

Weak passwords and absence of 2FA: Analysis of a ransomware attack on university

Mukhit Urazymbetov^{1,*†}, Bakhytzhan Akhmetov^{1,†}

¹Abai Kazakh National Pedagogical University, Dostyk Ave., 13, Almaty, 050010, Kazakhstan

Abstract

Ransomware attacks targeting universities have increased significantly in recent years. Virtualization platforms have become primary targets for attackers. This paper analyzes the causes and consequences of a cyberattack based on an actual incident that occurred in 2026. The study identifies the direct impact of weak passwords, absence of multi-factor authentication, and unmonitored remote access channels on security. The interconnection of VMware vSphere, Veeam Backup, and FortiGate VPN systems is examined. No sophisticated technical exploit was employed during the incident; the attack was executed through compromised credentials. A single weak password combined with the absence of 2FA led to the compromise of the entire university infrastructure. The majority of virtual machines were encrypted, and academic, financial, and administrative systems were temporarily disrupted. The backup server itself was also affected. The recovery process consisted of multiple stages. Research findings demonstrate that network segmentation, immutable backup technology, multi-factor authentication, and continuous auditing are essential defensive measures. The critical role of the human factor in security, comparable to technical vulnerabilities, has been proven.

Keywords

cybersecurity, two-factor authentication, password policy, higher education institutions, phishing, ransomware, information security, digital infrastructure, Zero Trust, cyber resilience

1. Introduction

Universities are no longer merely educational institutions; they have evolved into large-scale digital ecosystems. Student grades reside on one server, accounting systems on another, and library resources on a third. Typically, all operate within a single cluster. When one component fails, the entire university infrastructure halts.

According to Sophos's 2024 report, 66% of higher education organizations experienced at least one ransomware incident [1]. Previously, attacks primarily targeted banks. Currently, higher education institutions have become principal targets.

The reasons are evident: legacy systems are widespread, passwords are overly simplistic, and some employees install TeamViewer or AnyDesk without oversight. In many educational institutions, cybersecurity remains a low priority. The focus is primarily on educational processes, accounting, and admissions. Security concerns are typically addressed only after an incident occurs. This represents a critical problem.

This paper analyzes a ransomware attack on virtualization infrastructure. Three primary risk factors exist in information systems: absence of 2FA, weak passwords, and uncontrolled remote access. In recent years, this combination has compromised the security of numerous organizations. A single weak password is sufficient.

Many administrators deprioritize VPN security. For attackers, VPN has become the primary entry point, particularly when 2FA is absent.

CMiGIN'26: Fifth International Workshop on Conflict Management in Global Information Networks, June 26–27, 2026, Krakow, Poland

*Corresponding author.

† These authors contributed equally.

✉ 3155580@gmail.com (M. Urazymbetov); bakhytzhan.akhmetov.54@gmail.com (B. Akhmetov)

🆔 0009-0005-8179-5013 (M. Urazymbetov); 0000-0001-5622-2233 (B. Akhmetov)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

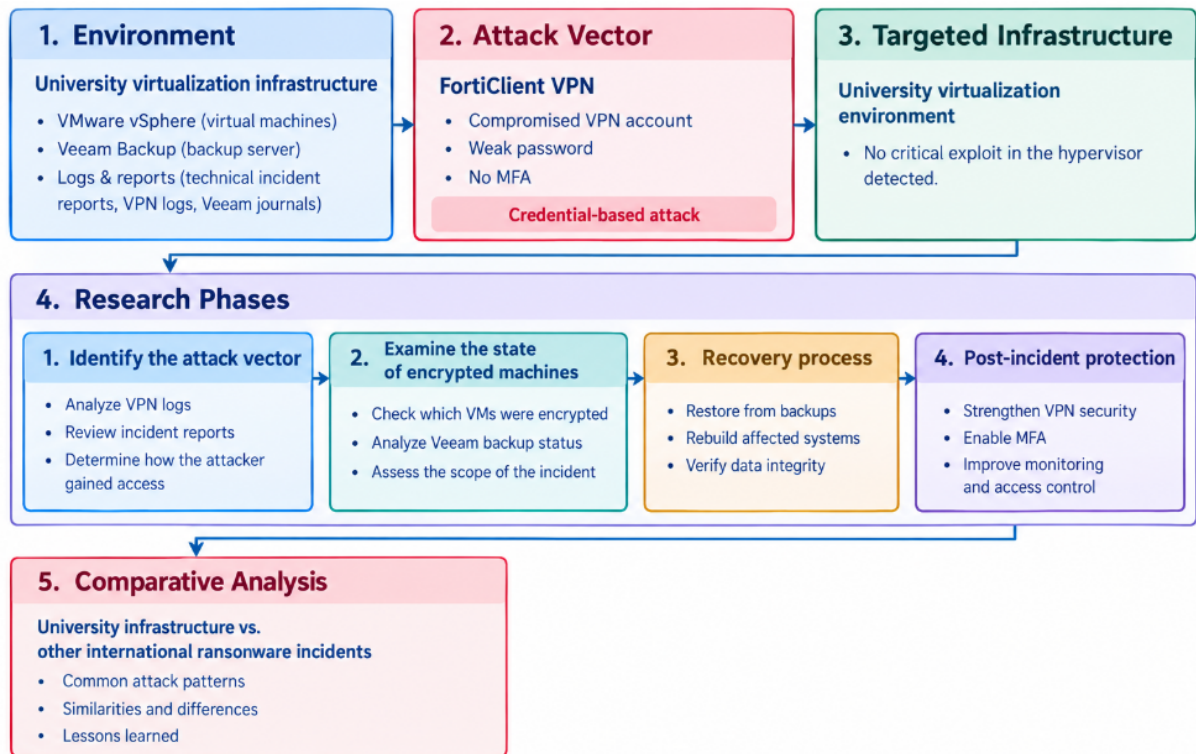


Figure 1: The flowchat of proposed method.

The objective is clear: to demonstrate the concrete consequences of weak passwords, absence of 2FA, and unregulated remote access channels.

2. Materials and methods

The study utilized technical incident reports, VPN logs, Veeam Backup journals, and VMware vSphere data. The primary subject was the university's virtualization infrastructure. The attack originated through FortiClient VPN. Notably, no critical exploit in the hypervisor itself was detected. This was not a classical vulnerability exploitation but rather a credential-based attack.

Initial analysis revealed that one VPN account possessed a weak password. Multi-factor authentication was absent. Such scenarios remain common.

The research comprised several phases: first, identifying the attack vector; second, examining the state of encrypted machines; third, the recovery process; and finally, post-incident protective measures.

Comparative analysis was also conducted. The university infrastructure was compared with other international ransomware incidents.

Theory diverges from practice. Many publications suggest that backups fully resolve the problem. In actual scenarios, the backup server itself may be encrypted. This study documented precisely such a case.

The flowchat of proposed method is shown in Figure 1.

3. Results

In 2026, a ransomware attack was recorded on the university infrastructure. In the morning, administrators discovered that a portion of virtual machines would not boot. VMDK files were encrypted. Text files demanding payment appeared in certain directories.

Investigation revealed GlobeImposter ransomware 2.0. File extensions and ransom note structure

matched this variant. The attacker gained access to the internal network through FortiClient VPN, then proceeded to vCenter and ESXi hosts.

The most critical issue was password policy. The password used for VPN was overly simplistic. Multi-factor authentication was absent.

This incident reflects current ransomware trends. Previously, attackers invested significant effort in identifying system vulnerabilities. Now, the approach is simpler.

Some researchers term this "low effort intrusion". Rather than sophisticated technical exploits, simple credential access suffices. When VPN credentials are weak and 2FA is absent, internal network penetration becomes trivial. Microsoft research indicates that password spraying and credential stuffing attacks remain effective [2, 3]. In many organizations, individuals still use "123456," "qwerty," birth dates, or phone numbers as passwords. When passwords are stolen or discovered through brute force, attackers immediately gain internal network access.

Following the attack, machines on ESXi hosts began encryption. According to VMware security guidelines [4], proper host hardening could have limited lateral movement. Primary affected systems included: UniverSystem, OnlineOffice, 1C accounting system, electronic library, and WSUS server.

The university's academic system was temporarily suspended. Students could not access the portal. Faculty members lost access to certain documents. Accounting operations were delayed.

An interesting detail: certain servers survived because they resided in different segments during the attack. Although segmentation was incomplete, network partitioning provided some degree of protection.

The attacker also compromised the Veeam Backup server. A portion of backups was encrypted – a dangerous scenario. The new wave of ransomware attacks specifically targets backup systems.

Palo Alto Networks researchers identified precisely this trend. Currently, 93% of ransomware groups initially seek backup infrastructure [5].

Recovery proceeded in multiple stages. First, clean ESXi hosts were isolated. Subsequently, unencrypted backups were located. Critical machines were restored from the last healthy backup.

UniverSystem and 1C systems were restored first. Educational processes and the finance department constituted the most critical services for the university. Certain data were not fully preserved. Information from specific time periods was lost. This occurs in many ransomware incidents.

Research findings revealed several issues.

First, weak passwords remain the primary threat.

Second, absence of 2FA facilitated the initial attack phase.

Third, lack of isolation in the backup system created additional risk. Fourth, unmonitored AnyDesk, TeamViewer, and RDP channels enabled lateral movement within the internal network.

Remote access tools are initially installed for convenience. Over time, they become shadow infrastructure. One employee installs AnyDesk, another uses TeamViewer, and eventually no one knows what is installed on which device.

In some cases, such applications operate with domain administrator privileges – convenient for ransomware operators. During incident response, several workstations were found to have unaccounted remote access tools. This enabled the attacker to move freely within the network.

Fifth, administrative privileges were excessively broad.

Following the incident, security policy was strengthened in accordance with ISO/IEC 27001:2022 information security management standards [6, 7]. 2FA was implemented for VPN. Password policy was revised. Open RDP was closed. Centralization of logging and monitoring systems commenced. Solutions such as SIEM systems were considered.

The main research findings are shown in Figure 2.

4. Discussion

This incident reflects actual conditions in many organizations. Frequently, attackers do not require sophisticated hacking tools. A simple password suffices. Verizon's Data Breach Investigations Report

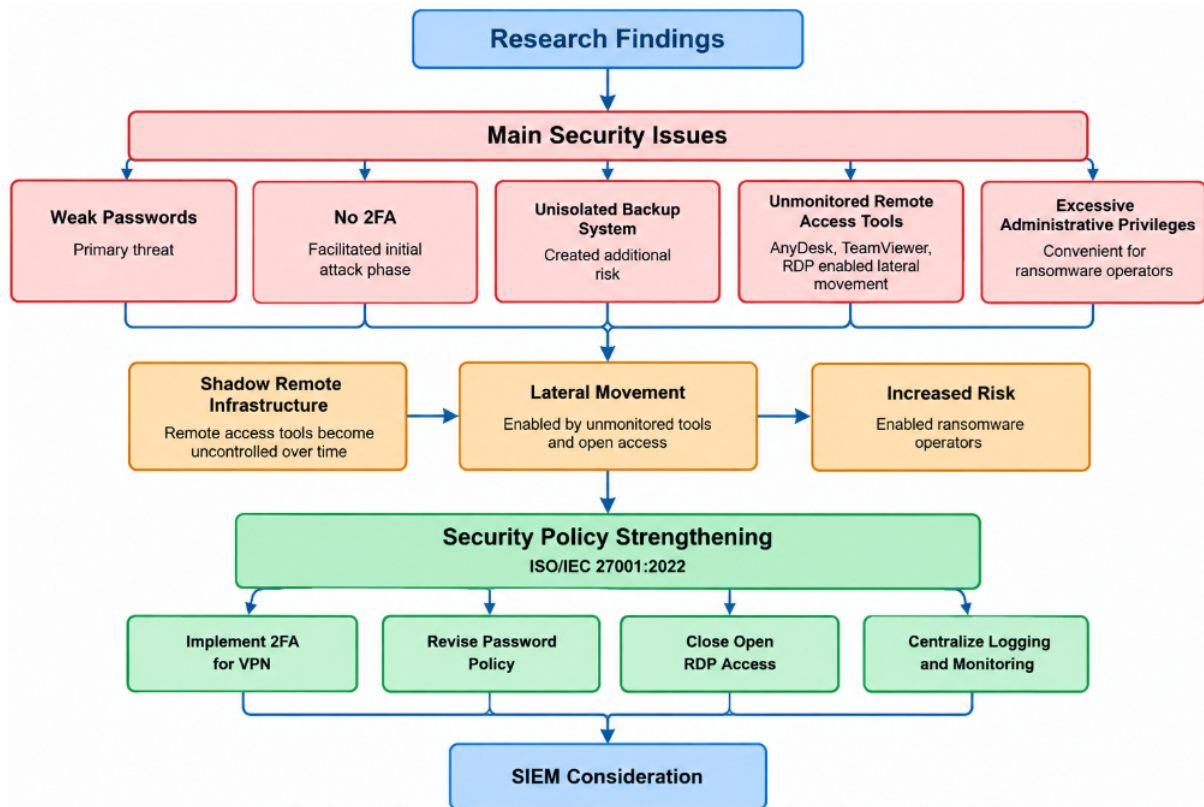


Figure 2: The main research findings.

indicates that 74% of data breaches involve the human factor [8]. This study's case aligns with this finding.

Many system administrators focus extensively on firewalls or antivirus solutions. However, authentication security remains secondary.

The majority of current ransomware attacks begin with credential theft. Password security remains a fundamental defensive layer.

MFA or 2FA can prevent the majority of ransomware attacks. Microsoft Security research demonstrates that MFA reduces account compromise probability by 99% [2]. While this metric may appear promotional, substantial differences are observed in practice.

Without 2FA, only a password is required for the attacker. With MFA enabled, an additional device, token, or temporary code is necessary. I contend that 2FA should be mandatory for VPN, Veeam, vCenter, and administrative panels.

Some organizations claim 2FA is inconvenient for employees. However, infrastructure disrupted for several days is considerably more inconvenient. 2FA does not solve all problems. However, it significantly complicates the attacker's work.

Universities face an additional complex issue: the user base is extensive – students, faculty, administrative staff, contractors. All require access. Balancing security and convenience is challenging.

Sometimes installing AnyDesk for a faculty member appears simpler. Sometimes a system administrator uses a shared account to save time. Such minor decisions subsequently escalate into major problems.

The study also identified backup issues. Merely having backups is insufficient. They must be isolated.

The immutable backup concept has gained prominence in recent years. The principle is straightforward: backup files cannot be modified or deleted within a defined timeframe.

Veeam research indicates that organizations employing immutable storage demonstrate higher recovery speeds [9, 10].

Segmentation is also critical. During the attack examined in this study, after the attacker gained

internal network access through VPN, they could freely access numerous systems. Had the management segment been isolated according to VMware best practices [4], damage could have been reduced.

The Zero Trust concept addresses such issues. The fundamental principle is simple: trust no one automatically.

Currently, some universities have begun implementing SIEM and EDR systems. For smaller educational institutions, their cost remains prohibitive.

Another issue is cyber hygiene. Even when technical tools are adequate, employees may fall victim to phishing emails. IBM research indicates that phishing remains one of the most prevalent initial attack methods [9].

Information security training in universities is often conducted formally. Some individuals do not review the materials. Perspectives change following an actual incident.

This study also observed changed attitudes toward passwords following the attack. Individuals who previously used "123456" or birth dates subsequently adopted complex passwords.

Such changes should occur before incidents, not after.

Sometimes cybersecurity publications become overly academic. In practice, problems originate from simple issues: one password, one open RDP, one unmonitored TeamViewer instance.

Subsequently, the entire university remains disrupted for several days.

5. Conclusions

Research demonstrates that the causes of ransomware attacks on university infrastructure extend beyond technical vulnerabilities. The human factor, weak passwords, and uncontrolled remote access play substantial roles.

During the incident, the majority of virtual machines in the VMware vSphere environment were encrypted. The university's academic, financial, and administrative systems were temporarily disrupted.

Research findings indicate.

First, 2FA is mandatory for VPN and administrative systems, as recommended by CISA ransomware prevention guidelines [11].

Second, backups must be stored in isolated and immutable formats. Third, university networks must be segmented.

Fourth, AnyDesk, TeamViewer, and RDP channels must be continuously monitored. This study contributes to understanding cybersecurity issues in the university sector and provides a foundation for developing practical protective measures.

Therefore, the defense strategy for educational organizations must be multilayered, aligning with frameworks such as NIST Cybersecurity Framework [12].

Merely implementing technical tools is insufficient; they must be integrated with users' cyber hygiene practices, continuous training, administrative oversight, and infrastructure management. Security reaches sustainable levels only when it transcends being solely the responsibility of the security department and becomes a shared responsibility of the entire university community.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

- [1] Sophos, The state of ransomware in education 2024, 2024. URL: <https://www.sophos.com/en-us/content/state-of-ransomware-education>, sophos Whitepaper.
- [2] A. Weinert, Your pa\$\$word doesn't matter, 2019. URL: <https://www.microsoft.com/en-us/security/blog/2019/10/03/password-doesnt-matter-mfa-does/>.

- [3] O. Holubnychyi, et al., Self-organization technique with a norm transformation based filtering for sustainable infocommunications within cns/atm systems, in: I. Ostroumov, M. Zaliskyi (Eds.), Proceedings of the 2nd International Workshop on Advances in Civil Aviation Systems Development, Springer Nature Switzerland, Cham, 2024, pp. 262–278. doi:10.1007/978-3-031-60196-5_20.
- [4] VMware, vSphere Security Configuration Guide: VMware vSphere 8.0, VMware, 2024. URL: <https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security-configuration-guide.pdf>.
- [5] Palo Alto Networks Unit 42, 2024 Unit 42 Ransomware and Extortion Report, Technical Report, Palo Alto Networks Unit 42, 2024. URL: <https://www.paloaltonetworks.com/resources/research>.
- [6] International Organization for Standardization, Iso/iec 27001:2022: Information security, cybersecurity and privacy protection — information security management systems — requirements, 2022.
- [7] F. M. Mustafa, S. M. Kallow, N. A. Thamer, H. H. Merzah, M. Mohammed, T. Konrad, D. Y. Abdulhussain, The importance of big data in the advancement of robotic capabilities, in: Proceedings of the 36th Conference of Open Innovations Association FRUCT, 2024, pp. 423–432. doi:10.23919/FRUCT64283.2024.10749938.
- [8] Verizon, Data Breach Investigations Report 2024, Technical Report, Verizon, 2024. URL: <https://www.verizon.com/business/resources/reports/dbir.html>.
- [9] IBM Security, Ponemon Institute, Cost of a Data Breach Report 2024, Technical Report, IBM Security, 2024. URL: <https://www.ibm.com/reports/data-breach>.
- [10] Veeam Software, Veeam Backup & Replication Best Practice Guide, Veeam Software, 2024. URL: <https://bp.veeam.com/vbr/>.
- [11] Cybersecurity and Infrastructure Security Agency, #stopransomware guide, 2023. URL: <https://www.cisa.gov/stopransomware/ransomware-guide>, originally published September 2020; updated May 2023.
- [12] National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, Technical Report CSWP 29, National Institute of Standards and Technology, 2024. URL: <https://doi.org/10.6028/NIST.CSWP.29>. doi:10.6028/NIST.CSWP.29.