Ransomware Attacks on Court Systems May Affect Background Screening Processes

Technological advancements in recent years have significantly changed the way businesses and other entities function. One such change is in access to and storage of data – data access and storage has mostly moved from a paper-based to an electronic format. Electronic access and storage of data has created many benefits for organizations, including convenience and increased operational efficiencies. Nevertheless, these benefits do not come without new risks.

Electronically-stored data can be accessed and modified from different locations by individuals who are authorized to access that data. However, if security measures are lacking or inadequate, unauthorized actors with nefarious purposes may also gain access to the data. Recently, ransomware attacks – or attacks using a type of malicious software designed to block access to a computer system until money is paid[1] – have increased in prevalence. According to the Federal Bureau of Investigation (FBI), in 2020, there were 2,474 reported incidents of ransomware attacks with adjusted losses of over $29.1 million.[2] These attacks have targeted various types of businesses and entities, including court systems and state and local governments.

The FBI implemented the Internet Crime Complaint Center (IC3) to investigate all cybercrime reports, including those involving ransomware, and to provide the public with information on cyber-criminal activity. The FBI urges for all organizations to report ransomware incident to a local field office of the IC3.

What is Ransomware?

Ransomware is a form of malware that targets an organization's critical data and systems for the purpose of extortion.[3] Attackers use encryption to lock up a victim's files, and then hold the files hostage until payment is made, typically in a hard-to-trace digital currency. Often, an attacker is able to encrypt all of the data on a network just by gaining access to one computer that is part of the network.

1 *2018 Internet Crime Complaint Center Annual Report*, Federal Bureau of Investigation, https://pdf.ic3.gov/2018_IC3Report.pdf.

2 *2020 Internet Crime Report,* Federal Bureau of Investigation, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

3 *How to Protect Your Networks from Malware*, U.S. Federal Agencies, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view?47.

Ransomware variants are continuously changing. In August 2019, a malicious software called "Ryuk" was the most common form of ransomware used in attacks. According to Coveware, a cybersecurity firm, Ryuk was used in roughly 24 percent of ransomware attacks in the second quarter of 2019.[4] In a recent study assessing Q1 of 2021, a variant known as Sodinokibi was named the most common form of ransomware.[5]

How Does a Ransomware Attack Happen?

> One commonly used vector for ransomware attacks is a spear phishing email -- a kind of email spoofing in which an unsuspecting recipient opens an email that looks to be from a trusted source.

The email then rapidly encrypts the files on the network. The cyber-attacker then sends a message to the user that the computer's files, photos, databases, and other vital systems have been encrypted. The message includes a demand for ransom payable through a form of untraceable cryptocurrency before keys are provided to unencrypt the files and restore functionality.

Ryuk ransomware attacks are specifically designed to get deep into the systems of larger organizations and are often orchestrated using a multistep process that can take weeks. A Ryuk attack might start with a phishing email, providing attackers with the access needed to install software that can discretely collect information about the network and any necessary credentials. The attackers then use the acquired information to disable antivirus protections and install the Ryuk ransomware, locking the files and network.[6]

Sodinokibi ransomware attacks are unique in that the payments are typically lower than those from the average ransomware because the collection sites automate a large amount of the hacker costs.[7] Sodinokibi can affect both small and large companies, and scale the ransom amount depending on the size of the organization. As of May 2021, the average Sodinokibi ransom payment was $124,499, with incident lengths averaging around 19 days. The attackers commonly use Remote Desktop Protocol as an attack vector.[8]

Options when Faced with a Ransomware Attack

An entity facing a ransomware attack generally has two options: 1) pay the ransom; or 2) try to restore access to the locked files without paying the ransom. According to Recorded Future, a cyber-threat intelligence company, only 17 percent of attacked cities pay the ransom set by the hackers.[9] Paying the ransom is a risk as it may embolden the cyber-attackers to continue attacks on other entities and does not guarantee that the cyber-attackers will restore access to the files. In the alternative, refusing to pay the ransom and instead choosing to try to unencrypt the files often takes more time and costs more money. Some entities have been able to quickly recover from attacks by ensuring secure backup files are in place that can be used to restore access. Additionally, entities can purchase insurance that covers ransomware and other cyberattacks in order to provide themselves with some protection in the event of such an attack.

---

4 *Ransomware Amounts Rise 3x in Q2 as Ryuk & Sodinokibi Spread*, COVEWARE, www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread

5 *Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound*, COVEWARE, https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

6 Jon Kamp & Scott Calvert, *How Ransomware Attacks Are Forcing Big Payments From Cities, Counties*, The Wall Street Journal (July 25, 2019), www.wsj.com/articles/how-ransomware-attacks-are-forcing-big-payments-from-cities-counties-11564078222?mod=searchresults&page=1&pos=1.

7 *Sodinokibi Ransomware Recovery, Payment & Decryption Statistics*, COVEWARE, https://www.coveware.com/sodinokibi-ransomware

8 *Id.*

9 Joseph Marks, *The Cybersecurity 202: Baltimore's slow recovery shows far-reaching consequences of ransomware*, The Washington Post (May 22, 2019), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/05/22/the-cybersecurity-202-baltimore-s-slow-recovery-shows-far-reaching-consequences-of-ransomware/5ce4a910a7a0a46b92a3fd6d/?utm_term=.8e7aad08fb55.

In July 2019, the U.S. Conference of Mayors -- an organization comprised of mayors representing cities with populations of 30,000 or more -- adopted a resolution opposing payment of any ransoms demanded through ransomware attacks.[10] This follows the FBI's recommendation that entities not pay ransoms demanded in ransomware attacks.[11]

How to prevent an attack

The Cybersecurity and Infrastructure Security Agency (CISA) recently provided guidance for government agencies and private companies for preventing ransomware attacks. The CSIA encourages organizations to implement recommendations from its fact sheet to reduce the risk to ransomware and protect personal information.[12] Some of the key recommendations to implement include:

- Ensuring antivirus and anti-malware software and signatures are up to date
- Implementing application allowlisting
- Ensuring user and privileged accounts are limited through account use policies, user account control, and privileged account management
- Employing MFA for all services to the extent possible, particularly for webmail, virtual private networks (VPNs), and accounts that access critical systems

The CSIA further recommends that entities maintain offline, encrypted backups of data and regularly test the backups. Entities should also create and maintain a basic cyber incident response plan, resiliency plan, and associate communications plan.

Ransomware Attacks on Governments and Court Systems

State and local governments are particularly vulnerable to ransomware attacks because they may have inadequate IT resources and their IT systems tend to be older and outdated. [13] [14] Attacks on governments also tend to draw more attention because they can disrupt public services.[15] Recorded Future reports that since 2013, there have been an estimated 169 ransomware attacks on state and local governments.[16] However, the exact number of attacks against governments is unknown because state and local governments do not always publicly report the attacks. Malwarebytes, a company that specializes in cybersecurity, reported that its government clients experienced seven times more ransomware attacks so far in 2019 than in all of 2018.[17]

In July 2019, Georgia's Administrative Office of the Courts suffered a ransomware attack that affected the state's municipal courts. In June 2019, Riviera Beach and Lake City in Florida were attacked and paid ransom demands of roughly $600,000 and $460,000, respectively.[18] In

10 Jon Kamp, *U.S. Mayors Unite Against Paying Ransom to Hackers*, The Wall Street Journal (July 10, 2019), www.wsj.com/articles/u-s-mayors-unite-against-paying-ransom-to-hackers-11562774950?mod=searchresults&page=1&pos=3; *Opposing Payment To Ransomware Attack Perpetrators*, U.S. Conference of Mayors (July 2019), http://legacy.usmayors.org/resolutions/87th_Conference/proposedcommittee-preview.asp?committee=Criminal%20and%20Social%20Justice.

11 *Incidents of Ransomware on the Rise: Protect Yourself and your Organization*, Federal Bureau Of Investigation (April 29, 2016), www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise.

12 *Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches*, Cybersecurity and Infrastructure Security Agency (CISA) (August 25, 2021) https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf

13 Ian Duncan & Colin Campbell, *Baltimore City Government Computer Network Hit by Ransomware Attack*, Baltimore Sun (June 30, 2019), www.baltimoresun.com/politics/bs-md-ci-it-outage-20190507-story.html.

14 Marks, *supra* note 6.

15 Kamp & Calvert, *supra* note 5.

16 Allan Liska, *Early Findings: Review of State and Local Government Ransomware Attacks,* Recorded Future (May 10, 2019), https://go.recordedfuture.com/hubfs/reports/cta-2019-0510.pdf.

17 Talal Ansari, *How One Texas County Stopped a Ransomware Attack,* The Wall Street Journal (Aug. 30, 2019), https://www.wsj.com/articles/how-one-texas-county-stopped-a-ransomware-attack-11567169059.

18 CBS News, *Georgia Court System Struck by Ransomware Attack*, CBS Interactive Inc. (July 2, 2019), www.cbsnews.com/news/georgia-court-system-attacked-by-hackers-using-ransomware-malware-software/.

May 2019, there was a ransomware attack in Baltimore, its second in two years.[19] In March 2019, Jackson County, Georgia paid attackers $400,00 after a ransomware attack locked agencies out of almost all of their systems, including the sheriff's office, which is responsible for criminal bookings.[20] Additionally, around the same time, a large ransomware attack in Atlanta shut down online city services, required police and courts to file paperwork manually, and forced the city to halt court proceedings. The attack cost the city's taxpayers more than $9 million.[21]

Most recently, Colonial Pipelines suffered a large ransomware attack that shut down the company's operational systems entirely and led to fuel shortages across the East Coast. This outcome was entirely the result of a compromised password that gave hackers access into the Colonial Pipeline network. The hackers stole 100 gigabytes of data and threatened to leak the information if Colonial did not pay. Colonial ended up paying the cybercrime group, DarkSide, $4.4 million in ransom.[22]

Other jurisdictions and systems that have been attacked include, but are not limited to:

- Albany, New York;
- Cartersville, Georgia;
- Collierville, Tennessee;
- Connecticut Court System;
- Fisher County, Texas;
- Georgia State Patrol;
- Genesee County, Michigan;
- Greenville, North Carolina;
- Imperial County, California;
- LaPorte County, Indiana;
- Lynn, Massachusetts.

Ransomware's Impact on Governments and Court Systems

The exact impact on governments and court systems varies depending on the systems affected by the ransomware and the security measures that are in place. For example, the Albany Policy Department was forced to write down incident and crime reports on paper during an attack. The Fisher County Sheriff's Office lost the ability to connect to a Texas statewide law enforcement database.[23]

State and local governments can be affected for months or even longer during and after an attack. Atlanta reported that for three months after the attack, courts were still processing cases by hand. In Baltimore, the Mayor believes full recovery could take months after its ransomware attack in May.

> However, the best way for governments to defend against a ransomware attack is to "avoid it altogether, by investing resources into giving employees phishing training, updating and patching software, and developing a way to restore data from secure backups in the event of a crisis."[24]

19 The first attack shut down the automated system that Baltimore emergency workers use to locate people who call 911 for assistance. *See* Emily Sullivan, *Ransomware Cyberattacks Knock Baltimore's City Services Offline*, NPR (May 21, 2019), www.npr.org/2019/05/21/725118702/ransomware-cyberattacks-on-baltimore-put-city-services-offline.

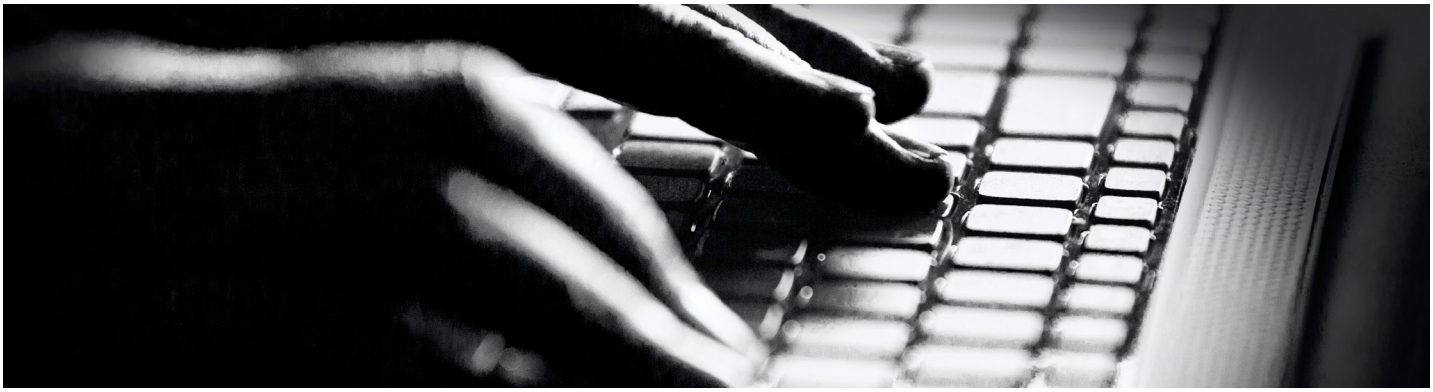
20 Linn E. Freedman, *Jackson County, Georgia Pays Hackers $400,000 After Ransomware Attack*, The National Law Review (March 14, 2019), https://www.natlawreview.com/article/jackson-county-georgia-pays-hackers-400000-after-ransomware-attack.

21 Marks, *supra* note 6.

22 William Turton & Kartikay Mehrota, *Hackers Breached Colonial Pipeline Using Compromised Password*, Bloomberg (June 4, 2021), https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

23 Kevin Collier, *Crippling ransomware attacks targeting US cities on the rise*, CNN (May 10, 2019), https://www.cnn.com/2019/05/10/politics/ransomware-attacks-us-cities/index.html.

24 Ben Kochman, *Ransomware Wave Has Cos., Gov'ts Scratching Their Heads*, Law360 (Sept. 9, 2019), https://www.law360.com/cybersecurity-privacy/articles/1194829/ransomware-wave-has-cos-gov-ts-scratching-their-heads.



Governments and court systems that follow the FBI's security recommendations, including more frequent security-patch updates and secure backup files, have a better chance of stopping the attacks in the early stages.[25] When Collierville, Tennessee was hit with a Ryuk attack, the town was able to recover files from backup systems and rebuild necessary servers within a week.[26] Imperial County, California was able to avoid a $1.2 million ransom demand by having secure backup data.[27]

Similarly, Lubbock County was one of 23 local government systems in Texas hit by a ransomware attack on August 16, 2019.[28] When Lubbock County's in-house director of technology and information systems received a call from a county employee claiming file icons on a computer screen were changing, the IT director immediately suspected malicious activity. The director instructed one of his staff to rush to the affected computer and take it off the network. "Within 40 minutes of witnessing the first signs of a ransomware attack, the threat was over."[29] Lubbock County "appears to be the only one that successfully stopped the hackers, saving the county potentially hundreds of thousands of dollars and hours of work to repair computers and restore lost files."[30] The Lubbock County IT department was lauded for catching the attack at such an early stage, with county officials pointing to the proper investment in infrastructure and the regular trainings the county's roughly 1,500 employees receive on suspicious computer activity.[31]

What This Means for Background Screening

It is impossible to predict when and where a ransomware attack will occur or the exact effect it will have. If a court system is affected by ransomware, it can cause court records to be inaccessible for an unknown period of time. Thus, employers who rely on court searches when screening applicants and employees should be aware that some of those searches could be delayed indefinitely if the court is hit with a ransomware attack and thus should plan accordingly.

If you have questions regarding availability of a particular court search, please contact your account manager or sales executive.

25 Kamp & Calvert, *supra* note 5.

26 *Id.*

27 *Id.*

28 Ansari, *supra* note 13.

29 *Id.*

30 *Id.*

31 *Id.*