Monthly Cyber Threat Intelligence Report

September 2024

e2e assure

Contents

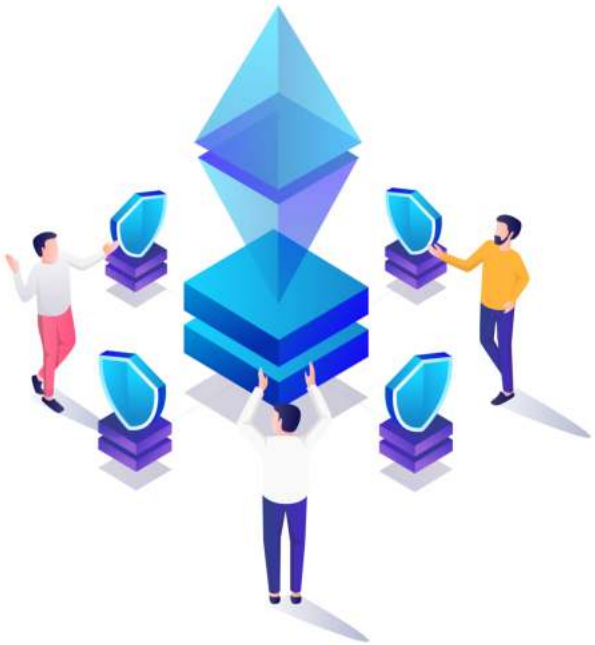
Welcome to our latest edition of the Monthly Cyber Threat Intelligence Report.

Autumn is a changing time of year, with striking colours appearing in nature and a return to normal after all the fun of the summer slowdown. For cyber security, however, there's no such luxury—with new breaches and vulnerabilities reported daily, there's plenty for us to keep up to date with and watch out for in the future.

We'll update you on existing breaches and investigate some notable stories. Then, in our regular monthly 'deep dive', we'll examine APT29, also known as 'Cozy Bear'.

Top Breach of the Month

A Wake-Up Call for Security Testing



In August 2024, Ronin Networks, an Ethereum blockchain virtual machine developed for gaming, experienced a breach orchestrated by white-hat hackers. The hackers breached Ronin's network to expose vulnerabilities that criminal actors could have otherwise exploited.

The attackers accessed Ronin Networks' internal systems, and vulnerabilities across the company's infrastructure were identified, including outdated software, weak access controls, and unpatched security flaws.

The attackers withdrew 4000 ETH and $2m USDC with a value of around $12m – the maximum withdrawal in a single transaction, highlighting the potential impact had this been a malicious attack.

Impact of the Breach on Ronin Networks

The breach forced Ronin to temporarily shut down several systems, review its security policies, and bolster its defences. In their post-breach report, the white-hat hackers revealed how easily attackers could have compromised sensitive data or disrupted operations without proper mitigations.

Regular penetration testing, vulnerability scanning, and red-teaming exercises are critical to identifying and remediating security gaps before malicious actors exploit them. White-hat hacking engagements are valuable because they simulate real-world attacks, revealing weaknesses that may not be apparent through automated tools alone.

In Ronin's case, the ethical hackers provided a detailed roadmap for improving network security, allowing the company to strengthen its defences and prevent future attacks. This attack was not malicious but carried out by a group who wanted to pre-warn, with their reward being a $500k bounty rather than illegal gains.

Recommendations

Only some companies will be lucky enough to benefit from a White-Hat attack; more are breached by groups looking to steal data, ransom information, or disrupt business. Adopting best practices in cyber security is essential to ensure cyber resilience:

Regular patch management and system updates are essential for reducing the attack surfaces available to attackers.

Routine network monitoring, anomaly detection, and intrusion prevention systems (IPS) can help identify suspicious behaviour before an attacker gains a foothold.

Implementing strict access control policies, such as multi-factor authentication (MFA) and the principle of least privilege (POLP), can limit exposure during a breach.

Invest in training staff to recognise and respond correctly to phishing and social engineering attacks.

Leveraging ethical hacking services and conducting periodic security audits can identify vulnerabilities before they become a liability.

The breach at Ronin Networks reminds us that cyber security is not a one-time investment but an ongoing process requiring constant vigilance and testing.

Updates: Snowflake Data Thefts

In June this year, the 'Snowflake' breaches emerged, with Mandiant attributing them to a threat actor known as UNC5537. Mandiant has notified 165 of their customers who may be exposed.

The cyber attacks have impacted high-profile businesses, including AT&T, Santander, Live Nation, Advance Auto Parts, and Pure Storage. UNC5537 exploited stolen credentials, targeting environments that lacked multi-factor authentication (MFA). Once inside, the group used credentials from previous data breaches and infostealer malware to gain unauthorised access to customer data hosted on Snowflake.

The breaches have resulted in extensive data theft, as with the stolen credentials, attackers could focus on retrieving customer information without triggering significant computational activity, thus evading early detection.

The operational and financial impacts on affected businesses have been severe. AT&T had nearly 110 million customers' call and text records stolen, while Pure Storage faced the exposure of sensitive telemetry data. Extortion attempts have followed, targeting companies like QuoteWizard (a LendingTree subsidiary) and Advance Auto Parts, where hackers have posted samples of stolen data on dark web forums to pressure victims into paying ransoms.

Lessons we can learn

Businesses must enforce rigorous MFA and credential management policies, ensuring regular credential rotation and monitoring for infostealer malware activity. Enhanced security practices like network segmentation and anomaly detection in data access patterns are essential to prevent unauthorised access.

The shared responsibility model of cloud platforms like Snowflake emphasises the need for proactive customer-side security. Cloud providers like Microsoft are rolling out MFA enforcement on their users as part of their security model. Snowflake does not enforce MFA and only states in current documentation that they 'strongly recommend' account admin role users have this enabled.

The lesson is that if you are a Snowflake customer, you must ensure MFA is correctly enabled and used. If your security is outsourced, speak to your provider about regular cyber security resilience reporting, as this will highlight weaknesses in posture and provide recommendations for adjustment.

Other Notable Incidents in Brief

OneBlood Nonprofit Hit by Ransomware

OneBlood, a nonprofit organisation supplying blood to over 350 hospitals across the southeastern United States, recently experienced a significant ransomware attack. On July 31st 2024, the attack was launched and disrupted OneBlood's systems, impacting its ability to deliver essential blood products across multiple states—the ransomware group behind the attack affected supply chain operations. Hospitals had to resort to emergency measures, such as rationing blood supplies and cancelling non-essential surgeries. The extent of the disruption led to the involvement of an AABB (American Association of Blood Banks) taskforce to coordinate support from other blood centres nationally.

Despite OneBlood's rapid deployment of incident response measures, including isolating affected systems and working closely with federal agencies, recovery has been slow, with operational impacts still affecting hospitals.
This incident follows similar attacks on blood suppliers Synnovis in the UK and Octapharma in the US, indicating a troubling trend targeting critical healthcare infrastructure.

Microsoft DDOS 'Amplified' by Rapid Response

Late in July, Microsoft experienced a significant Azure outage caused by a DDoS attack targeting Azure's network infrastructure and overwhelming it with a high traffic volume. Microsoft implemented updates to its DDoS protection system as part of the mitigation strategy. However, these updates introduced misconfigurations that inadvertently caused broader disruptions across multiple regions.

Core Azure services, including virtual machines, storage, and authentication services like Azure AD, were affected, causing a domino effect on global enterprises that rely on these services.

Microsoft's response further exacerbated the situation, with delays in diagnosing the root cause and inconsistent updates. This left affected customers in the dark and resulted in extended recovery times. The incident highlights the challenges of mitigating large-scale DDoS attacks and the risks associated with hasty mitigation measures.

Third-Party Breach Creates Phishing Risk for Users

On July 29th, Locata, a third-party software provider for housing applications, was hit by ransomware. The attack hit part of Greater Manchester and spread fast to take down housing websites in Salford and Bolton, causing significant disruption. Locata is the primary platform council authorities use to manage housing lists, allocate properties, and process applications. The cyber criminals behind the attack encrypted critical data, halting access to services and preventing councils from processing new applications or updating existing cases.

Affected users could face delays in receiving housing support and, if sensitive data has been compromised, be exposed to phishing scams or other fraudulent activities. The attack's geographical spread highlights the risks of relying on a single software vendor across various regions.

What can we learn from these cyber incidents?

In reviewing these breaches, attacks, and data theft incidents, there are recommendations we can look to for improving our security posture. As attack techniques evolve, so must our strategies to keep threat actors at bay.

Testing Changes During Incident Response

The Azure outage highlights the importance of testing when implementing mitigation updates, even under pressure. Validating before deployment across production environments could prevent introducing additional points of failure.

Enhanced Communication Protocols During Major Incidents

Clear, frequent, and accurate communication is essential during incidents. Organisations should structure incident response frameworks that provide clear timelines for recovery, allowing customers to make informed decisions.

Third-Party Risk Management

Prioritise vetting the cyber security practices of third-party vendors. Regular audits and penetration tests should be a condition for continued service agreements, especially for vendors managing sensitive public data.

Data Segmentation and Backup Strategies

Any organisation relying on centralised platforms should enforce robust data segmentation strategies. In a breach, this reduces the risk of widespread data loss. Offline and air-gapped backups should be maintained and tested regularly to ensure data recovery is possible.

Segment Critical Infrastructure

Enforce strict network segmentation for critical systems. Separating supply chain operations from less sensitive environments could limit the radius of ransomware attacks.

Enhance Cyber Hygiene Practices

Regular vulnerability assessments and robust patch management, particularly for systems handling operational technology (OT), are vital in preventing exploitation.

Evolving Stories to Watch

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

Museum Ransomware included the Olympic venue

On August 3rd, a ransomware attack targeted 40 museums in France, including the iconic Olympic venue Musée des Arts Forains in Paris. The attack disrupted operations by encrypting critical systems. This incident has drawn significant attention due to the Grand Palais Réunion des musées nationaux being a venue in the Paris 2024 Olympics. With museums housing sensitive visitor data and valuable artefacts, this attack shows the expansion of ransomware operations beyond traditional business targets.

Taiwanese Research Institute infiltrated by APT41

China's APT41 threat group in an attack around July 2023. The group was tracked by its use of specific malware, including ShadowPad and CobaltStrike, and open-source tools, several of which are written in Simplified Chinese. APT41 is known for sophisticated attacks that blend espionage with financially motivated activities. Their method of operation often includes infiltrating sensitive systems and maintaining long-term access for intelligence gathering.

Hackers breach MDM and remote-wipe devices

At the start of August 2024, Mobile Guardian, a UK-based mobile device management (MDM) platform used by schools, was the victim of a breach. The company detected unauthorised access to iOS and ChromeOS devices on August 4th, but by this time, it was too late, and they were using their access to remote wipe student devices. Around 13,000 students in Singapore were affected by this attack, although the global impact is unknown. The Ministry of Education in Singapore cancelled their contract following the breach, and on September 10th, it was reported that they had started legal action related to the incident.

New Malware with the capability to disable EDR

Researchers recently spotted a new malware named EDRKillShifter, which targets Endpoint Detection and Response (EDR) solutions. The tool is deployed as a 'loader, ' delivering a vulnerable driver that can be abused. This is known as 'bring your vulnerable driver' (BYOVD). Once delivered, the malware uses command-line tools to probe system processes and dynamically shut down EDR services or bypass them altogether. This method significantly complicates incident response efforts by disrupting real-time monitoring and delaying the detection of malicious activities.

Deepdive Into a Threat Actor:

APT29 (Cozy Bear)

APT29 primarily targets government agencies, think tanks and healthcare organisations. Its targets are often involved in areas of geopolitical interest, including national security, foreign policy, and vaccine development.

Here are some recommendations for detecting their activity:

Behavioural Analysis and Endpoint Detection

APT29 is known for using fileless malware and living-off-the-land techniques. Endpoint Detection and Response (EDR) tools that can detect unusual behaviour and memory-resident threat indicators, including:

Suspicious PowerShell commands
PowerShell scripts are used for lateral movement. Process Injection: Monitor for processes like 'svchost.exe' or 'explorer.exe' showing signs of DLL injection or unexpected network activity.

Scheduled Tasks and WMI Persistence
Windows Management Instrumentation (WMI) and scheduled tasks are abused for persistence.

Network Traffic Analysis

To detect encrypted and stealthy command-and-control (C2) communications which are relied upon for attacks:

Inspect DNS Traffic
Monitor for uncommon DNS requests, as they can indicate domain fronting and DNS tunnelling for C2 communications.

Detect Anomalous HTTPS Traffic
Use SSL inspection to identify unusual outbound encrypted traffic, particularly to unfamiliar or newly registered domains.

Behavioural Analytics
Deploy tools capable of detecting unusual user or system behaviour patterns, such as abnormal login attempts or data exfiltration during non-business hours.

Proactive Threat Hunting is essential in spotting stealth attacks

Focus on Privileged Accounts
Investigate unusual activity tied to privileged accounts, which are targets for lateral movement.

Monitor Cloud Services
Cloud environments (e.g. Microsoft 365) are commonly targeted. Ensure comprehensive logging and analysis for suspicious cloud admin activities or OAuth token abuse.

Memory Forensics
Use memory forensics to identify fileless malware or persistence mechanisms that evade traditional detection methods.

Log Analysis and SIEM Integration

Ensure comprehensive critical system (e.g., Active Directory, firewalls, proxy servers) and SIEM integration for correlation and alerting:

Brute-force Attempts
Look for patterns of failed login attempts followed by successful access. Unusual Service Creation: APT29 has been known to create services or modify registry keys to run custom services.

Patch Management and Security Configuration

Regularly patching critical software and hardening configurations can close off these vectors to avoid exploitation through known vulnerabilities.

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

Let’s connect!

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

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

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