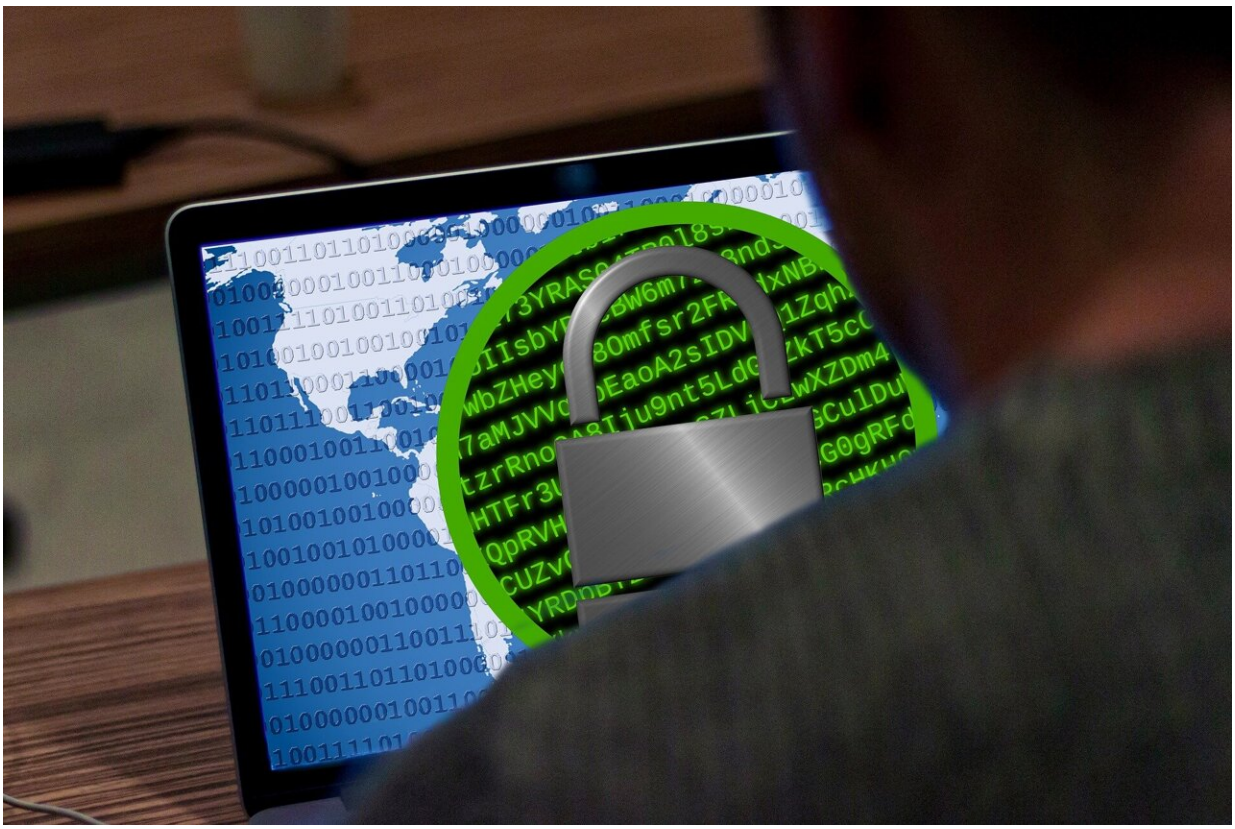
Cybersecurity researchers spotlight a new ransomware threat—be careful where you upload files

April 29 2024, by Selcuk Uluagac



Credit: Pixabay/CC0 Public Domain

You probably know better than to click on links that download unknown files onto your computer. It turns out that uploading files can get you

into trouble, too.

Today's web browsers are much more powerful than earlier generations of browsers. They're able to manipulate data within both the browser and the computer's local file system. Users can send and receive email, listen to music or watch a movie within a browser with the click of a button.

Unfortunately, these capabilities also mean that hackers can find clever ways to abuse the browsers to trick you into letting ransomware lock up your files when you think that you're simply doing your usual tasks online.

I'm a computer scientist who studies cybersecurity. My colleagues and I have shown how hackers can gain access to your computer's files via the File System Access Application Programming Interface (API), which enables web applications in modern browsers to interact with the users' local file systems.

The threat applies to Google's Chrome and Microsoft's Edge browsers but not Apple's Safari or Mozilla's Firefox. Chrome accounts for 65% of browsers used, and Edge accounts for 5%. To the best of my knowledge, there have been no reports of hackers using this method so far.

My colleagues, who include a Google security researcher, and I have communicated with the developers responsible for the File System Access API, and they have expressed support for our work and interest in our approaches to defending against this kind of attack. We also filed a security report to Microsoft but have not heard from them.

Double-edged sword

Today's browsers are almost operating systems unto themselves. They can run software programs and encrypt files. These capabilities,

combined with the browser's access to the host computer's files—including ones in the cloud, shared folders and external drives—via the File System Access API creates a new opportunity for ransomware.

Imagine you want to edit photos on a benign-looking free online photo editing tool. When you upload the photos for editing, any hackers who control the malicious editing tool can access the files on your computer via your browser. The hackers would gain access to the folder you are uploading from and all subfolders. Then the hackers could encrypt the files in your file system and demand a ransom payment to decrypt them.

Ransomware is a growing problem. Attacks have hit individuals as well as organizations, including Fortune 500 companies, banks, cloud service providers, cruise operators, threat-monitoring services, chip manufacturers, governments, medical centers and hospitals, insurance companies, schools, universities and even police departments. In 2023, organizations paid more than US$1.1 billion in ransomware payments to attackers, and 19 ransomware attacks targeted organizations every second.

It is no wonder ransomware is the No. 1 arms race today between hackers and security specialists. Traditional ransomware runs on your computer after hackers have tricked you into downloading it.

New defenses for a new threat

A team of researchers I lead at the Cyber-Physical Systems Security Lab at Florida International University, including postdoctoral researcher Abbas Acar and Ph.D. candidate Harun Oz, in collaboration with Google Senior Research Scientist Güliz Seray Tuncay, have been investigating this new type of potential ransomware for the past two years. Specifically, we have been exploring how powerful modern web

browsers have become and how they can be weaponized by hackers to create novel forms of ransomware.

In our paper, RøB: Ransomware over Modern Web Browsers, which was presented at the USENIX Security Symposium in August 2023, we showed how this emerging ransomware strain is easy to design and how damaging it can be. In particular, we designed and implemented the first browser-based ransomware called RøB and analyzed its use with browsers running on three different major operating systems—Windows, Linux and MacOS—five cloud providers and five antivirus products.

Our evaluations showed that RøB is capable of encrypting numerous types of files. Because RøB runs within the browser, there are no malicious payloads for a traditional antivirus program to catch. This means existing ransomware detection systems face several issues against this powerful browser-based ransomware.

We proposed three different defense approaches to mitigate this new ransomware type. These approaches operate at different levels—browser, file system and user—and complement one another.

The first approach temporarily halts a web application—a program that runs in the browser—in order to detect encrypted user files. The second approach monitors the activity of the web application on the user's computer to identify ransomware-like patterns. The third approach introduces a new permission dialog box to inform users about the risks and implications associated with allowing web applications to access their computer's file system.

When it comes to protecting your computer, be careful about where you upload as well as download files. Your uploads could be giving hackers an "in" to your computer.