

Rapid 랜섬웨어 분석

목차

1. 개요
 - 1.1 배경
 - 1.2 파일정보
 2. 분석
 - 2.1 Rapid 랜섬웨어 분석
 3. 탐지
 - 3.1 Privacy-i EDR 탐지 정보
 4. 대응
-

1. 개 요

1.1 배 경

Rapid 랜섬웨어는 지난 2018년 초 국내에 소개된 뒤 활발한 활동을 벌이고 있다. Rapid 랜섬웨어의 특징은 일반적인 랜섬웨어와 다르게 암호화 행위가 종료된 뒤에도 지속성을 유지하여 활성화 상태로 암호화 행위를 수행하는 것이다. 즉, 새롭게 생성한 파일도 암호화하며, 지속적으로 암호화에 방해가 되는 프로세스를 종료시켜 감염된 PC의 복구 시도조차 할 수 없도록 한다.

특히 이번에 발견된 Rapid 변종 랜섬웨어는 Rapid 랜섬웨어를 작업 스케줄러(Task scheduler)에 등록하여 복수의 랜섬웨어를 실행한다. 이는 동시다발적인 랜섬웨어 실행과 그에 따른 빠른 속도의 암호화를 가능하게 하며, 한번 실행된 랜섬웨어는 단순히 랜섬웨어 프로세스를 종료하는 방법으론, 이를 종료 & 제어할 수 없도록 한다. 또한 이번 Rapid 변종 랜섬웨어는 VMProtect Packer를 사용하여 신속한 분석을 통해 대응할 수 없도록 개발되었으며, 이는 Anti-Virus 및 EDR 제품을 비롯한 보안 프로그램에서 분석 및 탐지를 어렵게 하기 위함이다. 소만사는 본 보고서를 통해 Rapid 변종 랜섬웨어를 분석하여, 그 행위와 대응 방안을 제공하며 사전에 예방 및 차단할 수 있도록 본 보고서에 상세한 내용을 담았다.

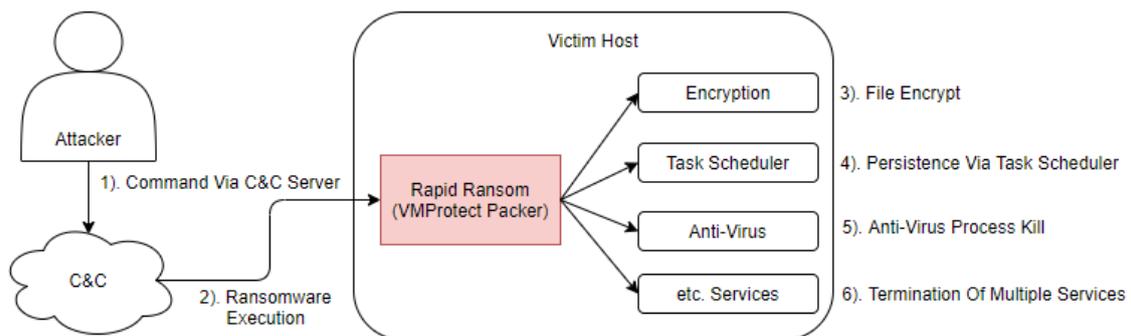
1.2 파일 정보

Name	[random].exe (가칭)
Type	Windows 실행 파일
Behavior	Ransomware
SHA-256	7c0cd587fe7b4ca55534b18ae1e1b45231b054ef58f41642b622e63291b7e35a
Description	Rapid Ransomware

2. 분석

이번에 발견된 Rapid 변종 랜섬웨어는 작업 스케줄러(Task scheduler)에 자가 복제 파일을 등록하여, 지속성을 유지한다. 작업 스케줄러(Task scheduler)를 통해 매분마다 자가 복제본이 실행되어 동시다발적인 암호화 행위가 수행되며, 이러한 이유로 단순히 랜섬웨어 프로세스를 종료하는 방법으로는 랜섬웨어를 중지할 수 없다. 또한 동시다발적 암호화 행위를 통해 PC 내 파일 암호화는 빠른 시간 내에 이루어진다. 이와 더불어 파일 암호화 행위에 방해가 되는 수십 여 가지의 프로세스와 서비스를 종료 및 제거한다.

2.1 Rapid 랜섬웨어 분석



[그림 1] Rapid 랜섬웨어 동작

1). Command Via C&C Server

- 공격자는 Rapid 랜섬웨어를 피해자 호스트 내 침투시킨 후 C&C 서버 명령을 통해 동작을 실행한다.

2). Ransomware Execution

- Rapid 랜섬웨어는 피해자 호스트 내에서 실행되며, 내부적으로 VMProtect Packer가 Unpack 되는 과정을 거쳐 실행된다.

3). Encryption

- Rapid 랜섬웨어는 감염된 PC 내의 파일을 암호화한다.

4). Persistence Via Task Scheduler

- 작업 스케줄러(Task Scheduler)에 Rapid 랜섬웨어를 등록하여 지속성을 유지하고, 동시다발적인 암호화를 가능하게 하여 빠른 속도로 암호화를 진행한다.

5). Anti-Virus Process Kill

- 다수의 Anti-Virus 프로세스를 종료시켜, Anti-Virus로부터 탐지/차단되는 것을 방지한다.

6). Termination Of Multiple Services

- 파일 암호화에 방해가 되는 서비스를 종료시킨다.

Rapid 변종 랜섬웨어는 내부적으로 VMProtect Packer라는 Packing Software를 이용해 압축되어 있는데, 이는 Themida Packer와 더불어 분석가들의 분석을 방해하는 악명높은 Packer이다. Rapid 변종 랜섬웨어는 실행 시 Unpack 과정을 거쳐, 작업 스케줄러(Task Scheduler)에 자가 복제본을 등록하여 지속성 유지 및 동시다발적인 암호화를 수행한다. 작업 스케줄러(Task Scheduler)에 의해 매 분마다 실행되는 Rapid 변종 랜섬웨어는 빠른 속도로 복수의 암호화 행위가 가능하며, 한번 감염이 시작된 PC는 암호화 행위를 중지시키기 어렵다. 또한 다수의 Anti-Virus 및 암호화에 방해가 되는 서비스 및 프로세스들을 종료시킨다.

[표 1] Rapid 변종 랜섬웨어 행위 요약

2.2 VMProtect Packer

00980000	00001000	rapid.exe		IMG	-R---	ERWC-
00981000	00013000	".text"	실행 가능한 코드	IMG	ER---	ERWC-
00994000	00009000	".rdata"	읽기 전용 초기화 데이터	IMG	-R---	ERWC-
0099D000	00005000	".data"	초기화 된 데이터	IMG	-RWC-	ERWC-
009A2000	0031F000	".vmp0"		IMG	ER---	ERWC-
00CC1000	00550000	".vmp1"		IMG	ER---	ERWC-
01211000	00001000	".reloc"	기준 재배치	IMG	-R---	ERWC-

[그림 2] VMProtect Packer 섹션

Rapid 랜섬웨어는 위 사진과 같이 내부적으로 .vmp0 및 .vmp1 섹션을 확인할 수 있으며, 해당 섹션을 통해 Rapid 랜섬웨어가 VMProtect Packer로 Packing되어 있음을 알 수 있다. VMProtect

Packer는 Themida Packer와 같은 악명높은 Packer로서 분석가의 신속한 대응을 어렵게 한다.

2.3. 코드 압축 해제 및 메모리 속성 변경

75745240	8BFF	mov edi,edi	WriteProcessMemory
75745242	55	push ebp	
75745243	8BEC	mov ebp,esp	
75745245	5D	pop ebp	
75745246	FF25 78137975	jmp dword ptr ds:[<&WriteProcessMemory>]	JMP.&WriteProcessMemory
7574524C	CC	int3	
7574524D	CC	int3	
7574524E	CC	int3	
757304C0	8BFF	mov edi,edi	VirtualProtect
757304C2	55	push ebp	
757304C3	8BEC	mov ebp,esp	
757304C5	5D	pop ebp	
757304C6	FF25 90137975	jmp dword ptr ds:[<&VirtualProtect>]	JMP.&VirtualProtect
757304CC	CC	int3	
757304CD	CC	int3	
757304CE	CC	int3	
757304CF	CC	int3	
757304D0	CC	int3	

[그림 3] 압축된 코드 적재 및 압축 해제 과정

Rapid 랜섬웨어는 VMProtect Packer의 Unpacking과정에서, WriteProcessMemory API 호출을 통해 메모리 내, 수 번의 압축된 코드를 적재하고 이를 다시 압축 해제하는 과정을 반복한다. 이러한 과정을 통해 압축된 코드는 메모리 내 특정 영역에 압축이 해제되며, VirtualProtect API 호출을 마지막으로 실행 가능한 메모리 영역으로 변경되어 랜섬웨어로서 악의적인 행위를 수행할 수 있게 된다.

009838D7	B9 34A89900	mov ecx,rapid.99A834	99A834:"msftesql.exe"
009838DC	E8 3FEFFFFF	call rapid.983720	
009838E1	B9 44A89900	mov ecx,rapid.99A844	99A844:"sqlagent.exe"
009838E6	E8 35FEFFFF	call rapid.983720	
009838EB	B9 54A89900	mov ecx,rapid.99A854	99A854:"sqlbrowser.exe"
009838F0	E8 2BFEFFFF	call rapid.983720	
009838F5	B9 64A89900	mov ecx,rapid.99A864	99A864:"sqlservr.exe"
009838FA	E8 21FEFFFF	call rapid.983720	
009838FF	B9 74A89900	mov ecx,rapid.99A874	99A874:"sqlwriter.exe"
00983904	E8 17FEFFFF	call rapid.983720	
00983909	B9 84A89900	mov ecx,rapid.99A884	99A884:"oracle.exe"

[그림 4] 압축 해제된 코드 (대상 프로세스 종료 로직)

소만사는 자체 기술로 VMProtect Packer를 Unpacking하여, 위와 같이 압축이 해제된 Rapid 변종 랜섬웨어의 코드를 확인하였다. 해당 코드를 통해 자가 복제본을 작업 스케줄러(Task Scheduler)에 등록하여 지속성을 유지하는 방법과 동시다발적인 실행으로 빠른 속도의 암호화를 수행하는 과정 및 어떠한 프로세스 및 서비스를 대상으로 종료하는지, 추가적으로 시스템을 복구 불가하도록 설정하는 과정 등의 악의적인 행위를 파악하였다.

VMProtect Packer란?

VMProtect Packer에 대한 설명에 앞서, Packing이란 기술은 난독화 기술로서 프로그램의 기능성은 그대로 유지하면서 자료구조, 제어 흐름 등 내부 로직을 복잡하게 변형함으로써 프로그램의 분석을 지연시키는 기술이다. VMProtect Packer는 이러한 Packing을 자동화한 상용 제품이다. VMProtect Packer는 Themida Packer와 더불어 코드 난독화 기술에 있어 악명 높은 Packer이며, 본래 목적은 코드의 역분석을 방지하기 위해 개발되었지만 악성코드 제작자들이 악성코드 분석 방지를 목적으로 사용한다.

[표 2] VMProtect Packer

2.4. 주요 프로세스 및 서비스 종료

009838D7	B9 34A89900	mov ecx,rapid.99A834	99A834: "msftesql.exe"
009838DC	E8 3FFEFFFF	call rapid.983720	
009838E1	B9 44A89900	mov ecx,rapid.99A844	99A844: "sqlagent.exe"
009838E6	E8 35FEFFFF	call rapid.983720	
009838EB	B9 54A89900	mov ecx,rapid.99A854	99A854: "sqlbrowser.exe"
009838F0	E8 2BFEFFFF	call rapid.983720	
009838F5	B9 64A89900	mov ecx,rapid.99A864	99A864: "sqlservr.exe"
009838FA	E8 21FEFFFF	call rapid.983720	
009838FF	B9 74A89900	mov ecx,rapid.99A874	99A874: "sqlwriter.exe"
00983904	E8 17FEFFFF	call rapid.983720	
00983909	B9 84A89900	mov ecx,rapid.99A884	99A884: "oracle.exe"

75C59DF0	8BFF	mov edi,edi	ShellExecuteA
75C59DF2	55	push ebp	
75C59DF3	8BEC	mov ebp,esp	
75C59DF5	83EC 3C	sub esp,3C	
75C59DF8	8B45 08	mov eax,dword ptr ss:[ebp+8]	
75C59DFB	8945 CC	mov dword ptr ss:[ebp-34],eax	
75C59DFE	8B45 0C	mov eax,dword ptr ss:[ebp+C]	
75C59E01	8945 D0	mov dword ptr ss:[ebp-30],eax	
75C59E04	8B45 10	mov eax,dword ptr ss:[ebp+10]	
75C59E07	8945 D4	mov dword ptr ss:[ebp-2C],eax	
75C59E0A	8B45 14	mov eax,dword ptr ss:[ebp+14]	
75C59E0D	56	push esi	
75C59E0E	57	push edi	
75C59E0F	8945 D8	mov dword ptr ss:[ebp-28],eax	[ebp-28]:L"C:\\Users
75C59E12	8D7D E4	lea edi,dword ptr ss:[ebp-1C]	
75C59E15	8B45 18	mov eax,dword ptr ss:[ebp+18]	
75C59E18	BE 00140000	mov esi,1400	
75C59E1D	8945 DC	mov dword ptr ss:[ebp-24],eax	
75C59E20	8B45 1C	mov eax,dword ptr ss:[ebp+1C]	[ebp+1C]:EntryPoint

0053FD10	00999CB0	"open"
0053FD14	00999CA8	"cmd.exe"
0053FD18	00999CB8	"rem Delite Service \"Hyper-V\""

[그림 5] 주요 프로세스 및 서비스 종료

Rapid 랜섬웨어는 암호화에 앞서, 이미 사용 중인 파일의 핸들 획득 시도 시 충돌이 발생하는 등의 상황을 방지하기 위해 파일 암호화에 방해가 되는 주요 프로세스들을 종료시킨다. 이는 ShellExecuteA API 호출을 통해 cmd.exe를 실행하여 진행되며, 주요 종료 대상 프로세스의 목록은 다음과 같다.

msftesql.exe
sqlagent.exe
sqlbrowser.exe
sqlservr.exe
sqlwriter.exe
oracle.exe
ocssd.exe
dbsnmp.exe
synctime.exe
mydesktopqos.exe
agntsvc.exe
isqlplussvc.exe
xfssvcon.exe
mydesktopservice.exe
ocautoupds.exe
encsvc.exe
firefoxconfig.exe
tbirdconfig.exe
ocomm.exe
mysqld.exe
mysqld-nt.exe
mysqld-opt.exe
dbeng50.exe
sqbcoreservice.exe
excel.exe
infopath.exe
msaccess.exe
mspub.exe
onenote.exe
outlook.exe
powerpnt.exe
steam.exe
thebat.exe
thebat64.exe
thunderbird.exe
visio.exe
winword.exe
wordpad.exe
taskmgr.exe

[표 3] 종료 대상 프로세스

Malware Analysis Report

No.24 | 2021년 04월

또한, sc delete * 및 REM Delite Service * 명령을 통해 주요 Anti-Virus 서비스 등을 제거하는데 그 목록은 다음과 같다. REM Delite Service * 명령은 배치 파일 등에 사용되는 명령으로, 해당 명령을 통해서도 지정된 서비스를 제거할 수 있다.

Hyper-V
vmickvpexchange
vmicguestinterface
vmicshutdown
vmicheartbeat
vmicrdv
Storflt
vmictimesync
vmicvss
SQL
MSSQLFDLauncher
MSSQLSERVER
SQLSERVERAGENT
SQLBrowser
SQLTELEMETRY
MsDtsServer130
SSISTELEMETRY130
SQLWriter
MSSQL\$VEEAMSQL2012
SQLAgent\$VEEAMSQL2012
MSSQL
SQLAgent
MSSQLServerADHelper100
MSSQLServerOLAPService
MsDtsServer100
ReportServer
SQLTELEMETRY\$HL
TMBMServer
MSSQL\$PROGID
MSSQL\$WOLTERSKLWUER
SQLAgent\$PROGID
SQLAgent\$WOLTERSKLWUER
MSSQLFDLauncher\$OPTIMA
MSSQL\$OPTIMA
SQLAgent\$OPTIMA
ReportServer\$OPTIMA
msftesql\$SQLEXPRESS
postgresql-x64-9.4
AV: ESET
ekrn
AV: Kaspersky

klm6
AVP18.0.0
KLIF
Klpd
klflt
klbackupdisk
klbackupflt
klkbfift
klmouflt
klhk
KSDE1.0.0
kltap
AV: Trend Micro
TmFilter
TMLWCSService
tmusa
TmPreFilter
TMSmartRelayService
TMiCRCScanService
VSApiNt
TmCCSF
tmlisten
TmProxy
ntrtscan
ofcservice
UniFi

[표 4] 제거 대상 서비스

▼ Rapid.exe	8052	6.14 MB	DES...#JeongGeonWoo
▼ C:\cmd.exe	4908	3.39 MB	DES...#JeongGeonWoo
C:\conhost.exe	1180	6.54 MB	DES...#JeongGeonWoo
▼ C:\cmd.exe	988	2.34 MB	DES...#JeongGeonWoo
C:\conhost.exe	7540	6.5 MB	DES...#JeongGeonWoo
▼ C:\cmd.exe	7992	2.33 MB	DES...#JeongGeonWoo
C:\conhost.exe	6180	6.5 MB	DES...#JeongGeonWoo
▼ C:\cmd.exe	3272	2.33 MB	DES...#JeongGeonWoo
C:\conhost.exe	4668	6.53 MB	DES...#JeongGeonWoo

[그림 6] 프로세스 및 서비스 종료 & 제거

Rapid 랜섬웨어는 위와 같이 총 39개의 프로세스를 종료하며, 67개의 서비스를 제거한다. 해당 작업은 Rapid 랜섬웨어의 자식 프로세스로 cmd.exe가 실행되어, 수많은 명령이 일괄 처리되며 수

행된다.

2.5. 볼륨 웨도우 삭제 및 복구 모드 불가 설정

00983B6C	6A 00	push 0	
00983B6E	6A 00	push 0	
00983B70	68 80AA9900	push rapid.99AAB0	99AAB0:"/c vssadmin.exe Delete Shadows /All /Quiet"
00983B75	68 A89C9900	push rapid.999CA8	999CA8:"cmd.exe"
00983B7A	68 809C9900	push rapid.999CB0	999CB0:"open"
00983B7F	6A 00	push 0	
00983B81	FFD6	call esi	
00983B83	6A 00	push 0	
00983B85	6A 00	push 0	
00983B87	68 DCAA9900	push rapid.99AADC	99AADC:"/c bcdedit.exe /set {default} recoveryenabled No"
00983B8C	68 A89C9900	push rapid.999CA8	999CA8:"cmd.exe"
00983B91	68 809C9900	push rapid.999CB0	999CB0:"open"
00983B96	6A 00	push 0	
00983B98	FFD6	call esi	
00983B9A	6A 00	push 0	
00983B9C	6A 00	push 0	
00983B9E	68 10AB9900	push rapid.99AB10	99AB10:"/c bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures"
00983BA3	68 A89C9900	push rapid.999CA8	999CA8:"cmd.exe"
00983BA8	68 809C9900	push rapid.999CB0	999CB0:"open"
00983BAD	6A 00	push 0	
00983BAF	FFD6	call esi	
75C59DF0	8BFF	mov edi,edi	ShellExecuteA
75C59DF2	55	push ebp	
75C59DF3	8BEC	mov ebp,esp	
75C59DF5	83EC 3C	sub esp,3C	
75C59DF8	8B45 08	mov eax,dword ptr ss:[ebp+8]	
75C59DFB	8945 CC	mov dword ptr ss:[ebp-34],eax	
75C59DFE	8B45 0C	mov eax,dword ptr ss:[ebp+C]	
75C59E01	8945 D0	mov dword ptr ss:[ebp-30],eax	
75C59E04	8B45 10	mov eax,dword ptr ss:[ebp+10]	
75C59E07	8945 D4	mov dword ptr ss:[ebp-2C],eax	
0096FC60	00000000		
0096FC64	00999CB0	"open"	
0096FC68	00999CA8	"cmd.exe"	
0096FC6C	0099AB10	"/c bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures"	

[그림 7] 볼륨 웨도우 복사본 삭제 및 복구 모드 불가 설정

주요 프로세스 종료 후 시스템의 복원을 불가능하게 하기 위해 볼륨 웨도우 복사본 삭제 및 복구 모드 불가 설정을 수행한다. 해당 행위도 이전의 주요 프로세스 종료 시와 마찬가지로 ShellExecuteA API 호출을 통해 cmd.exe를 실행하여 수행된다. 이를 수행하는 주요 명령은 다음과 같다.

```
cmd.exe /c vssadmin.exe Delete Shadows /All /Quiet
cmd.exe /c bcdedit.exe /set {default} recoveryenabled No
cmd.exe /c bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
cmd.exe /c wadmin DELETE SYSTEMSTATEBACKUP
cmd.exe /c wmic SHADOWCOPY DELETE
wmic.exe SHADOWCOPY DELETE
```

2.6. 동시다발적인 암호화 행위를 위한 작업 스케줄러(Task Scheduler) 등록

```

00981230 55          push ebp
00981231 8BEC       mov ebp,esp
00981233 83EC 0C   sub esp,C
00981236 8BC1     mov eax,ecx
00981238 8955 F4   mov dword ptr ss:[ebp-C],edx
00981238 53       push ebx
0098123C 33DB     xor ebx,ebx
0098123E 8945 F8   mov dword ptr ss:[ebp-8],eax
00981241 56       push esi
00981242 57       push edi
00981243 3818     cmp byte ptr ds:[eax],b1
00981245 74 07    je rapid.98124E
00981247 43       inc ebx
00981248 803C03 00   cmp byte ptr ds:[ebx+eax],0
0098124C 75 F9    jne rapid.981247
    
```

```

0096FC5C 00983C21 rapid.00983C21로 변환 (출발: ???)
0096FC60 00000000
0096FC64 00999C80 "open"
0096FC68 0099ABF0 "SCHTASKS"
0096FC6C 0177C638 "/Create /SC MINUTE /TN Encrypiter /TR C:\\Users\\JeongGeonWoo\\AppData\\Roaming\\nopusana.exe"
0096FC70 00000000
0096FC74 00000000
0096FC78 00000000
0096FC7C 0000000A
0096FC80 015E8000
    
```

이름	상태	트리거
Encrypiter	준비	2021-04-05 오후 9:05에 - 트리거된 후 무기한으로 00:01:00마다 반복합니다.

작업을 만들 경우 작업이 시작될 때 발생하는 동작을 지정해야 합니다. 이 동작을 변경하려면 [속성] 명령을 사용하여 작업 :

작업	자세히
프로그램 시작	C:\Users\JeongGeonWoo\AppData\Roaming\nopusana.exe

[그림 8] 작업 스케줄러(Task Scheduler) 등록

ShellExecuteA API 호출을 통해 cmd.exe를 실행하여 작업 스케줄러(Task Scheduler)에 앞으로 복제할 자가 복제본을 예약작업으로 등록한다. 해당 작업은 매분마다 무기한으로 자가 복제된 Rapid 변종 랜섬웨어를 실행하며, 동시다발적으로 랜섬 행위를 수행한다. 복제본을 등록하는 명령은 다음과 같다.

```

SCHTASKS /Create /SC MINUTE /TN Encrypiter /TR
C:#Users#[User]#AppData#Roaming#[Copy].exe
    
```

2.7. 재부팅 시 지속성을 위한 작업 스케줄러(Task Scheduler) 등록

이름	상태	트리거
Encrypiter	준비	2021-04-05 오후 9:05에 - 트리거된 후 무기한으로 00:01:00마다 반복합니다.
EncrypiterSt	준비	사용자가 로그인할 때

일반	트리거	동작	조건	설정	기록(사용 안 함)
작업을 만들 경우 작업이 시작될 때 발생하는 동작을 지정해야 합니다. 이 동작을 변경하려면 [속성] 명령을 사용하여 작업					
작업	자세히				
프로그램 시작	C:\Users\JeongGeonWoo\AppData\Roaming\noputana.exe				

[그림 9] 예약 작업으로 등록된 Rapid 변종 랜섬웨어

추가적으로 Rapid 변종 랜섬웨어는 예약 작업을 한번 더 수행하는데, 재부팅 시 로그인 할 때마다 실행될 수 있도록 다시 한번 예약 작업을 등록한다. 해당 명령은 다음과 같다.

```
SCHTASKS /Create /SC ONLOGON /TN EncrypiterSt /TR
C:\Users\%User%\AppData\Roaming\%Copy%.exe
```

2.8. 재부팅 시 지속성을 위한 레지스트리 등록

75904490	8BFF	mov edi,edi	RegOpenKeyExA
75904492	55	push ebp	
75904493	8BEC	mov ebp,esp	
75904495	51	push ecx	
75904496	6A 00	push 0	
75904498	FF75 18	push dword ptr ss:[ebp+18]	
7590449B	FF75 14	push dword ptr ss:[ebp+14]	
7590449E	FF75 10	push dword ptr ss:[ebp+10]	
759044A1	FF75 0C	push dword ptr ss:[ebp+C]	[ebp+C]: "Software\Microsoft\Windows\CurrentVersion\Run"
759044A4	FF75 08	push dword ptr ss:[ebp+8]	
759044A7	E8 14000000	call <kernelbase.RegOpenKeyExInternalA>	
759044AC	59	pop ecx	
759044AD	5D	pop ebp	
759044AE	C2 1400	ret 14	

758F5BC0	6A 38	push 38	RegSetValueExA
758F5BC2	68 08589C75	push kernelbase.759C5808	
758F5BC7	E8 C0E20300	call kernelbase.75933E8C	
758F5BCC	33DB	xor ebx,ebx	
758F5BCE	895D DC	mov dword ptr ss:[ebp-24],ebx	[ebp-24]: "C:\\Users\\J"
758F5BD1	895D D8	mov dword ptr ss:[ebp-28],ebx	[ebp-28]: L"C:\\Users\\"
758F5BD4	895D D0	mov dword ptr ss:[ebp-30],ebx	
758F5BD7	895D D4	mov dword ptr ss:[ebp-2C],ebx	
758F5BDA	817D 08 04000080	cmp dword ptr ss:[ebp+8],80000004	
758F5BE1	✓ 0F84 B10D0400	je kernelbase.75936998	
758F5BE7	395D 10	cmp dword ptr ss:[ebp+10],ebx	
758F5BEA	✓ 0F85 AC0D0400	jne kernelbase.7593699C	

0096FC5C	00983CD8	rapid.00983CD8로 반환 (출발: ???)
0096FC60	000005D0	
0096FC64	0099A820	"HelloAV"
0096FC68	00000000	
0096FC6C	00000001	
0096FC70	01763638	"C:\\Users\\JeongGeonWoo\\AppData\\Roaming\\nopotana.exe"
0096FC74	000000FF	
0096FC78	00000000	
0096FC5C	00983D46	rapid.00983D46로 반환 (출발: ???)
0096FC60	000005E0	
0096FC64	0099A828	"welcomeBack"
0096FC68	00000000	
0096FC6C	00000001	
0096FC70	017737F8	"C:\\Users\\JeongGeonWoo\\AppData\\Roaming\\putana.txt"

[그림 10] 재부팅 시 지속성을 위한 레지스트리 등록

RegOpenKeyExA 및 RegSetValueExA API 호출을 통해 HelloAV라는 이름으로 향후 자가 복제될 Rapid 변종 랜섬웨어를 등록한다. 이는 HKEY_LOCAL_MACHINE 경로 및 HKEY_CURRENT_USER 경로에 두 번 수행되며, 재부팅 시 자동 시작으로 Rapid 변종 랜섬웨어는 동작할 수 있다. 이와 더불어 텍스트 파일로 위장하여 자가 복제한 또 다른 putana.txt 이라는 파일을 WelcomeBack이라는 이름으로 등록하여 동시다발적인 랜섬 행위를 수행할 수 있도록 한다.

2.9. 임의의 경로에 자가 복제

00983BF6	6A 00	push 0	
00983BF8	6A 00	push 0	
00983BFA	BA B8AB9900	mov edx,rapid.99AB88	edx:"\\nopotana.exe", 99AB88:"\\nopotana.exe"
00983BFF	8BCB	mov ecx,ebx	ebx:"C:\\Users\\JeongGeonWoo\\AppData\\Roaming\\nopotana.txt"
00983C01	E8 2AD6FFFF	call rapid.981230	CopyFileExw
00983C06	8BD0	mov edx,eax	edx:"\\nopotana.exe", eax:"C:\\Users\\JeongGeonWoo\\AppData\\Roaming\\nopotana.txt"
75728B60	8BFF	mov edi,edi	CopyFileA
75728B62	55	push ebp	
75728B63	8BEC	mov ebp,esp	
75728B65	83EC 10	sub esp,10	
75728B68	8D45 F0	lea eax,dword ptr ss:[ebp-10]	
75728B6B	FF75 08	push dword ptr ss:[ebp+8]	[ebp+8]:"C:\\Users\\JeongGeonWoo\\AppData\\Roaming\\nopotana.txt"
75728B6E	50	push eax	
75728B6F	E8 FC680000	call <kernel32.Basep8BitStringToDynamicUnicode>	
75728B74	85C0	test eax,eax	
75728B76	74 48	je kernel32.75728BC0	
75728B78	56	push esi	esi:"C:\\Users\\JeongGeonWoo\\AppData\\Roaming\\nopotana.txt"
75728B79	FF75 0C	push dword ptr ss:[ebp+C]	[ebp+C]:"C:\\Users\\JeongGeonWoo\\AppData\\Roaming\\nopotana.txt"

[그림 11] 임의의 경로에 자가 복제

Rapid 변종 랜섬웨어는 작업 스케줄러(Task Scheduler)로 자가 복제본이 실행되기 전, 이전에 등록된 경로에 자가 복제를 수행한다. 해당 작업 후 작업 스케줄러(Task Scheduler)에 의해 자가 복제본은 실행되어, 지속성 유지 작업 및 동시다발적인 암호화가 수행된다. 자가 복제는 CopyFileA API 호출을 통해 이루어지며, C:\\Users\\[User]\\AppData\\Roaming* 경로에 자가 복제가 수행된다.

2.10. 레지스트리 내 암호화 키 정보 생성

754A2980	8BFF	mov edi,edi	RegCreateKeyA
754A2982	55	push ebp	
754A2983	8BEC	mov ebp,esp	
754A2985	8B4D 10	mov ecx,dword ptr ss:[ebp+10]	
754A2988	85C9	test ecx,ecx	
754A298A	74 2F	je advapi32.754A298B	
754A298C	8B45 0C	mov eax,dword ptr ss:[ebp+C]	
754A298F	85C0	test eax,eax	
754A2991	0F84 E6E70000	je advapi32.7548117D	
754A2997	8038 00	cmp byte ptr ds:[eax],0	
754A299A	0F84 DDE70000	je advapi32.7548117D	
0096FC30	0096FC70		
0096FC34	0098147C	rapid.0098147C	
0096FC38	80000001		
0096FC3C	009995C8	"Software\\EncryptKeys"	
0096FC40	0096FC64		
0096FC44	0176ABF8		
0096FC48	7549F9A0	advapi32.7549F9A0	
0096FC4C	0174C298	"tl"	

[그림 12] 레지스트리 내 암호화 키 정보 생성

HKEY_CURRENT_USER\Software\EncryptKeys 경로로 레지스트리 키를 생성한다. 해당 키에는 향후 암호화에 사용될 키 정보가 담기게 된다.

2.11. 레지스트리 내 암호화 키 값 등록

758F5BC0	6A 38	push 38	RegSetValueExA
758F5BC2	68 08589C75	push kernelbase.759C5808	
758F5BC7	E8 C0E20300	call kernelbase.75933E8C	
758F5BCC	33DB	xor ebx,ebx	
758F5BCE	895D DC	mov dword ptr ss:[ebp-24],ebx	[ebp-24]:"1024"
758F5BD1	895D D8	mov dword ptr ss:[ebp-28],ebx	
758F5BD4	895D D0	mov dword ptr ss:[ebp-30],ebx	[ebp-30]:"local_enc_privat
758F5BD7	895D D4	mov dword ptr ss:[ebp-2C],ebx	
758F5BDA	817D 08 04000080	cmp dword ptr ss:[ebp+8],80000004	[ebp+8]:"local_enc_private
758F5BE1	0F84 B10D0400	je kernelbase.75936998	
0096FBCC	00982067	rapid.00982067로 반환 (출발: ???)	
0096FBD0	00000760		
0096FBD4	009995E0	"local_enc_private_key"	
0096FBD8	00000000		
0096FBDC	00000003		
0096FBE0	0175E588		

[그림 13] 레지스트리 내 개인키 등록

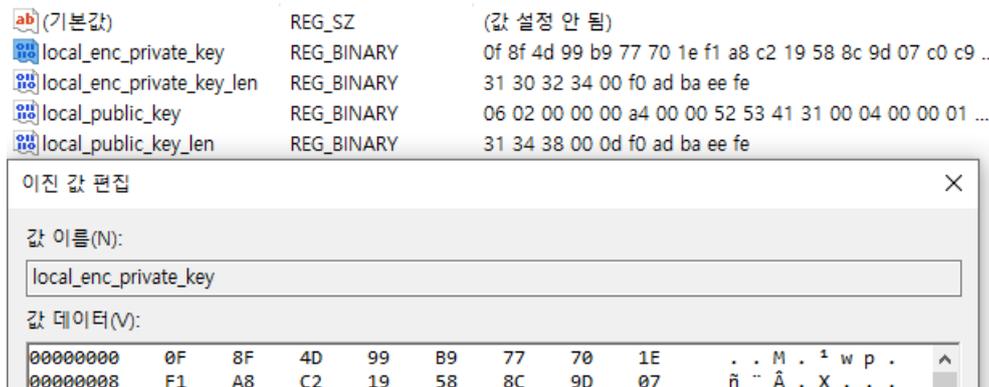
758F5BC0	6A 38	push 38	RegSetValueExA
758F5BC2	68 08589C75	push kernelbase.759C5808	
758F5BC7	E8 C0E20300	call kernelbase.75933E8C	
758F5BCC	33DB	xor ebx,ebx	
758F5BCE	895D DC	mov dword ptr ss:[ebp-24],ebx	[ebp-24]:"148"
758F5BD1	895D D8	mov dword ptr ss:[ebp-28],ebx	
758F5BD4	895D D0	mov dword ptr ss:[ebp-30],ebx	[ebp-30]:"local_
758F5BD7	895D D4	mov dword ptr ss:[ebp-2C],ebx	
758F5BDA	817D 08 04000080	cmp dword ptr ss:[ebp+8],80000004	[ebp+8]:"local_
758F5BE1	0F84 B10D0400	je kernelbase.75936998	
0096FBCC	00982067	rapid.00982067로 반환 (출발: ???)	
0096FBD0	000003B4		
0096FBD4	009995F8	"local_public_key"	
0096FBD8	00000000		
0096FBDC	00000003		

[그림 14] 레지스트리 내 공유키 등록

이전에 만든 HKEY_CURRENT_USER\Software\EncryptKeys 경로로 local_enc_private_len이라는 값을 생성한다. 이는 1024라는 데이터를 갖게 되며, 로컬 암호화 키의 길이를 저장하고 있다. 또

한 이후 local_enc_private 및 local_enc_public_key_len 및 local_enc_public_key 값을 등록하게 되는데 이는 향후 암호화에 사용될 개인키 및 공유키의 길이와 값을 등록하는 행위이다.

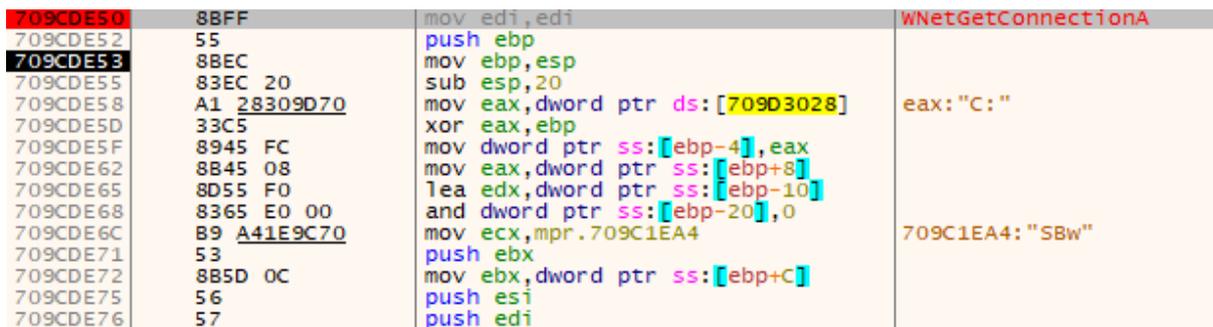
2.12. 레지스트리 내 암호화 키 등록



[그림 15] 레지스트리 내 암호화 키 등록

이전의 키 등록 행위로, 위와 같이 HKEY_CURRENT_USER\Software\EncryptKeys 경로에 개인키의 길이와 키 값, 공개키의 길이와 값을 저장한다.

2.13. 공유 폴더 탐색



[그림 16] 공유 폴더 탐색

WNetGetConnectionA API 호출을 통해 연결되어 있는 공유 폴더를 탐색하고, 연결된 공유 폴더가 확인될 시 해당 경로 또한 암호화를 진행한다.

2.14. 암호화 수행

759122D0	8BFF	mov edi,edi	FindFirstFileExW
759122D2	55	push ebp	
759122D3	8BEC	mov ebp,esp	
759122D5	83E4 F8	and esp,FFFFFFF8	
759122D8	81EC CC020000	sub esp,2CC	
759122DE	A1 308B9D75	mov eax,dword ptr ds:[759D8B30]	
759122E3	33C4	xor eax,esp	
759122E5	898424 C8020000	mov dword ptr ss:[esp+2C8],eax	
759122EC	837D 0C 02	cmp dword ptr ss:[ebp+C],2	
759122F0	8845 14	mov eax,dword ptr ss:[ebp+14]	
759122F3	53	push ebx	ebx:L"D:**"
759122F4	56	push esi	[ebp+8]: "D:\\\\"
759122F5	8B75 08	mov esi,dword ptr ss:[ebp+8]	
759122F8	57	push edi	
759122F9	8B7D 10	mov edi,dword ptr ss:[ebp+10]	
759122FC	897C24 44	mov dword ptr ss:[esp+44],edi	
75912300	0F8D 79000300	jge kernelbase.7594237F	

[그림 17] 암호화 수행

FindFirstFileExW 및 FindNextFileExW API 호출을 통해 드라이브 내 파일 목록을 획득하고 암호화를 수행한다.

2.15. 동시다발적 암호화 진행

svchost.exe	2068	6.23 MB	NT AUTHORITY\SYSTEM	Host Pr
taskhostw.exe	5332	8.87 MB	DES...#JeongGeonWoo	Window
noputana.exe	7736	6.27 MB	DES...#JeongGeonWoo	
cmd.exe	1764	4.37 MB	DES...#JeongGeonWoo	Window
conhost.exe	7628	6.55 MB	DES...#JeongGeonWoo	콘솔 창
cmd.exe	7124	4.37 MB	DES...#JeongGeonWoo	Window
conhost.exe	4148	6.55 MB	DES...#JeongGeonWoo	콘솔 창
cmd.exe	9724	4.38 MB	DES...#JeongGeonWoo	Window
conhost.exe	8972	6.57 MB	DES...#JeongGeonWoo	콘솔 창
cmd.exe	2772	4.37 MB	DES...#JeongGeonWoo	Window
conhost.exe	2288	6.55 MB	DES...#JeongGeonWoo	콘솔 창

[그림 18] 동시다발적 암호화 진행

이전에 등록한 작업 스케줄러(Task Scheduler) 예약 작업을 통해 매분마다 Rapid 변종 랜섬웨어가 실행되며, 기존에 실행되고 있던 Rapid 변종 랜섬웨어 또한 암호화를 진행한다. 이를 통해 빠른 속도의 암호화가 동시다발적으로 진행된다.

2.16. 암호화 확장자 및 랜섬노트

!!!_FILES_RECOVERY.txt	2021-04-05 오후 10:04	텍스트 문서	2KB
34214AKD7S.lock	2021-04-05 오후 10:04	LOCK 파일	5,327KB
hid.dat	2021-04-05 오후 10:04	DAT 파일	1KB
KCBYG45QNM.lock	2021-04-05 오후 10:04	LOCK 파일	61,511KB
LJM5WIC7Z1.lock	2021-04-05 오후 9:59	LOCK 파일	3KB
MDKB4QCINR.lock	2021-04-05 오후 9:59	LOCK 파일	4KB
QNSDDPONEH.lock	2021-04-05 오후 10:04	LOCK 파일	28,238KB
R3YIYRSVPK.lock	2021-04-05 오후 10:04	LOCK 파일	2KB
REHVIR6IOX.lock	2021-04-05 오후 10:04	LOCK 파일	4KB
X674FJXSV2.lock	2021-04-05 오후 10:04	LOCK 파일	2KB

!!!_FILES_RECOVERY.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

---> !!! RANSOMWARE Covid 19 !!! <---

!Attention!

Please read this important instruction.

All your content, files, photos, documents, databases, and other important files are encrypted.

All your encrypted files have extension: .lock

This is all very sad.

[그림 19] 랜섬노트

암호화 시 확장자는 .lock으로 암호화가 진행되며, 랜섬노트는 코로나 19 사태를 이용하여 코로나 19 관련 랜섬웨어로 위장한다. 즉, RANSOMWARE Covid 19라는 글은 Rapid 변종 랜섬웨어가 위장한 것이며, 암호화 속도는 동시다발적인 만큼 빠른 속도로 암호화된다. 또한 이전의 행위에서 확인한 것과 같이 예약 작업을 통해 매분마다 무기한으로 수행된다. 이후 사용자가 암호화 행위를 중지하기 위해 재부팅 하였을 때에도 레지스트리에 등록된 작업을 통해 암호화 행위는 수행된다.

3. Privacy-i EDR 탐지 정보

Privacy-i EDR은 Rapid 랜섬웨어에 Ransomware 타입의 악성코드로 탐지하고 있다.

3.1. 탐지 행위

>	High	Suspicious Behavior : impact.encrypt.many-files
>	High	Suspicious Behavior : impact.encrypt.decoy-file.1
>	Medium	Suspicious Behavior : impact.encrypt.file.1
>	Low	Suspicious Behavior : discovery.enumerate.file-directory.1
>	Medium	Suspicious Behavior : impact.encrypt.data.1
>	Medium	Suspicious Behavior : persistence.configure.auto-run.registry.2
>	Low	Suspicious Behavior : persistence.configure.scheduled-task.3
>	Medium	Suspicious Behavior : lateral-movement.execute.schtasks.1
>	High	Suspicious Behavior : impact.impair.system-recovery.2
>	Medium	Suspicious Behavior : impact.shutdown.system.1
>	Medium	Suspicious Behavior : evasion.configure.system-service.2
>	Low	Suspicious Behavior : discovery.acquire.active-window.1
>	Low	Suspicious Behavior : discovery.acquire.system-information.3
>	Medium	Suspicious Behavior : discovery.enumerate.process.1

[그림 20] Privacy-i EDR 탐지 행위

Rapid 변종 랜섬웨어의 악의적인 행위에 대해 위와 같이 탐지하고 있다. 각 행위는 이전에 확인할 수 있었던, 파일 암호화 및 작업 스케줄러(Task Scheduler) 예약 작업 등록 등 다양한 행위를 포함하고 있다. 또한 볼륨 웨도우 복사본 삭제 및 특정 서비스 종료 행위 등 주요 행위들을 확인할 수 있다.

3.2. 주요 탐지 행위

3.2.1. persistence.configure.scheduled-task.3

▼ Low Suspicious Behavior : persistence.configure.scheduled-task.3

이벤트 발생 일시: 2021-04-02 18:05:36

위험도: 3

이벤트 Guid: 859ec632-307a-4acc-9beb-3cc2b0921ab9

이름	값
Child process command-line	"C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /TN Encrypther /TR C:\Users\JeongGeonWoo\AppData\Roaming\noputana.exe

[그림 21] 작업 스케줄러(Task Scheduler) 예약 작업 등록 행위 정보

작업 스케줄러(Task Scheduler)를 통한 예약 작업 등록 및 지속성 유지 행위에 대해 위와 같이 주요 정보로서 탐지하며, 그에 해당하는 탐지 정보를 확인할 수 있다.

3.3.2. impact.impact.system-recovery.2

▼ High
Suspicious Behavior : impact.impact.system-recovery.2

이벤트 발생 일시: 2021-04-02 18:05:29

위험도: 8

이벤트 Guid: 741290be-f342-49fd-9792-855553ac89eb

	이름	값
	Child process command-line	"C:\Windows\System32\cmd.exe" vssadmin.exe Delete Shadows /All /Quiet

[그림 22] 볼륨 쉐도우 복사본 삭제 행위 정보

Vssadmin.exe를 이용한 볼륨 쉐도우 복사본 삭제로 시스템의 복구 불가 설정을 하는 행위를 위와 같이 주요 정보로서 탐지하며, 그에 해당하는 탐지 정보를 확인할 수 있다.

3.3.3. impact.encrypt.many-files

▼ High
Suspicious Behavior : impact.encrypt.many-files

이벤트 발생 일시: 2021-04-02 18:05:46

위험도: 10

이벤트 Guid: cffb9ca5-9b59-4613-9452-55f4bafb06fe

파일 경로	해시	대상 파일 이름
C:\Users\JeongGeonWoo\0ARTmpDcy\rdcyT...		R5OSYGDVYF.lock
C:\Users\JeongGeonWoo\Pictures\desktop.ini		TIT2AY7OFZ.lock

[그림 23] 다수의 파일 암호화 행위 정보

다수의 파일을 암호화하는 랜섬 행위에 대해 위와 같이 주요 정보로서 탐지하며, 그에 해당하는 탐지 정보를 확인할 수 있다.

3.3.4. evasion.configure.system-service.2

▼ Medium Suspicious Behavior : evasion.configure.system-service.2	
이벤트 발생 일시: 2021-04-02 18:05:18	
위험도: 4	
이벤트 Guid: ec119fc5-5b6f-4d52-9414-041a953eb3ae	
이름	값
Child process command-line	"C:\Windows\System32\cmd.exe" sc delete "vmickvpexchange"
Child process name	cmd.exe

[그림 24] 주요 서비스 제거 행위 정보

주요 서비스 및 프로세스를 종료하는 행위에 대해 위와 같이 주요 정보로서 탐지하며, 그에 해당하는 탐지 정보를 확인할 수 있다.

4. 대 응

1. OS 및 소프트웨어 보안 업데이트를 항상 최신으로 유지한다.
2. 랜섬웨어 탐지/차단이 가능한 EDR 제품을 통해 예방한다.
3. 주요 문서는 주기적으로 백업하고 물리적으로 분리하여 관리한다.
4. 신뢰할 수 없는 메일의 첨부파일은 실행을 금지한다.
5. 비 업무 사이트 및 신뢰할 수 없는 웹사이트의 연결을 차단한다.

본 자료의 전체 혹은 일부를 소만사의 허락을 받지 않고, 무단게재, 복사, 배포는 엄격히 금합니다. 만일 이를 어길 시에는 민형사상의 손해배상에 처해질 수 있습니다.

본 자료는 악성코드 분석을 위한 참조 자료로 활용 되어야 하며, 악성코드 제작 등의 용도로 악용되어서는 안됩니다. ㈜ 소만사는 이러한 오남용에 대한 책임을 지지 않습니다.

Copyright(c) 2021 ㈜ 소만사 All rights reserved.

궁금하신 점이나 문의사항은 malware@somansa.com 으로 해주세요.