TrendLabs

How Machine Learning Helped Us Find Massive Certificate Abuse by BrowseFox

Appendix

TrendLabs Security Intelligence Blog

Jon Oliver

Threat Researcher

May 2018

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

BrowseFox Signers

Abstract skill

Access backbone

Access beat

Access plex

Ace race

Active tera

Activity clear

Adanak

Advanceelite

Affirmative online

Air globe

Alactro llc

Aline tech

Amber flow

Anything or nothing

Aperture energy

App bud

Appenable

Application nation

Appstein

Arctic world

Assist point

Astro find

Atuzi

Avenue logic

Axial drive

Balance corner

Balance scout

Balanced primary

Banana phone

Bar none deals

Bargain central

Batbrowse

Beta rez

Betterbrowse

Between lines

Bill break

Blazer deals

Blisssearch

Blue bulletin

Bold byte

Bold letters

Bolt flow

Bolt view

Boozaka

Box rock

Brass search

Break force

Brick bank

Bringstar

Bronze aid

Broom stroke

Browse burst

Browse camo

Browse pax

Browseden

Browsemark

Browsesmart

Browsestudio

Browser gloss

Browser good

Browsify

Buy list

Buy online

Buying guide

Buzzsearch

Buzzyard

Byte certified

Byte folder

Byte label

Byte letter

Byte linux

Byte points

Candle jar

Cantataweb

Caramava

Care fiercely

Cash kitten

Cash tracker

Cat dog

Catered to you

Central index

Centralops

Chance energy

Chart choosing

Checked list

Clear active

Clearthink

Cling clang

Clock hand

Cloud innovate

Coast file

Coast finder

Coast sense

Coast tag

Coffee amigo

Command digitized

Complete maker

Complete port

Compusocial

Computer chair

Constasurf

Core capable

Coupon center

Coupon time

Course blue

Course squad

Course talent

Crazy front

Creativealign

Culvert cleats

Current method

Cyber shop

Cyber store

Cyber translation

Cyti web

Dallas mission

Data buzz

Data indicated

Deal depot

Deal keeper

Deal leaders

Deal maverick

Design synergism

Divapton

Dig deep

Digi docket

Digihelp

Digicada

Digital ig

Digital more

Digitalcure

Discount hunter

Discovery app

Dizzyding

Dolphin deals

Doughgo

Draco cut

Dragon branch

Drive moment

Drive roth

Drop model

Dynamo combo

Esight insight

Edge essence

Edu app

Emoticon flash

Enaptive

Encryptview

Engage forte

Engineignite

Enhanceempire

Enhancetronic

Enter voyage

Enterdigital

Eos advance

Ever central

Explore translation

Express find

Fact fire

Fantastic skill

Faster light

Favicon force

Featured recommendations

Findright

Firegrid

Fixlab

Flying deals

Follow rules

Forever net

Fortunitas

Four finders

Framed display

Fresh outlook

Fresh slot

Fresh sync

Gadgetprise

Gamma handle

Gem grab

General buddy

Geowide

Giant galaxy

Girafarri

Global bolt

Global fuse

Global synerguise

Global vine

Go lieutenant

Golden dock

Grabrez

Great guide

Great hub

Happy cloud

Hard case

Hard paint

Hasbrowse

Hatchiho

Helping handle

Hero offers

Horizon alliance

Hot sales

Hover first

Hulatoo

Hybris generation

Icon choice

Icon initiate

Icon tips

Index clip

Index course

Inergennow

Info double

Info trigger

Information station

Innovation edge

Inspiring guide

Inspiring market

Inspiring plus

Instant coast

Instant funnel

Intactgate

Intel reboot

Intelmodel

Internet program

Java index

Jazz spot

Jotzey

Key byte

Kingbrowse

Kit local

Klip pal

Knowledge gains

Knowledgeslot

Krab web

Laflurla

Lampy lighty

Lane pad

Leapexpo

Lemurleap

Leopard movement

Leopardrun

Leto elite

Lightning bolt

Linkidoo

Linux ignite

Liongene

List agile

List gadget

Lite web

Look around

Lucky bright

Macro leaf

Magic ball

Magic walk

Malt mark

Massage discover

Match pal

Media woods

Megabrowse

Metal maker

Middle rush

Mobile ridge

Mobile spirit

Modern results

Mokiray

Money viking

Moss net

Mountain bike

Multistic

Nano surfer

Net leight

Netcrawl

Nettock

Network haven

Norpalla

Number ascend

Oasis space

Ocean pool

Office sparks

Officepro tech

Okiitan

Online hits

Operations proximity

Optical host

Optical operator

Optical surf

Optimallive

Orange proof

Overclocking network

Pacfunction

Page alliance

Pass to post

Pathmaxx

Pepper plain

Perfect bid

Pine tree

Plain savings

Plumoweb

Podoweb

Polished patterns

Pop bubbles

Portalmore

Positive finds

Powerfulbrowse

Price clip

Price riot

Primary color

Primary result

Prootis

Product deals

Progressive digital

Project letter

Protocol clear

Pulse rate

Purchase time

Pure possession

Puredomain

Pursuepoint

Quantumzone

Quest enaptive

Quest initiation

Rad rater

Rad raven

Radar speed

Rain delay

Range blaze

Range future

Range lane

Range picks

Ready ranger

Resultsbay

Resultsshare

Reverse page

Ridge smart

Rightsurf

Roam wild

Rock turner

Rolimno

Roll around

Round world

Royal raid

Sale planet

Sale report

Sale tube

Saltarsmart

Save raven

Saving index

Savvy savings

Scan tack

Scape nano

Score escape

Screen flip

Self starter

Seque source

Serial movement

Serial protocol

Serialtrunc

Sharp angle

Shell resolution

Shop easy

Shop essentials

Shoptions

Side plaza

Silver save

Simple for you

Ski search

Skill legacy

Slot green

Smarterpower

Social custody

Solution real

Solutionate

Sonic plane

Source app

Source location

Sourcecom

Space skill

Spadecast

Spark style

Special box

Spectra work

Speed capsule

Spend city

Spirit idea

Spring smart

Square corner

Squaretrace

Steadystream

Steel cut

Storimbo

Stormvade

Stream freefall

Stylus ventures

Sub suit

Sugarsearch

Summit index

Sunrisebrowse

Super great

Superinstall

Surftastic

Swift browse

Swift equinox

Swift record

Symmetry energy

Syndicate development

Systems reddick

Systems smart

Tactical expand

Target practice

Tasticsurf

Teal kitty

Tech missions

Tech terafile

Terminal u

Tessview

Thrill bill

Togglemark

Topictron

Totalreboot

Towertilt

Trackball array

Traditional base

Traditional board

Traditional gear

Traditional link

Traffic spiral

Treasure safe

Treat receipt

Trend delivery

Trinity idea

Triple pose

Unitech solutions

Unite explore

Universal status

Unveil realtech

Upperfind

Urturn filter

Useful program

Venturium

View scholar

Viewplay

Viperout

Virtual slot

Virtual transit

Visual alignment

Wake rise

Water plant

Web amplified

Web crown

Web layers

Web protocol

Web tripp

Websize

Webspades

Webporpoise

Wheel drift

White winter

Wild west

Winning combination

Wire icon

Wiseenhance

Wooden seal

Wunderweb

Xaven

Yawtix

Yoshi technology

Yula

Zebar

Zen forte

Zip path

Zippy zarp

Zoom zoom

Zoomcheck

Albrechto

Alleybrowse

Allgenius

Berrybesearch

Blindbat

Browse pulse

Browsebit

Clearspace

Crimsolite

Elements peruse

Esuack

Findopolis

Focusbase

Gate snapper

Gerbillio

Glindorus

Global gadget

Gooternet

Inlane

Innoapp

Karatoh

Loffinam

Lookinglink

Matinooch

Maucampo

Melondrea

Middle pages

Monarimo

Neurowise

Nicer together

Optitroy

Outobox

Playcube

Qualitink

Secretsauce

Shamanul

Sizlsearch

Snipsmart

Squirrelweb

Surf slide

Techgile

Thirteen degrees

Waleisa

Web waltz

Webget

Webrunn

Wisen wizard

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

©2017 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Securing Your Journey to the Cloud

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO