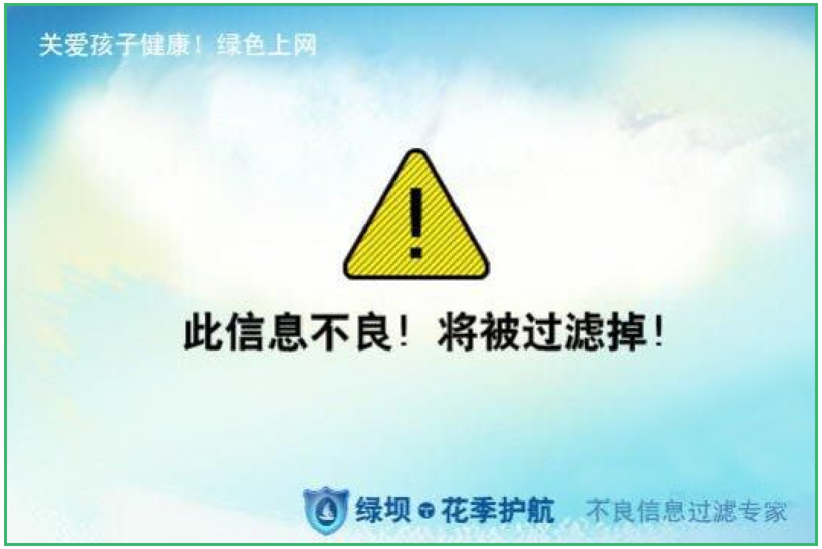
Host-Based Censorware

- Network-based censorship is *hard*
  - Thanks to Tor bridges and other evasion tools!
- Censors trying to strike a fine balance
  - Major restrictions (eg. whitelisting) = angry users
  - Whack-a-mole network filtering = leaky sieve
- “Hey, let's push down the censorship functionality to the end host!”

Green Dam Youth Escort

- Host-based censorship software introduced by the Chinese government



关爱孩子健康！绿色上网

此信息不良！将被过滤掉！

不良信息过滤专家

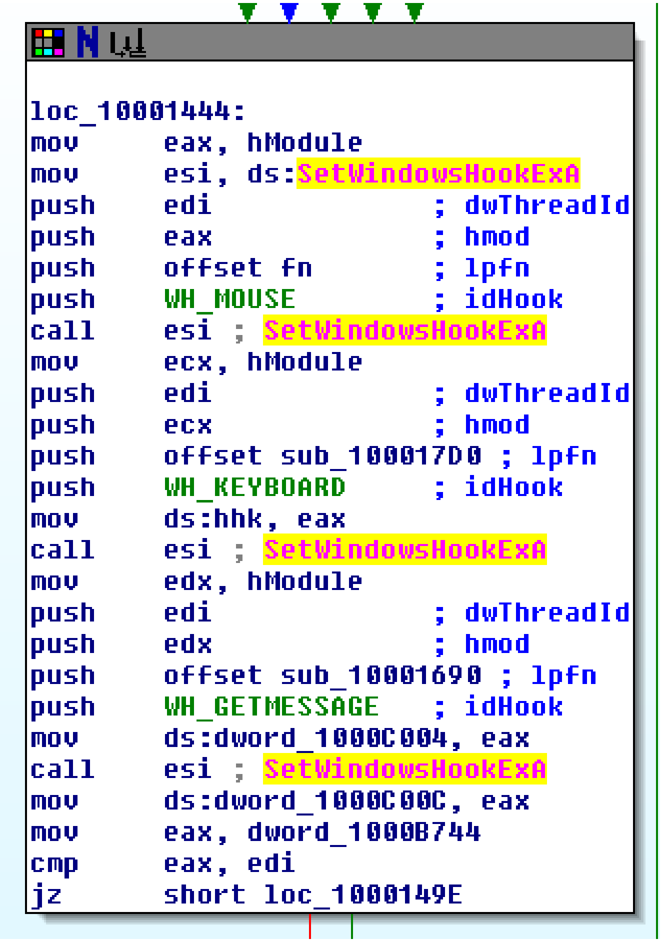
- Originally mandated to be installed on all personal computers purchased in China

Green Dam Features

- Content / text filter
  - Blocking political and adult content
- Networking filtering for URLs / keywords
  - Blacklists stolen from Cybersitter software
- Image pornography filtering
  - OpenCV skin tone detection heuristics
- Bonus “features”
  - Trivial stack smashes via long URL
- Great report from my U of M colleagues
  - http://www.cse.umich.edu/~jhalderm/pub/gd/

Technical Operation

- Lots o' interposition!
- SetWindowsHookEx hooks
  - WH_MOUSE, WH_KEYBOARD, WH_GETMESSAGE
- Winsock LSP hooks
  - eg. DBFP_Recv in SurfGd.dll
- Remote process DLL injection
  - eg. InjLib32.dll / HAServ.dll
- Select processes targeted
  - iexplore.exe, notepad.exe, winword.exe, qq.exe, outlook.exe, msgmsgr.exe, etc



```
loc_10001444:
mov     eax, hModule
mov     esi, ds:SetWindowsHookExA
push    edi                 ; dwThreadId
push    eax                 ; hmod
push    offset fn           ; lpfn
push    WH_MOUSE            ; idHook
call    esi ; SetWindowsHookExA
mov     ecx, hModule
push    edi                 ; dwThreadId
push    ecx                 ; hmod
push    offset sub_100017D0 ; lpfn
push    WH_KEYBOARD         ; idHook
mov     ds:hhk, eax
call    esi ; SetWindowsHookExA
mov     edx, hModule
push    edi                 ; dwThreadId
push    edx                 ; hmod
push    offset sub_10001690 ; lpfn
push    WH_GETMESSAGE       ; idHook
mov     ds:dword_1000C004, eax
call    esi ; SetWindowsHookExA
mov     ds:dword_1000C00C, eax
mov     eax, dword_1000B744
cmp     eax, edi
jz      short loc_1000149E
```

The token IDA screenshot

Ring-3 Hooking

- API hooking in userspace
  - Usually used in crappy “rootkits”, spyware, etc
  - IAT patching / jmp code overwriting
- Traditionally done with “viral” hooking
  - Inject into all running processes (CreateRemoteThread)
  - Hook CreateProcess routines
  - New processes will be auto-injected/hooked
- We're on a level playing field
  - Oh, you just injected yourself into Firefox?
  - I'll follow you in and undo everything you just did!

Dam Burst

dam burst

- The Dam Burst tool
  - Instead of pwn'ing Green Dam users, *let's actually help the users who may face censorship.*
  - Disables Green Dam without administrative access (eg. internet cafes, public computers)
  - Transient, in-memory patching (avoid persistent system changes)
  - Closes off the vulnerable Green Dam routines

In-Process Memory Patching

- Injection:

`VirtualAllocEx()`
`allocate memory in remote process`

`VirtualProtectEx()`
`make remote memory writeable`

`WriteProcessMemory()`
`inject our code`

```
    LoadLibrary(“damburst.dll”)
    burst = GetProcAddress(“Burst”)
    Call burst
```

`VirtualProtectEx()`
`restore memory protection`

`CreateRemoteThread()`
`execute injected code`

- Patching:

`Neuter Winsock LSP hooks`

```
    addr = GetProcAddres(“DBFP_*”)
    VirtualProtect(addr)
    memcpy(addr, NOP)
    VirtualProtect(addr)
    FlushInstructionCache(addr)
```

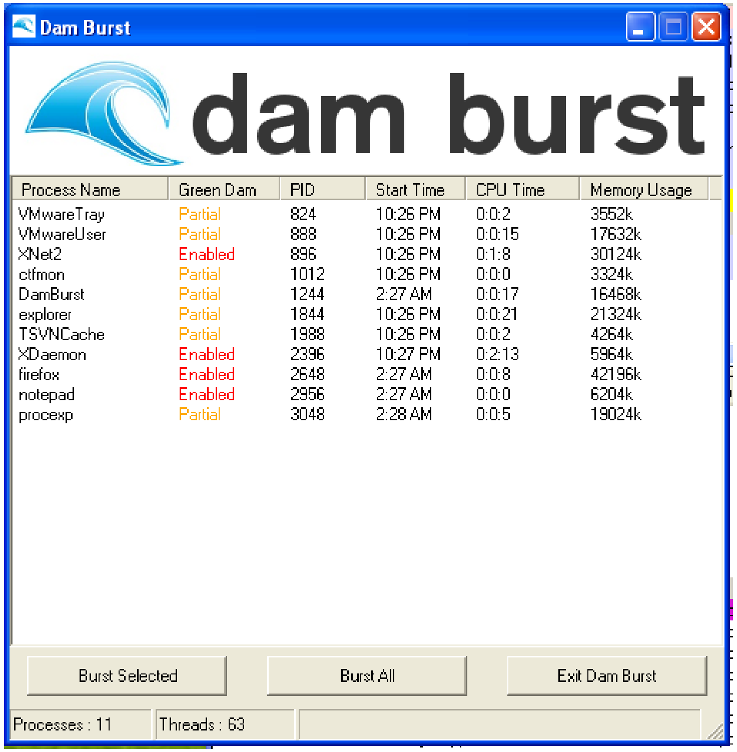
`Disable API hooks / SetWindowsHookEx`

```
    GetModuleHandle(“InjLib32.dll”)
    GetProcessAddress(“InjectLibrary”)
    InjectLibrary(FALSE) // HA!
```

`Unload Green Dam`

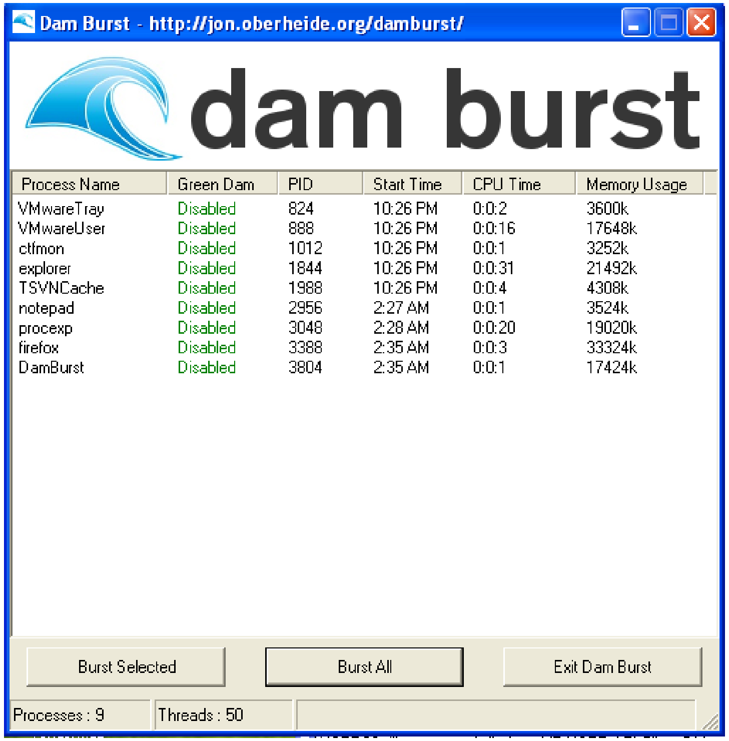
```
    FreeLibrary(“Handler.dll”)
    FreeLibrary(“InjLib32.dll”)
```

Demo



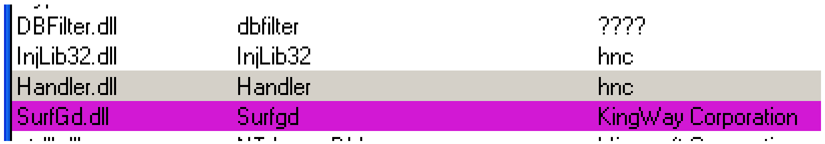
Process Name	Green Dam	PID	Start Time	CPU Time	Memory Usage
VMwareTray	Partial	824	10:26 PM	0:0:2	3552k
VMwareUser	Partial	888	10:26 PM	0:0:15	17632k
XNet2	Enabled	896	10:26 PM	0:1:8	30124k
ctfmon	Partial	1012	10:26 PM	0:0:0	3324k
DamBurst	Partial	1244	2:27 AM	0:0:17	16468k
explorer	Partial	1844	10:26 PM	0:0:21	21324k
TSVNCache	Partial	1988	10:26 PM	0:0:2	4264k
XDaemon	Enabled	2396	10:27 PM	0:2:13	5964k
firefox	Enabled	2648	2:27 AM	0:0:8	42196k
notepad	Enabled	2956	2:27 AM	0:0:0	6204k
procexp	Partial	3048	2:28 AM	0:0:5	19024k

Processes : 11 Threads : 63

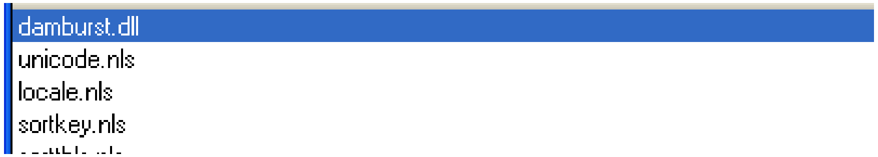


Process Name	Green Dam	PID	Start Time	CPU Time	Memory Usage
VMwareTray	Disabled	824	10:26 PM	0:0:2	3600k
VMwareUser	Disabled	888	10:26 PM	0:0:16	17648k
ctfmon	Disabled	1012	10:26 PM	0:0:1	3252k
explorer	Disabled	1844	10:26 PM	0:0:31	21492k
TSVNCache	Disabled	1988	10:26 PM	0:0:4	4308k
notepad	Disabled	2956	2:27 AM	0:0:1	3524k
procexp	Disabled	3048	2:28 AM	0:0:20	19020k
firefox	Disabled	3388	2:35 AM	0:0:3	33324k
DamBurst	Disabled	3804	2:35 AM	0:0:1	17424k

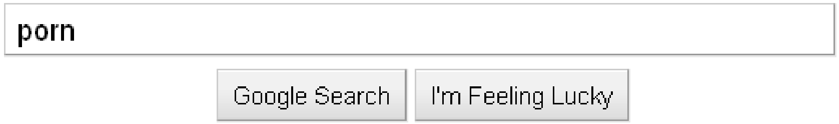
Processes : 9 Threads : 50



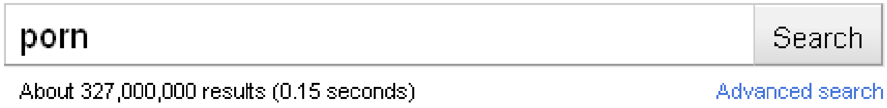
DBFilter.dll	dbfilter	????
InjLib32.dll	InjLib32	hnc
Handler.dll	Handler	hnc
SurfGd.dll	Surfgd	KingWay Corporation



damburst.dll
unicode.nls
locale.nls
sortkey.nls

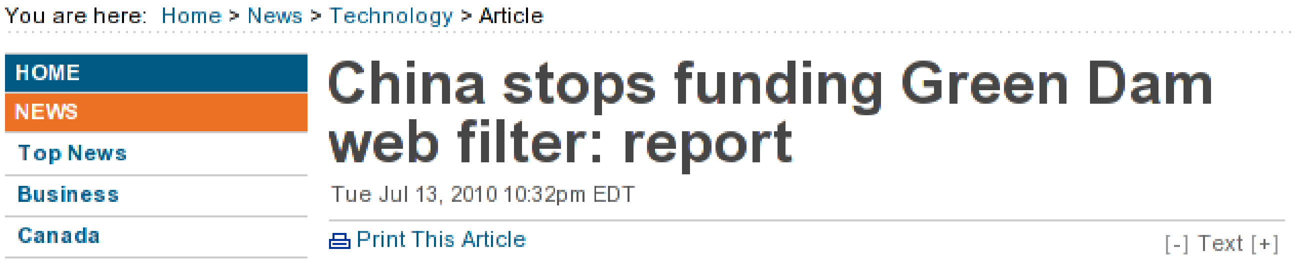


Greer



About 327,000,000 results (0.15 seconds)

Green Dam Defeated, But...

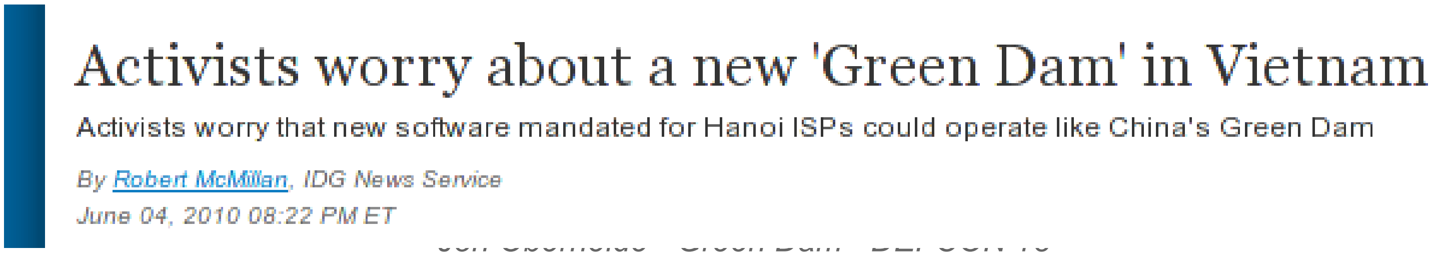


You are here: Home > News > Technology > Article

China stops funding Green Dam web filter: report

Tue Jul 13, 2010 10:32pm EDT

- An initial attempt at host-based censorware
  - Executed pretty poorly
  - Subsequent attempts will learn from Green Dam's mistakes
- We'll undoubtedly see more in the future...
  - Driven by proliferation of tools like Tor that effectively evade network-based censorship



Activists worry about a new 'Green Dam' in Vietnam

Activists worry that new software mandated for Hanoi ISPs could operate like China's Green Dam

By Robert McMillan, IDG News Service

June 04, 2010 08:22 PM ET