라자루스(Lazarus) 그룹, 이스라엘 군수업체 대상 APT 역습

By 알약(Alyac)

Published: 2019-03-27 · Archived: 2026-04-05 21:51:59 UTC

알약(Alyac) 2019. 3. 27. 10:13

안녕하세요? 이스트시큐리티 시큐리티대응센터(ESRC) 입니다.

2019년 03월 26일(현지시간) 이스라엘의 하레츠 매체에 따르면, 북한 연계 해커조직 라자루스(Lazarus)가 이스라엘의 특정 회사에 대한 사이버 공격 정황이 포착되었다고 밝혔습니다.

[그림 1] 이스라엘 보도 내용 (출처: North Korean Hackers Cited in Rare Attack in Israel)

■ 이스라엘 군수업체를 공격한 라자루스(Lazarus) 정부후원 연계 해킹 조직

ESRC에서는 이와 관련된 OSINT 기반 정보를 활용해 어떤 공격이 수행되었는지 조사하였습니다.

먼저 해당 위협은 스피어 피싱(Spear Phishing) 공격을 통해 내부 침투를 시도했습니다.

공격 대상은 이스라엘 국가가 전액 출자한 국방산업 분야의 'Israel Military Industries ltd (IMI)' 자회사인 'Ashot Ashkelon Industries Limited' 기업의 직원이었습니다.

이 곳는 국제 항공우주, 국방 및 기타 산업분야의 첨단 시스템 및 부품을 공급하는 이스라엘 군수업체입니다.

공격은 다음과 같이 이스라엘의 히브리어를 이용했고, 악성 파일이 첨부된 형태로 진행되었습니다.

[그림 2] 스피어 피싱 이메일 화면

이메일 발신은 2019년 03월 07일 진행되었고, 히브리어로 제목과 본문이 포함되어 있습니다. 이를 구글 번역기로 확인해 보면 다음과 같습니다.

여기서 언급되는 'SYSAID'는 IT전문가가 인프라와 서비스를 쉽고 효율적으로 관리(ITSM)할 수 있도록 지원해 주는 Help Desk 소프트웨어 솔루션입니다.

공격자는 마치 소프트웨어의 업데이트 안내 메시지로 사칭해 공격을 수행했습니다.

제목 :

SYSAID 업데이트를 사용하십시오.

본문 :

안녕,

SYSAID 관리자로부터 sysaid에 대한 업데이트를 받았습니다.

나는 그에게 당신에게 데이터를 보내 줄 것이다.

귀하의 참조 및 사용을 위해,

최고 감사합니다,

첨부파일 :

SysAid-Documentation.rar

공격에 사용된 이메일의 헤더를 살펴보면, 국가 및 언어코드 설정 부분에 이스라엘(IL) 히브리어(he), 미국(US) 영어(en), 한국(KR) 한글(ko) 내용이 포함된 것이 흥미롭습니다.

[그림 3] 이메일 헤더 부분에 포함된 국가 및 언어코드 화면

■ 'CVE-2018-20250' ACE 취약점 악성코드 분석

스피어 피싱 이메일에 첨부되어 있던 파일은 RAR 압축 확장자를 가지고 있으며, 파일명은 '**SysAid-Documentation.rar**' 입니다.

그러나 이 파일은 코드 내부적으로 ACE 압축포맷을 가지고 있으며, 지난 2월 국내에서도 보고된 바 있었던 '오퍼레이션 히든 파이썬'과 동일한 **'CVE-2018-20250'** 취약점을 사용했습니다.

압축 파일 내부에는 10개의 정상적인 파일들이 포함되어 있습니다. 그리고 'CVE-2018-20250' 취약점에 의해 시작 프로그램 경로(Startup)에 **'ekrnview.exe'** 악성 바이너리가 생성되도록 구성되어 있습니다.

File Name ekrnview.exe

File Size 98816 bytes

File Type PE32+ executable (GUI) x86-64, for MS Windows

MD5 96986b18a8470f4020ea78df0b3db7d4

SHA1 431c792fcc8ba9b58f0ffde5c8fe6fd93066ec45

SHA256 2eb447785e5b35c42d842706d593a907d0bdbc50ad9d0327c3591ac4ef17ce6e

[그림 4] ACE 압축 파일 내부 구조 화면

압축 파일 내부에는 다음과 같은 파일들이 포함되어 있습니다.

- About SysAid and our customer commitment.pdf

- Bug Fixes 17 - Cloud.pdf

- Cloud Release Notes _ SysAid.pdf

- Contact Us.png

- Contact Us.txt

- How to download SysAID 18 for Windows.txt

- InstandDemo-Preview.png

- Read up on SysAid.pdf

- Thumbs.db.lnk

- Vendor-Landscape_Mid-Market-Service-Desk-Software.pdf

'How to download SysAID 18 for Windows.txt' 파일에는 다음과 같이 'SysAid 18 Download' 다운로드 내용이 포함되어 있습니다.

---------- SysAid 18 Download ----------

httpshelpdesk.sysaid.comCustomPage.jsppageName=download_05.html&fileName=OnPremUpgrade18.1.54SysAidServerPatch_18_1_

'Thumbs.db.lnk' 바로가기 파일은 다음과 같은 메타데이터를 포함하고 있는데, 아이콘 로케이션이 '103.225.168.159' 주소로 연결되어 있고, 작업 경로에 존재하는 사용자 계정명은 'john' 입니다.

특히, '103.225.168.159' 주소는 최종 페이로드가 통신을 시도하는 C2 주소와 일치하고 있어, 공격자가 직접 만든 바로가기 파일로 증명됩니다. 따라서 공격자가 사용한 'john' 계정이 공격자가 사용한 계정이라는 것을 알 수 있습니다.

StringData

{

namestring: not present

relativepath: .\100m.bat

workingdir: C:\Users**john**\Desktop

commandlinearguments: not present

iconlocation: **103.225.168.159**\c$\windows\system32\PerfCenterCpl.ico

}

압축 파일에 설정된 시작 프로그램 경로는 특정 윈도우즈(OS) 사용자 계정명을 포함하고 있어, 공격자는 위협 대상 맞춤형으로 공격 코드를 제작했습니다.

[그림 5] 시작 프로그램(Startup) 경로에 생성된 악성 파일 화면

'ekrnview.exe' 파일은 64비트 기반으로 제작되었으며, 한국시간(KST) 기준으로 2019년 02월 26일 새벽 04시 37분에 빌드되었습니다.

이 악성 파일은 'GuiCache.db' 데이터와 'IDR_RESOURCE' 리소스 내용에 접근해 로드를 시도합니다.

```
v0 = GetModuleHandleW(0i64);
 v1 = v0;
 if ( v0 )
 {
   v3 = FindResourceW(v0, (LPCWSTR)0x6F, L"IDR_RESOURCE");
   v4 = v3;
   if ( v3 )
   {
     v5 = LoadResource(v1, v3);
     if ( v5 )
     {
       v6 = LockResource(v5);
```

```
if ( v6 )
{
  v7 = SizeofResource(v1, v4);
  v8 = LocalAlloc(0x40u, v7);
```

그리고 하드코딩된 명령제어(C2) 서버로 접속을 시도해, 공격자의 추가 명령을 대기하게 됩니다.

- http://www.alahbabgroup.com/bakala/verify[.]php (198.96.95.58)
- http://103.225.168.159/admin/verify[.]php
- http://www.khuyay.org/odin_backup/public/loggoff[.]php (170.239.84.243)
- http://47.91.56.21/verify[.]php

[그림 6] 하드코딩된 명령제어(C2) 화면

```
lea     rcx, [rbp+6260h+var_6220] ; lpBuffer
mov     [rsp+hMem], r13
mov     rbx, rax
mov     [rsp+arg_18], r13
call    cs:GetComputerNameA
lea     rax, [rbp+6260h+var_6220]
mov     rdx, r15
ea      r8, [rsp+hMem]
lea     rcx, [rbp+6260h+var_6220]
call    sub_140001C40
lea     r8, [rbp+6260h+phkResult] ; phkResult
mov     [rbp+6260h+nSize], 100h
lea     rdx, SubKey     ; "SOFTWARE\\Microsoft\\Windows NT\\Curren"...
mov     rcx, 0FFFFFFFF80000002h ; hKey
call    cs:RegOpenKeyA
mov     rcx, [rbp+6260h+phkResult] ; hKey
lea     rax, [rbp+6260h+nSize]
mov     qword ptr [rsp+dwService], rax ; lpcbData
lea     rdx, ValueName  ; "ProductName"
lea     rax, [rbp+6260h+Data]
```

'GetComputerNameA' API 함수를 통해 검색된 컴퓨터 명을 HTTP 매개 변수로 가져오며, 레지스트리키 'ProdcutName' 값을 통해 Windows 운영체제 버전을 확인합니다.

그리고 HTTP POST 통신 과정에서 다음과 같이 매개 변수로 사용됩니다.

- alive

- name

- key

- page

- session_data

```
lea     r8, [rsp+arg_28]

mov     rcx, rbx

call    sub_140001C40

mov     rcx, rbx        ; hMem

call    cs:LocalFree

mov     edx, 20000h     ; uBytes

mov     ecx, 40h        ; uFlags

call    cs:LocalAlloc

mov     r14, qword ptr [rbp+6260h+cbSize]

lea     rdx, aAliveVerify_se ; "alive=verify_session&name=%s&key=%s&page=%s&session_data="

mov     r9, [rsp+arg_18]

mov     r12, rax

mov     r8, [rsp+hMem]

mov     rdi, rax

xor     eax, eax

mov     [rsp+20h], r14

mov     ecx, 20000h
```

■ C2 서버 'B374k' 웹쉘(Webshell) 존재

C2 서버에 사용된 리스트 중에 한 곳은 디렉토리 리스팅(directory listing) 취약점에 의해 서버 내부 구조가 오픈되어 있습니다.

[그림 7] 디렉토리 리스팅 취약점으로 인해 보여지는 내부 화면

흥미로운 점은 이곳에 웹쉘(Webshell)이 등록되어 있는 것이 발견됐고, 특정 정부후원을 받는 해킹조직이 최근까지 한국의 침해사고 서버에서 사용한 바 있는 'B374k' 시리즈와 동일한 종류였습니다.

물론, 이 웹쉘은 코드가 인터넷에 공개되어 있기 때문에 이것만 가지고 공격자를 특정할 수는 없습니다.

그러나, 최근까지 한국의 일부 해킹공격에 연루된 서버에서 'b374k' 웹쉘이 여러차례 발견된 바 있고, 우연하게도 최신이 아닌 모두 v2.8 구 버전이 사용되었습니다.

ESRC에서는 한국 침해사고 공격조직과 이번 이스라엘 공격 조직은 같은 국가로 판단하지만, 세부 그룹으로는 다르게 분류하고 있습니다.

[그림 8] 이스라엘 침해사고 연관 웹쉘과 한국 침해사고 웹쉘 비교 화면

한편, 2019년 03월 10일 이스라엘 지역에서 'SysAid-Documentation.rar' 파일명이 동일한 다른 악성 파일이 추가로 바이러스 토탈에 업로드되었습니다.

두개의 내부 파일을 비교해 보면, 정상 파일들과 악성 파일 모두 100% 동일합니다. 다만, 생성되는 사용자 계정명만 다릅니다.

- C:\Users**idans**\AppData\Roaming\Microsoft\Windows\Start Menu\Programs

- C:\Users**ronpe**\AppData\Roaming\Microsoft\Windows\Start Menu\Programs

■ ACE 취약점을 이용하는 또 다른 형태

ESRC에서는 ACE 취약점을 이용하는 형태를 추적 하던 중에 다음과 같은 두개의 악성 파일을 발견했습니다.

이 내용은 ti.360.net 분석에서 APT-C-27 (Goldmouse)로 명명되었고, 중동지역 공격 연계로 분석되었습니다.

'APT-C-27 (Goldmouse): Suspected Target Attack against the Middle East with WinRAR Exploit'

- MD5 : 314e8105f28530eb0bf54891b9b3ff69

- MD5 : 102d3104a010e49f92a6903adc92c449

두개 파일 모두 'CVE-2018-20250' 취약점을 이용하고 있습니다.

'314e8105f28530eb0bf54891b9b3ff69' 파일의 경우 압축 파일 내부의 수정 날짜가 2019-02-21 오후 10:03분으로 지정되어 있는데, 이스라엘 공격에 사용된 압축 파일 내부랑 유사함을 알 수 있습니다.

[그림 9] 추가로 발견된 ACE 악성파일과 동일한 수정 날짜 화면

압축 파일에 포함되어 있는 '1.docx' 파일의 속성을 살펴보면 만든이와 마지막으로 저장한 사람 모두 '**Albany**' 이름을 가지고 있습니다.

[그림 10] 압축 파일 내부에 포함되어 있던 '1.docx' 문서 파일 속성

문서 파일을 실행하면 다음과 같이 아랍어로 작성된 내용이 보여집니다.

[그림 11] 아랍어 내용이 담겨져 있는 정상 문서파일

만약, 'CVE-2018-20250' 취약점이 작동하게 되면 시작 프로그램 경로에 '**Telegram Desktop.exe**' 악성 파일(Payload)이 등록됩니다.

이 페이로드는 윈도우즈가 시작될 때 자동으로 실행됩니다.

[그림 12] 시작 프로그램에 악성 파일이 등록된 화면

'Telegram Desktop.exe' 파일은 닷넷 기반으로 만들어진 32비트 악성파일로 한국시간(KST) 기준으로 2019년 03월 11일 22시 40분에 제작되었습니다.

그리고 내부에 다음과 같은 개발 경로를 포함하고 있습니다.

- C:\Users**Albany**\documents\visual studio 2012\Projects\New March\New March\obj\Debug**New March.pdb**

'1.docx' 문서 파일에 있던 것과 동일하게 'Albany' 계정에서 악성 파일이 제작된 것을 알 수 있습니다.

'Telegram Desktop.exe' 악성 파일이 실행되면, 임시 경로(Temp)에 **'Telegram_Desktop.vbs'** 파일을 생성하고 실행을 시도합니다.

[그림 13] 'Telegram_Desktop.vbs' 명령 함수 화면

'Telegram_Desktop.vbs' 파일에는 내부에 Base64 코드로 인코딩된 32비트 닷넷 기반 EXE 파일이 존재합니다.

[그림 14] BASE64로 코드로 인코딩된 EXE 파일

해당 파일을 디코딩해 보면, 한국시간(KST) 기준으로 2019년 03월 11일 21시 39분에 제작된 EXE 파일이 확인되며, 내부에는 다음과 같은 PDB 자료가 포함되어 있습니다.

첫번째 페이로드에는 'New March.pdb' 값이 있었지만, 두번째 페이로드에서는 'WriteString.pdb' 이름으로 변경되었습니다.

- C:\Users**Albany**\documents\visual studio 2012\Projects\New March\WriteString\obj\Debug**WriteString.pdb**

새로 생성된 파일이 작동되면, 임시 경로(Temp)에 '1717.txt' 파일을 생성합니다.

[그림 15] 임시 폴더에 '1717.txt' 파일 생성 명령 화면

ESRC에서는 해당 악성코드(njRAT)와 관련된 상세 내용과 인텔리전스 리포트를 '쓰렛 인사이드(Threat Inside)' 서비스를 통해 자세히 제공할 예정입니다.