WHAT THE HACK!

Several casinos and gaming firms have become victims of hackers, but how can you make sure your casino is protected?

BY ANDY GOLDBERG

Cache Creek Casino Resort, a beautiful property located just east of Napa County, California, shut itself down on September 20, and remained closed for three full weeks, reopening on October 12. This was not a coronavirus or health-related shutdown, nor was it due to wildfires.

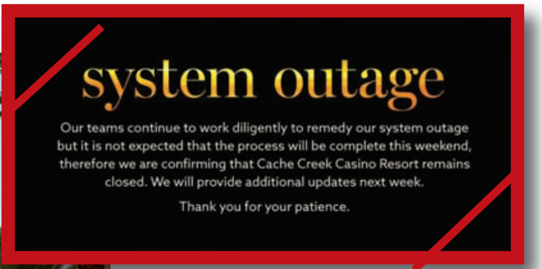
Cache Creek closed down due to a "major computer systems disruption," according to their press releases. Covid-19 has adjusted everyone's idea of "unthinkable," but prior to 2020, a self-imposed, multi-week casino shutdown would certainly have fit that description.

Cache Creek is not an amateur organization. It's a 2,700-slot, 120-table facility with a hotel, golf course, spa and showroom, and presumably, a capable and talented IT department. Although CCCR's public communication lacked specifics, the length of the shutdown—along with reporting from the *Sacramento Bee* that the FBI is investigating—strongly indicates that they were a victim of a "ransomware" attack.

Cache Creek Casino Resort

Ransomware attackers are rarely interested in stealing data per se; their goal is to prevent you from accessing your own data and systems by encrypting everything, then selling back the decryption key. Ransomware attackers migrated from locking up personal computers to corporate networks because they can extort far larger prices from large companies, municipal governments and health systems than from individual users. Ransomware attacks have accelerated greatly, according to a Bitdefender report claiming a sevenfold increase between 2019 and 2020.

This latest attack (actually it may not be the latest, as Clearwater River Casino and It'se Ye-Ye Casino were closed October 12-19 due to "technical difficulties," according to their Twitter feed) can be added to a list that is getting worrisomely long: Four Queens and Binion's in Las Vegas (suspected ransomware), sportsbook vendor SBTech (forced to set aside $30 million), Hard Rock Casino Las Vegas (twice), Eastern Band of Cherokee Indians (confirmed it paid a ransom), MGM Resorts (10 million-plus customer records exposed), Las Vegas Sands (potential $40 million total cost), Affinity Gaming (also twice), multiple national hotel chains, and possibly other casino properties, partners and vendors whose attacks remain undisclosed.



system outage

Our teams continue to work diligently to remedy our system outage but it is not expected that the process will be complete this weekend, therefore we are confirming that Cache Creek Casino Resort remains closed. We will provide additional updates next week.

Thank you for your patience.

OPAQUE PROCESS

Unfortunately, one thing all of these victims have in common is a lack of transparency into what exactly happened. The most powerful action a hacking victim can take to weaken cyberattackers is to share their methods and attack vectors, so similar operators can lock down those vulnerabilities on their own networks.

This isn't sufficient to fully prevent future attacks, because malware authors are constantly getting more sophisticated, but it certainly helps to stop repeats of the same attack at multiple companies within an industry.

Additionally, refusing to reveal details prevents casinos from evaluating the security practices of the system vendors upon which they rely. Casinos integrate CMS, LMS, POS, databases, marketing automation tools, payment processors, kiosks, revenue optimization software, business intelligence platforms, payroll and timekeeping systems, and allow access to internal applications to tons of external service providers, such as Expedia, OpenTable, Ticketmaster, in-room entertainment vendors, Wi-Fi networks, unlock-via-mobile-app providers, even LED lighting controllers, climate-control monitors, housekeeping pollers, and many more.

If any of the cyberattacks can be traced back to a third-party service, or if a specific vendor's software is a common factor among the compromised networks, it is essential to make that information public so other operators can avoid that vendor, or the vendor is pressured into securing its software.

Truthfully, major CMS vendors have made life difficult for security and IT teams for a very long time. Casino management systems are closed, proprietary systems with extremely wide reach into virtually every area of a casino's operations—finance, accounting, marketing, operations, tax compliance, complimentaries—and the underlying database contains all player records, including physical addresses and driver's license information.

Meanwhile, vendors employ many anti-security tactics, such as not sharing source code, storing data in plaintext (rather than utilizing encryption-at-rest), slowly investigating or fixing bugs, not fully documenting all aspects of the software, and severely limiting distribution of that documentation.

THE MOST EFFECTIVE WAY TO THWART A RANSOMWARE ATTACK IS TO HAVE RECENT, COMPREHENSIVE BACKUPS OF ALL DATA, STORED OFFLINE SO THEY AREN'T THEMSELVES ENCRYPTED.

Additionally, inter-system communications (between games, servers and applications) are either entirely proprietary or follow protocols developed by the International Gaming Standards Association, an organization whose lowest membership level costs $11,200. Of course, not every vendor is guilty of every violation here, but none are fully compliant with modern security standards and recommendations.

Because of the lack of access, it's impossible for independent security experts to audit the systems or to perform "pen-testing" (simulated hacking on behalf of the customer to find vulnerabilities that actual hackers would try to exploit). Casinos are essentially beholden to vendors to ensure their products are secure, but have no way to verify they are.

Nor are regulators and auditors much better. Most programs designed to thwart cyberattacks are outdated, many designed well before the existence of modern ransomware.

LACK OF CLARITY

To be clear, there is no proof that any CMS, or any specific vendor's software, has been compromised. The lack of disclosure from any of the victims prevents anyone from knowing. However, when a casino is closed for three weeks, it's fair to assume that attackers got to the heart of the network and its most valuable data.

The most effective way to thwart a ransomware attack is to have recent, comprehensive backups of all data, stored offline so they aren't themselves encrypted. This way, you can restore the backups and ignore the ransom demand (not entirely, as attackers will threaten to sell private data, which is why encryption-at-rest is essential).

Unfortunately, the secrecy surrounding vendor software makes it extremely difficult for a casino to plan or implement a backup and restoration process that is reliable, repeatable, and which can be continuously performed in the background without interrupting normal service. Simply put, if the casino isn't fully informed on how each system works, where the most essential data lies, and what the underlying software stacks are, it's just guessing when it comes to backing up.

Although vendor software usually relies on common, commercial databases (SQL Server, Oracle, DB2, etc.) underneath, casinos can't always utilize those databases' built-in backup or security features, or features provided by reliable third-party vendors and consultants, because the casino is never in full control of the data source and is unsure how it interacts with the application. Whichever CMS system Cache Creek runs, that vendor shouldn't be protected by the casino's silence. If it has become aware of vulnerabilities that could potentially affect other casinos running the same system, it is obligated to warn its other customers and to quickly create and distribute patched software.

The good news is that the gaming industry has strong trade groups and professional organizations, such as the American Gaming Association, National Indian Gaming Association, and many regional groups. Although casinos are generally in fierce competition with each other, when facing an external threat, like cyberattacks, they tend to unify, in partnership with vendors and regulators, to combat the threat together.

If these trade associations choose to take the lead in prioritizing cybersecurity, they have a number of levers to employ. They can pressure attack victims to share details of the attack—how the intrusion started, their full software stack, what vendor systems were compromised, what data was captured, what backups were safe, response from law enforcement, the ransom demands, and the quality of the restoration services (if any), so that other casinos can hopefully prevent an identical attack and can better deal with one if it does happen.

Trade associations can also pressure regulators to insist on full cybersecurity audits, which can only happen when vendors begin to share details on the internals of their code bases, and to only accept certifications from labs with recent, thorough cybersecurity tests, which would force labs to update their mandates, which in turn would require vendors to comply with much stricter security measures.

In addition, trade associations can encourage all parties to invite independent security researchers, software developers and database experts to participate in the review and direction of future system releases and network architectures, with access to common software, tools and protocols without the need to pay huge fees or to deny access to essential components of the systems they are attempting to review, or its documentation.

The alternative to proactively, and collaboratively, defending our industry against cyberattacks is simply to experience an increase in the frequency and severity of such attacks. A ransomware attacker's dream victim is one who pays up and who stays silent. Paying the ransom funds additional developers to find more sophisticated exploits, while the silence ensures that the exact same attack can be duplicated on another victim running the same software.

Given the long list of attack victims, it would be hard to justify a cyberattack as an unforeseen or non-preventable risk in an insurance dispute, or for a casino to not be held liable in the case of personal data exposure.

In the long run, working together to ward off attacks is going to be cheaper than consistently falling victim and paying the price of ransom, emergency data restoration services, the lost income from closing a casino for weeks, and the potential loss of value from losing the customer database entirely.

Andy Goldberg is a database consultant and data scientist dedicated to making casinos smarter and more efficient. He specializes in extracting value from existing databases and casino management systems. His consultancy, Centerfield Nine, is online at www.cfnine.com.