



black hat[®]

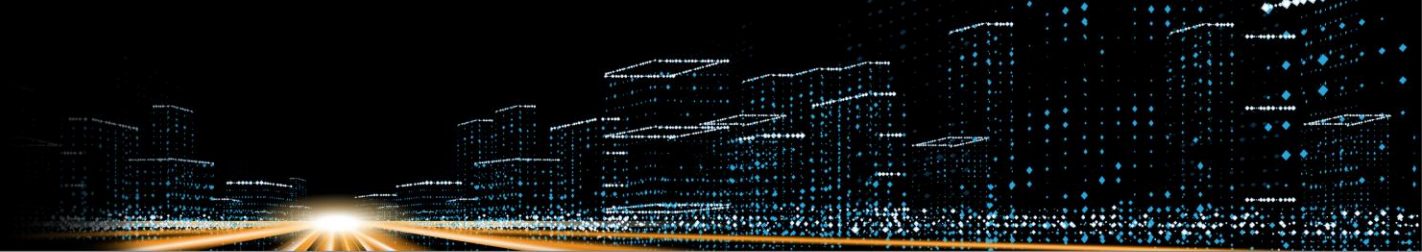
ARSENAL

MARCH 26-29, 2019

MARINA BAY SANDS / SINGAPORE

#BHASIA

 @BLACKHATEVENTS



ProcJack + Clove: Non-Invasive Code Instrumentation

Toshihito Kikuchi



About Me & Disclaimer

- Toshihito Kikuchi
Twitter [@msmanix](https://twitter.com/msmanix) | GitHub [@msmania](https://github.com/msmania)
- Browser engineer. Not a security guy.
- This is my personal project. Any statement is not related to my employer.
- The behavior of injected processes is completely out of support.
(i.e. This may not work on a future platform.)
- Do not run this tool on any production environments or any that might be used by another person.



ProcJack + Clove: Non-Invasive Code Instrumentation

- What can be done:
 - Inject your code into arbitrary places including the middle of a function (There are some limitations)
 - Without modifying the target program
- Leveraging the existing techniques:
 - Advanced version of Reflective DLL injection (= ProcJack)
 - Trigger Microsoft Detours as an injectee DLL (= Clove)



ProcJack + Clove: Non-Invasive Code Instrumentation

- Available on GitHub (PR/Issue is always welcome 😊):
 - ProcJack (Clove is included as a part of this repo):
<https://github.com/msmania/procjack>
 - More details about Clove:
<https://github.com/msmania/procjack/blob/master/clove/Intro.pdf>



Demo 1: Use ProcJack against a guarded process on Windows 10

- How to inject the code into Microsoft Edge or Google Chrome?
- This demonstrates:
 - Disable Code Integrity Guard (= CIG) of Edge and Chrome
 - Disable Arbitrary Code Guard (= ACG) of Edge
- To learn more about CIG/ACG:
 - <https://blogs.windows.com/msedgedev/2017/02/23/mitigating-arbitrary-native-code-execution/>
 - https://cansecwest.com/slides/2017/CSW2017_Weston-Miller_Mitigating_Native_Remote_Code_Execution.pdf



Demo 2: Find a bottleneck of Chrome's layout code

- Where is the slowest operation in `chrome_child!blink::Document::UpdateStyleAndLayoutTree?`
- This demonstrates:
 - Hook an instruction in the middle of a function
 - Multiple injected codes can interact with one another



Demo 3: See the heap allocation pattern of MemGC and BlinkGC

- Let's compare Microsoft Edge with Google Chrome
 - Edge's heap: MemGC
Monitor `edgehtml!MemoryProtection::HeapAllocClear<1>`
 - Blink's heap: PartitionAlloc and BlinkGC (aka Oilpan)
Hook `AllocationHook` because the code is inlined into many places
- This demonstrates:
 - Invoke a C++ function from the hook
 - Modify the register in the injected code