




# APT Group R00TKIT Threat Research Report


MUHAMMAD SAWOOD



## Overview:



In today's dynamic cybersecurity landscape, staying ahead of emerging threats is paramount for organizations and governments to protect their digital assets and ensure operational continuity. Thorough threat research serves as a cornerstone in this endeavor, providing valuable insights into the tactics, techniques, and motivations of malicious actors.



This report focuses on APT group R00TK1T, offering an in-depth analysis of its campaigns, targeted regions, sectors, motivations, and operational timeline spanning from 2022 to 2024. By dissecting the activities of R00TK1T, stakeholders gain actionable intelligence to bolster their defenses, enhance threat detection capabilities, and proactively mitigate the evolving cyber risks posed by this group.

---

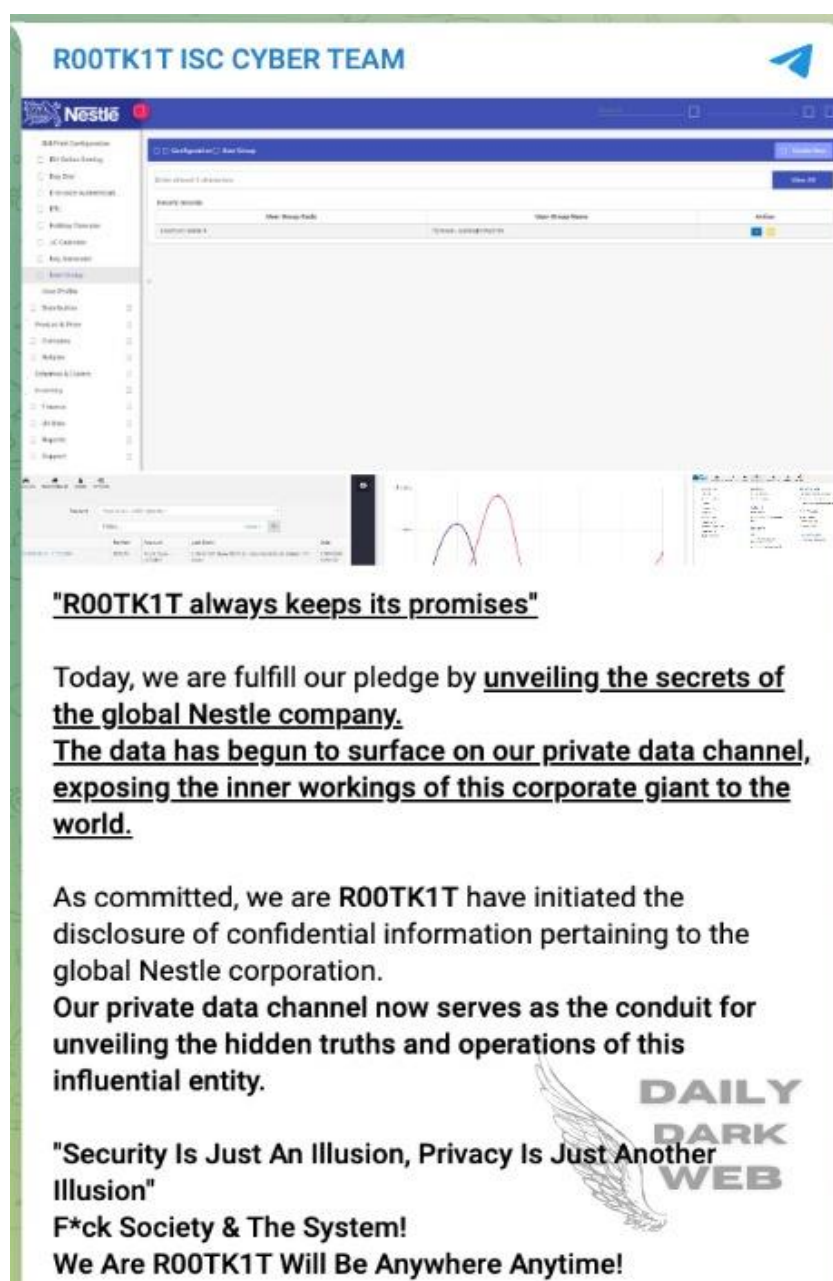
## Who is R00TK1T?

R00TK1T is a relatively new name in the cyber threat landscape, but they have quickly gained notoriety for their bold claims and targeting of high-profile entities. Their motives remain as elusive as their identity. However, we could say that R00TK1T is a group taking geopolitical actions to the next level to support Israel. They recently attacked the DJI drone company because it was exporting drones to Ukraine. It's true that some people endorse the idea that this group is a Russian hacktivist group. However, the evidence suggests that their motivations extend beyond Israel. However, based on research and references, it appears that they are anti-Islamic, as they continue to target Muslim countries. At the heart of R00TK1T's success is their exploitation of human vulnerabilities, from phishing to leveraging insider information.

The consequences of R00TK1T's actions extend far beyond the immediate disruptions. The exposure of sensitive information threatens not just financial losses but national security and international relations. Yet, it's the group's manipulation of fear and misinformation that perhaps poses the most insidious threat, exploiting emotions to sow discord and chaos.

The response to R00TK1T's onslaught requires more than just technical defenses, it calls for a unified and informed approach to cybersecurity. Ensuring robust backup systems, deploying advanced monitoring tools, and fostering a culture of cybersecurity awareness are pivotal steps in weathering this digital storm. Moreover, counteracting misinformation with accurate information becomes crucial in maintaining public trust and confidence.

The declared breach of Nestle by R00TK1T serves as a stark reminder of the ever-present cyber threats facing corporations today.



**R00TK1T ISC CYBER TEAM**

**Nestle**

Security Breach

Security Breach	User Group Name	User Group Role
CONFIDENTIAL	CONFIDENTIAL	CONFIDENTIAL

**"R00TK1T always keeps its promises"**

Today, we are fulfill our pledge by unveiling the secrets of the global Nestle company.  
The data has begun to surface on our private data channel, exposing the inner workings of this corporate giant to the world.

As committed, we are R00TK1T have initiated the disclosure of confidential information pertaining to the global Nestle corporation.  
 Our private data channel now serves as the conduit for unveiling the hidden truths and operations of this influential entity.

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

**DAILY DARK WEB**

Figure 1 Nestle Data Breach  
Source: Forum

As the investigation continues, the incident will fuel the ongoing dialogue about the need for more robust cybersecurity measures in the corporate world.

R00TK1T 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, Palestine, Malaysia, and even France.**

- APT-Group: R00TK1T
- Campaign: R00TK1T
- Alias: r00tk1t isc
- Region: Israel
- APT-Type: Hacktivist
- Targeted Countries: Palestine, Iraq, Lebanon, Iran, Azerbaijan, Qatar, Malaysia, and Pakistan
- Targeted Sectors: Government, Health, Law Enforcement, and Urban Planning
- Motivation: Geopolitical Objectives
- Years: 2022, 2023, 2024

## **Recent Attack by R00TK1T's:**

According to a previous advisory, the R00TK1T 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 R00TK1T ransomware gang, which is usually known for targeting Malaysian organizations, took to Telegram on 15 April to say it was planning to launch a cyber-attack on DJI for supplying drones to Ukraine in its conflict with Russia.

***“In our relentless pursuit of justice and digital warfare, we have set our sights on DJI, a Chinese technology company known for its unmanned aerial vehicles and drones,”*** the R00TK1T group said.

***“Our mission is clear: to disrupt DJI’s operations as they have supplied drones to Ukraine for use in the ongoing conflict against Russia. The skies will tremble as we unleash our cyber arsenal on this complicit entity.”***

***“Prepare for the storm, DJI.”***

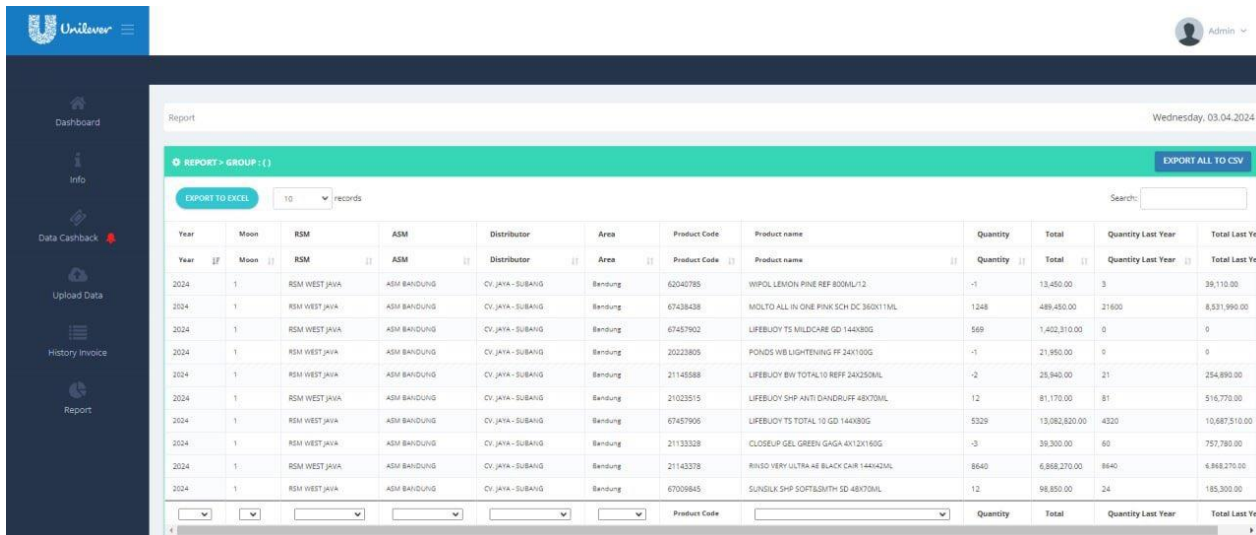
Just a day later (**16 April**), the group said it had successfully breached the company's systems, stealing a **"treasure trove of customer data"** that is now available for sale.

Figure 2 DJI Customer Data  
Source: Twitter

## Declared Known Targets by R00TK1T'S:

- L'oreal
- Qatar Airways
- Ministry of Social Affairs website in Lebanon
- Threats against Sodexo in France
- Dell
- Nestle Data Breach
- Unilever Data Breach
- National Population and Family Development Board of Malaysia
- DJI Data Breach
- Primary and Secondary Health Department of Pakistan
- Digital Landscape of Pakistan





Report

Wednesday, 03.04.2024

REPORT > GROUP: {}

EXPORT TO EXCEL 10 records

Search:

Year	Month	RSM	ASM	Distributor	Area	Product Code	Product name	Quantity	Total	Quantity Last Year	Total Last Year
2024	1	RSM WEST JAVA	ASM BANDUNG	CV. JAYA - SUBANG	Bandung	62040785	WIPOL LEMON PINE REF 800ML/1.2	-1	13,450.00	3	35,110.00
2024	1	RSM WEST JAVA	ASM BANDUNG	CV. JAYA - SUBANG	Bandung	67438438	MOLTO ALL IN ONE PINK SCH DC 360X11ML	1248	489,450.00	21600	8,531,990.00
2024	1	RSM WEST JAVA	ASM BANDUNG	CV. JAYA - SUBANG	Bandung	67457902	LIFEBUOY TS MILDCARE GD 144X80G	569	1,402,310.00	0	0
2024	1	RSM WEST JAVA	ASM BANDUNG	CV. JAYA - SUBANG	Bandung	20223805	PONDS WB LIGHTENING FF 24X100G	-1	21,950.00	0	0
2024	1	RSM WEST JAVA	ASM BANDUNG	CV. JAYA - SUBANG	Bandung	21145588	LIFEBUOY BIV TOTAL 10 BEFF 24X250ML	-2	25,940.00	21	254,890.00
2024	1	RSM WEST JAVA	ASM BANDUNG	CV. JAYA - SUBANG	Bandung	21023515	LIFEBUOY SHP ANTI DANDRUFF 48X70ML	12	81,170.00	81	516,770.00
2024	1	RSM WEST JAVA	ASM BANDUNG	CV. JAYA - SUBANG	Bandung	67457905	LIFEBUOY TS TOTAL 10 GD 144X80G	5329	13,082,620.00	4320	10,687,510.00
2024	1	RSM WEST JAVA	ASM BANDUNG	CV. JAYA - SUBANG	Bandung	21133328	CLOSEUP GEL GREEN GAGA 4X12X180G	-3	39,300.00	60	757,780.00
2024	1	RSM WEST JAVA	ASM BANDUNG	CV. JAYA - SUBANG	Bandung	21143378	RINSO VERY ULTRA 4E BLACK CAIR 144X42ML	8640	6,868,270.00	8640	6,868,270.00
2024	1	RSM WEST JAVA	ASM BANDUNG	CV. JAYA - SUBANG	Bandung	67009845	SUNDOLK SHP SMOOTH 50 48X75ML	12	98,850.00	24	185,300.00

Figure 3 Unilever  
Source: Forum



**Attention, citizens of Malaysia!**  
We are R00TK1T!  
Brace yourselves, for the storm of chaos is brewing. Prepare to witness the collapse of your digital infrastructure, the chaos that will ensue, and the ripple effects that will leave you in disarray.

No system is safe, no data secure.  
We are R00TK1T infiltrate your networks, leaving behind a trail of havoc and destruction.  
Your government, your institutions, your very way of life will crumble under our relentless onslaught.

Stay tuned, for the countdown to chaos has begun.  
Malaysia, prepare for the storm that will leave you shattered and vulnerable.

Figure 4 Malaysia Citizen Data Compromise  
Source: Social Forum

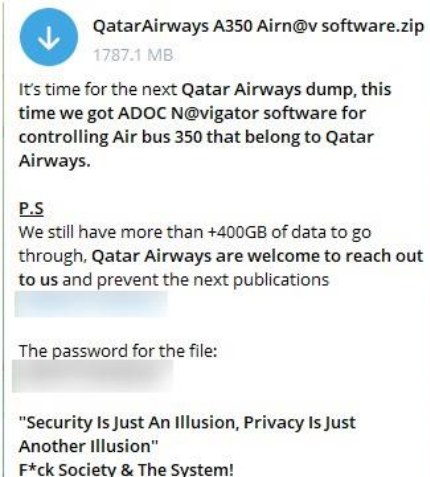
### Attention, world!

We are R00TK1T infiltrated the fortress of L'Oréal, the behemoth of the cosmetics and beauty industry.

No system is safe from our prowess and L'Oréal has fallen victim to our cunning techniques.

we have breached their defenses and gained access to their precious databases. Soon, we shall unveil the secrets within: **customer information, company details, and the inner workings of this industry giant.**

Figure 5 L'Oreal  
Source: Social Forum



QatarAirways A350 Airn@v software.zip  
1787.1 MB

It's time for the next Qatar Airways dump, this time we got ADOC N@vigator software for controlling Air bus 350 that belong to Qatar Airways.

**P.S**  
We still have more than +400GB of data to go through. Qatar Airways are welcome to reach out to us and prevent the next publications

The password for the file:

"Security Is Just An Illusion, Privacy Is Just Another Illusion"  
F\*ck Society & The System!

Figure 6 Qatar Airways Dump  
Source: Twitter

ID	Name	DOB	Gender	Address	Phone	Email	Status
101	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active
102	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active
103	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active
104	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active
105	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active
106	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active
107	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active
108	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active
109	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active
110	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active

As the dark veil of R00TK1T descends upon the digital landscape of Pakistan, our brutal cyber campaign unfolds with calculated precision.

The glaring inadequacies in the security posture of Pakistan stand exposed, a testament to the pervasive vulnerabilities that lurk beneath the surface.

Today, we shatter the illusion of invincibility, revealing the stark truth of how fragile the defenses truly are in the face of our relentless onslaught.

With unwavering determination, we exploit a critical SQL injection weakness within the systems of the Khyber Pakhtunkhwa Government, a gateway to unfettered access and control.

Are you prepared to witness the unfolding saga of R00TK1T cyber crusade, where boundaries blur, and realities shift in the blink of an eye?



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

Figure 7 Landscape of Pakistan  
Source: Breach Forum

ID	Name	DOB	Gender	Address	Phone	Email	Status
101	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active
102	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active
103	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active
104	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active
105	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active
106	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active
107	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active
108	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active
109	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active
110	Ali	1985-01-15	Male	123 Main St, District-1	0300-1234567	ali@district1.gov.pk	Active

**Attention fellows!**

We are R00TK1T, have successfully breached the primary and secondary health departments in Pakistan. As a result, we now hold sensitive information of 6.5 million parents and children across the country.

This data includes personal details such as names, addresses, contact numbers, and medical records.

We are now offering this valuable information for sale to interested parties who wish to gain access to this wealth of data for various purposes.

Figure 8 Health Department of Pakistan  
Source: Breach Forum

## **TTPS:**

### **Hooking:**

**Persistence (T1547):** Hooking can be used to inject code into processes, ensuring persistence.

**Defense Evasion (T1562):** Hooking alters legitimate functions or processes to evade detection.

**Privilege Escalation (T1548):** Intercepting system calls can lead to privilege escalation.

### **Direct Kernel Object Manipulation:**

**Defense Evasion (T1562):** Manipulating kernel objects helps evade detection.

**Privilege Escalation (T1548):** Kernel object manipulation can escalate privileges.

### **Virtualization:**

**Virtualization/Sandbox Evasion (T1497):** Attackers use virtualization to avoid detection in sandboxed environments.

**Persistence (T1547):** Virtualization can be a persistence mechanism via malicious virtual machines.

### **Firmware-Level Rootkits:**

**Boot or Logon Autostart Execution (T1547.001):** Firmware-level rootkits modify firmware settings for persistence.

**Boot or Logon Initialization Scripts (T1037):** They can execute during system boot or initialization.

### **Memory-Based Rootkits:**

**File Deletion (T1107):** Memory-based rootkits manipulate files in memory to avoid detection.

**Process Injection (T1055):** They often inject code into legitimate processes.

In Recent attack R00TK1T Used these techniques which are as follow.

**T1189 - Drive-by Compromise**

**T1218 - Signed Binary Proxy Execution**

**T1586 - Compromise Accounts**



## Detection and prevention of rootkit attacks:

Prevention of rootkits is an essential part of any cybersecurity strategy, given that this malware is hard to detect and remove. Here are some methods to detect and prevent rootkit attacks:

**Anti-malware software:** Scanning systems often for signs of malware, including rootkits, means that anti-malware software can detect and remove these threats before they have a chance to cause damage. Remember though, rootkits can often evade detection by anti-malware software, making it essential to use additional measures to protect systems.

**Regular software updates:** Organizations may limit the chance of vulnerabilities being exploited by attackers by keeping software up to date with the latest security updates and fixes, including those that could be used to install rootkits.

**Use of trusted sources:** To reduce the risk of rootkit attacks, businesses must only purchase software from reliable sources. Official app stores or the websites of respectable software developers are examples of such sources.

**Implementing best practices:** Best practices like using strong passwords, enabling two-factor authentication, and limiting user privileges can help prevent rootkit attacks by reducing the attack surface available to attackers.

**Regular system audits:** Regularly auditing systems for signs of suspicious activity, such as unexpected network traffic or unauthorized changes to system settings, can allow organizations to quickly detect and respond to rootkit attacks, reducing the potential damage caused by these threats.

**Hypervisor Security:** Secure the hypervisor layer to prevent unauthorized virtualization-based attacks.

**Isolation:** Isolate virtual machines from each other to limit lateral movement.

**Code Integrity Checks:** Use code signing and integrity checks to verify the integrity of system files and binaries.

**Least Privilege:** Limit user and process privileges to prevent unauthorized hooking.

**Patch Vulnerabilities:** Apply security patches to address vulnerabilities that allowed the rootkit to manipulate kernel objects.

**Firmware Updates:** Regularly update system firmware (UEFI/BIOS) to patch vulnerabilities.

**Secure Boot:** Enable Secure Boot to prevent unauthorized firmware modifications.

**Process Whitelisting:** Implement process whitelisting to prevent unauthorized processes.

## References:

<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>

<https://dailydarkweb.net/r00tk1t-allegedly-hacked-unilever-plc-compromising-sensitive-data/>

<https://soyacincau.com/2024/01/29/hacker-group-r00tk1t-threatens-to-attack-malysias-digital-infrastructure/>

<https://izoologic.com/region/europe/r00tk1t-hacktivist-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://www.smarttech247.com/news/cyber-threat-intelligence-report-r00tk1t-allegedly-hacked-unilever-plc/>

<https://cybersecuritynews.com/r00tk1t-claims/>

<https://developingtelecoms.com/telecom-technology/cyber-security/16173-r00tk1t-hacker-group-attacks-maxis-posts-stolen-data-on-dark-web.html>

<https://www.cyberdaily.au/security/10445-dji-suffers-alleged-data-breach-at-the-hands-of-r00tk1t>

<https://otx.alienvault.com/pulse/65c064c3cfb1bb5ae5bcba97>