

ARMOR™

VANTAGEPOINT

Feb. 2018

CLOUD SECURITY:



THE

HONEYPOT PROJECT

by Armor

INTRODUCTION

Protecting sensitive data no longer means simply safeguarding on-premises infrastructure. The cloud is gaining tremendous momentum as organizations are feeling the gravitational pull of faster-go-to-market, flexibility and pricing advantages versus legacy on-premise approaches to IT. As a result, today's organizations are increasingly concerned with how best to migrate their security and compliance controls into the cloud alongside their data and applications. In this new reality, defense-in-depth requires understanding not only how to correctly utilize the native security controls of cloud providers, but also how to layer security on top of those controls to address the risks of an expanded attack surface.

While this shared responsibility model allows customers to hand off a portion of accountability to cloud service providers, the price of failing to properly protect data is continually being demonstrated. Take for example news of an open AWS S3 bucket exposing sensitive information on 123 million U.S. households – all due to a configuration error. Every breach risks harming business reputations and leaving concerned customers in its wake.

It is in this climate that Armor teamed with Crusade Partners to launch a honeypot to provide a real-world demonstration of the types of attacks targeting public cloud environments for small and midsized businesses (SMBs). The research, which was conducted over the course of several weeks, sent a clear message – that while hyperscale cloud providers offer standard security protections for customers, third-party security technologies and expertise can make the difference between preventing an incident and paying to remediate one.



EXECUTIVE SUMMARY

More than 560 per week – that is the average number of scans and attempted attacks launched against just one of the honeypot servers. Hidden inside those numbers are hundreds of attempts to move deeper into the system. Just as the power of cloud computing has captured the interest of businesses, the prospect of vulnerable applications and data has captured the interest of attackers as well.

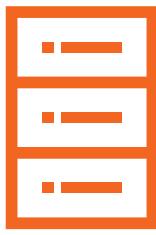
One misconfiguration can expose mountains of data. In this environment, having multiple layers of security is simply good business. As the saying goes however, the proof is in the pudding. The researchers created a scenario that happens all too often – one where a small business without significant time or expertise to spend on security looks to take advantage of the cloud's promises of cost savings and agility.

As part of the experiment, the researchers constructed a honeypot – decoy server instances designed to lure in attackers so that their activity can be observed and studied. The engineers built a web portal and site for an imaginary doctor's office, placed it in the cloud and waited. The wait didn't last long, as attackers began targeting the servers almost immediately after they were established. Roughly two weeks after all the servers were online, a message about the site appeared on Pastebin that read "new target...medical [expletive] to be hacked." Afterwards, the attacks picked up

As the data will show, those attacks largely took the form of SSH authentication brute-force attacks, followed by MySQL authentication attacks and then attacks targeting FTP. The key to protecting against these attacks is visibility – not just in terms of logs, but also identifying suspicious traffic and stopping it at the gate. That same commitment to visibility should extend to the overall health of the environment as well. On one of the honeypot servers, the Armor Anywhere security-as-a-service discovered 13 vulnerabilities, most of which were caused by the use of an unpatched version of Ubuntu and software running on the servers. Now as much as ever, visibility into your security posture that stretches from the cloud to your on-premises infrastructure is a necessary element of protecting your organization.

INSIDE THE HONEYPOD

The goal of the honeypot project is to mimic a public cloud environment that would be deployed by small and midsized businesses. To do so, researchers leveraged a widely-used hyperscale cloud provider, and set up three instances:



SERVER A

A server running no services, without a firewall configured



SERVER B

A server running a LAMP stack, FTP and Drupal with a basic firewall setup



SERVER C

A server running a LAMP stack, FTP and Drupal with  Armor | Anywhere

The servers were connected to a server running the Modern Honeypot Network software on Ubuntu 14.04 LTS. Each of the server instances were running on Ubuntu 14.04 LTS as well. Server A was run with no security controls to establish a baseline of attacks. Server B was protected by a firewall offered by the cloud provider with a basic setup and had no outbound rules. This is not that uncommon among SMBs, who often will set up a server in the cloud, add an application or two and leave everything else virtually unchanged.

The last server, Server C, was defended by Armor Anywhere, a security-as-a-service which includes intrusion detection, vulnerability scans, patch monitoring, file integrity monitoring, log and event monitoring and malware protection. Each

capability provides a critical, complimentary layer of security to the protections offered by cloud providers and is further backed by up-to-the minute threat intelligence and the expertise of Armor's researchers and Security Operations Centers.

For the experiment, the researchers built web portals and sites for a small doctor's office. The sites were running at MetropolisPrimary.com and MetropolisMed.com. This make-believe business migrated a variety of IP addresses, domains, and infrastructure to the cloud. The site and its associated patient portal were fully operational, and links to linkedin.com, twitter.com, and facebook.com were included to add to the realism.



“ The goal of the honeypot project is to mimic a public cloud environment that would be deployed by small and midsized businesses. ”

THE ATTACK LANDSCAPE

Unsurprisingly, the network was hit early and often. Attacks started within minutes of the honeypot sensors being activated. Ultimately, each instance was scanned thousands of times by likely attackers. Server A, the server with no protections enabled, was hit more than 19,000 times by the end of the project – approximately 2,500 per week. Server B, with just the native firewall running, was hit an average of roughly 563 times a week. Server C meanwhile was hit by attackers an average of about 509 times per week.

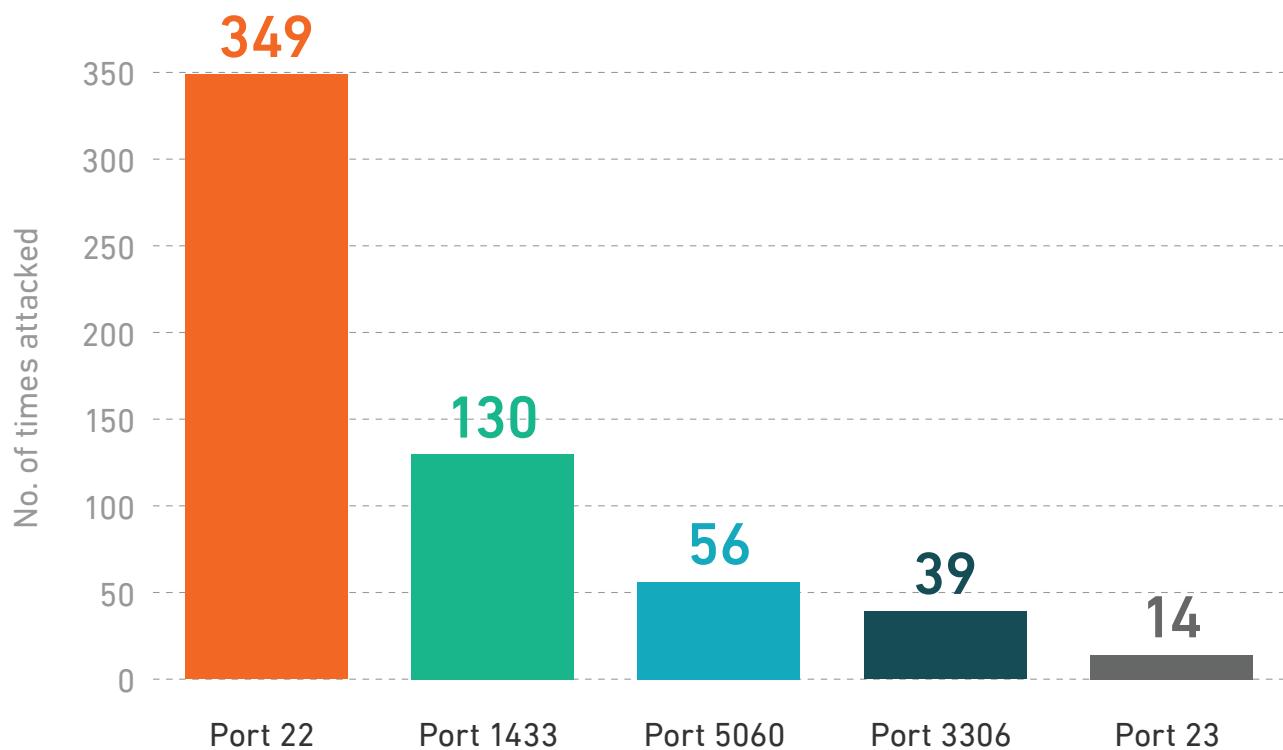
The vast majority of the threats were SSH brute force authentication attacks, which constituted 79 percent of the attacks on the server protected by Armor Anywhere and 71 percent on the instance using just native security controls. These attacks were likely automated, meaning the attackers were using an automated list of usernames and passwords to try and gain access to the servers via SSH. The next biggest group were MySQL authentication attacks.

Some of the attacks we saw were for:

- VoIP (Port 5060)
- Microsoft SQL Server and MySQL Databases (Ports 1433, 3306)
- FTP (Port 21)
- Telnet (Port 23)
- SSH (Port 22)

The attack data includes evidence of many scanners looking for open ports but not trying to break in. Unlike the SSH attacks, the attacks targeting FTP were not as persistent. Illustrated on page 6 is a snapshot of attacks against the three servers during a 24-hour period.

Top 5 Attacked Ports



Examining the country of origin yielded evidence that China and the United States were the most common sources of attacks, though it should be stated that while the MHN network was able to check whether the attack came from a TOR exit node, it was not able to determine whether the source IP of the traffic was a proxy. Still, the data suggests that roughly two-thirds of the suspicious/malicious traffic came from China (36 percent) or the U.S. (31 percent).

THE ATTACK LANDSCAPE (cont.)

Sixty-one distinct IPs came from the Netherlands, making it the largest suspected source of attacks in Europe. The other major countries of Europe were split evenly. Still, as a continent, Europe accounted for half as many attack IPs as the U.S. There was a sprinkle of IPs from South America, with most coming from Brazil. These Brazilian addresses were some of the first observed after turning on the honeypot.

As for the United States, its spot as the second most common source of attacks is likely due to the service being hosted in the U.S. Interestingly however, 14 of the 449 IP addresses from the U.S. were other servers from the same cloud provider we used in the experiment that were not associated with the honeypot servers or the account being used. While it is not clear that the traffic coming from those 14 IP addresses was malicious, it is believed to be suspicious.

From a defensive standpoint, the attack data shows the importance of paying close attention to SSH security. Hackers certainly are. Following best practices for hardening SSH servers and password management should be critical elements of your cloud security strategy, and businesses generally should ensure they are doing a good job keeping track of and managing their SSH keys.

While the firewall protecting Server B provided basic protection against the SSH attacks, the server protected by Armor Anywhere received the additional benefit of vulnerability management. In less than one work day of being online, the Armor Anywhere system alerted the researchers to the presence of a major vulnerability on the network and provided them with remediation actions. In addition, Armor Anywhere detailed the attacks being launched against the honeypot and provided the researchers with concise analytics to enhance reporting and remediation efforts.

TIPS FROM THE TRU TEAM

Armor's Threat Resistance Unit (TRU) research team is at the forefront of the company's efforts to collect and disseminate the threat intelligence that informs and strengthens Armor's ability to protect customer environments. Their experience helping secure more than 1,200 customer environments around the globe has given them insight into the common challenges organizations face when adopting the cloud.

HERE ARE A FEW TIPS AND BEST PRACTICES THEY HAVE LEARNED FROM THE FIELD:



Limit Access: This means using a firewall to only expose services that you need to the outside world



Restrict administrative control: For protocols such as RDP or SSH, consider adding Source IP based restrictions. For CMS products (such as WordPress or Joomla) consider using configuration options to limit administrative login page access to trusted IPs



Keep your software up to date: This single step will help prevent a majority of exploit-based attack vectors. This means patching your operating system, system utilities, and any code running on your server, such as application plugins and themes for CMS products.

Two common cloud configuration errors and what can be done about them:

- Using password-based authentication for administrative access: As the honeypot showed, brute force attacks are all too common. By limiting SSH access to key-based mechanisms this attack surface can largely be mitigated.
- Default or simple passwords for application components: Make sure that any systems or applications that require a password to authenticate are using good passwords for this authentication. Our recommendation for a password is one that is unique and long.
- Don't worry too much about the old rule about letters, numbers, and symbols



USERNAME

PASSWORD



This is a bad password



USERNAME

PASSWORD



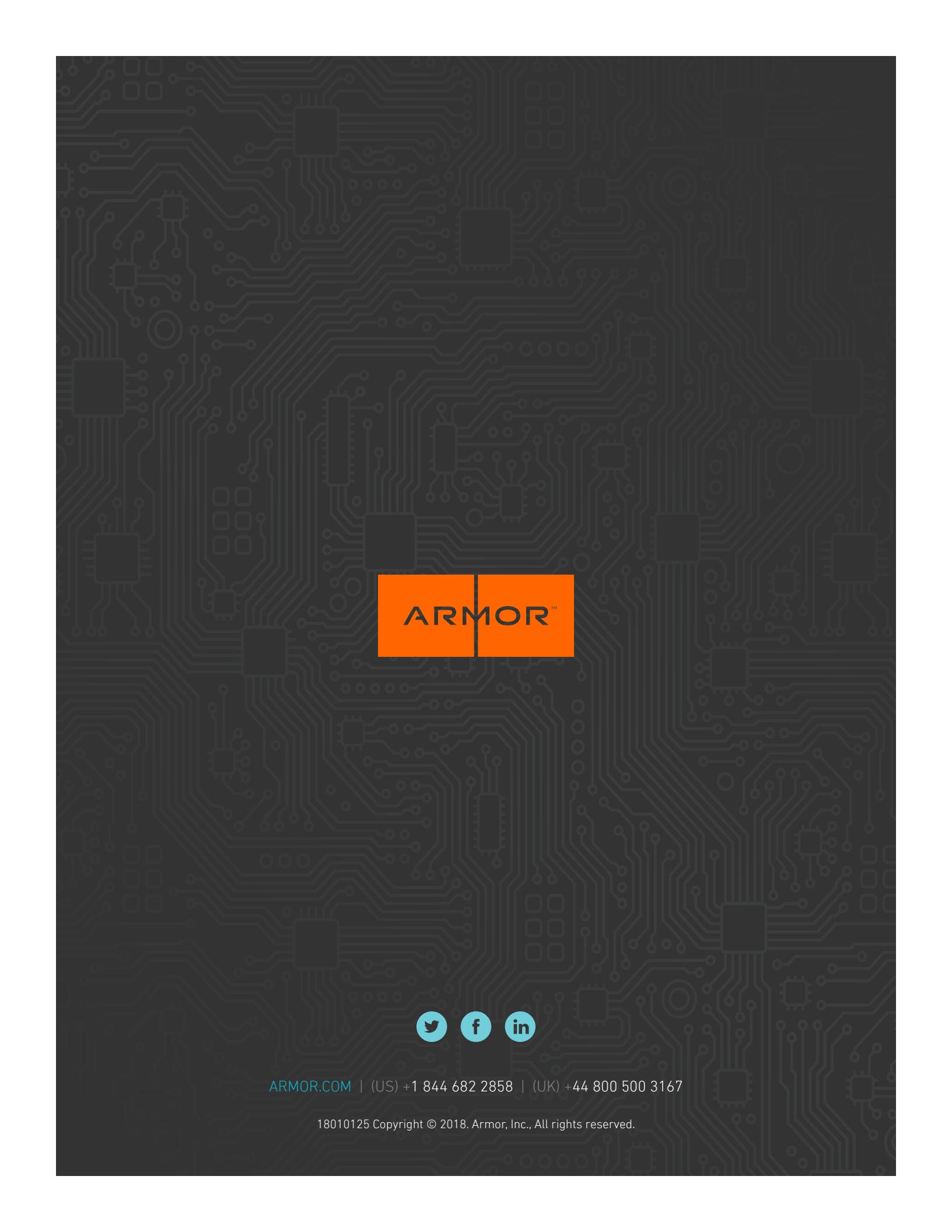
This is a much better password

BOLSTER YOUR DEFENSES

Protecting cloud infrastructure can be challenging, but it is far from an insurmountable challenge. It is vital to remember that the responsibility of security does not fall solely on the shoulders of cloud providers.

Whether your organization is big or small, there must be an assessment of what aspects of security are under your control, which aren't, and what is necessary for your organization to maintain the proper security and compliance levels. In a SaaS scenario for example, the cloud provider is responsible for most of the security controls, but the customer still must be prepared to configure certain controls and maintain the security and privacy of the data they are migrating.

Poorly configured native controls can be disastrous and have been at the heart of several cloud breaches during the past few years. Securing cloud instances has to be approached with the same level of careful planning as securing on-premises environments, making it vital that small and midsized businesses lacking sufficient internal resources or knowledge consider using complimentary technologies and third-party experts such as consultants and managed security providers as a force multiplier. Given the high price of even the smallest mistakes, bolstering a cloud provider's native controls with additional security is essential to bring defense in-depth concepts to the cloud.

A dark gray background featuring a dense, intricate pattern of white circuit boards and microchips, creating a high-tech, digital feel.

ARMOR™



ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167

18010125 Copyright © 2018. Armor, Inc. All rights reserved.