AIVD and MIVD identify new Russian cyber threat actor

This is a joint publication of the Netherlands General Intelligence and Security Service (AIVD) and the Netherlands Defence Intelligence and Security Service (MIVD). An accompanying press release has been published on the websites of the AIVD and the Ministry of Defence of the Netherlands.

1. Summary

- The AIVD and MIVD ('the Dutch services') have identified a publicly unknown, highly probably Russian state-supported threat actor and have named the group LAUNDRY BEAR.

- LAUNDRY BEAR is responsible for conducting various cyber operations against Western government organisations since 2024 and is specifically interested in the armed forces, government organisations, defence contractors, social and cultural organisations, and digital service providers.

- This investigation into the threat actor was initiated because of an opportunistic cyber attack on the Dutch police in September 2024. During this attack the work-related contact information of police employees was obtained by the threat actor. The Dutch services and the police have not been able to ascertain that other information was obtained. It is highly probable that other Dutch organisations were also a victim of this threat actor.

- LAUNDRY BEAR has successfully managed to fly below the radar by employing simple attack methods and attack vectors involving tools which are readily available on victims' computers and are therefore difficult for organisations to detect and distinguish from other known Russian threat actors.

2. Origins and attribution

On 23 September 2024, the Dutch police was a victim of a cyber attack resulting in the loss of the work-related contact information of all police employees to a threat actor. Subsequent technical investigations by the Dutch services revealed that the cyber attack was the work of a previously unknown highly probable Russian state-supported threat actor.

The Dutch services have named this threat actor LAUNDRY BEAR.[1] The investigations also revealed that LAUNDRY BEAR has been mounting cyber attacks against Western government organisations, commercial entities and other organisations since at least 2024. As such, LAUNDRY BEAR appears to be a relatively new threat actor. The Dutch services consider LAUNDRY BEAR and its target selection to be consistent with previously established patterns in Russia's state-sponsored offensive cyber programme targeting the West and Western interests.

The services are now making this information public even though a complete picture of this threat actor and their activities has not yet been formed. The intention of the Services at this time is to raise awareness to enable others to take the right resilience measures to better protect organisations.

2.1 Actor activity

Based on a technical investigation conducted in concert with the Dutch police, the Dutch services have succeeded in gaining insight into the activities of LAUNDRY BEAR, including information on the countries and sectors targeted by the threat actor.

2.1.1 Cyber operation typology

The non-destructive cyber attacks conducted by LAUNDRY BEAR to date highly probably indicate an espionage motive. Technical investigation by the Dutch services reveals that LAUNDRY BEAR has successfully gained access to sensitive information from a large number of government organisations, commercial entities and other organisations around the world, with a specific interest in European Union and NATO member states. The group obtains this

[1] The AIVD and MIVD are working with Microsoft in the investigation into LAUNDRY BEAR. Microsoft tracks this threat actor as Void Blizzard.

information by penetrating (cloud-based) email environments, in particular exchange servers. LAUNDRY BEAR's process involves the rapid and large-scale theft of email messages and other information relating to an organisation's email contacts, such as a Global Address List (GAL). This information may be obtained when a threat actor has gained access to a user account. The Dutch services have ascertained that in some cases LAUNDRY BEAR has also managed to obtain files, including data stored on cloud servers.

*2.1.2 **Targeting***

Similar to other Russian cyber threat actors, LAUNDRY BEAR targets countries that are European Union or NATO members. Almost all of the countries within these international coalitions are targeted by the threat actor. LAUNDRY BEAR primarily targets entities that are relevant to Russia's war efforts in Ukraine: NATO member defence ministries, their ambassadors to other organisations, branches of the armed forces and defence contractors. In keeping with Russian threat actors conducting espionage activities in the West, LAUNDRY BEAR also attacks foreign affairs ministries and EU institutions. Apart from targeted cyber attacks against EU and NATO member states, the Dutch services have also identified attacks by LAUNDRY BEAR against entities in other regions, especially in East- and Central-Asia.

In 2024, LAUNDRY BEAR mounted attacks against defence contractors, aerospace firms and other high tech businesses involved in military production. Technical investigation of the victims revealed that LAUNDRY BEAR highly probably intended to obtain sensitive information relating to the procurement and production of military goods by Western governments, and weapons deliveries to Ukraine from Western countries. The Dutch services have noticed that the group appears to have some degree of knowledge about the production and delivery of military goods and the corresponding dependencies. Furthermore, LAUNDRY BEAR has mounted cyber attacks against businesses producing advanced technologies which are difficult for Russia to obtain due to Western sanctions. Given the current information, it is not possible to say with certainty what the exact goals of these espionage attacks might be.

This threat actor has also displayed a broader range of interests, with civilian organisations and commercial businesses being targeted as well. Those attacks tend to focus on the IT and high tech sectors, including digital service providers to enterprise customers, such as government organisations. Networks operated by these organisations often not only include information relating to processes but also afford direct or indirect access to information or networks of their clients (which may include government organisations), making them targets of choice for cyber threat actors.[2] Furthermore, the Dutch services have observed that LAUNDRY BEAR has also targeted non-governmental organisations, political parties, media and education organisations. Finally, the services have seen attacks targeting several critical sectors, highly probably exclusively for espionage purposes. Compared to some other Russian threat actors under investigation by the services, LAUNDRY BEAR has a high success rate. For the most targeted sectors see figure 1.

Figure 1: overview of most targeted sectors

[2] The penetration of an organisation by a threat actor by first compromising a trusted supplier is known as a supply chain attack.

*2.1.3 **Attacks targeting Dutch interests***

In September 2024, LAUNDRY BEAR gained access to an account belonging to a Dutch police employee. The actor then succeeded in stealing the work-related contact information of police employees through the GAL. The technical investigation revealed that the threat actor highly probably targeted the Dutch police opportunistically using a pass-the-cookie attack.[3] This is an attack in which the threat actor poses as the owner of a cookie. Based on the technical investigation, the Dutch services believe that the cookie was likely stolen using infostealer malware, possibly operated by a third party, and was then bought by LAUNDRY BEAR via a criminal marketplace. Using the stolen cookie, the threat actor could then gain access to certain information without having to enter a username and password.

Neither the Dutch services nor the Dutch police have been able to ascertain whether LAUNDRY BEAR was able to exploit the account in question to obtain any data apart from the GAL. The technical investigation revealed that other organisations in the Netherlands have highly probably also fallen victim to LAUNDRY BEAR.

2.2 Impact of technology on speed and success of attacks

Because LAUNDRY BEAR conducts its cyber operations at a rapid pace, the Dutch services consider it highly probable that the threat actor conducts these operations with some level of automation. Given the number of attacks in a short time span, the automation appears to be efficiently organised, with the chosen attack methods resulting in a high number of successful compromises.

LAUNDRY BEAR uses relatively simple techniques, which in some cases can also be difficult to detect. As far as the Dutch services can ascertain, LAUNDRY BEAR does not seem to be using its own custom malware but is successfully exploiting living-off-the-land (LOTL) techniques,[4] which emphasises the opportunistic nature of the actor.

The group attempts to use phishing or authentication tokens or cookies retrieved through criminal marketplaces to gain access to targets.[5] LAUNDRY BEAR also employs password spraying, an attack method in which threat actors attempt to access large numbers of accounts using only a few commonly used passwords. With this technique, the number of login attempts for a given account is spread over time by first using the same password to try to log into other accounts before trying a different password. The benefit of this is that network monitoring tools and system administrators will not receive alerts of failed logins, allowing the threat actor to remain unseen. This differs from standard brute force attacks where a threat actor repeatedly tries to log into a single account in a short space of time. The list of passwords used in a password spraying attack typically consists of compromised passwords which have been published online following data breaches. These lists typically include passwords such as *password123*, *welcome123* and *qwerty*, which work more often than expected.

After being successfully authenticated and obtaining access to an account, LAUNDRY BEAR approaches victims through Microsoft Exchange Web Services (EWS) and Outlook Web Access (OWA) in an attempt to run certain actions on victim networks. The Dutch services consider it highly probable that LAUNDRY BEAR first tries to download the GAL. Information from the GAL is then used for password spraying attacks to gain access to other accounts. Investigation has revealed that the threat actor is specifically interested in mail accounts that manage other accounts (delegated access). In a successful attack, LAUNDRY BEAR manages to expand its access within the compromised Microsoft environment, highly probably allowing the group to collect emails and other information from the environment. Technical investigation has revealed that LAUNDRY BEAR is capable of stealing email messages from compromised systems at scale. In some cases, the Dutch services have established that LAUNDRY BEAR has stolen data from compromised SharePoint environments, where the group exploits known vulnerabilities to collect login credentials for later operations. Because LAUNDRY BEAR highly probably restricts its actions to existing access to

[3] A cookie is a small text file that is saved by a website on a user's computer or mobile device to collect and store information about the user, such as browsing behaviour and login credentials. One use of cookies is to allow a user to stay logged into a website.

[4] Living-off-the-land refers to a tactic in which a threat actor uses existing systems and the native tools available on the victim's computer or network to mount an attack rather than introducing malware. One benefit of this is that the threat actor leaves fewer traces behind. It makes detection difficult for security systems because the activities appear to come from a legitimate user.

[5] Phishing is where a target is mislead by email (or other messaging systems), where that message contains something other than is clear at first glance. It is likely that LAUNDRY BEAR uses themes in their phishing mails to targets that align with their interests.

Microsoft accounts without attempting to expand its access to underlying networks or systems, it appears to have flown under the radar of network and system administrators relatively easily and for an extended period.

The Dutch services are working closely with Microsoft in the investigation into LAUNDRY BEAR to mitigate the abuse of Microsoft's systems.

2.2.1 LAUNDRY BEAR and APT28

Many of the attack vectors used by LAUNDRY BEAR are also used by other cyber threat actors, highly probably because the techniques used are not particularly complex and therefore easier to deploy. An additional benefit for the actor is that it makes attribution to a particular group especially difficult.

During the investigation into LAUNDRY BEAR, the Dutch services regularly observed certain similarities between these attacks and the modus operandi of APT28. APT28 is a Russian state-sponsored threat actor which the MIVD attributes to Unit 26165 of the Russian military intelligence service GRU. In addition to a similar target selection, there are also similarities in using password spraying attacks. Nevertheless, LAUNDRY BEAR and APT28 are two distinct threat actors.

2.3 The outlook on LAUNDRY BEAR

The Dutch services consider LAUNDRY BEAR to be an emerging threat actor and consider it possible that the group will add more complex attack vectors to its arsenal going forward. The information stolen from the GAL may also be used in later attacks, including spearphishing. As a relative newcomer it is challenging to assess the outlook on LAUNDRY BEAR. Given that LAUNDRY BEAR makes a significant impact using automated techniques, the services assess the corresponding espionage threat level as high.

3. Resilience measures

The Dutch services have decided to release information on the attack vectors employed by LAUNDRY BEAR to offer insight into the group's methods. The services use the MITRE ATT&CK framework[6] to report on resilience measures that can be taken.

Tactic	Technique ID	Technique name
Initial Access / privilege escalation	T1078	Valid accounts
Persistence / privilege escalation	T1098.002	Account manipulation
Credential access	T1539	Steal web session cookie
Credential access	T1110.003	Password spraying
Discovery	T1087	Account discovery
Collection	T1114.002	Remote email collection
Command and control	T1090	Proxy
Exfiltration	T1048.003	Exfiltration over alternative protocol (non-C2 protocol)

3.1 Gaining access via valid accounts (T1078)

Threat actors may obtain and abuse credentials as a means of gaining initial access, persistence, privilege escalation or defence evasion.

Mitigation and recommendations:

- **Use Least Privilege principles** Users and services are assigned the lowest possible privileges needed to perform their tasks, thereby minimising potential damage.

- **Implement Privileged Access Management (PAM)** PAM can be used to audit for, monitor and reduce accounts with elevated privileges. This can help with the detection and prevention of accounts with unauthorised elevated privileges.

- **Implement Zero-Trust architecture** Consider implementing a zero-trust security architecture that treats all users and devices on or off the network as potentially untrusted and only grants access subject to strict authorisation and verification processes.

- **Use strong authentication** Implement multifactor authentication (MFA) to prevent threat actors from gaining access to accounts using only a password, even if they have the password.

3.2 Account manipulation: additional email delegate permissions (T1098.002)

In the case of account manipulation, threat actors may grant additional permission levels or privileges to existing email accounts to expand access to sensitive information or systems, or to maintain persistent access to an adversary-controlled email account. This can be done in various ways, such as by granting additional privileges, changing group memberships and changing user privileges.

This type of attack is dangerous as it can be difficult to detect. Threat actors may use existing accounts that are trusted by the system so that activity is less conspicuous compared to the creation of a new account with suspect privileges.

[6] More information on the MITRE ATT&CK framework is available at attack.mitre.org.

Mitigation and recommendations:

- **Audits** Regularly audit user accounts and the corresponding privileges.
- **Access management** Enforce strict monitoring of access management according to the least privilege principle. This ensures users have only privileges that are absolutely essential for the tasks they perform.
- **Logging and monitoring** Enforce logging and monitoring of account activity to receive alerts about unusual changes to user privileges or user behaviour.

3.3 Steal web session cookie (T1539)

Threat actors may attempt to steal web application or service session cookies and use them to gain access to networks as an authenticated user without needing credentials. Cookies are probably obtained from criminal marketplaces after being stolen by other malicious actors using malware such as infostealer.

Mitigation and recommendations:

- **Device management** Do not allow users to bring their own device (BYOD), such as a personal laptop or smartphone, or restrict their use to a bare minimum. Enforce centralised device management for all devices that have access to the organisation's IT systems. This reduces the chance of malware-infected devices being allowed onto the network. It also allows the organisation to better monitor device behaviour. The risk from session cookie theft is greater in an organisation that does not enforce centralised device management.
- **System management** Only use managed systems to access sensitive environments such as SharePoint and Exchange Online. Permit access to critical accounts only from trusted IP addresses.
- **Cookie expiration** Set cookies to expire as quickly as practically possible to reduce the window of opportunity within which a threat actor can gain access. This immediately serves to reduce the usability of a stolen cookie with an access token. Choosing the right expiration time for session cookies is a trade-off between user convenience and security.
- **Browser cookies** Enforce routine deletion of browser cookies and monitor at set intervals as a matter of security policy.
- **Session rebinding** Disable session rebinding so that a session cookie may only be used by a single IP address. This makes it extremely difficult to use stolen session cookies.
- **Conditional access** Consider implementing conditional access to restrict user logins to specific IP address locations, IP address ranges or specific devices.
- **Multifactor authentication** Implement phishing-resistant MFA based on FIDO2 hardware tokens.
- **ID protection** Consider using Microsoft Entra ID Protection or comparable solutions from Amazon Web Services (AWS) or Google. These can help detect pass-the-cookie type attacks.

3.4 Brute force: password spraying (T1110.003)

Password spraying is a type of cyber attack in which threat actors use a small list of commonly used passwords against many different accounts in an attempt to acquire valid account credentials. Traditional brute force attacks target a single account with a large set of passwords, while password spraying attacks target multiple accounts with a small set of weak or commonly used passwords. In some cases, threat actors will run password spraying attacks very slowly with only a few login attempts per hour.

Mitigation and recommendations:

Organisations may detect an attack by inspecting the logfiles of applications, networks or cloud environments for unusually high levels of login failures for multiple accounts. Because login attempts may originate from different IP

addresses, it is prudent to develop a detection logic that detects multiple login failures within a predefined timeframe. The timeframe chosen will depend on normal levels of traffic within the organisation. Traditional detection based on IP address location will often prove ineffective because of the use of residential proxies.[7] The following measures may offer protection from password spraying attacks.

- **Authentication logs** Monitor authentication logs of systems and applications for login failures of valid accounts.

- **Monitor login attempts** as a matter of routine and implement security tools capable of detecting suspicious patterns such as rapid successive login attempts from a single IP address.

- **Old accounts** Disable old or inactive user and administrator accounts. Threat actors home in on these accounts to obtain initial access.

- **Set maximum login attempts** To help combat password guessing, set policies for account lockout after a predetermined number of login failures.

- **Multifactor authentication** Use MFA based on authenticator apps or hardware tokens.

- **Exclude** Block any IP addresses either temporarily or permanently that are the source of multiple login attempts.

- **Conditional access** Consider implementing expanded conditional access with conditions other than IP location. Conditional access allows users to log in using valid credentials only when other conditions are also met, such as group membership, device specifications and use of prescribed applications. Using only IP location for conditional access does not offer sufficient protection against password spraying because threat actors may obfuscate or spoof their login location.

- **ID protection** Consider using Microsoft Entra ID Protection or comparable solutions from AWS or Google. Solutions like these can help your organisation detect malicious login attempts.

3.5 Account discovery (T1087)

Threat actors may attempt to obtain a listing of valid accounts, usernames or email addresses on a system or within a compromised environment. This information can help threat actors take targeted action including brute force attacks, spearfishing attacks or unauthorised account takeovers.

Various techniques can be used to expose credentials including abuse of native system admin tools, built-in system commands and config error exploits that cause unwanted exposure of accounts, roles and privileges.

Cloud environments can be particularly vulnerable because they often offer interfaces which allow relatively easy access to user lists. Threat actors may also use standard PowerShell features and other command line tools on endpoints to identify accounts. Email addresses and credentials can be extrapolated by running malicious searches against files in a compromised system.

Mitigation and recommendations:

Effective defence requires a proactive strategy focused on minimising account detection risks, monitoring unusual behaviour and strengthening access controls. The following measures can help reduce risk:

- **Multifactor authentication** Ensure all accounts have additional authentication layers to prevent unauthorised access even when credentials have been compromised.

- **Least Privilege Access** Limit user privileges to the bare minimum necessary for their roles so that threat actors have only minimal access even after a compromise.

[7] A residential proxy is a type of proxy server that uses IP addresses assigned by a genuine internet service provider to a residential household. This means that the IP address used by the proxy looks like a normal home network so would not ordinarily be flagged as a proxy.

- **Security Information and Event Management (SIEM)** Implement a SIEM solution to monitor login attempts and account-related activity in real time, enabling rapid detection of unusual activity.

- **Restrict account enumeration** Configure systems and applications so that usernames and email addresses are not exposed to threat actors on public interfaces or in error messages.

- **Awareness and training programmes** Ensure that users can recognise and report phishing attempts, social engineering and account abuse.

- **Security audits and misconfiguration checks** Conduct periodic audits to identify and immediately remedy unwanted exposure of accounts, permissions and roles.

3.6 E-mail collection: remote email collection (T1114.002)

Threat actors may steal emails using external access to email servers or cloud-based email platforms such as Microsoft Exchange Online (Office 365). Threat actors often use stolen login credentials, access tokens or unauthorised API access to gain direct access to mailboxes and email archives.

This type of attack can be particularly harmful for organisations because emails often contain business-critical information. Furthermore, threat actors are becoming increasingly proficient in filtering and automating their searches within email environments to collect relevant data quickly.

Mitigation and recommendations:

- **Multifactor authentication** Enforce MFA for access to email platforms, preferably using hardware or app-based methods rather than SMS.

- **Access limits** Check and limit API access and use context-sensitive access controls.

- **Anomaly detection** Implement monitoring tools to detect unusual login attempts and data traffic.

- **Awareness and training programmes** Ensure that users recognise phishing attempts and renew access codes on a regular basis.

- **Encryption and DLP** Encrypt sensitive emails and enforce data loss prevention (DLP) policies.

3.7 Proxy (T1090)

Threat actors may use a connection proxy to direct network traffic between systems or act as an intermediary to a command and control (C2) server to avoid direct connections to their infrastructure and complicate detection. Threat actors use proxies to manage C2 communications, to reduce the number of simultaneous outbound network connections, provide resilience in the face of connection loss, or utilise existing trusted network paths to avoid suspicion.

Threat actors may chain together multiple proxies (multi-hop proxy) to further disguise the source of their activities. They may also take advantage of routing schemes used by content delivery networks (CDNs) to obfuscate C2 traffic and ensure it uses trusted routes.

Mitigation and recommendations:

- **Network segmentation** Ensure that sensitive systems and networks are segregated from low trust environments to limit the freedom of movement of threat actors.

- **Firewall rules and access control** Enforce strict policies to block unauthorised traffic attempting to bypass proxy and port rules. Use access control lists (ACLs) to restrict traffic to only trusted sources.

- **Detect unusual network traffic** Use intrusion detection and intrusion prevention systems (IDS/IPS) and network monitoring tools to identify unusual connections, multi-hop proxy chains or other unusual traffic.

- **Encryption and authentication** Implement strong encryption and authentication of network communications to prevent threat actors from intercepting data.

- **Content Delivery Network monitoring** Monitor traffic carried by CDNs to help detect abuse by threat actors.

- **Logfile analysis and monitoring** Analyse network and system logfiles to identify suspicious activities, such as attempts to use proxy tools.

- **Restrict external tools** Restrict the use of unauthorised software and tools within the organisation to prevent proxy tool use by threat actors.

3.8 Exfiltration over alternative protocol: unencrypted non-C2 protocol (T1048.003)

Threat actors may steal data by exfiltrating it over a different, non-encrypted protocol than that of the existing C2 channel. The stolen data may also be sent to an alternative network location that differs from the main C2 server.

It is possible for threat actors to obfuscate this data without the use of encryption within network protocols that are natively unencrypted (such as HTTP, FTP or DNS). This can be done using custom or publicly available encoding and compression algorithms (such as Base64) or embedding data within protocol headers and fields.

Mitigation and recommendations:

- **Network monitoring and analysis** Implement advanced network monitoring tools that are capable of detecting unusual network activity, including the use of unusual protocol-port pairings for data transfers. These tools can use machine learning algorithms to learn normal network activity and identify anomalous patterns.

- **Protocol restrictions** Restrict network access to non-essential protocols and ports. Permitting only protocols that are strictly necessary reduces the attack surface for threat actors looking to use alternate protocols.

- **Data loss prevention (DLP)** Implement DLP solutions to identify sensitive data and prevent unauthorised attempts to exfiltrate data. DLP systems can be configured to detect specific types of sensitive data such as credit card numbers or personally identifiable information and to raise the alarm when this data is carried over unusual channels.

- **Encryption** Ensure that all sensitive data in transit is appropriately encrypted. This makes it more difficult for threat actors to use exfiltrated data even if they succeed in transmitting it.