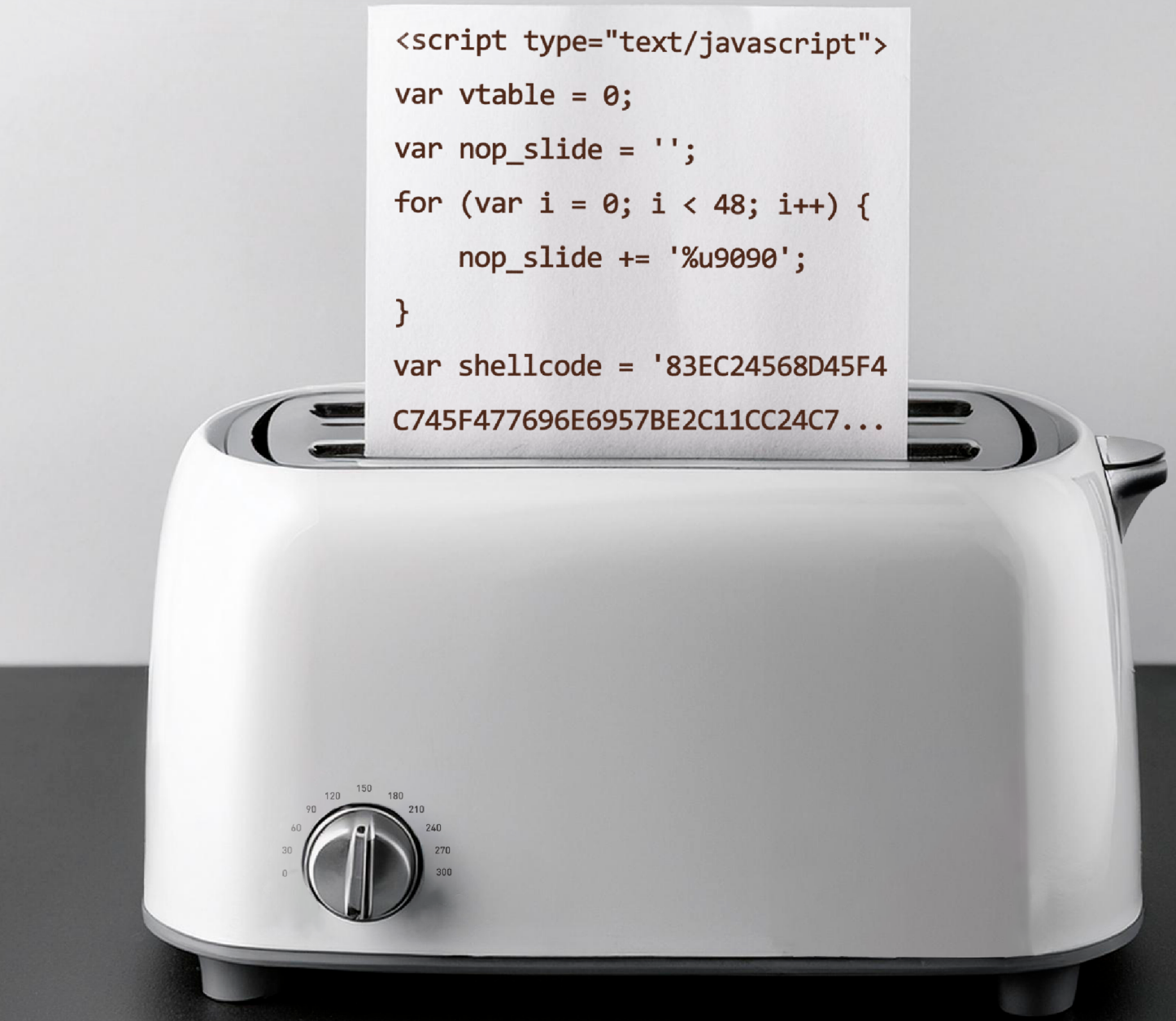
NCSC REPORT
Cyber Threat Analysis

2024

Operation "Code on Toast" (요약본)

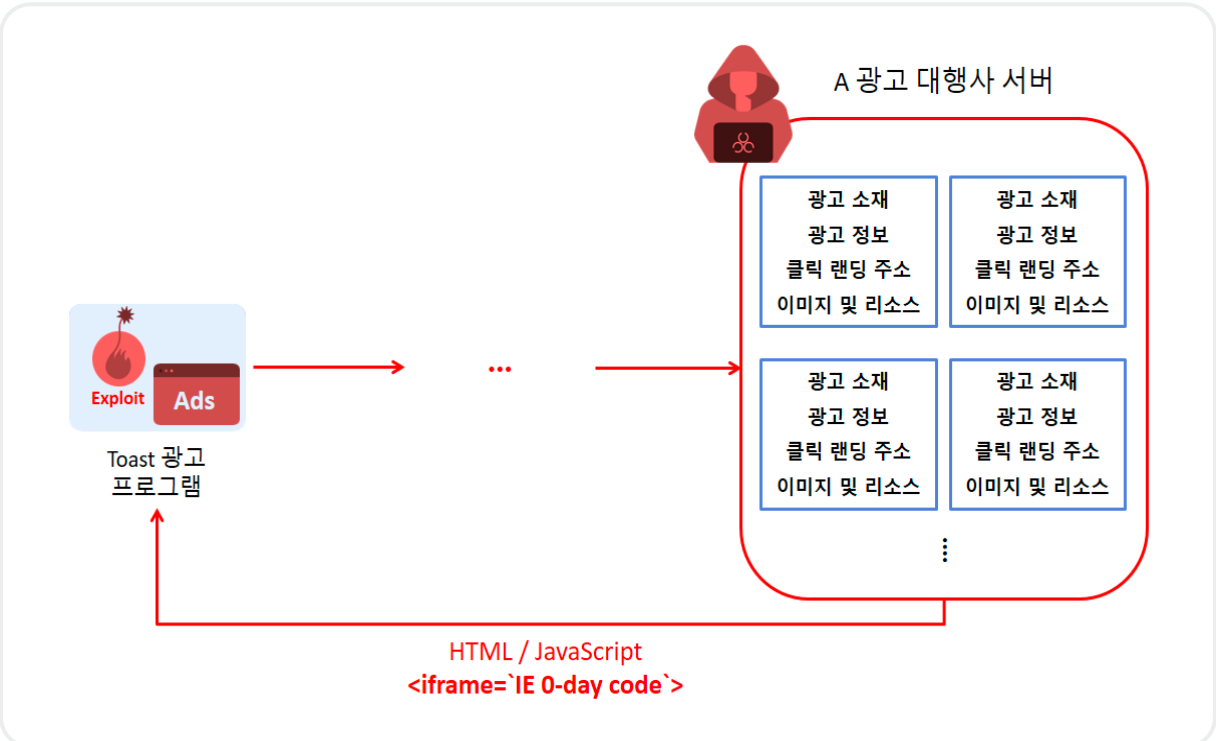
by TA-RedAnt



국가사이버안보센터 합동분석협의체
NCSC CYBER THREAT ANALYSIS TEAM

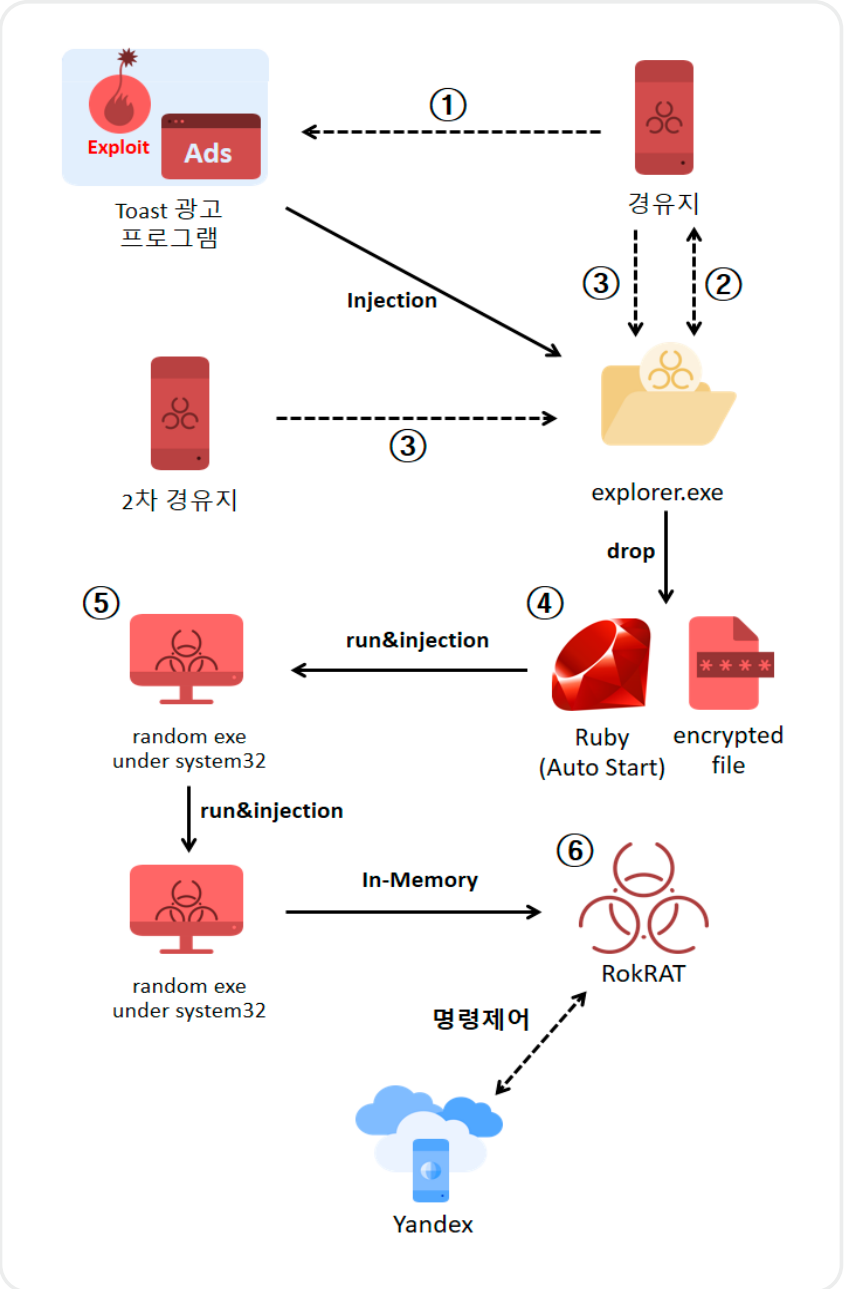
AhnLab

TA-RedAnt[1](APT37, ScarCruft, Group123 등)는 국내 북한 관련 인물들을 주로 공격하는 북한의 해킹 조직이다. 2024년 5월 무료 S/W의 팝업(Toast) 광고 프로그램을 악용한 TA-RedAnt의 대규모 공격이 탐지되어 국가사이버안보센터와 안랩社는 이에 대응하였으며, 대응 과정에서 인터넷 익스플로러(IE)의 자바스크립트 엔진 “jscript9.dll”에 존재하는 제로데이 취약점(CVE-2024-38178[2], CVSS 7.5)이 함께 악용된 사실을 확인하였다. 해당 취약점은 TA-RedAnt가 2022년 악용한 IE의 type confusion 취약점(CVE-2022-41128[3])에 간단한 코드를 추가하여 보안 패치를 우회한 원격 코드 실행(RCE) 취약점이다.



무료 S/W와 함께 설치되어 동작하는 Toast 광고 프로그램은 광고 대행사 서버에서 컨텐츠를 다운로드 받아 PC 화면 우측 하단에 광고창을 띄우는데, 이때 IE나 관련 모듈을 사용하여 컨텐츠를 렌더링한다. 해커는 이 점을 악용하기 위해 국내 광고 대행사 서버들 중 하나를 해킹하여 Toast 광고 프로그램의 응답값에 IE 취약점 코드를 삽입했고, Toast 광고 프로그램은 서버에서 받은 광고 컨텐츠를 렌더링하는 과정에서 exploit되었다.

1 TA-RedAnt는 북한과 연관된 위협 행위자(Threat Actor)로 2024년에 안랩(AhnLab)에서 새로운 분류법에 따라 명명한 그룹이다.
2 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178
3 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41128



Toast 광고 프로그램이 exploit되어 실행되는 쉘코드부터의 과정은 아래와 같다.

① 1차 악성코드(43) 다운로드 및 explorer.exe에 인젝션

- 실행 PC의 파일·프로세스를 확인하여 분석 환경인지 탐지

② 2차 악성코드(23) 다운로드 및 실행

- 컴퓨터 이름 등 시스템 정보를 수집하고 추가 감염 여부 선별

③ 3차 악성코드(move) 다운로드 및 실행 + 추가 파일 다운로드

- 악성 스크립트를 삽입한 ruby standalone 드롭 및 악성 행위 지속성 확보

④, ⑤ system32 폴더에 있는 exe를 무작위로 선택하여 실행하고 인젝션

- PC에 설치된 백신(AVAST·SYMANTEC)을 확인하여 다르게 동작

⑥ In-Memory로 RokRAT 실행

- 상용 클라우드(얀덱스 등)를 경유지로 명령제어를 수행하여 PC 정보 절취

Microsoft社는 2022년 6월 IE의 지원을 종료하였으나 일부 윈도우 어플리케이션들에선 여전히 IE를 내장하여 사용하고 있어 해커들의 공격 벡터로 악용되고 있다. 북한 해킹 조직들은 IE 외에도 최근 다양한 취약점을 악용하는 등 고도화된 공격 추세를 보이고 있다. 이에, 사용자들은 운영체제 및 S/W의 보안 업데이트를 준수하는 한편, S/W 제조사들도 제품 개발 시 보안에 취약한 라이브러리 및 모듈 등이 사용되지 않도록 주의가 필요하다.