Bromium Labs says it bypassed protections in Microsoft's EMET

February 25 2014, by Nancy Owano

Good news: Microsoft's Enhanced Mitigation Experience Toolkit (EMET) is, as its title suggests, an anti-exploit tool and a free download, provided by Microsoft, to enhance the security of an endpoint PC. Bromium Labs news: Its research team bypassed all protections.

Bromium studied EMET 4.0 and 4.1. The Cupertino, California-based security company presented its findings Monday in the Bromium Labs blog and in a technical whitepaper, "Bypassing EMET 4.1." In deciding to take up EMET, Jared DeMott, security researcher and author of the paper, noted how good EMET was at stopping pre-existing memory corruption attacks, a type of exploit, but "we wondered: is it possible for a slightly more technical attacker to bypass the protections offered in

EMET?"

They found ways to bypass all EMET protections. They said they used a typical modern computer, and focused on "32-bit userland processes running on 64-bit Windows 7." They said they successfully bypassed EMET's protections in example code and with a real-world browser exploit. A conclusion that the tool would not be effective against determined attackers needs to place an accent on the word *determined*. DeMott wrote in the paper that, "as seen in our research, deploying EMET does mean attackers have to work a little bit harder; payloads need to be customized, and EMET bypass research needs to be conducted." In gaining perspective, DeMott added, "The question really is not can EMET be bypassed. Rather, does EMET sufficiently raise the cost of exploitation? The answer to that is likely dependent upon the value of the data being protected."

The whitepaper was provided to Microsoft before speaking about the research findings publicly, according to DeMott. Meanwhile, Microsoft on Tuesday issued news and offer of download of its EMET 5.0 Technical Preview. The announcement from the "EMET team" said, "Today, we are thrilled to announce a preview release of the next version of the Enhanced Mitigation Experience Toolkit, better known as EMET." The Technical Preview, said Microsoft, introduces new features and enhancements expected to be components of the final EMET 5.0 release.

"We are releasing this technical preview to gather customer feedback about the new features and enhancements. Your feedback will affect the final EMET 5.0 technical implementation." The new features are the Attack Surface Reduction (ASR) and the Export Address Table Filtering Plus (EAF+).

Microsoft included Bromium Labs in its acknowledgments. "We'd like

to thank Spencer J. McIntyre from SecureState, Jared DeMott from Bromium Labs, along with Peleus Uhley and Ashutosh Mehra from the Adobe Security team for their collaboration on the EMET 5.0 Technical Preview."

More information: bromiumlabs.files.wordpress.co … passing-emet-4-1.pdf
labs.bromium.com/2014/02/24/bypassing-emet-4-1/
blogs.technet.com/b/srd/archiv … chnical-preview.aspx

Citation: Bromium Labs says it bypassed protections in Microsoft's EMET (2014, February 25) retrieved 28 April 2024 from
https://techxplore.com/news/2014-02-bromium-labs-bypassed-microsoft-emet.html