CERT-EU

Insecure S3 buckets can lead to serial exploitation

Threat Memo - Date: 06/08/2020 - Version: 1.0
TLP:WHITE

	Category	Type	Domain	Sector	Confidence
FOR INFORMATION	Vulnerability	Misconfiguration, Worm	World	Cloud storage services	A1

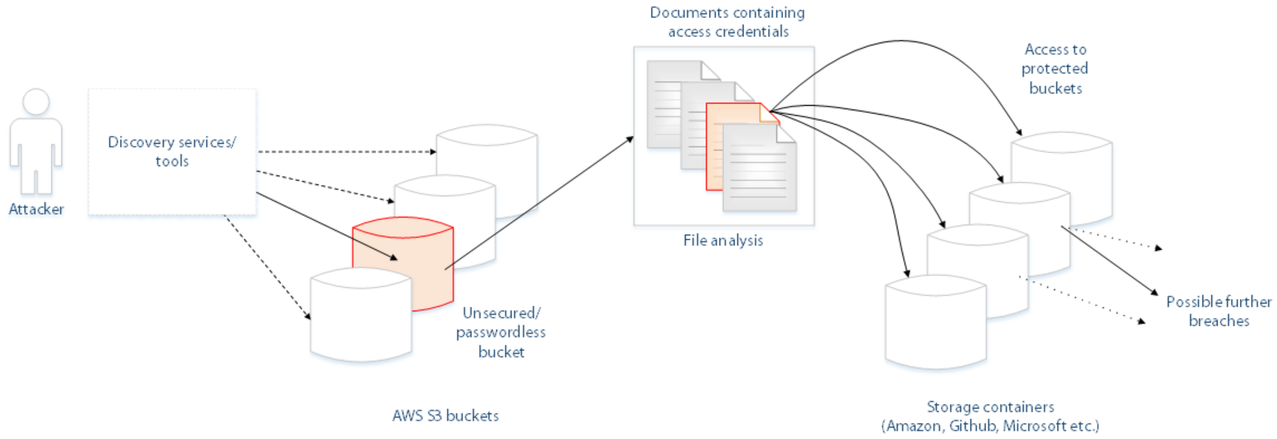
Key Points

- Research shows that unsecured cloud-based storage buckets can be scanned for the existence of credentials.
- The process of harvesting credentials and using them to exploit additional services has the potential to become automated.

Summary

A recent security analysis[1] of the threats posed by insecure cloud services storage buckets indicates the real possibility of automated, cascading breaches of such repositories in a worm-like manner.

In particular the researcher used the case of misconfigured Amazon Web Services (AWS) S3 buckets that had been left accessible over the internet. In numerous cases this accessibility was not a choice to provide publicly accessible content but rather the result of bad administration. Breaches resulting from accessibility misconfigurations have been quite frequent in the recent past. In these cases however, the accessible storage containers were further searched for the existence of access credentials to other services. Indeed in several cases, insecure S3 buckets contained passwords for other, better secured services. The researcher managed use these passwords to access additional storage containers that themselves also kept credentials for other services. The researcher points to the real possibility of such cascading accesses could be automated by a worm malware.


Documents containing access credentials
Access to protected buckets
Discovery services/ tools
Attacker
File analysis
Unsecured/ passwordless bucket
Possible further breaches
AWS S3 buckets
Storage containers (Amazon, Github, Microsoft etc.)

Overview of the cascading breach process

The process followed highlights many of the cloud services features that could be used in the realisation such an attack:

- *Discovery of open S3 buckets*. As these have unique names it is possible to use either DNS taps, lists maintained by security vendors, or tools that generate random names and check if they exist and are exposed.
- *Search specific content*. Additional tools allow to search inside the open buckets for content of interest.
- *Map credential files*. Found credential files can be analysed and associated with the systems they provide access to.
- *Extend to other cloud storage*. Even though the research started with AWS S3 buckets, very soon the results pointed to additional cloud storage services that would very quickly escalate the results of a possible automated (worm) attack.

It should be noted that access to open databases provides the potential of several types of attack including data leakage, ransomware, and destruction of data.

Comments

[1] https://trufflesecurity.com/blog/an-s3-bucket-worm-in-the-making-thousands-of-secrets-found-in-open-s3-buckets

The presence of misconfigured and unsecured databases or storage containers, exposed to the internet is a recognised problem and has resulted in serious breaches. The attack described by the researcher is a logical next step, technically feasible, and could be implemented with threat actors having limited technical capabilities.

When cloud services (storage or others) are used in an organisation it is imperative to:

- Ensure their correct and secure configuration.
- Strongly control information stored in them to avoid potentially harmful leaks.
- Check their visibility by third parties and what pieces of information they disclose about the organisation and their contents.
- If possible perform scans and exploitation tests in the same manner an attacker would.

Additionally, organisations should have a strict policy on which services (including databases) could be internet-exposed and limit these to the maximum extend.