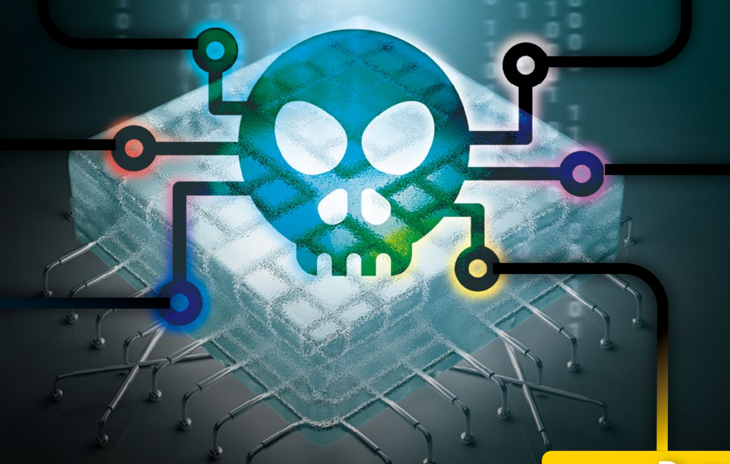
Malware Features

한국인터넷진흥원은 악성코드가 가지는 세부적인 정보의 유형을 6개 카테고리로 총 72가지 특징정보로 분류하여 관리하고 있다.

- **메타데이터(Metadata)**
  기본적인 파일정보와 PE정보
- **정적정보(Static Info)**
  개발경로 및 문자열 등 코드 내에서 확인 가능한 정보
- **동적정보(Dynamic Info)**
  레지스트리, 프로세스 등 악성코드 실행 시 동작하는 주요 행위 정보
- **네트워크(Network)**
  악성코드 실행 시 접속 시도 및 파일/메모리내 포함된 URL/IP
- **ATT&CK Matrix**
  악성코드를 전략, 전술별(TTPs) 행위를 기술단위별로 추출한 정보
- **기타 정보(ETC)**
  악성코드 함수단위 등의 정보와 악성문서에 대한 정보



MetaData

Hash

악성코드의 지문이라고 할 수 있는 해시는 각 함수를 통해 얻어지는 고정된 길이의 데이터이며, 악성코드를 쉽고 빠르게 식별할 때 널리 사용

File Hash	
MD5	b1c3debed9e8ddccafb6b1e741061a93
SHA1	dff913742500747a10fcfa8f59ad056af4549fe5
SHA256	9c0e96510c9278e400c4490ae57c6cdce2ada6e9b8d27eee9911547f376bc150
Import Hash	f34d5f2d4577ed6d9ceec516c1f5a744
FullFuzzyhash	12288:xVc5452Uap4D2hvl9Q70V/9JW4H2VVGG3Ogw91P:xU4adQ72Z2N3OgW1

PE Infomation

악성코드가 최초로 시작되는 지점과 주소 정보

Entry	EntryPoint	EntryPoint Data	ImageBase
Info	41cf5a	Assembly code	400000

악성코드 내 리소스 영역 정보

Resource

	NAME	RVA	SIZE	TYPE	Language	Country
Info	RT_ICON	0xe81a0	0x7cc	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	Korean	North Korea
	RT_ICON	0xe897c	0x10828	dBase III DBT, version number 0, next free block index 40	Japanese	Japan
	RT_GROUP_ICON	0x100ed4	0x5a	data	English	United States
	RT_VERSION	0x100f40	0x3e8	data	Korean	North Korea
	RT_MANIFEST	0x101338	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators	Korean	North Korea

악성코드의 속성 정보 확인

Image File Characteristics

LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED

악성코드의 컴파일러 정보와 링커 정보를 포함하여 유사도 비교에 활용

Rich Header

44616e53000000000000000000000000736201010300000000000010001000000106605010400000001066
0001010000001066020101000000

악성코드의 섹션(Section) 정보로 각 섹션 별 해시와 주소, 사이즈를 통해 유사도 및 패킹 유무 확인 가능

Section MD5

.text : eb177dd93c04b8dfc808ef9aea3ff889
.rdata : 613a87733c74f0e1694200310844bbad
.data : 5853bc7b24f2a2514faa5066ece2b53d
.reloc : b237847ea5bef1f950230fd0746a938d

Section Fuzzy Hash(.data)

.data : 12288:e3mA9qPKUYmC1hSUOw1K3HOOHYFGl46J:eH95UWSUzcuL54C

Section Info

	name	Virtual address	virtual size	raw address	raw size	entropy
Info	.text	0x20000	0xe4c14	0x20000	0xe4e00	6.8887760226
	.data	0xe8000	0x19600	0xe5000	0x19600	1.76797083113
	.reloc	0x102000	0xc0000	0xfe600	0x20000	0.101910425663

File Infomation

악성코드의 기본 파일 정보를 확인

Basic Info	FileSize	Original FileName	Entropy	Timestamp
Info	285840	LIBPNG16.DLL	7.958	2016-04-16 19:06:04(2016-04-16 10:06:04UTC)

악성코드가 패킹된 패커의 종류와 개발 언어 및 컴파일러의 정보 확인

Compile Info	Packer	Compiler	Linker
Info	NsPacK(3.x)	Microsoft Visual C/C++(6.0)	Microsoft Linker(6.0)[EXE32]

악용 혹은 변조된 인증서의 대한 정보를 확인

Digitally Signed Name Qizhi Software (beijing) Co. Ltd
Digitally Signed S/N 33000000BCE120FDD27CC8EE930000000000BC

악성코드의 생성, 접근, 수정 시간을 통해 변조 여부 및 침투 시간 등 확인

Create Time 2021-03-30 00:52:00(2021-03-29 15:52:00 UTC)
Access Time 2021-03-29 15:52:00(2021-03-29 06:52:00 UTC)
Modify Time 2021-03-26 23:26:46(2021-03-26 14:26:46 UTC)

프로파일링을 통해 공격조직을 지정하고 이를 통한 연관성 분석으로 유포되는 악성코드와 침해사고의 공격조직을 유추

Profiling	Attacker Group	Family
Info	Barium	shadowpad

ATT&CK Matrix

악성코드에서 사용된 전술 및 기술을 ATT&CK Matrix를 활용하여 각 기술별 행위 정보를 추출 및 분류

ATT&CK Matrix	
Initial Access	9 Techniques
Execution	10 Techniques
Persistence	17 Techniques
Privilege Escalation	12 Techniques
Defense Evasion	32 Techniques
Credential Access	14 Techniques
Discovery	22 Techniques
Lateral Movement	9 Techniques
Collection	15 Techniques
Command and Control	16 Techniques
Exfiltration	8 Techniques
Impact	13 Techniques

Network

악성코드 실행시 메모리 및 바이너리에 삽입된 URL/IP와 실제 접속을 시도하는 네트워크 행위를 추출하여 정보유출지 및 C&C를 파악하여 대응하고 유사 침해사고 및 악성코드 그룹 식별

Memory & Binaries

- https://users.qzone.qq.com/fcg-bin/cgi_get_portrait.fcg?uins=1829860377
- http://users.qzone.qq.com/fcg-bin/cgi_get_portrait.fcg?uins=1829860377
- http://a9.com/-/spec/opensearch/1.1

Connected

- nds.qzone.qq.com
- users.qzone.qq.com
- 203.205.xxx.xxx

ETC

악성코드를 이미지화한 그림 파일

PE Image

악성코드 실행시 동작하는 Windows API 함수의 순서

API Sequence

RegOpenKey
VirtualAlloc
VirtualProtec
PostMessage
MessageBox
CreateFile
WriteFile
....

악성코드간 유사도 확인을 위해 함수의 코드를 블럭 단위로 쪼개 비교 분석

Function Code Block

AI 학습을 통한 악성코드 유형 분류 결과

Type(AI Result)

악성코드의 OPCode를 나열

opcode

push,mov,push,mov,mov,call,jz,push,call,add,mov,pop,pop,push,mov,sub,push,xor,push,mov,call,mov,mov,mov, mov,mov,mov,mov,mov,cmp,pop,jnz,lea,push,lea,mov,call,push,lea,push,mov,call,push,push,call,add,mov,mov, pop,push,mov,mov———생략———

악성코드의 ByteCode를 나열

bytecode

C70124724100E975460000CCCCCCCCC558BEC568BF1C70624724100E85F460000F6450801740956E8714B000083C4048BC65E5DC20400CCCCCCCCCCCCCCCCCE93B460000CCCCCCCCCCCCCCCCCCCCCCC558BEC83EC105333DBC ———중략——— CCCCCCCCC558BEC51578B3985FF743B6A008D4DFCE8553F00008B470485C0740983F8FF730448894704568B7704F7DE1BF68D4DFCF7D6E85B

악성문서에서 추출한 특징정보

Title 입사지원서.hwp
Language Korean Unified Hangul Code (Hangul TongHabHyung Code)
Author 문서 최초 작성자
Last saved by 문서 마지막 수정자

Version info	document version	program version
Info	5.0.3.0	8, 0, 0, 466 WIN32LEWindows_7

mail body 실제 본문 내용

Section hash	MD5
Section 1	e7898e08ed91042f23e08075071d89c6
Section 2	211d5ecb63e7b31dcdfa8b37225b2e39
Section 3	dbb4da3ad961f00c0c4a91c687ef8a6b
Scripts	dfc5bdd6dc24f817cac357eca1116747
EPS	a0748e19b043ffe9bdf04c5d2df26689section

Dynamic Info

Files Activities

악성코드가 실행시 동작하는 주요 파일 행위를 파악

FilesActivities	
FileCreated	C:₩Users₩user₩AppData₩Roaming₩guide.exe
FiledDeleted	C:₩Users₩user₩Desktop₩notepad.exe
FileWritten	C:₩ReadMe.txt
FileRead	C:₩Windows₩System32₩drivers₩etc₩hosts

Registry Activities

PC 부팅시 자동실행 등 악성코드 실행시 동작하는 주요 레지스트리 키/값을 파악

KeyCreated	KeyValueCreated
HKEY_LOCAL_MACHINE₩SOFTWARE₩Classes₩.allcry	HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run

Process Activities

악성코드 실행시 동작하는 주요 프로세스 행위를 파악

ProcessActivities	
ProcessCreated	'C:₩Program Files₩internet explorer₩iexplore.exe' SCODEF:2392 CREDAT:145409
ProcessSupended	C:₩Users₩user₩Desktop₩yCfQkD9FxbSrv.exe
ProcessTerminated	C:₩Windows₩System32₩taskkill.exe
ShellExecuted	C:₩Program Files (x86)₩Microsoft₩DesktopLayer.exe

Static Info

악성코드의 개발경로를 통해 개발자의 환경을 파악할 수 있고 연관성 분석을 통해 공격조직을 유추

PDB Path

- C:₩₩Users₩₩test-win64₩₩Desktop₩₩界面漂亮的VC 屏幕保镖（锁屏程序）及源代码₩₩www.NewXing.com₩₩Release
- f:₩软件工程₩驱动编程₩OK₩KernelYK₩bin
- C:₩Users₩jihun₩source₩repos₩Project2₩Debug

오픈 소스 및 자체 생성 YARA Rule을 통해 악성코드 특징 및 그룹 파악

YARA Rule

AppleSeed, Operation BookCode

악성코드 바이너리에서 확인되는 String 문자열

String 문자열

중복 실행 방지 등을 위해 사용하는 Mutex 이름 확인

MutexName

DC_MUTEX-4Z07U55

KISA 한국인터넷진흥원