The Desert Sands

Date: 2024-11-27

Handler: Chao Tang

Executive Summary

In February 2014, Sands Corp.’s IT team identified unusual activity across its computing systems, including files being compressed for potential exfiltration. Investigation revealed malware that wiped data on servers and computers, which caused system crashes and significant operational disruption. The attack was contained by disconnecting Sands from the internet to avoid further damage. Approximately three-quarters of Sands' U.S. servers were affected, but international (largely Asia region) systems remained secure. Total financial impact is estimated at over $40 million, considering system replacements and recovery efforts. Operationally, core services were disrupted, but key functions like hotel reservations continued to operate on isolated systems.

Background

The February 2014 cyberattack, code-named “Yellowstone 1”, targeted critical casino computing systems within Las Vegas Sands Corp., causing cascading IT catastrophes and widespread business service disruptions. The attackers, later identified as likely Iranian-based hacktivists, deployed malware that spread through the company’s networks. The attackers infiltrated and compromised multiple systems integral to the operations of Sands' U.S. casino properties. These systems included loyalty rewards programs, the software that manages customer rewards, which is essential for tracking and maintaining customer satisfaction and retention; slot machines and table games monitoring programs, systems used to monitor performance and payout rates, critical for maintaining gaming integrity and compliance; and enterprise storage systems, a multimillion-dollar infrastructure used for data storage and management. This malware attack wiped out about three-quarters of the company’s Las Vegas computer servers, as well as thousands of desktop PCs, laptops, and hard drives. The cascading failures

disrupted day-to-day operations across multiple functions, from customer-facing services to backend operational systems.

The Sands cybersecurity team became aware of the incident on the morning of Monday, February 10, 2014, when logs showed that hackers had begun compressing batches of sensitive files. By then, the malware had already spread extensively, leaving a trail of destruction that wiped out system functionality. Sands security staff responded immediately, isolating affected systems to mitigate further damage. At the time of the attack, Sands' cybersecurity capabilities were under-resourced relative to the scale of its operations. The organization employed only five cybersecurity staff members to protect 25,000 computers. Although the board had approved a major upgrade to cybersecurity tools and staffing in 2013, the project was still in its infancy, leaving the company ill-prepared for a sophisticated attack. Investigators later determined, through computer logs and movement reconstructions, that attackers began probing Sands' network perimeter for vulnerabilities a month before the breach, and the reconnaissance was undertaken without triggering the casino company's notice. Although brute-force attempts to access accounts were detected, these were deemed routine and met with only basic countermeasures, such as adding additional authentication layers so that entering the company's network requires more than just a password. It wasn't until the malware was released that the scale and intent of the attack became evident.

The hackers were not after financial assets or customer credit card data but instead sought to damage the company in retaliation for public comments by Sands' CEO and majority owner, Sheldon Adelson, advocating for military action against Iran. Executives suspected Iranian involvement almost immediately, and post-incident investigations by Dell SecureWorks confirmed the attack was likely carried out by hacktivists within Iran. While there was no conclusive evidence linking the attack directly to the Iranian government, investigators believed it was unlikely the hackers could have operated without its knowledge, given the close scrutiny of Internet use within its borders. Experts worry that America's rivals may have found the sweet spot of cyberwar -- strikes that are serious enough to wound American companies but below the threshold that would trigger a forceful government response. More remarkable still, Sands has managed to keep the full extent of the hack secret for 10 months.

The attack crippled Sands' ability to conduct normal operations. The aftermath includes: customer-facing services, such as loyalty programs and gaming systems, were offline; core IT infrastructure was damaged beyond immediate repair; and sensitive data was compressed and exfiltrated, raising concerns about data breaches. The incident cost Sands $40 million or more to recover data and rebuild systems. The attack served as a stark reminder of the vulnerabilities faced by companies slow to adapt to evolving cybersecurity threats.

Timeline

2018-01-08 – The hackers launched a first, hourlong attack to try to break into the Sands Bethlehem virtual private network.

2018-01-26 – IT managers in Bethlehem, alarmed at the sudden surge in failed login attempts, began a conference call with Sands security managers in Las Vegas.

2018-02-01 – The hackers found a weakness in a Web development server used by Sands Bethlehem to review and test Web pages before they went live.

2018-02-09 – The hackers found the login credentials of a senior computer systems engineer who normally worked at company headquarters but whose password had been used in Bethlehem during a recent trip.

2018-02-10 – The perpetrators released their malware through the company's networks.

2018-02-11 – The hackers took aim at the company's websites, which were hosted by a third party and still running, and defaced them.

2018-02-16 – The hackers took to YouTube, posting an 11-minute video begun by scrolling through a news article that highlighted Adelson's comments about nuking Iran. Then it showed a computer screen packed with thousands of files and folders, with names such as IT Passwords and Casino Credit, which had been pilfered from Sands.

Findings

The attackers gained initial access to Sands' network using brute-force password-cracking software capable of testing thousands of letter combinations per minute. Once they successfully compromised an account, they employed **Mimikatz**, a well-known credential harvesting tool, to extract previously used passwords from compromised systems. Using these credentials, the attackers escalated their privileges and navigated Sands' IT environment (lateral movement), eventually gaining access to key servers in the Las Vegas network.

From within the network, the attackers crafted a small but highly effective malware program. Written in the **Visual Basic** programming language, the malware consisted of approximately 150 lines of code. The program was designed to:

1. Wipe data stored on targeted computers and servers.
2. Reboot machines after wiping, exposing otherwise protected data.
3. Overwrite wiped data with random patterns of ones and zeros, making recovery prohibitively expensive and forcing Sands to replace entire systems.

This malicious payload was deployed with precision, targeting Sands' Active Directory servers—a critical component of network management and security. By attacking these systems early, the attackers inadvertently limited the spread of the malware to Sands' U.S.-based operations. This mistake prevented the malware from reaching Sands' international properties in Singapore and China, a fortunate break for the company.

As the attackers moved through the network, logs indicated they were compressing large batches of sensitive files, likely preparing to exfiltrate private documents. These files potentially included credit checks on high-roller customers, detailed diagrams and inventories of global computer systems, and other proprietary information. While it remains unclear how much data was successfully exfiltrated, the attackers demonstrated a clear intent to gather sensitive information alongside their destructive efforts. Realizing the severity of the attack, Sands' leadership, led by President Michael Leven, made the decision to disconnect the company entirely from the Internet. This bold measure of system containment, though disruptive, effectively halted further infiltration and data exfiltration. While severing online connectivity paralyzed many business functions reliant on digital systems, Sands managed to maintain some core operations thanks to the isolation of an IBM mainframe critical to hotel reservations and other essential services.

The attack wiped out approximately three-quarters of Sands' computer servers in Las Vegas, along with thousands of desktop PCs and laptops. The cost of replacing hardware and recovering data was estimated at over $40 million. A few key observations are that, first, Sands' existing cybersecurity defenses and its nascent security upgrade project leave the organization vulnerable to sophisticated attack. Second, the custom-built malware was highly effective. Its simplicity (150 lines of code) and precision underscore the attackers' technical expertise. Third, nevertheless, the decision to target Active Directory servers early in the attack inadvertently confined the scope of the malware to only U.S. operations. Had the attackers waited to deploy the wiper software, the impact could have extended to Sands' properties in Asia, causing far greater disruption.

In conclusion, “Yellowstone 1” is a well-coordinated attack that leveraged credential harvesting, malware engineering, and data compression techniques. Although Sands’ containment efforts mitigated further damage, the attack exposed the company’s critical cybersecurity vulnerabilities and accentuated how robust IR measures can protect business operations.

Actions Taken

Immediate Network Isolation

Upon detecting unauthorized access and system compromise, the Sands IT team promptly disconnected affected systems from the internet. This measure aimed to halt the attackers' ability to infiltrate further into the network and exfiltrate sensitive data.

IT staff were mobilized across the Venetian and Palazzo casino properties to manually unplug network cables from every computer they could access. This included vital devices such as PCs used by pit bosses to monitor gamblers and kiosks where slot machine players redeemed their winnings. The decision to prioritize network isolation, even at the expense of operational disruptions, was critical in containing the attack.

Cybersecurity Experts Engagements

Recognizing the complexity and scope of the breach, Sands engaged Dell SecureWorks to perform a detailed forensic investigation. The team worked to trace the origins of the attack, analyze the techniques employed by the attackers, and evaluate the full extent of system compromise. Thorough investigations include risk analysis, vulnerability scanning, disaster recovery, and business continuity. Their findings helped guide subsequent remediation efforts and provided valuable insights into the sophistication of the attack.

Malware Eradication and System Restoration

A comprehensive system-wide cleanup operation was initiated to remove all traces of malicious code from the network. IT teams focused on rebuilding compromised servers and workstations to restore functionality securely. This effort required significant coordination and resources, as it was essential to ensure that no lingering threats remained within the infrastructure. Restoration efforts prioritized critical systems to minimize downtime and resume operations as quickly as possible.

Collaboration with Law Enforcement

Sands worked closely with federal authorities, including the FBI, to investigate the cyberattack. Law enforcement was instrumental in uncovering the attackers' motives, methods, and potential links to state-sponsored activities. By sharing detailed forensic evidence and cooperating in the investigation, Sands contributed to broader efforts to address cyber threats targeting private enterprises.

Enhanced Security Measures Implementations
In the aftermath of the breach, Sands overhauled its cybersecurity practices to strengthen its defenses against future attacks. These proactive steps reflected the organization's commitment to improving resilience against emerging cyber warfare. Key measures included: advanced threat detection systems capable of identifying and mitigating potential incidents in real-time; regular security audits that introduce routine assessments to identify vulnerabilities and ensure compliance with industry standards; and comprehensive training programs to educate staff on recognizing phishing attempts, secure data handling, and best practices in cybersecurity.

Financial Impact

Item	Cost
Equipment Damage (servers and hardware, data storage devices, networking equipment, workstation and end-user devices, software licenses and configuration, peripheral equipment, physical repairs)	$10,000,000
Data Recovery	$15,000,000
Investigative Costs [1]	$5,000,000
Labor [2]	$10,000,000
Total	**$40,000,000**

1. Investigative costs were calculated based on 5,000 hours of forensic analysis at $1,000 per hour.

2. Labor costs include time spent by employees on incident response and system restoration, calculated at standard hourly rates

Lessons Learned

Successes

1. Basic logging and monitoring controls in threat identification alerted the Sands cybersecurity team to the occurring malicious activity rather early in stage.
2. The IT team responded to the cyber attack by disconnecting the malware-affected systems from the internet, which indicated the value of rapid containment strategies in minimizing damage.
3. President Michael Leven demonstrates strong leadership in the crisis, effectively halting the attackers' ability to infiltrate further.
4. Sands collaborated closely with Dell SecureWorks and the FBI to investigate the attack. External expertise was leveraged to understand the nature of the threat and its geopolitical implications.
5. The IBM mainframe, critical for core operations, remained unaffected due to its isolated architecture. It highlighted the importance of designing systems with segmentation to protect critical business functions.
6. IT teams across properties, including the Venetian and Palazzo, collaborated to disconnect compromised devices manually, reflecting efficient on-the-ground response coordination.
7. The incident became a prominent example of state-aligned hacktivism targeting private enterprises for geopolitical purposes. This brings attention to the rising risks of cyberattacks that operate below the threshold of government retaliation.
8. Sands managed to maintain limited operational capacity by isolating and preserving key systems and infrastructure, which demonstrates the importance of strategic planning and prioritization in maintaining business continuity during a major cyberattack.

Opportunities for Improvement

- Control Weakness:
    - Password Protection: The attackers leveraged brute-force attacks and tools like Mimikatz to exploit weak or reused passwords, gaining access to critical systems.
    - Network Segmentation: The malware was able to spread fast across the network due to insufficient segmentation between different systems and regions.
    - Limited Cybersecurity Staffing: A team of only five cybersecurity personnel was responsible for managing and protecting a network of 25,000 computers, creating resource constraints during both proactive and reactive efforts.
    - Lack of IR Plan: The absence of a mature incident response plan delayed coordinated action and limited preparedness for handling a major cyberattack.
    - Cyber Threats Awareness: The organization underestimated the geopolitical risk of being a target for state-aligned cyberattacks, which led to a lack of preparation for this type of threat.
- Recommendation:
    - (Password Protection) Implement strong password policies, including complex password requirements, mandatory periodic changes, and restrictions on reusing previous passwords. Deploy multi-factor authentication (MFA) for all critical systems to minimize risk from credential theft.
    - (Network Segmentation) Implement robust network segmentation to isolate sensitive systems and servers. Establish distinct zones for critical, sensitive, and general-purpose systems, with firewalls and access controls between them to limit lateral movement.
    - (Limited Cybersecurity Staffing) Increase cybersecurity staffing to an appropriate level for the organization's size and complexity. Augment internal expertise with managed security services to address advanced threats.
    - (Lack of IR Plan) Develop and regularly test a formal incident response plan. Conduct tabletop exercises and simulations involving cross-departmental teams to prepare for potential attack scenarios. Deploy real-time security information and event management (SIEM) solutions with automated alerts for suspicious behavior.
    - (Cyber Threats Awareness) Conduct regular threat assessments to identify risks from adversaries. Collaborate with industry groups and government agencies to stay informed about emerging threats and best practices.

- Action Item Owner:
    - (Password Protection) IT Security Team
    - (Network Segmentation) Network Architecture Team
    - (Limited Cybersecurity Staffing) Human Resources and IT Leadership
    - (Lack of IR Plan) IT Risk Management Team, Security Operations Center
    - (Cyber Threats Awareness) Threat Intelligence Team