# Lord Nemesis Strikes: Supply Chain Attack on the Israeli Academic Sector - OP INNOVATE

By Roy Golombick

Published: 2024-03-07 · Archived: 2026-04-05 23:41:56 UTC

**“Lord Nemesis Strikes: Supply Chain Attack on the Israeli Academic Sector**

The Iranian hacktivist group Lord Nemesis, also known as ‘Nemesis Kitten’, which emerged onto the cyber scene in late 2023, has previously declared its intention to target Israeli-based organizations. One of this Iranian funded hacking group’s goal is to instill fear in their victims. From the dramatic website portraying a malicious looking dark lord to their way of action which entails hacking silently, downloading data and slowly releasing findings to the global web whilst sending warning messages to their victims about future actions. The damage they cause , whilst on the technical front a concern to any organization – can be reduced by understanding that panic is part of their goals and reduce the reaction to their activity.

From their dramatic website, which features a sinister-looking dark lord, to their modus operandi, which involves silently infiltrating networks, exfiltrating data, and gradually releasing their findings to the global web, the group’s actions are calculated to maximize the psychological impact on their victims. By sending ominous warning messages about future actions, Lord Nemesis aims to create an atmosphere of uncertainty and anxiety among their targets.

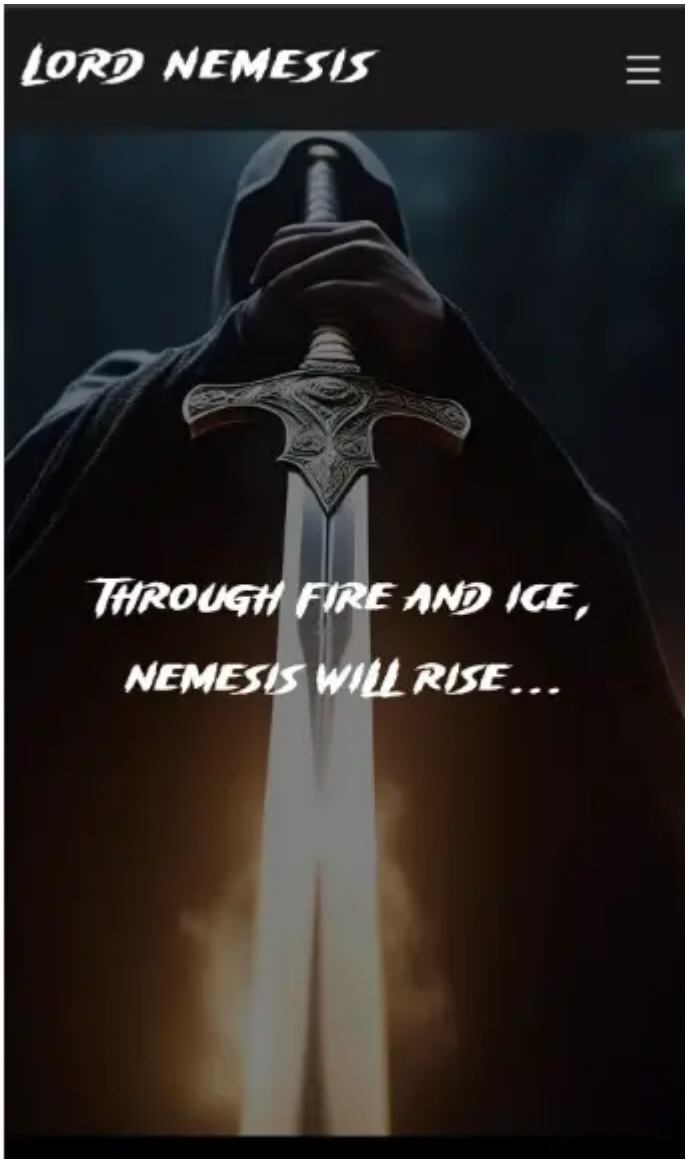



*Figure 1: Image on LordNemesis website*

The group's first significant success came in late November 2023 when they claimed responsibility for breaching Rashim Software, a leading provider of academic administrations and training management software solutions in Israel. Lord Nemesis allegedly used the credentials obtained from the Rashim breach to infiltrate several of the company's clients, including numerous academic institutes.

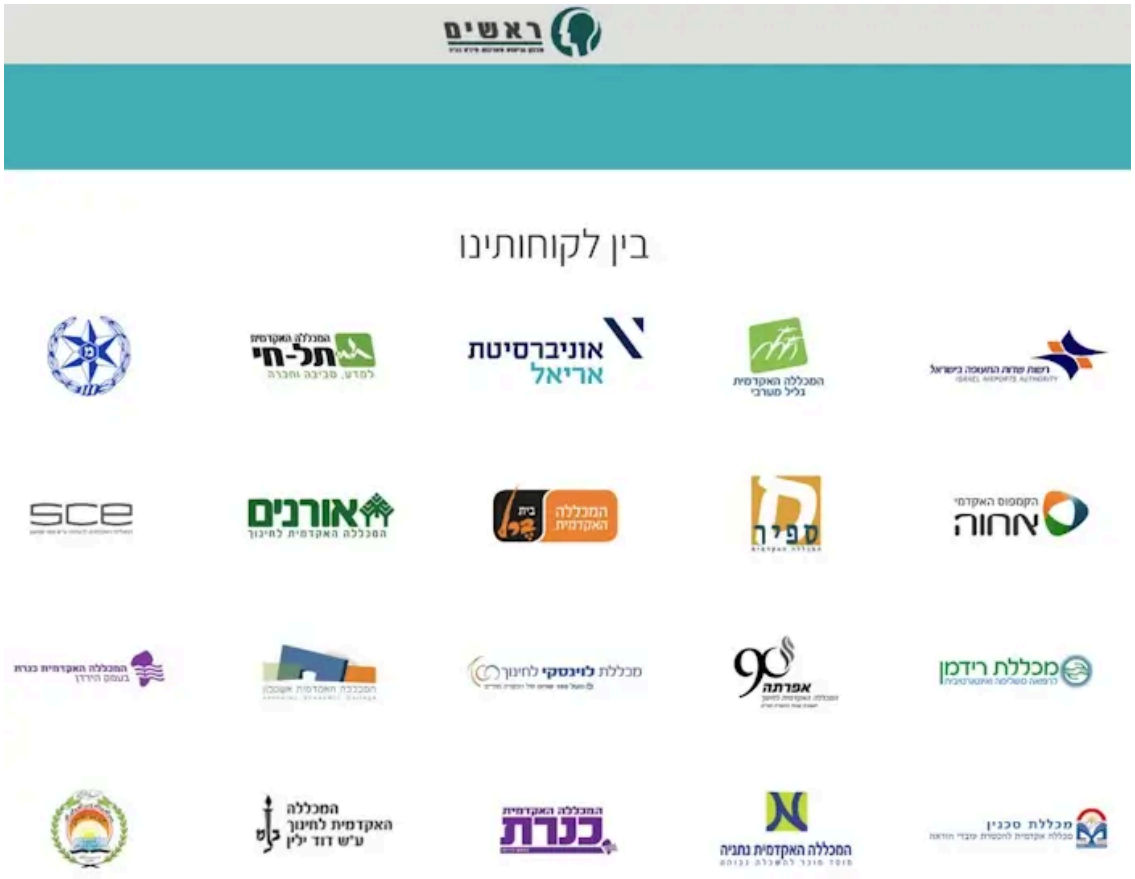
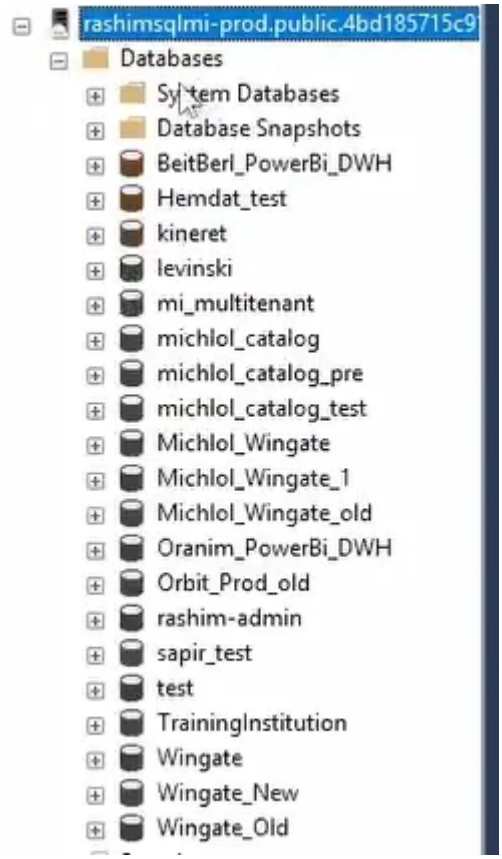



*Figure 2: Rashim Customers*

Rashim Software Ltd. is a prominent player in the Israeli market, offering a wide range of software solutions to universities and colleges. One of their key products is a student CRM called Michlol, which is widely used by academic institutions across the country.

According to Lord Nemesis, they managed to gain complete access to Rashim’s infrastructure and exploited this access to send an email to over 200 of Rashim’s customers and colleagues. The group claims to have obtained sensitive information during the breach, which they may use for further attacks or to exert pressure on the affected organizations.


rashimsqlmi-prod.public.4bd185715c9
Databases
System Databases
Database Snapshots
BeitBerl_PowerBi_DWH
Hemdat_test
kineret
levinski
mi_multitenant
michlol_catalog
michlol_catalog_pre
michlol_catalog_test
Michlol_Wingate
Michlol_Wingate_1
Michlol_Wingate_old
Oranim_PowerBi_DWH
Orbit_Prod_old
rashim-admin
sapir_test
test
TrainingInstitution
Wingate
Wingate_New
Wingate_Old

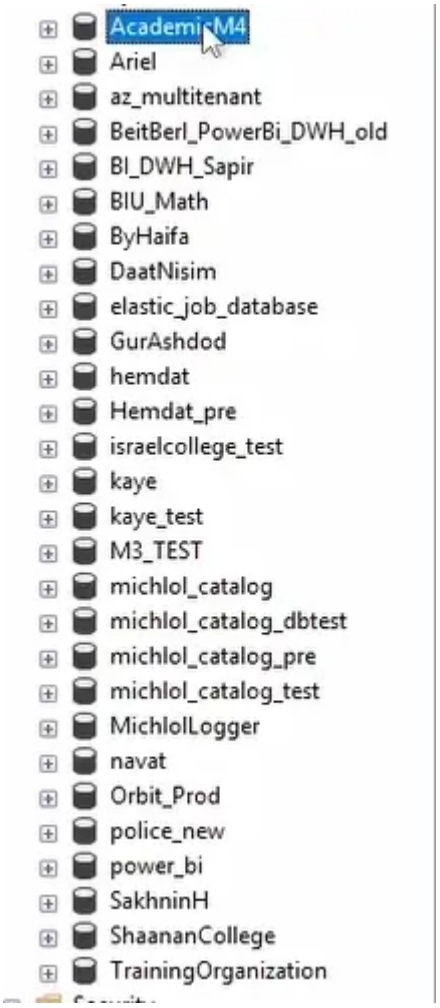

AcademicM4
Ariel
az_multitenant
BeitBerl_PowerBi_DWH_old
BI_DWH_Sapir
BIU_Math
ByHaifa
DaatNisim
elastic_job_database
GurAshdod
hemdat
Hemdat_pre
israelcollege_test
kaye
kaye_test
M3_TEST
michlol_catalog
michlol_catalog_dbtest
michlol_catalog_pre
michlol_catalog_test
MichlolLogger
navat
Orbit_Prod
police_new
power_bi
SakhninH
ShaananCollege
TrainingOrganization

*Figure 3: List of Rashim databases before deletion*

One of the critical factors that allowed Lord Nemesis to extend its attack beyond Rashim was the company's practice of maintaining an admin user account on some of its customer systems. By hijacking this admin account, the attackers were able to access numerous organizations by using their VPN that relied on the Michlol CRM, potentially compromising the security of these institutions and putting their data at risk.

In some cases, the multi-factor authentication (MFA) implemented by Rashim proved inadequate in defending against the malicious actor. The attacker managed to circumvent the MFA by compromising Rashim's Office365 infrastructure, which served as the basis for the email-based authentication.

To instill fear in his victims and demonstrate the extent of his access, "Lord Nemesis," contacted a list of Rashim's users and colleagues via Rashim's email system on March 4th. This communication occurred four months after the initial breach of Rashim's infrastructure, highlighting the attacker's prolonged presence within the system.

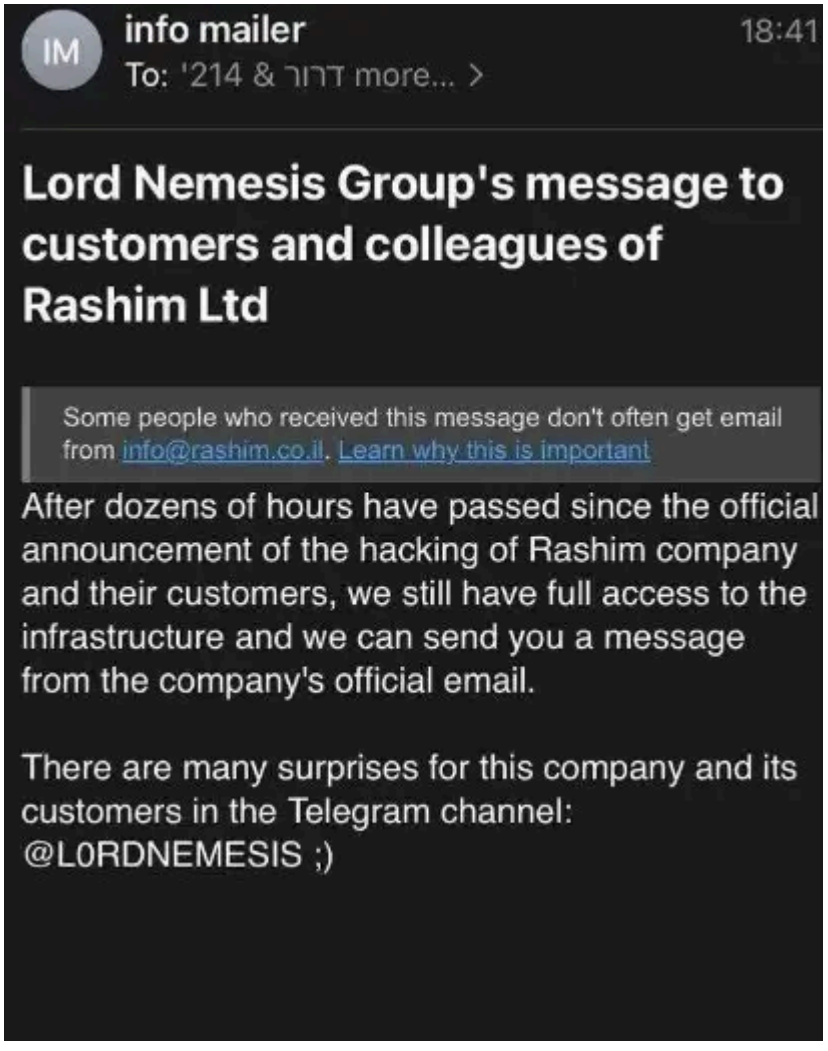



*Figure 4. LordNemesis message to customers and colleagues of Rashim.*

Lord Nemesis, in an unusual move for a hacktivist group, provided an accurate description of the attack in an online post. This demonstrates their direct involvement and desire for public attribution, setting this incident apart from financially-motivated attacks typically carried out by cybercriminals.

Our incident response team was called to assist one of the victims, an Israeli academic institute, in the wake of the breach. The initial investigation confirmed that Lord Nemesis operatives had successfully hijacked the admin account of Rashim Software Ltd., which held privileged access to the institute's student CRM system. Exploiting these elevated credentials, the attackers connected to the institute's VPN outside of regular business hours and initiated data exfiltration.

A thorough examination of the logs revealed that the attackers had specifically targeted critical servers and databases, with a particular focus on the SQL server containing sensitive student information. Although conclusive evidence of data theft was not found, our incident response team assessed a high probability that personal student data had been extracted during the attack.

**Attack Highlights Third-Party Risk**

The incident highlights the significant risks posed by third-party vendors and partners (supply chain attack). By successfully compromising Rashim's admin account, the Lord Nemesis group effectively circumvented the security measures put in place by numerous organizations, granting themselves elevated privileges and unrestricted access to sensitive systems and data.

Our investigation into the attack revealed that the perpetrators likely possessed prior knowledge and familiarity with both Rashim's infrastructure and its customers' IT environments. This allowed the attackers to swiftly identify and compromise critical systems with minimal probing or enumeration, indicating a level of sophistication and planning that goes beyond typical opportunistic attacks.

*Video of Lord Nemesis deleting databases from Rashim server.*

**Strengthening Defenses Against Hacktivists**

The attack carried out by Lord Nemesis indicates that they may have compromised Rashim's systems well in advance, using the intervening time to perform reconnaissance and planning. This theory is supported by the lack of widespread scanning or probing activity during the attack, as the group appeared to have a clear understanding of their targets and objectives didn't trigger any alerts once they accessed the victims infrastructure as they worked under the radar acting as a legitimate user.

**Nation-state hackers vs. limited-resource companies**

This attack highlights the growing threat of nation-state actors targeting smaller, resource-limited companies as a means to further their geopolitical agendas. In this case, Iran, a well-known sponsor of cyber terrorism, has set its sights on Israeli organizations, seeking to disrupt operations, steal sensitive data, and sow fear within the cyber domain. The attackers went as far as leaking personal videos and images of Rashim's CEO, demonstrating their willingness to employ any means necessary to intimidate and harass their targets.

Figure 5. *Snapshot of private video of Rashim CEO published by LordNemesis*

This incident is a clear example of a David vs. Goliath scenario, where smaller companies like Rashim find themselves pitted against the vast resources and capabilities of a nation-state. It is highly unlikely that a single individual orchestrated this attack; rather, it bears the hallmarks of a coordinated effort by a well-organized group with significant backing and support.

Unlike financially motivated cybercriminals, the attackers, in this case, were not driven by the prospect of monetary gain. Instead, their actions align with the goals of a terror attack, aiming to undermine the sense of security and stability within the targeted organizations and, by extension, the wider Israeli society.

In the face of such daunting odds, it is crucial for companies like Rashim and their clients to have access to expert assistance when dealing with the aftermath of a cyber attack. This is where firms like OP Innovate play a vital role, providing the knowledge, experience, and resources needed to investigate, contain, and remediate the

incident. By acting swiftly and decisively, OP Innovate was able to uncover the extent of the compromise, assess the potential impact, and guide the affected organization (Academic Institute) towards a path of recovery.

*Video of Lord Nemesis revealing the SQL password.*

The implications of this attack extend far beyond the Israeli academic institutes that engaged our incident response team. The fact that a single compromised admin account at a third-party vendor could lead to the breach of multiple organizations highlights the urgent need for more robust vendor risk management practices and increased scrutiny of third-party access privileges.

Organizations must recognize that their security posture is only as strong as the weakest link in their supply chain. Conducting thorough due diligence on vendors, implementing strict access controls, multi-factor authentication (to mobile), Just in time access, and continuously monitoring third-party activity should be prioritized to mitigate the risk of cascading breaches originating from trusted partners.

Furthermore, the attack demonstrates the evolving nature of the threat landscape, with hacktivist groups like Lord Nemesis increasingly targeting organizations for ideological and political purposes. As such, organizations must remain vigilant and proactive in their cybersecurity efforts, staying abreast of emerging threats and implementing adaptive security measures to safeguard their assets and data.

In response to the attack, OP Innovate has provided a number of our customers with a series of recommendations to bolster their cyber defenses and reduce their third-party attack surface. Key measures include deploying EDR across endpoints, enforcing MFA, limiting vendor access privileges, upgrading legacy systems, mapping all of the external assets (ASM), and conducting regular internal infrastructure and external penetration testing.

While the unique motivations of hacktivist groups like Lord Nemesis can make deterrence challenging, improving the institute's overall security posture can help minimize damages and hasten recovery in the event of future incidents. As geopolitical tensions continue to rise, organizations must remain vigilant against hacktivists seeking to advance their cause through disruptive cyber attacks.

Attackers IOCs for FW block:

- 45.150.108.242
- 195.20.17.128
- 195.20.17.171

Timeline analysis

1. 30/11/23 – Attacker gained access to Rashim CEO (Ron Hary)
2. 04/12/23 – Attacker sent videos portraying the attacker using Ron's user to access emails and meetings (on teams)
3. 13/01/2024 – 1st academic institute noticed malicious access using Rashim VPN credentials. MFA bypassed using access to Rashim email
4. 13/02/2024 – 2nd academic institute noticed malicious access using Rashim VPN credentials
5. 23/02/24 – 3rd academic institute noticed malicious access using Rashim VPN credentials
6. 03/03/24 – Lord Nemesis publish his acts on Rashim network, prove his deletion of the SQL DB

7. 04/03/24 – Lord nemesis contacts all Rashim customers via Rashim domain user and ‘warns’ of future activities.
8. 04/03/24 – Lord Nemesis targets Academic institutes and leaks sensitive information claimed to be exfiltrated from their DB
9. We know about at least 2 more victims that the details about the attacker activities are disclosed

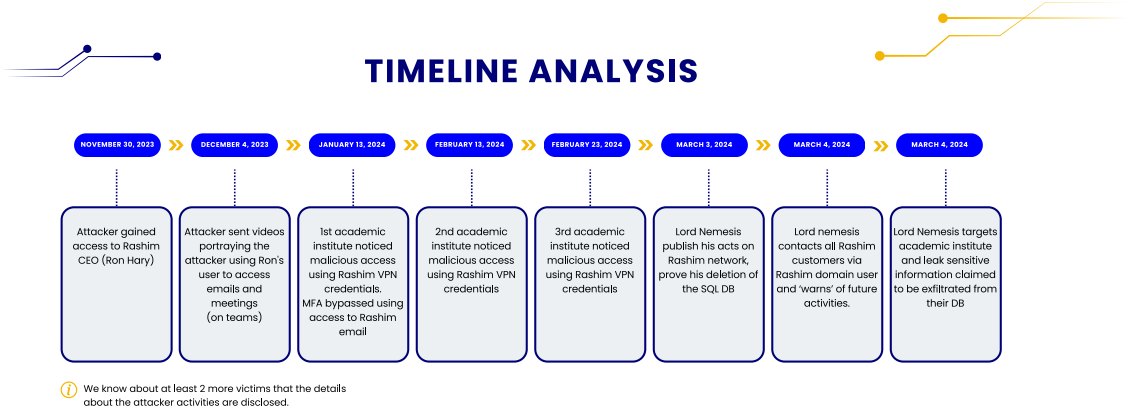



*Figure 6 – Lord Nemesis Attack Timeline*

---

Source: https://op-c.net/blog/lord-nemesis-strikes-supply-chain-attack-on-the-israeli-academic-sector/