F5 Threat Analysis: It's a mad, mad, mad, mad ... bot

Lori MacVittie, 2015-26-02

Madness. It's an aptly named bot, as it's likely to evoke just that reaction in those who find it lurking in their systems or at whom its sets it sights.

A disturbing trend illustrated by the focus of our latest threat analysis is the increase in attention being paid to application layer attacks. Not just directly, but also as part of larger volumetric attacks. Increasingly application layer attacks are seen as part of a larger attack that takes advantage of volumetric network DDoS techniques as a "smokescreen" to hide their real intent. A 2014 Neustar report found that 55% of DDoS attack victims experienced application layer attacks at the same time that successfully deposited malware (over 50%) or exfiltrated customer data (26% of victims). While the focus of our analysis today, Madness, appears to be solely concerned with Denial of Service and not intended or capable of perpetrating attacks designed to exfiltrate or corrupt customer or corporate data, its increasing capabilities at layer 7 are indicative of a general trend toward attacks on applications rather than the network.

That's the bad news.

The good news is that organizations overwhelming feel confident in their ability to withstand such attacks; our State of Application Delivery 2015 survey found that 92% of customers were confident to very confident they were ready and able to handle such attacks. Given that a majority protect all three attack surfaces "all the time", this confidence is likely warranted.

But as complacency is as dangerous to security as complexity, it's always a good idea to know thine enemy - particularly with respect to what weapons their arsenals contain.

With that proverbial advice in mind, let's get a quick look at Madness, shall we?

Madness is, according to its authors, a superior successor to notorious DDoS malware families “BlackEnergy”, “gbot”, “DirtJumper”, “Darkness Optima”, “iBot” and “w3Bot”.

Though the bot employs standard persistency techniques its attacks show an increasing level of sophistication. In terms of the former it employs a fairly traditional Marco Polo technique of constantly polling for the existence of specific registry keys that, if found to be missing, will be added again.

On the attack front, however, Madness displays a growing awareness of the richer attack surfaces at layer 7 (application). While supporting traditional network-based DoS capabilities, Madness also offers a number of application layer attacks with growing detection evasion options. Madness' HTTP flood options can be categorized into low-level and high-level attacks. Low-level attacks allow the attacker to control all aspects of the HTTP request. By enabling complete control over the request, attackers can better construct requests that can bypass many DDoS protection mechanisms. Higher-level attacks provide automatic handling of all protocol level concerns such as request construction, TCP connection management, caching, cookies and even redirections.

Madness adds an interest twist to traditional HTTP GET flood attack by adding a slight delay in between the initial GET request and the completion of the request as indicated by the standard carriage return-line feed combination ("\r\n"). As this version of the attack does not include many of the traditional HTTP request headers - it comprises only the Host header - attacks from Madness using this attack should be fairly easy to detect.

Our Security Research Team, which is dedicated to performing research of DDoS, web, mobile and malware threats, has put together a comprehensive analysis of Madness. You can get the full report here, which includes details on:

1. Persistency techniques
2. C&C methods
3. Attack types and capabilities
4. Mitigation guidance

They've also penned a technical blog detailing their analysis.

Stay safe out there!

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113