THE HIDDEN REASON WHY COMPANIES ARE STRUGGLING TO SECURE CLOUD INFRASTRUCTURE

By Gus Evangelakos, Director Field Engineering, XM Cyber

Most of us have read about the recent Capital One breach, which exposed more than 100 million customer accounts. Yet far fewer people are familiar with the broader security conditions that led to that breach. That fact that the cloud is accessible through public APIs introduces a huge attack vector for exploitation.

THE URGENT CHALLENGE OF PUBLIC CLOUD INFRASTRUCTURE MANAGEMENT

Misunderstanding the public cloud comes with grave risks attached, often in the form of misconfiguration errors. Security professionals struggle to follow the best practices guide due to lack of resources or time, or because of the large and complex infrastructure to deal with.

Here's what we mean: When researching common cloud-based threats, we at XM Cyber discovered that most cloud security solutions are narrowly focused on hygiene, compliance, and prevention. These approaches suffer from a fundamental flaw: They are purely defensive, rather than predictive.

WHY PUBLIC APIs REPRESENT THE NEWEST SECURITY BATTLEGROUND

While APIs help power the modern Web, they have also created a tempting new avenue of attack for enterprising cyber-criminals. Those challenges and conventions that used to work on prem previously don’t apply to cloud infrastructure anymore.

Responsibility for managing these networks falls to DevOps and IT teams, who usually rely on command line tools and development kits. Yet even experienced and skilled people can be victimized by credential theft -- one of the reasons why it's such an effective technique and so popular with hackers. Once team members have their accounts compromised, it takes only a single API call to jeopardize critical kind of assets. This is a nightmare scenario, as it makes the most painful kind of breaches trivially easy.

Many cloud provider tools save credential information within files stored in the user directory in some prefixes. This, once again, makes a breach almost trivially easy to execute and puts an organization's most critical assets needlessly at risk.

Here's the bottom line: Traditional defensive tools are largely focused on protecting networks, applications and operating systems. Public APIs present a new attack surface -- one that is beyond the ability of traditional defense mechanisms to effectively protect.

DEVELOPING AN ALTERNATIVE APPROACH

In an upcoming talk for Black Hat Europe 2019 ("Inside Out: The Cloud Has Never Been So Close"), XM Cyber senior security researchers will outline a new approach to attacking cloud infrastructure. This technique illustrates the relationships between various identities, resources and policies, in the process identifying vulnerable choke points that require immediate remediation.

By creating this relationship graph, researchers Igal Gofman and Yaron Shani have allowed for deeper insight into permission relationships within cloud environments. By mapping these relationships, it can be clearly illustrated how attackers can exploit features to escalate privileges and access a company's most critical assets.

Most cloud providers publicly document security features in detail, something that can serve the interests of attackers and defenders. For a skilled person, it won't be hard to understand all the minor stuff and use it for privilege escalation.

We believe that continuous monitoring of all potential attack paths to critical assets is the best thing an organization can currently do to fend off attacks of this nature. Ultimately, however, stronger tools will be needed, and we hope today's organizations will build on our research to create their own tools for security and risk assessment.

WHY OFFENSE IS THE BEST DEFENSE

At XM Cyber, we believe that defenders must go on the offensive. Developing an offensive tool incorporating our research is far easier than constructing a defensive system around it. Yet currently there is no open source offensive tool that automates the entire stack of Gofman and Shani's research.

So what should organizations do to prepare for the likelihood of such attacks? A critical first step is to closely follow best practices from cloud providers. As organizations grow larger and more complex, it becomes increasingly difficult to maintain clear and comprehensive visibility into large cloud infrastructure permissions. Properly assessing risk factors likewise grows more challenging.

Vigilance, adherence to best practices and the right software tool -- that's the ideal combination for protection of your most critical resources within a public cloud infrastructure. With all three elements in place, organizations will be in the best possible position to safeguard their highest value assets.

ABOUT XM CYBER

XM Cyber was founded by security executives from the elite Israeli intelligence sector.

XM Cyber's core team is comprised of highly skilled and experienced veterans from the Israeli Intelligence with expertise in both offensive and defensive cyber security.

XM Cyber has developed more than 15 patented technologies based on a proprietary set of algorithms that enable the continuous and automatic simulation of a hacker's techniques and methods.

GUS EVANGELAKOS

is the Director of North American Field Engineering, at XM Cyber. He has extensive experience in cyber security, having managed implementations and customer success for manymajor global brands such as Varonis, Bromium and Comodo. Gus has spent a decade also working on the client side, supporting IT infrastructure and cybersecurity projects. He has a strong background in micro virtualization, machine learning, deep learning (AI), sandboxing, containment, HIPS, AV, behavioral analysis, IOCs, and threat intelligence.