Return to ROKRAT!! (feat. FAAAA...Sad...)

By velocy

Published: 2018-11-16 · Archived: 2026-04-05 22:21:50 UTC

Simple Analysis blog

Analysis

Return to ROKRAT!! (feat. FAAAA...Sad...)

velocy 2018. 11. 16. 15:42

2018-11-16, VirusTotal에 "※ 기 록 부.hwp" 라는 이름의 한글파일이 헌팅되었다.

2018-11-16, VirusTotal has hunted a HWP file named "※ 기 록 부.hwp".

해당 한글파일은 RedEyes, 스카크러프트 그룹의 ROKRAT 라고 알려진 유형의 악성코드로 추정된다.

The Korean file is estimated to be a malicious code of the type known as the ROKRAT of the Scraft group.

* RedEyes, Scarcruft : 한국의 유명기관이나 정치단체를 대상으로 데이터 탈취와 파괴를 모두 수행하는 공격 그룹

* RedEyes, Scarcruft: Attack group that performs data capture and destruction on famous institutions or political groups in Korea

"※ 기 록 부.hwp" 파일를 열어보면 의미없는 값들로 채워져 있음을 볼 수 있다.

When you open the "※ 기 록 부.hwp" file, you can see that it is filled with meaningless values.

위 한글파일은 "BIN0001.eps" 를 이용하여 악성코드를 인젝션 한다.

Inject malicious code using "BIN0001.eps".

%APPDATA% 경로에 "Pemnn01.hje01", "Pemnn02.hje01" 파일을 생성하여 두 파일을 합쳐 "MemoryOrder85584031.com" 파일로 생성한다.

Create "Pemn01.hje01" "Pnn02.hje01" file in the %APPDATA% path and combine the two files to create the "MemoryOrder85584031.com" file.

생성된 파일에서는 cmd.exe에 Thread Injection을 시도하며, 이때 xor 복호화된 바이너리가 사용된다.

The generated file has a try Thread Injection on cmd.exe, and xor decryt binary is used.

Xor key : 0x4A

이후 인젝션 되는 악성코드는 이전 "ROKRAT is BACK" 에서 분석한 내용과 동일하다.

The injected malicious code is the same as the previous analysis of "ROKRAT is BACK".

해당 샘플에서 사용되는 Token 값은 "tgaNZQXaLAwmirSFZfdPhI7ZCC8LqqvoBSkBdhfC5Fzw1SFeOr70" 이며, 이전 악성코드와 샌드박스, 가상환경일 경우 재부팅되어 MBR이 파괴된다.

The Token value used in the sample is "tgaNZQXaLAwmirSFZfdPhI7ZCC8LqqvoBSkBdhfC5Fzw1SFeOr70".

In case of previous malicious code, sandbox, or virtual environment, the MBR is destroyed by rebooting.

[추가]

현재 alyac에서는 해당 케이스를 Operation KoreanSword 라고 명명함.

Currently, alyac calls the case Operation EnglishSword.

[IOC]

[HWP File]

FileName :

Author : (주)한글과컴퓨터

Last Saved By : User1

Create Time/Data : 2004-11-26 06:23:46.535000 (UTC)

Last saved Time/Data : 2018-11-16 02:54:41.390000 (UTC)

MD5 : 804a8c076b4aaa2e21ab4f06453d1c4e

SHA-1: 35eda3c7aedcfaa69e4b2ad0f613eb587a519960

SHA-256: d0cac300272954919538888c2e8b2be81113a60fa0bbb1d4a5a0a0367037050e

[Drop File]

Filename : %APPDATA%\\MemoryOrder85584031.com

TimeStamp : 2018-11-14 15:47:51 (UTC)

MD5: 80a2a804e12ad9c039c3de1466fac46f

[Injection File]

TimeStamp : 2018-11-07 07:06:11 (UTC)

MD5: fb80235fbf92da08bc8bcddd241c3d42

Token: tgaNZQXaLAwmirSFZfdPhI7ZCC8LqqvoBSkBdhfC5Fzw1SFeOr70

[Similar malware]

[HWP File]

FileName : 7주 신뢰와 배려의 커뮤니케이션.hwp

Author : gichang

Last Saved By : User1

Create Time/Data : 2014-02-2613:45:17.799000 (UTC)

Last saved Time/Data : 2018-08-29 00:22:26.729000 (UTC)

MD5 : 3f92afe96b4cfd41f512166c691197b5

SHA-1: eeae06fc31982f992993ef0ff12e2d94981d9bff

SHA-256: 51e35a7a4e2c49670ecfba7b55045cfa893aa1459246fa5b23ff0bba91225b76

[Decoded File (Themida)]

Filename : %APPDATA%\\WinUpdate148399843

TimeStamp : 2018-08-28 01:22:27 (UTC)

MD5: 6ec89edfffdb221a1edbc9852a9a567a

SHA-1: 52976314913289a61282ee1f172a30cce29147ac

SHA-256: 98498b97b7cdce9dd6b1a83057e47bd74dc2be5bb12f42ce505981bff093de73

[Injection File]

TimeStamp : 2018-08-28 01:13:58 (UTC)

MD5: 7a751874ea5f9c95e8f0550a0b93902d

SHA-1: 41a3e61adf853edaddc999e547a246cc4c173480

SHA-256: f885c37b3368faf2ae11d70e15aa75a641de9357dda038d875fe5513d9841582

token: VdZhAhd9YXAAAAAAAAAACQaGEx0mpQnzlWKtxGGNveuPx0XtDTzynRk4fnra1-9E

Thank's to kino, savNi

References

'**Analysis**' 카테고리의 다른 글

Return to Satan, Lucky Ransomware **(0)**	2018.12.11
We will become back very soon! ;) **(0)**	2018.12.05
GandCrab & (CoinMining??) **(1)**	2018.11.09
Are you VenusLocker? or GandCrab? **(1)**	2018.10.22
ROKRAT is Back!! **(0)**	2018.09.21

공유하기 링크

Comments
