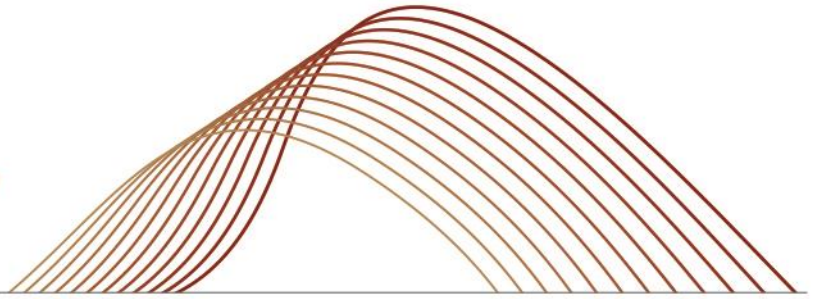
PAUL HASTINGS

STAY CURRENT



May 2017

Follow **@Paul_Hastings**

컴퓨터 네트워크 및 브랜드 보호: 랜섬웨어 공격에 대한 예방 및 대응책

By 로버트 P. 실버스 (Robert P. Silvers)[1], 베남 다이야님 (Behnam Dayanim)[2], 아담 M. 라이크 (Adam M. Reich)[3]

전세계적으로 기업 및 개인용 컴퓨터들이 '워너크라이 (WannaCry)'라 명명된 랜섬웨어에 의해 처음으로 공격당한 지 며칠이 경과하였을 뿐이나, 머지 않아 2 차 공격이 발생할 가능성 역시 높은 상황입니다.

랜섬웨어는 위협적입니다 - 하지만 이는 예방 가능하다는 점을 유념하시기 바랍니다. 저희 폴 헤이스팅스는 귀사를 이러한 위험으로부터 어떻게 보호할 수 있고, 만약 귀사가 공격을 받을 경우 어떻게 대처해야 할 지에 대해 아래에 간략히 정리해 두었습니다.

랜섬웨어란?

랜섬웨어는 컴퓨터를 잠궈 버리는 디지털 악성코드 (malware)로, 사용자가 비트코인 (bitcoin)과 같은 암호화폐 (cryptocurrency) 등으로 컴퓨터 데이터의 몸값을 지불하기 전까지는 컴퓨터에 담겨 있는 데이터에 접근하지 못 하도록 합니다. 랜섬웨어 공격은 데스크톱, 노트북, 서버, 휴대폰 등에 영향을 미치고 있으며, 미래에는 사물인터넷 (IoT)으로 연결된 여러 장치들도 공격할 것으로 예상됩니다. 워너크라이는 가장 최근에 등장한 랜섬웨어 중 하나로서, 이번 사건은 유례없는 규모로 수십만 대의 컴퓨터들을 동시다발적으로 공격했다는 점에서 많은 충격을 주었습니다.

랜섬웨어 방어

워너크라이 등 랜섬웨어의 공격으로부터 기업을 방어하기 위해서 고려해야 할 다섯 가지 일반적인 전략이 있습니다.

1. **신속한 패치 (patch) 설치.** 소프트웨어 개발자들은 새로 발견되는 취약점들을 보완하는 패치들을 주기적으로 개발/제공하지만, 이는 설치되기 전에는 효과를 발휘하지 못합니다. 기업들은 출시되자마자 가능한 한 빨리 패치를 설치해야 하는 것을 표준 업무 절차로 삼아야 합니다. 패치를 설치하지 않는 기업들은 워너크라이와 같이 이미 알려져 있고 보완 가능한 취약점들을 노리는 공격에 노출되는 위험에 처하게 됩니다. 만약 기업들이 패치를 설치하지 않아 고객 또는 파트너사에 부정적인 영향을 끼치는 결과를 초래할 경우, 과실로 인한 손해 배상 문제에 직면할 수 있습니다. 마이크로소프트 (Microsoft)는 지난 3 월 워너크라이가 공략하는 취약점에 대한 최신 버전 운영체제 (OS)용 패치를 출시하였고, 지난 주말에는 마이크로소프트가 원칙적으로는 더 이상 지원하지 않는

[1] 로버트 P. 실버스 (Robert P. Silvers)는 미국 국토안보부 (DHS)의 사이버 정책 담당 차관보 (Assistant Secretary)를 역임하였는데, 이는 국토안보부 내 사이버 보안 정책 담당 분야의 최고위직입니다.

[2] 베남 다이야님 (Behnam Dayanim)은 폴 헤이스팅스 워싱턴 D.C. 사무소의 파트너 변호사로, 개인정보 보호 및 사이버 보안 분야 공동 대표를 맡고 있습니다.

[3] 아담 M. 라이크 (Adam M. Reich)는 폴 헤이스팅스 LA 사무소 소속의 소송 담당 변호사 (associate)입니다.

구 버전 운영체제인 윈도우 XP 를 위한 패치도 출시했습니다. 만일 아직 이와 같은 패치를 설치하지 않은 기업이 있다면, 즉시 설치해야 할 것입니다.

2. **데이터 백업.** 기업의 IT 팀은 랜섬웨어가 데이터를 잠궈 버리더라도 회사가 다른 곳에 보관된 사본에 접근할 수 있도록 중요한 데이터들을 정기적이고 빈번한 주기로 백업해야 합니다.

3. **위협을 알리는 표식 (signatures) 배포.** 워너크라이 위협과 관련된 바이러스 백신 프로그램 및 악성코드의 표식을 배포해야 합니다. 미국 국토안보부의 사이버 운영 센터는 이러한 표식들을 홈페이지에 공개하였습니다.[4]

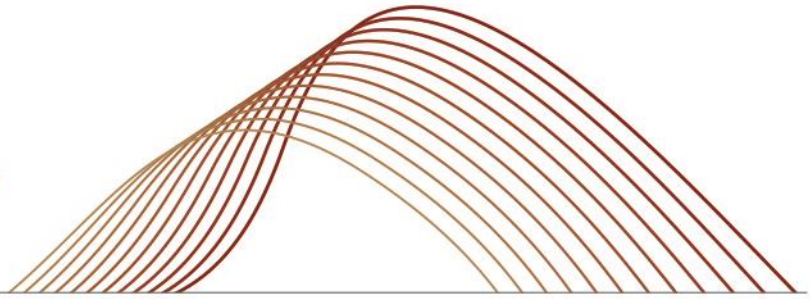
4. **랜섬웨어 대응 방안 고안.** 이 분야 전문가와 상의하여 랜섬웨어 대응 방안을 마련하여 기업이 어떠한 침투에도 신속하고 효과적으로 대처할 수 있도록 해야 합니다. 이러한 대응 방안에는 다음과 같은 요소들이 포함되어야 합니다: 데이터의 몸값을 지불할 것인지 여부 검토; 사법 기타 유관 기관들에 연락할 것인지 여부 및 접촉 방식 검토; 신속한 업무 운영 복구를 위한 절차; 홍보 및 고객 관계 관리 실무 지침 계발; 랜섬웨어 공격으로 촉발될 수 있는 계약상의 의무, 고지 의무, 소송 위험 등에 대한 법무팀과의 협의를 통한 이해 등.

5. **임직원 훈련 강화.** 랜섬웨어는 임직원들이 피싱 (phishing) 이메일을 엶으로써 (click) 광범위한 사내 네트워크로 침투 및 확산되는 경우가 많습니다. 사내 이메일 접근이 가능한 전 임직원들에 대해 피싱 예방 교육 참가 및 주기적인 업데이트를 의무화하는 정책을 검토해 보시기 바랍니다.

결론

폴 헤이스팅스(Paul Hastings)는 랜섬웨어를 예방하기 위한 최선의 절차에 대해 자문을 제공할 수 있고, 랜섬웨어 공격이 실제로 발생할 경우 이에 대한 대응 방안, 소송, 상사 분쟁, 당국 조사 등에 대해 안내해 드릴 준비가 되어 있습니다.

[4] 미국 국토안보부, 미국 컴퓨터 비상 대응팀, *공지(TA17-132A), 워너크라이 랜섬웨어에 관한 징후* (2017 년 5 월 17 일 수정), <https://www.us-cert.gov/ncas/alerts/TA17-132A>



Protecting Your Networks, and Your Brand: How to Avoid and Respond to Ransomware Attacks

By Robert P. Silvers, Behnam Dayanim, and Adam M. Reich

Days have passed since enterprise and personal computing devices were first held hostage around the world by the aptly-named "WannaCry" ransomware, and a "second wave" attack may not be far off.

Ransomware is daunting, but make no mistake: it is preventable. Below we outline how to protect your company, and how to respond if attacked.

What is Ransomware?

Ransomware is digital malware that locks a computing device, preventing the user from accessing data contained on the device until a ransom is paid, usually in a cryptocurrency like bitcoin. Ransomware attacks have impacted desktops, laptops, servers, and cellular phones, and in the future we expect it to hit the many connected devices comprising the Internet of Things. WannaCry was just the latest form of ransomware to hit in recent years, but the episode was unsettling because of its unprecedented scale, with hundreds of thousands of computers being targeted simultaneously.

Defending Against Ransomware

There are five general strategies that companies should consider for defending against Wannacry and other prospective ransomware attacks.

1. **Install patches quickly.** Software developers regularly make patches available to close newly-discovered vulnerabilities, but they only work if companies install them. Companies, as a standard operating procedure, should install patches as soon as possible after they are released. Companies that do not risk exposing themselves to attacks, like WannaCry, that prey on already-known and fixable vulnerabilities. If companies fail to patch and suffer consequences that adversely impact customers or commercial partners, they may face liability for negligence. Microsoft released in March a patch for the vulnerability exploited by WannaCry for its recent operating systems, and last weekend released a patch for Windows XP, an older operating system that Microsoft generally no longer supports. Companies should install these patches immediately if they haven't already done so.

2. **Back up data.** Corporate IT teams should back up critical data at regular and frequent intervals, so that even if data is locked up by ransomware, the company will be able to access copies elsewhere.

3. **Deploy known threat signatures.** Deploy antivirus and malware signatures associated with the WannaCry threat. The United States Department of Homeland Security's cyber operations center has posted these signatures.[1]

4. **Develop a ransomware incident response plan.** Consult with knowledgeable professionals to formulate a ransomware incident response plan so that the company can quickly and effectively respond to any infiltration. Plans should include consideration of whether to pay ransom; whether and how to interact with law enforcement and regulators; ensuring processes to restore operations quickly; development of public relations and customer relations action plans; and coordination by the legal team to understand any contractual obligations or notification requirements that may be triggered, as well as the risk of litigation resulting from the attack.

5. **Double-down on employee training.** Many ransomware attacks spread through phishing emails, which unsuspecting employees click through and allow the adversaries into the broader corporate network. Consider a policy that requires all employees with corporate email access to engage in and routinely update on counter-phishing training.

Conclusion

Paul Hastings is available to counsel clients through these best steps to prevent ransomware, and to guide them through the incident response, litigation, commercial disputes, and regulatory investigations that can arise when attacks do occur.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Washington, D.C.

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Robert P. Silvers
1.202.551.1216
robertsilvers@paulhastings.com

Los Angeles

Adam M. Reich
1.213.683.6190
AdamReich@paulhastings.com

Seoul

Jong Han Kim
82.2.6321.3801
jonghankim@paulhastings.com

[1] United States Department of Homeland Security, United States Computer Emergency Readiness Team, *Alert (TA17-132A), Indicators Associated With WannaCry Ransomware* (rev. May 17, 2017), *available at* https://www.us-cert.gov/ncas/alerts/TA17-132A.