Global Knowledge®

Expert Reference Series of White Papers

Zero Day Exploits

Zero Day Exploits

James Michael Stewart, CISSP, ISSAP, SSCP, MCT, CEI, CEH, TICSA, CIW SA, Security+, MCSE+ Security Windows 2000, MCSA Windows Server 2003, MCDST, MCSE NT & W2K, MCP+I, Network+, and iNet+

Introduction

For several years most news articles about a computer, network, or Internet compromise has mentioned the phrase "zero day exploit" or "zero day attack," but rarely do these articles define what this is. A zero day exploit is any attack that was previously unknown to the target or security experts in general. Many believe that the term refers to attacks that were just released into the wild or developed by hackers in the current calendar day. This is generally not the case. The "zero day" component of the term refers to the lack of prior knowledge about the attack. That the victim has zero day's notice of an attack. The main feature of a zero day attack is that since it is an unknown attack, there are no specific defenses or filters for it. Thus, a wide number of targets are vulnerable to the exploit.

Zero day attacks have been discovered recently that are potentially at least seven years old. I'm specifically referencing the Flame or Skywiper discovered in early 2012. However, it is much more common for zero day exploits to have existed for months before discovery. Again, whenever you see the phrase zero-day exploits, keep in mind it just means a newly discovered, previously unknown attack, for which there is no defense at the time of discovery.

Once security researchers become aware of a new zero day exploit, they quickly develop detection and prevention measures in the process of their forensic analysis. These new detection and defense options are distributed and shared with the security community. Once organizations and individuals install updates or make configuration changes, they can be assured that their risk of compromise from that specific attack as been significantly reduced or eliminated. Once detection and defense is possible, then an exploit is not longer considered a zero day as there is now notification of its existence.

A search using the term "zero day" reveals numerous recent compromises and exploitations. In fact, this should be obvious as new attacks are by nature zero day. But since we often label the attack as a zero day exploit at the time of discovery and for a moderate period of time afterwards, that label is a useful term for tracking down the appearance of historical attacks.

In 2012, there have been several fairly significant discoveries of exploits and attacks that were labeled as zero day. These include:

- Flame/Skywiper is used for targeted cyber espionage against Middle Eastern countries
- An IE exploit that allows hackers to remotely install malware onto Windows systems running IE 7, 8, or 9
- A Java exploit that allows hackers to remotely install malware onto system running Java 5, 6, or 7

Exploit and Vulnerability Awareness Sites

To learn of more examples of zero day exploit discoveries, I recommend visiting a few sites on a regular basis.

- exploit-db.com
- cve.mitre.org
- us-cert.gov

Exploit Database (exploit-db.com) is a community driven notification site about newly discovered zero day attacks. What I like about this site, and which is unique to this site, is that in addition to disclosing the attack, it also provides access to the exploit itself. Most other vulnerability and exploit research sites do not provide you the actual attack code. I think this is an overlooked opportunity. When you have access to the exploit code, you can develop your own filter for the attack. You don't need to wait for a vendor to release a patch or a security vendor to update their tool's database; instead, you can add in your own detection filter and stop the attack.

The MITRE organization's Common Vulnerability and Exploit database (cve.mitre.org) is one of the better known collections of attack and compromise information and research. Perusing their collection will help you stay aware of recently discovered exploits and steps you can take to avoid compromise and reduce your vulnerability.

The US Cert site (us-cert.gov) is a US government-managed site with emphasis on providing security and exploit information to protect the nation's IT. Their mission is to provide information, promote awareness, and assist in protection preparations against all forms of compromise and abuse of computers and networking. I recommend signing up for their weekly bulletin which summaries the previous week's newly discovered exploits and vulnerabilities, but also provides references back to their main site as well as the CVE from MITRE.

If you visit these exploit and vulnerability awareness sites, you will notice that new zero day exploits are uncovered on a fairly consistent basis - daily. Malicious hackers across the globe (as well as security experts we perceive as being good guys) are writing new attack code with new exploits in an attempt to develop the next best computer weapon. They seek to compromise the most systems in the shortest amount of time, while gaining the most control, learning the most information, all while going without detection for as long as possible. It is a race and a battle of intelligence and creativity.

How Do Hackers Uncover New Vulnerabilities and Weaknesses?

A common question I hear from students is, "How does a hacking programmer learn about a flaw or vulnerability in the first place?" There are many ways by which new weaknesses or vulnerabilities are uncovered, but three are the most common: source code review, patch dissection, and fuzzy testing.

1. **Source code review** is the process of looking through the original code or decompiled code of the target software of choice. If the hacker can obtain the original source code of a specific software product, he often has a good chance of reading through the code and noticing a typo, error, logical issue, design flaw, etc. If only the final compiled software is available, decompiles can create source code that may not be as elegant

as the original in terms of layout and variable labeling (not to mention it is unable to recreate or extract any embedded comments from the original source code), but which can still reveal errors and flaws to a skilled programmer.

2. **Patch dissection** is the process of examining the parts of a target application that are patched or altered when a software update is applied. By monitoring the changes made by patches, hackers discover issues in code that they were previously unaware of. Generally, once a hacking programmer is aware of a software bug or error, an exploit can be crafted to take advantage of that error in a matter of hours.

   Even though a vendor now offers a fix for the vulnerability, most companies and individuals who use the software will not even be aware of the patch for days or more, and there may be delays in getting patches installed. Companies often have a patch management procedure that only operates once a week or once a month. A patch management procedure typically involves testing new code on isolated lab systems to determine the effects the update would have on the production environment. Only after the consequences of new code are understood, it is considered for rollout. If the ramifications of new updates are too impactful on production, the installation may be delayed or put off indefinitely.

3. **Fuzzy testing** is a form of software stress testing that sends random, invalid, and unexpected data to a target application. The purpose is to test the reaction and response of the software to a wide range of unexpected input. If abnormalities are detected or errors are generated, the findings of the fuzzy tool can be used to develop new exploit code. Fuzzy tools could be run against a target software product for months without finding a single issue. However, when issues are discovered (which occurs much more often than we might wish), new exploits are crafted taking advantage of those newly discovered vulnerabilities.

Zero-Day Exploits: Defining What We Don't Know

Zero day exploits are an area of serious concern. However, it is one of the more difficult issues to address. Future Zero day exploits are not just unknowns; they are unknown unknowns. While we have the vague understanding and expectation that there will be up and coming attacks, we don't know:

- When they will occur
- If vulnerabilities are already being exploited that we have yet to detect
- When a new vulnerability will be discovered
- What OS, platform, or application will be the target;
- Whether the attack will be local or remote; and
- The extent or breadth of the attack (i.e., is it just able to gather data, able to plant data or code, or grant full remote backdoor access).

Best Defense: Be Prepared

Generally, the best defense against the future unknown zero-day attacks is to be prepared: don't expect to always be in a safe and stable operating environment. Assume the worst will happen at some point and plan for recovery. This should include redundancy planning, avoiding single points of failure, implementing backup and fail-

over options, and performing simulation and testing of recovery procedures. I also suggest implementing a more detailed and exhaustive logging, monitoring, and auditing scheme. This should include not only long-term archival logs but also real-time analysis of events using intrusion detection and prevention tools. Train personnel to avoid risky behavior, to be skeptical of others, and report anything and everything suspicious to the security team.

Conclusion

With these efforts an organization increases the chance of noticing a new abnormal occurrence within the infrastructure that could be a symptom of a zero day attack. All zero day attacks are discovered by someone noticing something odd or out of place, then being curious enough to investigate further. By having business continuity and disaster recovery plans in place, if you discover or uncover a zero day attack (or vulnerability) too late to prevent a compromise, you are in the best position possible to implement a successful repair and recovery.

When it comes to zero day attacks, your best option is to be prepared and be on the lookout.

Learn More

To learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge, Global Knowledge suggests the following courses:

- ADTRAN Technical Support Professional for Unified Threat Management (ATSP/UTM) (1600NUTME)
- Cybersecurity Foundations
- Foundstone Ultimate Hacking
- Foundstone Forensics & Incident Response
- Cyber Security Compliance & Mobility Course (CSCMC)

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

James Michael Stewart has been working with computers and technology for over 25 years. His work focuses on security, certification, and various operating systems. Recently, Michael has been teaching job skill and certification courses, such as CISSP, CEH, and Security+. He is the primary author on the CISSP Study Guide 4th Edition and the Security+ 2008 Review Guide. Michael has also contributed to many other CISSP- and Security+-focused materials, including exam preparation guides, practice exams, DVD video instruction, and courseware.

In addition, Michael has co-authored numerous books on other security and Microsoft certification, and administration topics. He has developed certification courseware and training materials and has presented these materials in the classroom. Michael holds the following certifications: CISSP, ISSAP, SSCP, MCT, CEI, CEH, TICSA, CIW SA, Security+, MCSE+ Security Windows 2000, MCSA Windows Server 2003, MCDST, MCSE NT & W2K, MCP+I, Network+, and iNet+. Michael graduated in 1992 from the University of Texas at Austin with a bachelor's degree in Philosophy. Despite his degree, his computer knowledge is self-acquired, based on seat-of-the-pants,