



## 系統級沙箱弱點及逃逸技巧

MJ0011  
th\_decoder@126.com



## 自我介紹

- ID: MJ0011
- 內核驅動工程師
- 專長：內核漏洞、安全對抗、Rootkit、逆向工程
- 演講：
  - XCON2008(Bootkit)
  - POC2009(外部即時分析Vmware)
  - POC2010(Anti Virus軟體內核漏洞)
- MSN : tyjaaa@163.com



## 360介紹

奇虎360科技有限公司

- 2005/9月成立於中國北京
- 2011/3/30 美國紐約交易所上市, NYSE: QIHU
- 2011/3月底止, 3.45億用戶, 覆蓋88%中國上網用戶
- 主力安全產品
  - 360安全衛士 - 全方面安全防護軟體
  - 360殺毒 - 輕量擁有四引擎防護, 包括 BitDefender / Avira 国际知名引擎
  - 360安全瀏覽器
  - 360極速瀏覽器
  - 360安全桌面



## 議程

- 系統級沙箱防禦技術一覽
- Avast! AV6 AutoSandbox 弱點分析及逃逸
- Kaspersky KIS2012 SafeRun 弱點分析及逃逸
- Comodo CIS2011 AutoSandbox 弱點分析及逃逸
- Kingsoft KAV2012 AutoSandbox 內核安全性漏洞

## 系統級沙箱防禦技術一覽

Kaspersky Internet Security 2012 Premium Protection

Kaspersky Internet Security 2012 delivers premium protection from viruses, Trojans, spyware, hackers, and more. Its cutting-edge, hybrid approach to digital security is based on a combination of advanced signature-based and heuristic detection methods. You, your private data and PC are completely protected as you work, bank, shop and play online.

- 系統級沙箱 隔離可疑程式或易受攻擊的程式
- 集成到殺毒軟體中 結合可疑識別的新一代惡意程式防禦技術

Key Features

- **Kaspersky URL Advisor**  
Marks web links with a color-coded tag that shows their danger level and allows you to choose whether to open them *Improved!*
- **Kaspersky File Advisor**  
Checks file safety with a single click of the mouse *New!*
- **System Watcher**  
Monitors suspicious application activities and allows you to roll back system changes made by malware *Improved!*
- **Application Control**  
Restricts program access to personal data and system files according to the level of danger that each program presents *Improved!*
- **Safe Run Mode**  
Lets you launch suspicious applications and websites in a special, isolated environment where they cannot harm your computer
- **Two-way personal firewall**  
Protects against hacker attacks
- **Anti-Phishing and Anti-Spam technology**  
Provides reliable protection for your personal information and guards against unwanted spam and adware *Improved!*
- **Parental Control**  
Provides flexible and effective settings to keep children extra-safe when they use computers and the Internet *Improved!*
- **Completely redesigned interface**

## 系統級沙箱防禦技術一覽

- 必備防禦及實現方式
- I/O隔離：FsFilter/RegCallback/Api Hook
- 程式行為隔離：Restricted Token/Api Hook
- RPC隔離：Restricted Token/Api Hook
- UI隔離：Job/Api Hook

## 系統級沙箱防禦技術一覽

- 沙箱面臨的安全挑戰
- 隔離必須面面俱到，任何一點的隔離被突破，都將導致整個沙箱失效、惡意程式從沙箱逃逸
- 沙箱中惡意程式逃逸後的安全問題：比普通惡意程式更嚴重，虛擬化可能使其他防禦機制失效
- 沙箱驅動Hook實現不當可導致內核安全性漏洞

## Avast! 沙箱弱點和逃逸

- Avast! AutoSandbox 弱點
- 弱點1：RPC隔離可被繞過
- Avast!通過Ring3 Api Hook攔截部分RPC行為操作:SCM、Remote Registry ...
- 突破：恢復Ring3 Api Hook，穿透Avast! 沙箱註冊表虛擬化，寫入系統關鍵註冊表位置
- Demo



## Avast! 沙箱弱點和逃逸

- 弱點2：進程行為防護可被繞過
- Avast! Hook SSDT NtOpenProcess防止沙箱內部進程訪問外部進程
- Hook處理方式漏洞：先調用原始函數，成功打開後再使用NtDuplicateObject將獲得的Handle降權後，關閉原始Handle，返回降權Handle，Duplicate失敗則不關閉
- 突破：Handle洪水攻擊，填滿當前進程Handle Table，使NtDuplicateObject失敗，獲得沙箱外部進程高許可權Handle，注入外部進程
- Demo



## Kaspersky沙箱弱點和逃逸

- Kaspersky SafeRun 弱點：
- UI隔離功能缺失
- 突破：keybd\_event模擬鍵盤消息在沙箱外運行任意程式
- Demo



## Comodo沙箱弱點和逃逸

- Comodo AutoSandbox實現：
- 沙箱安全性分級，其中“不可信任級別”防護非常嚴格，超過其他三家沙箱，擁有行為防禦+受限用戶+JOB UI隔離
- 弱點：UI隔離幾乎完全依賴JOB
- 突破：利用系統機制，繞過註冊表虛擬化載入輸入法，對外廣播消息，注入外部進程
- Demo



## Comodo沙箱弱點和逃逸

- 詳解突破依賴作業系統實現的沙箱的方式：繞過註冊表虛擬化添加輸入法的原理
- 系統KeyboardLayout鏈載入方式
- ImmLoadLayout的機制導致註冊表虛擬化無效，成功在註冊表虛擬化下添加全域輸入法
- 消息廣播使全域輸入法生效，注入外部進程



## Kingsoft沙箱內核安全性漏洞

- SSDT Hook的安全性問題：參數檢查的疏漏
- 十年前就被提及，BSODHook
- 在過去防禦軟體的SSDT Hook中，參數檢查的疏漏，通常只能引發內核拒絕服務攻擊，影響有限
- 沙箱的SSDT Hook中，由於要改寫訪問資源的最終路徑，參數檢查疏漏將可能導致內核任意位址寫入漏洞，沙箱中任意許可權進程可以直接在內核態運行代碼



## Kingsoft沙箱內核安全性漏洞

- Kingsoft KAV2012安全沙箱：幾乎完全沒有參數檢查
- Kiskrnl.sys NtQueryValueKey Hook Local Kernel Mode Privilege Escalation Vulnerability
- 運用沙箱機制觸發NtQueryValueKey hook的漏洞：分別以讀、寫許可權，打開註冊表handle a、b，寫入a，讀取b，讀取時傳遞觸發漏洞的參數
- Demo



## Q&A

- 感謝:
- CHROOT Security Group
- 360Safe HIPS Team



杀木马 打补丁 保护隐私  
www.360.cn