Report

Cyber Risk Report 2015

Executive summary

The cyber landscape

The 2015 edition of HP's annual security research Cyber Risk Report details a threat landscape still heavily populated by old problems and known issues, even as the pace of the security world quickens. The environment is one in which well-known attacks and misconfigurations exist side-by-side with mobile malware and connected devices (Internet of Things [IoT]) that remain largely unsecured. As the global economy continues its recovery, enterprises have continued to find inexpensive access to capital; unfortunately, network attackers did as well, some of whom launched remarkably determined and formidable attacks over the course of the year.

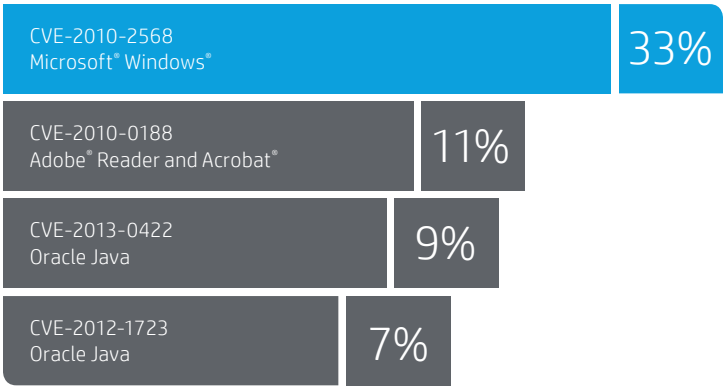
The Cyber Risk Report 2015, drawn from innovative work by HP Security Research (HPSR), covers multiple focus areas. It examines both the nature of currently prevalent vulnerabilities that leave organizations open to risk, and how adversaries take advantage of those vulnerabilities. The report challenges the reader to rethink how and where their organization can be attacked, as it is no longer a question of "if" but "when". This intelligence can be used to better allocate security funds and personnel resources to counter the threats.

Some of the key findings in the 2015 report are:

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 back; some are even decades old (Figure 1). Adversaries continue to leverage these classic avenues for attack.

Figure 1. Top four exploits discovered by HPSR in 2014

Top exploits noted in 2014



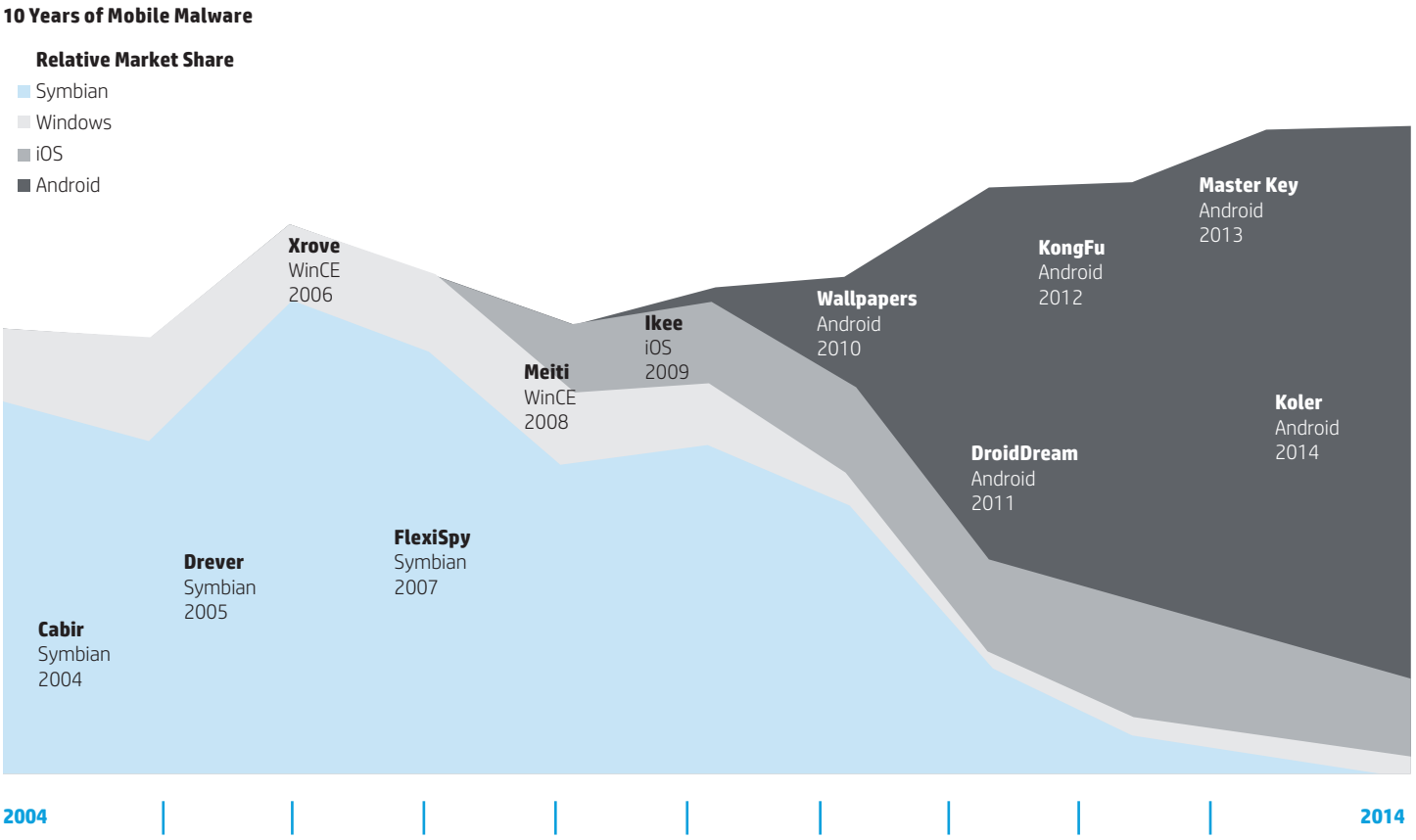
Exploitations of widely deployed client-side and server-side applications are still commonplace. These attacks are even more prevalent in poorly coded middleware applications, such as software as a service (SaaS). While newer exploits may have garnered more attention in the press, attacks from years gone by still pose a significant threat to enterprise security. Network defenders should employ a comprehensive patching strategy to ensure systems are up to date with the latest security protections to reduce the likelihood of these attacks succeeding.

Misconfigurations are still a problem: The HP Cyber Risk Report 2013 (published in early 2014) documented that a large percentage of vulnerabilities reported were related to server misconfiguration. The trend continued in 2014, with misconfigurations being the number-one issue across all analyzed applications. Our findings show access to unnecessary files and directories dominates the list of misconfiguration-related issues.

The information disclosed to attackers through these misconfigurations provides additional avenues of attack and allows attackers the knowledge needed to ensure their other methods of attack succeed. Regular penetration testing and verification of configurations by internal and external entities can identify configuration errors before attackers exploit them.

Newer technologies introduce new avenues of attack: As new technologies are introduced into the computing ecosystem, they bring with them new attack surfaces and security challenges. This past year saw a rise in already prevalent mobile-malware levels. Even though the first malware for mobile devices was discovered a decade ago, 2014 was the year in which mobile malware stopped being considered just a novelty (Figure 2). Connecting existing technologies to the Internet also bring a new set of exposures. Point-of-sale (PoS) systems were a primary target of multiple pieces of malware in 2014. As physical devices become connected through the Internet of Things (IoT)—a paradigm that brings ubiquitous computing and its security implications closer to the average person—the diverse nature of these technologies gave rise to concerns regarding security and privacy. To help protect against new avenues of attack, enterprises should understand and know how to mitigate the risk being introduced to a network prior to the adoption of new technologies.

Figure 2. Ten years of mobile malware; as market share changes, so do malware targets



Determined adversaries are proliferating: Attackers use both old and new vulnerabilities to penetrate all traditional levels of defenses. They maintain access to victim systems by choosing attack tools that will not show on the radar of antimalware and other defense technologies. In some cases, these attacks are perpetrated by actors representing nation-states, or are at least launched in support of nation-states. In addition to the nation-states traditionally associated with this type of activity, newer actors such as Turkey were observed in 2014. Network defenders should understand how events on the global stage impact the risk to systems and networks.

Cyber-security legislation is on the horizon: Activity in European and US courts linked information security and data privacy more closely than ever. As legislative and regulatory bodies consider how to raise the general level of security in the public and private spheres, there was an avalanche of reported retail breaches in 2014. This spurred increased concern over how individuals and corporations are affected once private data is exfiltrated and misused. The high-profile Target and Sony compromises bookended those conversations during the period of this report. Companies should be aware that new legislation and regulation will affect how they monitor their assets and report on potential incidents.

Secure coding continues to pose challenges: The primary causes of commonly exploited software vulnerabilities are consistently defects, bugs, and logic flaws. Cyber security research professionals have discovered that most vulnerabilities stem from a relatively small number of common software programming errors. Much has been written to guide software developers on how to integrate best secure-coding practices into their daily development work. Despite all of this knowledge, we continue to see old and new vulnerabilities in software. These are, in turn, swiftly exploited by attackers. It may be challenging, but it is long past the time that software development be synonymous with secure software development. While it may never be possible to eliminate all code defects, a properly implemented secure development process can lessen the impact and frequency of such bugs.

Complementary protection technologies fill out coverage: In May 2014, a senior executive of a prominent anti-malware vendor declared antivirus dead. The industry responded with a resounding "no, it is not." Both are right. Studies show that antimalware software catches only about half of all cyberattacks—a truly abysmal rate. In our review of the 2014 threat landscape, we find that enterprises most successful in securing their environment employ complementary protection technologies. These technologies work best when paired with a mentality that assumes a breach will occur, instead of one that only aims to prevent intrusions and compromise. By using all tools available and not relying on a single product or service, defenders place themselves in a better position to prevent, detect, and recover from attacks.

Actions and reactions

In the face of increasing threats, software vendors continue to make it more difficult for attackers with the implementation of security mitigations. However, these mitigations are not enough when they are built on inherently vulnerable legacy code.

On multiple occasions in 2014, high-profile vulnerabilities were discovered that left enterprises scrambling to deploy patches and clean up compromised machines. Watching the industry respond to the Heartbleed vulnerability highlighted how unprepared we were for this type of event. Due to the severity and active exploitation of the vulnerability, corporations were forced to respond quickly, and to patch servers that were not routinely patched. The issue existed in an application library that did not have a clear update path, further complicating efforts; enterprises did not have a solid understanding of which applications were using this library and where it was located inside their networks.

Discovery of information disclosure vulnerabilities such as Heartbleed illustrates why information disclosure vulnerabilities are highly valued by the exploitation community. Heartbleed was a clear demonstration of a highly controllable information disclosure vulnerability due to a buffer over-read. Vulnerabilities found in legacy code were also a significant factor in 2014. As the quality of exploits continue to improve, they reveal a deep understanding of the nature of the vulnerability and the internals of the target applications.

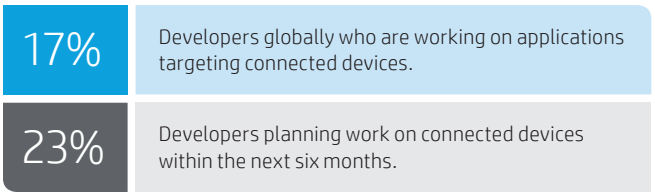
Our research throughout 2014 (covered in multiple Security Briefings throughout the year and summarized in the Risk Report) indicated that intellectual property continues to be targeted by Chinese interests, in particular. Other nations also pose significant threats in our globally connected world. North Korea has continued its tradition of asymmetric warfare in the age of the Internet, with a remarkable commitment to developing cyberwarfare capabilities even as it copes with aging infrastructure. Iran continues to develop its cyber capabilities and views hacker groups as a force multiplier to be used to target Western entities, particularly corporations and government entities. The Turkish hacker underground, among others in the region, continues to flourish. We expect escalations in this area to continue.

2014 was also a significant year for mobile malware, not least because it finally entered the general consciousness as a genuine threat. While the majority of Android malware discovered in 2014 was found outside of the Google™ Play market, there have been instances when malware was placed there by maliciously created developer accounts. Ransomware was also a key theme throughout the past year as attackers continued to exploit a business model in which users' data is held for ransom by malware, often using asymmetric encryption algorithms. Perhaps the most notable ransomware of the year was CryptoLocker, which appeared at the end of 2013 and caused significant damage prior to an FBI-led takedown. Despite this action, the business model of holding users' data for ransom through malware using encryption has spurred a number of copycats, with CryptoWall being the most prevalent.

The threat from malware continues to rise as the attacks on Target and Home Depot highlighted the risk from PoS devices. Our investigations uncovered ongoing development, increasing sophistication, and a divergent code base in current PoS malware. Significantly, these malicious programs were built by people with specific knowledge of the targeted environments. This highlights the planned nature of these attacks and reminds us that attackers are increasingly playing the long game. Enterprises must be able to monitor their networks and systems in a manner that allows them to discover malicious intelligence gathering and reconnaissance activities that may herald an approaching attack.

Figure 3. Developing for the Internet of Things (from Evans Data survey of over 1400 developers, 2014)

Developing for the Internet of Things



There appears to be growing consumer awareness about privacy issues at the connected-devices (IoT) level, whether that's concern over security and privacy risks posed by basic connected devices or something broader. The IoT is much more than a buzzword—it's a paradigm that brings ubiquitous computing and its security implications closer to the average person (Figure 3).

Attacks often involve various layers of the device infrastructure. This could include applications running on smartphones or tablets, and on cloud services as well as the firmware and application layers residing on the host processor. Various vectors of propagation can also be used, including compromised update files and exploited network and host processor communication layer vulnerabilities, as well as possible vulnerabilities in cloud service infrastructures and smart device applications.

While the threat from the Internet itself exists on a global scale, a worldwide network of security researchers stand ready to help the software industry secure its code. HPSR's Zero Day Initiative (ZDI) is the world's largest vendor-agnostic bug bounty program, with almost ten years' experience coordinating vulnerability disclosure. At of the end of 2014, it had grown to a network of over 3,000 independent researchers working to expose and remediate weaknesses in the world's most popular software and platforms. Over the past two years, researchers representing several new regions (including Germany, South Korea, China, and the Russian Federation) emerged, submitting high-quality technical analysis (Figure 4). Researchers in these countries are not only focusing on vulnerability discovery but also on innovative exploitation techniques.

Figure 4. External ZDI researchers report in from all hemispheres

Researcher coverage map

Conclusion

In a world where more and more people and devices connect to the Internet, greater focus must be placed on security and privacy. The past year saw the manifestation of several vulnerabilities that gathered a storm of media attention. Network defenders should use the information in the Cyber Risk Report 2015 to better understand the threat landscape, and to best deploy resources to minimize security risk.

Looking ahead, technology will continue to enhance our world in numerous ways, and with those benefits comes the challenge of maintaining security and privacy throughout our digital lives. However, with increased collaboration and a thorough understanding of the imminent threats, we can continue to increase the both physical and intellectual costs an attacker must accept to successfully exploit a system.

For more information on how HP can help your organization to implement a successful security program, fix the gaps in your environment, or aid you in recovery from a breach, visit hp.com/go/hpsr.

Learn more at
hp.com/go/hpsr

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA5-0920ENW, February 2015, Rev. 1