HB 635

Department of Legislative Services

Maryland General Assembly
2020 Session

FISCAL AND POLICY NOTE
First Reader

House Bill 635 (Delegate Cox)
Judiciary

Criminal Law - Crimes Involving Computers - Malware and Ransomware

This bill prohibits a person from knowingly possessing "ransomware" or "malware" with the intent to use either for specified purposes and establishes criminal penalties for violations. Violators are guilty of a misdemeanor, punishable by imprisonment for up to 10 years and/or a $10,000 maximum fine. The bill applies prospectively to any cause of action arising on or after the bill's October 1, 2020 effective date.

Fiscal Summary

State Effect: Potential minimal increase in general fund revenues and expenditures due to the bill's penalty provision.

Local Effect: Potential minimal increase in local revenues due to the bill's penalty provision. The bill is not expected to materially affect local expenditures.

Small Business Effect: None.

Analysis

Bill Summary: With the exception of the use of ransomware or malware for research purposes, a person may not knowingly possess ransomware or malware with the intent to introduce the ransomware or malware into the computer, computer network, or computer system of another person without the authorization of the other person.

"Ransomware" means a computer or data contaminant, encryption, or lock that (1) is placed or introduced without authorization into a computer, a computer network, or a computer system and (2) restricts access by an authorized person to a computer, computer

data, a computer network, or a computer system in a manner that results in the person responsible for the placement or introduction of the contaminant, encryption, or lock demanding payment of money or other consideration to remove the contaminant, encryption, or lock.

"Malware" means a computer or data containment that is designed to (1) disrupt or deny operation of an authorized person to a computer, computer data, computer network, or a computer system; (2) gather information that leads to loss of privacy or exploitation; or (3) gain unauthorized access to system resources. Malware includes spyware.

Current Law: Under § 7-302 of the Criminal Law Article, a person may not intentionally, willfully, and without authorization, access or attempt to access, cause to be accessed, or exceed the person's authorized access to all or part of a computer or a computer network, language, software, system, service, or database.

Also, a person may not intentionally, willfully, and without authorization, copy, attempt to copy, possess, or attempt to possess the contents of all or part of a computer database that was unlawfully accessed. A violation of these provisions is a misdemeanor, and the violator is subject to maximum penalties of imprisonment for three years and/or a fine of $1,000.

A person may not intentionally, willfully, and without authorization, commit unlawful access or attempted access, as specified, with the intent to (1) cause the malfunction or interruption of any or all parts of a computer, network, language, software, service, or data; (2) alter, damage, or destroy all or any part of data or a program stored, maintained, or produced by a computer, network, software, system, service, or database; or (3) possess, identify, or attempt to identify a valid access code or publicize or distribute a valid access code to an unauthorized person.

If the aggregate amount of the loss is $10,000 or more, the violator is guilty of a felony and is subject to maximum penalties of imprisonment for 10 years and/or a fine of $10,000. If the aggregate loss is less than $10,000, the violator is guilty of a misdemeanor and is subject to maximum penalties of imprisonment for 5 years and/or a fine of $5,000.

Under § 7-302(c)(4) of the Criminal Law Article, a person may not gain or attempt to gain unauthorized access to computer services with the intent to interrupt or impair the functioning of (1) State government; (2) a service provided in the State by a public service company; or (3) a natural gas or electric service, device, or system provided in the State by a person other than a public service company.

If the aggregate amount of the loss associated with this prohibition is $50,000 or more, a violator is guilty of a felony and subject to maximum penalties of 10 years imprisonment and/or a $25,000 fine. If the aggregate loss is less than $50,000, a violator is guilty of a

misdemeanor and is subject to maximum penalties of 5 years imprisonment and/or a $25,000 fine.

Access achieved in a prohibited manner under a single scheme or a continuing course of conduct may be considered one violation. A defendant may be tried in any county in Maryland where the act was performed or the accessed computer was located.

Background: Malware attacks typically involve the introduction of software or firmware to compromise the integrity or confidentiality of an information system. Malware attacks are usually intended to disrupt the operations of their victims or access sensitive information, sometimes for financial gain.

Ransomware attacks are an increasingly popular method in which individuals, who are often hackers based overseas, use software viruses to assume control of or encrypt computers, data stored in computers, or computer networks and refuse to release control of the computers or data unless a ransom is paid, often through the Internet currency Bitcoin. Unpaid ransoms can result in escalating demands or permanent loss of data. Victims of ransomware attacks include ordinary citizens, small businesses, public libraries, hospitals, local governments, and larger businesses/entities. Because the perpetrators are often based overseas, there is very little local and federal law enforcement can do, especially within the narrow window of time in which victims must pay a ransom.

In March 2016, computers at MedStar Health, a prominent health care system in the Maryland/Washington, DC area, were attacked by a virus that blocked some users from logging into its system. MedStar employees reported seeing pop-up screens on their computers demanding payment in Bitcoin. MedStar responded to the attack by shutting down extensive portions of its computer network. In November 2018, two Iranian hackers were charged in federal court in connection with the attack against MedStar and attacks against several other entities, including the cities of Atlanta, Georgia, and Newark, New Jersey; the Colorado Department of Transportation; the Port of San Diego; and other health care companies. The two hackers, who are believed to be in Iran, are alleged to have accessed computer networks remotely, installed ransomware on the networks, and demanded payment from their victims in return for unlocking data. According to prosecutors, their efforts netted $6 million and caused their victims to lose at least $30 million.

The Federal Bureau of Investigation (FBI) estimates that ransomware payments in 2016 totaled $1 billion, a significant increase from the $24 million in estimated payments during 2015. In an attempt to understand the scope of ransomware attacks and develop solutions and approaches to attacks, the FBI issued an alert in September 2016 asking victims to file reports through its Internet Crime Complaint Center. The lucrative nature of the attacks has created a growth industry within criminal networks, with reports of ransomware

applications and toolkits being available for purchase and "ransomware as a service," through which individuals can purchase time on a criminal network designed to launch attacks in return for paying the network provider a percentage of the extorted funds.

On January 9, 2019, the Salisbury Police Department was the victim of a ransomware attack. According to news reports, as of January 24, 2019, some data remained inaccessible. However, a backup system prevented the loss of data.

On May 7, 2019, approximately 7,000 Baltimore government employees were denied access to their computers due to a ransomware attack that seized operation of their devices. Those persons withholding access to the computers demanded roughly $100,000 in Bitcoin from Baltimore City officials for them to relinquish control. Baltimore City went weeks without major services caused by inaccessibility of critical systems involved in the attack. In May 2019, the city's budget office estimated that the attack cost approximately $18 million ($10 million for restoring and repairing computer networks and $8 million in potential lost or delayed revenues).

Additional Information

Prior Introductions: SB 151 of 2019, a similar bill, received a hearing in the Senate Judicial Proceedings Committee, but no further action was taken on the bill. Its cross file, HB 211, received a hearing in the House Judiciary Committee, but no further action was taken on the bill.

Designated Cross File: None.

Information Source(s): Baltimore City; Baltimore, Garrett, and Montgomery counties; City of Laurel; Maryland State Commission on Criminal Sentencing Policy; Judiciary (Administrative Office of the Courts); Office of the Public Defender; Department of State Police; Maryland State's Attorneys' Association; Department of Public Safety and Correctional Services; *The Baltimore Sun; The New York Times; The Washington Post;* Federal Bureau of Investigation; National Institute of Standards and Technology*;* Department of Legislative Services.

Fiscal Note History: First Reader - February 16, 2020
af/aad

Analysis by: Donavan A. Ham

Direct Inquiries to:
(410) 946-5510
(301) 970-5510