National Cyber Alert System

Technical Cyber Security Alert TA12-024A

Archive

"Anonymous" DDoS Activity

Original release date: January 24, 2012
Last revised: --
Source: US-CERT

Overview

US-CERT has received information from multiple sources about coordinated distributed denial-of-service (DDoS) attacks with targets that included U.S. government agency and entertainment industry websites. The loosely affiliated collective "Anonymous" allegedly promoted the attacks in response to the shutdown of the file hosting site MegaUpload and in protest of proposed U.S. legislation concerning online trafficking in copyrighted intellectual property and counterfeit goods (Stop Online Piracy Act, or SOPA, and Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act, or PIPA).

I. Description

US-CERT has evidence of two types of DDoS attacks: One using HTTP GET requests and another using a simple UDP flood.

The Low Orbit Ion Cannon (LOIC) is a denial-of-service attack tool associated with previous Anonymous activity. US-CERT has reviewed at least two implementations of LOIC. One variant is written in JavaScript and is designed to be used from a web browser. An attacker can access this variant of LOIC on a website and select targets, specify an optional message, throttle attack traffic, and monitor attack progress. A binary variant of LOIC includes the ability to join a botnet to allow nodes to be controlled via IRC or RSS command channels (the "HiveMind" feature).

The following is a sample of LOIC traffic recorded in a web server log:

```
"GET /?id=1327014400570&msg=We%20Are%20Legion! HTTP/1.1" 200 99406 "hxxp://pastehtml.com
/view/blafp1ly1.html" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:9.0.1) Gecko/20100101
Firefox/9.0.1"
```

The following sites have been identified in HTTP referrer headers of suspected LOIC traffic. This list may not be complete. Please do not visit any of the links as they may still host functioning LOIC or other malicious code.

```
"hxxp://3g.bamatea.com/loic.html"
"hxxp://anonymouse.org/cgi-bin/anon-www.cgi/"
"hxxp://chatimpacto.org/Loic/"
"hxxp://cybercrime.hostzi.com/Ym90bmV0/loic/"
"hxxp://event.seeho.co.kr/loic.html"
"hxxp://pastehtml.com/view/bl3weewxq.html"
"hxxp://pastehtml.com/view/bl7qhhp5c.html"
"hxxp://pastehtml.com/view/blafp1ly1.html"
"hxxp://pastehtml.com/view/blakyjwbi.html"
"hxxp://pastehtml.com/view/blal5t64j.html"
"hxxp://pastehtml.com/view/blaoyp0qs.html"
"hxxp://www.lcnongjipeijian.com/loic.html"
"hxxp://www.rotterproxy.info/browse.php/704521df/ccc21Oi8/vY3liZXJ/jcmltZS5/ob3N0emk
/uY29tL1l/tOTBibVY/wL2xvaWM/v/b5/fnorefer"
"hxxp://www.tandycollection.co.kr/loic.html"
"hxxp://www.zgon.cn/loic.html"
"hxxp://zgon.cn/loic.html"
"hxxp://www.turbytoy.com.ar/admin/archivos/hive.html"
```

The following are the A records for the referrer sites as of January, 20, 2012:

```
3g[.]bamatea[.]com              A    218[.]5[.]113[.]218
cybercrime[.]hostzi[.]com       A    31[.]170[.]161[.]36
```

```
event[.]seeho[.]co[.]kr          A    210[.]207[.]87[.]195
chatimpacto[.]org                A    66[.]96[.]160[.]151
anonymouse[.]org                 A    193[.]200[.]150[.]125
pastehtml[.]com                  A    88[.]90[.]29[.]58
lcnongjipeijian[.]com            A    49[.]247[.]252[.]105
www[.]rotterproxy[.]info         A    208[.]94[.]245[.]131
www[.]tandycollection[.]co[.]kr  A    121[.]254[.]168[.]87
www[.]zgon[.]cn                  A    59[.]54[.]54[.]204
www[.]turbytoy[.]com[.]ar        A    190[.]228[.]29[.]84
```

The HTTP requests contained an "id" value based on UNIX time and user-defined "msg" value, for example:

```
GET /?id=1327014189930&msg=%C2%A1%C2%A1NO%20NOS%20GUSTA%20LA%20
```

Other "msg" examples:

```
msg=%C2%A1%C2%A1NO%20NOS%20GUSTA%20LA%20
msg=:)
msg=:D
msg=Somos%20Legion!!!
msg=Somos%20legi%C3%B3n!
msg=Stop%20S.O.P.A%20:)%20%E2%99%AB%E2%99%AB HTTP/1.1" 200 99406 "http://pastehtml.com
/view/bl7qhhp5c.html"
msg=We%20Are%20Legion!
msg=gh
msg=open%20megaupload
msg=que%20sepan%20los%20nacidos%20y%20los%20que%20van%20a%20nacer%20que%20nacimos%20para%2(
msg=stop%20SOPA!!
msg=We%20are%20Anonymous.%20We%20are%20Legion.%20We%20do%20not%20forgive.%20We%20do%20not%2
```

The "msg" field can be arbitrarily set by the attacker.

As of January 20, 20012, US-CERT has observed another attack that consists of UDP packets on ports 25 and 80. The packets contained a message followed by variable amounts of padding, for example:

```
66:6c:6f:6f:64:00:00:00:00:00:00:00:00 | flood.........
```

Target selection, timing, and other attack activity is often coordinated through social media sites or online forums.

US-CERT is continuing research efforts and will provide additional data as it becomes available.

III. Solution

There are a number of mitigation strategies available for dealing with DDoS attacks, depending on the type of attack as well as the target network infrastructure. In general, the best practice defense for mitigating DDoS attacks involves advanced preparation.

- Develop a checklist or Standard Operating Procedure (SOP) to follow in the event of a DDoS attack. One critical point in a checklist or SOP is to have contact information for your ISP and hosting providers. Identify who should be contacted during a DDoS, what processes should be followed, what information is needed, and what actions will be taken during the attack with each entity.
- The ISP or hosting provider may provide DDoS mitigation services. Ensure your staff is aware of the provisions of your service level agreement (SLA).
- Maintain contact information for firewall teams, IDS teams, network teams and ensure that it is current and readily available.
- Identify critical services that must be maintained during an attack as well as their priority. Services should be prioritized beforehand to identify what resources can be turned off or blocked as needed to limit the effects of the attack. Also, ensure that critical systems have sufficient capacity to withstand a DDoS attack.
- Have current network diagrams, IT infrastructure details, and asset inventories. This will assist in determining actions and priorities as the attack progresses.
- Understand your current environment and have a baseline of daily network traffic volume, type, and performance. This will allow staff to better identify the type of attack, the point of attack, and the attack vector used. Also, identify any existing bottlenecks and remediation actions if required.
- Harden the configuration settings of your network, operating systems, and applications by disabling services and applications not required for a system to perform its intended function.
- Implement a bogon block list at the network boundary.
- Employ service screening on edge routers wherever possible in order to decrease the load on stateful security devices

such as firewalls.
- Separate or compartmentalize critical services:
  - Separate public and private services
  - Separate intranet, extranet, and internet services
  - Create single purpose servers for each service such as HTTP, FTP, and DNS
- Review the US-CERT Cyber Security Tip Understanding Denial-of-Service Attacks.

IV. References

- Cyber Security Tip ST04-015 - <http://www.us-cert.gov/cas/tips/ST04-015.html>
- Anonymous's response to the seizure of MegaUpload according to CNN - <http://money.cnn.com/2012/01/19/technology/megaupload_shutdown/index.htm>
- The Internet Strikes Back #OpMegaupload - <http://anonops.blogspot.com/2012/01/internet-strikes-back-opmegaupload.html>
- Twitter Post from the author of the JavaScript based LOIC code - <http://www.twitter.com/#!/mendes_rs>
- Anonymous Operations tweets on Twitter - <http://twitter.com/#!/anonops>
- @Megaupload Tweets on Twitter - <http://twitter.com/#!/search?q=%2523Megaupload>
- LOIC DDoS Analysis and Detection - <http://blog.spiderlabs.com/2011/01/loic-ddos-analysis-and-detection.html>
- Impact of Operation Payback according to CNN - <http://money.cnn.com/2010/12/08/news/companies/mastercard_wiki/index.htm>
- OperationPayback messages on YouTube - <http://www.youtube.com/results?search_query=operationpayback>
- The Bogon Reference - Team Cymru - <http://www.team-cymru.org/Services/Bogons/>

Feedback can be directed to US-CERT.

Revision History

January 24, 2012: Initial release

Last updated January 24, 2012

Print This Document