I.T. RIGHT *Information Technology Solutions that Work for Local Government*

"Bad Rabbit" Ransomware Attacks

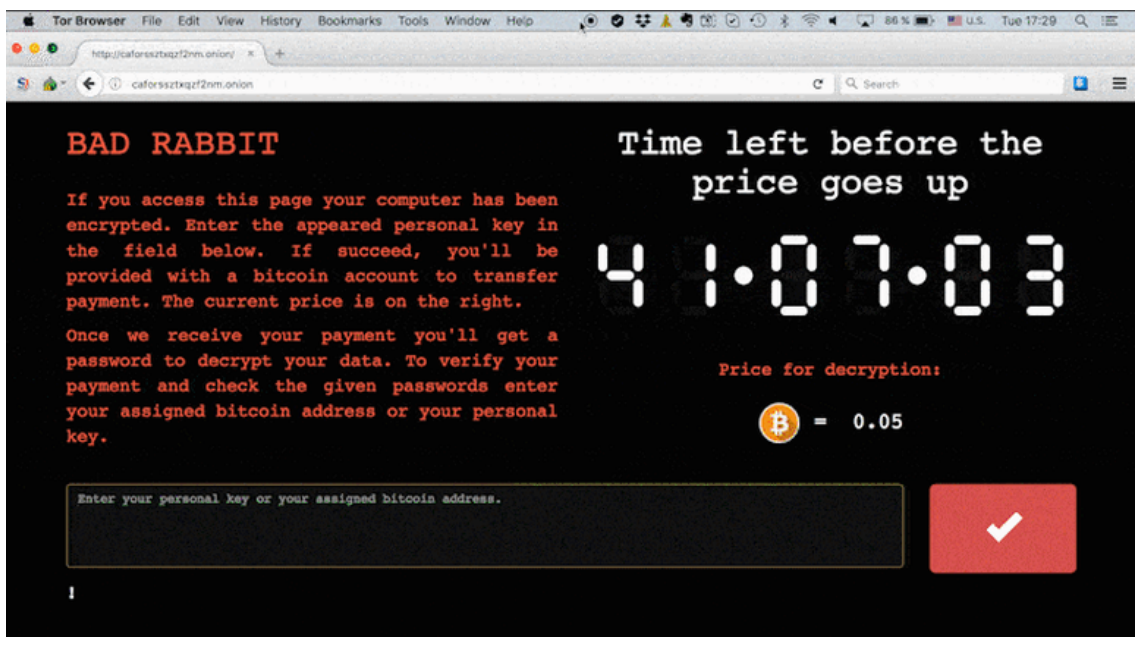
On October 24th a new strain of ransomware, dubbed "Bad Rabbit," has detected masquerading as an Adobe Flash update. Current estimates put the number of infected systems at 200, and the majority of these are in Russia and Eastern Europe. Please follow our advice below, because it will help secure your network against Bad Rabbit.

How To Avoid Getting Infected

- **Make sure that your users know not to download installers from any sites without express permission from IT, and to avoid insecure sites entirely.**
- **Do not update Adobe Flash. We recommend that you have Adobe Flash uninstalled.**
- **If you suspect you've been infected, drop everything and follow our instructions below.**

What To Do If You Get Infected

- **Stop immediately and call your IT Professionals. Do not remove the virus or run software that could possibly remove the virus. The virus should only be removed AFTER backups have been verified good/restored.**
- **Call your IT Professionals *immediately*. This virus has a 40 hour count down timer. After 40 hours it becomes much more difficult and expensive to deal with.**
- **If you know what you clicked on that caused it, fess up. It is a huge help to us to know how it happened, both in cleaning up and preventing future infections.**
- **Don't feel badly. Many of the smartest people we know have fallen victim to computer viruses. You are not the first and will not be the last virus call we ever take. Remember that we are here to help, and that any frustration you hear in our voice is directed at the criminals who attacked your network.**



More About Bad Rabbit

Using insecure websites as a channel for what is called a "drive-by attack," the hackers behind Bad Rabbit plant false Adobe Flash installers for unsuspecting users to click. Because of the ubiquity of Flash updates, users are less likely to suspect a trap.

For the attack to work, users must click on the installer. Unclicked, nothing will be downloaded and the attack is harmless. If it is clicked, the installer will download ransomware and lock the computer, encrypting all available files and spreading laterally across the network. Users are then given about 40 hours to pay the given fee and get their data decrypted.

Bad Rabbit has been compared to the WannaCry and NotPetya attacks earlier this year. While the scope is smaller, it appears that the attack is more targeted than its predecessors. **Please remember, think before you click and avoid updating Flash.**