Nov 03 2023

NETMANAGEIT

Intelligence Report

CloudKeys in the Air: Tracking Malicious Operations of Exposed IAM Keys

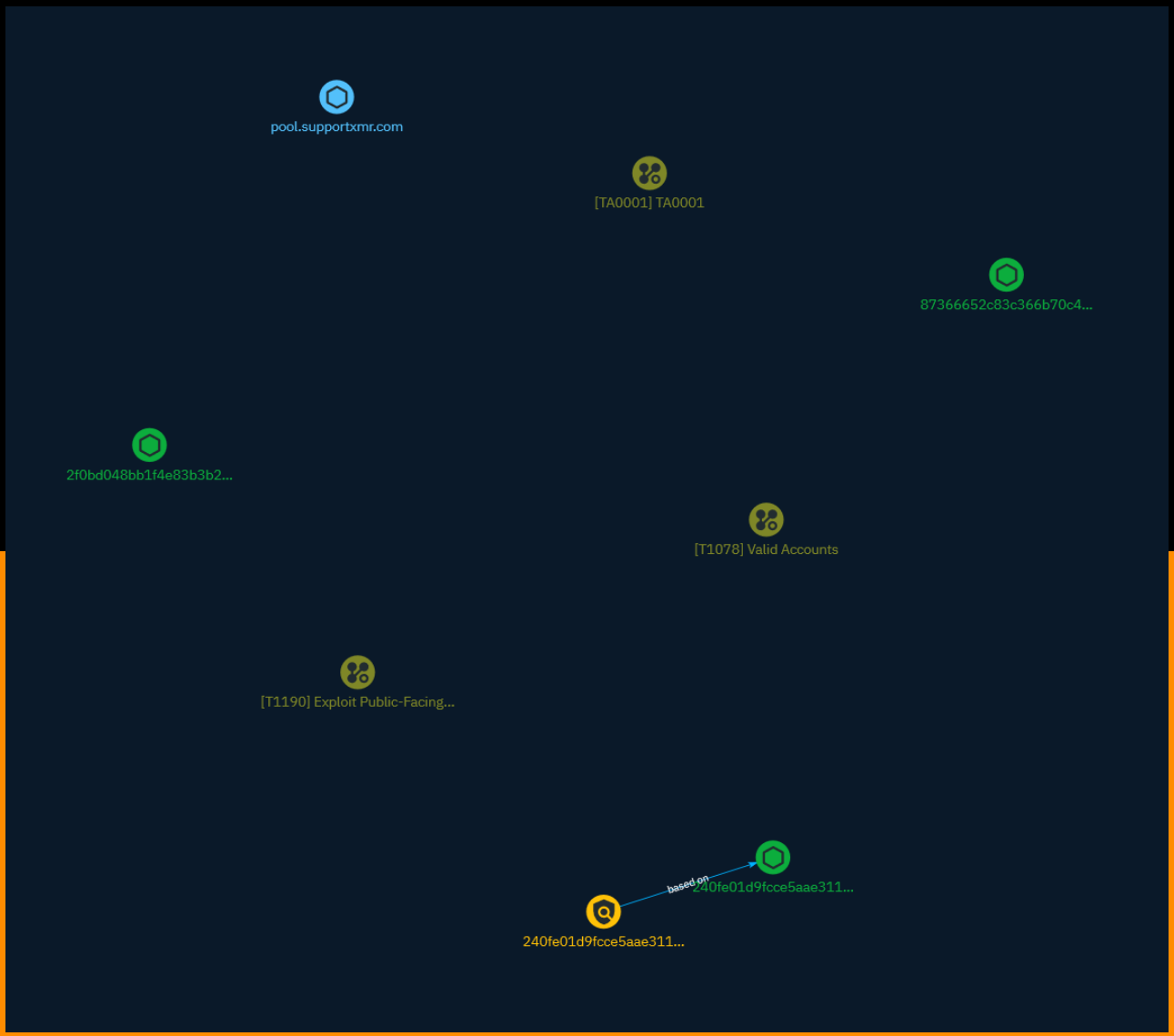

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Unit 42 researchers have identified an active campaign they are calling EleKtra-Leak, which performs automated targeting of exposed identity and access management (IAM) credentials within public GitHub repositories. As a result of this, the threat actor associated with the campaign was able to create multiple AWS Elastic Compute (EC2) instances that they used for wide-ranging and long-lasting cryptojacking operations. We believe these operations have been active for at least two years and are still active today.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Attack-Pattern

Name
Valid Accounts
ID
T1078
Description
Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop.(Citation: volexity_0day_sophos_FW) Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence. In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account.(Citation: CISA MFA PrintNightmare) The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.(Citation: TechNet Credential Theft)
Name

Exploit Public-Facing Application

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

Name

TA0001

ID

TA0001

Indicator

Name
240fe01d9fcce5aae311e906b8311a1975f8c1431b83618f3d11aeaff10aede3
Description
Multios.Coinminer.Miner-6781728-2 SHA256 of 555332faa336ed0e06e9b04d998cd53c5e192f1f
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '240fe01d9fcce5aae311e906b8311a1975f8c1431b83618f3d11aeaff10aede3']

StixFile

Value
240fe01d9fcce5aae311e906b8311a1975f8c1431b83618f3d11aeaff10aede3
2f0bd048bb1f4e83b3b214b24cc2b5f2fd04ae51a15aa3e301c8b9e5e187f2bb
87366652c83c366b70c4485e60594e7f40fd26bcc221a2db7a06debbebd25845

Hostname

Value
pool.supportxmr.com

External References

- https://unit42.paloaltonetworks.com/malicious-operations-of-exposed-iam-keys-cryptojacking/
- https://otx.alienvault.com/pulse/6544c1c4cbb991c0a6114742