OUCH! | 2017 년 6월호

전 국민대상 월간 정보보호 인식제고 뉴스레터

OUCH!

이달 호 주제..

- 개요
- 패치
- 백업
- 피싱

워너크라이 랜섬웨어의 교훈

개요

최근에 “워너크라이(WannaCry)”라는 새로운 사이버공격에 대한 엄청난 뉴스를 보았을 것입니다. “워너크라이”는 전 세계 20만대의 컴퓨터를 감염시켰으며, 영국의 병원을 포함하여 다양한 조직의 데이터를 사용하지 못하도록 하였습니다. 이 공격이 많은 관심을 받은 몇 가지 이유가 있습니다. 첫째 윈도 컴퓨터의 취약점을 공격하여 컴퓨터에서 컴퓨터로 빠르게 확산되었습니다. 둘째 이 공격은 “랜섬웨어”라고 불리는 일종의 악성코드였습니다. 이 악성코드가 컴퓨터를 감염시키면 모든 파일을 암호화하여 사용자가 데이터에 접근할 수 없게 만듭니다. 데이터를 복구 할 수 있는 유일한 방법은 백업 또는 모든 데이터를 복호화하기 위해 공격자에게 300 달러의 몸값을 지불하는 것입니다. 셋째 가장 중요한 것은 이 공격이 결코 일어날 수 없는 것이었습니다. “워너크라이”가 공격한 윈도 컴퓨터의 취약점은 마이크로소프트에서 수 개월 전에 패치를 발표하여 잘 알려져 있었습니다. 그러나 많은 조직에서 패치를 설치하지 않았거나, 윈도 XP와 같은 구형의 운영체제를 사용하고 있어서 더 이상 사용할 수 있는 패치가 없었습니다. “워너크라이”와 같은 공격에 결코 감염되지 않도록 하기 위해 취할 수 있는 세 가지 간단한 단계가 있습니다.

객원 편집자

조한스 울리치박사는 SANS 기술연구소장이며, Dshield.org 창립자이다. 조한스는 사이버보안 위협을 모니터링하는SANS 인터넷 스톰센터을 운영하고 있다. 조한스는 웹 응용보안(DEV522), 침입탐지(SEC503) 및 IPv6(SEC546)을 강의한다.

패치

무엇보다 먼저 컴퓨터, 모바일 기기, 앱 및 인터넷에 연결된 모든 것이 최신 버전인지 확인해야 합니다. 사이버 범죄자는 컴퓨터 기기가 사용하는 소프트웨어의 새로운 취약점을 끊임없이 찾고 있습니다. 취약점을 발견하면 특수한 프로그램을 사용하여 사용중인 기기를 해킹합니다. 한편, 기기에 사용되는 소프트웨어를 만든 회사는 업데이트를 발표하면서 이러한 취약점을 열심히 수정합니다. 컴퓨터와 모바일 기기에 이러한 업데이트를 설치하면, 누군가가 해킹하는 것을 훨씬 더 어렵게 만듭니다. 그래서 이번 워너크라이의 확산이 굉장히 실망스러운 일입니다. 이 공격을 중단할 수 있는 업데이트가 마이크로소프트에서 거의 2개월 전에 발표되었습니다. 회사에서 컴퓨터를 최신 상태로 유지했다면 이 공격은 결코 효과가 없었을 것입니다. 기기를 최신 상태로 유지하려면 가능하다면 자동 업데이트를 사용하십시오. 이 규칙은 컴퓨터 및 모바일 기기뿐만 아니라

워너크라이 랜섬웨어의 교훈

인터넷에 연결된 TV, 홈 라우터, 게임 콘솔 또는 언젠가는 차에 이르기까지 네트워크에 연결된 거의 모든 기술에 적용됩니다. 운영체제나 모바일 기기가 오래되어 윈도 XP와 같은 보안 업데이트로 더 이상 지원되지 않는 경우, 지원되는 새로운 버전으로 교체하시기 바랍니다.

워너크라이와 같은 공격으로부터 자신을 보호하는 핵심은 다음 세 가지입니다. 컴퓨터를 최신 상태로 유지하고, 피싱 공격에 유의하고 및 시스템을 백업하는 것입니다.

백업

경우에 따라 랜섬웨어와 같은 사이버공격은 최신의 시스템을 감염시킬 수 있습니다. 그래서 우리를 보호할 수 있는 두 번째 방법은 데이터를 백업하는 것입니다. 백업은 컴퓨터 또는 모바일 기기가 아닌 다른 곳에 저장하는 사용자의 정보 복사본입니다. 중요한 데이터를 잃어 버리더라도 백업에서 해당 데이터를 복구할 수 있습니다. 불행히도, 너무 간단하고 저렴하더라도 정기적인 백업을 수행하지 않는 사람이 너무 많습니다. 데이터 백업에는 물리적 미디어 또는 클라우드 기반 스토리지 등 두 가지 방법을 이용할 수 있습니다. 각 방법에는 장단점이 있습니다. 어떤 방법을 사용할 지 잘 모르는 경우 두 가지 방법을 동시에 사용할 수 있습니다.

물리적 미디어는 집이나 사무실에 있는 외장형 USB 드라이브 또는 네트워크로 연결된 드라이브와 같이 사용자가 제어하는 장치입니다. 자신의 실제 미디어를 사용하면 많은 양의 데이터를 매우 빠르게 백업하고 복구할 수 있다는 장점이 있습니다. 이러한 접근 방식의 단점은 랜섬웨어와 같은 악성코드에 감염된 경우 감염이 백업으로 확산 될 수 있다는 것입니다. 백업 시 물리적 미디어를 사용하는 경우 백업 복사본을 오프 사이트의 안전한 위치에 저장해야 합니다. 저장한 백업의 레이블이 올바른지 확인하십시오. 클라우드 기반 솔루션은 파일을 인터넷에 백업하고 저장하는 온라인 서비스입니다. 일반적으로 모든 것을 관리하는 프로그램을 컴퓨터에 설치합니다. 클라우드 솔루션의 장점은 단순합니다. 또한 랜섬웨어에 감염되면 일반적으로 클라우드 기반 백업에 접근할 수 없습니다. 단점은 매우 많은 양의 데이터를 백업하거나 복구하는 데 오랜 시간이 걸릴 수 있다는 것입니다. 클라우드 백업은 개인정보와 보안에 대해서 연구해야 합니다. 즉 백업 서비스는 데이터를 암호화하고 강력한 인증과 같은 강력한 보안 기능을 제공하는 지 확인해야 합니다.

워너크라이 랜섬웨어의 교훈

피싱

마지막으로 악의적인 사람은 항상 공격 방법을 업데이트하고 변경합니다. 사이버 범죄자는 피해자를 공격하고 감염시키기 위해 피싱(Phishing)이라고 하는 또 다른 공격 방법을 사용합니다. 피싱은 사이버 범죄자가 사용자를 속여 감염된 첨부 파일을 열거나 악성 웹 사이트를 방문하도록 유도하는 이메일을 보내는 것입니다. 둘 중 하나를 수행하면 컴퓨터가 감염될 수 있습니다. "워너크라이"는 피싱 공격 방법을 사용하지 않지만, 대부분의 랜섬웨어 공격 등 여러 가지 유형의 공격에 피싱이 사용됩니다. 또한 워너크라이를 개발한 사이버 범죄자들은 앞으로 몇 달 안에 공격 방법을 업데이트하고 피싱과 같은 새로운 기술을 사용하여 더 많은 컴퓨터를 감염시킬 것입니다. 이러한 전자 메일 기반 공격으로부터 자신을 보호하는 열쇠는 상식입니다. 전자 메일이나 메시지가 이상하거나 의심스럽거나 사실로 보기에 좋지 않은 경우 공격 일 가능성이 큽니다.

자세히 알아 보기

securingthehuman.sans.org/ouch/archives를 방문해서 OUCH! 뉴스레터를 읽어 보시고, 월간 OUCH! 정보보호지식 뉴스레터를 구독하십시오. 그리고 SANS 정보보호지식 솔루션에 대해서 좀 더 알아보시기 바랍니다.

한글판

본 문서는 한국의 ITL(http://www.itlkorea.kr)에서 번역하였습니다. ITL 은 미국 SANS 연구소의 한국 파트너로서 IT 거버넌스 및 IT 보안 분야의 최신의 지식과, 양질의 교육과 세미나를 진행하는 교육기관입니다. 추가적인 사항은 itl@itlkorea.kr 로 문의해주시기 바랍니다.

참고자료

악성코드란 무엇인가:	https://securingthehuman.sans.org/ouch/2016#march2016
랜섬웨어:	https://securingthehuman.sans.org/ouch/2016#august2016
백업:	https://securingthehuman.sans.org/ouch/2015#august2015
피싱:	https://securingthehuman.sans.org/ouch/2015#december2015
클라우드 서비스 안전한 사용방법:	https://securingthehuman.sans.org/ouch/2016#november2016

편집위원회 : Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley, 번역:진수희(ITL Inc.)