봇넷 활동 분석

# 정보 및 수치

FORCEPOINT™ SECURITY LABS™

# JAKU

## JAKU 피해 상위 5개국

대한민국 · 일본 · 중국 · 대만 · 미국

평균 체류 시간:
93 일

최대 체류 시간:
348 일

**피해자 위치:**

**전 세계**
(일본, 대한민국과 중국에서 눈에 띄는 클러스터링)

**페이로드 전달 경로:**

감염된 BITTORRENT 사이트에 노출, 라이센스가 없는 소프트웨어의 사용과 와레즈(WAREZ) 소프트웨어 다운로드

멀웨어 유형:
**다단계 추적과 데이터 탈취 멀웨어**

명령 및 제어 서버 위치:
**말레이시아, 태국과 싱가포르**

JAKU 피해자가 위치한 국가 수
**134**

고유의 피해자 수
**19k**

**사용된 회피 기법:**

암호화, 스테가노그래피, 허위 파일 형식, 스텔스 삽입, 백신 엔진 탐지 (및 기타)

현재까지의 조사 기간:
**6 개월**

FORCEPOINT
POWERED BY Raytheon

FORWARD WITHOUT FEAR

©2016 Forcepoint LLC. All rights reserved.
Forcepoint™는 Forcepoint LLC의 상표입니다.

# 특정 피해자를 노리는 JAKU

JAKU는 Forcepoint 보안 연구소 특수 조사 팀(Special Investigations Team)이 발견한 봇넷 활동의 이름입니다. 수많은 봇넷 피해자들의 소리 중에서 JAKU를 고유하게 만드는 것은 JAKU가 소수의 특정 대상을 노려서 삼아 추적한다는 것입니다. 이 대상에는 NGO(국제 비정부기구) 구성원, 엔지니어링 회사, 교육 기관, 과학자와 공무원 등이 포함됩니다. 북한(DPRK)과 평양은 이 대상들이 공유하는 공통 주제입니다.

JAKU는 주로 '감염된(poisoned)' BitTorrent 파일 공유를 통하여 피해자(19,000명은 특정 시간에 발생한 보수적으로 잡은 피해자의 추정치)를 겨냥하고 있습니다. 피해자는 전 세계에 분포해 있지만, 피해자의 상당수는 대한민국과 일본에 있습니다. Forcepoint 보안 연구소는 확인된 봇넷 명령 및 제어(Command and Control :C2) 서버도 싱가포르, 말레이시아, 태국을 포함한 아시아 태평양 지역에 있는 것을 확인했습니다.

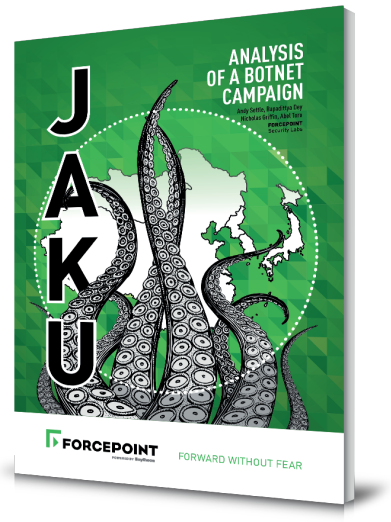
# 지능적인 봇넷 활동

JAKU는 세 가지 다른 C2 메커니즘을 사용하여 매우 강력합니다. 봇넷 컨트롤러가 난독화 SQLite 데이터베이스를 통해 봇넷 구성원을 감시하면서 이미지 파일 내의 압축과 암호화된 코드를 사용하여 두 번째 단계의 멀웨어를 전달하는 데 사용됩니다. 컨트롤러는 또한 영리하게 오픈 소스 소프트웨어(UDT 네트워크 전송 프로토콜, 한국 블로거 사이트에서 복사한 소프트웨어와 이전에 출시된 코드의 다시 쓰기)를 재사용합니다.

# 누가 JAKU 봇넷 활동의 배후인가?

Forcepoint 보안 연구소는 동기에 대한 인식과 이해에 초점을 맞추었습니다. 이 가능성이 미래의 행위를 파악하는 데 유용합니다. 우리는 특정 속성에 초점을 두지는 않지만, 확인된 멀웨어의 저자(들)는 한국인이란 지표가 있습니다.

JAKU 봇넷 활동에 대한 상세 정보는 **www.forcepoint.com/jaku** 에서 보고서를 다운로드하십시오.




FORCEPOINT
POWERED BY Raytheon

FORWARD WITHOUT FEAR

©2016 Forcepoint LLC. All rights reserved.
Forcepoint™는 Forcepoint LLC의 상표입니다.