ARS Technica, New Microsoft security defense to take aim at potent exploit technique

Microsoft engineers plan to adopt new security defenses that will help their software better withstand a powerful exploitation technique hackers are increasingly using to install malware on end users' computers.

The technique, known as ROP (return oriented programming), is a regular staple of attacks used at the annual Pwn2Own hacker contest. It's also found in real-world attacks that install malicious software by exploiting garden-variety bugs in widely used pieces of software. It works by rearranging benign pieces of code already present in memory to form a malicious payload. Ironically, the popularity of ROP grew because of its ability to bypass another security mitigation known as data execution prevention, which has been added to software from Microsoft, Apple, and others over the past decade.

Microsoft unveiled the anti-ROP defenses on Thursday morning in a blog post announcing three finalists to its own competition. Microsoft's initiative will award more than $260,000 in cash and prizes for the development of new security protections to make its software more resistant to hack attacks. The BlueHat contest was unveiled at last year's Black Hat security conference in Las Vegas, and the grand prize winner will be announced next month. Microsoft hasn't said when it expects the technologies to go live, or exactly which products will use them.

The three finalists include Jared DeMott, a security researcher who submitted an entry called "/ROP." It checks the security of target addresses of return instructions, which are regularly exploited in ROP attacks. Ivan Fratric, who earned a PhD in computer science and is a researcher at the University of Zagreb, was named for his entry of ROPGuard. This defines a set of checks that can be used to detect when certain functions are being used in malicious ways. Columbia University PhD student Vasilis Pappas proposed a ROP mitigation called kBouncer, which detects abnormal control transfers using common hardware features. Microsoft has additional details of the three finalists here.

The winner will receive a grand prize of $200,000, while the first runner-up will take $50,000 and the second runner-up will get a MSDN Universal subscription worth $10,000. The program is aimed at helping develop novel defense mechanisms that can block entire classes of software attacks.

Over the past decade, developers from Microsoft, Apple, Google, Adobe, and elsewhere have fortified their code with a growing number of mitigations. They include address space layout randomization, which randomizes memory locations where code is loaded. The mitigations also include data execution prevention—which prevents data loaded into memory from being executed—and sandboxing. That confines Web content and other untrusted data in a closely guarded perimeter, separate from sensitive operating-system functions such as writing files.

.