Volume 104 Number 3 | Fall/Winter 2020-21
Judicature
BOLCH JUDICIAL INSTITUTE
Published by the Bolch Judicial Institute at Duke Law.
JUDICATURE.DUKE.EDU

Contracting the Virus: Not if, but when

In the early months of the COVID-19 outbreak, the Texas judiciary focused on its response to the global pandemic. The Office of Court Administration (OCA), the judicial branch agency tasked with providing resources and assistance to the Texas state courts, released its guidance on how courts could safely resume in-person proceedings starting June 1.

However, despite social distancing measures, moving the court's hearings and operations online, and vigorous handwashing, another virus wreaked havoc in the Texas courts during May of this year. This virus spread with ease and alarming speed from one office to the next, bringing the court's ability to function to a halt. Instead of attacking immune systems, this new virus, known as the Netwalker, infected nearly all of the judiciary's computers and servers, threatening the integrity of the entire technological system — a system that had become even more important because of COVID-19. Within several hours, 85 percent of the court's servers were destroyed.

The attack

For many years, OCA has provided direct technological support for Texas' state appellate courts and judicial branch agencies, including the machines on desks, data storage systems, and statewide technology solutions for the trial courts. At approximately 3 a.m. on May 8, 2020, the courts' computer systems came to a crashing halt when an unknown foreign attacker infiltrated the OCA-supported network. Once inside, the attacker deployed a ransomware variant called Netwalker to all devices connected to the judiciary's network.

Netwalker, believed to have been created by a group of likely Russian hackers, is distributed as "ransomware-as-a-service," meaning that the owner of the ransomware provides others with the means to deploy the ransomware.[1] Through this distributed model, many people can access the tools necessary to leverage an attack. Once deployed, Netwalker encrypts all the files on the targeted network and deletes any stored backups. Each file on the computer is encrypted with a specific five-digit key at the end of the filename (such as Article.pdf.ds14g), effectively locking each document from use. A readable ransom note file is left on each device informing the computer's user of the ransomware, directing the user to a dark-website to obtain instructions on how to decrypt the files in exchange for payment, and providing a customer service webpage (in Russian) if the user has any follow-up questions. This variant of the Netwalker ransomware was new at the time of the Texas attack, and the anti-virus protection systems on the OCA network were unable to detect the attack as it occurred.

At 6:45 a.m., a few hours after the attack commenced, OCA technology staff received the first report of a problem from a user who was unable to open files on her computer. Within an hour of the first report, OCA disabled the network to prevent further damage. But the damage was already done — 142 of the court's 167 servers (85 percent) had been destroyed. Luckily, due to the COVID-19 pandemic, many of the one thousand users affected had brought their computers home and had disconnected from the network, so only 45 percent of the court's computers were directly impacted.

The damage varied by court and agency, with some seeing little impact and others left with little capacity to function normally. The appellate courts' case management system was completely disabled, and related technology systems prevented the courts from receiving appellate records. By contrast, the attack did not seem to impact cloud-based technology solutions, such as the state's electronic filing system or documents that had already been uploaded to the cloud.

In fact, the court's use of the cloud was a significant mitigating factor. Several years ago, OCA began backing up data from most of the network in two places: on-site and in a cloud-based vault. The ransomware attack corrupted the on-site backups, but did not affect the daily cloud backups. While not all the network data was backed up to the cloud,[2] these replications were current through the evening prior to the attack, meaning that OCA could restore most of the corrupted data.

Still, OCA immediately brought in several outside cybersecurity experts and law enforcement agencies to assist in investigating and responding to the ransomware attack. The response involved three phases: investigation, remediation, and recovery. During the investigation phase, law enforcement and cybersecurity experts searched for the intrusion point and for other remnants of the attack that could later disable the network again. While the investigation continued, the network remained disabled to prevent further damage. The investigation lasted nine long days, but the experts determined that no data had been exfiltrated from the network and confirmed that there were no further active vulnerabilities. Next, the remediation phase began. Due to the damage and the method of intrusion, the Texas judicial branch

network had to be rebuilt essentially from scratch. Once the experts re-established the basic network hardware systems, they began the recovery phase, restoring files and functionality to the users of the system. Overall, the process to restore the functionality of the network lasted close to four months, with much of the functionality returning within the first six weeks.

Lessons learned

The Texas judiciary's experience provides insight into ways that other courts might prepare their own systems for inevitable future attacks:

Plan as if an attack is inevitable. The federal Cybersecurity and Infrastructure Security Agency has reported an increase in ransomware attacks,[3] with at least eight successful attacks on court systems since 2016.[4] In light of these statistics, courts should prepare as if an attack is inevitable, rather than a mere possibility. While taking steps to protect against an attack is prudent, courts should focus equally if not more on how to recover after an attack has already occurred. Courts should also learn how to initiate the immediate deployment of cybersecurity experts when an attack occurs, including procuring contracts for such services in advance.

Don't sacrifice safety for convenience. Many of the steps necessary to protect against an attack inconvenience users. These steps include multi-factor authentication, stronger password requirements, forced computer patching and rebooting, segregated network structures, and limitations on network access points. When balancing the issues, a court should not sacrifice security for convenience.

Back up … and then back up the backups. Is the point strong enough here? The key to successfully recovering from a ransomware attack is having a strong data backup system that ensures that there are copies of the data available from which to restore corrupted data. But having a backup that is inaccessible or can be corrupted is, of course, not sufficient. The court should test and review the backups regularly to ensure all data is being replicated appropriately. Additionally, one copy of the backup should be physically disconnected from the network to ensure that there is no pathway for an attacker to access it.

The appellate courts' case management system was completely disabled, and related technology systems prevented the courts from receiving appellate records. By contrast, the attack did not seem to impact cloud-based technology solutions.

For sunnier days, move data to the cloud. Despite the hesitance by some to move data to "the cloud," the dispersed nature of the data and the built-in replication of the cloud provide additional security from the harm of ransomware. Obviously, courts should consider security, reliability, costs, and other factors as part of any migration to the cloud.[5]

Manage expectations. Courts have become dependent on computer networks to function. A ransomware attack is likely to limit the functionality of a network for weeks, if not longer. It is important that court personnel understand the impact that a ransomware attack will have and make plans for how to function in such an environment.

Realize your weakest link. Our susceptibility to a ransomware attack is heightened by our weakest link — ourselves. It is easy for judges and court employees to fall victim to increasingly sophisticated social engineering tactics, such as phishing, that expose networks to attacks. Training judges and court employees can help, but it is not foolproof.[6]

Court networks are enticing targets for hackers who wish to wreak havoc on and increase distrust of governmental institutions. Understanding the risks of ransomware and preparing for the certain onslaught of attacks is critically important for all court leaders. I hope that other courts can gain from the Texas judiciary's experience, as we all continue to prepare for the inevitable next attack.

DAVID SLAYTON is the administrative director of the Texas Office of Court Administration in Austin, Texas.

1 Alina Georgiana Petcu, *Netwalker Ransomware Explained: What You Need to Know [Updated]*, Heimdal Security (Sept. 9, 2020), https://heimdalsecurity.com/blog/netwalker-ransomware-explained/.

2 The courts of appeals' data was backed-up both on-site at the court of appeals and at OCA. Most of those backups had some level of corruption.

3 Ransomware, Cybersec. & Infrastructure Sec. Agency, *Ransomware Guidance and Resources*, https://us-cert.cisa.gov/Ransomware (last visited Nov. 18, 2020).

4 Tim Starks, *The Cyberthreat to U.S. Courts*, Politico (July 13, 2020, 10:00 AM), https://www.politico.com/newsletters/weekly-cybersecurity/2020/07/13/the-cyberthreat-to-us-courts-789121.

5 Courts considering migration to the cloud should consult the Conference of State Court Administrators-National Association for Court Management Joint Technology Committee's Resource Bulletin on Cloud Computing. *See JTC Resource Bulletin: Cloud Computing*, Joint Tech. Comm. (Dec. 5, 2014), https://www.ncsc.org/__data/assets/pdf_file/0020/17921/cloud-1-0-12-16-2014-final.pdf.

6 The users of the OCA network all received cybersecurity training the month before the attack.