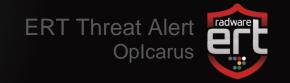# ERT RESEARCH ALERT

#OpIcarus

Taking down world banks

February 2016

Abstract

Anonymous announced its plan to attack leading financial banks & institutes on Monday, February 8th 2016, at 6AM UTC, and take down their services. As part of that, they will equip participants with dedicated VPN and LOIC tools to launch multiple and simultaneous Denial of Service attacks, and encourage protesters to accompany the operation by protesting in front of the Bank of England and New York Stock Exchange.
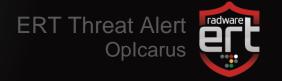
Table of Contents

Background:

In the Greek mythology Icarus tried to escape the labyrinth in Crete using a pair of wings made of wax and feathers. He was too proud to listen to his father's advice not to fly too close to the sun. Eventually, the sun melted Icarus's wings and he has fallen into the sea & drowned.

Members of the collective Anonymous have recently announced operation OpIcarus. This operation is scheduled for 6am on February 8th , targeting both The Bank of England and The New York Stock Exchange. The campaign will include both offline protests and denial of service (DoS) attacks. This event is intended to bring public attention to what Anonymous calls 'corruption' inside of the financial industry. Anonymous argues that leading banks are supporting and funding global terrorism:

> *"Like Icarus, the powers that be have flown too close to the sun and the time has come to set the wings of their empire ablaze and watch the system their power relies on come to a grinding halt and come crashing down around them. We must strike at the heart of their empire by once again throw a wrench into the machine, but this time we face a much bigger target; the global financial system. This time our target is the New York Stock Exchange and Bank of England."i -OpIcarus*

Those behind Operation Icarus are planning to launch a simultaneous DoS attacks with the tool, **Low Orbit Ion Cannon**, also known as LOIC. LOIC allows laying heavy network traffic loads on servers, and has been widely used by Anonymous as a DDoS tool. Anonymous has made available a VPN and LOIC tool free to whoever wants to take part in the attack.
With thousands of protesters using LOIC to attack a single target, the effects on the network performance can be much more significant than that of a "normal" coordinated LOIC attack. When targeting the financial industry, the loss of network performance could lead to people being unable to access their money.

OpIcarus' Facebook event page lists sixty central banks and monetary authorities (all members of the BIS) that could also expect DDoS attacks during the February 8th protests.
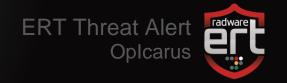
Known Targets

- Bank of England – Threadneedle st, London EC2R 8AH– 6am UK
- New York Stock Exchange – 11 Wall St, New York NY 10005 – 1am NYC

Potential targets also include BIS member banks[ii]

- Bank of Algeria
- Central Bank of Argentina
- Reserve Bank of Australia
- Central Bank of the Republic of Austria
- National Bank of Belgium
- Central Bank of Bosnia and Herzegovina
- Central Bank of Brazil
- Bulgarian National Bank
- Bank of Canada
- Central Bank of Chile
- People's Bank of China
- Bank of the Republic (Colombia)
- Croatian National Bank
- Czech National Bank
- Danmarks Nationalbank (Denmark)
- Bank of Estonia
- European Central Bank
- Bank of Finland
- Bank of France
- Deutsche Bundesbank (Germany)
- Bank of Greece
- Hong Kong Monetary Authority
- Magyar Nemzeti Bank (Hungary)
- Reserve Bank of India
- Bank Indonesia
- Bank of Israel
- Bank of Italy
- Bank of Japan
- Bank of Korea
- Bank of Latvia
- Bank of Lithuania
- Central Bank of Luxembourg
- National Bank of the Republic of Macedonia
- Central Bank of Malaysia
- Bank of Mexico
- Netherlands Bank
- Reserve Bank of New Zealand
- Central Bank of Norway
- Central Reserve Bank of Peru
- Bangko Sentral ng Pilipinas (Philippines)
- National Bank of Poland
- Bank of Portugal
- National Bank of Romania
- Central Bank of the Russian Federation
- Saudi Arabian Monetary Agency
- National Bank of Serbia
- Monetary Authority of Singapore
- National Bank of Slovakia
- Bank of Slovenia
- South African Reserve Bank
- Bank of Spain
- Sveriges Riksbank (Sweden)
- Swiss National Bank
- Bank of Thailand
- Central Bank of the Republic of Turkey
- Central Bank of the United Arab Emirates
- Bank of England

- Board of Governors of the Federal Reserve System (United States)
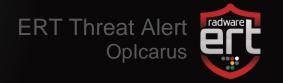
How to Prepare

Radware advises that both The Bank of England and The New York Stock Exchange, along with BIS member banks, put in place security protections for DDoS attacks prevention and mitigation. **Radware** calls parties under attack to contact Radware's **ERT** directly for immediate, real time mitigation and protection from downtime.

Radware's hybrid attack mitigation solution provides a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced threats. With dedicated hardware and cloud solutions that protect against attacks in real-time, **Radware** can help ensure service availability.

With **Radware**, companies can protect their infrastructure from multi-vector attacks network and application based DDoS attacks as well as volumetric attacks that may saturate the Internet pipe, defacement, information-loss, and other reputation loss impacts of Denial of Service. **Radware** solutions include proven LOIC protection mechanisms.
To understand how Radware's 24x7 attack mitigation solutions can better protect your network contact us.

Sources:

Event Information
- https://opicarus.wordpress.com/
- https://occupylondonoccupywallstreetblog.wordpress.com/2016/01/25/occupy-londonoccupy-wall-street/

Event Video
- http://www.dailymotion.com/video/x2vopsf

Facebook Page
- https://www.facebook.com/events/964150270338381

Promoter
- https://www.facebook.com/HarveyHarris6

Hashtags in use
- #OpIcarus
- #OccupyLondon
- #OccupyWallStreet
- #DDOS
- #Anonymous
- #Anarchists

Tools
- CyberGhostVPN.com
- LOIC

---

[i] https://www.facebook.com/events/964150270338381
[ii] http://hejevent.se/event/jezgutaf5cxxua/shut-down-the-banks-opicarus