**LNK (바로가기) 파일을 이용한 피싱 공격 분석 및 방어 방법**

LNK(바로가기) 파일은 많은 피싱 캠페인의 시작점으로 흔히 사용됩니다. 공격자들은 LNK 파일의 독특한 속성을 악용하여 사용자를 속이고 탐지 및 예방 조치를 회피하며, 이는 시스템과 네트워크를 타겟으로 삼는 강력한 도구가 됩니다.

이 블로그에서는 최근의 LNK 피싱 캠페인을 심층 분석하고, 공격자들이 사용하는 전술, 기술 및 절차(TTP)를 살펴보겠습니다. 또한, 방어자들이 악성 LNK 사용에 대비할 수 있도록 시뮬레이션 도구와 기술을 소개하고, 최근 캠페인과 관련된 침해 지표(IOCs) 및 Splunk 탐지 방법을 제시하겠습니다.

이 게시물을 통해 다음과 같은 내용을 얻을 수 있습니다:

* LNK 기반 피싱 캠페인에 대한 통찰력 습득
* 이러한 공격에 대한 방어를 강화하기 위한 지식과 도구를 보유

이제 LNK 파일이 무엇인지, 그리고 어떻게 피싱 공격에 악용될 수 있는지부터 이해해 보겠습니다.

**LNK 파일이란 무엇인가?**

먼저, LNK 파일에 대해 이해해 보겠습니다. LNK(‘링크’로 발음됨) 파일은 Windows 운영 체제에서 파일, 폴더, 응용 프로그램 또는 웹사이트에 접근하기 위한 바로가기 파일입니다.

이 파일은 사용자가 Windows 탐색기 또는 바탕 화면에서 파일, 폴더, 응용 프로그램에 대한 바로가기를 만들 때 자동으로 생성됩니다.

LNK 파일은 일반적으로 작은 아이콘에 곡선 화살표 오버레이가 표시되며, 바로가기를 나타냅니다. 사용자가 LNK 파일을 우클릭하고 "속성"을 선택하면 다음과 같은 속성을 볼 수 있습니다:

* 대상 파일 또는 폴더
* 작업 디렉토리
* 명령줄 인수

이외에도 LNK 파일에는 다음과 같은 보조 정보가 포함되어 있습니다:

* LNK 파일이 작성된 기계 식별자
* 폴더 ID
* 볼륨 식별자
* 드라이브 유형
* 드라이브 일련번호
* 볼륨 레이블
* GUID

Windows OS에서 LNK 파일 확장자는 기본적으로 표시되지 않으므로, 사용자는 LNK 파일을 쉽게 식별하지 못할 수 있습니다.

**LNK 파일의 피싱 악용**

LNK 파일의 속성은 피싱 캠페인에서 악용되기에 적합합니다. 이들의 독특한 특성은 사용자를 속이기 쉬우며, 탐지 조치를 우회하기도 용이합니다.

다양한 위협 행위자와 캠페인들이 LNK 파일을 악용해 왔습니다. 이들은 다음과 같은 경우를 포함합니다:

* Qakbot과 같은 악성코드 계열
* Rhadamanthys와 Redline Stealer와 같은 트로이안 스틸러 변종
* Remcos 및 ROKRAT과 같은 원격 액세스 트로이안(RAT)
* Amadey, DarkGate, DbatLoader 및 GuLoader와 같은 로더
* Cisco Talos에서 추적한 기타 캠페인

이러한 기만적인 바로가기 파일들은 종종 합법적인 실행 파일이나 PDF 파일로 위장되어 사용자에게 클릭을 유도하고, 결국 시스템이나 네트워크를 타겟으로 삼습니다.

이 비디오는 LNK 파일이 Windows OS의 파일 확장자 숨김 동작으로 인해 기만적인 파일 유형을 생성하는 데 효과적일 수 있음을 보여줍니다.

**LNK 피싱 캠페인 및 진화**

배경 설명이 끝났으니, 최근 관찰된 여러 활성 캠페인에 대해 살펴보겠습니다. 이들 캠페인은 .LNK 파일 형식을 이용하여 감염 체인을 시작합니다.

이제 공격자들이 사용하는 전술, 기술 및 절차(TTP)를 탐구하고, 방어자들이 LNK 파일의 내용을 추출할 수 있는 도구, 예를 들어 LECmd를 사용하는 방법을 시연하겠습니다.

**LNK 피싱 캠페인의 TTPs**

아래는 최근 피싱 캠페인에서 사용된 TTPs입니다:

**명령 및 스크립트 인터프리터(T1059.001)**

일반적인 피싱 캠페인에서는 악성 LNK 파일을 배포하여 악성코드를 유포합니다. 이 LNK 파일은 스크립트 또는 명령줄 인수를 포함하여 사용자 상호작용 시 특정 동작을 유도합니다.

예를 들어, LNK 파일을 클릭하면 원격 도메인에서 file.bat를 %USERPROFILE%\Music\file.bat 디렉토리로 복사하고, AsyncRAT을 배포하여 시스템을 감염시킬 수 있습니다.

**데이터 인코딩(T1132)**

Rhadamanthys와 같은 트로이안 스틸러는 .LNK 파일을 활용하여 Base64로 인코딩된 PowerShell 스크립트를 포함시킵니다. 이 스크립트는 악성 C2 URL에서 파일을 다운로드하는 첫 번째 단계로 사용됩니다.

Base64 문자열을 디코딩하면 단순한 PowerShell 스크립트가 드러나며, 이는 또 다른 PowerShell 스크립트를 다운로드하고 실행하는 역할을 합니다.

**정보 난독화(T1027)**

피싱 LNK 캠페인에서는 PowerShell 또는 배치 스크립트와 같은 스크립트를 난독화하여 보안 도구의 탐지를 회피합니다.

CyberChef를 사용하여 인코딩된 문자열을 디코딩하여 C2 서버에서 파일을 다운로드하는 명령을 확인할 수 있습니다.

**정찰(TA0043)**

위협 행위자들은 시스템 정보를 수집하기 위해 정찰용 .LNK 샘플을 설계하였습니다. 실행 시 이 .LNK 파일은 PowerShell 스크립트를 트리거하여 다음과 같은 시스템 정보를 수집합니다:

* 프로세서 사양
* 컴퓨터 이름
* 현재 사용자
* 로드된 모듈
* 프로세스 목록
* 메모리 사용량
* MAC 주소
* 레지스트리 크기
* IP 주소

수집된 정보는 JSON 형식으로 변환되어 C2 서버로 전송됩니다.

**간접 명령 실행(T1202)**

악성 .LNK 파일은 Windows 유틸리티를 악용하여 명령줄 인터프리터 사용에 대한 보안 제한을 우회합니다. 이를 통해 명령 실행을 은밀하게 수행하고 시스템에 대한 무단 접근 또는 데이터 손상을 유도할 수 있습니다.

**사용자 실행: 악성 파일(T1204.002)**

이 섹션에서는 복잡한 악성 LNK 파일을 분석하여 공격자가 사용하는 전술과 기술을 세부적으로 살펴봅니다.

이 LNK 파일은 PowerShell 스크립트를 트리거하여 난독화 기술을 사용해 스크립트 기능을 숨깁니다. 이후, 스크립트는 XOR 암호화를 통해 바이트를 추출하고 두 개의 파일을 생성합니다:

* 하나는 더미 DOCX 파일로, 정당한 문서로 위장합니다.
* 다른 하나는 '$env

\UHCYbG.cab'로 저장된 .CAB 아카이브 파일로, 공격 체인을 지속합니다.

다음으로, PowerShell 스크립트는 expand.exe를 사용하여 .CAB 파일의 내용을 추출합니다.

파일은 start.vbs를 실행하여 추가 악성 활동을 수행합니다.

**LNK 피싱 캠페인 시뮬레이션**

조직 방어자들은 방어를 테스트할 수 있어야 합니다. 분석, XDR 또는 AV 제품의 적절한 조정과 탐지 또는 예방 여부를 확인하기 위해 다음 세 가지 방법으로 방어를 테스트할 수 있습니다:

1. **Atomic Red Team** 사용
2. **LNK Generator** 사용
3. **LNK에 CAB 파일 삽입**하기

**Atomic Red Team**

Atomic Red Team의 T1547.009 테스트 번호 2를 사용하여 PowerShell을 이용해 .LNK 파일을 생성하고, 시작 디렉토리에 배치하여 다음 사용자 로그인 시 cmd.exe를 실행할 수 있습니다.

powershell

코드 복사

$Shell = New-Object -ComObject ("WScript.Shell")

$ShortCut = $Shell.CreateShortcut("$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup\T1547.009.lnk")

$ShortCut.TargetPath="cmd.exe"

$ShortCut.WorkingDirectory = "C:\Windows\System32";

$ShortCut.WindowStyle = 1;

$ShortCut.Save();

**LNK Generator**

LNK Generator를 사용하여 LNK 파일을 만들고, 이를 사용하여 테스트를 수행할 수 있습니다. LNK Generator는 LNK 파일의 모든 필드 및 속성을 설정할 수 있는 도구입니다.

**LNK에 CAB 파일 삽입하기**

LNK 파일에 CAB 아카이브 파일을 삽입하여 공격 체인을 테스트합니다. 이 방법은 다양한 방식으로 파일을 생성하여 보안 시스템의 탐지 및 방어 능력을 평가합니다.

**탐지 및 방어**

탐지 및 방어를 위해 Splunk와 같은 SIEM 도구를 활용할 수 있습니다. LNK 파일의 악성 행위를 탐지하는 데 도움이 되는 쿼리 및 로그 분석 방법을 다음과 같이 제시합니다:

**Splunk 쿼리 예시**

Splunk에서 다음 쿼리를 사용하여 악성 LNK 파일의 행동을 탐지할 수 있습니다:

spl

코드 복사

index=security sourcetype=Sysmon EventCode=1

| where Image like "%LNK%"

| table \_time, User, Image, CommandLine, ParentImage, ParentCommandLine

이 쿼리는 LNK 파일 관련 이벤트를 검색하고, 악성 파일이 호출하는 명령줄 인수를 분석하는 데 유용합니다.

**결론**

LNK 파일은 강력한 피싱 도구로, 공격자들이 시스템을 감염시키거나 정보를 유출하는 데 효과적으로 활용될 수 있습니다. 이를 방지하기 위해, LNK 파일의 동작과 특성을 이해하고, 방어 및 탐지 도구를 적극적으로 활용하는 것이 중요합니다.

이 블로그가 LNK 파일을 활용한 피싱 공격을 이해하고 방어하는 데 유용한 정보를 제공했기를 바랍니다. 추가 질문이나 특정 방어 방법에 대한 조언이 필요하면 언제든지 문의해 주세요.