ERT Threat Alert
OpIcarus Re-Engaged
May 6, 2016

Abstract
The Hacktivist Group Anonymous announced its plans to relaunch its cyber assaults on leading financial services companies worldwide. Named Operation Icarus, this event is intended to bring public attention to what Anonymous calls 'corruption' inside of the financial services industry. Anonymous contends that leading banks are supporting and funding global terrorism. Several groups, including DragonSec, DeamonSec, Ghost Squad Hackers, and those behind OpIcarus have joined forces to launch a 30-day DDoS campaign.

Background
Radware issued an ERT Alert in February when OpIrcarus was created. At that time, the attackers didn't possess the ability or the organizational skills needed to execute a largescale operation, resulting in a low success rate. The attackers were able to build a large target list but suggested the use of tools (such as LOIC) that can be blocked by a protected site.

This time, attackers appear to have learned from their mistakes and are now suggesting more advanced tools in comparison to LOIC. They are now suggesting hackers to use tools such as TorHammer, SlowLoris, Xerxes and other scripted attacks. In addition, they are claiming this second round of attacks will last for 30 days and target hundreds of sites.

Targets
Target list: http://pastebin.com/raw/dVyqyJi5

Down Sites
- www.dnb.nl
- www.banxico.org.mx
- www.bancentral.gov.do
- www.bankofgreece.gr
- www.centralbank.gov.cy

Attack Vectors
- TorsHammer
- SlowLoris
- PyLoris
- TorStress
- Slowhttptest
- Xerxes

- Ufonet

Anonymization

- VPNbook
- Tor

Sources

Event Pages

- https://www.facebook.com/groups/1114271735258436/
- https://www.facebook.com/events/964150270338381

Twitter

- https://twitter.com/Op_Icarus

YouTube

- https://youtu.be/mf6JGltELzQ
- https://youtu.be/GpGWaa3uCNo

Updated target list

- https://nopaste.me/view/61113fc5

Opertionl information

- http://pastebin.com/sudrRrB3

DangonSec Operation Infomation and Tools

- http://pastebin.com/cYPD0AJy

DeamonSec Anon Guide v3

- http://pastebin.com/6CtvsXUB

Reasons for Concern

Financial organizations should proactively prepare their networks with an attack mitigation solution designed to detect, mitigate and report today's most advance threats. This operation has more supporters and is well organized. Attackers have transitioned from suggesting LOIC to a series of scripted tools as well as using VPN's and Tor to mask their identity.

With more attackers and more tools, it is expected that targeted victims will see multiple vectors of attacks at a persistent rate. This operation is set to last for 30 days and it's expected that these attacks will continue to grow in size as a greater audience becomes more aware of the operation.

How to Prepare

Political and ideological-driven attacks such as these can be difficult to avoid. Radware's hybrid attack mitigation solution provides a set of patented and integrated technologies designed to detect, mitigate and report today's most advanced threats. Dedicated hardware and cloud solutions protect against attacks in real time and 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 protection mechanisms from the vectors listed above. To understand how Radware's 24x7 attack mitigation solutions can better protect your network contact us.

Organizations Under Attack Should Consider

- A security solution that can protect its infrastructure from multi-vector attacks including protection from network and application-based DDoS attacks as well as volumetric attacks that can saturate the Internet pipe
- A hybrid solution that includes on-premise detection and mitigation with cloud-based protection for volumetric attacks. This provides quick detection, immediate mitigation and protects networks from volumetric attacks that aim to saturate the Internet pipe.
- A solution that provides protection against sophisticated web-based attacks and website intrusions to prevent defacement and information theft.
- A cyber-security emergency response plan that includes an emergency response team and process in place. Identify areas where help is needed from a third party.
- Monitor security alerts and examine triggers carefully. Tune existing policies and protections to prevent false positives and allow identification of real threats if and when they occur.

In addition to Radware products, we recommend that you review your network patch your system according. Maintaining and inspecting your network often is necessary in order to defend against these types of risks and threats.

Under Attack and in Need of Expert Emergency Assistance?

Radware offers a full range of solutions to help networks properly mitigate attacks similar to these. Our attack mitigation solutions provide a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced DDoS attacks and cyber threats. With dedicated hardware, fully managed services and cloud solutions that protect against attacks, Radware can help ensure service availability. To understand how Radware's attack mitigation solutions can better protect your network contact us today.

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

Target List

Federal Reserve of America
http://www.federalreserve.gov/
http://www.ny.frb.org/
http://www.federalreserveonline.org/
http://www.federalreserveeducation.org/
http://www.chicagofed.org/webpages/index.cfm
https://www.richmondfed.org/
http://www.frbservices.org/
http://www.stlouisfed.org/
https://www.minneapolisfed.org/index.cfm
http://www.dallasfed.org/
http://www.bostonfed.org/
http://www.newyorkfed.org/
http://www.frbsf.org/
http://www.philadelphiafed.org/

http://www.federalreservehistory.org/
http://www.ffiec.gov/
http://www.federalreserveconsumerhelp.gov/
http://www.frbatlanta.org/

IMF
https://www.imf.org/external/index.htm
https://imf.taleo.net/
http://imfsite.org/

World Bank
http://www.worldbank.org/
http://www.centralbanking.com/
www.centralbanksguide.com
http://www.doingbusiness.org/
http://ieg.worldbankgroup.org/
http://info.worldbank.org
http://www.globalexchange.org/
http://data.worldbank.org/
http://www.worldbankpresident.org/
http://www.ifc.org

Central Banks around the globe
http://www.centralbank.ae/index.php
http://www.bankofengland.co.uk/Pages/home.aspx
https://www.bankofengland-ar.com/
http://www.centralbank.gov.af/
http://www.bankofalbania.org/
http://www.meduniwien.ac.at/hp/0/gerichtsmedizin/
http://oenb.at/en/
http://www.rba.gov.au/
http://www.cbaruba.org/cba/home.do
https://www.cba.am/am/SitePages/Default.aspx
http://www.bcra.gov.ar/index_i.htm
http://www.bank-of-algeria.dz/
http://en.cbar.az/
http://www.cbar.az/
http://www.nbb.be/pub/home.htm?l=en
http://www.nbrb.by/
http://www.centralbank.org.bb/
http://www.bangladesh-bank.org/
http://www.cbb.gov.bh/
http://www.centralbankbahamas.com/
http://www.bnb.bg/
http://www.bcb.gov.br/pt-br/paginas/default.aspx
https://www.centralbank.org.bz/
http://www.bceao.int/
http://www.bma.bm/SitePages/Home.aspx
http://www.rma.org.bt/
http://www.bcb.gob.bo/

http://www.cbbh.ba
http://www.bankofbotswana.bw/
http://www.brb.bi/
http://www.cnb.cz/cs/index.html
http://www.centralbank.gov.cy/nqcontent.cfm?a_id=1
http://www.hnb.hr/
http://www.bccr.fi.cr/
http://www.banque-comores.km/
http://www.banrep.gov.co/
http://www.pbc.gov.cn/
http://www.bc.gob.cu/Espanol/default.asp
http://www.bcentral.cl/index.asp
http://www.cimoney.com.ky/
http://www.bank-banque-canada.ca/
http://www.banqueducanada.ca/
http://www.bankofcanada.ca/
https://www.beac.int/
http://www.nbc.org.kh/
http://www.nationalbanken.dk/en/Pages/default.aspx
www.nationalbank.dk/
http://www.bancentral.gov.do/
http://www.eccb-centralbank.org/
http://www.cbe.org.eg/English/
http://www.eestipank.ee/
http://www.nbe.gov.et/
http://www.bcr.gob.sv/esp/
https://www.ecb.europa.eu/home/html/index.en.html
http://www.rbf.gov.fj/
http://www.suomenpankki.fi/fi/Pages/default.aspx
http://www.cbg.gm/
https://www.tnbg.net/
https://www.nbg.gov.ge/index.php?m=2
https://www.banque-france.fr/accueil.html
http://www.bundesbank.de/Navigation/DE/Home/home_node.html
http://www.bog.gov.gh/
http://www.bankofgreece.gr/Pages/default.aspx
http://www.banguat.gob.gt/
http://www.bankofguyana.org.gy/bog/
http://www.brh.net/
http://www.bch.hn/
http://www.hkma.gov.hk/eng/index.shtml
http://www.mnb.hu/
http://www.sedlabanki.is/
http://www.rbi.org.in/home.aspx
http://www.bi.go.id/id/Default.aspx
http://www.centralbank.ie/Pages/home.aspx
http://www.cbi.ir/
http://www.cbi.iq/
https://www.bancaditalia.it/
http://www.boi.org.il/he/Pages/Default.aspx
http://www.boj.org.jm/

https://www.boj.or.jp/
www.cbj.gov.jo/
www.nationalbank.kz/
https://www.centralbank.go.ke/
www.bok.or.kr/
www.cbk.gov.kw/
www.nbkr.kg/
www.bank.lv/
www.bdl.gov.lb/
www.centralbank.org.ls/
www.cbl.gov.ly/
www.bcu.gub.uy/
https://www.lb.lt/
www.bcl.lu/
www.amcm.gov.mo/
www.nbrm.mk/
www.banque-centrale.mg/
https://www.rbm.mw/
www.bnm.gov.my/
www.centralbankmalta.org/
https://www.bom.mu/
www.banxico.org.mx/
www.bnm.org/
www.mongolbank.mn/
www.cb-mn.org/
www.bkam.ma/
www.bancomoc.mz/
bank.gov.ua/
www.rbv.gov.vu/
www.bcv.org.ve/
www.sbv.gov.vn/
www.centralbank.gov.ye/
www.boz.zm/
www.rbz.co.zw/
https://www.bon.com.na/
www.nrb.org.np/
www.dnb.nl/
www.centralbank.an/
www.rbnz.govt.nz/
www.bcn.gob.ni/
www.cenbank.org/
www.norges-bank.no/
www.cbo-oman.org/
www.sbp.org.pk/
www.bankpng.gov.pg/
www.bcp.gov.py/
www.bcrp.gob.pe/
www.bsp.gov.ph/
www.nbp.pl/
www.bportugal.pt/
www.qcb.gov.qa/

www.bnro.ro/
www.cbr.ru/
www.bnr.rw/
www.bcsm.sm/
www.cbs.gov.ws/
www.sama.gov.sa/
www.nbs.rs/
www.cbs.sc/
www.bsl.gov.sl/
www.mas.gov.sg/
www.nbs.sk/
https://www.bsi.si/
www.cbsi.com.sb/
https://www.resbank.co.za/
www.bde.es/
www.cbsl.gov.lk/
www.cbos.gov.sd/
www.cbvs.sr/
www.centralbank.org.sz/
www.riksbank.se/
www.snb.ch/
http://www.nbt.tj/
https://www.bot-tz.org/
www.bot.or.th/
www.reservebank.to/
www.central-bank.org.tt/
www.bct.gov.tn/
www.tcmb.gov.tr/
https://www.bou.or.ug/