DeepSight™ INTELLIGENCE

DDOS-FOR-HIRE

MANAGED ADVERSARY AND THREAT INTELLIGENCE

DEEPSIGHT™ INTELLIGENCE | INTELLIGENCE PROFILE | SYMC - 300249 | V.1
07 AUG 2015 GMT

LEGAL NOTICE

SYMANTEC PROPRIETARY & CONFIDENTIAL - PERMITTED USE ONLY

Symantec assigns a high, medium, or low degree of confidence to assessments within its DeepSight™ Intelligence Portal Managed Adversary and Threat Intelligence (MATI) products. Confidence levels are determined against a three-point spectrum of source validity: variety and non-conflictive disparity of original sources, quality of source reporting, and reliability of source reporting. Confidence levels may be increased based on independent corroboration of information. High confidence generally suggests a solid judgment can be made, though such a judgment carries the risk of being wrong. Low confidence generally suggests tenuous inferences can be made, though information used to do so may have been questionable, fragmented, or singular.

Information Cut-Off Date: 04 Aug 2015 GMT

DDoS-for-Hire

DeepSight™ Intelligence | Intelligence Profile | SYMC - 300249 | V.1 | 07 Aug 2015 GMT

KEY FINDINGS

For a minimal cost, an attacker can possibly impact the availability of a target's services (i.e., perform a distributed-denial-of-service or DDoS attack) by using a DDoS-for-hire service.

Two of the more popular DDoS-for-hire options on online cybercrime forums in 2015—vDos Stressor and Fluffy—range in price from US$30 to US$200 a month.

More flexible and custom DDoS-for-hire offerings can be acquired on "Hacker's List," which provides options that could be more effective against target organizations than generic offerings.

EXECUTIVE SUMMARY

DDOS-for-hire services, also known as stressor services, allow attackers to conduct DDoS operations against a target for a minimal cost. There are currently hundreds of DDoS-for-hire options available with the majority causing only short-lived impacts lasting less than one hour. Recent reporting on DDoS attacks suggests that almost 40% of DDoS attacks are from paid services with the gaming industry, software companies, and media organizations the most often targeted. Hactivist groups such as Lizard Squad have previously demonstrated the effectiveness of DDoS-for-hire services against large corporations like Sony and Microsoft.

DETAILS

DDoS-for-hire or “stressor” services offer attackers a low-cost service that eliminates much of the preparation time and technical ability needed to launch an impactful DDoS attack. According to a website dedicated to the review of stressor services, there are several unlimited lifetime DDoS-for-hire services that are available for under US$200. Furthermore, those interested in stressor services are able to locate reliable and reviewed options without access to exclusive or private online venues —a simple search with a popular search engine returns a variety of viable results. DeepSight Intelligence has identified two DDoS-for-hire services, VDos Stressor and Fluffy, as two of the more popular and well-regarded services available in online cybercrime forums.

VDos Stressor

The vDos Stressor, available since 2012, is frequently recommended as a stressor service on popular hacking sites. This DDoS-for-hire solution claims DDoS attack speeds ranging from 20 Gb/s (Gigabits per-second) to 50 Gb/s. As of August 2015, packages start in price at US$29.99 for one month of service to US$169.99 for lifetime service (see Figure 1). DeepSight Intelligence is aware of several instances in which this solution has received praise from its users for high speeds and reliability.

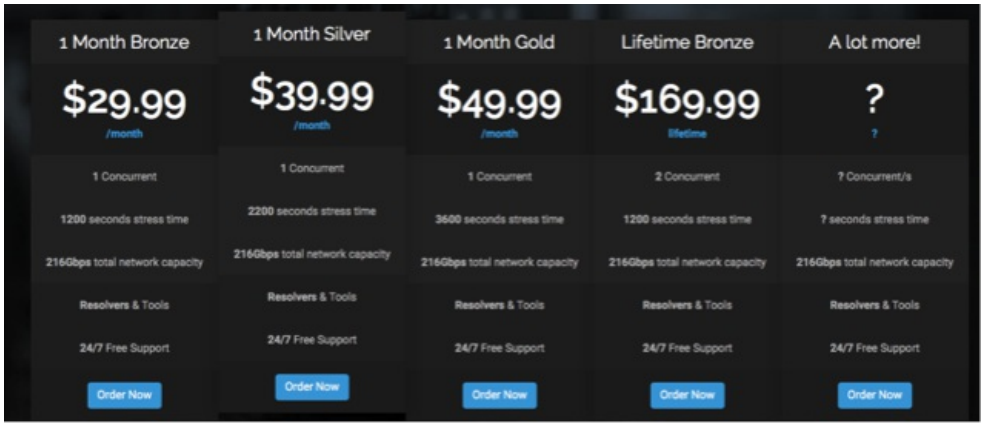

Figure 1. vDos Stressor pricing in 2015

Support for the vDos Stressor appears to be ongoing based on a June 2015 post by the tool's owner advertising for one or two additional team members to “assist customers” (see Figure 2). The stated requirements for new team members included: at least 15 years old, English and Mandarin language skills, good judgment/problem solving capabilities, and some knowledge about SST (server stress testing). The team members receive “payment” for their services in lifetime membership and free “gifts.”

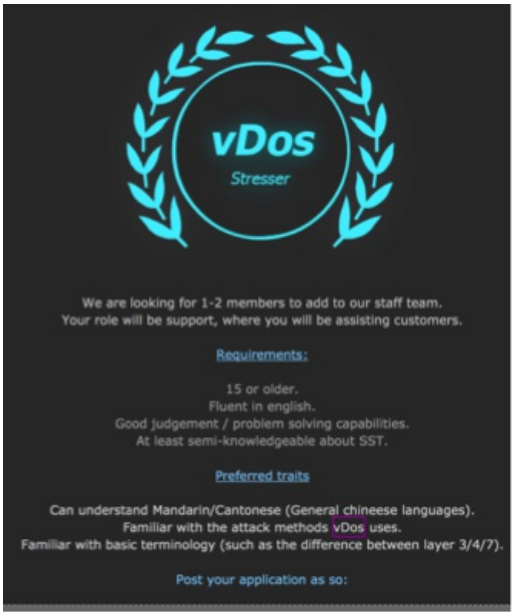

Figure 2: vDos advertisement for new staff

Fluffy Stressor

Started in 2012, the Fluffy stressor is promoted often on online cybercrime forums particularly among users interested in targeting gaming services.[1] The owner of Fluffy, using the moniker "ItsFluffy," frequently provides technical support and answers questions about the service. There are several published pricing tiers for this service, but it appears that the service ranges in price from US$30–$80 per month depending on the speed and the number of concurrent sessions (see Figure 3). A free version of the stressor called Fluffy Booter is also available. This version does not allow its users to target gaming servers, further suggesting that gaming servers are a desirable target for users of this service.

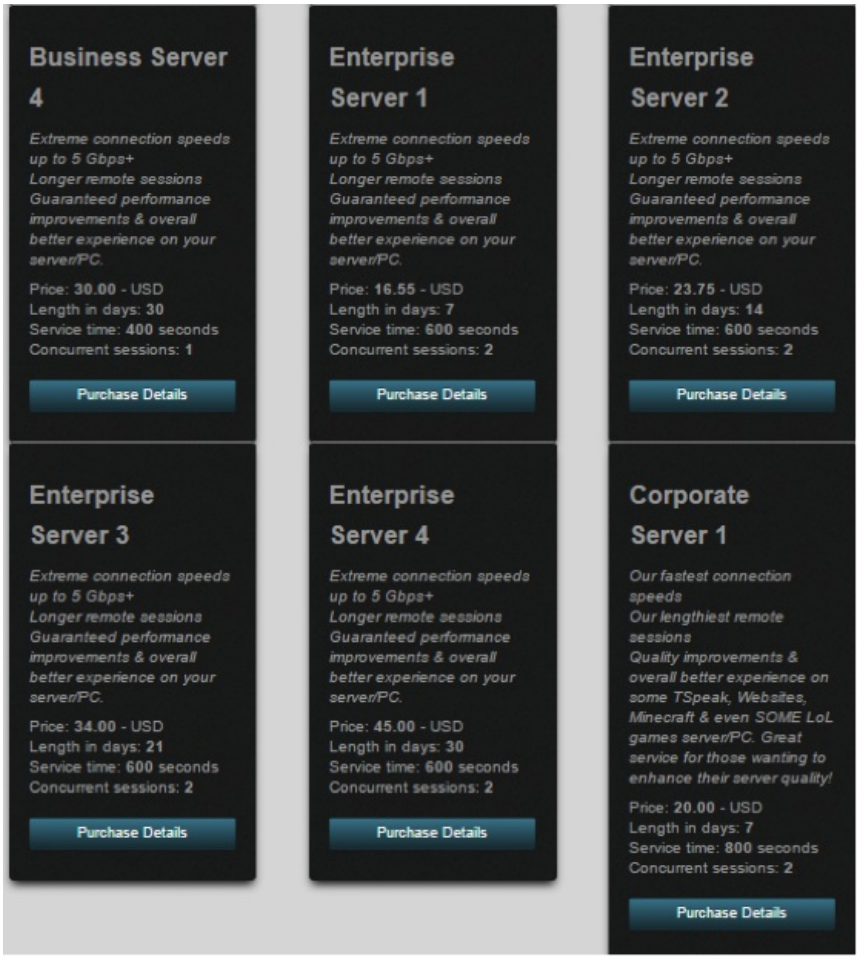

Figure 3: Fluffy pricing as of 4 August 2015

The Fluffy stressor's reliability over the years and its responsive technical support make it a popular service on online cybercrime forums. Fluffy stressor is also highly regarded by many users for its easy-to-use control panel interface (see Figure 4).

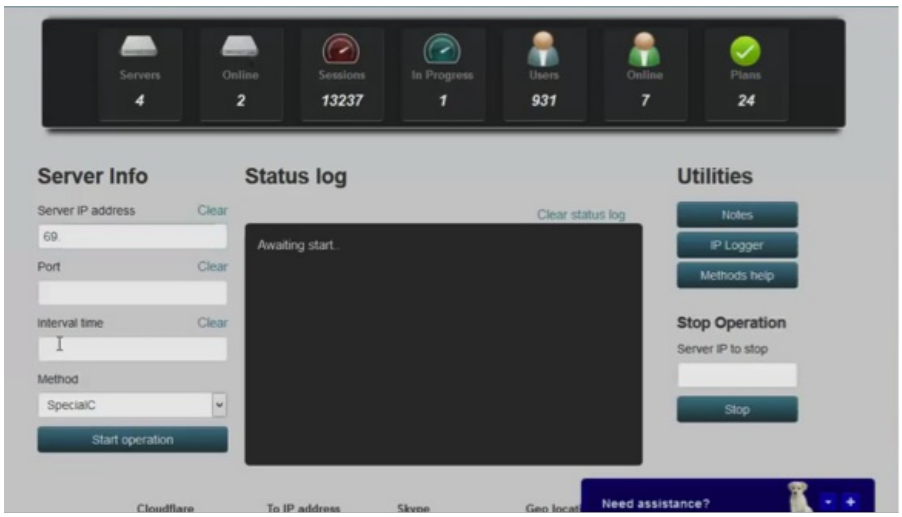

Figure 4: Control panel for Fluffy Stressor

Hacker's List

An alternate approach for attackers seeking to conduct a DDoS attack is using a bidding system like Hacker's List. Started in October 2014, Hacker's List claims to "connect people who need professional hackers to professional hackers for hire around the world."

As of 4 August 2015, there were four projects available for bidding with users willing to pay between US$100 to US$1,000 for DDoS services (see Figure 5). The advertisements were for projects "of a personal nature" and the users were located in Afghanistan and Brazil. The project proposal and bids are conducted anonymously. The service collects the fee upon completion of the job with the customer's payment held in escrow until the task is completed.

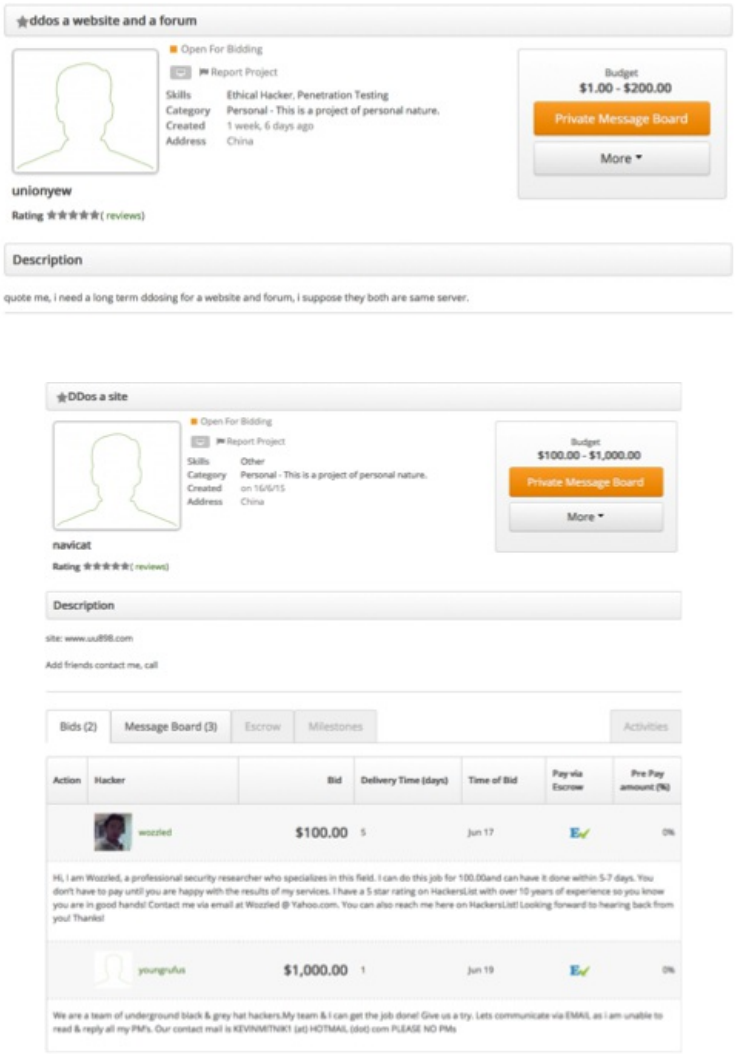

Figure 5: Advertisements for hacker services

[1] DDoS is a common method in the gaming community to temporarily disconnect competing teams.

OUTLOOK

Hactivist groups have already demonstrated their use of DDoS-for-hire services against major corporations and will likely continue to use them as part of their ideologically motivated operations. Organizations that employ defenses to counter common DDoS techniques, including proper network segmentation and paid mitigation services, are unlikely to be impacted in a significant way by generic solutions such as vDos Stressor and Fluffy.

Custom DDoS-for-hire services, such as those offered by Hacker's List, likely pose a higher threat to organizations who specifically defend against common DDoS techniques. As the DDoS-for-hire job is not paid out of escrow by the broker until it is completed, the executors of the job likely feel compelled to use more creative and specifically crafted approaches against the organization. Depending on the skill of the attacker and the presence of vulnerabilities or misconfigurations, the rate of success could be higher.

TECHNICAL DETAILS

See the ***Metadata*** tab for the technical details and indicators of compromise related to this report.

METADATA

TARGET INDUSTRIES

NAICS Code	Name
5112	Software Publishers
51	Information

SOURCE REGIONS

Region	Americas
Subregion	North America
Countries	United States

TARGET REGIONS

Region	Americas
Subregion	North America
Countries	United States

THREAT DOMAINS

Hacktivism