

Hacktivism Focus Group Report

January 2011



CONTENTS

Introduction	3
Hacktivism: Cyberattacks Based on Personal Beliefs	3
Hacktivism Is Not a Fundamentally New Threat.....	4
Hackers' Motivations and Methods Are Evolving	4
Securing Your Network against Attack.....	5
Conclusion	6

Introduction

On January 18, 2011, F5 Networks moderated a focus group of nine high-level IT professionals, discussing the ramifications of the recent WikiLeaks-related, large-scale DDoS attacks on businesses. The IT professionals agreed to participate on grounds of anonymity.

Hacktivism: Cyberattacks Based on Personal Beliefs



“We’ve been seeing an uptick in attacks over the last year or so, but I don’t think I could attribute any of it to WikiLeaks.”

—senior architect of an electronic publishing company

In 2010, the controversial organization known as WikiLeaks released thousands of previously confidential and classified documents to the public. The documents dealt with sensitive political issues, including the involvement of the U.S. military in Afghanistan and Iraq, and diplomatic cables from U.S. embassies. In response to the dissemination of this information, the U.S. government began to exert pressure on organizations linked to WikiLeaks in order to stem the flow of sensitive information, citing concerns regarding national security. The pressure resulted in backlash from various groups championing unrestricted transparency of government actions. As part of this backlash, a group of hackers collectively known as Anonymous began coordinated Distributed Denial of Service (DDoS) attacks on a number of websites operated by organizations opposing WikiLeaks. For example, in response to government pressure PayPal had ceased to process donations being made to WikiLeaks, and it became one of the primary targets of attack. This kind of concentrated attack motivated by a sense of justice on the part of the hackers is being referred to as “hacktivism.”

DDoS attacks prevent a website or other network resources from being available to users, often by flooding it with communications requests, which can cost a business hundreds of thousands of dollars in lost revenue. In addition to PayPal, related attacks were made on other high-profile websites including mastercard.com and amazon.com. The attacks were well publicized by the media, and many people have consequently assumed that these massive attacks represent a new danger to the Internet, and that no website can be completely protected from this new threat.

In order to secure the opinion of IT professionals, F5 Networks conducted a focus group with nine high-level security experts from medium and large enterprises. The purpose of the focus group was to see the issue from the perspective of those with IT and security experience, to accurately ascertain the level of risk and learn what enterprises might do to improve their network and application security.

Hacktivism is Not a Fundamentally New Threat

As part of the discussion, the participants were asked whether their respective companies had seen increased cyberattacks that appeared related to the WikiLeaks issue. Of the nine participants in the focus group, only two had noticed attacks, and they were directed at other companies for which they provide web-related services. Overall, the pattern of malicious activity did not drastically increase in the wake of the WikiLeaks controversy. For the most part, IT departments do not distinguish this kind of attack from any other. As one VP of information systems for a large hosting company noted, “It’s just a part of doing business. I mean, attacks happen daily, hourly.” They view it as simply another attack in the spectrum of threats that they are already monitoring.

“It’s just a part of doing business. I mean, attacks happen daily, hourly.”

—VP of information systems for a large hosting company

Hackers’ Motivations and Methods Are Evolving

There were, however, a few things about the WikiLeaks-inspired attacks that differed from previous threats. First, these attacks were “opt-in.” This is notable because instead of looking for computers which were susceptible to malware, users were voluntarily allowing their machines to be controlled for the purpose of implementing the DDoS attacks. By downloading a single piece of software, these volunteers became part of a botnet, which is controlled remotely to coordinate an attack. The result of this practice is hackers can now more easily gain access to large numbers of machines for illegal purposes. Not only that, but when using a machine covertly, a hacker only has access to a fraction of the resources in order to remain undetected. By having willing subjects, this new breed of hackers, or “hacktivists,” can fully utilize the resources of each machine, making them many times more effective. Thus a smaller number of machines can do more damage.

“We had some content we put out that angered some groups a couple years ago, and they attacked us pretty strongly.”

—senior technology architect of an electronic publishing company

The mobilization of these hacktivists on a large scale is a new development. This is inadvertently fueled in part by the media, as controversies of this nature become more widely covered. As the senior security architect for a financial institution pointed out, “Whenever we are in the media or customers are in the media, that makes us a target.” Hacktivists are primarily concerned with righting a perceived wrong, either uncaring or unaware that cybercrime is considered a real crime by law enforcement agencies, despite the relative anonymity of Internet actions. This differs from traditional hackers, whose motives are primarily financial.

“Whenever we are in the media or customers are in the media, that makes us a target.”

—VP of information systems for a large hosting company

“We made sure that our internet service providers have the capability to block these attacks, and keep that traffic off of our pipe so we can keep serving our customers.”

—senior security architect of a large financial institution

One additional concern related to the moral aspect of this kind of hacking is that even a company’s own employees may participate in the attacks, directly or indirectly. An employee might be willing to risk termination or even legal action for the sake of personal belief or a political agenda.

In terms of the severity of these coordinated attacks, the focus group participants felt that the scale of the threat was represented disproportionately by the media. They pointed out that the attacks were within the realm of what they currently experience, and that the intensity of hacking attempts had been steadily increasing in any event. “We’ve been seeing an uptick in attacks over the last year or so,” noted the senior architect of an electronic publishing company, “but I don’t think I could attribute any of it to WikiLeaks.” The participants also noted that it’s important to continue applying fundamental security measures, upgrading network infrastructure regularly. The attacks are constantly increasing in sophistication, so security must respond the same way.

Securing Your Network against Attack

In response to the findings of the focus group, F5 Networks has offered recommendations for bolstering network security in the face of ever-evolving threats. These recommendations focus on implementing policy and laying the proper foundation for reacting quickly to reduce the damage caused by DDoS attacks.

As one of the focus group participants said, “I think anybody who would say that they’re foolproof or perfect is a fool.” In light of that statement, one of the most important recommendations offered by F5 is to plan adequately, considering current threat levels and anticipating what might come in the future. In particular, good communication with Internet service providers can help stop malicious traffic before it affects a company’s network. The senior security architect of a large financial institution stated, “We made sure that our internet service providers have the capability to block these attacks, and keep that traffic off of our pipe so we can keep serving our customers.” Work together to develop a plan to detect and shut down malicious traffic *before* resources are compromised.

Another precaution companies can take to secure their networks is to pay attention to the social networking landscape. In contrast to typical hackers, hacktivists often communicate openly through public channels on the Internet to coordinate attacks. “We’re involved in watching discussions and code sharing and chat groups,” stated the director of security services for a large communication solutions provider. Several other companies represented in the focus group noted that they also

have staff members who monitor the Internet for such clues. Being aware of an impending attack greatly increases the chances of reducing or entirely eliminating network problems caused by hacktivist attacks.

According to F5, awareness also plays an important role in network security. When a company releases any information to the media, they should be aware that the more visible they are, the more likely people are to take issue with something the company has said. Carefully consider the potential implications of your corporate communications. As one senior technology architect pointed out during the focus group, “We had some content we put out that angered some groups a couple years ago, and they attacked us pretty strongly.”

Another problem posed by these attacks is that multiple attack vectors might be employed simultaneously by separate groups of hacktivists. One botnet might be directly attacking the network infrastructure, while another is seeking to take advantage of vulnerabilities in specific applications. In the future, attacks of such complexity will become far more common. IT staff should be aware that security software will need to handle attacks on multiple levels; simple firewalls will easily be overwhelmed by the scale of the attacks.

Conclusion

Large-scale DDoS attacks perpetrated by hacktivists have been billed as an unprecedented threat to the security of corporate networks. While there are new aspects to these attacks, the result is much the same as what IT departments are currently defending against. A focus group with security professionals revealed that while large-scale attacks are real and can cause serious problems, they are no cause for undue panic when companies are well prepared. As long as IT departments communicate with their service providers, work to keep the network infrastructure up to date, and install proper safeguards, they can ensure continued network functionality in the face of hacktivism.

“We’re involved in watching discussions and code sharing and chat groups.”

—director of security services for a large communication solutions provider

