Jul 13 2023

NETMANAGEIT

Intelligence Report

Agile Approach to Mass Cloud Credential Harvesting and Crypto Mining Sprints Ahead

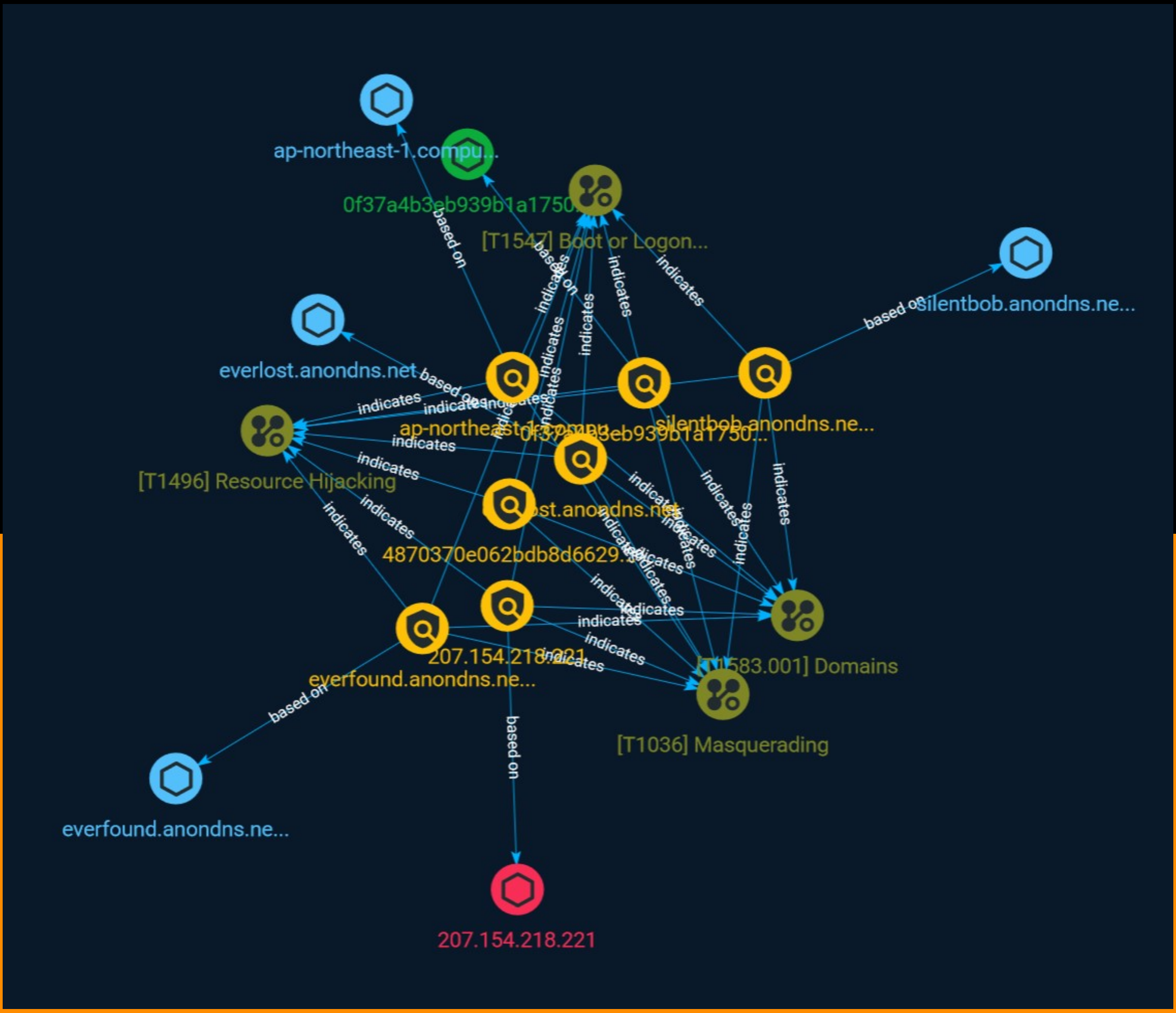

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A security team from Permiso Security and Aqua Security are sharing their insights into a multi-cloud credential harvesting and crypto mining campaign, as well as their own in-development toolset, which is currently in development.

Confidence

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

15 / 100

Indicator

Name

0f37a4b3eb939b1a1750a7a132d4798aa609f0cd862e47f641dd83c0763d8c8f

Description

SUSP_ELF_LNX_UPX_Compressed_File SHA256 of 87c8423e0815d6467656093bff9aa193

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0f37a4b3eb939b1a1750a7a132d4798aa609f0cd862e47f641dd83c0763d8c8f']

Name

everfound.anondns.net

Pattern Type

stix

Pattern

[hostname:value = 'everfound.anondns.net']

Name

ap-northeast-1.compute.internal.anondns.net

Pattern Type

stix

Pattern

[hostname:value = 'ap-northeast-1.compute.internal.anondns.net']

Name

everlost.anondns.net

Pattern Type

stix

Pattern

[hostname:value = 'everlost.anondns.net']

Name

4870370e062bdb8d6629a3e4b355b7658ae39200

Description

Detecting presence of known credential harvester scripts (commonly used by TeamTNT) containing specific section banner output commands

Pattern Type

yara

Pattern

rule P0_Hunting_Common_TeamTNT_CredHarvesterOutputBanner_1 { meta: description = "Detecting presence of known credential harvester scripts (commonly used by TeamTNT) containing specific section banner output commands" author = "daniel.bohannon@permiso.io (@danielhbohannon)" date = "2023-07-12" reference = "https://permiso.io/blog/s/agile-approach-to-mass-cloud-cred-harvesting-and-cryptomining/" md5_01 = "b9113ccc0856e5d44bab8d3374362a06" md5_02 = "d9ecceda32f6fa8a7720e1bf9425374f" md5_03 = "0855b8697c6ebc88591d15b954bcd15a" md5_04 = "f7df739f865448ac82da01b3b1a97041" md5_05 = "1a37f2ef14db460e5723f3c0b7a14d23" md5_06 = "99f0102d673423c920af1abc22f66d4e" md5_07 = "99f0102d673423c920af1abc22f66d4e" md5_08 = "5daace86b5e947e8b87d8a00a11bc3c5" strings: $sectionBanner_01 = "-------- AWS INFO --" $sectionBanner_02 = "-------- EC2 USERDATA ---" $sectionBanner_03 = "-------- GOOGLE DATA --------------------------------------" $sectionBanner_04 = "-------- AZURE DATA --------------------------------------" $sectionBanner_05 = "-------- IAM USERDATA ---" $sectionBanner_06 = "-------- AWS ENV DATA --------------------------------------" $sectionBanner_07 = "-------- PROC VARS -----------------------------------" $sectionBanner_08 = "-------- DOCKER CREDS -----------------------------------" $sectionBanner_09 = "-------- CREDS FILES -----------------------------------" condition: (5 of them) }

Name

silentbob.anondns.net

Pattern Type

stix

Pattern

[hostname:value = 'silentbob.anondns.net']

Name

207.154.218.221

Description

ISP: DigitalOcean, LLC **OS:** Linux 5.15.0-75-generic -------------------------- Hostnames: -------------------------- Domains: -------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBB8chIaQ30hHOwtvjddO300q KVe4E1cf6XKVHQp5Unkhl7sPr39OtGv29qCfRxbSFKXdALOssnUrnI9WvI0v7KE= Fingerprint: 20:39:85:08:82:63:f5:9e:4c:83:53:88:d6:9f:80:18 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ------------------ **80:** ``` HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Wed, 21 Jun 2023 05:17:21 GMT Content-Type: text/html Content-Length: 564 Connection: keep-alive ``` ------------------ **2375:** ``` HTTP/1.1 404 Not Found Content-Type: application/json Date: Thu, 13 Jul 2023 16:13:32 GMT Content-Length: 29 Docker: Version: 24.0.2 API Version: 1.43 Go Version: go1.20.4 OS: Linux 5.15.0-75-generic ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '207.154.218.221']

Attack-Pattern

Name
Domains

ID
T1583.001

Description
Adversaries may acquire domains that can be used during targeting. Domain names are the human readable names used to represent one or more IP addresses. They can be purchased or, in some cases, acquired for free. Adversaries may use acquired domains for a variety of purposes, including for [Phishing](https://attack.mitre.org/techniques/T1566), [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), and Command and Control.(Citation: CISA MSS Sep 2020) Adversaries may choose domains that are similar to legitimate domains, including through use of homoglyphs or use of a different top-level domain (TLD).(Citation: FireEye APT28)(Citation: PaypalScam) Typosquatting may be used to aid in delivery of payloads via [Drive-by Compromise](https://attack.mitre.org/techniques/T1189). Adversaries may also use internationalized domain names (IDNs) and different character sets (e.g. Cyrillic, Greek, etc.) to execute "IDN homograph attacks," creating visually similar lookalike domains used to deliver malware to victim machines.(Citation: CISA IDN ST05-016)(Citation: tt_httrack_fake_domains)(Citation: tt_obliqueRAT)(Citation: httrack_unhcr)(Citation: lazgroup_idn_phishing) Adversaries may also acquire and repurpose expired domains, which may be potentially already allowlisted/trusted by defenders based on an existing reputation/history.(Citation: Categorisation_not_boundary)(Citation: Domain_Steal_CC)(Citation: Redirectors_Domain_Fronting)(Citation: bypass_webproxy_filtering) Domain registrars each maintain a publicly viewable database that displays contact information for every registered domain. Private WHOIS services display alternative information, such as their own company data, rather than the owner of the domain. Adversaries may use such private WHOIS services to obscure information

about who owns a purchased domain. Adversaries may further interrupt efforts to track their infrastructure by using varied registration information and purchasing domains with different domain registrars.(Citation: Mandiant APT1)

Name

Resource Hijacking

ID

T1496

Description

Adversaries may leverage the resources of co-opted systems in order to solve resource intensive problems, which may impact system and/or hosted service availability. One common purpose for Resource Hijacking is to validate transactions of cryptocurrency networks and earn virtual currency. Adversaries may consume enough system resources to negatively impact and/or cause affected machines to become unresponsive.(Citation: Kaspersky Lazarus Under The Hood Blog 2017) Servers and cloud-based systems are common targets because of the high potential for available resources, but user endpoint systems may also be compromised and used for Resource Hijacking and cryptocurrency mining.(Citation: CloudSploit - Unused AWS Regions) Containerized environments may also be targeted due to the ease of deployment via exposed APIs and the potential for scaling mining activities by deploying or compromising multiple containers within an environment or cluster.(Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro Exposed Docker APIs) Additionally, some cryptocurrency mining malware identify then kill off processes for competing malware to ensure it’s not competing for resources.(Citation: Trend Micro War of Crypto Miners) Adversaries may also use malware that leverages a system's network bandwidth as part of a botnet in order to facilitate [Network Denial of Service](https://attack.mitre.org/techniques/T1498) campaigns and/or to seed malicious torrents.(Citation: GoBotKR)

Name

Boot or Logon Autostart Execution

ID

T1547

Description

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

Name

Masquerading

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)

StixFile

Value
0f37a4b3eb939b1a1750a7a132d4798aa609f0cd862e47f641dd83c0763d8c8f

Hostname

Value
everlost.anondns.net
silentbob.anondns.net
everfound.anondns.net
ap-northeast-1.compute.internal.anondns.net

IPv4-Addr

Value
207.154.218.221

External References

- https://otx.alienvault.com/pulse/64b0248bb9dc57e662e04ef0
- https://permiso.io/blog/s/agile-approach-to-mass-cloud-cred-harvesting-and-cryptomining/