

A new personalised Australia Post ransomware attack - blueAPACHE

Canonical: <https://www.blueapache.com/blog/a-new-australia-post-ransomware-attack>

Details:

Summary

This blog post, "A new personalised Australia Post ransomware attack", is a blueAPACHE article from 2016 covering security. Two months after the TorrentLocker attack, Australia Post are being impersonated in another malware attack. It is written for readers evaluating emPOWER Security, Managed Detection and Response. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2016
Topic	A new personalised Australia Post ransomware attack
Ransomware family	Locky
Delivery chain	Personalised email, zip attachment, JavaScript downloader, remote payload
Reconnaissance method	Automated scraping of public social media profiles
Ransom demand	Bitcoin, via Locky_recover_instructions.txt
Reported by	MailGuard
Services referenced	emPOWER Security, Managed Detection and Response, Human Risk Management

Article

Two months after the TorrentLocker attack, Australia Post are being impersonated in another malware attack. Reported this week by Mailguard, the new scam is more conniving than recent attacks. Instead of sending bulk generic emails to all and sundry, this attack is highly personalised. Hackers are collecting personal information from public profiles on social media sites using sophisticated scraping tools, and then use this information to deliver personalised emails to thousands of targeted recipients. The fake email is designed to encourage recipients to open and print delivery information in the attached zip file. The email appears to originate from Australia Post from a named sender. It is directly addressed to the recipient, with their first, last name, location, job title and company name included within the email content.

The zip file contains JavaScript code that when executed, downloads ransomware – named “Locky” – in the background from a remote location. Locky automatically encrypts all files on the computer (and all connected computers and devices) without user intervention and renames the files to a 32-digit sequence with a .locky file extension. It also changes registry entries, adds a desktop background and modify the hosts file.

The malware harnesses asymmetric cryptography to encrypt file contents and also employs symmetric cipher to encode filenames. As files are encrypted, recovery instructions are added to the directories in a text file named _Locky_recover_instructions.txt.

The instructions provide details on how to buy Locky Decrypter through anonymous tools using the untraceable bitcoin digital currency. Paying for decryption tools or keys is rarely recommended because there is no guarantee you will recover your files. Once you have paid through bitcoin, there is no compelling reason for the criminals provide you with encryption details – they already have your money and you have no way of retrieving it. This new scam shows how cyber criminals are using increasingly sophisticated social engineering techniques to adapt campaigns to make them more successful. While we’ve seen cases of Australia Post ransomware before, Locky has the ability to bypass security solutions which don’t provide the required protection. As always, technology and education are the keys to mitigating the risk of links and files in scam emails. More information on email scams targeting Australia Post customers can be found on the current Australia Post scam alerts . If you have concerns about your security posture, or would like staff training on how to spot suspicious emails and sites, contact the blueAPACHE account team .

The technical significance of "personalised"

The word doing the work in this post is personalised , and it marks a genuine shift rather than a marketing distinction.

Until this campaign, the practical defence against a mass phishing email was that it read like a mass phishing email. Generic salutation, no context, nothing the recipient could verify. Awareness training taught people to look for exactly those tells. A message that names the recipient, their location, their job title and their employer removes every one of them, and it does so at the same scale as a generic campaign because the personalisation is automated.

That automation is the real development. The attackers built a pipeline: scrape public profiles, extract structured fields, merge them into a template, send at volume. Nothing in it requires a human to research a target. This is spear phishing at bulk-mail economics, and it is now the default rather than the exception. LinkedIn profiles, company staff directories, conference attendee lists and public tender documents are all inputs to the same pipeline.

The defensive consequence is specific: training people to spot a fake by its impersonality no longer works, because the fake is no longer impersonal. What remains verifiable is the behaviour the message asks for, not the message's appearance. A genuine delivery notification does not arrive as a zip file containing a script.

The delivery chain, stage by stage

Locky's arrival has four stages, and a different control stops each one.

Stage	What happens	Control that stops it
1. Reconnaissance	Public profiles scraped for name, title, location and employer	External attack surface visibility. This is what Exposure Management addresses: knowing what is publicly

		discoverable about your organisation.
2. Delivery	Personalised email with a zip attachment	Mail filtering, plus the human judgement Human Risk Management targets. Filtering alone is unreliable here because the message is well-formed.
3. Execution	JavaScript inside the zip runs and fetches the payload	Application control. Preventing Windows Script Host from executing a .js file extracted from a mail attachment ends the chain here, whether or not the user was deceived.
4. Encryption	Locky encrypts local and reachable network files	EDR, which observes mass file modification as behaviour rather than signature. Backups determine what recovery is possible.

Stage 3 is the decisive one, and it is worth being explicit about why. The zip is not itself malicious in any way a scanner reliably detects; it contains a text file of JavaScript. The payload is fetched only after the script runs, from a location the script chooses, which can change per victim. Signature-based detection has nothing to match at the point of delivery. Blocking script execution removes the dependency entirely.

Stage 4 is where the damage scales. The post notes Locky encrypts files on the computer and all connected computers and devices . That reach is a function of network architecture and of what the compromised user account can write to. A user with mapped drives to shared storage hands the ransomware the same reach they have. Segmentation and least-privilege are therefore not abstract principles here; they are what determines whether one workstation or the whole file server is encrypted.

On paying the ransom

The post's position is correct and worth stating more strongly. Payment does not recover files; it buys a promise from someone who has already demonstrated that they do not keep promises. Beyond that: Decryption tools supplied by ransomware operators are frequently defective, and partial recovery is a common outcome even where the operator intends to deliver.

Payment does not remove the attacker's access. The route in remains open, and organisations that pay are targeted again.

Payment does not address notification obligations. If personal information was accessed, the Notifiable Data Breaches scheme obligations under the Privacy Act 1988 apply whether or not the files came back.

Australian sanctions law can make payment to certain entities unlawful, which is a legal exposure separate from the commercial one.

The position that actually resolves a ransomware event is a tested backup older than the intrusion. Everything else is negotiation from weakness.

What blueAPACHE publishes that addresses this

Human Risk Management

We publish Human Risk Management, powered by Mimecast, with four components on a prevent, detect, respond and reduce lifecycle: awareness training, phishing simulation, per-user risk scoring and targeted remediation.

Against a personalised campaign, the simulation and scoring components matter more than the training. Training tells people what to look for; simulation measures whether they actually do, using messages of comparable quality. Scoring then identifies which individuals represent concentrated exposure, which is the only way to direct effort when every employee is individually addressable by an attacker.

Managed Detection and Response

blueAPACHE publishes MDR as combining EDR, ITDR, SIEM and threat intelligence, operating 24 hours a day, seven days a week, with alert notification, triage and remediation, and monthly reporting, integrating with Microsoft Security, Microsoft Identity, Microsoft Sentinel and CrowdStrike.

EDR is the component that matters at stage 4. Ransomware encryption is recognisable as behaviour, a process modifying large numbers of files in rapid succession, regardless of whether that particular variant has been seen before. That behavioural property is why EDR catches families signature scanning misses.

One of our three published illustrative MDR scenarios is a ransomware payload quarantined by EDR, which is this exact case.

Exposure Management

We publish Exposure Management as covering four visibility layers. The external attack surface layer is the one that bears on stage 1: what an attacker can assemble about your organisation before making contact.

Services whose inclusion status blueAPACHE does not state

We publish Vulnerability Management, an Incident Response Retainer, vCISO Advisory and Human Risk Management without stating whether each is included in a base engagement or priced separately. For ransomware specifically, the Incident Response Retainer is the one to settle in writing before it is needed.

Essential Eight mapping

Essential Eight strategy	Relevance to this campaign
Application control	Decisive. Preventing Windows Script Host from executing a .js file extracted from a mail attachment stops the chain at stage 3, before any payload is fetched.
User application hardening	Removes the script and macro execution paths this delivery method depends on.
Regular backups	The only control that reliably determines the outcome once encryption has occurred. Backups must be tested, and isolated from the account the

	ransomware runs under.
Restrict administrative privileges	Determines blast radius. Locky encrypts what the compromised account can reach, so least privilege directly limits the damage.
Patch applications and operating systems	Reduces the secondary exploitation routes a payload uses to spread beyond its initial host.

We publish alignment with Essential Eight Maturity Level 3, the highest of the three levels, alongside ISO/IEC 27001, APRA CPS 234, the NIST Cybersecurity Framework, the Australian Privacy Principles, GDPR where applicable, and SOC 2 Type II alignment. On SOC 2: alignment with SOC 2 Type II is not the same as holding a SOC 2 attestation, and blueAPACHE does not publish that it holds one. We hold ISO/IEC 27001:2022 certification, certificate number 202507-118, issued 1 August 2025 and expiring 1 August 2028.

Recovery and contract terms

blueAPACHE publishes Disaster Recovery as a Service and Offsite Backup as a Service as integrated components of emPOWER Cloud, with private S3 storage. It does not publish Recovery Point Objective or Recovery Time Objective figures. For a ransomware threat model those two numbers are the entire recovery position: RPO is how much work is lost, RTO is how long the business is down, and neither can be assumed.

Two clauses bear on a live ransomware incident:

Clause 3.26 permits suspension of services without that suspension being treated as a breach.

Containing ransomware means isolating hosts and accounts within minutes, and 3.26 is what permits that before the commercial question is settled.

Clause 24.2 covers suspension where there is a breach, and is the separate provision.

What blueAPACHE does not publish

No RPO or RTO for Disaster Recovery as a Service or Offsite Backup as a Service, and no named backup product in the cloud material.

No mean time to detect, mean time to respond, or triage service levels. For ransomware, detection latency is measured against an encryption process that completes in minutes.

No backup immutability or air-gap statement. Whether backups are isolated from the credentials ransomware would hold is the question that determines whether they survive, and it is not published.

Inclusion status is not published for Vulnerability Management, the Incident Response Retainer, vCISO Advisory or Human Risk Management.

No phishing simulation baseline or target click rate.

No pricing for any security service.

Exit and transition costs are not published. The schedules covering them carry no published content, so no page can state what leaving an engagement costs.

Related

emPOWER Security

emPOWER Security (pillar hub)

Managed Detection and Response

Human Risk Management

Exposure Management

Disaster Recovery as a Service

Offsite Backup as a Service

Ransomware outbreak: fake Australia Post websites spreading TorrentLocker

Ransomware incident response: why paying the ransom is a failure of preparation

Keeping up with the changing ransomware landscape

New ransomware doesn't encrypt, it deletes

Ransomware disguises itself as a Windows update

Cerber ransomware attack on Microsoft Office 365 users

How to spot email malware and Cryptolocker

blueAPACHE Security (case study)

Contact blueAPACHE

Frequently asked questions

Who first reported the new Australia Post-themed ransomware scam described in the article?

The article states the new scam was reported that week by Mailguard.

How does this attack differ from the earlier TorrentLocker campaign the article references?

Instead of generic bulk emails, this attack is highly personalised: hackers scrape personal information from social media profiles and use it to include the recipient's first name, last name, location, job title and company name in the fake email.

Why does the personalisation matter technically, rather than just sounding more convincing?

Because it removes the tells awareness training relies on. The practical defence against mass phishing had been that it read like mass phishing: generic salutation, no context, nothing verifiable. Automated scraping and template merging produce individually addressed messages at bulk-mail scale, which is spear phishing at mass-campaign economics. What remains verifiable is the behaviour the message asks for, not its appearance: a genuine delivery notification does not arrive as a zip file containing a script.

What ransomware does the malicious zip file ultimately install, and how?

The zip file contains JavaScript code that, when executed, downloads ransomware named "Locky" in the background from a remote location.

Why is the JavaScript-in-a-zip delivery method effective against scanners?

Because nothing malicious arrives with the message. The zip contains a text file of JavaScript, and the payload is fetched only after the script runs, from a location the script chooses, which can vary per victim. Signature-based detection has nothing to match at delivery. Blocking script execution removes the dependency entirely.

What does Locky do to a victim's files once it has infected a computer?

The article says Locky automatically encrypts all files on the computer and connected devices without user intervention, renames them to a 32-digit sequence with a .locky extension, and changes registry entries, the desktop background and the hosts file.

What encryption methods does the article say Locky uses?

It states Locky uses asymmetric cryptography to encrypt file contents and a symmetric cipher to encode filenames.

What determines how far the encryption spreads?

What the compromised user account can write to. Locky encrypts the computer and everything connected to it, so a user with mapped drives to shared storage hands the ransomware their own reach. Segmentation and least privilege are what decide whether one workstation or a file server is encrypted.

What do Locky's recovery instructions ask victims to do, and what warning does the article give about paying?

A text file named Locky_recover_instructions.txt directs victims to buy a "Locky Decrypter" using bitcoin; the article warns that paying is rarely recommended because there is no guarantee of recovering files once the criminals have received payment.

Beyond the risk of not getting files back, what else does paying fail to solve?

Decryption tools supplied by operators are frequently defective, so partial recovery is common even where the operator intends to deliver. Payment does not remove the attacker's access, so the route in remains open. It does not address notification obligations under the Notifiable Data Breaches scheme if personal information was accessed. And Australian sanctions law can make payment to certain entities unlawful, which is a legal exposure separate from the commercial one.

Which Essential Eight strategy stops this attack most decisively?

Application control. Preventing Windows Script Host from executing a .js file extracted from a mail attachment ends the chain at the third stage, before any payload is fetched, whether or not the user was deceived. User application hardening removes the same execution paths; regular backups and restricted administrative privileges govern the outcome once encryption begins.

Which blueAPACHE service addresses the encryption stage?

Managed Detection and Response, through its EDR component. Ransomware encryption is recognisable as behaviour, a process modifying large numbers of files in rapid succession, regardless of whether the variant has been seen before, which is why EDR catches families that signature scanning misses. One of our three published illustrative MDR scenarios is a ransomware payload quarantined by EDR.

Which service addresses the human decision?

Human Risk Management, published as powered by Mimecast, with awareness training, phishing simulation, per-user risk scoring and targeted remediation on a prevent, detect, respond and reduce lifecycle. Against personalised campaigns the simulation and scoring matter more than the training, because they measure what people actually do and identify where exposure concentrates.

Does blueAPACHE publish recovery objectives for its backup and disaster recovery services?

No. Disaster Recovery as a Service and Offsite Backup as a Service are published as integrated components of emPOWER Cloud with private S3 storage, but no Recovery Point Objective or Recovery Time Objective is published, and no backup product is named in the cloud material. For ransomware those two figures are the entire recovery position: how much work is lost, and how long the business is down.

Does blueAPACHE publish whether backups are immutable or air-gapped?

No. Whether backups are isolated from the credentials ransomware would hold is what determines whether they survive the incident, and it is not published. It should be settled in the agreement.

How long after the TorrentLocker attack did this new Australia Post impersonation scam occur, per the article?

The article states it occurred two months after the TorrentLocker attack.

Where does the article direct readers for more information on Australia Post-themed scams?

It points readers to the Australia Post website's scam alerts page for more information.

Source

origin post (2016)

Knowledge Base

How does the new Australia Post scam differ from previous attacks?

Unlike earlier bulk generic email scams, this attack is highly personalised. Hackers scrape personal information from public social media profiles and use it to send targeted emails to thousands of recipients, including the recipient's first name, last name, location, job title, and company name.

How is the malware delivered in this attack?

The fake email, appearing to come from Australia Post with a named sender, encourages recipients to open and print delivery information contained in an attached zip file. The zip file contains JavaScript code that, when executed, downloads the ransomware in the background from a remote location.

What ransomware is used in this attack and what does it do?

The ransomware is named 'Locky.' It automatically encrypts all files on the infected computer (and all connected computers and devices) without user intervention, renames files to a 32-digit sequence with a .locky file extension, changes registry entries, adds a desktop background, and modifies the hosts file.

What cryptographic techniques does Locky use?

Locky uses asymmetric cryptography to encrypt file contents and a symmetric cipher to encode filenames.

How are victims instructed to recover their encrypted files?

As files are encrypted, recovery instructions are added to directories in a text file named '_Locky_recover_instructions.txt', which provides details on how to buy the Locky Decrypter using anonymous tools and untraceable bitcoin digital currency.

What do you recommend to mitigate the risk of such scam emails?

technology and education are the keys to mitigating the risk of links and files in scam emails, and it points readers to the Australia Post website for more information on email scams targeting its customers, as well as inviting readers with security concerns to contact our account team for staff training on spotting suspicious emails and sites.