Oct 28 2023

NETMANAGEIT

Intelligence Report

Analysis of the expansion of fraudulent backdoors claimed to have been implanted in 20 million devices

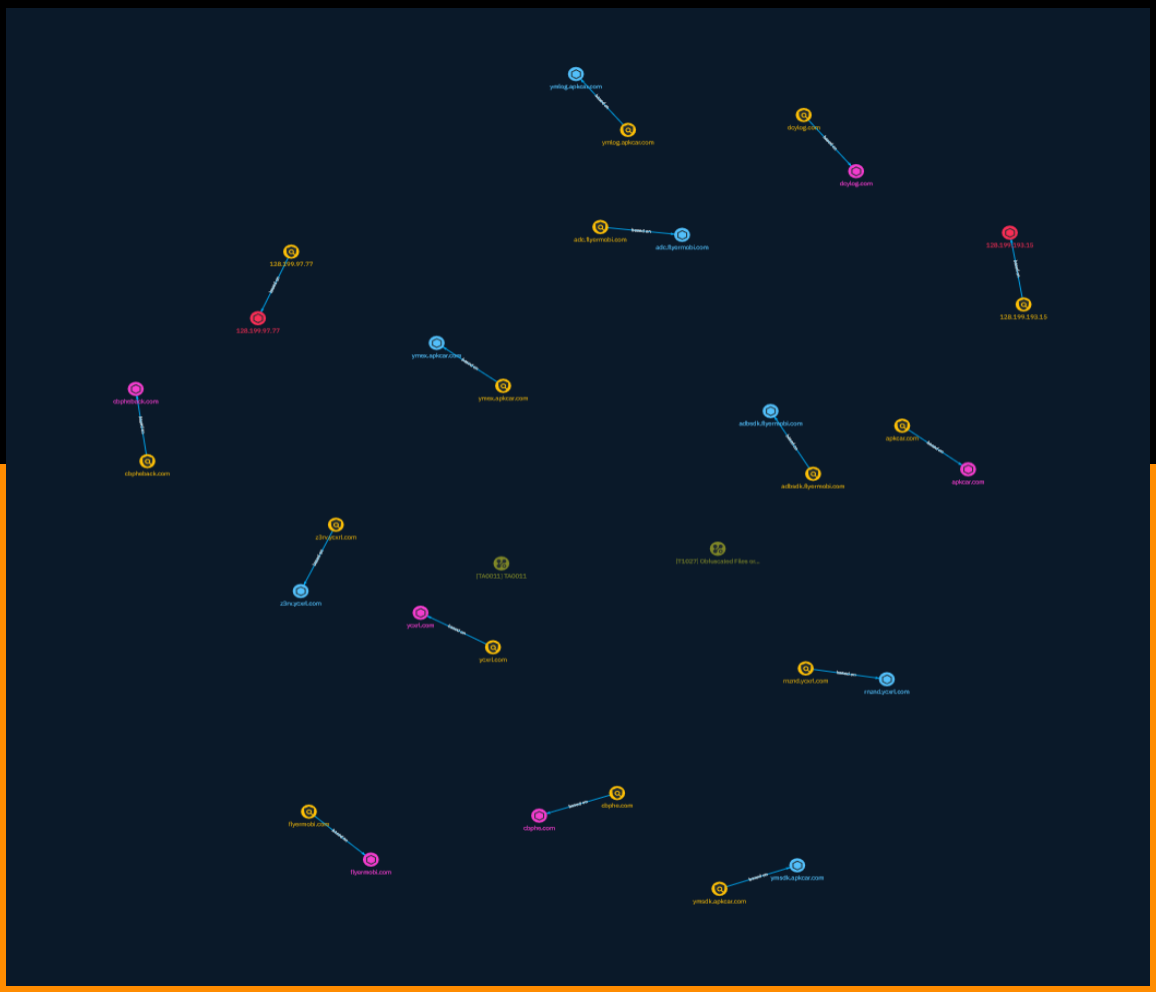

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Recently, the QiAnXin Threat Intelligence Center noticed that human security, a foreign security vendor, disclosed an incident called BADBOX on the Internet. It reported that at least 74,000 Android-based mobile phones, tablets, and global Internet-connected TV boxes were observed to have encountered BADBOX.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Obfuscated Files or Information
ID
T1027
Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name
TA0011

ID
TA0011

Indicator

Name
dcylog.com
Pattern Type
stix
Pattern
[domain-name:value = 'dcylog.com']
Name
ycxrl.com
Pattern Type
stix
Pattern
[domain-name:value = 'ycxrl.com']
Name
rnznd.ycxrl.com

Pattern Type

stix

Pattern

[hostname:value = 'rnznd.ycxrl.com']

Name

ymex.apkcar.com

Pattern Type

stix

Pattern

[hostname:value = 'ymex.apkcar.com']

Name

ymsdk.apkcar.com

Pattern Type

stix

Pattern

[hostname:value = 'ymsdk.apkcar.com']

Name

apkcar.com

Pattern Type

stix

Pattern

[domain-name:value = 'apkcar.com']

Name

128.199.193.15

Description

ISP: DigitalOcean, LLC **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDVsF6/zSSjIRe/7nPijYhk9rS7td5ZVWjaYhzy6a1N8dvG tJWnpqFt5puvFEUzZuUu1ja1aaOJtwFSlMq+pCyFU06NDpZ1O5vZyPIHwOhA+ADcPvpzkZP4AKtO CUADJt9FHlCr9Vpoi8xvWwa789hNJAqAJzCgb/I49qm6swdBRLrvTOGmQGNu3nIxeVZd6vk8tvHY WvecQwp+IAd0zGPUS2SrVFLgTLMmwwpmZEgqFhGG+wj5ydMTc5jMWNeZ+FwxPw3r2uOIpcut wzCr muHFRxSeIBAOL/BlrMsQMd/IhOdzqHOd7EPYy2ItogCOa+eZTpo7LYnooRVmE2yrGSur Fingerprint: 31:f1:fe:a8:1a:94:a4:d8:48:60:7f:5a:48:39:80:9b Kex Algorithms: curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: ssh-rsa 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/1.10.3 (Ubuntu) Date: Tue, 24 Oct 2023 07:33:50 GMT Content-Type: text/html Content-Length: 580 Connection: keep-alive ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '128.199.193.15']

Name

flyermobi.com

Pattern Type

stix

Pattern

[domain-name:value = 'flyermobi.com']

Name

128.199.97.77

Description

CC=SG ASN=AS14061 DIGITALOCEAN-ASN

Pattern Type

stix

Pattern

[ipv4-addr:value = '128.199.97.77']

Name

adbsdk.flyermobi.com

Pattern Type
stix
Pattern
[hostname:value = 'adbsdk.flyermobi.com']
Name
adc.flyermobi.com
Pattern Type
stix
Pattern
[hostname:value = 'adc.flyermobi.com']
Name
ymlog.apkcar.com
Pattern Type
stix
Pattern
[hostname:value = 'ymlog.apkcar.com']
Name
cbpheback.com

Pattern Type
stix
Pattern
[domain-name:value = 'cbpheback.com']
Name
z3rv.ycxrl.com
Pattern Type
stix
Pattern
[hostname:value = 'z3rv.ycxrl.com']
Name
cbphe.com
Pattern Type
stix
Pattern
[domain-name:value = 'cbphe.com']

Domain-Name

Value
ycxrl.com
dcylog.com
flyermobi.com
cbpheback.com
apkcar.com
cbphe.com

Hostname

Value
adbsdk.flyermobi.com
ymsdk.apkcar.com
ymex.apkcar.com
adc.flyermobi.com
z3rv.ycxrl.com
ymlog.apkcar.com
rnznd.ycxrl.com

IPv4-Addr

Value
128.199.97.77
128.199.193.15

External References

- https://otx.alienvault.com/pulse/6531315c5029eeeaab2f94c0
- https://mp.weixin.qq.com/s/MKDRGVnJFoUd4v1tc47PXQ