보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

2022년 사이버 위협 트렌드 Top 10 돌아보기

AhnLab 2022-12-05

2021년 12월 촉발된 Log4j 취약점 여파가 잔존하는 상태에서 출발한 2022년은 전 세계적으로 정치와 문화 이벤트가 다수 예정되어, 사이버 영역에서의 보안 위협이 그 어느 때 보다 많이 예견된 해였다. 매년 그 어떤 글로벌 행사보다 가장 빨리 개최되고, 여러 기업들이 기술력과 한 해 전략 방향성을 선보이며 전 세계인의 이목을 집중시키는 CES에서도 2022년의 5개 화두 중 하나로 사이버 보안이 등장했다. 이는 사이버 보안 영역에서의 활동에 보다 몰입하게 만드는 동기가 되지 않았나 생각한다. 또, 누구도 예상치 못했던 러시아-우크라이나 전쟁과 치열한 사이버 공격자들의 활동은 지금까지 경험할 수 없었던 새로운 상황을 맞기도 했다.

정신 없이 달려온 2022년 한 해 동안 국내/외에서 등장했던 주요 사이버 보안 위협들을 되돌아 보며, 현재 우리의 보안 현황을 짚어보고, 문제를 해결 혹은 완화해 나가는 방안들을 생각해 보았으면 한다.

#1. Log4j 취약점 등장과 여파, 그리고 남은 것은...

Log4j는 인기있는 오픈소스이며, 오랫동안 다양한 버전이 등장했다. Log4j 취약점이 발견된 이후, Log4j를 필수 요소로 활용한 응용 프로그램들이 많아 제조사와 사용 기업에서 현황 파악을 수행하는 것 자체가 만만치 않았다. 또, 악용 가능한 보안 취약점들이 계속 등장하여 관련 대응을 수행하는 조직들의 무중단 업무가 지속되었다.

Log4j 취약점이 존재하는 보안이 취약한 서버에 암호화폐 채굴기 및 연관된 악성코드가 설치된 사례들이 많지는 않지만 일부 확인된 경우가 있다. 그 중, 가장 주목할만한 것은 타깃 랜섬웨어 그룹 '나이트스카이(NightSky)'의 Log4j 취약점 악용이다.

나이트스카이는 기업 내부 정보를 탈취해 모두 암호화한 뒤, 복호화 조건으로 금전적 보상을 요구하는 것으로 한 차례 협박을 가하며, 기업이 침해를 당했다는 소식과 함께 내부 정보를 다크 웹(Dark Web)에 공개하겠다는 것까지 이중 협박을 가하는 것으로 유명하다. 이는 암호화폐 채굴기나 인포스틸러(InfoStealer)와 같이 PC 사용자의 정보를 수집해 유출하는 정도의 악성코드가 설치되는 것과는 규모가 다른 사이버 공격이다.

나이트스카이는 다른 타깃 랜섬웨어 그룹들처럼 왕성한 활동을 하지는 않았으나, Log4j 보안 취약점을 악용했다는 점과 피해 기업과의 소통에 토르(Tor)가 아닌 로켓챗(Rocket.Chat)을 이용했다는 특징들이 주목받고 있다. 다른 타깃 랜섬웨어들의 행보에 영향력을 행사할 정도의 랜섬웨어는 아니지만, 비교적 무게감 있는 랜섬웨어가 Log4j를 악용한 사례에 해당된다.

다시 Log4j 취약점으로 돌아오면, 대부분은 최종 악성코드 설치까지 진행되지 않고 문자열 처리 후 악의적인 서버와의 통신까지만 진행했는데, 이는 오히려 보안 담당자들의 부담을 가중시켰다. 이는 공격자들의 의도를 파악할 수 없을 뿐만 아니라, 보안 패치를 완료하기 전까지는 언제 어떤 보안 사고가 발생할 지 모른다는 불안감이 계속되기 때문이다.

개별적인 보안 패치에 대한 가이드는 완료되었고, 관련 모니터링도 국가와 기업 수준에서 철저하게 진행되고 있는 현 시점, 각 애플리케이션 수준에서의 문제점은 없는지 되짚어봐야 한다. 이제, 기업들이 취약한 문자열을 지속적으로 보내오는 서버들과의 통신을 과감하게 차단하는 정책도 잘 적용하고 있으므로, 그 현황과 변화 추이를 함께 분석하고 결론을 도출해 추후 유사한 사이버 보안 위협 등장 시 의사결정에 활용하면 도움이 될 것이다.

그리고, Log4j 취약점에 혼신을 다해 맞대응하고, 현재도 각자의 위치에서 묵묵히 임무에 충실하고 있을 모든 보안 담당자들 및 유관 부서에 감사함과 수고의 박수를 보낸다.

#2. 타깃 랜섬웨어들의 마스터키 공개와 복호화 도구 제작

먼저, 마스터 키를 공개한 주요 타깃 랜섬웨어 그룹과 활동 기간은 [표 1]과 같다.

랜섬웨어 그룹	활동 기간
메이즈(Maze)	2019.05 ~ 2020.10
에그레고르(Egregor)	2020.09 ~ 2021.02
세크메트(Sekhmet)	2020.03 ~

[표] 마스터 키 공개 랜섬웨어 그룹 및 활동 기간

타깃 랜섬웨어 그룹의 1세대라 할 수 있는 메이즈(Maze) 랜섬웨어 그룹은 여러 글로벌 기업(국내 기업 포함)들을 표적 공격하고, 내부 정보를 자신들의 공식 웹 페이지에 공개해 이중 압박을 수행하며 유명세를 탔다. 활발한 공격으로 금전적 이득과 명성을 쌓아가던 이들은 2020년 10월 돌연 은퇴를 선언하고 사라졌다. 다만, 이들이 사라지기 직전에 에그레고르(Egregor) 랜섬웨어 그룹이 등장하는데, 분석가들 중 일부는 메이즈 랜섬웨어 그룹 중 일부가 에그레고르 그룹에 합류한 것으로 추정하는 이들도 있다.

에그레고르 랜섬웨어 그룹은 대형 서점체인 '반즈앤노블(Barnes & Noble)', 소프트웨어 개발사 '크라이텍(Crytek)', '유비소프트(Ubisoft)' 등을 공격하며 타깃 랜섬웨어의 유명세에 편승했다. 이후 2021년 2월, 유럽 수사기관의 공조에

따라 넷워커(Netwalker) 랜섬웨어 그룹과 함께 검거되면서 서비스가 강제 종료된다. 세크메트(Sekhmet) 랜섬웨어는 랜섬노트가 에그레고르와 동일해 같은 랜섬웨어 그룹인 것으로 판단된다.

이상 언급된 랜섬웨어들의 마스터키와 이를 활용한 복호화 도구가 제작 및 공개되었다. 공개한 이는 이들 랜섬웨어 제작자 그룹에 속했던 인원으로 추정되며, 유럽과 동구권에서 진행되고 있는 랜섬웨어 제작자 그룹 검거와는 무관하다고 밝히고 있다.

랜섬웨어를 수학적으로 암호를 찾아 풀어내는 것은 현재 기술로는 한계가 있다. 최근 화두가 되고 있는 양자 컴퓨팅이 특별한 제약 없이 일상적으로 이용 가능한 환경이 되면 이야기가 달라지겠지만, 현 시점에서는 안타깝지만 불가능하다고 보는 것이 맞다. 그렇다고 이번 사례와 같이 제작자 그룹 혹은 수사기관에 의한 마스터키 공개를 기다리는 것 또한 항상 긍정적이라고만 볼 수는 없다. 이번 마스터키 공개는 이들 타깃 랜섬웨어 그룹이 은퇴 혹은 퇴출되고 어느 정도 시간이 흐른 뒤 누군가의 선의에 의해 진행된 것이며, 현재까지 마스터키가 공개된 사례는 손에 꼽을 정도로 드물다.

어찌 되었건, 전 세계적으로 큰 피해를 일으켰던 1세대 타깃 랜섬웨어 그룹 메이즈의 마스터키 공개와 복호화 도구 제작은 그 사실 자체만으로 충분히 의미 있는 사건이다. 혹시, 이들 랜섬웨어로부터 피해를 입어 복호화가 필요한 기업/기관이 있다면, 복호화 도구를 이용한 복구를 시도해 볼 것을 권한다. 참고로, 복호화를 위해서는 랜섬노트 파일이 필요하다.

#3. 랜섬웨어의 양극화

우리가 이름만 들어도 아는, 활발한 공격으로 맹위를 떨치는 랜섬웨어들이 있다. 그 중 하나가 바로 록빗(LockBit) 랜섬웨어다. 진화를 거듭한 록빗 3.0은 파일 암호화, 탈취한 정보 공개에 디도스(DDoS) 공격까지 더해, 3중 협박을 가하는 타깃형 랜섬웨어로 발전했다.

'타깃형' 랜섬웨어라는 단어에서도 알 수 있듯, 이제 랜섬웨어가 누군가를 우발적으로 공격하는 경우는 거의 없다. 이들은 항상 치밀하게 계산된 의도를 가지고 철저하게 준비된 공격을 감행한다는 사실을 잊어서는 안 된다.

안랩이 ASEC 블로그를 통해 공개한 록빗 3.0의 공격 사례를 보면, 공격자는 입사지원서를 위장한 악성 워드 문서를 유포하는데, 유포 파일명에 '임규민.docx', '전채린.docx' 등 사람 이름을 사용해 교묘하게 위장했다.

공개된 공격 패턴만 보더라도 이들의 공격이 우발적인 것이 아님을 알 수 있다. 이와 같은 유형의 공격들은 대부분 '조직 내부 네트워크 또는 피해자 컴퓨터 침투 > 악성코드 설치 > 의도에 따라 추가적인 악성코드 혹은 공격 도구 배포 > 관리자 계정 도용 > 시스템 복구 방해 목적의 복원 이미지 삭제 및 서비스 종료 > 목표 달성' 순으로 전개된다. 이들이 기업이나 조직 내부 접속에 성공한 이후 행동들을 봐도 의도를 가지고 접근했다는 것을 충분히 유추할 수 있다.

한 가지 주목할 것은 신규 랜섬웨어의 제작 비율은 해를 거듭할수록 줄어들고 있다. 이제, 일반적인 랜섬웨어 제작 & 유포는 큰 이익을 가져다 주지 못하며, 랜섬웨어 시장에서도 일종의 양극화가 진행되고 있는 것이다. 유명하고 규모가 큰 타깃형 랜섬웨어들은 적극적으로 정부 기관과 주요 기업들을 공격하여 이윤을 챙기고 있는 반면, 다른 수 많은 랜섬웨어들은 한두번 활동하고 사라지기도 한다. 전체적인 랜섬웨어 수치가 감소하는 양상을 보이고 있지만, 실제 위협이 되고 있는 상위권 타깃형 랜섬웨어는 공격의 수위를 낮추지 않고 있음을 기억해야 한다.

#4. 보안 체계 무력화에 진심인 공격자들

PC와 서버에서 가동 중인 보안 체계를 무력화하는 것은 마치 영화에서 침입자가 보초를 제거하는 것과 동일한 원리이다. 보초의 역할 또한 미확인 혹은 의심스러운 상대를 막는 것이니, 그 역학 관계도 유사한 면이 있다.

사이버 보안의 영역에서도 공격자와 방어자의 공방은 지속되고 있으며, 기술의 발전 역시 계속되어 오늘날에 이르렀다. 안티바이러스(AV) 제품은 정상적인 OS 환경에서 악성코드로 인식되는 파일들을 제거하고, 공격자들은 자신을 방해하는 AV 제품이 정상 동작하지 못하도록 하기 위해 다양한 시도들을 하고 있다.

그 동안은 공격자가 AV 제품 제거(uninstall)를 시도할 경우, 캡챠 코드를 입력하는 과정을 적용해 이를 방어해왔다. 하지만, 최근에는 공격자가 직접 개입하는 등 다양한 방식으로 방어 체계를 무력화하기 위한 시도들이 확인되고 있다. 두 가지 예시를 살펴보자.

먼저, 안랩이 지난 9월 발간한 '라자루스 공격 그룹의 BYOVD를 활용한 루트킷 악성코드 분석 보고서'를 보면, 공격자는 오래된 버전의 이니텍(INITECH) 프로세스를 악용해 기업에 초기 침투를 수행한 뒤 공격자 서버로부터 루트킷 악성코드를 다운로드 받아 실행했다. 루트킷 악성코드는 취약한 드라이버 커널 모듈을 악용하여 직접적으로 커널 메모리 영역에 대해 읽기/쓰기 행위를 수행해 AV를 포함한 시스템 내 모든 모니터링 시스템을 무력화시켰다.

또, 최근 '한국형' 랜섬웨어로 이름을 알리고 있는 '귀신(Gwisin)' 랜섬웨어는 안전모드로 재부팅시킨 후 파일을 암호화하는 방식으로 AV 제품을 우회한다. 안전모드에서는 최소한의 서비스만 동작하므로, 윈도우 기본 드라이버를 제외하고는 로딩되지 않아 AV 제품의 감시도 우회할 수 있게 된다.

이처럼, 공격자가 보안 체계 무력화에 힘을 쏟고 있는 상황에서 방어자가 선택할 수 있는 최선의 방안은 자신의 보안 체계를 모니터링하고 이를 적극적으로 관리하여 공격자에게 빌미를 제공하지 않는 것이다. 공격자의 공격 동향을 예의 주시하는 것은 물론 자신의 현재 상태를 적극적으로 파악하고 대처하는 것이 중요하다. 우리의 보안 체계를 무너뜨리는데 진심인 공격자에게 우리도 '빈틈없는' 진심으로 맞서야 한다.

#5. 국제 공조를 통한 사이버 위협자 검거

사이버 위협자들의 검거 소식은 1년 전 국내 클롭(CLOP) 랜섬웨어 공조자 검거로부터 출발했다고 해도 과언이 아니다. 이 사건은 주도 세력 검거의 시발점이 되었고, 이후 우크라이나에서의 국제 공조를 통한 검거로까지 이어졌다. 이 밖에도, 2021년 10월 록커고가(LockerGoga) 랜섬웨어 관련자와 그 외 다수 사이버 공격을 수행한 관련자 검거 소식까지 확인할 수 있었다.

최근에는 랜섬웨어 그룹의 이름은 명확치 않으나 50여개국에서, 약 100만 달러 규모의 피해를 일으켰던 사이버 위협자를 검거했다는 소식까지 나오는 등 우리나라 뿐만 아니라 서방 주요국들과의 적극적인 공조를 통해 사이버 범죄에 가담한 인원들을 색출해 검거하고 있다.

한편, 지난 1월에는 러시아에서 국내에서 블루크랩(BlueCrab) 랜섬웨어로 알려져 있고, 해외에서는 소디노키비(Sodinokibi) 랜섬웨어로 알려진 레빌(Revil) 랜섬웨어 그룹 관련자를 검거 했다는 소식이 전해졌다. 러시아에서 사이버 범죄자 검거 소식이 전해진 것은 상당히 이례적이다. 자국민 보호보다 국제 사회와의 공조를 선택하는 것이 전략적으로 낫다는 판단일 수 있으며, 다크사이드(DarkSide) 랜섬웨어 그룹 및 레빌 랜섬웨어 그룹 배후와 러시아는 무관하다는 일종의 '액션'일 가능성도 있다.

미국과 러시아 상호 간 사이버 위협에 대해서는 인정하지도, 협력하지도 않았던 전례들을 볼 때, 러시아의 선택은 향후에 어떤 전략적 선택을 해 나갈 것인지 주의 깊게 살펴보게 하는 단초를 제공했다고 할 수 있다.

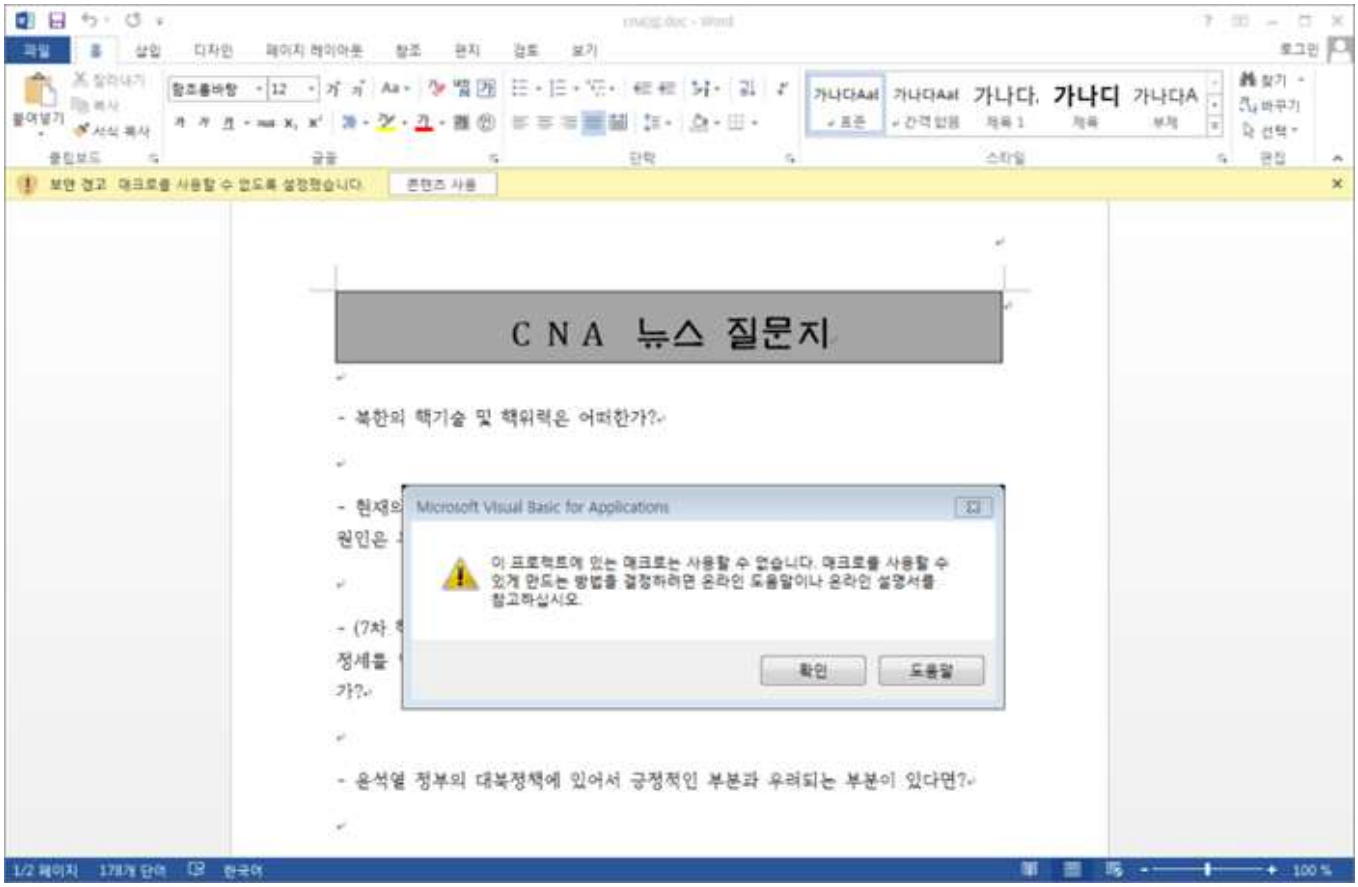
#6. 국가 배후 사이버 공격 그룹의 행보

지난 3월, 우리나라에서는 제20대 대통령 선거가 있었다. 당시, '빅 이벤트'가 있는 우리나라를 두고 각국의 사이버 공격이 어떻게 전개될 것인지 각자의 영역에서 예의 주시했을 것이다.

현재는 우리나라와 정치 혹은 군사적인 대척점에 있는 국가들이 이처럼 특정 시기에 직접적인 사이버 공격을 감행할 경우 실제 이익을 취할 수 있는 부분이 거의 없다. 다만, 간접적으로는 여러 상황에 대비해, 각 분야에 자신들이 필요로 하는 정보가 있는지 찾을 방법들을 강구해온 것으로 보인다.

그 일환으로, 악의적인 스크립트가 삽입된 문서 파일을 제한된 수신자에게만 발송하는 공격을 지속하고 있다. 이 공격에 사용되는 악의적인 스크립트는 기본적으로 일반 사용자들이 읽을 수 없도록 난독화(Obfuscation) 되어 있다. 문서 파일을 열람해 악의적인 스크립트가 동작하면, 사용자 PC에 저장된 민감 정보를 수집 및 유출하며, PC 자체에 대한 정보도 함께 수집해 가는 형식이다. 이는 공격자들이 목표 대상을 명확하게 구분하기 위한 방편인 것으로 해석된다.

한 가지 사례를 예시로 보면, 최근 안랩은 '뉴스 설문지로 위장하여 유포 중인 악성 워드 문서' 게시글을 ASEC 블로그에 공개했다. 악성 워드 문서의 파일명은 'CNA[Q].doc'로 대북 관련 인사를 대상으로, CNA 싱가포르 방송 인터뷰를 위장했다. 사용자가 타이핑을 시작하면 매크로를 실행해야 한다는 메시지 박스가 나타난다. 사용자는 문서 작성을 위해 콘텐츠 허용 버튼을 클릭하게 되고, 문서에 포함된 악성 VBA 매크로가 실행되는 형태다.



[그림] 워드 문서 내용과 타이핑 시 나타나는 메시지 박스

이러한 유형의 공격은 사용자 정보를 수집해 유출하는 인포스틸러(InfoStealer)와도 유사하다고 볼 수 있다. 하지만, 위 사례와 같이 국가 배후 사이버 공격 그룹은 뚜렷한 목적을 가지고 움직인다는 결정적인 차이가 존재한다. 현재 공격의 주요 타깃이 되고 있는 산업군은 정치, 통일, 외교, 항공우주, 방위 산업, 에너지 & 재생 에너지 등이 있다. 따라서, 국가 관련 주요 기술 혹은 기업의 핵심 기술 및 자료를 다루는 조직에서는 경계를 더욱 철저히 해야 한다.

#7. 주목 받는 멀티팩터 인증, 우리에게 남겨진 숙제는?

2021년 5월, 러시아 사이버 범죄자가 비정부기구(NGO)에서 기본 멀티팩터 인증(MFA) 프로토콜로 설정되었지만, 구성이 잘못된 계정을 이용해 MFA용 새 장치를 등록하고 피해자 네트워크에 접근하는 사건이 발생했다. 이 과정에

서, 공격자는 윈도우 인쇄 스풀러(spooler) 취약점인 'Print Nightmare(CVE-2021-34527)'를 악용해 시스템 권한으로 임의의 코드를 실행했다.

MFA는 허가된 2개 이상의 기기를 통해 사용자를 확인하기 때문에, 분명 공격자들이 껄끄럽게 생각하는 방어 체계 중 하나다. 다만, 이를 우회하는 사고가 발생하다 보니 여러 고민들이 생겨나고 있는 것이다. 물론 MFA가 모든 공격을 막아주는 100% 완벽한 보안 체계라고 할 수는 없지만, 올바르게 잘 활용한다면 공격자들에게 불편을 초래하여 손쉽게 의도하는 바를 이룰 수 없도록 할 수 있다.

따라서, 위와 같은 보안 사고가 발생했다는 이유로 MFA 자체를 의심하고 적용하지 않는 것보다는 이를 적극적으로 적용하되, 구성 정책을 제대로 검토하여 오남용 될 수 있는 여지를 없애는 것이 올바른 접근법이다. 또한, 조직 내 사용자 계정 중 더 이상 존재하지 않는 계정정보는 주기적으로 점검하여 제거하고, 알려진 보안 취약점에 대해 패치를 빠르게 적용한다면 위험 요소를 최소화할 수 있다. 이와 같은 조치들을 지속적으로 수행하면, MFA의 효과도 극대화할 수 있고 나아가 보다 안전한 환경에서 비즈니스에 집중할 수 있을 것이다.

#8. 인포(Info)를 스틸(Steal)하라

인포스틸러(InfoStealer)는 정보 탈취형 악성코드로, 웹 브라우저나 이메일 클라이언트 같은 프로그램에 저장되어 있는 사용자 계정 정보나 암호화폐 지갑 주소, 파일과 같은 사용자의 정보들을 탈취하는 것을 목적으로 한다. 2022년 3분기 ASEC 리포트를 보면, 해당 기간 동안 유포된 악성코드 중 인포스틸러가 55.1%를 차지할 정도로 활발하게 공격에 활용되고 있다.

최근, 인포스틸러 악성코드 동향을 보면 서로 간의 연계와 변화가 활발하게 이뤄지고 있다. 대표적인 사례로, 온라인 뱅킹(Banking) 악성코드 계열 중 하나인 이모텟(Emotet)이 있다. 그 동안 등장과 사그라짐이 잦았던 이모텟은 트릭봇(Trickbot)과의 연계를 통해 빠르게 유포되었지만, 2021년 초 인프라가 수사기관에 압수되며 잠잠해졌다.

그로부터 9개월 뒤인 2021년 말 다시 부활한 이모텟은 종전 봇(bot) 계열 악성코드와의 연동을 멈추고, 자체적인 스팸 발송 기능을 탑재하여 스스로 유포하는 능력을 갖춰 돌아왔다. 여기에, 이모텟 본연의 정보 수집 & 유출 기능이 고도화되었다. 이제 이모텟은 지난해부터 주요 악성코드 계열로 급부상한 인포스틸러에 포함되어도 무리가 없으며, 안랩에서도 향후 행보를 예의주시하고 있다.

#9. IoT 기기 취약점 공격

네트워크로 연결되는 각종 IoT 기기들에 대한 취약점 공격이 끊임 없이 이어지는 가운데, 전 세계적으로 여러 고객들이 사용하는 무선공유기(혹은 라우터) 취약점을 악용한 사이버 공격이 기승을 부리고 있다. 공유기 한 대로 유/무선 인터넷에 연결되는 기기들을 모두 조종할 수 있다는 점을 감안할 때 파급 효과가 상당하다고 볼 수 있다.

공격자들이 무선공유기 혹은 라우터를 장악해서 무슨 이득을 얻을 수 있을까? 사용자가 입력하는 각종 개인정보를 가로챌 수 있고, 사용자 눈에는 정상적인 사이트인 것처럼 위장한 피싱 사이트를 제작해 접속하도록 유도할 수도 있다. 또, 장악된 라우터는 네트워크 망에 연결된 불특정 다수를 상대로 디도스 공격을 감행하는데 활용될 수도 있다. IoT 기기를 대상으로 공격을 감행하는 대표적인 악성코드로는 미라이(Mirai)와 쓰나미(Tsunami) 등이 있다.

이와 같은 공격에 대한 보안을 위해서는 1차 공격 대상이 되는 라우터(혹은 유/무선 공유기)에 대한 보안 취약점 패치를 수행하고, 장악된 라우터에 의해 감행되는 디도스 공격 및 로그인 계정에 대한 Brute Force 공격 여부에 주의를 기울여야 한다. 또, 로그인 계정을 지속적으로 관리하고, 로그인 가능한 미사용 계정은 가능한 제 때 제거해야 하며, 기기에 대한 접근을 제한된 사용자에게만 허용하는 보안 정책을 적용해야 위협으로 인한 피해를 최소화할 수 있다.

#10. 마이너(Miner), 그들만의 경제

마이너(Miner)는 암호화폐 채굴을 위한 목적으로 제작된 응용프로그램을 통칭하는 것으로, 정식 명칭은 코인 마이너(Coin Miner)이나 줄여서 마이너라 부른다.

암호화폐에 대한 관심이 높았던 2018년 초에는 웹 브라우저를 통한 크립토재킹(Crypto Jacking) 악성코드가 엄청난 피해를 발생시켰다. 올해, 경제 침체가 가속화되면서 주목도는 떨어졌지만 암호화폐 채굴 관련 악성코드는 관심도의 차이만 존재할 뿐 꾸준히 제작되고 유포되고 있다.

오히려, 최근의 마이너는 영역을 확장하기 위한 움직임을 보이면서, 사용자 정보를 수집해 유출하는 인포스틸러(InfoStealer)와 연대하는 모습까지 연출하고 있다. 앞서 설명한 바와 같이 인포스틸러가 탈취하는 정보에는 웹 브라우저나 응용 프로그램에 저장된 사용자 계정정보와 더불어 암호화폐 지갑주소도 포함되는데, 여기에 아주 긴 암호화폐 지갑 주소를 공격자의 지갑 주소로 바꾸는 하는 클리퍼(Clipper) 기능까지 탐재한 악성코드가 등장하기 시작했다.

참고로, 암호화폐 지갑주소를 바꿔치기 하는 기능을 가진 악성코드로는 2017년에 활동했던 크립토 셔플러(Crypto Shuffler)가 있었는데, 이것이 클리퍼(Clipper)로 다시 태어나면서 기능이 보강되었다. 지갑 주소를 악성코드 내에 담고 있어, 파일 사이즈가 수십 메가 바이트에 달했던 크립토 셔플러와 달리 클리퍼는 내부 연산구조를 통해 연관 암호화폐를 판단하고 공격자의 주소로 바꿔치기 하는 기능을 통해 크기를 대폭 축소했다. 공격자 입장에서는 크기에 대한 부담을 줄이면서 다양한 암호화폐 지갑을 노릴 수 있고, 정보를 유출하는 인포스틸러 기능 뿐만 아니라 코인 마이너의 채굴 기능까지, 다양한 악성코드의 장점을 종합적으로 누릴 수 있는 악성코드인 것이다.

그 동안, 마이너는 조직과 기업의 자원을 고갈시키는 정도의 위해만 가하는 것으로 인식되어 왔다. 하지만, 그들만의 경제 구조 속에서 지속적으로 생산되어 활동하고 있으며, 단순한 기능만 수행하던 과거에서 벗어나 주요 정보를 수집 및 유출하고 암호화폐 지갑 주소까지 탈취하는 등 직접적인 타격을 가할 수 있게 됐다. 조직들은 이러한 변화를 인지하고, 내부 인프라에서의 마이너 활동에 대한 점검을 지속적으로 수행해야 한다.

AhnLab 대응팀 박태환 팀장