slashdotmedia
Pure Technology. Pure Engagement.

sourceforge Slashdot

Behind the Mask:

The Changing Face of Hacking

June 2015

Think your users and data are safe? Think again. Today's mega-trends of mobility and cloud computing not only bring great promise for IT, they offer an array of new attack surfaces for bad actors to exploit for nefarious purposes.

The opportunity for gain is so compelling that hackers have evolved from the stereotype of bored students to today's reality of highly organized criminal enterprises that seek not just notoriety but profit. What's worse, all the information needed to execute successful attacks – from employee profiles to holes in network defenses – are available for sale in online marketplaces. Current advantage, attackers. How can organizations level the playing field?

This SlashGuide takes an in-depth look at how hackers have changed, what new targets they are focusing on, and what risks enterprises of all sizes should be aware of in today's security-conscious climate.

Introduction

When it comes to modern security efforts, the stakes are higher than ever. Old vulnerabilities continue to plague organizations while new threats only grow in complexity and sophistication. Meanwhile, the weakest link remains users themselves.

Many major breaches in the last few years have shown that thieves are combining attacks, frequently piggybacking multiple types of attacks one on top of another. Once they get even a tiny foothold into an organization – compromising one account or one system – they then use that as a starting point for more encompassing and destructive forays.

These factors are making it ever more challenging to protect corporate systems and data. To defend against these multi-faceted, multi-pronged attacks, organizations require an aggressive strategy that includes high-level support from management, an appropriate budget, multiple forms of protection, and continued user education.

Scope of the Problem

Cybersecurity is no longer just an IT issue. It's a business issue that is getting attention at the highest levels in many organizations.

The extensive media coverage of high-profile breaches over the last several years at Target, Home Depot, Sony Pictures, JPMorgan Chase, Anthem, and others has spurred board members to care more about IT risk than ever before. Corporate boards are on high alert and cybersecurity is the foremost issue currently on directors' minds now because it's tied into the risk structure of the organization.[i]

Numerous studies peg the scope of the problem.

In 2014, 42.8 million security incidents were detected, a 48 percent increase over the previous year, according to PricewaterhouseCoopers. The average size of the financial hits attributed to those incidents was $2.7 million, and the number of organizations reporting incident-related losses of more than $20 million increased 92 percent last year, PwC reports.

Individuals are also being targeted. The government's Internet Crime Complaint Center (IC3), said in its annual report that the number of complaints about scammers using social media to perpetrate frauds is also on the rise. Overall, online scams reported to the government cost Americans $800 million last year alone, according to IC3.[ii]

In the past, such personal attacks were not of concern to corporate IT and security staff. But with the blurring of work and personal use of company computers and the broad adoption of bring-your-own-device (BYOD) policies in most companies, such attacks can do double duty and provide access to corporate resources as well.

New Attack Methods Require New Thinking

A number of factors are making protection of corporate resources more challenging for IT managers and security administrators. These factors include:

Well-Known Attacks Are Still Commonplace: Attackers continue to leverage well-known techniques to successfully compromise systems and networks. Many vulnerabilities exploited in 2014 took advantage of code written many years ago and were aimed at commonly installed software including Microsoft Windows, Adobe Reader and Acrobat, and Oracle Java, according to the 2015 edition of HP's annual security research Cyber Risk Report.[iii]

In fact, the HP report found that exploitations of widely deployed client-side and server-side applications are still commonplace. While newer exploits may have garnered more attention in the recent press, vulnerabilities discovered in the past continue to pose a significant threat to enterprise security if unpatched systems are in use within an organization.

The Rise of "Do-It-Yourself" IT: For years, employees and departments have used non-sanctioned applications and services to get their work done. For example, in most companies it was quite common for employees to use web-based email and instant messaging accounts for both personal business and for work.

Today, cloud services and mobile applications are the norm. Workers and business units often use file-sharing services to collaborate with people inside and outside of the company. And users frequently download applications to mobile devices that are used for both their private and professional lives.

Use of these services and applications can lead to security problems. Protected information can be leaked. Unmanaged applications can introduce exploitable vulnerabilities.

Users seem to know that there are potential problems working this way, yet many continue to do so. One study found that even though 66 percent of workers *acknowledge* that using a new application without the IT department's consent is a serious cybersecurity risk to the business, more than a quarter (26 percent) still admitted to *doing* so.[iv]

Phishing Attacks Remain Effective: Multiple studies have found varying degrees of success (all of which are frightening) for phishing aimed at corporate users.

In particular, hackers now target corporate users with attachments in high-volume campaigns, piggybacking on legitimate messages like email newsletters and opt-in marketing emails.[v] As a result, users receive many malicious emails that they do not recognize as threatening.

Most troubling, about 25 percent of those who received a phishing email were likely to open it.[vi] In many cases, it took less than two minutes for freshly sent phishing emails to catch their first victim. And half of the victims had clicked on the message within the first hour of it being sent.

Another study found that attackers typically lure two or three users into clicking on malicious content immediately. Unfortunately, it typically takes companies far longer to notice they have been compromised.

Multi-stage Attacks Are More Common: Several of the large breaches over the last year have been the result of patient hackers. Once gaining access to a system or user account, they can build on that access and develop a much larger attack from within the organization.

With some compound attacks, hackers infiltrate a third-party (a supply chain partner, insurance processor, or credit card clearing service, for example) and then bide their time posing as an authorized user, all the while collecting information that can either be used in a more targeted attack or to steal information. This was the case with the massive breach at Target.[vii]

Newer Technologies Introduce New Avenues of Attack: This past year saw a rise in already prevalent mobile-malware levels, according to the 2015 HP Cyber Risk Report. Even though the first malware for mobile devices was discovered a decade ago, 2014 was the year in which mobile malware became a viable corporate threat.

Additionally, as a variety of physical devices become connected through the Internet of Things (IoT), the diverse nature of these technologies opens up new attack possibilities and exposes organizations to new vulnerabilities.

Teaming with a Technology Partner

Security threats are growing in complexity. Hackers and cyberthieves are using new techniques and more sophisticated attacks to compromise systems and steal data. Security solutions must be as agile as the attackers in changing their tactics. They must be able to locate intruders as quickly as possible. They must be able to receive updated security intelligence. And they must be "smart" security solutions capable of communication and correlation.

These are all areas where HP can help.

HP offers enterprise security software and solutions that provide a proactive approach to security. The solutions integrate information correlation, application analysis, and network-level defense. Offerings include:

Security Research: To understand the nature of today's evolving threats, HP offers innovative vulnerability research delivered as actionable security intelligence.

Network Security: HP TippingPoint offers a wide range of network security solutions that are easy to use, configure, and install while providing real-time network protection, visibility, and centralized management and analytics. Solutions include a next-generation firewall, intrusion prevention system, network security management, advanced threat appliance, and threat intelligence. The solutions protect virtual and physical networks, applications, and data against sophisticated threats including known, unknown, and zero-day vulnerabilities.

Security Information and Event Management (SIEM): ArcSight SIEM is a comprehensive SIEM solution that enables cost-effective compliance and provides advanced security analytics to identify threats and manage risk, so companies can protect their business. The solution offers real-time threat detection, simplified compliance, application monitoring, and it helps companies manage risk and detect insider threats.

Application Security: HP Fortify offers application security testing and management solutions, available on-premise or on-demand. The products within the solution line can help companies secure their software applications including legacy, mobile, third-party, and open source applications.

Mobile Application Security: HP Fortify helps secure mobile applications before deployment. The solution offers comprehensive testing and malware discovery and provides end-to-end security of mobile applications. The solution offers flexible application security testing that includes both static code analysis and regularly scheduled dynamic scans that do not interfere with today's fast-paced software development cycles.

Data Security and Encryption: HP Atalla and HP Security Voltage solutions help protect, manage, and control access to sensitive data. Atalla solutions provide continuous protection through classification, data encryption, and key management, offering flexibility, reliability, and manageability. HP Security Voltage makes encryption and tokenization of data simple for even the most complex use cases.

Conclusion

The cybersecurity challenge will continue to grow as threats evolve and thieves see greater value in the information they can steal. Protecting against today's (and tomorrow's) attacks requires real-time information about threats and security solutions that work together to detect, prevent, and combat complex attacks of the day.

For more information on how HP can help your organization implement a successful security program, fix the gaps in your environment, or aid you in recovery from a breach, click here.

---

[i] http://www.networkworld.com/article/2914740/network-security/boards-are-on-high-alert-over-security-threats.html

[ii] http://www.nydailynews.com/life-style/online-fraudsters-swindled-800-million-year-article-1.2229449

[iii] http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/index.html

[iv] http://www.eweek.com/small-business/employees-engaging-in-risky-cyber-security-activities.html

[v] http://www.cioinsight.com/security/slideshows/hackers-target-middle-managers-and-corporate-emails.html

[vi] http://www.bbc.com/news/technology-32285433

[vii] http://www.technewsworld.com/story/79908.html