tRoCSXH2tb8v
000000C0002040D6	71 6C 5A 70 55 53 31 50 42 56 61 0A 41 41 62 32	qlZpUS1PBVa.AAb2
000000C0002040E6	56 57 71 2F 68 7A 64 33 54 34 62 35 45 30 73 36	VWq/hzd3T4b5E0s6
000000C0002040F6	64 71 4C 76 6F 75 6A 4F 34 53 4E 34 4A 65 53 6E	dqLvoujO4SN4JeSn
000000C000204106	46 70 5A 53 4D 73 53 52 72 4E 32 51 71 49 2B 62	FpZSMsSRrN2QqI+b
000000C000204116	4E 6B 2B 4D 53 6F 6A 76 62 7A 70 4A 0A 4F 68 71	Nk+MSojvbzpJ.Ohq
000000C000204126	6E 35 69 69 45 5A 61 41 50 32 62 78 31 56 52 52	n5iiEZaAP2bx1VRR
000000C000204136	4C 39 78 73 30 78 72 39 35 34 4B 57 32 2B 52 79	L9xs0xr954KW2+Ry
000000C000204146	6A 67 74 74 2B 4B 57 54 71 5A 54 71 4B 58 68 35	jgtt+KWTqZTqKXh5
000000C000204156	41 37 72 37 33 62 41 63 72 5A 2F 4D 77 0A 6B 54	A7r73bAcrZ/Mw.kT
000000C000204166	32 6F 36 75 30 51 62 75 39 52 54 6D 32 41 75 47	2o6u0Qbu9RTm2AuG
000000C000204176	53 50 44 54 47 33 4D 6D 69 48 6D 69 71 70 56 6E	SPDTG3MmiHmiqpVn
000000C000204186	4C 79 6D 41 6E 4C 39 59 46 50 55 56 41 45 6C 70	LymAnL9YFPUVAElp
000000C000204196	41 72 50 71 6E 2F 32 42 69 38 56 64 54 68 0A 65	ArPqn/2Bi8VdTh.e
000000C0002041A6	51 49 44 41 51 41 42 0A 2D 2D 2D 2D 2D 45 4E 44	QIDAQAB.-----END
000000C0002041B6	20 52 53 41 20 50 55 42 4C 49 43 20 4B 45 59 2D	RSA PUBLIC KEY-
000000C0002041C6	2D 2D 2D 0A 00 00 00 00 00 00 00 00 00 00 00 00	----............
000000C0002041D6	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
000000C0002041E6	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
000000C0002041F6	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
000000C000204206	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
000000C000204216	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....

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` ":

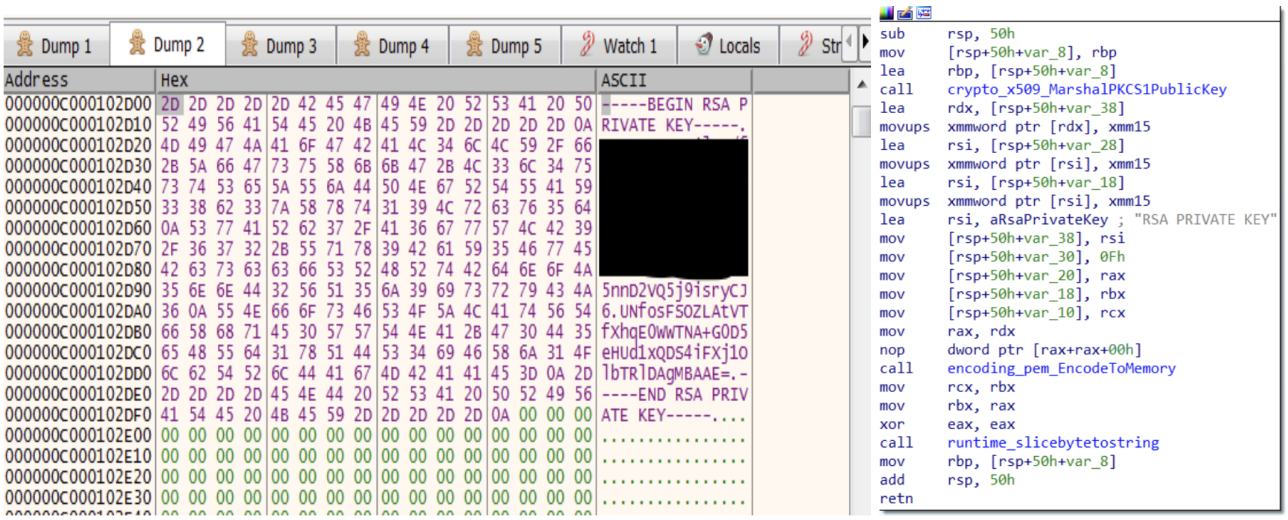


Figure 7. Key generation function (Click to enlarge)

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 “
- “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”
- “service mysql stop”
- “/etc/init.d/mysqld stop”
- “service oracle stop”
- “systemctl disable \”postgresql*\””
- “systemctl disable \”mysql*\””
- “systemctl disable \”oracle*\””

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 • 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	• /bin • /boot • /sbin • /tmp • /etc • /lib • /proc • /dev • /sys • /usr/include • /usr/java

Table 3. TellYouThePass directory exclusions for encryption

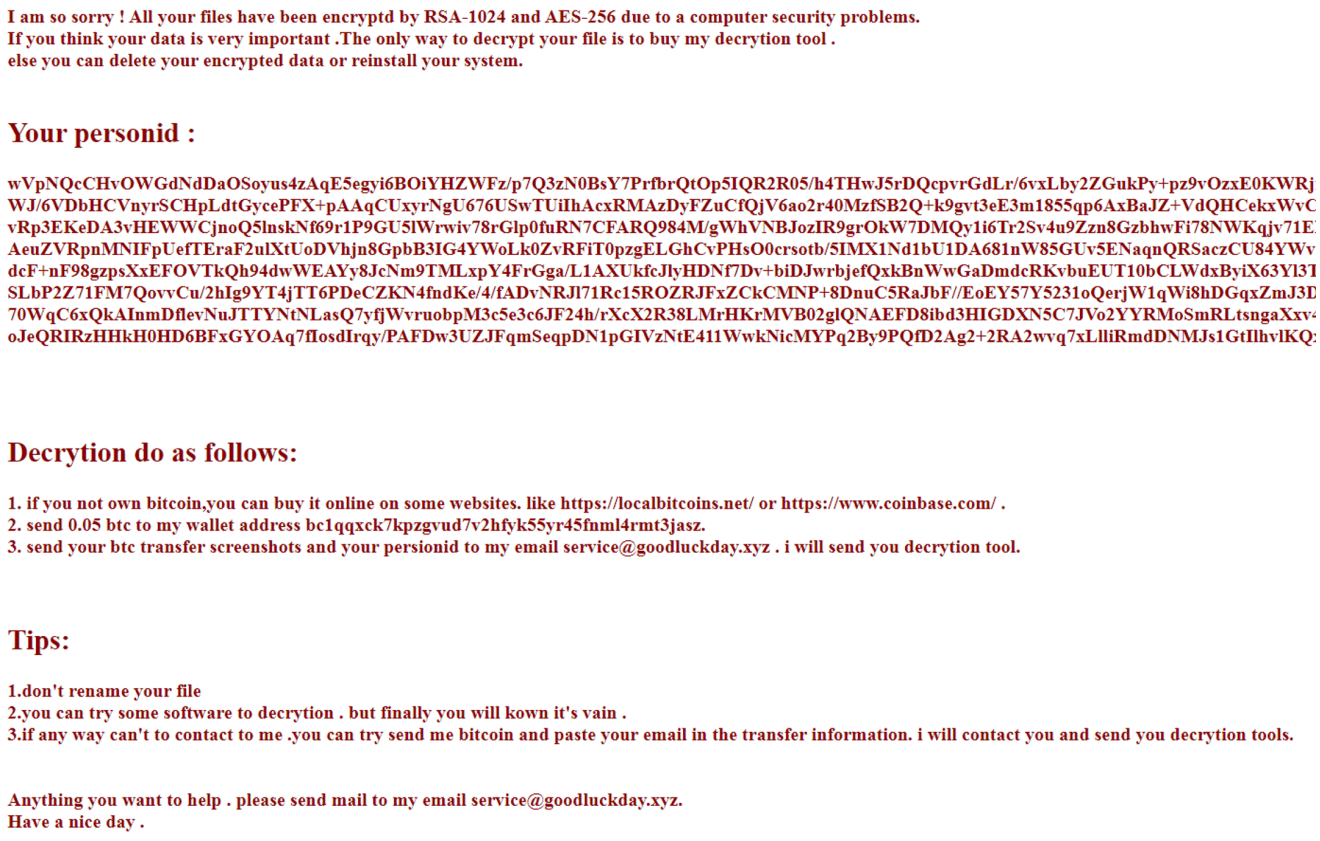
The TellYouThePass ransomware focuses on encrypting popular media and file extensions, saving their paths in the “ `encfile.txt` “ text file, located in the same folder as “ `public.txt` “ and “ `showkey.txt` ”.

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.


I am so sorry ! All your files have been encryptd by RSA-1024 and AES-256 due to a computer security problems.
If you think your data is very important .The only way to decrypt your file is to buy my decrytion tool .
else you can delete your encrypted data or reinstall your system.

Your personid :

wVpNQcCHvOWGdNdDaOSoyus4zAqE5egyi6BOiYHZWFz/p7Q3zN0BsY7PrfbrQtOp5IQR2R05/h4THwJ5rDQcpvrGdLr/6vxLby2ZGukPy+pz9vOzxE0KWRj
WJ/6VDbHCVnyrSCHpLdtGycePFX+pAAqCUxyrNgU676USwTUiIhAcxRMAzDyFZuCfQjV6ao2r40MzfSB2Q+k9gvt3eE3m1855qp6AxBaJZ+VdQHCekxWvC
vRp3EKeDA3vHEWWCjnoQ5lnskNf69r1P9GU5lWrwiv78rGlp0fuRN7CFARQ984M/gWhVNBJozIR9grOkW7DMQy1i6Tr2Sv4u9Zzn8GzbhwFi78NWKqjv71E
AeuZVRpnMNIFpUefTEraF2ulXtUoDVhjn8GpbB3IG4YWoLk0ZvRFiT0pzgELGhCvPHsO0crsotb/5IMX1Nd1bU1DA681nW85GUv5ENaqnQRSaczCU84YWv
dcF+nF98gzpsXxEFOVTkQh94dwWEAYy8JcNm9TMLxpY4FrGga/L1AXUkfcJlyHDNf7Dv+biDJwrbjefQxkBnWwGaDmdcRKvbuEUT10bCLWdxByiX63Yl3T
SLbP2Z71FM7QovvCu/2hIg9YT4jTT6PDeCZKN4fndKe/4/fADvNRJl71Rc15ROZRJFxZCkCMNP+8DnuC5RaJbF//EoEY57Y5231oQerjW1qWi8hDGqxZmJ3D
70WqC6xQkAInmDflevNuJTTYNtNLasQ7yfjWvruobpM3c5e3c6JF24h/rXcX2R38LMrHKrMVB02glQNAEFD8ibd3HIGDXN5C7JVo2YYRMoSmRLtsngaXxv
oJeQRIRzHHkH0HD6BFxGYOAq7flosdIrqy/PAFDw3UZJFqmSeqpDN1pGIVzNtE411WwkNicMYPq2By9PQfD2Ag2+2RA2wvq7xLlliRmdDNMJs1GtIlhvlKQ

Decrytion do as follows:

1. if you not own bitcoin,you can buy it online on some websites. like https://localbitcoins.net/ or https://www.coinbase.com/ .
2. send 0.05 btc to my wallet address bc1qqxck7kpzgvud7v2hfyk55yr45fnml4rmt3jasz.
3. send your btc transfer screenshots and your persionid to my email service@goodluckday.xyz . i will send you decrytion tool.

Tips:

1.don't rename your file
2.you can try some software to decrytion . but finally you will kown it's vain .
3.if any way can't to contact to me .you can try send me bitcoin and paste your email in the transfer information. i will contact you and send you decrytion tools.

Anything you want to help . please send mail to my email service@goodluckday.xyz.
Have a nice day .

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.

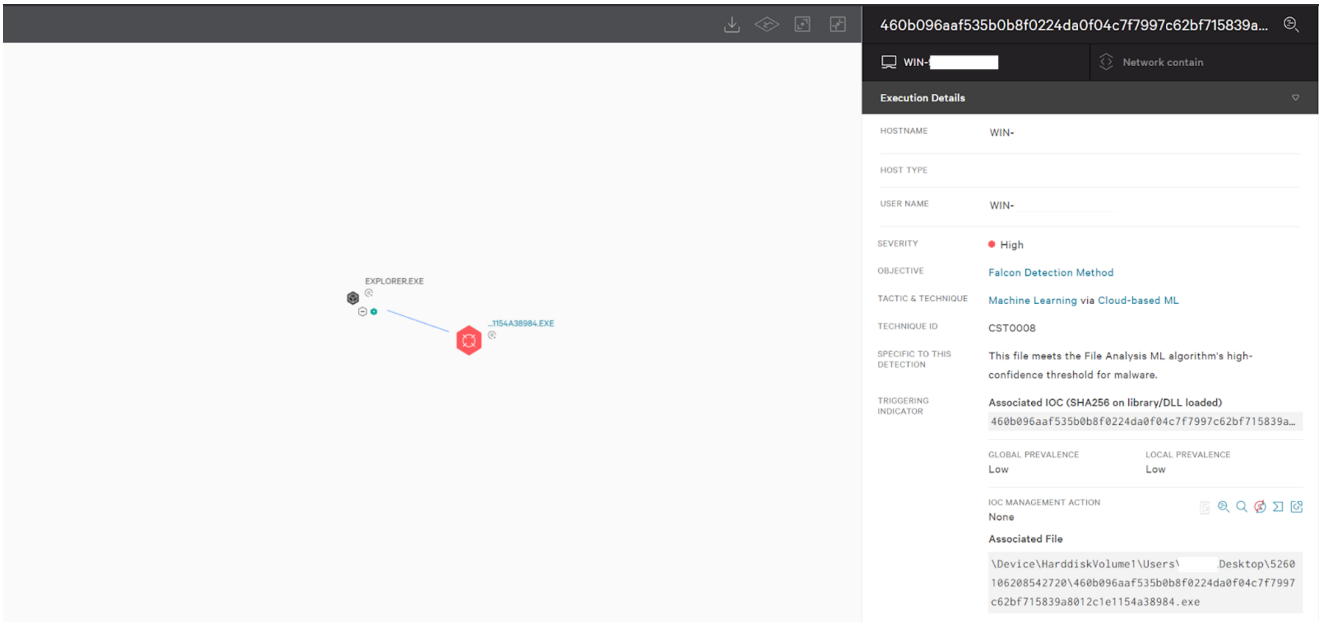


Figure 10. Falcon detection of Golang-written Windows TellYouThePass ransomware sample (Click to enlarge)

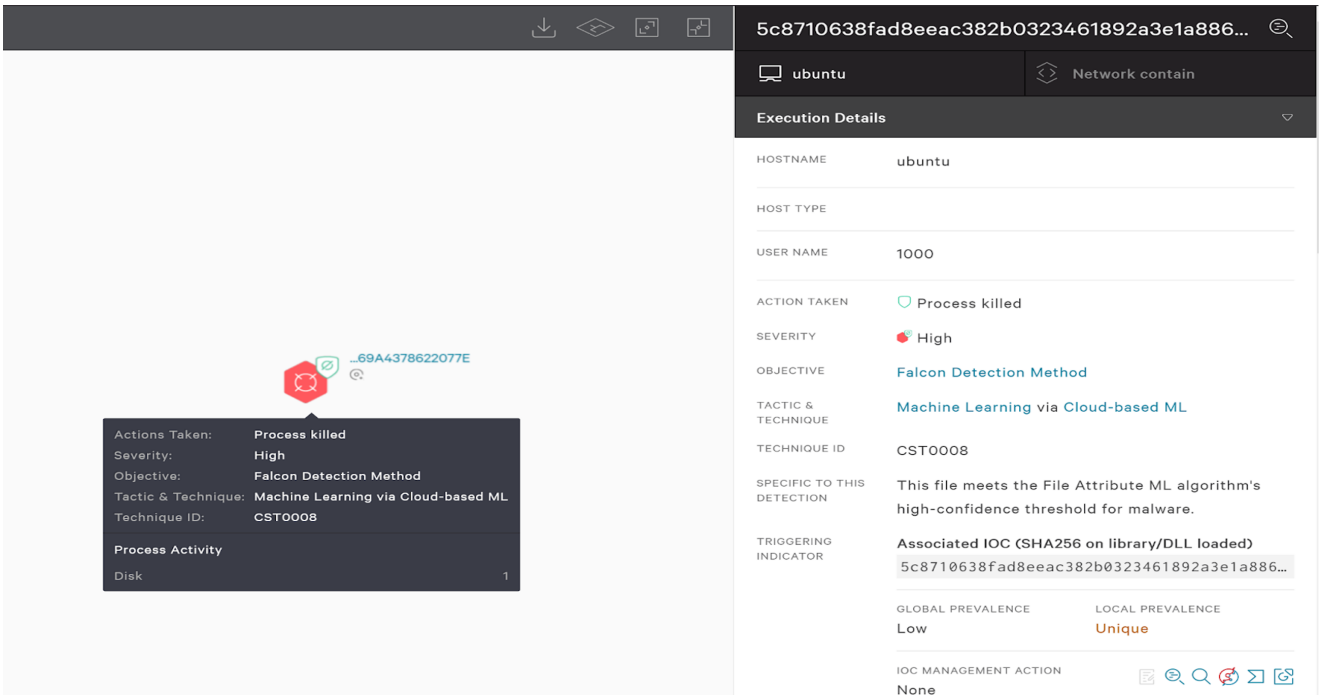


Figure 11. Falcon detection of Golang-written Linux TellYouThePass ransomware sample (Click to enlarge)

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.*