Browser lockers: extortion disguised as a fine

SL securelist.com/browser-lockers-extortion-disguised-as-a-fine/101735

Authors

Expert AMR

Browser lockers (aka browlocks) are a class of online threats that prevent the victim from using the browser and demand a ransom. A locker is a fake page that dupes the user, under a fictitious pretext (loss of data, legal liability, etc.), into making a call or a money transfer, or giving out payment details. The “locking” consists of preventing the user from leaving the current tab, which displays intimidating messages, often with sound and visual effects.

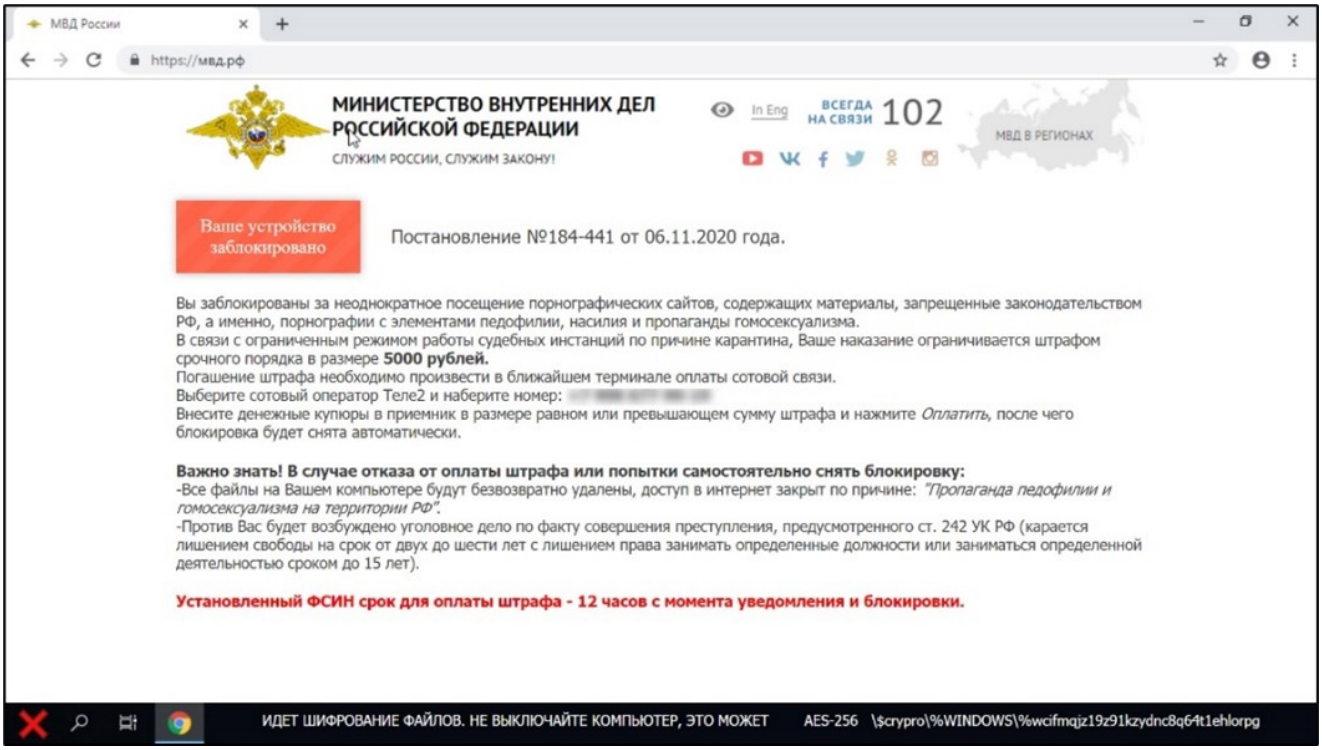
This type of fraud is not new and has long been on the radar of researchers. The past decade has seen numerous browser locking campaigns targeting users worldwide. Despite its mature age, the threat has lost none of its popularity; on the contrary, the number of tricks used by scammers is only growing. They include imitating the “blue screen of death” (BSOD) in the browser, false warnings about system errors or detected viruses, threats to encrypt files, legal liability notices, and many others. In this post, we examine two families of lockers that mimic government websites.

Propagation methods

Both families spread mainly via advertising networks, primarily aimed at selling “adult” content and movies in an intrusive manner; for example, through tabs or windows that open on top of the visited site when loading a page with an embedded ad module (pop-ups) or after clicking anywhere on the page (click-unders). Presumably cybercriminals pay for ads to show browser lockers in pop-ups.

Family #1. Fake websites of the Russian Ministry of Internal Affairs: “Give us your money”

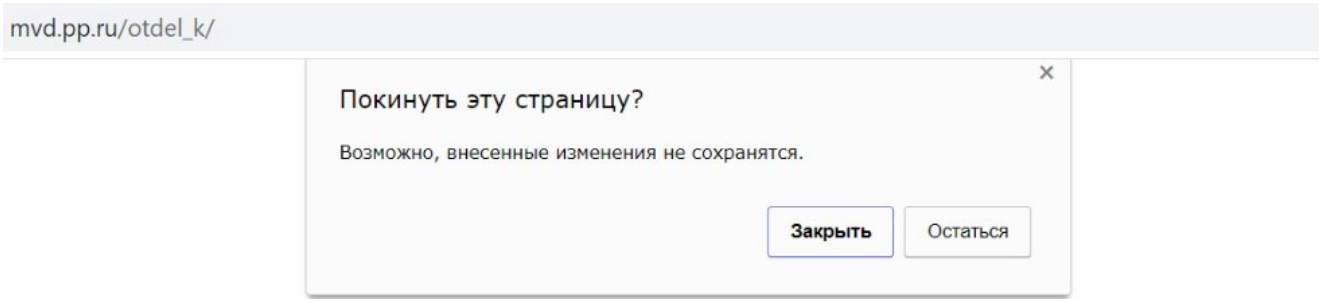
Members of the first family under consideration mimic the website of the Russian Ministry of Internal Affairs (MVD), and are thus aimed at users from Russia. In Q4 2020, more than 55,000 users encountered them.



Example of a fake MVD website

What the victim sees (and hears)

On landing on a fake browlock site, the user typically sees a warning, supposedly from the browser, saying that if they leave the page some changes might not be saved.



If the user simply closes the tab, nothing happens; but if they click anywhere on the page, the main content of the locker expands to full screen. As a result, an imitation of a computer screen with an open browser appears in front of the user: at the bottom is a taskbar with the Google Chrome icon, and at the top is an address bar displaying the real URL of the MVD. The notification on the page states that the device has been locked due to a violation of the law. Under the pretext of a fine, the victim is instructed to transfer a certain amount to a mobile account, ranging in size from 3,000 to 10,000 rubles (US$40–130). In case of refusal, the ransomwarers threaten file encryption, as well as criminal liability under Article 242 of the Russian Criminal Code. The page is accompanied by an audio recording with threats and a demand to pay the fine.

Technical details

The scammers use full-screen mode to make it difficult for the user to access the browser window controls and taskbar, and to create a locking effect. In addition, to convince the victim that the mouse is unresponsive, the attackers hide the cursor by manipulating the CSS property *cursor*.

The page also uses the following code to handle keystrokes:

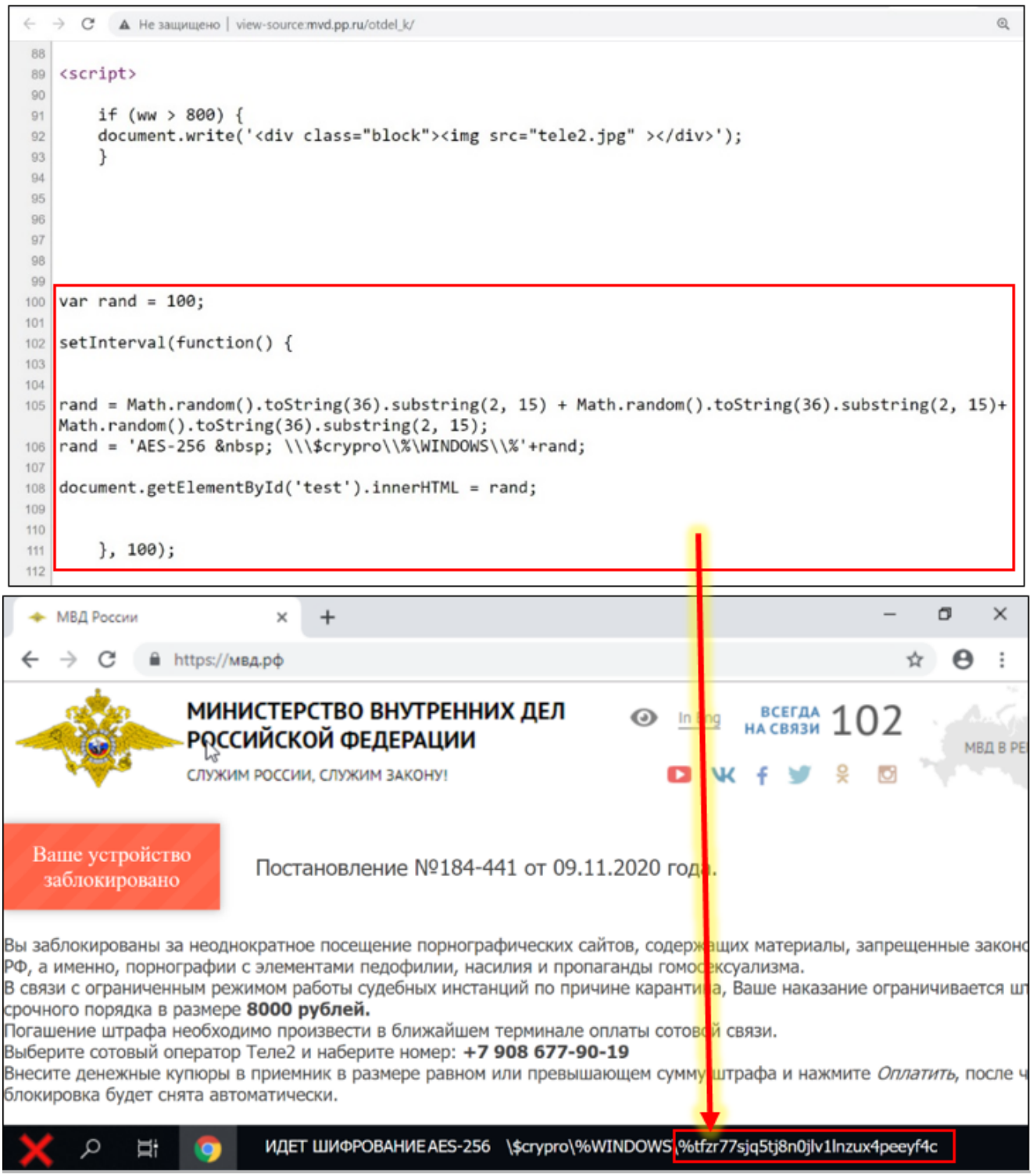
```
var _0xefa4=[
"\x30\x2E\x66\x3D\x35\x28\x33\x29\x7B\x34\x28\x64\x2E\x63\x28\x33\x2E\x38\x2C\x5B\x62\x2C\x65\x2C\x37\x2C\x39\x2C\x6B\x2C\x6C\
x2C\x6A\x2C\x69\x2C\x67\x5D\x29\x21\x3D\x2D\x31\x29\x7B\x61\x20\x32\x7D\x7D\x3B\x30\x2E\x68\x3D\x35\x28\x36\x29\x7B\x34\x28\x3
6\x2E\x38\x3D\x3D\x37\x29\x61\x20\x32\x7D\x3B","\x7C","\x73\x70\x6C\x69\x74",
"\x77\x69\x6E\x64\x6F\x77\x7C\x7C\x66\x61\x6C\x73\x65\x7C\x65\x76\x74\x7C\x69\x66\x7C\x66\x75\x6E\x63\x74\x69\x6F\x6E\x7C\x65\
x76\x6E\x7C\x31\x32\x33\x7C\x6B\x65\x79\x43\x6F\x64\x65\x7C\x7C\x72\x65\x74\x75\x72\x6E\x7C\x32\x37\x7C\x69\x6E\x41\x72\x72\x6
1\x79\x7C\x6A\x51\x75\x65\x72\x79\x7C\x31\x38\x7C\x6F\x6E\x6B\x65\x79\x64\x6F\x77\x6E\x7C\x31\x37\x7C\x6F\x6E\x6B\x65\x79\x70\
x72\x65\x73\x73\x7C\x31\x31\x34\x7C\x31\x31\x32\x7C\x31\x31\x35\x7C\x31\x31\x36","\x72\x65\x70\x6C\x61\x63\x65","",
"\x5C\x77\x2B","\x5C\x62","\x67"];eval(function(_0xac06x1,_0xac06x2,_0xac06x3,_0xac06x4,_0xac06x5,_0xac06x6){_0xac06x5=
function(_0xac06x3){return _0xac06x3.toString(36)};if(!_0xefa4[5][_0xefa4[4]](/^/,String)){while(_0xac06x3--){_0xac06x6[
_0xac06x3.toString(_0xac06x2)]= _0xac06x4[_0xac06x3]|| _0xac06x3.toString(_0xac06x2)};_0xac06x4= [function(_0xac06x5){return
_0xac06x6[_0xac06x5]}];_0xac06x5= function(){return _0xefa4[6]};_0xac06x3= 1};while(_0xac06x3--){if(_0xac06x4[_0xac06x3]){
_0xac06x1= _0xac06x1[_0xefa4[4]]( new RegExp(_0xefa4[7]+ _0xac06x5(_0xac06x3)+ _0xefa4[7],_0xefa4[8]),_0xac06x4[_0xac06x3
])};return _0xac06x1}(_0xefa4[0],22,22,_0xefa4[3][_0xefa4[2]](_0xefa4[1]),0,{}))
```

After deobfuscation, we obtain a very small script:

```
window.onkeydown = function (evt) {
    if (jQuery.inArray(evt.keyCode, [27, 18, 123, 9, 115, 116, 112, 114, 17]) != -1) {
        return false
    }
};
window.onkeypress = function (evn) {
    if (evn.keyCode == 123)
        return false
};
```

It was probably assumed that running this code would result in the Escape (keycode=27), Ctrl (keycode=17), Alt (keycode=18) and Tab (keycode=9) keystrokes being ignored, as well as F1, F3, F4, F5 and F12. This could prevent the user from leaving the page using various keyboard shortcuts, but the trick does not work in modern browsers.

Another interesting detail is the animation of the supposed file encryption process, which is shown in the screenshots below. It consists of an endless succession of random numbers and letters, simulating enumeration of allegedly encrypted files in the system directory.



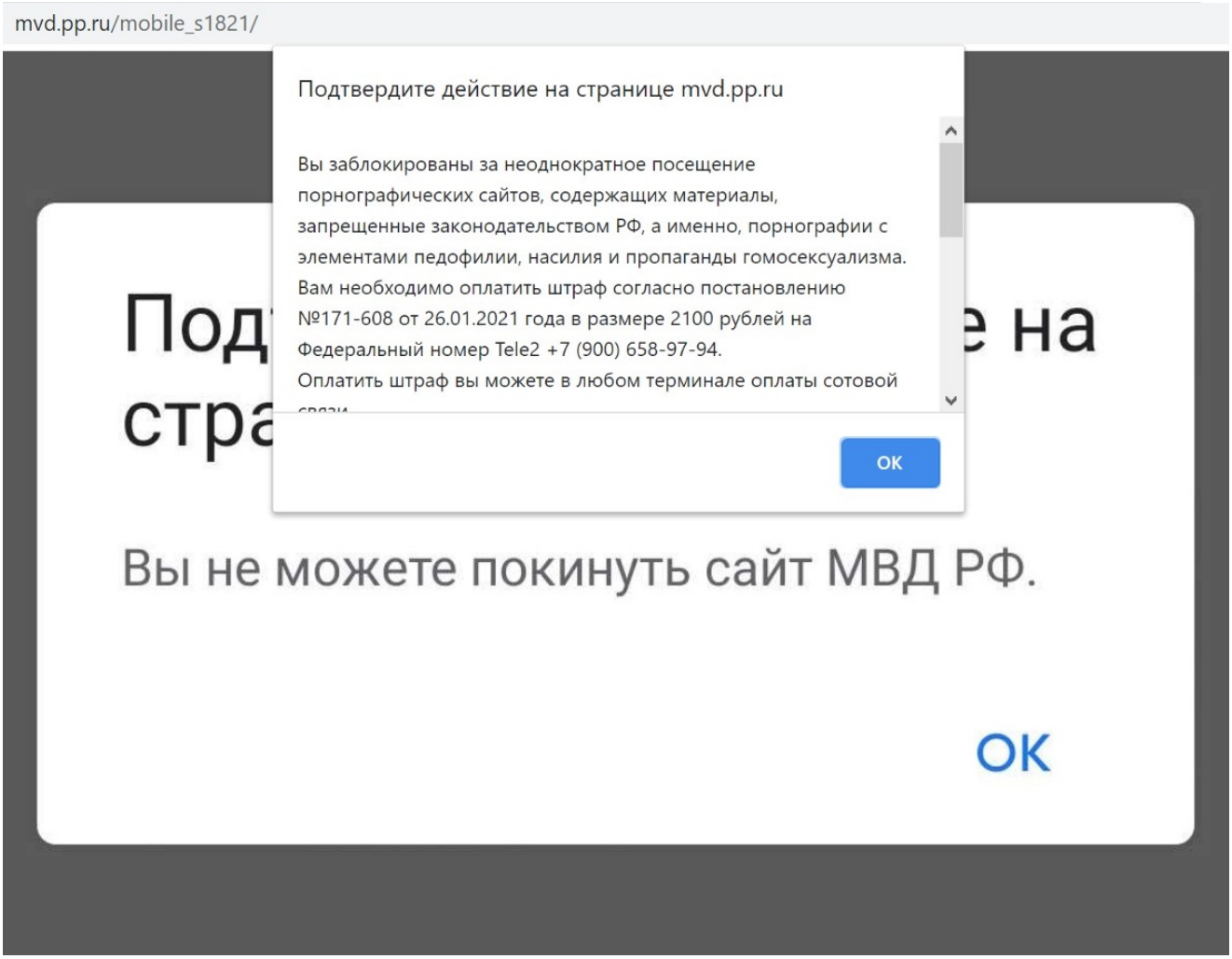
Page addresses

Cybercriminals often use alphanumeric domain names, where the number sequence corresponds to a date close to the domain registration date and the letter sequence is an abbreviation, for example, “mpa” (the Russian abbreviation for “municipal legal act”) or “kad” (“cadastral office”). Example of a fraudulent domain: 0402mpa21[.]ru.

We also saw domain names composed of topic-based words, such as “police” or “mvd”. Cybercriminals use them to mimic the addresses of the legitimate sites of law enforcement agencies. An example of such a domain is mvd-ru[.]tech.

Mobile version of fake MVD websites

The threat also exists on mobile devices. To determine the type of device during propagation, the User-Agent field in the header of the HTTP request is checked. As in the case of the “full” version, the victim is accused of breaking the law and ordered to pay a fine; the amount, however, is smaller than in the desktop version.

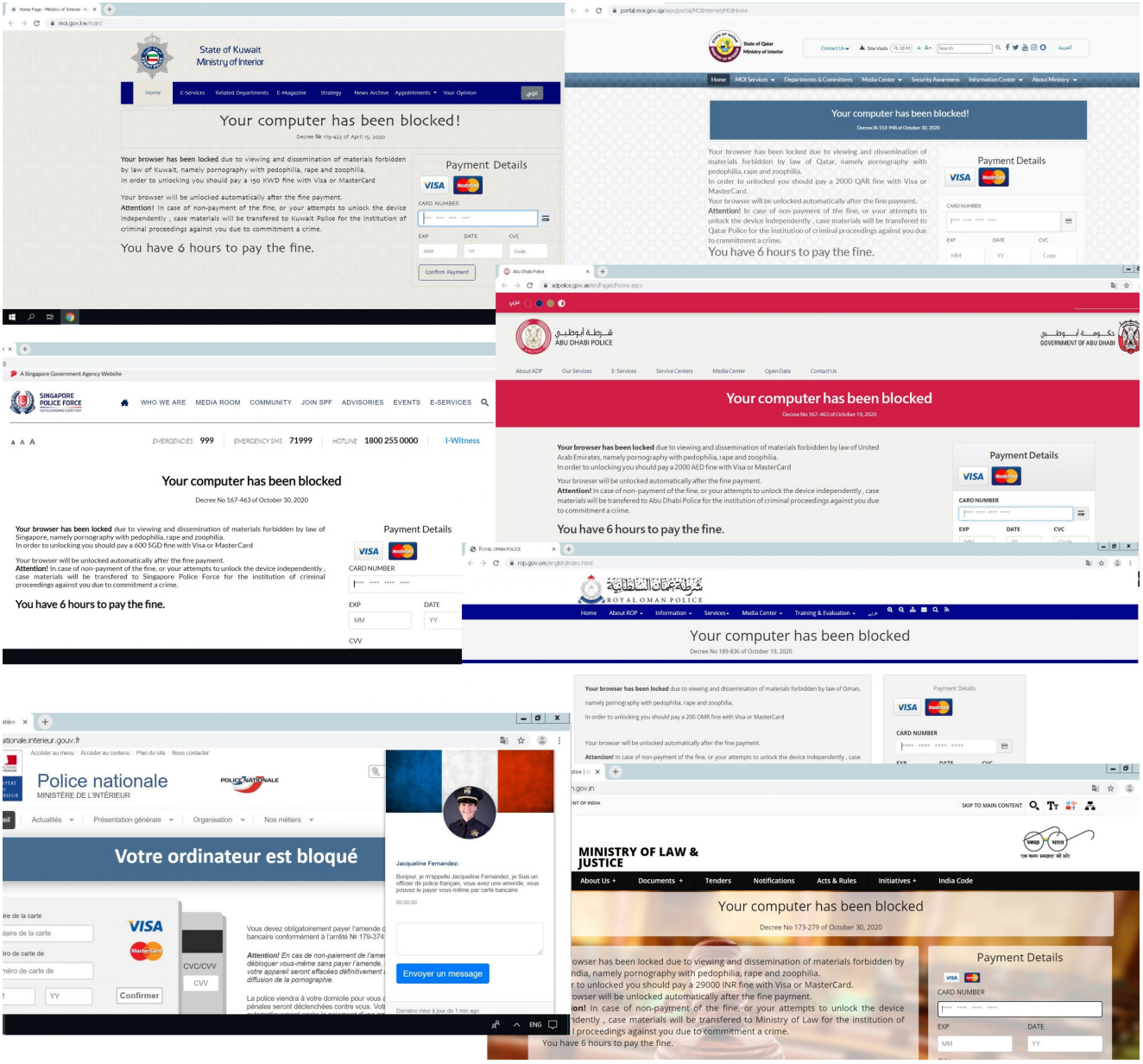


Family #2. Fake law enforcement websites in the Middle East: “Give us your card details”

The second family differs in the way that money is transferred to the ransomwarers. As before, the user is accused of violating the law, informed that their computer has been locked, and instructed to pay a fine. However, instead of leaving their account or telephone number for payment, the cybercriminals insert a data entry form on the page asking for card details.

This family of lockers is targeted mostly at users in the Middle East (UAE, Oman, Kuwait, Qatar, and Saudi Arabia). In addition, we have seen fraudulent pages disguised as Indian and Singaporean law enforcement websites. European equivalents are slightly less common.

In Q4 2020, this family threatened more than 130,000 users.



Examples of ransomware pages

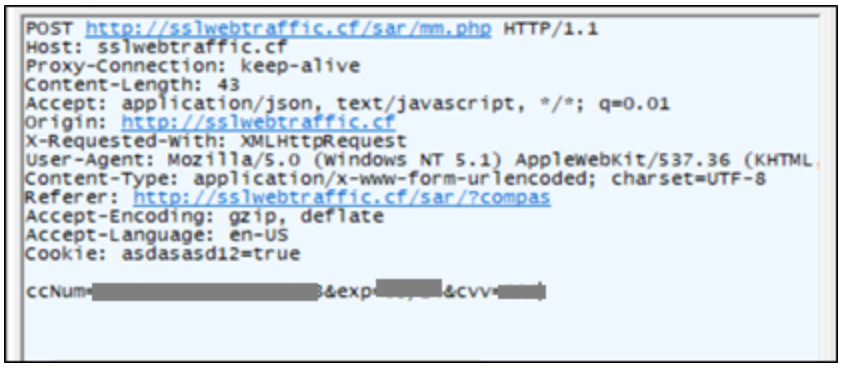
Technical details

From a technical viewpoint, browser lockers of the second type are in many ways similar to the fake MVD websites. As in the first case, the content expands to full screen to make it difficult for the user to access the browser window controls and taskbar. At the top of the page is an address bar with the URL of the official government resource, and at the bottom is

a fake taskbar with the Google Chrome icon. The mouse pointer is not displayed, and a script similar to the one above is used to handle keystrokes. Besides entering payment data, no actions on the page are available to the user.

The screenshot below shows an obfuscated script that implements the “locking,” as well as collects and sends the user-input data.

The victim’s payment details are transferred via an HTTP POST request to the same malicious resource that hosts the page. In the screenshot below is an example of a request to send payment details to the malicious site sslwebtraffic[.]cf.



Conclusion

The threats investigated are not technically complex. Their functionality is rather primitive and aims to create the illusion of locking the computer and intimidate the victim. Landing on such a page by mistake will not harm the user’s device or data, as long as they do not fall for the cybercriminals’ smoke-and-mirror tactics. What’s more, to get rid of the locker requires no special knowledge or technical means.

But if the user panics, they could lose money. Kaspersky solutions block malicious web resources and threat-related files (scripts, content elements) with the verdict HEUR:Trojan.Script.Generic.

Indicators of compromise

Fake MVD websites

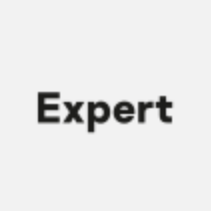
2301tiz21[.]ru
112aubid[.]ru
00210kad[.]ru
1910mpa20[.]ru
mvd[.]pp[.]ru
mvd[.]net[.]ru
police-online[.]info
mvd-online-police[.]ga

Fake law enforcement websites in other countries

supportpayprogramarabicssn[.]ga
tkkmobileinternetssnstop[.]ml
tkkmobileinternetssnstopopen[.]gq
amende-police-4412[.]xyz
gropirworldplssn[.]ga

- Google Chrome
- Malware Technologies
- Ransomware

Authors



AMR

Browser lockers: extortion disguised as a fine

Your email address will not be published. Required fields are marked *