

The background is a deep teal color. On the left side, there is a complex, isometric arrangement of 3D cubes. The faces of these cubes are covered in a dense pattern of white binary code (0s and 1s). Several of the cubes have glowing blue rectangular openings. Bright blue and red laser beams originate from these openings and other points, crisscrossing the scene. There are also several small, solid-colored circles in shades of blue, green, and red scattered across the right side of the image.

ShimCache

91913232 김우종

Contents

What is ShimCache?

ShimCache Forensic's
perspective

ShimCache Registry Path

ShimCache Structure

ShimCache Parser

What is ShimCache?

ShimCache 정의

- AppCompatCache로 불리기도 함
- 응용 프로그램 간 호환성을 제어하고 문제 해결을 위해 만든 파일
 - 악성코드 실행 시 호환성 문제 발생하기 때문에 침해분석에 활용한다.
- 모든 실행 파일의 경로, 크기, 마지막 수정 시간 등의 정보를 저장한다.
- 프리패치와 비슷한 응용프로그램의 실행 정보를 저장한다.
 - 하지만 프리패치는 한정적이라 사라질 가능성이 있다.

ShimCache Forensic's perspective



실행 파일의 이름, 경로 정보를
확인



마지막 수정 시간 확인



침해사고 분석에 활용 가능

ShimCache Registry Path

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

ShimCache Structure (Header)

이진 값 편집

값 이름(N):
AppCompatCache

값 데이터(V):

00000000	34	00	00	00	03	00	00	00	4
00000008	00	00	00	00	03	00	00	00
00000010	03	00	00	00	00	00	00	00
00000018	00	00	00	00	01	00	00	00
00000020	00	00	00	00	00	00	00	00
00000028	00	00	00	00	00	00	00	00
00000030	00	00	00	00	31	30	74	73 1 0 t s
00000038	AB	34	E2	2D	AC	00	00	00	« 4 â - 7 . . .
00000040	62	00	43	00	3A	00	5C	00	b . C . : . \ .
00000048	57	00	69	00	6E	00	64	00	W . i . n . d .
00000050	6F	00	77	00	73	00	5C	00	o . w . s . \ .
00000058	53	00	79	00	73	00	74	00	S . y . s . t .
00000060	65	00	6D	00	33	00	32	00	e . m . 3 . 2 .
00000068	55	00	55	00	45	00	50	00	\ " " " " " " "

확인 취소

이진갑 편집

이진 값 편집

값 이름(N):

AppCompatCache

값 데이터(V):

000000E8	00	00	00	00	31	30	74	73 1 0 t s
000000F0	94	28	1A	4F	8A	00	00	00	. (. 0
000000F8	40	00	43	00	3A	00	5C	00	@ . C . : . \ .
00000100	57	00	69	00	6E	00	64	00	W . i . n . d .
00000108	6F	00	77	00	73	00	5C	00	o . w . s . \ .
00000110	73	00	79	00	73	00	74	00	s . y . s . t .
00000118	65	00	6D	00	33	00	32	00	e . m . 3 . 2 .
00000120	5C	00	69	00	70	00	63	00	\ . i . p . c .
00000128	6F	00	6E	00	66	00	69	00	o . n . f . i .
00000130	67	00	2E	00	65	00	78	00	g . . . e . x .
00000138	65	00	B8	2D	19	97	0E	DE	e . , - p
00000140	D4	01	3C	00	00	00	00	02	Ô . <
00000148	00	00	04	00	00	00	01	00
00000150	00	00	00	00	00	00	00	00	

확인

취소

오프셋	길이	설명
0x00 ~ 0x03	4byte	10ts (시그니처)
0x04 ~ 0x07	4byte	Unknown
0x08 ~ 0x1B	4byte	엔트리 크기
0x1C ~ 0x1D	2byte	경로 길이
0x1E ~ 0x??	가변byte	파일 경로
0x?? ~ 0x?? + 8	8byte	마지막 수정 시간
0x?? + 8 ~ 0x?? + 9	1byte	데이터 길이
0x?? + 9 ~	데이터 길이byte	데이터

이진 값 편집

값 이름(N):

AppCompatCache

값 데이터(V):

000000E8	00	00	00	00	31	30	74	73 1 0 t s
000000F0	94	28	1A	4F	8A	00	00	00	. (. 0
000000F8	40	00	43	00	3A	00	5C	00	@ . C . : . \ .
00000100	57	00	69	00	6E	00	64	00	W . i . n . d .
00000108	6F	00	77	00	73	00	5C	00	o . w . s . \ .
00000110	73	00	79	00	73	00	74	00	s . y . s . t .
00000118	65	00	6D	00	33	00	32	00	e . m . 3 . 2 .
00000120	5C	00	69	00	70	00	63	00	\ . i . p . c .
00000128	6F	00	6E	00	66	00	69	00	o . n . f . i .
00000130	67	00	2E	00	65	00	78	00	g . . . e . x .
00000138	65	00	B8	2D	19	97	0E	DE	e . . - . . . P
00000140	D4	01	3C	00	00	00	00	02	Ô . <
00000148	00	00	04	00	00	00	01	00
00000150	00	00	00	00	00	00	00	00	

확인

취소

ShimCache Parser



QnA