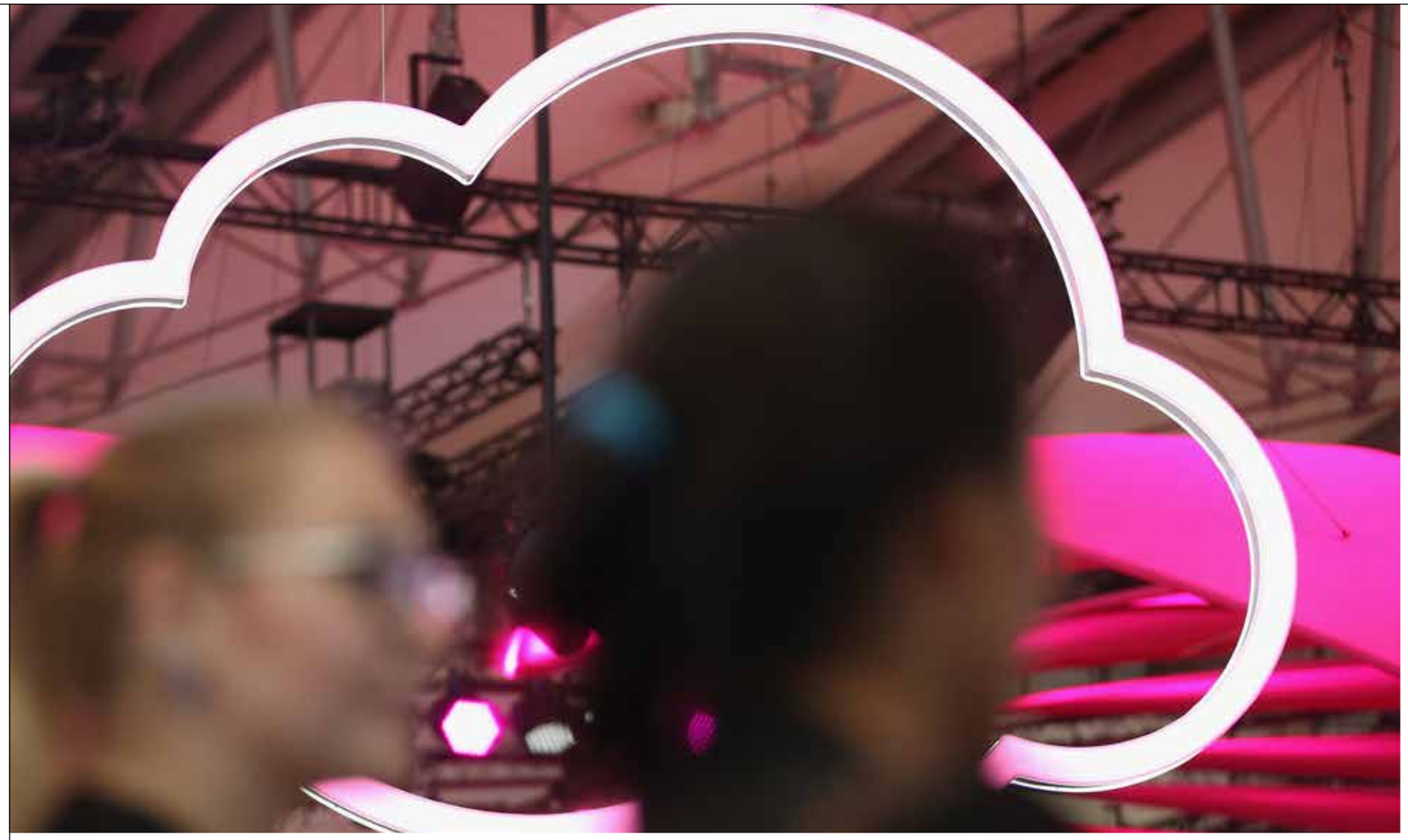

Picture credit: Getty

SKY HIGH

Chris Doman *examines how organisations can respond to evolving threats in the cloud*

The seismic shift towards cloud migrations has been impossible to ignore. While the pandemic necessitated the adoption of cloud models for many organisations to efficiently accommodate remote workforces, businesses swiftly recognised the benefits that a departure from on-premises setups could offer on a long-term basis.

While the operational advantages are evident, organisations must not overlook the potential security hurdles that can accompany cloud migrations, maintaining a balanced perspective that acknowledges both the vast opportunities and potential challenges.

One of the most obvious benefits of cloud models is that they ensure data accessibility for employees at any time and from any location. In addition to supporting the flexible working models that many organisations have come to rely on, cloud computing supports innovation by simplifying the process of testing new concepts and developing applications. It also provides enhanced flexibility – resources and storage can be swiftly scaled up to meet evolving demands, eliminating the need for substantial investments in on-prem infrastructure.

From speed gains and lower costs, to better scalability and collaboration enhancements, the cloud has become an indispensable tool. According to data cited by Wissen Technology, 61 percent of businesses migrated their workloads to the cloud as a result of the COVID-19 pandemic. And while cloud adoption reached near-ubiquity with 94 percent penetration in 2023, the total spend associated with cloud technologies continues to grow.

Looking ahead, Gartner estimates that worldwide end-user spending on public cloud services will grow 20.4 percent to $678.8-billion in 2024 – up from $563.6-billion in 2023 – as businesses continue to explore the opportunities associated with deepening their cloud-based operations. As their investment in and reliance on cloud services rise, it's crucial that organisations do not overlook the associated security implications.

As much as 61 percent of businesses migrated their workloads to the cloud as a result of the COVID-19 pandemic

In on-premise environments, safeguarding entry points was a relatively straightforward endeavour. Enterprises had direct physical control over both hardware and software, facilitating direct oversight of potential risks.

In the cloud, however, they are presented with an entirely different challenge. The proliferation of potential vulnerabilities – from cloud misconfigurations and insecure APIs, to zero-day threats and poor access management practices – creates a significantly more complex landscape.

It has been a challenge for many enterprises to secure the rapid migrations they have executed adequately and quickly enough, and attackers are taking full advantage of this. We're also seeing a rise in cloud threats due to the increasing amount of infrastructure being hosted in the environment.

To capitalise on the instabilities of those enterprises that haven't adequately adapted and improved their security practices in line with their cloud migrations, adversaries are developing an increasingly expansive arsenal of attack methods specifically designed to exploit cloud-centric vulnerabilities. In fact, research from Crowdstrike suggests that cloud-based attacks increased by 75 percent in 2023.

Cado Security's most recent Cloud Threat Findings Report delves deeper into this trend, uncovering three principal ways in which cyber criminals are actively targeting enterprises in the cloud.

First, many current malware campaigns are targeting web-facing cloud services such as Docker, Redis, Kubernetes and Jupyter as a means of gaining unauthorised access to their target environments.

Looking at the Qubitstrike campaign that was uncovered in October 2023 as an example, we saw how threat actors worked to exploit a Jupyter Notebook, spawn a Bash terminal using Jupyter's terminal feature and run additional payloads on the underlying host. Furthermore, not only are threat actors using credential exfiltration scripts to hunt for cloud service provider credentials, but they're also seeking to identify and exploit misconfigured service deployments.

Second, threat actors are looking beyond using cloud and Linux-centric campaigns for cryptojacking, diversifying their toolbox of techniques to exploit a wider range of cloud vulnerabilities.

The recent discovery of cloud-centric hack tools such as Legion, Fbot and AndroxGh0st all highlight this shift, the latter having been the subject of an advisory released by the Cybersecurity & Infrastructure Security Agency (CISA). Instead of being centred around cryptojacking, these hack tools seek to automate the hijacking of cloud SMTP services, leveraging their speed and scalability to carry out mass-spamming attacks.

Thirdly, threat actors are also exploiting novel programming languages, resulting in the continued proliferation of Rust malware. In the same way that Rust enables developers to compile services for several operating systems at once, ransomware developers are using cross-platform development support to target Linux systems.

Given that very few malware analysis tools can handle Rust binaries effectively, and very few malware specialists are familiar with the language, the volume of malicious payloads developed in Rust is likely to continue to grow moving forward.

The message comes through loud and clear: as threat actors intensify their cloud-focused assaults, organisations must act decisively to counter this trend through the rapid identification, investigation and containment of threats and attacks.

In this environment, prompt and effective incident response and forensic analysis are essential to the protection of digital assets. Cloud forensics is a field that applies the traditional scientific techniques of digital forensics to attacks in the cloud. This domain can be divided into two primary categories: the forensics of a cloud estate and the forensics of cloud-specific systems and controls.

USING CLOUD FORENSIC PLATFORMS ENABLES PROFESSIONALS TO CURB THE SPREAD OF MALWARE

Done manually, the process involves a heavy burden of data collection and normalisation, before malicious activity can be identified, and the root cause and scope of an incident determined.

It's important to access and investigate both logs and resources. The ability to unearth 'undocumented logs' is really important, for instance, as these often hold essential information and history about activities and incidents within the cloud infrastructure. They sometimes reside in unexpected locations.

Access to the required resources is one of the biggest obstacles here: analysts often have to wait for access to be granted while the attacker runs riot. What's more, data is often distributed across multiple cloud services, making it difficult to capture everything that's required.

Security professionals must also have a solid grasp of the most common anti-forensics techniques used by attackers. One such tactic is log tampering, where an attacker manipulates system logging tools to obscure their actions. Attackers can tamper with log files or forensic artefacts, which allows them to remove entries related to their activities or even insert new events to mislead investigators and waste their time. When done properly, log tampering can keep an intrusion undetected without arousing suspicion.

Lastly, data destruction is a very common technique. Attackers will often delete payloads from the disk following executions, so responders do not have direct access to the malware sample. They will also often shred log files such as bash history or audit logs, eliminating evidence of their actions and making it significantly harder for responders to figure out the attacker's activities on the system.

Inadequate or outdated incident response strategies will give attackers the upper hand and can lead to potential damage. Traditional forensics tools and approaches have made investigation and response strategies overly tedious and complex – especially in cloud environments. Organisations must embrace a modernised approach, taking advantage of cloud automation and data processing technologies and tools. This will lighten the load on analysts' shoulders by simplifying the cloud forensics process, accelerating mean time to response (MTTR) and reducing risk.

Adopting a specialised cloud forensics and incident response platform that provides the right capabilities and incident management tools can pay dividends.

It's crucial that the platform can handle deep datasets. There's a common misconception that cloud forensics revolves solely around log analysis. While logs offer valuable insights, investigations demand a deeper understanding from additional data sources such as disk, network and memory within the infrastructure. Full disk analysis, for example, can supplement log analysis by providing crucial context for identifying the root cause and scope of an incident. Therefore, a holistic approach that integrates diverse data sources is vital.

MANY OF THE CURRENT MALWARE CAMPAIGNS ARE TARGETING WEB-FACING CLOUD SERVICES

A platform must also protect the chain of custody, guaranteeing the integrity of data throughout the investigation of an incident. In complex, multi-cloud environments, preserving unaltered copies of forensic evidence securely is easier said than done. Organisations should look to ensure that any solution can autonomously manage and maintain the chain of custody, recording and safeguarding evidence without human intervention.

Automated data capture across key cloud resources – including virtual machines, containers and serverless functions – will also be highly useful in accelerating the speed at which security teams can respond to an incident. This is especially important in ephemeral environments in which resources are constantly spinning up and down, and where data can simply disappear if it's not captured quickly.

By enabling immediate access to forensic evidence in the cloud, and automating both data collection and system isolation if an event is detected, cloud forensic platforms will equip professionals to curb the spread of malware and limit potential damage while investigations take place. The ability to automatically surface key malicious activities in parallel with a complete timeline of events, meanwhile, will boost both the efficiency of an investigation and accuracy of incident response.

Implementation can also open up the opportunity for parallel data processing, allowing security teams to look at hundreds of systems simultaneously, reducing the time it takes to kick off a deeper dive investigation once something malicious has been identified.

A platform must also be easy to use, streamlining the process rather than adding to the increasing operational pressures security professionals already face.

Cross cloud support will ensure a platform works as intended – even if incidents span several cloud service providers at once. Further, usability features such as an incident dashboard, single timeline evidence view, saved search and faceted search can all be extremely useful, making the navigation of platforms easier. Not only will features such as these help analysts achieve greater efficiency, they will also support novel analysts in undertaking more complex investigations.

Advanced data forensics and incident response capabilities are more crucial than ever. With threat actors continually developing and enhancing a diverse array of cloud-specific threats, organisations must embrace the tools and solutions needed to modernise their security setups and counter evolving cloud threats.

By helping organisations to navigate the complexities of resource-level cloud forensics and expedite incident response, sophisticated solutions will enable enterprises to stay ahead of attackers and fundamentally reduce their exposure to evolving cloud risks ●

Chris Doman is CTO and co-founder, Cado Security and is well known for building the popular threat intelligence portal ThreatCrowd, which subsequently merged into the AlienVault Open Threat Exchange, later acquired by AT&T.

There is a rise in cloud threats due to the increasing amount of infrastructure being hosted in the environment

Picture credit: AdobeStock