Aug 28 2023

NETMANAGEIT

Intelligence Report

Smoke Loader Drops Whiffy Recon Wi-Fi Scanning and Geolocation Malware

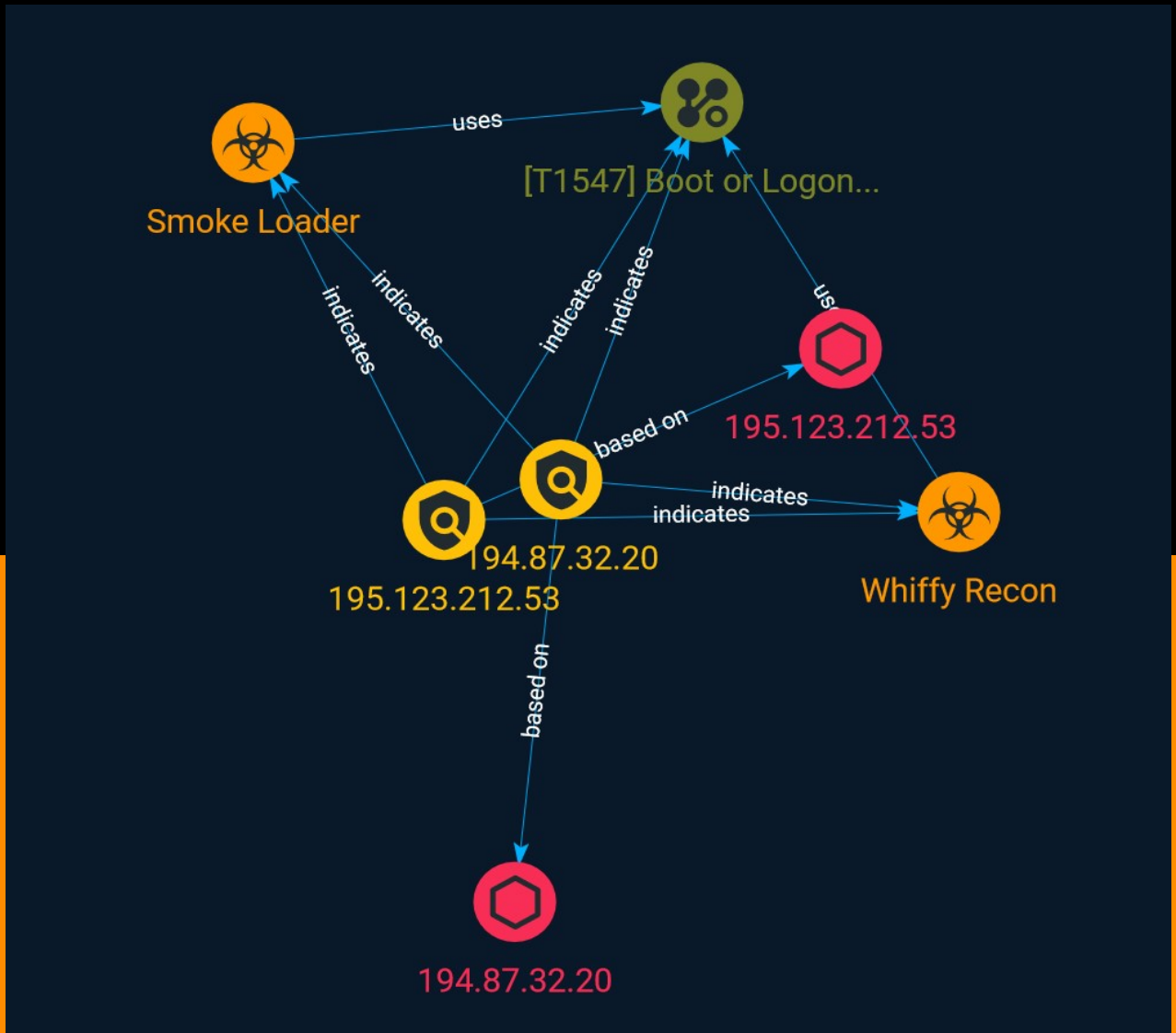

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Security researchers have observed malware that uses Google's geolocation API to track compromised systems and track their locations.

Confidence

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

15 / 100

Indicator

Name

194.87.32.20

Description

ISP: GorillaServers, Inc. **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDZaHAxaaxDxbvWbV62NqMJcrZUIsGP6Yxcb5vEXgfOaGeJ t0mxttFA0YbgG3D7HK+TwrFREuCP4Q7RoJKLZ1HTIu1vwf8RpG11INilZijLdoMGCbr4GnP+uJMB9f7Rsdn8NCh+3NKtR4005AJpSwThwScLUTAR91bt9RuzPjsFlm1YcJyrUxd24ZprYK+2jD2gs9d4sGBTZjaFUeeXPYS7r75D/d9iUnmzAMYxjU1enAV5qGzf7vvKHxBwqunr1iMVVg3+OVkT+hOmac/Dd3RFFLnqRHRk7PWhHxTXbD1/ogHx1WCOx/cpcOs5tGYaTcPR7d33kxj4D6euNiH3fyrUclawba0lnSbggmgkIFRlci98XnlEucVJmiYWSEYhhueyE7PrI5KEuk+LU/qUfSyhcqqNm48vgBS2gfVqd5Ys336km07VyirrczRn2vtG88HWyDKiugOcG7UWDoDkbJVpLiYnohEEhG6LtteO2lK8JUxzk0jcGuTEmbpNvzlHUrE= Fingerprint: af:0c:3f:86:41:be:65:44:c9:ba:f6:eb:f5:9f:58:d6 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 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 ssh-rsa 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.87.32.20']

Name

195.123.212.53

Description

ISP: ITL LLC **OS:** Ubuntu ---------- Hostnames: - vds1166461.hosted-by-itldc.com ---------- Domains: - hosted-by-itldc.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCoxblibFMTfe96KyxfLmfOvvB3g52Uu0Ou+BRxg02cF5wCZtjeOV3GSIViO08osvJPqfb0BXs54KrdpWDDM9Hl5q3jwTLHMdDFMSmNkt1gBmEKS+VK+I+cab9c4McdRWk4vyX98tNd4ccxu00gmxfu8hAg4Bb508PojPVwQdablnzPdBXY0RiHwNMUdLcV/Q0MMNhk Vmk+5Dr0rv+1ZXNBbYi/dpL25v+STAqDiX+oQ0lbcCqLfUyOsGatwvAKP7KJo/VB2qD+RxvgapuZ eJe0XFmx2rqii92Qn97LAFkUSj6OhFmOgP3cx9WhmH83CnfS/oJOr6jS/d5uXB0hnDg2rH5ueewY d2T7tc7Ce4tgfN0wlT+3XfbUdeSeuVf0PwjKHM0F60sE61QSO82DP5IKFEb9JzULI34DP7H4mWjOzA5hqyd/XAZkHJ3XHgPJPrlH+p1QTfGBdHT/X54PSNqCEGmb7fub04nMMK95b3b00UPzplY+SDmN exv2DOdJm2s= Fingerprint: cb:ec:d3:8d:2a:12:85:b0:55:1f:5e:5a:71:85:1a:23 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 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 ssh-rsa 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/1.1 200 OK Date: Fri, 25 Aug 2023 16:56:32 GMT Server: Apache/2.4.41 (Ubuntu) Vary: Accept-Encoding Content-Length: 556 Content-Type: text/html;charset=UTF-8 ``` ----------

Pattern Type
stix
Pattern
[ipv4-addr:value = '195.123.212.53']

Malware

Name
Whiffy Recon

Name
Smoke Loader

Description
[Smoke Loader](https://attack.mitre.org/software/S0226) is a malicious bot application that can be used to load other malware. [Smoke Loader](https://attack.mitre.org/software/S0226) has been seen in the wild since at least 2011 and has included a number of different payloads. It is notorious for its use of deception and self-protection. It also comes with several plug-ins. (Citation: Malwarebytes SmokeLoader 2016) (Citation: Microsoft Dofoil 2018)

Attack-Pattern

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.

IPv4-Addr

Value
195.123.212.53
194.87.32.20

External References

- https://otx.alienvault.com/pulse/64eca0ac44f7afd8582ec134
- https://www.secureworks.com/blog/smoke-loader-drops-whiffy-recon-wi-fi-scanning-and-geolocation-malware