ANATOMY OF A HACKER: PROFILES, MOTIVATIONS & TOOLS OF THE TRADE

In the old days, hacking was as much an art as it was a science. It required a distinct set of skills, proficiencies and capabilities. Today, attack services are purchased and sold via the Clearnet and Darknet – a phenomenon that's closing the gap between skilled digital accosters and amateur hackers while fueling an exponential increase in threats.

It's now possible to wreak havoc even if you know virtually nothing about computer programming or networks thanks to the growing array of online marketplaces. As attack tools and services become commoditized, the pool of possible attackers—and possible targets—is larger than ever. While many hacktivists still prefer to enlist their own digital "armies," some are discovering that it's faster and easier to pay for DDoS-as-a-Service than to recruit members or build their own botnet. Highly skilled, financially-motivated hackers can be invaluable resources to hacktivists seeking to take down a target.

By commoditizing hacktivist activities, hacking marketplaces have also kicked off a dangerous business trend. Vendors are now researching new methods of attack and incorporating more efficient and powerful vectors into their offerings. Already some of the marketplaces offer a rating system so users can provide feedback on the tools. Ultimately, this new economic system will reach a steady state—with quality and expertise rewarded with a premium.

Profiles in Hacking: Who's Participating in Today's Hacking Community?

- **Consumers**. This is the largest segment—and the one driving the rapid growth of attack marketplaces. These are low or non-skilled hacktivists who pay to participate in an operation. Without the knowhow for do-it-yourself campaigns, they spend $20 to $200 per month on attack services that give them access to an easy-to-use attack portal.

- **Hackers**. These are the hackers who have the wherewithal to carry out their own attacks and spearhead hacktivist operations. They have a good enough understanding of networking and programming to write their own attack programs, as well as build their attack platforms by exploiting cloud and trusted services. Given their skills, hackers are not constrained by an attack time limit or power. Consequently, they are capable of launching sustained, long-term attacks against their targets, sometimes at very high volumes.

- **Vendors**. This segment is home to hackers who have realized they can generate a great profit by providing attack services to consumers. As in any economic system, higher quality or sophistication yields greater returns and forces improvement. Some vendors are selling enough services to generate more than $100,000 a year. AppleJ4ck, the vendor behind vDoS, the DDoS-for-hire service,[1] allegedly made $600,000 in just two years before being arrested.

What Motivates Hacking?

In previous reports, Radware has used Richard Clarke's acronym—C.H.E.W. (Cybercrime, Hacktivism, Espionage, Warfare)—to categorize the origins of cyber risk. Now we introduce P.E.D. (Profit, Evasion, Disruption) as an acronym for the three core motivations reflecting the evolution of the hacker community:

- **Profit**. Not surprisingly, money is the primary motivation in the attack marketplace. Those who want to commit a crime—but don't know how to execute—will always pay someone to do it for them. And with demand outpacing supply, this is one crime that pays. Stressers – services orchestrating generation of massive amount of traffic - are known to bring in more than $100,000 a year. Vendors offering application exploits can generate thousands of dollars from selling one exploit on the Darknet.

- **Evasion**. The ability to evade detection is one of the most important capabilities a vendor offers to his or her business and clients. Vendors are highly motivated to stay on top of the market. After all, detection or mitigation of their services will cost them customers and profits. Thus, vendors continually research and discover new attack methods to help their clients bypass mitigation techniques and take down their targets undetected.

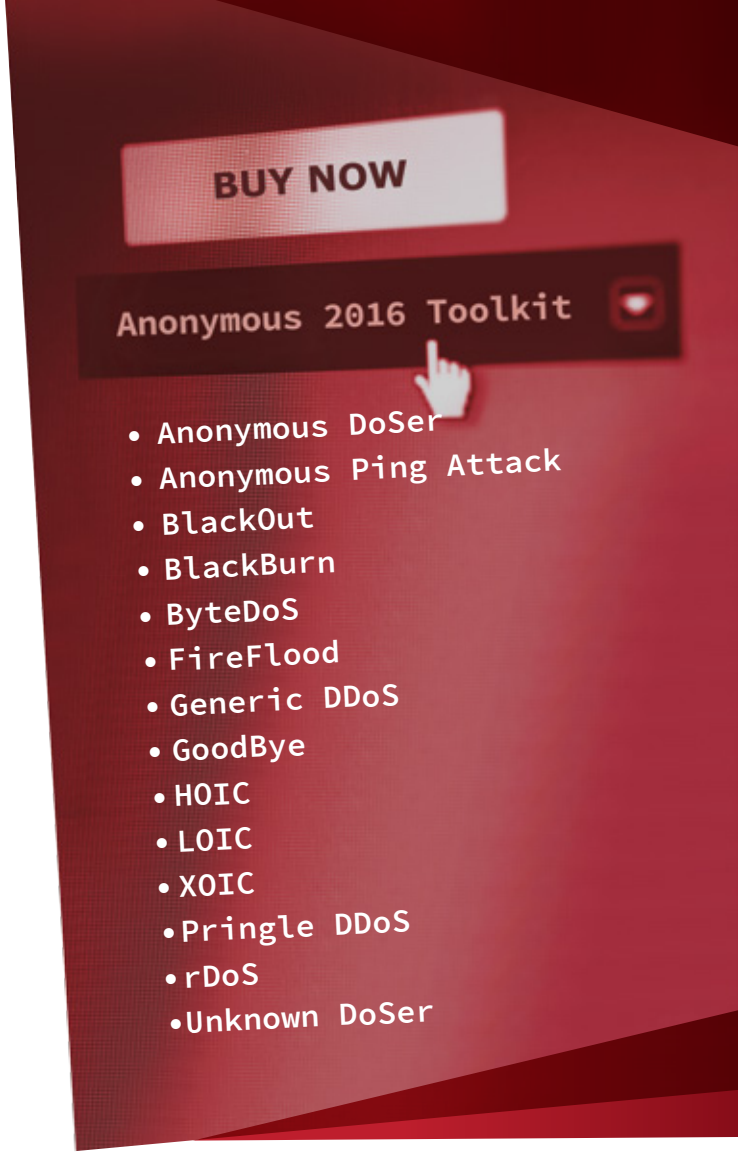
- **Disruption**. This represents one of the primary motivators for hacktivist groups. Hacktivists are motivated to disrupt their target's operations and/or reputation; vendors thrive by investing in researching and discovering new attack vectors. A vendor offering the most disruptive power for the lowest price will stand to do more business than his or her competition.

Tools of the Trade

The Anonymous 2016 toolkit has been passed around in a number of operations. It provides attack tools with a simple, easy-to-use graphical user interface (GUI). Using these tools requires little knowledge as they are often accompanied by instruction videos posted to YouTube.

1 http://www.newsbtc.com/2016/09/18/professional-ddos-service-vdos-offline-two-arrested/

Most tools offer basic TCP, UDP and HTTP attack vectors with slight variations. Some enable the attacker to customize payload options—including packet size, randomized data, threads and sockets per thread—in the tools. While low and slow attacks are not prevalent in the popular 2016 toolkits, HTTP attacks are a popular vector. When an operation is underway, hackers can easily bypass mitigation solutions and overwhelm server resources with simple POST/GET floods that appear to be legitimate traffic.



Attacks as a Service

Denial of service (DoS) attacks have come a long way since the days of LOIC and other GUI-based tools. Today, hackers are abandoning "old school" GUI and script tools and opting to pay for attacks via stresser services. They no longer need to acquire technical expertise or tools; instead, they can simply engage attack services to carry out an attack on their behalf.

Many notorious DDoS groups—including Lizard Squad, New World Hackers and PoodleCorp—have entered the DDoS-as-a-Service business, monetizing their capabilities in peacetime by renting their powerful stresser services. Groups sometimes use their tools against high-profile targets to showcase and promote their attack services. As the point of entry continues to decrease, novice attackers can carry out larger, more sophisticated assaults. For just $19.99 a month, an attacker can run 20-minute bursts for 30 days using a number of attack vectors, such as DNS, SNMP and SSYN, and slow GET/POST application-layer DoS attacks.

A prime example of a DDoS-as-a-service is Shenron—the second-generation stresser service from Lizard Squad. Shenron prices used to range from $19.99 to $999.99 a month for access to the attack network. Each package includes a specific attack time—ranging from 20 minutes to five hours. Shenron's network strength claims the ability to launch attack sizes up to 500Gbps. It offers customers different attack vectors, including two UDP attacks, DNS and SNMP, along with a TCP attack method (SSYN).

Download the 2016-2017 Global Application & Network Security Report to learn more.

www.radware.com/ert-report-2016

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.