보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

해커가 자동 로그인 기능을 좋아하는 이유

AhnLab 2022-09-05

최근 유행하는 악성코드를 논할 때 빠지지 않고 등장하는 것이 바로 '인포스틸러(InfoStealer)'다. 인포스틸러는 단어 그대로 사용자의 여러 정보들을 노린다. 특히, 웹사이트나 프로그램의 '자동 로그인' 기능을 사용하면 인포스틸러에 감염 시, 여러 서비스 계정의 자격증명을 탈취당하게 된다. 일반 사용자들은 보통 동일한 계정과 패스워드로 다수의 서비스를 이용하고 있으므로, 그 위험성이 매우 높다고 할 수 있다.

이번 글에서는 인포스틸러가 자동 로그인을 사용하는 피해자의 정보를 탈취하는 원리와 이로 인한 피해를 최소화할 수 있는 방안들을 소개한다.

인포스틸러(InfoStealer)는 운영체제나 프로그램에 저장된 자격 증명과 각종 정보를 훔치는 악성코드다. 일반적으로, 악성코드가 실행되면 자동으로 각종 정보를 수집해 유출하는 형태를 의미한다.

인포스틸러는 공격 빈도 수가 계속해서 늘어나고 있고, 그 종류와 탈취하는 정보도 다양해지고 있다. 안랩이 자사 ASEC블로그를 통해 매주 공개하는 'ASEC 주간 악성코드 통계'에서도 인포스틸러는 상당히 오랜 기간 동안 1위를 차지하고 있다.

[그림 1] 8월 2주차 주간 악성코드 통계

인포스틸러 악성코드는 여러가지 형태로 사용자들의 정보를 탈취하는데, 본 문서에서는 프로그램, 특히 웹 브라우저의 자동 로그인 기능 사용 시 정보가 유출되는 원리를 설명한다.

기본 개념

사용자가 프로그램의 '자동 로그인' 기능을 사용하면 자격증명 정보는 보통 파일 또는 데이터베이스 형태로 암호화되어 저장된다. 일부 프로그램의 경우 암호화 방식이 아닌 인코딩, 심지어 평문 형태로 저장하기도 한다. 암호화 방식도 비교적 쉽게 깰 수 있는 경우가 많아, 공격자가 탈취하고자 하는 프로그램의 암호 정보 저장 위치와 알고리즘을 알면 자격증명 정보를 탈취할 수 있다.

공격자들의 정보 탈취 방법은 크게 ▲암호 복구 프로그램 이용 ▲악성코드 내 정보 유출 기능 포함 두 가지 형태로 구분할 수 있다.

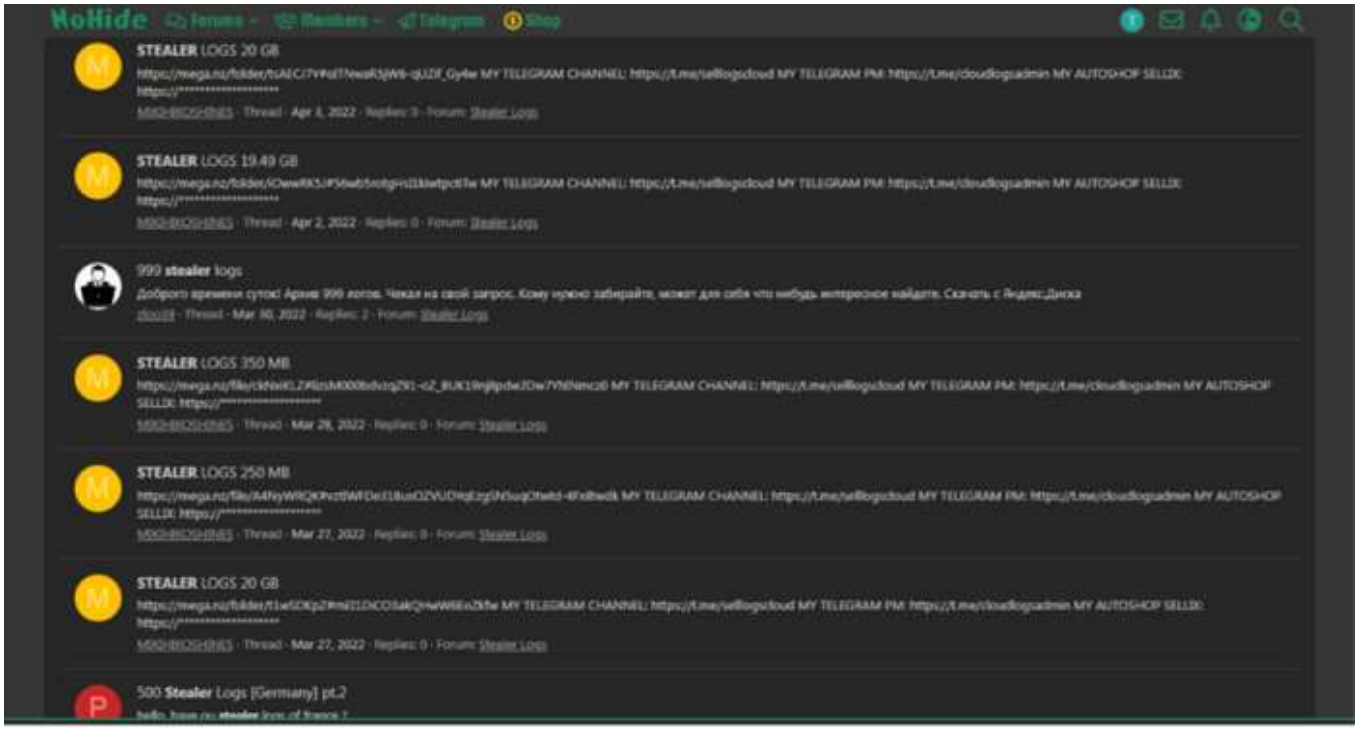
암호 복구 프로그램은 윈도우나 웹 브라우저 로그인 암호를 잊어버린 사용자들이 이용할 수 있는 프로그램이다. 공격자들은 암호를 알아내기 위해 이 프로그램을 활용하는데, 암호 복구 프로그램을 있는 그대로 사용하는 경우도 있지만, 메모리에서 실행해 사용자가 알 수 없게 하는 경우도 많다.

악성코드 내 정보 유출 기능은 비교적 잘 알려져 있으며, 인터넷 뱅킹 정보 유출 악성코드나 백도어 등의 악성코드 기능으로 포함되어 있기도 하다. 다크크리스탈(DarkCrystal), 폼북(Formbook), 엑스로더(XLoader) 등의 악성코드가 대표적으로 정보 유출 기능을 가지고 있다.

인포스틸러, 왜 위협적인가?

인포스틸러 악성코드의 가장 큰 문제는 공격자가 프로그램에 저장된 자격증명 정보를 모두 훔쳐 가기 때문에, 사용자가 사용한 몇 개의 암호를 분석해 다른 사이트의 암호나 앞으로 사용할 암호도 예상할 수 있다. 간단히 말해, 2차 피해를 야기할 가능성이 높은 것이다.

또한, 단순히 사용자 로그인 정보, 신용카드 번호 등의 정보 탈취에서 끝나지 않고 수집된 정보를 바탕으로 조직에 침투하는데 활용될 수도 있다. 인포스틸러를 이용해 수집된 정보는 다크웹(Dark Web)에 공개 혹은 판매되기도 하는데, 공격자는 특정 기업이나 조직의 자격증명 정보를 다운로드하거나 구매해 공격에 활용한다.



[그림 2] 다크웹에 공개된 자격증명 정보

최근에는 사이버 범죄 조직 뿐 아니라 국가 지원을 받는 것으로 추정되는 위협 그룹도 인포스틸러 악성코드를 활발하게 이용하고 있다. 대표적으로 2020년 10월, 북한의 지원을 받는 것으로 추정되는 안다리엘(Andariel) 그룹의 인포스틸러 악성코드가 발견되었다. 해당 악성코드는 크롬(Chrome), 파이어폭스(Firefox), 인터넷 익스플로러(Internet Explore) 등 웹 브라우저에 저장된 로그인 정보를 탈취한다.

그간 공격자들이 노려왔던 정보는 시스템 정보나 각종 프로그램의 로그인 정보였다. 하지만, 최근에는 암호화폐 지갑, 게임 등으로 대상이 점점 확대되는 것으로 나타났다. 반면, 2018년 이후에 사용이 급격히 줄어든 인터넷 익스플로러(Internet Explorer)는 대상 프로그램에서 제외한 악성코드들이 증가했다. 공격자들도 최대한의 이익을 얻기 위해 트렌드에 맞게 공격 방식을 진화시키고 있는 것이다.

인포스틸러는 다른 악성코드와 동일하게 메일, 웹 사이트 방문, 프로그램 다운로드 등으로 감염된다. 공격자가 크랙(Crack), 시리얼 키 생성 프로그램(Keygen), KMS(Key Management Service) 등에 악성코드를 포함시켜 유포하는 경우가 많다. 특히, KMS 인증 프로그램은 가정 뿐만 아니라 대기업에서도 널리 사용되고 있어 악성코드 제작자가 유포 방법으로 많이 활용한다.

또, 팬데믹 기간 동안 원격 근무가 확대되면서 개인 컴퓨터 혹은 가족 공용 컴퓨터를 업무에 이용하는 경우도 많아졌다. 이 때, 업무에 필요한 프로그램을 라이선스 없이 사용하기 위해 크랙 등을 다운로드 받으면서 인포스틸러에 감염되는 경우도 종종 발생했다. 드물지만 공급망 공격 사례도 확인되고 있다.

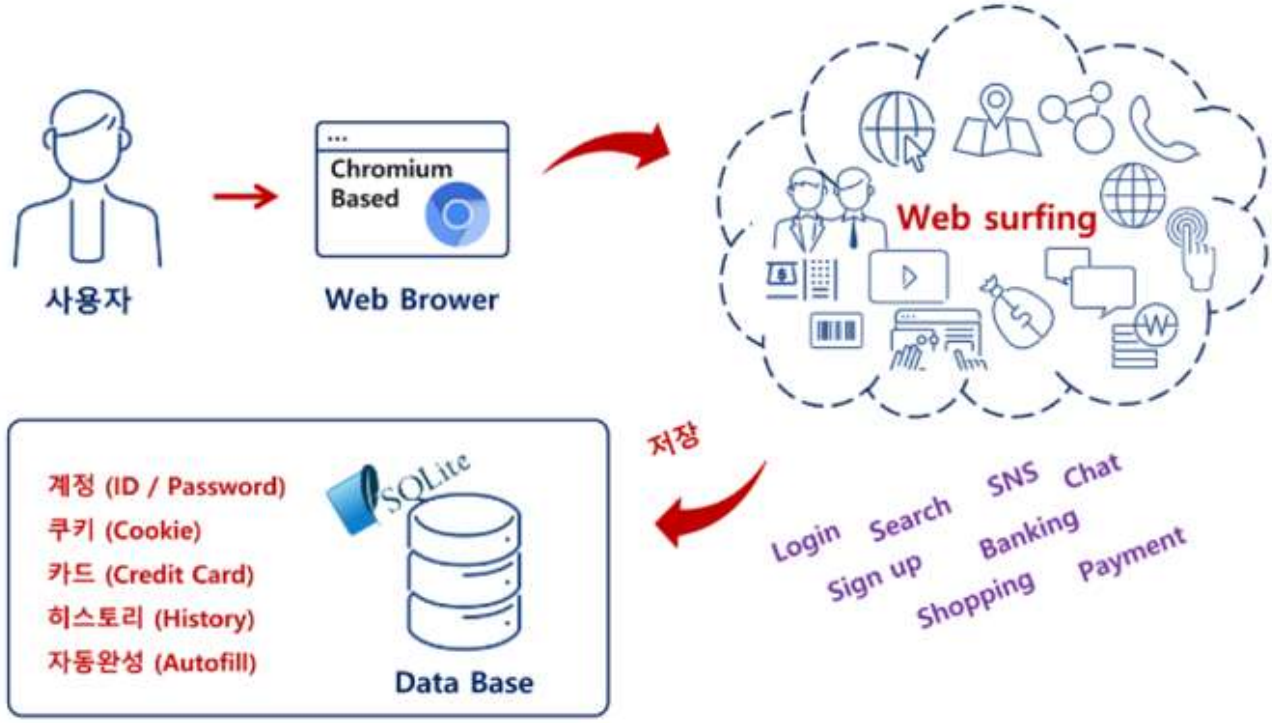
'자동 로그인' 기능 활용 시 정보 탈취 원리

본문 서두에서, 프로그램 및 웹 브라우저의 자동 로그인 기능을 사용할 경우, 인포스틸러 악성코드를 활용한 정보 탈취가 쉬워진다고 언급한 바 있다. 그 이유는 무엇일까? 관련된 여러 사례 중, 사용자들이 흔히 접하는 웹 브라우저의 저장 정보 유출 원리를 알아보도록 하자.

1. Chromium 기반 브라우저

Chromium은 구글(Google)에서 개발 및 관리되는 오픈소스 웹 브라우저로, 현재 제일 많이 사용되고 있는 웹 브라우저 엔진이다. 대표적으로 크롬(Chrome), 엣지(Edge), 오페라(Opera) 등이Chromium 코드를 베이스로 개발되었다.

Chromium 기반 웹 브라우저는 사용자가 웹 서핑을 하면서 저장하는 계정(아이디, 패스워드) 정보, 쿠키(Cookie) 데이터, 카드 정보, 히스토리, 자동 완성(Autofill) 등을 로컬 시스템의 SQLite DB 파일에 저장하는 특징이 있다.



[그림 3] 브라우저 내 저장 내용

SQLite DB 파일 내부의 일부 민감 데이터는 AES(Advanced Encryption Standard)에 의해 암호화된 상태로 관리된다. Chromium의 암호화 데이터 관리는 로컬 시스템의 사용자만 해당 정보를 복호화 할 수 있도록 하며, AES 키를 DataProtection API에 의해 암호화된 DPAPI blob 형태로 보관한다. 해당 데이터는 Base64 인코딩된 상태로, (생략)...₩User Data₩Local State JSON 파일의 "os_crypt" : {"encrypted_key"} 위치에 저장되어 있다.

인포스틸러는 계정, 쿠키, 카드, 히스토리, 자동 완성 정보를 저장하고 있는 대상 DB 파일에 SQL 쿼리를 통해 필요한 데이터를 추출한다. 그리고, AES 키를 복호화하여 암호화된 데이터의 평문화된 정보를 수집할 수 있다.

이름	경로	테이블	암호화
계정(ID/Password)	%LocalAppData%₩Google₩Chrome₩User Data₩Default₩Login Data	logins	O
쿠키(Cookies)	%LocalAppData%₩Google₩Chrome₩User Data₩Default₩Network₩Cookies	cookies	O
카드(Card)	%LocalAppData%₩Google₩Chrome₩User Data₩Default₩Web Data	credit_cards	O
히스토리(History)	%LocalAppData%₩Google₩Chrome₩User Data₩Default₩History	urls	X
자동완성(Autofill)	%LocalAppData%₩Google₩Chrome₩User Data₩Default₩Web Data	autofil	X

[표 1] Chromium에 저장되는 주요 데이터 파일

이름	대상 파일	SQL Query
계정(ID/Password)	Login Data	SELECT origin_url, username_value, password_value FROM logins
쿠키	Network₩Cookies	SELECT host_key, name, Path, expires_utc, is_secure, value, encrypted_value FROM cookies
카드	Web Data	SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted FROM credit_cards
히스토리	History	SELECT url, title, visit_count, last_visit_time FROM urls
자동완성	Web Data	SELECT name, value FROM autofill

[표 2] Chromium 정보 수집 SQL 쿼리

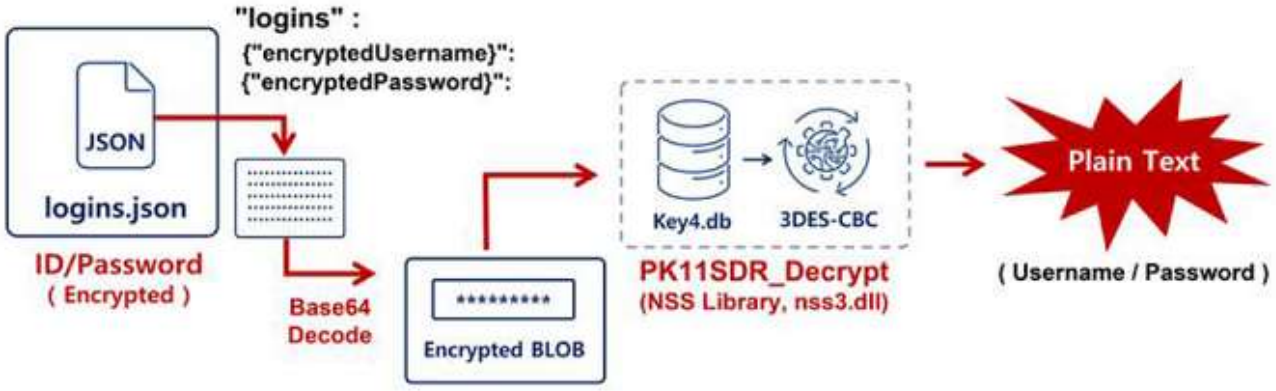
아울러, 비밀번호 외 모든 암호화된 필드값도 동일한 방법을 활용해 평문으로 복호화 할 수 있다. 복호화할 수 있는 정보는 ▲Cookies 테이블의 encrypted_value ▲Credit_Card 테이블의 card_number_encrypted 필드 등이 있다.

2. Gecko 기반 브라우저

Gecko는 모질라(Mozilla) 재단에서 개발 및 관리하는 오픈소스 웹 브라우저 엔진이다. 해당 엔진을 사용하는 웹 브라우저로는 대표적으로 파이어폭스(Firefox), 썬더버드(Thunderbird), 아이스드래곤(IceDragon), 사이버폭스(Cyberfox) 등이 있다. Chromium 이어 두 번째로 많이 사용되는 웹 브라우저 엔진이다.

Gecko 브라우저에서 저장된 계정 정보는 logins.json 파일에 암호화된 상태로 저장 된다. Gecko 브라우저의 암호화 데이터 관리는 모질라에서 개발한 NSS 라이브러리의 PK11SDR_Encrypt / PK11SDR_Decrypt 함수를 이용한다. 해당 함수의 내부적인 동작 과정을 간단히 요약하면, key4.db 파일에서 Master Key, Salt 값을 추출하여, 3DES-CBC 연산에 의해 암/복호화되는 형태다.

인포스틸러는 Gecko 기반 브라우저가 사용하는 nss3.dll의 PK11SDR_Decrypt 함수를 동적으로 로드하고, logins.json 에서 추출한 암호화된 계정 정보를 평문으로 복호화 할 수 있다.



[그림 4] Gecko 기반 복호화 과정

Gecko 기반 브라우저 관련 주요 파일 및 브라우저 정보 수집 SQL 쿼리 정보는 각각 [표 3], [표 4]와 같다.

이름	경로	암호화
계정(ID/Password)	%AppData%Mozilla₩Firefox₩Profiles₩[랜덤값]₩logins.json JSON	O
쿠키	%AppData%Mozilla₩Firefox₩Profiles₩[랜덤값]₩cookies.sqlite	X
히스토리	%AppData%Mozilla₩Firefox₩Profiles₩[랜덤값]₩places.sqlite	X

[표 3] Gecko 기반 주요 파일 정보

이름	대상 파일	SQL Query
쿠키	cookies.sqlite	SELECT host, name, path, value, creationTime, expiry, isSecure FROM moz_cookies
히스토리	places.sqlite	SELECT url, title, visit_count, last_visit_date FROM moz_places

[표 4] Gecko 정보 수집 SQL 쿼리

Gecko 브라우저의 쿠키 정보는 cookies.sqlite, 히스토리는 places.sqlite DB 파일에 저장된다. 계정이외에는 별 다른 암호화 없이 평문으로 저장되어 있어 공격자가 쉽게 정보를 획득할 수 있다.

자동 로그인을 노리는 인포스틸러, 공격은 진짜다

웹 브라우저 혹은 프로그램의 자동 로그인 기능을 활용할 경우 인포스틸러에 의해 쉽게 정보를 탈취당할 수 있다. 그리고, 이와 같은 공격으로 인한 침해 사고는 국내에서도 실제로 일어나기 때문에 더욱 경각심을 가져야 한다.

안랩 ASEC 분석팀은 지난 2021년 12월, 한 기업의 내부망 침해 사고 조사에서 기업망 접근에 사용된 VPN 계정이 재택 근무 중인 한 직원의 개인 PC에서 유출된 것임을 확인했다. 피해가 발생한 기업에서는 재택 근무 중, 사내망에 접근할 수 있도록 VPN 서비스를 제공하고 있었으며, 직원들은 지급된 노트북 또는 개인 PC로 VPN 연결 후 업무를 수행했다.

피해 직원은 웹 브라우저에서 제공하는 비밀번호 관리 기능을 이용해 VPN 사이트에 대한 계정과패스워드를 웹 브라우저에 저장해 사용했다. 그러던 중 계정 정보를 노리는 악성코드에 감염돼 다수의 사이트 계정과 패스워드가 유출되었다. 이 중에는 기업의 VPN 계정도 포함돼 있었고, 유출된 VPN 계정은 약 3개월 후 해당 기업 내부 망 해킹에 사용됐다.

피해 직원 PC는 가정에서 온 가족이 사용했고, 안전하게 관리되고 있지 않았던 것으로 확인됐다. 다양한 악성코드에 오래전부터 감염돼 있었으며, 타사 백신이 설치돼 있었으나, 제대로 탐지 및 치료되지 않았다.

감염된 악성코드 중에는 레드라인 스틸러(Redline Stealer) 계열 악성코드가 포함되어 있었다. 2020년 3월, 러시아 다크웹에 처음 등장한 레드라인 스틸러는 웹 브라우저에 저장된 계정 정보를 수집한다. 해당 레드라인 스틸러는 음정 보정 프로그램인 사운드시프터(SoundShifter)의 크랙 프로그램으로 위장하여 온라인상에 유포되어 있었다. 사용자는 소프트웨어 이름과 'crack', 'free' 등을 검색어로 입력해 파일을 검색하고 다운로드했으며, 다운로드한 파일을 직접 실행해 악성코드에 감염됐다.

유출된 정보 확인하고 대응하기

위 사례처럼, 인포스틸러 악성코드에 의해 발생한 정보 유출은 개인과 기업을 가리지 않고 심각한 피해를 야기할 수 있다. 또, 공격자들은 탈취한 정보를 활용해 2차, 3차 공격을 감행하기 때문에 피해는 더 확산될 가능성이 있다.

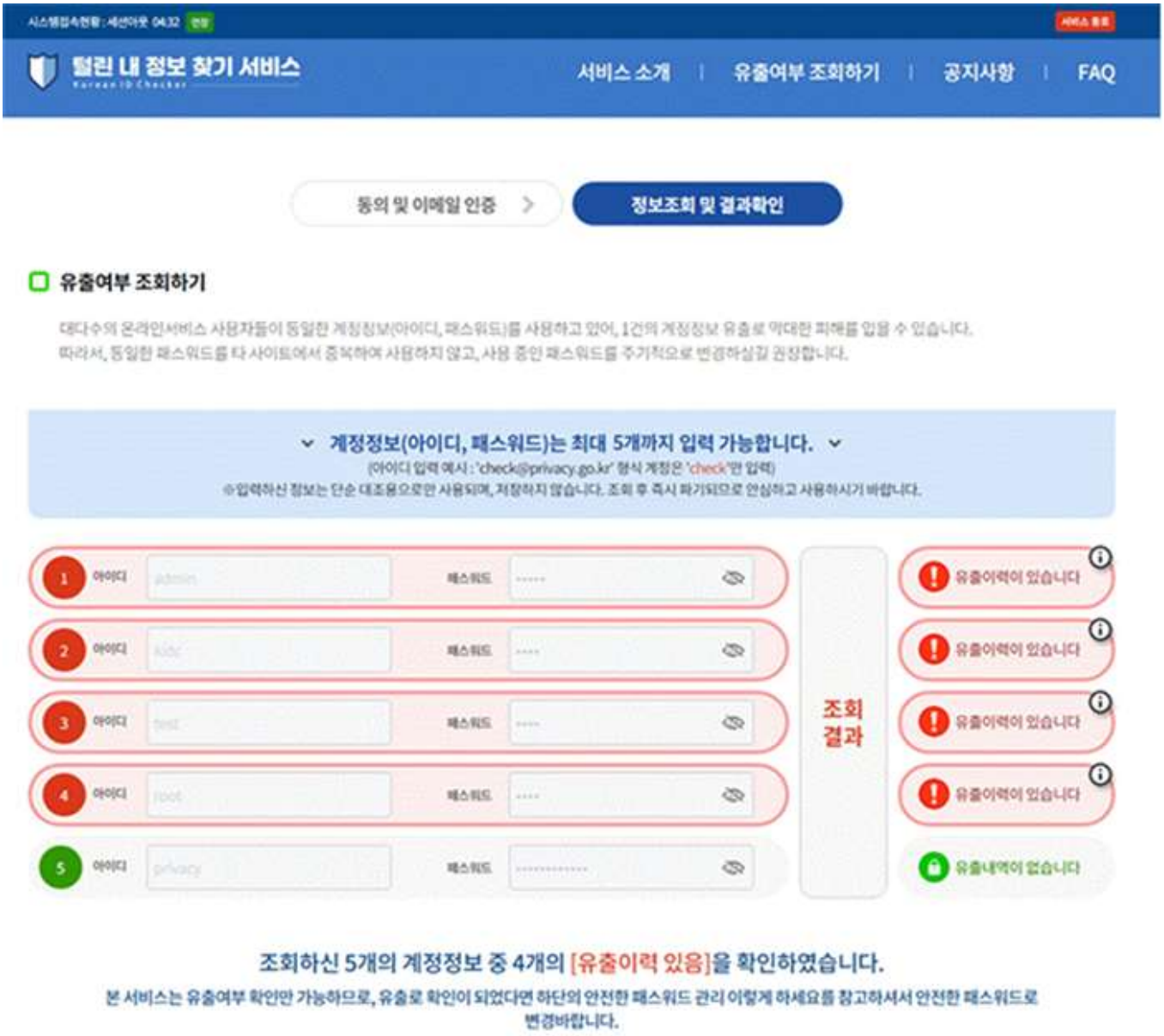
정보 유출로 인한 피해를 최소화하기 위해 사용자들이 당장 실행에 옮겨 효과를 볼 수 있는 조치는 정보가 유출되었는지 여부를 확인하고 적절하게 대응하는 것이다. 이와 같은 대응을 지원하고 사용자들을 보호하자는 취지에서 국가와 보안 기업에서 관련 서비스 및 보안 기능들을 제공하고 있다.

1. 개인정보보호위원회 '털린 내정보 찾기 서비스'

개인정보보호위원회는 2021년 11월 16일부터 '털린 내정보 찾기 서비스'를 시작했다. 해당 서비스는 평소 온라인상에서 사용하는 계정정보(아이디, 패스워드)를 입력하면, 유출된 이력을 알려준다. 본 서비스는 ▲이메일 인증 ▲계정탈취 방지인증 등 2단계 이용자 인증을 적용해 안전성을 높였고, 이메일 계정 하나로 총 5개 계정정보를 조회할 수 있다 (PC/모바일 모두 이용 가능).

[그림 5] 털린 내정보 찾기 서비스 이용 순서

털린 내정보 찾기 서비스는 개인정보위원회와 한국인터넷진흥원이 자체 확보한 다크웹 불법 유통 국내 계정정보 2천 3백만여건과 구글(Google)의 패스워드 진단 서비스 40억여건 등을 활용하여 유출여부를 확인할 수 있도록 구성했다.



[그림 6] 유출된 정보가 있을 경우 화면

사용자가 조회를 통해 유출 이력을 확인한 경우에는 우선, 서비스 내 '안전한 패스워드 선택 및 이용 안내' 메뉴에 따라 비밀번호를 변경한다. 또, 유출된 계정의 웹사이트에서 '휴대전화 인증코드 적용' 등 2차 인증 서비스를 제공하는 경우, 이를 적용하여 추가 피해를 예방한다. 더 이상 사용하지 않는 웹사이트는 회원탈퇴를 위해 'e프라이버시 클린서비스(https://www.eprivacy.go.kr)'를 이용하여 삭제 처리하는 것도 가능하다.

실제 서비스 이용 및 자세한 정보는 '털린 내정보 찾기 서비스' 홈페이지에서 확인할 수 있다.
▶털린 내정보 찾기 서비스 바로가기

2. AhnLab TIP 딥웹 & 다크웹 모니터링

안랩은 올 8월, 자사 차세대 위협 인텔리전스 플랫폼 'AhnLab TIP'에 딥웹·다크웹 및 언더그라운드 포럼의 다양한 사이버 보안 위협요소를 수집 및 가공해 고도화된 위협 인텔리전스를 제공하는 'DDW(Deep & Dark Web) 모니터링 기능'을 도입했다.

AhnLab TIP의 'DDW 모니터링 기능'은 ▲Tor(토르)네트워크/I2P 등 익명 네트워크 내 유통되는 다양한 사이버 위협 정보에 대한 키워드 검색 ▲딥웹·다크웹 상 침해지표(IOC, Indicator of Compromise) 및 공격자 정보 확인 ▲소속 조

직 및 서비스 계정 데이터의 딥웹·다크웹 상 노출여부 확인 ▲DDW 동향 보고서 등 다양한 위협 추이 데이터를 제공한다.

*Tor(The Onion Router): 온라인 상에서 익명을 보장하고 검열을 피할 목적으로 사용하는 네트워크 우회 및 익명화 툴

* I2P(Invisible Internet Project): 애플리케이션이 서로 익명으로 안전하게 메시지를 송수신할 수 있게 해주는 네트워크 레이어

안랩은 자체 개발한 'DDW 스크랩퍼(Deep & Dark Web Scraper)'를 활용해 다크웹 상의 데이터를 자체 수집·처리·분석해 연계 정보를 제공하는 한편, DDW 전문업체와의 제휴를 기반으로 더욱 풍부하고 심화된 정보를 제공한다.

AhnLab TIP를 사용하는 조직 보안 담당자는 'DDW 모니터링 기능'을 통해 접근이 어려운 익명 네트워크 및 커뮤니티에서 수집된 주요 보안위협 관련 정보를 확인하고, AhnLab TIP에서 제공하는 다양한 위협정보와 연계해 통합 위협 인텔리전스를 확보할 수 있다. 특히, 고객이나 직원의 개인정보, 보안 장비 및 IT 환경 취약점, 악성코드 정보 등을 파악해 신속하게 위협을 인지하고 대책 수립 및 대응이 가능해 조직의 전반적인 정보보호 절차를 강화할 수 있다.

결론: 가장 효과적인 보안 방법은 '예방'

우리는 감기에 걸리면, 병을 낫게 하고 아픔을 최소화하기 위해 다양한 방법을 활용한다. 병원을 찾아 진료를 받은 뒤 해열제 혹은 항생제를 처방 받거나, 자체적으로 따뜻한 차를 마시고 충분한 휴식을 취한다. 이와 같은 조치를 취하면, 대부분의 경우 감기가 호전되는데 도움이 된다. 하지만, 근본적으로 가장 좋은 것은 감기에 걸리지 않고 건강을 유지하는 것이다. 이를 위해, 손을 자주 씻고, 수분을 충분히 보충하는 등 기본 건강 수칙을 지키며 생활한다. 코로나19 팬데믹 이후 마스크를 쓰고 생활하는 것도 같은 이유에서다.

사이버보안, 특히 이번 글에서 다뤘던 정보 유출과 관련된 피해는 위 감기 예시와 같은 맥락에서 이해해 볼 수 있다. 정보가 유출된 후에 후속 조치들을 통해 피해를 제어하는 것도 중요하지만, 최선은 기본 보안수칙을 잘 지켜 정보 탈취를 사전에 차단하는 것이다. 우선, 웹 사이트나 프로그램을 사용할 때 가급적 계정정보는 저장하지 않는 것이 좋다. 물론 편리한 기능이지만, 이번 글에서 살펴본 바와 같이 인포스틸러 악성코드에 감염되면 저장된 정보는 쉽게 유출되기 때문에 사용을 최소화해야 한다.

또, 안랩 뿐만 아니라 다른 기관들에서도 항상 강조하는 ▲불법 소프트웨어 다운로드 및 사용 ▲신뢰할 수 없는 웹사이트 접속 ▲의심스러운 메일 첨부파일 실행 및 URL 클릭 등을 '지양'해야 한다. 또한, 백신 등 보안 소프트웨어와 사용 중인 프로그램들이 최신 버전으로 업데이트 되어 있는지 항상 확인해야 한다.

인포스틸러는 그 동안, 그리고 지금 이 순간에도 다양한 유형의 악성코드가 생성되어 사용자들의 민감 정보를 노리고 있다. 안랩은 2018년부터 2022년까지 인포스틸러 악성코드의 동향을 상세 분석한 '인포스틸러 악성코드 동향 보고서'를 자사 위협 인텔리전스 플랫폼 'AhnLab TIP'를 통해 공개했다. 해당 보고서에서 분석한 주요 악성코드들의 목록은 다음과 같다.

이름	경로
Arkei	Vidar, Oski, Mars 등 변형 존재
Bhunt	VMProtect혹은 Themida로 패킹. NirSoft사의 WebBrowserPassView로 정보 수집
BlackGuard	2021년 4월부터 판매 중. 버그가 많다는 평가
Cold	2022년 2월 처음 발견
Eternity	2022년 3월 발견된 Eternity Project 중 하나.
FFDroider	2022년에 발견되었으며 소셜 미디어 세션이 확인되면 추가 정보 탈취
Ginzo (Zingo)	소스코드가 공개되어 변형 등장 가능
Jester	2021년 7월 발견. TOR 를 통해 통신
Lightning	2022년 3월 처음 발견. 러시아어 다크 웹에서 판매
Mars	2021년 발견 Arkei 계열 최신 변형
Oski	Oski 2019년 발견 Arkei 계열 변형
Prynt	Prynt Market에서 판매 중인 상용 프로그램
Raccoon	2019년부터 판매 중이며 2022년 3월 중단 선언 후 2022년 5월 새로운 버전으로 재등장
Redline	2020년 2월부터 판매 중. 인기 스틸러 중 하나
Stealerium	2022년 5월 등장. 소스 및 빌더 공개
Vidar	2018년 발견 Arkei 계열 변형

[표 5] 주요 인포스틸러 악성코드

각 인포스틸러 악성코드에 관한 상세 분석 내용 및 보고서 전문은 AhnLab TIP 구독 서비스를 통해 확인할 수 있다.

▶ATIP 포털 바로가기

AhnLab TI개발팀