CERT-EU

A cryptomining worm that steals AWS credentials

Threat Memo - Date: 19/08/2020 - Version: 1.0
TLP:WHITE

FOR INFORMATION	Category	Type	Domain(s)	Sector(s)	Confidence
	Cybercrime	Cryptomining Credential theft	World	Cloud computing	A1

Key Points

- A new piece of malware is targeting Amazon Web Services and steals credentials from them.
- Furthermore it uses these credentials to breach and exploit other cloud-based services for cryptomining.
- There is a proliferation of automated cloud attacks, largely based on insufficient security measures on these services.

Summary

Cloud security researchers disclosed[1] on 17 of August information of a new worm-malware[2] that targets cloud services with the aim to steal credentials and install cryptomining processes. The worm, that is called TeamTNT (as also the threat actor behind it), has been observed so far to target Amazon Web Services (AWS) as well Docker and Kubernetes systems. Docker and Kubernetes are both cloud-based platforms that allow the piecemeal installation of software products in predefined, independent environments.

The malware has the capability to acquire AWS system passwords and use them to pivot to additional systems, functionality that defines it as worm. Although the researchers do not give details on the initial phase of infection, this is supposedly either due to insufficiently secured AWS installations or as a result of credential stuffing attacks[3]. An attestation to this tactic is the capability included in the malware to scan for unsecured Docker instances. The demonstrated code for most of the worm activities is quite simple nevertheless sufficient to take advantage of systematic weaknesses (e.g. AWS stores credentials unencrypted and accessible by the command line interface).

The credentials are then sent to the attackers using basing HTTP protocol and further reused in the next infection activities. It is not clear at this moment if the credentials are automatically reused in other breach attempts (leading to fully automated operations) or they are managed by the human operators of the malware who choose the next victim.

On the breached systems, the malware uses the access it has acquired to install the XMRig crypto-miner for the mining of the Monero cryptocurrency. According to the researchers, observations in crypto-mining pools (collections of mining resources that provide reports on their members) show there have been at least 119 systems affected, including some Jenkins servers. The latter is a service that streamlines and automates software development processes. The small scale of infections does not preclude the scaling up of the operation via the use of TeamTNT.

Comments

Earlier in the August 2020, it was discovered that unsecured AWS S3 buckets could lead to serial breaches. The case of TeamTNT is the second time in a short period that cloud services are found to be vulnerable to cascading exploitation. This underlines the potential interest of threat actors to get access to computing resources pools to use for various purposes (e.g. for cryptomining as in the case of TeamTNT) as well as to information stores in cloud facilities. It should also be noted that access to open databases provides the potential of several types of attack including data leakage, ransomware, and destruction of data.

The case of TeamTNT also points to the need for strong security policies and the implementation of protection measures when an organisation moves to cloud services.

[1] https://www.cadosecurity.com/2020/08/17/teamtnt-the-first-crypto-mining-worm-to-steal-aws-credentials/

[2] Worms, as opposed to viruses, self-propagate through networks and can thus spread much quicker.

[3] In this type of attack the threat actors are checking username/password combinations known to belong to organisation personnel, which had previously been acquired by other means (e.g. breaches of third parties and the personnel is reusing passwords etc.)