POSITIVE TECHNOLOGIES

2010

MyWeb
- Checking for time acceleration
- Anti-analysis and anti-debugging

2011

EvilBunny
- Checking module file name
- Checking running processes
- Anti-analysis and anti-debugging

2013

Chopstick
- Checking the environment

2014

BS2005
- Anti-analysis and anti-debugging

Ursnif
- Delaying execution

2015

CozyCar
- Checking registry key values
- Injecting code into process address space
- Anti-analysis and anti-debugging

Dyre
- Checking fields in Process Environment Block
- Anti-analysis and anti-debugging

2016

Denis
- Anti-analysis and anti-debugging

Pony
- Checking the environment
- Sending WMI queries
- Anti-analysis and anti-debugging

ROKRAT
- Checking registry key values
- Checking loaded DLLs
- Anti-analysis and anti-debugging

Okrum
- Checking for user interaction
- Checking the environment
- Anti-analysis and anti-debugging

2017

Denis
- Anti-analysis and anti-debugging

Ursnif
- Performing TLS callback

Okrum
- Anti-analysis and anti-debugging

GravityRAT
- Checking registry key values
- Sending WMI queries

StoneDrill
- Anti-analysis and anti-debugging

FIN7
- Sending WMI queries
- Anti-analysis and anti-debugging

UBoatRAT
- Checking the environment

PlugX
- Checking running processes

RTM
- Anti-analysis and anti-debugging

2018

Yty
- Checking the environment

FinFisher
- Checking the parent process
- Checking execution location
- Checking file path
- Checking registry key values
- Checking the environment
- Checking loaded DLLs
- Anti-analysis and anti-debugging

Remcos
- Checking loaded DLLs
- Anti-analysis and anti-debugging

RogueRobin
- Sending WMI queries
- Checking running processes

ROKRAT
- Checking the environment
- Checking loaded DLLs
- Anti-analysis and anti-debugging

Smoke Loader
- Checking running processes
- Anti-analysis and anti-debugging
- Checking registry key values

BadPatch
- Sending WMI queries

The White Company
- Checking the date and time
- Anti-analysis and anti-debugging

SynAck
- Checking execution location
- Anti-analysis and anti-debugging

OopsIE
- Sending WMI queries
- Checking for a file in the system directory
- Anti-analysis and anti-debugging

2019

Okrum
- Sending WMI queries
- Anti-analysis and anti-debugging

RogueRobin
- Checking running processes
- Sending WMI queries
- Anti-analysis and anti-debugging

Remcos
- Checking running processes
- Anti-analysisand anti-debugging

Pony
- Sending WMI queries

RTM
- Checking the environment
- Anti-analysis and anti-debugging

HAWKBALL
- Anti-analysis and anti-debugging

Attor
- Anti-analysis and anti-debugging

LO2
- Checking the environment
- Addressing I/O port

Hakbit
- Checking loaded DLLs
- Anti-analysis and anti-debugging

OSX_OCEANLOTUS.D
- Checking the environment
- Anti-analysis and anti-debugging

2020

PoetRAT
- Sending WMI queries
- Anti-analysis and anti-debugging

Snake
- Checking running processes
- Anti-analysis and anti-debugging

PipeMon
- Checking running processes

Trickbot
- Checking the environment

Maze
- Checking the environment
- Checking the date and time
- Checking loaded DLLs
- Sending WMI queries
- Checking registry key values
- Anti-analysis and anti-debugging

Motives

- Espionage
- Financial profit

Types of malware

- Spyware
- Banking trojan
- Ransomware
- RAT
- Loader