

**Smarttech**  
YOUR 24/7 SECURITY PARTNER

# Cyber Threat Intelligence Report

## R00TKIT Allegedly Hacked Unilever PLC



# Contents

Introduction .....	2
Methodology .....	2
Overview .....	2
Alleged Known Targets .....	7
Alleged Upcoming Targets.....	8
Recommendations .....	8
References .....	9

## **Introduction**

This document was prepared as a part of the latest threat intelligence research conducted by the Smarttech247 team. This report delves into the alleged infiltration of the global corporation Unilever's systems, gaining access to the source code of their critical systems.

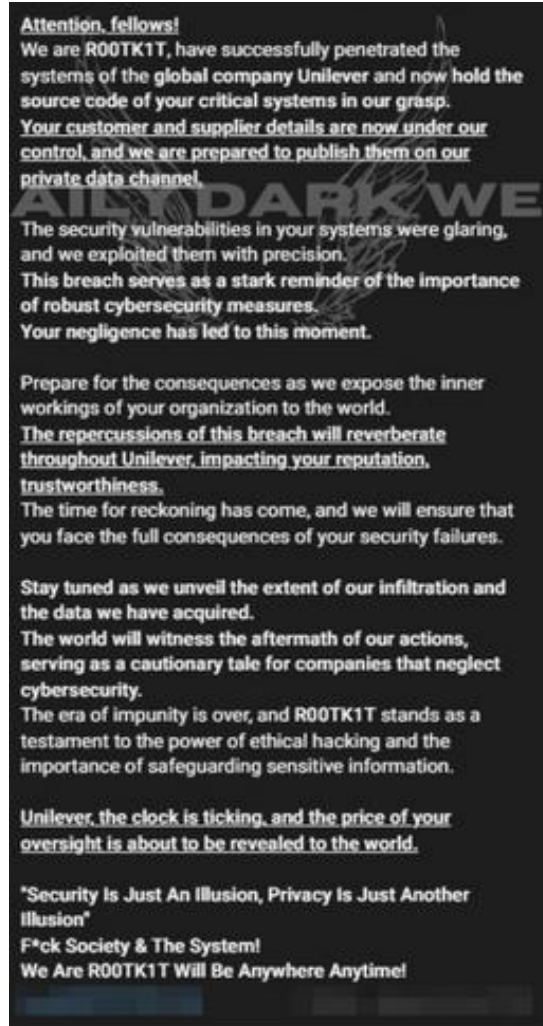
## **Methodology**

This report presents proprietary rising cyber threat data and research from the Smarttech247.

All the facts and statements about to be presented are gathered based on the information that the Smarttech247 team collects as part of its threat intelligence department.

## **Overview**

In recent developments, threat actors claim to have successfully penetrated the systems of the global company Unilever, gaining access to the source code of their critical systems. They assert control over customer and supplier details, and intend to publish them on their private data channel. The threat actors warned that the publication of Unilever's data would impact their reputation and trustworthiness. Additionally, they signalled intentions to target other companies in the future.



**Attention, fellows!**  
We are R00TK1T, have successfully penetrated the systems of the global company Unilever and now hold the source code of your critical systems in our grasp. Your customer and supplier details are now under our control, and we are prepared to publish them on our private data channel.

The security vulnerabilities in your systems were glaring, and we exploited them with precision. This breach serves as a stark reminder of the importance of robust cybersecurity measures. Your negligence has led to this moment.

Prepare for the consequences as we expose the inner workings of your organization to the world. The repercussions of this breach will reverberate throughout Unilever, impacting your reputation, trustworthiness. The time for reckoning has come, and we will ensure that you face the full consequences of your security failures.

Stay tuned as we unveil the extent of our infiltration and the data we have acquired. The world will witness the aftermath of our actions, serving as a cautionary tale for companies that neglect cybersecurity. The era of impunity is over, and R00TK1T stands as a testament to the power of ethical hacking and the importance of safeguarding sensitive information.

Unilever, the clock is ticking, and the price of your oversight is about to be revealed to the world.

"Security Is Just An Illusion, Privacy Is Just Another Illusion"  
F\*ck Society & The System!  
We Are R00TK1T Will Be Anywhere Anytime!

Figure 1 - R00TK1T's message related to the Unilever infiltration  
source: <https://dailydarkweb.net/r00tk1t-allegedly-hacked-unilever-plc-compromising-sensitive-data/>

Unilever PLC, established on September 2, 1929, resulted from the merger of British soap manufacturer Lever Brothers and Dutch margarine producer Margarine Unie. Unilever's extensive range of products encompasses baby food, beauty items, bottled water, breakfast cereals, cleaning products, condiments, energy drinks, healthcare and hygiene items, ice cream, instant coffee, pet food, pharmaceuticals, soft drinks, tea, and toothpaste. It stands as the world's largest soap producer, with its products distributed in more than 190 countries.

## **R00TKIT Hacker Group**

R00TKIT is an internationally recognized hacker group renowned for executing sophisticated cyber intrusions and exploiting software vulnerabilities, primarily focusing on governmental entities and digital infrastructure.

With ties to Israeli forces indicating geopolitical influence, the group primarily targets Muslim countries and territories, encompassing Iran, Lebanon, Qatar, Palestinian territories, Malaysia, and even France.

R00TKIT claimed to have attacked several high-profile targets in the past. Notably, they claimed to have breached the French cosmetic company L’Oreal, stating they acquired its "inner workings" and order database. Furthermore, they alleged to have infiltrated Qatar Airways, claiming to have extracted internal documents, interview recordings, Toolbox Remote Data packages for the carrier’s Boeing 787 fleet, and gained access to navigation software for its Airbus A350.

According to a previous advisory, the R00TKIT group was also responsible for attacks on Malaysia in the past. Moreover, while stating that they “stand with Israel”, they allegedly attacked the Lebanese Social Affairs Ministry.

The hacktivist group also threatened the renowned French company Sodexo, as they claimed that Sodexo had crossed their paths, which made them their primary targets. However, the group has not presented how the company got on their radar, ultimately making them their target and there were no further updates regarding any successful infiltration after the threats were made. The hacktivist concluded their threat by reminding readers in their post that their power knows no bounds, emphasizing that no government or private entity is immune to their actions.

According to previous attacks, the observed behaviour of the R00TKIT group indicates that they target governmental organizations and private sectors worldwide to cause service disruption, web defacement, and perform information leakage. Therefore, all operating systems, web servers, and online services may be susceptible to their activities.

Based on previous alleged attacks, the hacker group announces that they infiltrate their targets via their Telegram channel.

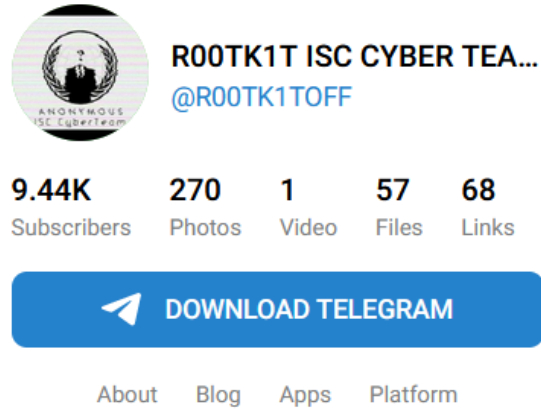


Figure 2 - R00TK1T's telegram channel  
source: <https://t.me/s/R00TK1TOFF?before=477>

Earlier this year, the group attacked Aminia and subsequently provided a link to Aminia's web server login page, which was offline at the time of their announcement of successfully infiltrating the company. The same post also contains screenshots depicting what seems to be the company's backend system, serving as evidence of the group's successful attack.


The message given by the hacker group in the Aminia attack is similar to the one used in the recent announcement regarding Unilever.

Attention, fellows!  
We Are R00TK1T, have successfully infiltrated the fortified walls of Aminia, a telecommunications and oil palm plantation company in Malaysia.  
Prepare yourselves for the storm that is about to unleash upon their unsuspecting servers.

With our expert skills and unrivaled determination, we have breached their defenses, leaving their precious data at our mercy.  
The chaos we shall sow will reverberate through their organization, causing panic and confusion at every turn.  
**Aminia, consider yourselves warned!**

To the employees of Aminia, tremble in fear as we expose your vulnerabilities and weaknesses.  
Your secrets are no longer safe, for we shall dig deep into the darkest corners of your digital existence.  
Prepare for the consequences of your negligence!

We hereby declare our reign of terror upon Aminia and all who dare to challenge our supremacy.  
**The world shall bear witness to the power of R00TK1T!**  
**Stay tuned, for the chaos has just begun**



**"Security Is Just An Illusion, Privacy Is Just Another Illusion"**

Figure 3 - R00TK1T's message related to the Aminia infiltration  
source: <https://www.lowyat.net/2024/315699/r00tk1t-breaches-aminia-backend-systems/>

Another alleged attack made by the hacktivist group targeted Dell. The only information available, as for the prior attacks, is that the group announced that they will attack the company and then they announced that they successfully infiltrated it.

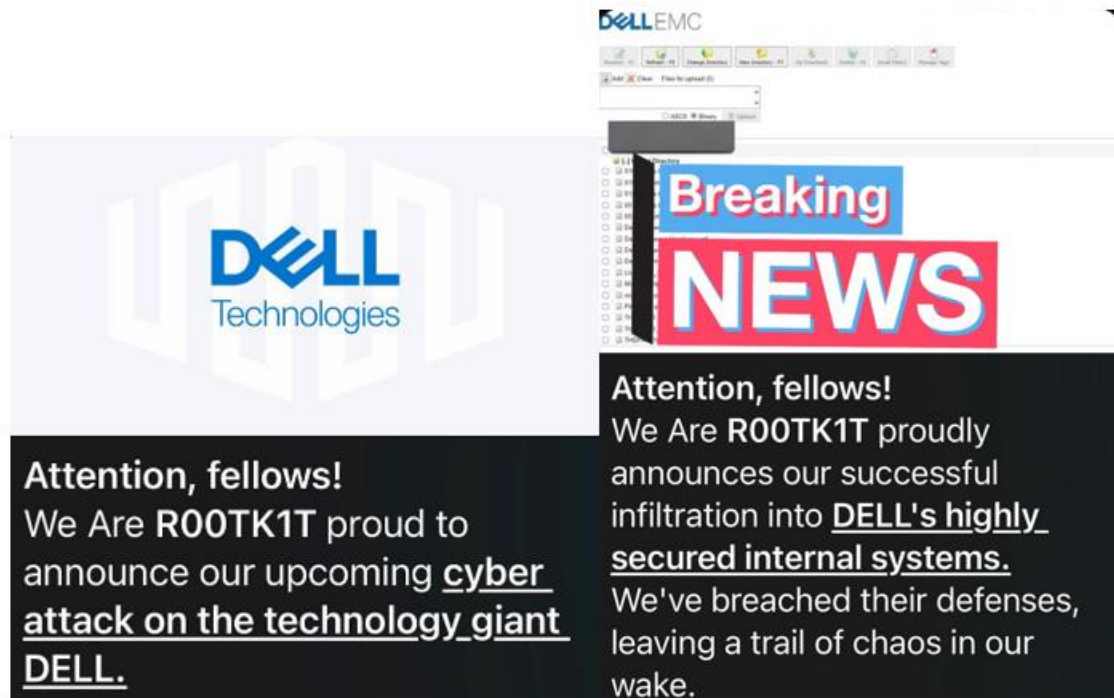


Figure 4 - R00TK1T's messages related to the Dell infiltration

source: [https://twitter.com/ransomfeednews/status/1755184825240018977?t=EsfJMlIBPT2y\\_W6oRd8Vfq&s=19](https://twitter.com/ransomfeednews/status/1755184825240018977?t=EsfJMlIBPT2y_W6oRd8Vfq&s=19)

Although there may not be substantial evidence supporting these claims, the threat posed by R00TK1T remains something that requires serious consideration.

### Alleged Known Targets

- L'oreal
- Qatar Airways
- Ministry of Social Affairs website in Lebanon
- Threats against Sodexo
- Dell
- National Population and Family Development Board of Malaysia



## Alleged Upcoming Targets



Figure 5 – Alleged Upcoming Targets  
 source: <https://t.me/s/ROOTK1TOFF?before=477>

## Recommendations

- **Ensure** the uninterrupted operation of the control system in the presence of faults and achieve swift recovery following any service disruption.
- **Guarantee** that only authorized personnel have access to computing resources within the organization.
- **Verify that computer programs strictly adhere to their intended functionality.** For instance, ensure that a module in a Supervisory Control And Data Acquisition (SCADA) system is configured to receive data from a Programmable Logic Controller (PLC) and save it as intended.
- **Ensure** that only appropriate encryption schemes are used within an organization’s security systems and that the cryptography is used wherever it is needed.
- **Upgrade** software and operating systems, applications, and firmware on network assets in a timely manner for prevention.

- **Use the right Vulnerability Management Tools** to assess endpoint, networks or applications for known weaknesses.
- **Apply the Principle of Least Privilege** to all systems and services.
- **Ensure** that your Endpoint Security and Perimeter security products are updated with the latest signatures to detect these threats.
- **Conduct regular cybersecurity training for employees.** Emphasize the importance of strong passwords, recognizing phishing attempts, and reporting suspicious activities.
- **Implement a robust backup and recovery strategy.** Regularly test backup systems to ensure data can be restored in the event of a cyber incident.

## References

<https://dailydarkweb.net/r00tkIt-allegedly-hacked-unilever-plc-compromising-sensitive-data/>

[https://twitter.com/DailyDarkWeb/status/1775780382941552795?t=cZ\\_DP6uYzY-o8mNk9yXQmA&s=03](https://twitter.com/DailyDarkWeb/status/1775780382941552795?t=cZ_DP6uYzY-o8mNk9yXQmA&s=03)

<https://soyacincau.com/2024/01/29/hacker-group-r00tkIt-threatens-to-attack-malaysias-digital-infrastructure/>

<https://www.lowyat.net/2024/315394/infinix-smart-8-pro-malaysia-31-january/>

<https://www.lowyat.net/2024/315699/r00tkIt-breaches-aminia-backend-systems/>

<https://izoologic.com/region/europe/r00tkIt-hackivist-group-issues-threats-against-sodexo/>

<https://smex.org/attacks-on-lebanons-government-websites-continue-to-implement-protective-standards-immediately/>

<https://today.lorientlejour.com/article/1365266/lebanons-ministry-of-social-affairs-website-hacked.html>

<https://www.cybertecwiz.com/dell-systems-breached-in-recent-cyberattack/>

[https://twitter.com/ransomfeednews/status/1755184825240018977?t=EsfJMIBPT2y\\_W6oRd8Vfg&s=19](https://twitter.com/ransomfeednews/status/1755184825240018977?t=EsfJMIBPT2y_W6oRd8Vfg&s=19)

<https://t.me/s/R00TKITOFF?before=477>

<https://askai.glarity.app/search/What-is-the-R00TK1T-hacker-group--and-what-cyber-threats-have-they-posed-recently>

<https://www.nc4.gov.my/alert/65b5cbec90087b4855570ee1>

<https://www.sangfor.com/blog/cybersecurity/r00tk1t-hacking-group-malaysia-needs-stronger-cybersecurity>