



Wisconsin Statewide Intelligence Center (WSIC)

608.242.5393 • 888.DCI.WSIC • Fax: 608.240.3592 • wsic@doj.state.wi.us



TLP: WHITE

WSIC Analytic Note

June 7, 2021


The Wisconsin Statewide Intelligence Center (WSIC) has developed this intelligence product based on information from multiple trusted third parties. If you have information or suggestions for future products, please e-mail wsic@doj.state.wi.us

60-Second Survey: *The WSIC is constantly working to improve the quality and relevance of our products. We encourage recipients of this product to provide feedback (both positive and negative) via the following link: <https://www.surveymonkey.com/r/WSICAnalyticalReport>.*

TLP:WHITE: Disclosure is not limited. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.¹



Ransomware Alert from Wisconsin Department of Administration

WSIC Comment: The Wisconsin Department of Administration (DOA), Division of Enterprise Technology (DET) authored the alert below. WSIC concurs with the content of the alert. In addition to the mitigations mentioned below, WSIC encourages Wisconsin organizations to strongly consider adding multifactor authentication anywhere employees provide credentials. The White House recently published a memorandum addressed to corporate executives and business leaders on the topic of ransomware. That letter is attached here for additional reference: 

Alert from WI DOA²: Ransomware attacks making national news highlight a growing threat for Wisconsin organizations. Criminals are using ransomware as a method to make money. In numerous cases, ransomware attacks have targeted counties, municipalities, law enforcement and courts, and especially K-12 schools. Some ransomware groups focus on targets that the criminals deem “easier” to attack, or who are deemed vulnerable based on automated scanning. Think of a car thief – who will keep searching, until finding the car that is sitting unlocked with the keys in the visor.

How can you become infected: A malicious link or attachment in an email message; infected websites; fake apps; malicious ads on legitimate websites, or leaked credentials. Once your machine is infected, ransomware can encrypt all manner of files, from documents to pictures and videos. It can encrypt your data, lock you out of your operating system, and spread to other computers on the network.

To get your data back, the criminals usually request payment in cryptocurrency, such as Bitcoin, because it is perceived as harder to trace. Another hallmark of ransomware is to give you a short time-limit to pay the ransom or risk losing your data forever.

TLP:WHITE

We that you take the following precautions to help protect yourself.

1. Ensure you have an offline backup of your critical data. Backup everything, every day: However, you must know how to back up your data correctly. This means backing up your data into the cloud – or on a local storage device that is offline and not directly connected to your system. If you backup your data to an external hard drive, only connect the hard drive when backing up your data, then immediately disconnect it.
2. Apply security patches to all your applications as quickly as possible.
3. Do not click suspicious attachments, links, or ads.
4. Ensure anti-virus is present and updated on each endpoint and server.
5. Develop a disaster recovery plan (DRP): A DRP can help you spring into action during a host of different emergencies, from hackers to hailstorms. Here are some steps you might include in a DRP for a ransomware attack: Shut down most of the organization’s network immediately to prevent infection from spreading; Shut down Wi-Fi and Bluetooth right away.
6. Contact the DOA Help Desk at 608-267-6930 if you believe you are a victim of ransomware.

Reporting Notice: To report suspicious activity to the WSIC, please visit <https://wifusion.widj.gov/>.

For Administrative Purposes Only:
Produced: W13C10A8
Contributed: D1C0I7SO
Reviewed: W19C13A16; W19C12A6S

Sources:

¹ FIRST, Undated, *TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance – Version 1.0*, <https://www.first.org/tlp/>

² Email from WI DOA DET employee to WSIC Employee, June 3, 2021, *Ransomware Alert Draft*.