radware

THE CHANGING FACE OF HACKING

Change is the only constant, and hacking is no exception to this rule. A hacking evolution is underway - fueled by greater automation, growing monetization and increasing chaos and conflict by those aiming to prosper from hacking products and services.

To safeguard your organization's most prized digital assets starts with understanding what motivates hackers, their tools and techniques and the increasing consumerization of the attack landscape.

For years, the industry waited for an IoT botnet to execute a large-scale DDoS attack that would test modern-day defenses. It finally happened in 2016, introducing a new era in hacking. The botnet threat landscape evolved in 2017 via hackers' growing use of automated features in cyber-attack programs and tools to increase the monetization of hacking. Launching an attack is no longer the sole purview of individuals or groups with hacking experience and expertise. Hacking services are now purchased and sold via online marketplaces—making it possible for virtually anyone to pursue a target.

THE CHANGING FACE OF THE HACKING COMMUNITY

In 2017, Radware witnessed three primary types of hackers:

- **Consumers.** Arguably the fastest-growing segment within the community, these are the non-skilled users who pay to play. They can now easily obtain Cyber-Attack-as-a-Service (CAaaS) tools in marketplaces on the Clearnet and Darknet.
- **Purists.** These are the skilled hackers who have the expertise to conduct their own operations without paid services or other outside help.
- **Vendors.** These are the skilled hackers who want to turn their capabilities into products and services to meet growing demand from hacking consumers.

The Market

As hacking and automation continue to converge, more vendors are stepping up to reap the financial gains. This strong shift toward monetization reflects three opportunities:

- Applying one's own talent to build and market CAaaS tools
- Offering hacking services on a freelance basis
- Participating in activities that yield substantial financial payoffs

Attack service vendors are seeking to replicate their successes by offering services via marketplaces. These marketplaces, which sell everything from DDoS-as-a-Service (DDoSaaS) to Ransomware-as-a-Service, have hit some potholes recently. Raids and takedowns have become common on the Darknet as federal agents around the world step up enforcement. Even as they are targeted by law enforcement, market operators and vendors face another set of threats from competitors, rogue users, vigilantes and extortionists. These players are looking to profit by exposing administrators' personal details as well as vulnerabilities in their respective marketplaces.

For the onion network, 2017 has been an eventful year. In February a vigilante hacker took down more than 10,000 hidden services, representing about one-fifth of the network. The services were running on Freedom Hosting 2, one of the largest Darknet hosting providers. When a hacker discovered it was hosting child pornography, the hacker took the provider offline and leaked the databases and private keys in a public dump.

On July 20, 2017, Hansa was shut down following the July 4th takedown of AlphaBay. During a press interview on July 20, it became known that Hansa was originally taken over on June 20, but law enforcement officials did not immediately take the market offline. They instead operated Hansa for several weeks—quietly collecting user names, passwords and activities of users and vendors alike.

Ultimately, a takedown creates a vacuum that others will rush to fill. A new and improved marketplace will emerge—only to be taken down and replaced by yet another new marketplace. With so much money on the line, vendors use trial and error to continually rebuild bigger and better. They research new attack methods and continue incorporating more efficient and powerful vectors, including automation of attack services. They will continue to be targeted by law enforcement and researchers along with criminal hackers seeking their own paydays.

Morphing Motivations

Hacktivism historically has been a major motivation for hackers, with most operations carried out through collectives. In 2017, a growing number of hackers seem unfulfilled by joining an Anonymous operation and are choosing to work alone. Radware has observed a decline in organized operations by Anonymous and similar collectives. While there is still outrage in cyberspace, it is not necessarily coordinated (though this is admittedly difficult to track given how many individuals and small teams coopt the "Anonymous" brand when launching an attack).

We see several contributors to this shift from coordinated hacktivism to lone-wolf hacking:

- **Maturity.** Many who participated in hacktivism or vandalism in the virtual space a few years ago have since grown in skill and personality. Material needs have grown, prompting them to seek not only justice but also profit.
- **Cryptocurrencies.** The perceived value of Bitcoin and other cryptocurrencies has skyrocketed. Cryptocurrencies are also the only way to monetize skills and services over the Darknet—today and in the future. Hackers do not want to miss the "party."
- **Market dynamics.** Hacking isn't immune to the laws of supply and demand. Online marketplaces provide a vehicle to deliver hacking services regardless of what's motivating the person buying and executing an attack.

In the past, launching a massive DDoS campaign required gathering a group of people, while leaking sensitive information required a surgical attack and much trial and error. Today even those without extensive hacking skills can easily find a mercenary or a service to do the dirty work. Damage can be done without the need to work through a collective, and even the most complicated operation is within reach. All you need is inspiration—and money.

Even as hacktivist collectives diminish in importance, we see another type of group ascending: hacking "businesses." A growing number of these operations have enough scope and scale to require a supporting team. Instead of rallying around a shared cause, these groups are focused on profit. The CAaaS market is highly competitive. Vendors offering hosting, anonymization and advanced attack tools need to do more than build those tools. They must also market them, support them and maintain an infrastructure for collecting and managing revenue.

There is an emerging trend of creating infrastructure to power cyber-attack tools. Beyond hosting attack tools, such infrastructure serves up a "buffet" of malware installations that can be leveraged for different purposes—from stealing data and spreading spam to launching ransom attacks and mining cryptocurrency. Hackers can rent this infrastructure and run any attack tool they desire on the infected machines.

The Tools and Techniques

The tools of the trade have not significantly changed in 2017. Hackers are still using VPN and the Tor network to obfuscate their identities and operations. Commonly used virtual private servers in Anonymous operations have included proXPN, Cyberghost and Tor VPN. Hackers will normally use these services when launching denial-of-service attacks from their personal devices or while communicating over social media (typically Jabber or IRC). Interestingly, some groups have moved completely to the Darknet where hidden and mirrored services are used. Facebook is an example, as it provides a Clearnet version (Facebook.com) and hidden service (Facebookwwwi.onion).

Hacktivists are using a number of tools for reconnaissance, which helps in mapping networks and looking for vulnerabilities. Scanning is typically an automated process used to discover devices, such as PCs, servers and other endpoints on the network. Results can include details of the discovered devices, such as IP addresses, device names, operating systems, running applications/servers, open shares, usernames and groups. The two types of scanning are horizontal scan (searching the same port on multiple IPs) and vertical scan (searching multiple ports on one IP). Many web applications enable administrators to access the site using interfaces that could give hackers full access to it.

What follows is an overview of some of the application scanning and web application reconnaissance tools to have on your radar.

Application Scanning Tools

- **Nmap.** Nmap is 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, what operating systems (and OS versions) they are running and what type of packet filters/firewalls are in use, among dozens of other characteristics.

- **Nikto.** This open source (GPL) web server scanner performs comprehensive tests against web servers for multiple items including 6,700+ potentially dangerous files/programs. It also checks for outdated versions of more than 1,250 servers and version-specific problems on some 270 servers. Nikto also checks for server configuration items such as the presence of multiple index files and HTTP server options and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated. These updates can be automated.

- **SQLmap.** This open source penetration testing tool automates the process of detecting and exploiting SQL injection flaws and taking over database servers. It comes with a powerful detection engine and many niche features for the ultimate penetration tester. These features include a broad range of switches—from database fingerprinting and data fetching from the database to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

Additional Web Application Reconnaissance Tools

- **Sniper** is an automated scanner that can be used during a penetration test to enumerate and scan for vulnerabilities.
- **The Harvester** harvests e-mail, subdomain and people names.
- **Sublist3r** is a fast subdomains enumeration tool for penetration testers.
- **Metasploit** is a tool for developing and executing exploit code against a remote target machine.
- **WAFW00f** identifies and fingerprints the Web Application Firewall (WAF) products protecting a website.
- **XSStracer** is a small python script to check for Cross-Site Tracing (XST).
- **WPScan** is a black box WordPress vulnerability scanner.
- **Arachni** is a Web Application Security Scanner Framework
- **Shocker** is a tool to find and exploit servers vulnerable to Shellshock.
- **UNURLBR** supports advanced search in search engines and enables analysis provided to exploit GET/POST capturing emails and URLs. It offers an internal custom validation junction for each target or URL it finds.
- **TestSSL** makes it possible to test TLS/SSL encryption anywhere on any port.

Prominent Attacks

DDoS and IoT botnet attacks—both covered in their own chapters in this report—are two of the most prominent types of hacker attacks of 2017.

Record-breaking volumetric DDoS attacks still flash in the headlines, but low-profile denial-of-service attacks keep hitting business worldwide. These low-profile campaigns are largely fueled by political or social justice and can cause widespread outages. Hackers continue to leverage many of the same tools even as they search for new attack vectors and methods. HTTP floods, which are harder to block, are a hacktivist favorite when it comes to causing a business disruption. Dozens of HTTP flood tools are already available to the hacker community and are being continually improved by their vendors. Most of these tools leverage botnets for rent (DDoSaaS or stresser services) that include HTTP flood attacks as part of their offering.

An IoT botnet is a collection of compromised IoT devices, such as cameras, routers, DVRs, wearables and other embedded technologies, that have been infected with malware. That malware empowers the attacker to take control of the devices and use them to carry out tasks just like a traditional botnet. Adoption of connected devices is growing exponentially. Hackers use automatic tools to scan for and infect IoT devices for enslavement into botnets to launch powerful DDoS attacks. Not surprisingly, these tools are available for rent in hacking marketplaces. What's more, today's hackers can even create customized versions of open source botnets and use these programs to launch attacks not already classified by traditional security solutions.

DOWNLOAD THE *2017-2018 GLOBAL APPLICATION & NETWORK SECURITY REPORT* TO LEARN MORE

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.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.

©2018 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this press release are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details please see: https://www.radware.com/LegalNotice/. All other trademarks and names are property of their respective owners.