Shellcode & Process Injection

11-15 JAN 21

Tasking

Getting familiar with native encryption and in-memory execution techniques.

Detourer

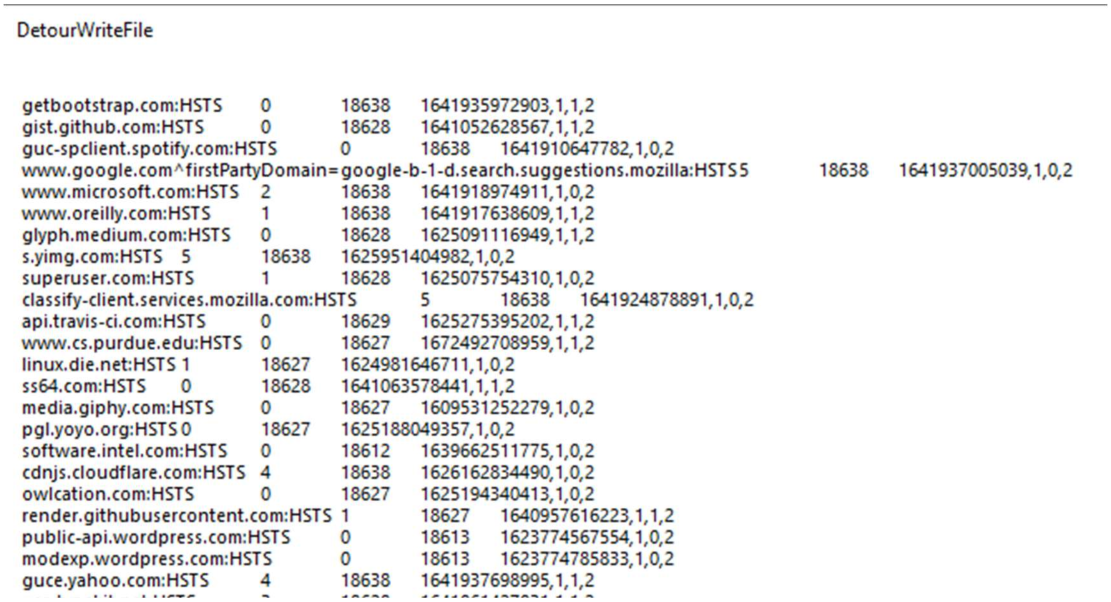
I spent a good bit more time trying to expand the other hooking project, but manually parsing, targeting, and crafting is—after spending plenty of time on it—pretty wasteful. Instead, I opted to use MS Detours so I can focus on interacting with the target process rather than just achieving execution.

From this came Detourer, a quick and lightweight wrapper for Detours that lets me hotswap target modules and payloads. With plenty of arbitrarily commented out code, Detourer is doing a fantastic job so far.

Ideally, Detourer will allow for further modularization such that an operator can build against any target function to passively exfil data or modify/inject requests in-line. I've been able to do both so far against Chrome, Firefox, and a few other random processes—see attached screenshots on following pages.

Future Plans

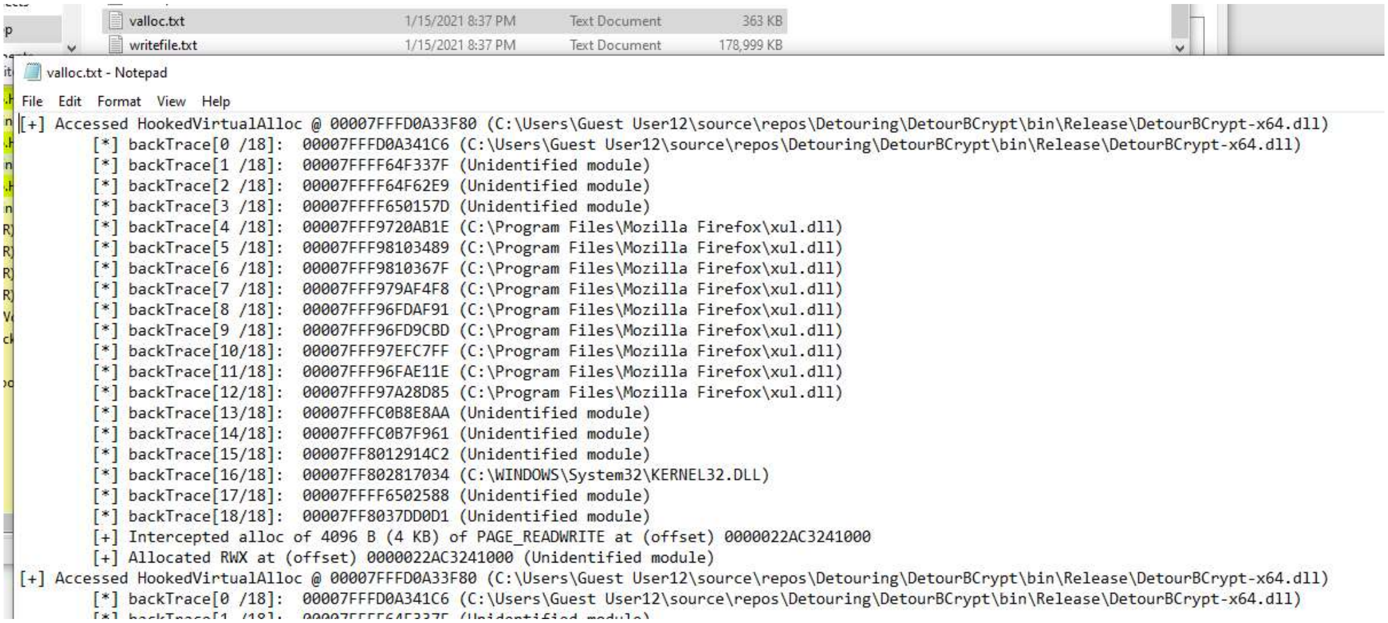
- Optimize away some stability issues from the sheer volume of exfil IO.
    - Some processes are SUPER fragile. E.g., Discord 100% of the time crashes almost instantly, even with minimal interaction.
    - Firefox was impressively resilient to haphazardly attaching/detaching modules and stalling it with IO. I appreciate this.
- Develop a loader.
- Add support for more targets and payloads. Make the base even more lightweight such that an operator can simply add a list of target functions (or even libraries) and ship it.



DetourWriteFile

```
getbootstrap.com:HSTS      0          18638    1641935972903,1,1,2
gist.github.com:HSTS       0          18628    1641052628567,1,1,2
guc-spclient.spotify.com:HSTS         0        18638    1641910647782,1,0,2
www.google.com^firstPartyDomain=google-b-1-d.search.suggestions.mozilla:HSTS5          18638    1641937005039,1,0,2
www.microsoft.com:HSTS     2          18638    1641918974911,1,0,2
www.oreilly.com:HSTS       1          18638    1641917638609,1,1,2
glyph.medium.com:HSTS      0          18628    1625091116949,1,1,2
s.yimg.com:HSTS   5        18638    1625951404982,1,0,2
superuser.com:HSTS         1          18628    1625075754310,1,0,2
classify-client.services.mozilla.com:HSTS         5        18638    1641924878891,1,0,2
api.travis-ci.com:HSTS     0          18629    1625275395202,1,1,2
www.cs.purdue.edu:HSTS     0          18627    1672492708959,1,1,2
linux.die.net:HSTS 1       18627    1624981646711,1,0,2
ss64.com:HSTS     0        18628    1641063578441,1,1,2
media.giphy.com:HSTS       0          18627    1609531252279,1,0,2
pgl.yoyo.org:HSTS 0        18627    1625188049357,1,0,2
software.intel.com:HSTS    0          18612    1639662511775,1,0,2
cdnjs.cloudflare.com:HSTS  4          18638    1626162834490,1,0,2
owlcation.com:HSTS         0          18627    1625194340413,1,0,2
render.githubusercontent.com:HSTS 1            18627    1640957616223,1,1,2
public-api.wordpress.com:HSTS         0        18613    1623774567554,1,0,2
modexp.wordpress.com:HSTS             0        18613    1623774785833,1,0,2
guce.yahoo.com:HSTS        4          18638    1641937698995,1,1,2
```

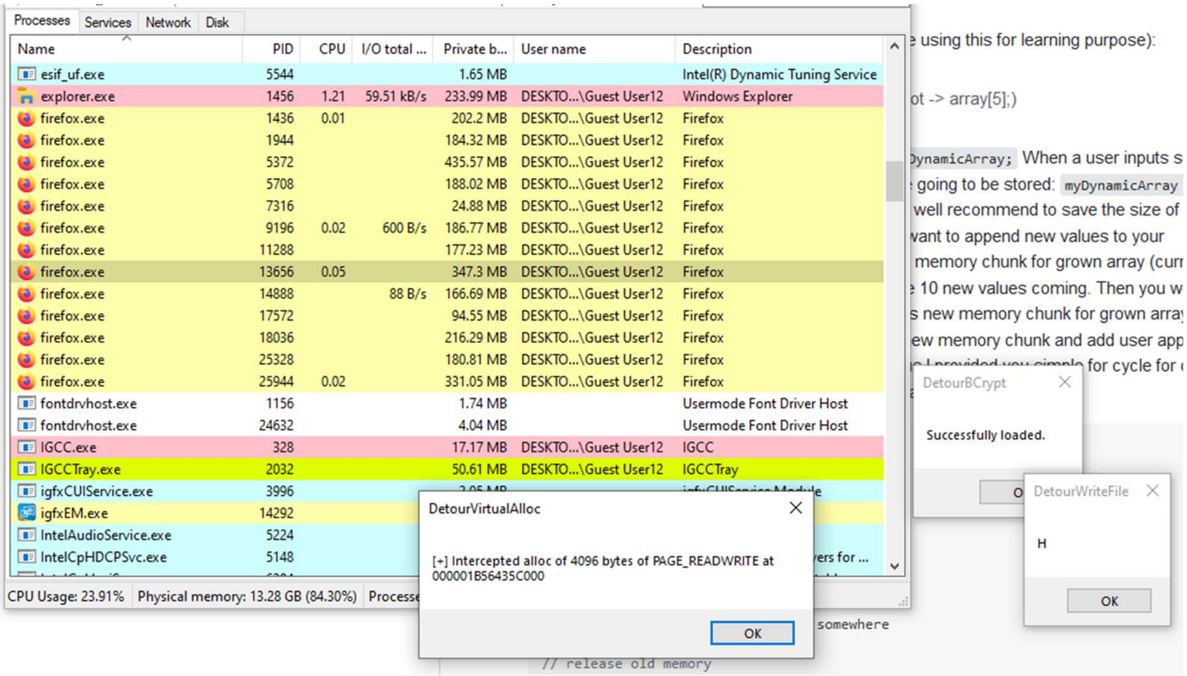
Figure 2 Courtesy of Firefox



```
[+] Accessed HookedVirtualAlloc @ 00007FFFD0A33F80 (C:\Users\Guest User12\source\repos\Detouring\DetourBCrypt\bin\Release\DetourBCrypt-x64.dll)
        [*] backTrace[0 /18]:  00007FFFD0A341C6 (C:\Users\Guest User12\source\repos\Detouring\DetourBCrypt\bin\Release\DetourBCrypt-x64.dll)
        [*] backTrace[1 /18]:  00007FFFF64F337F (Unidentified module)
        [*] backTrace[2 /18]:  00007FFFF64F62E9 (Unidentified module)
        [*] backTrace[3 /18]:  00007FFFF650157D (Unidentified module)
        [*] backTrace[4 /18]:  00007FFF9720AB1E (C:\Program Files\Mozilla Firefox\xul.dll)
        [*] backTrace[5 /18]:  00007FFF98103489 (C:\Program Files\Mozilla Firefox\xul.dll)
        [*] backTrace[6 /18]:  00007FFF9810367F (C:\Program Files\Mozilla Firefox\xul.dll)
        [*] backTrace[7 /18]:  00007FFF979AF4F8 (C:\Program Files\Mozilla Firefox\xul.dll)
        [*] backTrace[8 /18]:  00007FFF96FDAF91 (C:\Program Files\Mozilla Firefox\xul.dll)
        [*] backTrace[9 /18]:  00007FFF96FD9CBD (C:\Program Files\Mozilla Firefox\xul.dll)
        [*] backTrace[10/18]:  00007FFF97EFC7FF (C:\Program Files\Mozilla Firefox\xul.dll)
        [*] backTrace[11/18]:  00007FFF96FAE11E (C:\Program Files\Mozilla Firefox\xul.dll)
        [*] backTrace[12/18]:  00007FFF97A28D85 (C:\Program Files\Mozilla Firefox\xul.dll)
        [*] backTrace[13/18]:  00007FFFC0B8E8AA (Unidentified module)
        [*] backTrace[14/18]:  00007FFFC0B7F961 (Unidentified module)
        [*] backTrace[15/18]:  00007FF8012914C2 (Unidentified module)
        [*] backTrace[16/18]:  00007FF802817034 (C:\WINDOWS\System32\KERNEL32.DLL)
        [*] backTrace[17/18]:  00007FFFF6502588 (Unidentified module)
        [*] backTrace[18/18]:  00007FF8037DD0D1 (Unidentified module)
        [+] Intercepted alloc of 4096 B (4 KB) of PAGE_READWRITE at (offset) 0000022AC3241000
        [+] Allocated RWX at (offset) 0000022AC3241000 (Unidentified module)
[+] Accessed HookedVirtualAlloc @ 00007FFFD0A33F80 (C:\Users\Guest User12\source\repos\Detouring\DetourBCrypt\bin\Release\DetourBCrypt-x64.dll)
        [*] backTrace[0 /18]:  00007FFFD0A341C6 (C:\Users\Guest User12\source\repos\Detouring\DetourBCrypt\bin\Release\DetourBCrypt-x64.dll)
```

Figure 1 I know exactly where my malicious memory is going. Note the replacement with RWX.

No complaints from system.



Name	PID	CPU	I/O total ...	Private b...	User name	Description
esif_uf.exe	5544			1.65 MB		Intel(R) Dynamic Tuning Service
explorer.exe	1456	1.21	59.51 kB/s	233.99 MB	DESKTO...\Guest User12	Windows Explorer
firefox.exe	1436	0.01		202.2 MB	DESKTO...\Guest User12	Firefox
firefox.exe	1944			184.32 MB	DESKTO...\Guest User12	Firefox
firefox.exe	5372			435.57 MB	DESKTO...\Guest User12	Firefox
firefox.exe	5708			188.02 MB	DESKTO...\Guest User12	Firefox
firefox.exe	7316			24.88 MB	DESKTO...\Guest User12	Firefox
firefox.exe	9196	0.02	600 B/s	186.77 MB	DESKTO...\Guest User12	Firefox
firefox.exe	11288			177.23 MB	DESKTO...\Guest User12	Firefox
firefox.exe	13656	0.05		347.3 MB	DESKTO...\Guest User12	Firefox
firefox.exe	14888		88 B/s	166.69 MB	DESKTO...\Guest User12	Firefox
firefox.exe	17572			94.55 MB	DESKTO...\Guest User12	Firefox
firefox.exe	18036			216.29 MB	DESKTO...\Guest User12	Firefox
firefox.exe	25328			180.81 MB	DESKTO...\Guest User12	Firefox
firefox.exe	25944	0.02		331.05 MB	DESKTO...\Guest User12	Firefox
fontdrvhost.exe	1156			1.74 MB		Usermode Font Driver Host
fontdrvhost.exe	24632			4.04 MB		Usermode Font Driver Host
IGCC.exe	328			17.17 MB	DESKTO...\Guest User12	IGCC
IGCCTray.exe	2032			50.61 MB	DESKTO...\Guest User12	IGCCTray
igfxCUIService.exe	3996			2.05 MB		igfxCUIService Module
igfxEM.exe	14292					
IntelAudioService.exe	5224					
IntelCpHDCPSvc.exe	5148					ers for ...

CPU Usage: 23.91% Physical memory: 13.28 GB (84.30%) Processe

DetourVirtualAlloc

[+] Intercepted alloc of 4096 bytes of PAGE_READWRITE at 000001B56435C000

OK

DetourBCrypt

Successfully loaded.

DetourWriteFile

H

OK

e using this for learning purpose):

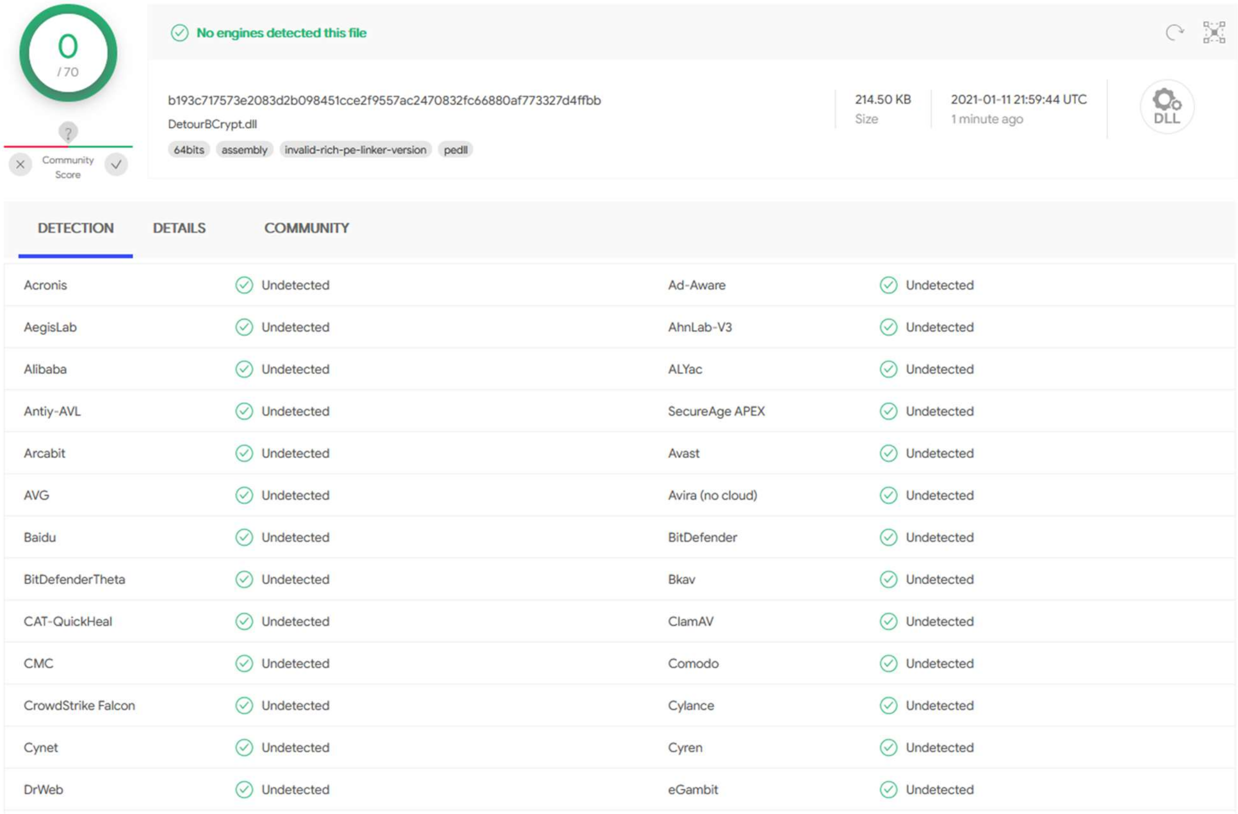
ot -> array[5];)

DynamicArray; When a user inputs s
going to be stored: myDynamicArray
well recommend to save the size of
want to append new values to your
memory chunk for grown array (curr
e 10 new values coming. Then you w
s new memory chunk for grown array
ew memory chunk and add user app
s I provided you simple for cycle for

somewhere

// release old memory

Figure 3 Had to quickly swap to file stream output because it triggered so often.


0 / 70

No engines detected this file

b193c717573e2083d2b098451cce2f9557ac2470832fc66880af773327d4ffbb
DetourBCrypt.dll
64bits assembly invalid-rich-pe-linker-version pedll

214.50 KB
Size

2021-01-11 21:59:44 UTC
1 minute ago

Acronis	✓ Undetected	Ad-Aware	✓ Undetected
AegisLab	✓ Undetected	AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	SecureAge APEX	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
AVG	✓ Undetected	Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected
BitDefenderTheta	✓ Undetected	Bkav	✓ Undetected
CAT-QuickHeal	✓ Undetected	ClamAV	✓ Undetected
CMC	✓ Undetected	Comodo	✓ Undetected
CrowdStrike Falcon	✓ Undetected	Cylance	✓ Undetected
Cynet	✓ Undetected	Cyren	✓ Undetected
DrWeb	✓ Undetected	eGambit	✓ Undetected

Figure 4 Despite *aggressively* replacing all memory allocation requests with RWX.