Incident Response Team

Report №1

Capcom Ransomware Attack

November 2, 2020

20.09.2025

Almaty

Table of Contents

Introduction

Capcom remains one of the major and most beloved video game industries of the world. Founded in Japan in 1979, the studio produced truly legendary franchises such as *Resident Evil*, *Street Fighter*, *Monster Hunter*, *Devil May Cry.*

On November 2, 2020, the company suffered a ***ransomware*** attack at the hands of the Ragnar Locker gang, and has been having a hard time with the criminals since. Luckily, the gang was taken down in late 2023, but the damage was done.

Rumors have suggested that the crooks opened the bidding with eight digits worth of blackmail, demanding $11,000,000 in cryptocurrency in return for two things:

- A decryptor to recover files scrambled in the attack.
- A promise not to reveal corporate data stolen before the files were scrambled.

Additionally, an ominous note in broken English was made – “If No Deal is made then all your data will be Published and/or Sold through an auction to third parties”. The bargain didn’t work and in the end data was leaked.

The Algorithm of The Attack

Behind the scenes (early October 2020)

- **Target:** An outdated backup VPN (Virtual Private Network) device at Capcom's North American subsidiary.
- The threat actors identified this legacy system as a vulnerable entry point. It was maintained as an emergency backup due to increased network strain from COVID-19, making it a weak link in the security perimeter.
- Using an unspecified exploit, the attackers weaponized this vulnerability to gain an initial, unauthorized foothold into Capcom's internal network. This was the critical first step in the kill chain.

Movement Escalation (mid-late October 2020)

- From the compromised North American VPN, the attackers began pivoting across the network. They moved from the initial entry point to other systems, targeting both U.S. and Japanese offices.
- During this phase, they performed internal reconnaissance to map the network, identify high-value targets (such as file servers and databases), and exfiltrate sensitive data. This data was likely stolen before the ransomware was deployed to be used for double extortion tactics.

Detonation (November 1, 2020)

- After weeks of lurking within the network, the attackers initiated the final phase of their operation.
- The ransomware payload was deployed and detonated, simultaneously encrypting files on compromised devices across Capcom's global network. This caused immediate and widespread disruption, crippling email and file servers.

Impact (November 2, 2020)

- The encryption of critical systems led to a forced operational shutdown of certain business functions. Capcom was forced to halt operations to contain the breach and begin recovery efforts.

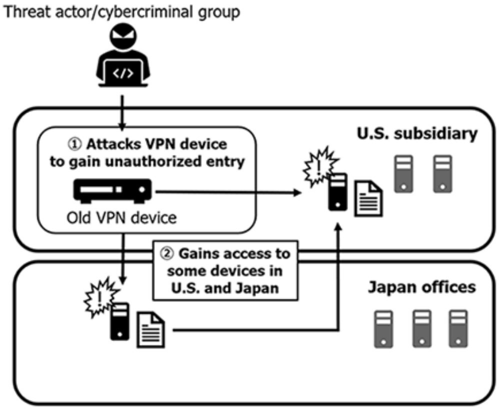
Threat actor/cybercriminal group
① Attacks VPN device to gain unauthorized entry
Old VPN device
U.S. subsidiary
② Gains access to some devices in U.S. and Japan
Japan offices

Figure 1. Capcom official report

The Damage Made

Victims

The victims of this ransomware attack were people ranging from regular gamers to business partners and employees. Official claims made it clear that no credit card or sensitive information was exposed, however, most leaks did contain private information of some sort, such as names and email addresses.

Capcom official statement post-investigation:

The cumulative total for information verified to have been compromised is *15,649* people, data theft ranging from varying levels of severity. None of the at-risk data contained credit card information due to all online transactions being handled by a third-party service provider on a separate system that was not involved in the attack.

Company offers its deepest apologies, swears to has strengthen the security measures, and assures it is safe to use its services and products as for now.

The other sources:

Up to 350,000 customers, business partners, and other employees were affected. The information leaked includes email addresses, names, birthdates, phone numbers, photos, HR information, Japan Customer service video game support help desk information, sales and business-related confidential corporate data.

Consequences

- Reputational and financial damage
- Operational disruption due to company shutting down its internal network system
- Private information such us names, email addresses, gender, was exposed
- Affected individual were notified about the compromised data

Vendors’ Recommendations

The core lesson is that modern defense requires a "Assume Breach" mentality: make initial access harder, detect lateral movement faster.

National Institute of Standards and Technology (NIST) - nist.gov

Preventive recommendation: implement the NIST Cybersecurity Framework (CSF), specifically the "Protect" function. This includes maintaining and managing the security of hardware and assets (like VPN devices) on an ongoing basis. Outdated devices must be promptly patched or decommissioned and removed from the network entirely.

Cybersecurity and Infrastructure Security Agency (CISA) - cisa.gov

Preventive recommendation: immediately patch known exploited vulnerabilities and enforce multi-factor authentication (MFA) on all remote access solutions, especially VPNs. CISA's “Known Exploited Vulnerabilities Catalog” is a critical resource. They also recommend segmenting networks to limit an attacker's ability to move laterally after a breach.

IBM Security, Cisco - cisco.com

Preventive recommendation: employ a 24/7 Security Operations Center (SOC) service, either in-house or outsourced. A SOC provides continuous monitoring and threat hunting, which is crucial for identifying and stopping attackers during the dwell time (the period between initial breach and ransomware detonation).

Capcom solution

Capcom took several measures to secure its platform and prevent future incidents. This included introducing a Security Operation Center (SOC) service to continuously monitor external connections and implementing Endpoint Detection and Response (EDR) for early detection of unusual activity on devices.

Capcom also worked with a leading software company to clean all compromised devices, reviewed accounts used for business purposes, and improved management methods for VPN and other devices. Additionally, the company launched the Information Technology Security Oversight Committee, which functions as an advisory group for matters related to system security with external security experts.

My Recommendations

Note: the assumed role was chosen randomly, by a generator.
My role: non—tech employee, HR manager.

The Capcom attack clearly demonstrates that every employee is a part of the security fabric. As an HR Manager, my role in preventing such an attack or mitigating its impact is fundamental and strategic. I would focus not on technical fixes, but on the human factor, which, according to an IBM study, is the main cause of 95% of cybersecurity breaches. If human error were eliminated, 19 out of 20 cyber breaches might not happen at all. My goal would be to get as close to that reality as possible by building a "human firewall."

Preventive measures

My main goal would be to make safety a natural part of our everyday work culture. I would make sure everyone - *absolutely everyone* - understands the small but important habits that keep us secure. This means regular, simple training that teaches us all how to spot a tricky email or why using an extra login code (like on our phones) is so important. It's about turning each of us into a strong first line of defense.

I would make safety part of our core routines - from the first day a new person joins the team to the day someone moves on. It's about building a workplace, where looking out for each other's digital safety becomes second nature.

Minimizing negative consequences

If an attack did happen, my focus would be on keeping everyone calm and informed. Panic can sometimes cause more damage than the hackers themselves. I would make sure we have a clear, easy-to-follow plan that everyone knows - like where to get information and who to contact if something seems wrong. Good communication can keep the business running even when systems are down.

Appendix

1. "6 of the most notorious cyber attacks in the gaming history", AnimationXpress, https://www.animationxpress.com/games/here-are-6-of-the-most-notorious-cyber-attacks-in-the-gaming-history
2. "Capcom hack: Up to 350,000 people's information stolen", BBC, https://www.bbc.com/news/technology-54958782
3. "Rangar Locker ransomware gang taken down", Europol, https://www.europol.europa.eu/media-press/newsroom/news/ragnar-locker-ransomware-gang-taken-down-international-police-swoop
4. "4th Update regarding Data Security Incident due to Unauthorized Access: Investigation Results", Capcom, https://www.capcom.co.jp/ir/english/news/html/e210413.html
5. "Notice regarding Network Issues due to Unauthorized Access", Capcom, https://www.capcom.co.jp/ir/english/news/html/e201104.html
6. "Video game company Capcom details attack, data breach by ransomware gang", Cyberscoop, https://cyberscoop.com/capcom-ransomware-data-breach-ragnar-locker/
7. "Capcom Data Breach: What & How It Happened?", Twingate, https://www.twingate.com/blog/tips/Capcom-data-breach/
8. "The Role of Human Error in Successful Cyber Security Breaches", Usecure, https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches