

# Monthly Cyber Threat Intelligence Report

---

August 2024



# Contents

<b>1</b>	<b>Top Breach of the Month: Disney Internal Slack Hack</b>	<b>03</b>
<b>2</b>	<b>Updates: CrowdStrike Fake Repair Manual Incident</b>	<b>05</b>
<b>3</b>	<b>Cyber Security In Brief (June-August 2024)</b>	<b>06</b>
<b>4</b>	<b>Evolving Stories to Watch</b>	<b>09</b>
<b>5</b>	<b>Deepdive into a Threat Actor: APT35 (Charming Kitten)</b>	<b>10</b>
<b>6</b>	<b>Summary</b>	<b>12</b>

Welcome to our latest edition of the Monthly Cyber Threat Intelligence Report.

We like to kick back and relax in the summer, but there's no holiday for cyber criminals. In the last month, we've seen a wave of breaches and will be digging into these across companies ranging from Disney to banking and Formula 1.

We'll update you on existing breaches and investigate some notable stories. Then, in our regular monthly 'deep dive', we'll examine APT35, also known as 'Charming Kitten'.

## Top Breach of the Month

### Disney Internal Slack Hack

In July 2024, [Disney](#) experienced a significant cyber security incident involving its internal Slack channels. A hacking group known as "NullBulge" gained unauthorised access to more than a terabyte of internal communication data from almost 10,000 channels. Nullbulge stated in a blog that the breach was facilitated by a developer installing a compromised [BeamNG](#) game modification on their device. This allowed the attackers to infiltrate Disney's Slack workspace and extract sensitive information.

[Nullbulge](#) is a hacktivist group that claims to be motivated by 'the desire' to protect artists' rights. The group immediately posted an initial dataset from the breach with no ransom demand, but historically, this group has been known for selling its info-stealing data and ransomware groups are driven by financial gain, whatever they state.



#### Impact of the Breach on Disney

[The breach disrupted](#) Disney operations and raised concerns about the overall security of confidential communications. Externally, the breach highlighted vulnerabilities in Disney's cyber security defences.

The breach exposed sensitive corporate information, potential trade secrets, and details of future projects, which could have strategic implications for Disney if competitors leveraged the information competitively.



## Lessons we can learn

The breach shows the importance of securing internal communication platforms and highlights the risks of using third-party communication tools without sufficient security oversight. Furthermore, the breach emphasises the importance of employee awareness and training to recognise phishing attempts and protect their login credentials.

## Recommendations

To enhance cyber security resilience, consider the following recommendations:



### Implement Multi-Factor Authentication (MFA)

Strengthen access controls by requiring at least a password plus a device-based PIN or token, making it more difficult for attackers to verify and gain access with stolen credentials.



### Data Encryption/Loss Prevention

Ensure all communications and data within internal platforms are encrypted at rest, in motion and in transit. Implement real-time monitoring to detect anomalies.



### Employee Training and Awareness Programs

Educate employees across multiple security disciplines, from password strength to phishing attacks and device-based security requirements.



### Regular Security Audits and Penetration Testing

Conduct periodic assessments of security infrastructure to identify and rectify vulnerabilities in communication platforms and other critical systems. If security is outsourced, these tests must be included in the standard contract with your provider.



### Principle of Least Privilege (PoLP)

PoLP significantly reduces the risk of unauthorised access by ensuring users have only the minimum permissions required for their role. By limiting access to potential attackers, PoLP prevents the deployment of infected payloads and other malicious actions.



### Incident Response Planning

Develop and regularly update incident response plans to ensure an effective response to breaches, minimising damage and quickly restoring normal operations.



### Roles-Based Security Controls

Implement Role-Based Access Controls across devices, software and systems access to prevent users from installing code without proper authorisation, reducing the risk of infected payloads being deployed.

# Updates: CrowdStrike Fake Repair Manual Incident

The [CrowdStrike](#) Falcon software incident early in July was not a breach but a software update that caused Windows computers to blue-screen and crash. A fix was quickly issued with apologies, but this incident has provided an ideal opportunity for malware and phishing groups to take full advantage.

The most recent of these involves the distribution of fake CrowdStrike repair manuals designed to deploy the Daolpu [information-stealer](#) malware. The attackers capitalised on the confusion following CrowdStrike's previous software update issues, leveraging the situation to target users seeking fast solutions. The threat actors disseminated fraudulent repair documents that, when

downloaded, installed malware capable of exfiltrating sensitive data from the victim's system. This campaign targeted users via phishing emails and compromised websites promoting the fake manuals.



## Why is this significant?

- **This attack** demonstrates how cyber criminals exploit existing vulnerabilities and public awareness issues to further their goals.
- **The misuse** of CrowdStrike's reputation to propagate malware indicates a highly sophisticated level of social engineering.
- **The deployment** of the Daolpu infostealer underscores the nature of malware threats, as attackers continuously adapt their tactics and leverage social engineering to bypass security measures.



## Lessons we can learn

The CrowdStrike incident provides critical lessons:

### The Importance of Timely Communication:

Organisations must ensure rapid and clear communication during software issues or breaches to reduce or remove the opportunity window for misinformation and malicious exploitation.

### Awareness of Social Engineering Tactics:

The use of fake repair manuals exemplifies the ongoing threat posed by social engineering. Training users to recognise and report suspicious communications can reduce the risk of attacks.

# Cyber Security In Brief (June-August 2024)

## Roblox Vendor Data Breach Exposes Conference Attendee Information

On 5th July, using a [post on X](#), Roblox announced that a data breach involving a third-party vendor had exposed [personal information](#) from attendees of the Roblox Developer Conference between 2022 and 2024.

The breach occurred when an unauthorised party accessed a vendor database containing details, including the conference participants' names, email addresses, and other identifiable information. This spotlights the risks with third-party vendors. As organisations increasingly rely on external service providers, the security posture of these vendors becomes critically and equally important as their own.



## Formula 1 Governing Body Data Breach



The Formula 1 governing body, the Fédération Internationale de l'Automobile (FIA), [recently disclosed](#) a data breach caused by unauthorised access to its email systems. Cyber criminals used phishing to exploit email vulnerabilities and access sensitive information. [The breach came](#) to light when the internal security team spotted unusual activities and cut access before starting an internal investigation.

This breach is significant due to the nature of the data handled by the FIA, including confidential communications and proprietary information related to Formula 1, World Rally and global motorsport. The incident underlines the vulnerability of email systems, which remain a primary target for cyber criminals seeking to access high-profile, sensitive information.

Lessons from this breach highlight the importance of robust email security measures, including multi-factor authentication (MFA), regular security audits, and user training to recognise phishing attempts. It also demonstrates the need for proactive monitoring and rapid response capabilities to identify and mitigate unauthorised access.

## TeamViewer Cyber Attack Exposes Encrypted Passwords

[A recent cyber attack on TeamViewer](#) exposed its employee directory and encrypted passwords. The attackers gained access through a phishing campaign that targeted employees with legitimate-looking emails, tricking them into revealing their login credentials. Once inside the network, the attackers could access the internal directory and retrieve encrypted password hashes.



TeamViewer provides remote access capabilities to users and organisations worldwide, making this a significant break that poses a risk to internal security and users if leveraged to exploit further vulnerabilities. The attack highlights the constant threat of phishing campaigns and the importance of securing internal networks against unauthorised access.

## Hackers Exploit API to Verify Millions of Authy MFA Phone Numbers



On 1st July 2024, Twilio released a [security update](#) related to a recent security incident revealing that hackers exploited an API vulnerability in Twilio's Authy service to verify millions of multi-factor authentication (MFA) phone numbers.

The attackers used a technique known as [enumeration](#), which allowed them to check whether specific phone numbers were registered with Authy, thereby identifying which numbers were used for MFA. This vulnerability was exploited by automating the

verification process through an exposed API endpoint, potentially compromising user privacy and security.

The breach has implications for MFA security, a critical component of many organisations' cyber security strategies. By validating phone numbers associated with MFA, attackers can target specific accounts for further attacks, such as phishing or SIM swapping, to gain unauthorised access to sensitive accounts.

## What can we learn from these cyber incidents?

As we examine these breaches, attacks and data thefts, there are recommendations we can look to for implementation in our environment. There's always a new method of attack, meaning there's always something new to learn in keeping the bad actors on the outside. The following bullets are considerations across the stories in this section:



Implement additional layers of security beyond SMS-based MFA, such as hardware tokens or app-based authentication. Regular security audits and real-time monitoring can help detect and respond to suspicious activity.



Organisations should apply comprehensive email security protocols to improve cyber resilience, including end-to-end encryption and stringent access controls. Regular penetration testing and system updates are crucial to protect against evolving threats.



Stringent vendor management and regular security assessments of third-party partners are requirements, not an option. To mitigate such risks, design and enforce robust due diligence processes and maintain clear vendor security standards.



API endpoints need robust security. These should include strict rate limiting, authentication checks, and monitoring of unusual activity. Any organisation using APIs needs to conduct regular security assessments of their APIs to identify and mitigate vulnerabilities.

## Evolving Stories to Watch

There are too many cyber security stories to report every month, but in this section, we summarise some of the incidents worth reading that could evolve further before our next report update.

### Patelco Credit Union Ransomware (June 2024)

Patelco Credit Union were targeted by a ransomware attack, locking users out of their bank accounts and causing significant disruption. Attackers infiltrated the credit union's network through a phishing email campaign, deploying ransomware that encrypted critical systems and customer data.

(<https://arstechnica.com/tech-policy/2024/07/everythings-frozen-ransomware-locks-credit-union-users-out-of-bank-accounts/>)

### Evolve Bank Data Breach (June 2024)

Evolve Bank suffered a data breach exposing customer data, including Social Security numbers and account details. This breach increased the risk of identity theft and fraud for affected customers.

(<https://www.spiceworks.com/it-security/cyber-risk-management/news/investigation-finds-lockbits-attack-impacted-7-6-million-americans/>)

### Neiman Marcus Data Breach (July 2024)

A breach linked to vulnerabilities in Snowflake's systems impacted over 64,000 customers. Attackers accessed customer information, including names and contact details. The hacker responsible, Sp1d3r, has suggested that a ransom was demanded but not paid by Neiman Marcus. The data is now being advertised on the dark web for sale.

(<https://www.darkreading.com/cloud-security/nieman-marcus-customers-impacted-snowflake-data-breach>)

### LockBit Ransomware Attack on Federal Reserve (July 2024)

The LockBit group claimed responsibility for a ransomware attack on the US Federal Reserve, allegedly compromising 33 TB of data. However, this story has fizzled somewhat since it's turned out that the data—still a breach—only relates to a single bank in Arkansas, USA.

(<https://www.techtarget.com/searchsecurity/news/366591934/LockBit-claim-about-hacking-US-Federal-Reserve-fizzles>)



# Deepdive Into a Threat Actor:

## APT35 (Charming Kitten)

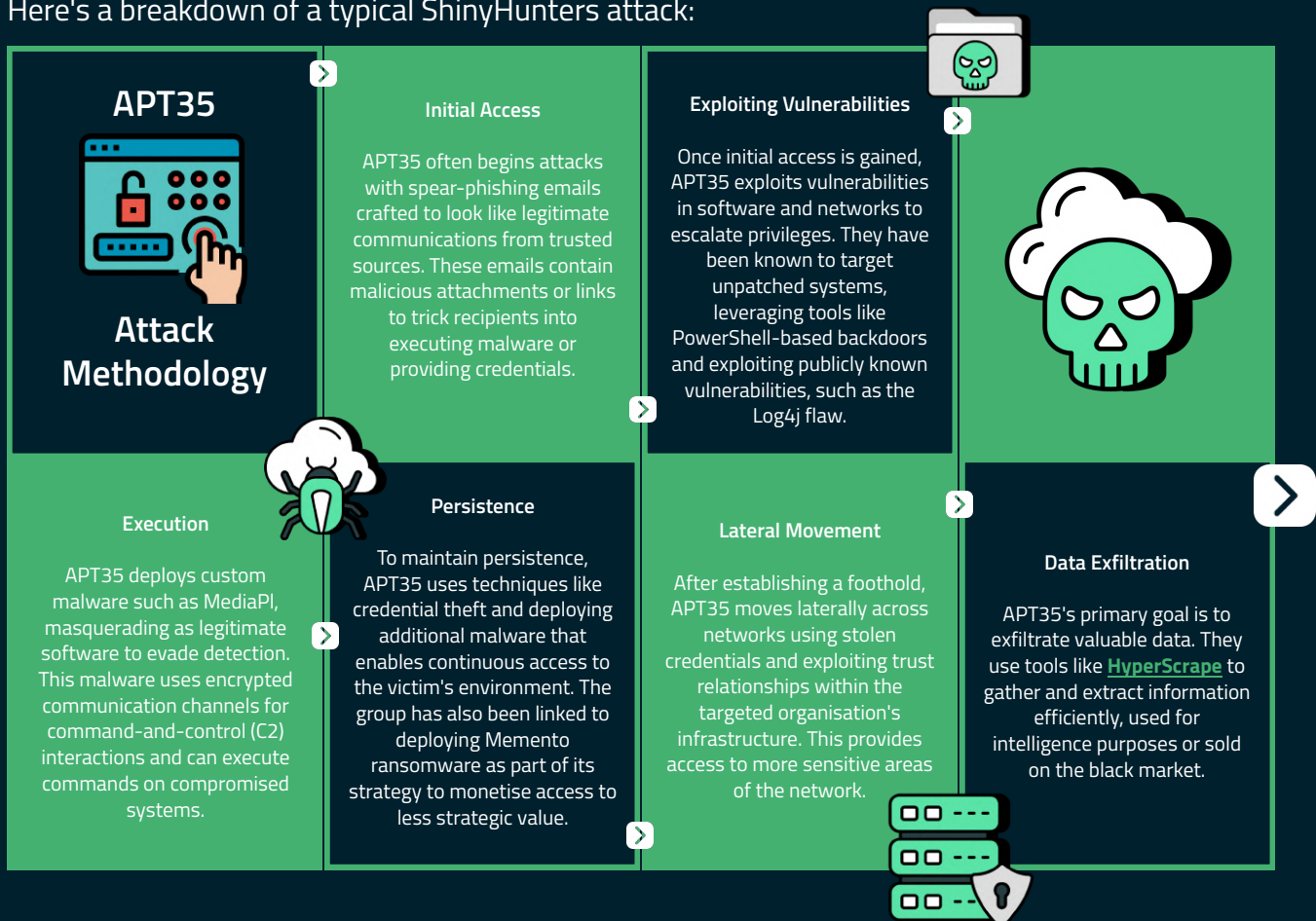
APT35, also known as Charming Kitten or Phosphorus, is a state-sponsored cyber espionage group linked to the Iranian government. This group is known for conducting complex and resource-intensive operations to collect intelligence, mainly targeting individuals and organisations involved in Middle Eastern affairs, journalism, and other sectors with strategic value.

Recent campaigns by APT35 have highlighted their evolving tactics and increased sophistication in targeting high-profile entities across Europe and the United States. [Microsoft issued a statement](#) warning about the potential involvement of APT35 in the Presidential campaign.

### Typical Attack Chain

ShinyHunters is infamous for employing sophisticated tactics, techniques, and procedures (TTPs) to breach security defences and exfiltrate data.

Here's a breakdown of a typical ShinyHunters attack:



### Who They're Actively Targeting



APT35 targets a wide range of sectors, focusing on high-value individuals who can provide insights into geopolitical issues and other strategic interests of the Iranian government. Recent campaigns have targeted researchers and professionals working on Middle Eastern policy issues.

# Recommendations

Detecting APT35 on your network requires monitoring specific Indicators of Compromise (IOCs), recognising their tactics, techniques, and procedures (TTPs), and employing robust security measures.

## Detection Recommendations

1. Look for emails with suspicious attachments or links, especially job postings, resumes, or official-looking communications that might lead to credential harvesting pages.
2. The group is known for deploying malware such as MediaPI, PowerLess, and IMAPLoader. Ensure your antivirus and endpoint detection systems include the latest signatures for these malware variants.
3. Monitor for unexpected outbound network traffic, especially encrypted connections to command-and-control (C2) servers. APT35 uses custom encryption for their C2 communications, which can indicate compromise.
4. Implement multi-factor authentication (MFA) and monitor for failed login attempts or unusual access patterns.
6. The group uses persistence techniques, such as web shells on compromised servers or creating scheduled tasks. Regularly audit scheduled tasks, startup folders, and web server directories.
7. Look for anomalous login activity, such as lateral logins to sensitive systems, and employ network segmentation to limit movement.

## Mitigation Recommendations

1. Deploy advanced email filtering and anti-phishing technologies. Train employees to recognise phishing attempts and report suspicious emails.
2. Use network intrusion detection systems (NIDS) to monitor traffic for known APT35 C2 patterns. Employ tools like Security Information and Event Management (SIEM) to correlate alerts and identify potential threats.
3. Ensure that endpoint detection and response (EDR) solutions are in place to detect and respond to suspicious activities, such as unauthorised software execution or unexpected file modifications.
4. Subscribe to threat intelligence services to stay updated on the latest IOCs and TTPs associated with APT35. Use this information to update security measures and inform incident response plans proactively.
5. Develop and regularly test an incident response plan designed to handle sophisticated threats. Ensure that all staff members know their roles during a breach.

If you would like to discuss how e2e-assure can help to develop a cyber resilient approach to security, don't hesitate to contact us at [cti@e2e-assure.com](mailto:cti@e2e-assure.com). One of our team will assist you.





## Let's connect!

That concludes this month's edition of our cyber security newsletter. We hope you found the insights and updates in this report useful.

Stay tuned for next month's newsletter, where we will bring you the latest developments, in-depth analyses, and expert advice to help you stay ahead in cyber security. We can't wait to share more with you. Until then, remain vigilant and proactive in your defence strategies.

We always look for ways to improve and would love your feedback. Your suggestions and the topics you want us to cover in future editions are important. Please email us at [cti@e2e-assure.com](mailto:cti@e2e-assure.com).