TTPs #9: 개인의 일상을 감시하는 공격전략 분석

Archived: 2026-04-05 15:10:19 UTC

본 보고서에서는 2021년부터 현재까지 개인의 PC(사무용 포함)를 타겟으로 단말기 정보를 탈취하는, 고도화된 정보수집 활동과 공격 기법, 전술 그리고 절차에 대해 설명합니다. 상세한 정보를 도출하기 위하여 공격자가 악용한 서버를 직접 분석했으며, 분석결과를 검증하기 위해 글로벌 백신업체로부터 추가적인 정보를 공유받아 TTPs(Tactics, Techniques, and Procedures)를 도출하였습니다.

공격자는 피싱메일의 미끼 파일과 IP 필터링을 통해 특정 개인을 Chinotto 악성코드에 감염시키고, 사무용 컴퓨터와 스마트폰에 대한 정보탈취를 시도합니다. 본 보고서에서는 이러한 과정에서 사용된 공격자의 명령과 사용된 기법 등 공격그룹 특유의 행위를 명시합니다.

이번 보고서에서 확인한 Chinotto 악성코드는 보안전문가 사이에서 ScarCruft 그룹이 사용하는 악성코드라고 알려져 있습니다. 그러나 사고조사 과정에서 확보한 공격자의 자원을 수집 및 분석한 결과, ▲ 피싱메일 정보수집기 내 메일송신기능 ▲ 백도어용 계정명 ▲ 피싱 이메일 형식 ▲ 명령어(파라미터 포함)를 기준으로 Kimsuky 그룹의 공격 자원과도 유사하다고 확인하였습니다. 백신업체들은 본 보고서에서 다루는 사건의 주체를 ScarCruft, 금성121, Kimsuky 등으로 각각 정의하고 있습니다. 하지만, 위의 유사성에도 불구하고 Kimsuky 그룹이 아니라 ScarCruft라고 판단한 이유는 공격그룹의 목적과 목표에 따라 대응범위를 차별화하여 집중시킬 수 있기 때문입니다.

본 보고서를 통해 공개한 TTPs는 직접적으로 공격자의 공격 속도를 늦출 수 있으며, 유관기관의 방어능력 강화를 위한 새로운 인사이트 도출로 이어질 것입니다.

정보유출 사고는 매년 끊임없이 지속적으로 발생하고 있습니다. 한국인터넷진흥원(KISA)은 정보유출 사고를 분석하는 과정에서 한국에 거주하는 특정 인물들을 대상으로 한 정보 수집 활동을 포착할 수 있었습니다. 개인 PC가 감염되면, 공격 대상 뿐 아니라 공격 대상의 주변인 정보까지 유출 될 수 있으며, 이 정보를 바탕으로 피해자를 사칭해 주변인에게까지 악성 메일을 발송하는 등 추가적인 피해를 야기할 수 있습니다.

일반적으로 유출된 정보의 가치는 개인보다 기업이 크기 때문에, 고 수준의 공격전략을 활용하는 공격 그룹은 기업을 타겟으로 활동합니다. 하지만, 본 보고서에서는 기존 보고서의 기업정보 탈취가 중심이 아닌, 공격 대상(인물)의 개인 PC, 업무용 PC를 노려 단말기 정보(데스크톱, 모바일 기기)를 탈취하는 고도화된 정보수집 활동과 공격 기법, 전술 그리고 절차에 대해 서술합니다.

본 보고서에서 정의한 공격 활동은 2021년부터 현재까지 계속 진행 중인 공격입니다. 우리는 공격자가 악용한 서버를 분석 했으며, 이 과정에서 공격자의 서버에서 확인된 여러 공격 기법과 전략, 전술 등을 파악할 수 있었습니다. 추가로, 우리는 글로벌 백신업체(AhnLab, ESTsecurity, Kaspersky)에서 해당 공격 활동과 관련된 악성코드, 명령어 등 정보를 공유받아 더욱 명확하게 공격 프로세스에 대해 확인 했습니다.

백신업체들은 이 공격의 주체를 각각 ScarCruft, 금성121, Kimsuky 등으로 구분 짓고 관리합니다. 우리는 이번 보고서에서 특정 인물들을 대상으로 한 정보수집 공격 분석 뿐 아니라, 본 사고가 해당 그룹들과 어떠한 연관성을 가지고 있는지 이야기합니다.

상세한 분석결과는 공격의 흐름을 파악할 수 있도록 구성한 3장 Attack Scenario와 TTPs를 기준으로 정리한 4장 ATT&CK Matrix에서 확인할 수 있습니다. 이후 5장 Attribution에서는 사고 분석을 통해 공격그룹의 특징이 중첩되어가는 현상과 이에 대한 고민을 공유하고, 마지막 결론을 통해 마무리합니다.
