

Project:Rosenbrdige - 'Hardware Backdoors in x86 CPUs'

[Originalartikel](#)

[Backup](#)

<html> <p><a href=„<https://github.com/xoreaxeaxeax/rosenbridge>“><img src=„<https://cdn-blog.adafruit.com/uploads/2018/08/rosenbridge.gif>“ alt=„“ class=„img-responsive“/></p> <p>In this 50-minute presentation (video below) from <a href=„<https://www.blackhat.com/us-18/briefings/schedule/#god-mode-unlocked---hardware-backdoor-s-in-x86-cpus-10194>“ rel=„noopener“ target=„_blank“>black hat USA 2018, Christopher Domas discusses hardware backdoors in “some” x86 processors 😮 with special attention given to VIA C3 CPUs.</p> <p>Thankfully he’s open-sourced all his research, including his <a href=„<https://i.blackhat.com/us-18/Thu-August-9/us-18-Domas-God-Mode-Unlocked-Hardware-Backdoors-In-x86-CPUs.pdf>“ rel=„noopener“ target=„_blank“>presentation slides, <a href=„<https://i.blackhat.com/us-18/Thu-August-9/us-18-Domas-God-Mode-Unlocked-Hardware-Backdoors-In-x86-CPUs-wp.pdf>“ rel=„noopener“ target=„_blank“>white paper discussing the topic, and crucially a <a href=„<https://github.com/xoreaxeaxeax/rosenbridge>“ rel=„noopener“ target=„_blank“>GitHub repo of the tools used to test his theories.</p> <p>From the white paper,</p> <blockquote> <p>Abstract—As the complexity of x86 processors grows unbounded, the realities of the hidden and unexpected behaviors of these chips become apparent. While micro-architectural vulnerabilities such as speculative execution side channels are unsettling, more powerful, unknown capabilities remain buried deeper still. Here, we finally demonstrate what everyone has long feared but never proven: there are hardware backdoors in some x86 processors, and they’re buried deeper than we ever imagined possible.</p> </blockquote> <p><img src=„<https://cdn-blog.adafruit.com/uploads/2018/08/x86.png>“ alt=„“ class=„img-responsive“ srcset=„<https://cdn-blog.adafruit.com/uploads/2018/08/x86.png> 1371w, <https://cdn-blog.adafruit.com/uploads/2018/08/x86-150x114.png> 150w, <https://cdn-blog.adafruit.com/uploads/2018/08/x86-300x228.png> 300w, <https://cdn-blog.adafruit.com/uploads/2018/08/x86-768x585.png> 768w, <https://cdn-blog.adafruit.com/uploads/2018/08/x86-600x457.png> 600w, <https://cdn-blog.adafruit.com/uploads/2018/08/x86-574x437.png> 574w“ sizes=„(max-width: 1371px) 100vw, 1371px“/></p> <p><img src=„<https://cdn-blog.adafruit.com/uploads/2018/08/msr.png>“ alt=„“ class=„img-responsive“ srcset=„<https://cdn-blog.adafruit.com/uploads/2018/08/msr.png> 1488w, <https://cdn-blog.adafruit.com/uploads/2018/08/msr-150x100.png> 150w, <https://cdn-blog.adafruit.com/uploads/2018/08/msr-300x201.png> 300w, <https://cdn-blog.adafruit.com/uploads/2018/08/msr-768x514.png> 768w, <https://cdn-blog.adafruit.com/uploads/2018/08/msr-600x401.png> 600w, <https://cdn-blog.adafruit.com/uploads/2018/08/msr-654x437.png> 654w“ sizes=„(max-width: 1488px) 100vw, 1488px“/></p> <p>Watch:</p> <p><iframe width=„500“ height=„281“ src=„https://www.youtube.com/embed/_eSAF_qT_FY?feature=oembed“ frameborder=„0“ allow=„autoplay; encrypted-media“ allowfullscreen=„allowfullscreen“>[embedded content]</iframe></p> <div class=„ctx-subscribe-container ctx-personalization-container ctx_default_placement ctx-clearfix“/> <div class=„ctx-social-container ctx_default_placement ctx-clearfix“/> <div class=„ctx-module-container ctx_default_placement ctx-clearfix“/> </html>

From:

<https://schnipsl.qgelm.de/> - Qgelm

Permanent link:

https://schnipsl.qgelm.de/doku.php?id=wallabag:project_rosenbrdige--hardware-backdoors-in-x86-cpus

Last update: **2021/12/06 15:24**

