A brief history of TA505


intel471.com/blog/a-brief-history-of-ta505

INTEL471

A BRIEF HISTORY OF TA505

TA505 arguably is one of the most significant financially motivated threat groups because of the extraordinary volumes of messages the members send. The variety of malware developed by the group also demonstrated a deep connection to the underground malware ecosystem.

JULY 2014
First recorded campaign to distribute Dridex malware using botnet ID 125 targeting Canada, the U.K and the U.S.

MARCH 2015
Targeted Australia and the UK utilizing the Dridex botnet ID 220 and a range of email attachments.

OCT 2015
Targeted organizations in Japan and the U.K. with Shifu banking malware delivered via macro-laden Microsoft Office document attachments, and used the Neutrino bot.

FEB 2016
Began utilizing Locky ransomware Affid=3.

APRIL 2016
Introduced the use of RockLoader as a loader for Locky Ransomware, Pony malware and later Kegotip email & credential-harvesting malware.

JUNE 2016
Introduced the use of the Bart ransomware deployed as a secondary payload to Rockloader.

APRIL 2017
Briefly distributed the Kegotip information stealer using macro-

laden Microsoft documents and zipped VBScript (VBS) attachments.

MAY 2017

Introduced the use of Jaff ransomware.

JUNE 2017

Distributed Trickbot banking trojan aka The Trick via zipped Windows Script Files (WSF) and VBS scripts, malicious Microsoft Excel and password protected Word documents, HTML attachments, malicious Javascript and more.

JULY 2017

Introduced the use of the GlobelImposter and Philadelphia ransomware.

OCT 2017

Introduced their first geographically targeted campaign that dropped Locky or Trickbot.

FEB 2018

Deployed Pharmaceutical-targeted spam campaigns via BlackTDS, and smaller campaigns that distributed DreamSmasher, Dridex, GandCrab and QuantLoader malware.

MARCH 2018

Used Necurs botnet to deliver the FlawedAmmyy remote access trojan (RAT).

JUNE 2018

Attempted to deliver portable document format (.pdf) attachments with an embedded SettingContent-ms file via a large campaign with

hundreds of thousands of messages.

NOV 2018

Introduced the use of FlawedGrace and ServHelper malware, and deployed email campaigns against the food and beverage industry and large retail, restaurant and grocery chains.

DEC 2018

Targeted large U.S.-based retailers, food and beverage industry and financial institutions via spear-phishing campaigns with attached malicious, macro-enabled Microsoft files to download backdoor malware.

APRIL 2019

Targeted financial enterprises with benign scripts called Living Off the Land Binaries (LOLBins) to hide malicious content and used new backdoor malware.

MAY 2019

Increased targeting the banking sector and suspicious attacks against Italian organizations likely signified a potential expansion of operations.

JULY 2019

Targeted Singapore, South Korea, United Arab Emirates (UAE) and the U.S. using the FlawedAmmyy aka AndroMut malware to distribute backdoor malware, information stealers and other RATs via macro-enabled files.

SEPT 2019

Employed email campaigns to deliver and install the Get2 Loader used to download the FlawedAmmyy, FlawedGrace, SDBot and Snatch

malware as secondary payloads.

FEB 2020

Launched a campaign that used HTML redirectors attached to email to download a malicious Excel file that drops the payload dubbed Dudear.

MARCH 2020

Targeted human resources departments in Germany using business email compromise (BEC)-style phishing emails that leveraged malicious PowerShell scripts to steal browser and email login credentials and payment card data.
Used a Coronavirus Disease 2019 (COVID)-19 themed lure to deliver a downloader to a victim and download malware, such as banking trojans and ransomware.