

2024 년 7 월 둘째 주, 위협 동향 보고서 (Threat Intelligence Report)



– 목 차 –

1	2024 년 7 월 둘째 주, 최신 위협 현황	3
1.1	스페인어 사용자를 대상으로 하는 Agent Tesla 캠페인	3
2	관련 용어.....	9

1 2024 년 7 월 둘째 주, 최신 위협 현황

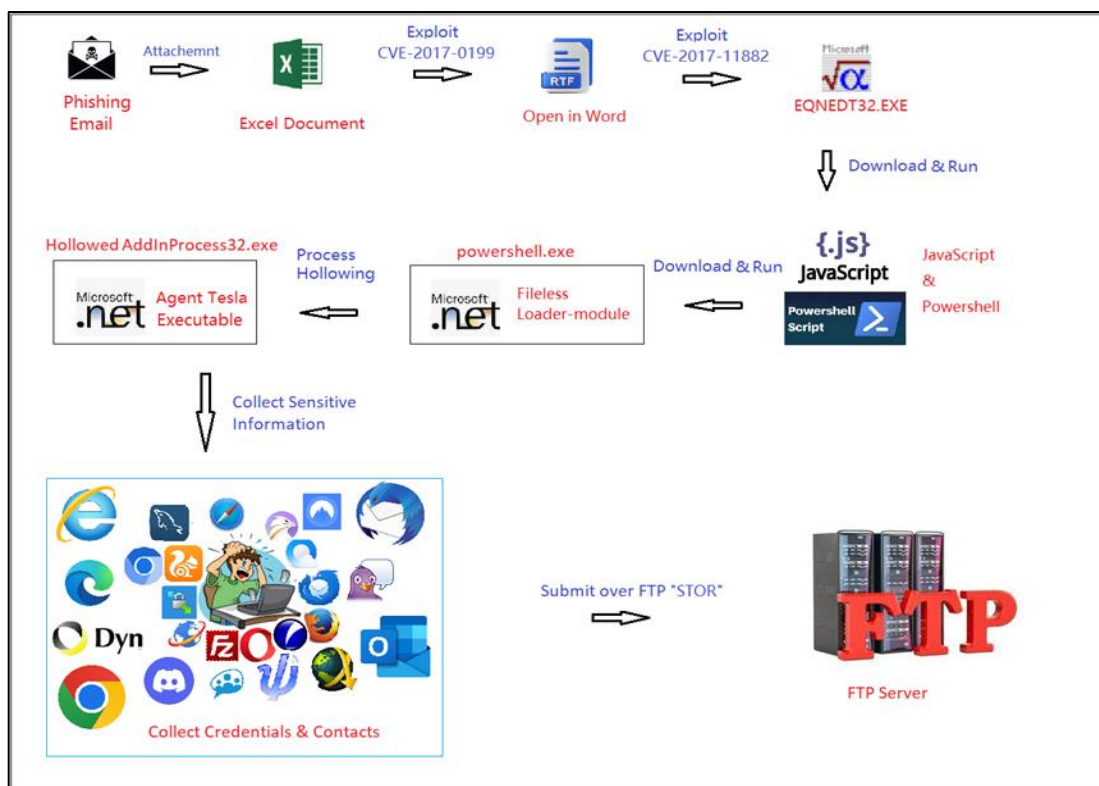
1.1 스페인어 사용자를 대상으로 하는 Agent Tesla 캠페인

1.1.1 키워드 및 요약

- + 키워드: Malware, Trojan, Infostealer, Phishing
- + 요약: 스페인어를 사용하는 사람들을 노리는 Agent Tesla 변종 확산 공격

1.1.2 위협 설명

- + 스페인어를 사용하는 사람들을 대상으로 새로운 Agent Tesla 변종 악성코드를 유포하는 캠페인이 식별됨
- + Fortinet 社 FortiGuard Labs 에 따르면 공격자는 보안 솔루션의 탐지로부터 악성 코드를 보호하기 위해 Fileless 모듈을 사용하거나 MS Office 취약점, JavaScript 코드, PowerShell 코드 등을 사용
- + Agent Tesla 에 감염될 경우 감염 시스템의 하드웨어 정보와 컴퓨터 이름, CPU 및 RAM 정보, 로그인 사용자 정보, Keylogging, 스크린샷, 소프트웨어에 저장된 자격 증명 정보 등 수많은 민감 데이터 탈취



[Agent Tesla 캠페인의 공격 프로세스]

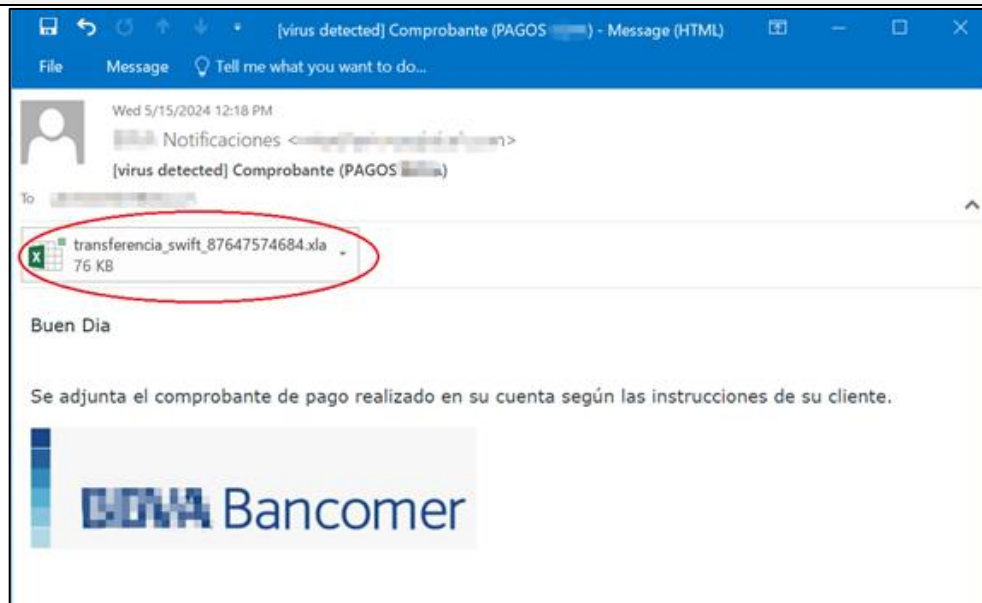
1.1.3 위협 분석

- + 최초 공격 벡터로 스페인어로 작성된 피싱 이메일을 사용하였으며, 대규모 금융 기관에서 발송한 표준 SWIFT 이체 알림 관련 내용으로 위장

-첨부파일 명 : transferencia_swift_87647574684.xla

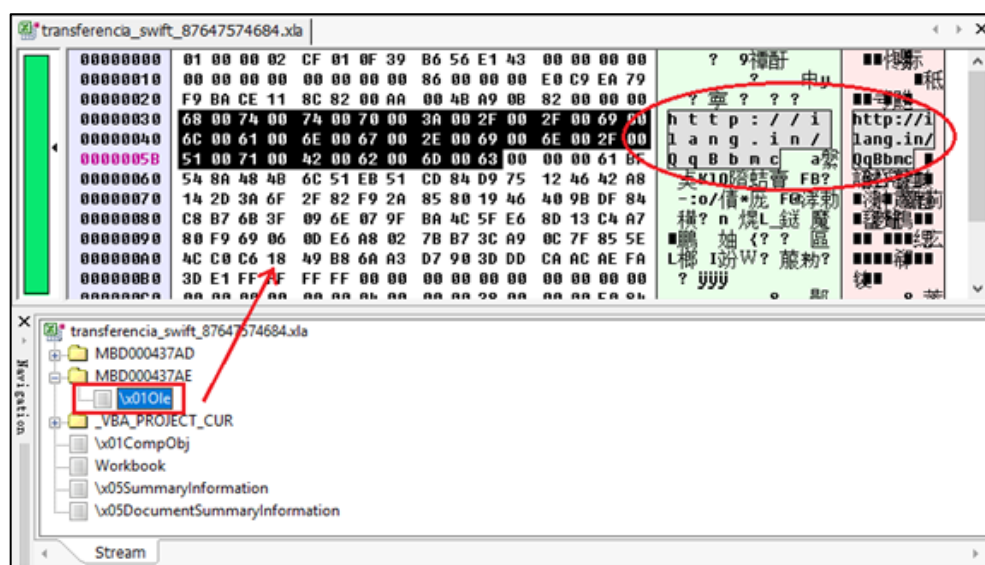
-내용 : 안녕하세요,

고객의 지시에 따라 귀하의 계정으로 결제가 이루어졌다는 증거가 첨부되어 있습니다.



[공격에 사용된 피싱 이메일 화면]

- + 피해자가 첨부된 Excel 문서를 실행할 경우 공격자에 의해 삽입된 OLE 하이퍼링크가 실행되어 추가 RTF 문서 다운로드 및 실행

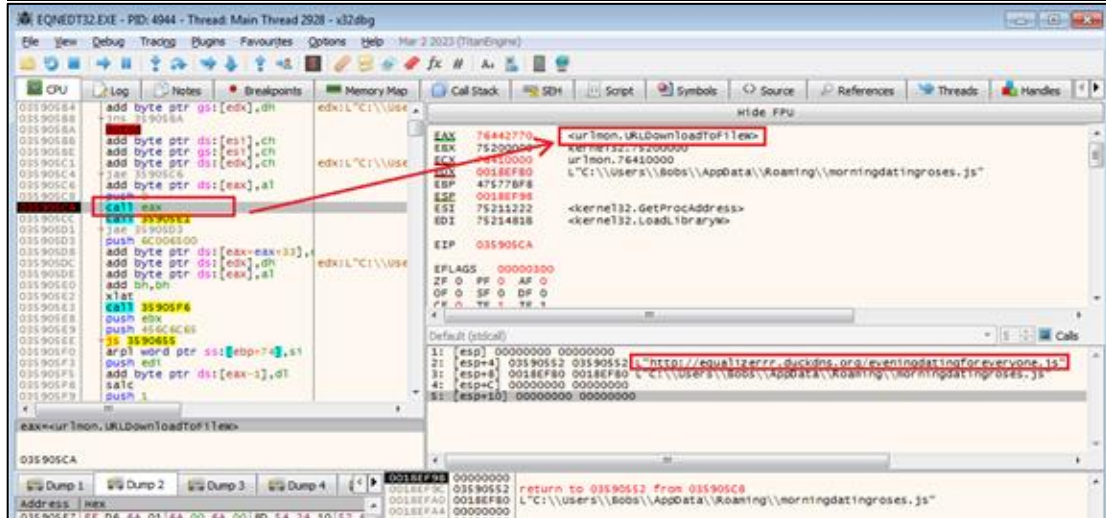


[RTF 문서에 대한 OLE 하이퍼링크]

- + RTF 문서에는 CVE-2017-11882 취약점이 악용되어 열람 시 공격자에 의해 설정된 임의 코드(셸코드)가 실행되며, 추가 JavaScript 파일 다운로드 및 실행

hxxp[://equalizerrr[.]duckdns.org/eveningdatingforeveryone.js

↳ C:\Users\WBobs\AppData\Roaming\morningdatingros.js

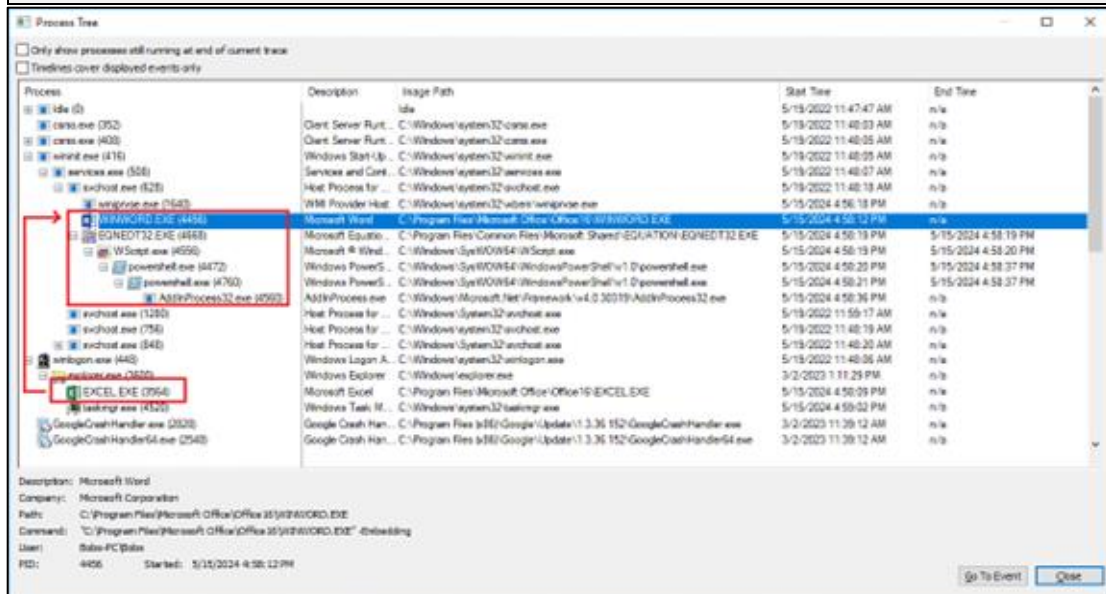


[JavaScript 다운로드 URL 및 셸코드]

- + 실행된 JavaScript는 특정 URL로 접근하여 PowerShell 스크립트를 실행하며, 인코딩된 추가 모듈을 다운로드하고 디코딩하는 과정을 거쳐 Fileless 형태의 Agent Tesla 로더 모듈인 'AddInProcess32.exe' 실행

hxxps[://paste[.]jee/d/yWWXG

↳ hxxps[://uploaddeimagens[.]com[.]br/images/004/773/812/original/js.jpg?1713882778



[PowerShell 프로세스에 의해 실행된 Agent Tesla 로더 모듈]

+ 실행된 Agent Tesla 는 다양한 형태의 방법을 통해 분석 환경 여부 감지

- Windows API CheckRemoteDebuggerPresent()를 호출하여 Debugging 여부 확인
- 샌드박스 및 가상화 환경 관련 실행 중 프로세스 검사
 - Sandboxie(SbieDLL.dll), Qihu360(Sxln.dll), Avast(Sf2.dll), Sophos Intercept X(snxhk.dll), Comodo(cmdvrt32.dll)
- WMI Query 를 통해 비디오 컨트롤러 정보 확인
- 비디오 컨트롤러의 '제조업체', '모델', '이름' 하드웨어 정보 검색
 - Microsoft Corporation, VMware, Virtual, VBOX, VBox
- 'hxxp://ip-api[.]com/line/?fields=hosting' URL 방문 후 응답이 "TRUE" 인지 확인

[Agent Tesla 의 분석 환경 여부 감지 방법]

+ 위 과정에 특이사항이 없는 경우 시스템 정보 및 설치된 소프트웨어에 저장된 민감 정보 수집

[웹브라우저]

Orbitum, Elements Browser, Cool Novo, Sputnik, 360 Browser, Uran, Iridium Browser, Liebao Browser, Vivaldi, Chromium, Sleipnir 6, Coowon, Coccoc, Amigo, Chedot, Epic Privacy, CentBrowser, Edge Chromium, Chrome, Citrio, Opera Browser, QIP Surf, Brave, Kometa, Comodo Dragon, 7Star, Torch Browser, Yandex Browser, Firefox, CyberFox, WaterFox, K-Meleon, Postbox, Thunderbird browser, IceCat, Flock, IceDragon, BlackHawk, PaleMoon, SeaMonkey, Falkon Browser, Flock Browser, IE/Edge, QQ Browser, Safari for Windows, UC Browser

[이메일 클라이언트]

Outlook, Opera Mail, PocoMail, The Bat!, Becky!, ClawsMail, FoxMail, IncrediMail, eM Client, Mailbird, Eudora, Windows Mail App

[FTP 클라이언트]

CoreFTP, Flash FXP, FTPGetter, FTP Navigator, FileZilla, SmartFTP, FtpCommander, WinSCP, WS_FTP

[VPN 클라이언트]

NordVPN, TightVNC, RealVNC, UltraVNC, OpenVPN, Private Internet Access

[IM 클라이언트]

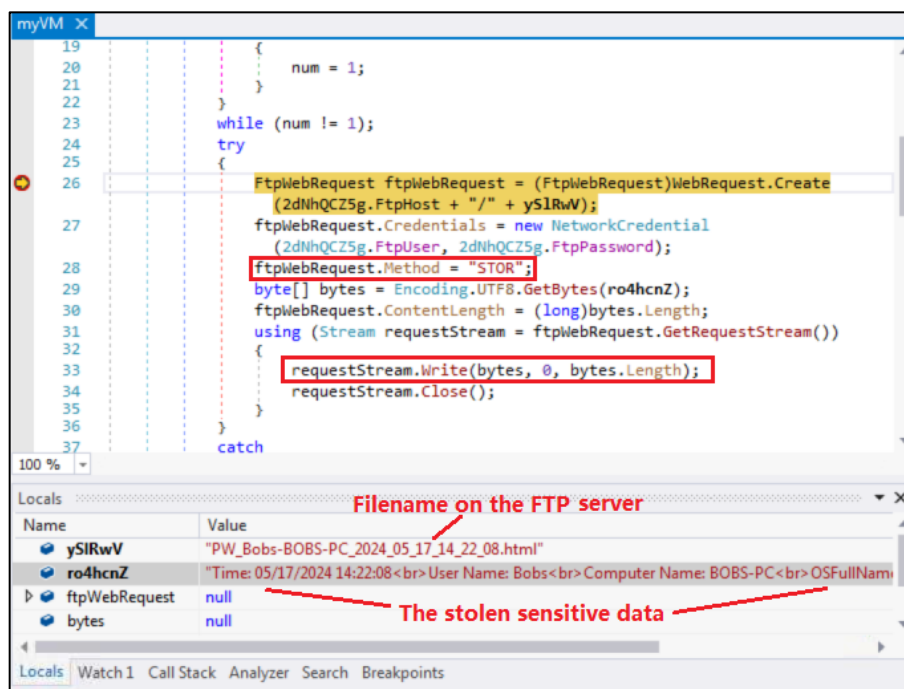
Discord, Pidgin, Trillian, Psi/Psi+, Paltalk

[기타]

MysqlWorkbench, DynDns, Microsoft Credentials, Internet Downloader Manager, JDownloader
시스템 정보(시스템 날짜/시간, 로그인 사용자 이름, 컴퓨터 이름, IP 주소, CPU/RAM 등)

[탈취 대상 소프트웨어 리스트]

- + 수집된 정보는 FTP 프로토콜을 사용하여 정보 유출



[FTP 를 이용한 수집 데이터 유출]

1.1.4 침해 지표 (Indicators of Compromise)

Indicator type	Indicator
URL	hxxps[:]//ilang[.]in/QqBbmc
URL	hxxp[:]//equalizerrr[.]duckdns[.]org/eveningdatingforeveryone.js
URL	hxxp[:]//equalizerrr[.]duckdns[.]org/droidbase64controlfire.txt
URL	hxxps[:]//paste[.]ee/d/yWWXG
URL	hxxps[:]//uploaddeimagens[.]com[.]br/images/004/773/812/original/js.jpg?1713882778
URL	ftp[.]fosna.net
FileHash-SHA256	8406A1D7A33B3549DD44F551E5A68392F85B5EF9CF8F9F3DB68BD7E02D1EABA7
FileHash-SHA256	208AF8E2754A3E55A64796B29EF3A625D89A357C59C43D0FF4D2D30E20092D74
FileHash-SHA256	7230CC614270DCA79415B0CF53A666A2198EB48EED90C85A1AC09F082AEA613B
FileHash-SHA256	A1475A0042FE86E50531BB8B8182F9E27A3A61F204700F42FD26406C3BDEC862

1.1.5 대응 가이드

- 위 IOC 상에 발견된 정보에 대하여 업무 영향도 평가 후 설정 가능한 보안 솔루션을 통해 탐지 및 차단 설정
- 신뢰할 수 없는 발신자의 첨부파일 및 링크 클릭 주의

- 단말 상에서 사용되는 안티 바이러스 프로그램을 최신버전으로 유지
- 사용되는 어플리케이션 또는 운영체제에 대하여 최신 패치를 반영

1.1.6 참고 자료

- <https://www.fortinet.com/blog/threat-research/new-agent-tesla-campaign-targeting-spanish-speaking-people>

2 관련 용어

- **트로이목마 (Trojan):** 외형적으로는 정상 프로그램 같아 보이지만 시스템 파괴 등의 악의적인 행위를 포함하고 있는 악성 프로그램
- **백 도어 (Backdoor):** 일반적인 인증을 통과, 원격 접속을 보장하고, plaintext 의 접근을 취득하는 등의 행동을 들키지 않고 행하는 방법
- **인포스틸러 (Infostealer):** 트로이목마 악성코드의 한 종류로 자격증명 정보 및 문서, 파일 등 정보 탈취를 목적으로 하는 악성코드
- **키로거 (Keylogger):** 컴퓨터의 입력 정보를 기록하는 목적의 악성 프로그램으로 일반적으로 키보드를 통한 입력을 가로채는 동작을 수행함
- **파일리스 멀웨어 (Fileless Malware):** 컴퓨터 메모리 기반 아티팩트(예: RAM)로만 존재하는 컴퓨터 관련 악성 소프트웨어로 활동의 어떤 부분도 컴퓨터의 하드 드라이브에 기록하지 않음
- **C2 (C&C 서버):** 악성코드(봇넷 등)을 제어하기 위해 사용되는 명령 제어 서버
- **피싱 (Phishing):** 전자우편 또는 메신저를 통해 신뢰할 수 있는 사람 또는 기업이 보낸 메시지인 것처럼 가장하여, 비밀번호 및 신용카드 정보와 같이 기밀을 요하는 정보를 부정하게 얻으려는 social engineering 공격의 한 종류
- **스피어 피싱 (Spear Phishing):** 특정 기관이나 특정인을 표적으로 삼아 악성메일을 발송하고, 컴퓨터를 감염시켜 정보 등을 탈취하는 '표적형 악성 메일' 공격

End of Document



서울특별시 종로구 종로 51 3~6F (종로2가, 종로타워)
tel 02 3783 6600 fax 02 3783 6499 www.secui.com

대표전화 080-331-6600

기술지원/침해대응센터 02-3783-6500

보안관제센터 02-3782-4030

평일 : 오전 8시 ~ 오후 5시 (토, 일, 공휴일 제외)

Copyright® SECUI All Rights Reserved. 본 카탈로그에 게재된 회사명, 상품명은 당사의 등록 상표입니다.

사양과 외관은 개량을 위해 예고 없이 변경되는 경우가 있습니다.