Abstract

OpIcarus is a multiphase operation originally launched by Anonymous on February 8, 2016 and is now entering its fifth phase on June 11, 2017. Its goal is to take down the websites and services associated with the global financial system. These attackers accuse the system with 'corruption' and want to raise public awareness; not financially motivated like cyber-criminals are. Their objective is to target these financial institutions with persistent denial-of-service (DoS) attacks and data dumps. Among the targets of previous attacks are the New York Stock Exchange, Bank of England, Bank of France, Bank of Greece, Bank of Jordan and the Bank of South Korea, among others.

Figure 1: Operation image of OpSacred

OpSacred – OpIcarus Phase 5

OpIcarus has become highly organized since it first launched and has evolved into its 5th campaign, named OpSacred. Announced on Facebook[i] on May 12, 2017, hackers posted the documentation, tools and associated Facebook accounts. In the manifesto, OpIcarus makes ten statements:

- Governments need to cease and desist all wars
- Governments need to return governance of the masses to the masses.
- Debt wage slavery is evil.
- Greed and materialism is evil
- That when a government no longer serves the needs of it's people that it is the duty of its citizens to resist this tyranny.
- That pollution of our planet for the purposes of greed and resource extraction must stop. We only have one planet and it is sacred.
- That capitalist lobbying of government is corruption.
- That all humanity should enjoy equality.
- That borders and nations are a manmade construct and are disingenuous as we are one.
- That all decisions should be made based on an unconditional love for humanity.

According to a Facebook post[ii], OpIcarus2017 will start on June 11th and run till June 21st. The post included a target list for the operation that includes most of the organizations targeted during previous phases.

Figure 2: OpIcarus Facebook Event Page

Reasons for Concern

This operation has more supporters than previous phases and is very 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. They are consolidating this information in centralized location - GitHub page - to make it easier to participants to join the operation.

There are more advanced cyber-attack tools compared to previous campaigns available on the GitHub page. The Github documentation folder contains information about several large organizations. In phase 5, attackers use open source intelligent tools and scanners to visualize and analyze targeted networks. For example, Zed Attack Proxy, Z.A.P., a tool used to find security vulnerabilities in web applications.

Targets

Target list for OpIcarus2017 is featured on Pastebin. Targeted sites include the International Monetary Fund, the Federal Reserve of America, and central banks of various countries around the world. The full list is available at https://pastebin.com/CLeFfFRA.

OpIcarus DDoS Arsenal

The operation Github page features a set of denial of service tools ranging from basic GUI tools to scripts coded in Python, Perl and C. These tools were not created for OpIcarus but are rather a collection of tools used by other hacktivist and security professionals.

R U Dead Yet (RUDY) – a slow-rate HTTP POST (Layer 7) denial-of-service tool using long form field submissions. By injecting one byte of information into an application POST field at a time and then waiting, R.U.D.Y. causes application threads to await the end of never-ending posts in order to perform processing (this behavior is necessary in order to allow web servers to support users with slower connections). Since R.U.D.Y. causes the target webserver to hang while waiting for the rest of an HTTP POST request, by initiating simultaneous connections to the server the attacker is ultimately able to exhaust the server's connection table and create a denial-of-service condition.

Tor's Hammer- a Layer 7 DoS tool that executes a DoS attack by using a classic slow POST attack, where HTML POST fields are transmitted in slow rates under the same session (actual rates are randomly chosen within the limit of 0.5-3 seconds).

Similar to R.U.D.Y., the slow POST attack causes the web server application threads to await the end of boundless posts in order to process them. This causes the exhaustion of the web server resources and causes it to enter a denial-of-service state for any legitimate traffic.

A new functionality added to Tor's Hammer is a traffic anonym capability. DoS attacks can be carried out

through the Tor Network by using a native socks proxy integrated in Tor clients. This enables launching the attack from random source IP addresses, which makes tracking the attacker almost impossible.

XerXeS - an extremely efficient DoS tool providing the capacity to launch multiple automated independent attacks against several target sites without necessarily requiring a botnet.

KillApache – takes advantage of an old vulnerability allowing attackers to send requests to an Apache server to retrieve URL content in a large number of overlapping "byte ranges" or chunks, effectively causing the server to run out of useable memory - resulting in a denial-of-service condition.

Other DDoS attack tools include:

- BlackHorizon
- CescentMoon
- ChiHULK
- GoldenEye
- HellSec
- IrcAbuse
- MasterK3Y
- OpIcarusBot
- PentaDos
- Purple
- Saddam
- Saphyra
- Asundos
- Asundos2
- B0wS3rDdos
- Blacknurse
- Botnet
- Clover
- D4rk
- Finder
- Getrekt
- L7
- M60
- wso

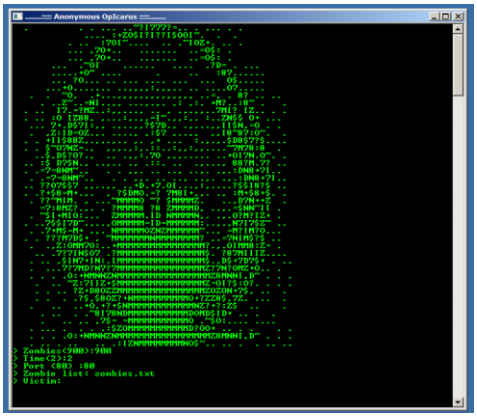


Figure 3: OpIcarusBot – A Layer 7 attack tool for OpIcarus

OpIcarus Github Pages

OpIcarus - https://github.com/opicaruscollective/OpIcarus/
Documentation - https://github.com/opicaruscollective/OpIcarus/tree/Documentation
Tools - https://github.com/opicaruscollective/OpIcarus/tree/Tools
YouTube channel - https://youtu.be/rkS2RfPkTkY

Attack Vectors

Nmap – a security scanner designed for network discovery and security auditing. It uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering. In addition, they identify what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

Zed Attack Proxy – The OWASP Zed Attack Proxy, ZAP, is a popular and open source security tool that helps users automatically scan and find security vulnerabilities in web applications.

Malrego – an open source intelligence and forensic tool allowing users to discover data from open sources and visualize the data in graphs and detailed reports for data mining and link analysis[iii]

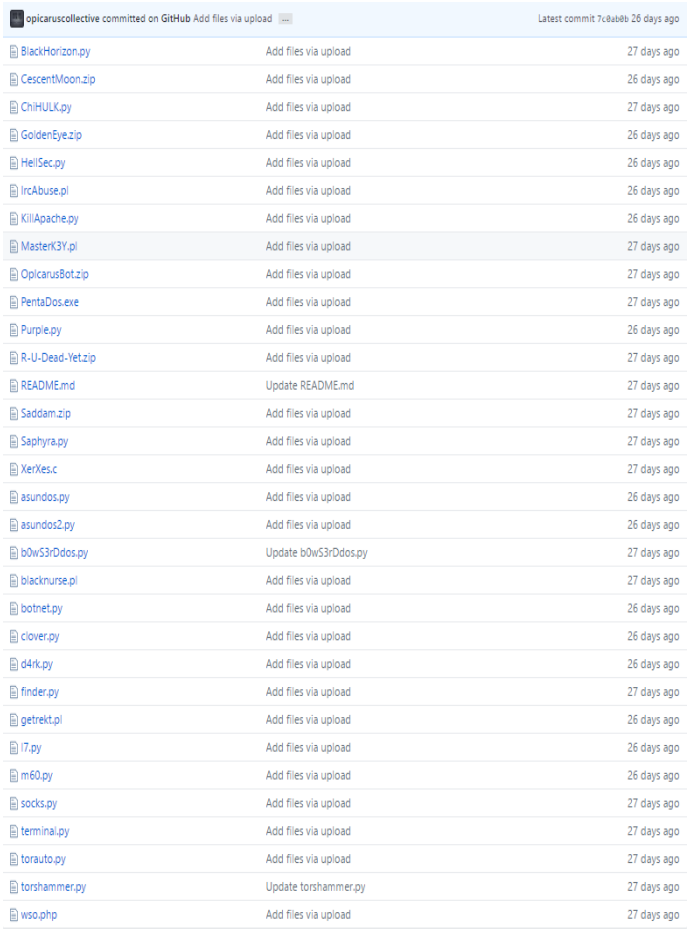
TCP flood - One of the oldest yet still very popular DoS attacks. It involves sending numerous SYN packets to the victim. In many cases, attackers will spoof the SRC IP so the reply (SYN+ACK packet) will not return, thus overwhelming the session/connection tables of the targeted server or one of the network entities on the way (typically the firewall). Servers need to open a state for each SYN packet that arrives and they store this state in tables that have limited size. As big as this table may be it is easy to send sufficient amount of SYN packets that will fill the table, and once this happens the server starts to drop a new request, including legitimate ones. Similar effects can happen on a firewall that also has to process

and invest in each SYN packet. Unlike other TCP or application level attacks the attacker does not have to use a real IP - this is perhaps the biggest strength of the attack.

UDP Flood –attacker sends large UDP packets to a single destination or to random ports. Since the UDP protocol is “connectionless” and does not have any type of handshake mechanism, the main intention of a UDP flood is to saturate the Internet pipe. In most cases the attackers spoof the SRC (source) IP

HTTP/S Flood - An attack method used by hackers to attack web servers and applications. These floods consist of seemingly legitimate session-based sets of HTTP GET or POST requests sent to a targeted web server. HTTP floods do not use spoofing, reflective techniques or malformed packets. These requests are specifically designed to consume a significant amount of the server’s resources, and therefore can result in a denial-of-service. Such requests are often sent en masse by means of a botnet, increasing the attack’s overall power. HTTP and HTTPS flood attacks are one of the most advanced threats facing web servers today since it is hard for network security devices to distinguish between legitimate and malicious HTTP traffic.

SQL Injection – This technique takes advantage of poor application coding. When the application inputs are not sanitized, it becomes vulnerable. Attackers can modify an application SQL query to gain access to unauthorized data with administrator access, run remote commands on the server, drop or create objects in the database, and more.



opicaruscollective committed on GitHub Add files via upload ... Latest commit 7c0ab0b 26 days ago

BlackHorizon.py	Add files via upload	27 days ago
CescentMoon.zip	Add files via upload	26 days ago
ChiHULK.py	Add files via upload	27 days ago
GoldenEye.zip	Add files via upload	26 days ago
HellSec.py	Add files via upload	26 days ago
IrcAbuse.pl	Add files via upload	26 days ago
KillApache.py	Add files via upload	26 days ago
MasterK3Y.pl	Add files via upload	27 days ago
OpIcarusBot.zip	Add files via upload	27 days ago
PentaDos.exe	Add files via upload	27 days ago
Purple.py	Add files via upload	26 days ago
R-U-Dead-Yet.zip	Add files via upload	27 days ago
README.md	Update README.md	27 days ago
Saddam.zip	Add files via upload	27 days ago
Saphyra.py	Add files via upload	27 days ago
XerXes.c	Add files via upload	27 days ago
asundos.py	Add files via upload	26 days ago
asundos2.py	Add files via upload	26 days ago
b0wS3rDdos.py	Update b0wS3rDdos.py	27 days ago
blacknurse.pl	Add files via upload	27 days ago
botnet.py	Add files via upload	26 days ago
clover.py	Add files via upload	26 days ago
d4rk.py	Add files via upload	26 days ago
finder.py	Add files via upload	27 days ago
getrekt.pl	Add files via upload	26 days ago
i7.py	Add files via upload	26 days ago
m60.py	Add files via upload	26 days ago
socks.py	Add files via upload	27 days ago
terminal.py	Add files via upload	27 days ago
torauto.py	Add files via upload	27 days ago
torshammer.py	Update torshammer.py	27 days ago
wso.php	Add files via upload	27 days ago

Figure 4: These tools can be found on GitHub at: https://github.com/opicaruscollective/OpIcarus/tree/Tools

Effective DDoS Protection Essentials:

- **Hybrid DDoS Protection** - (on-premise + cloud) – for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - to quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - to promptly protect from unknown threats and 0-day attacks
- **A cyber-security emergency response plan** - that includes a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Effective Web Application Security Essentials

- **Full OWASP Top-10 application vulnerabilities coverage**– against defacements, injections, etc.
- **Low false positive rate** – using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options** - on-premise, out-of-path, virtual or cloud-based

For further security measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button".

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.

---

[i] https://www.facebook.com/HarveyHarris6/posts/421743798183945
[ii] https://www.facebook.com/events/236685386815328/
[iii] https://en.wikipedia.org/wiki/Maltego