ptsecurity.com

aranc Ø chronology 2011

2012

2013

2014

2015

ZeroAccess | 🔐 🎎

- Runs a miner or clicker after infection
- Can be used to attack GSM stations

Hikit



- Used by the Axiom APT group
- Provides remote access to compromised hosts
- Aimed at data harvesting

Ebury



- Used by the Windigo APT group
- Steals OpenSSH credentials
- Provides remote access to compromised hosts

Flame



- Used by the Equation APT group
- Intercepts network traffic
- Erases traces of the attacker's activity on the infected machine
- · Can record sound and take screenshots, as well as transmit captured data, including via Bluetooth

Necurs



- Can download ransomware and banking Trojans; was observed in the Dridex distribution campaign
- Disables protection tools
- Uses domain generation algorithms (DGA)
- Contains a spam email module for other attacks, and a traffic redirection module

Regin



- Used by the Equation APT group
- Can infect GSM station controllers
- Contains a set of espionage tools
- Provides remote access to compromised hosts

Careto | 🐧 🖒 🛱 🔡 🕒

- Used by the Mask APT group
- Has two modules: rootkit and bootkit
- Source code is signed with a digital certificate
- Collects VPN and RDP configuration files and SSH keys
- Allows attackers to run commands

Kronos



- Performs data collection for Internet banking access
- Combines banking Trojan and downloader functions
- Distributed as part of phishing campaigns

Shedun



- Used by the Yingmob group
- Mimics popular apps
- Can be used to download additional malware, including adware

Umbreon





- Installs the Espeon backdoor
- Creates local users to access the infected system
- Intercepts libc calls to hide the presence of a new user in the /etc/passwd file

2016

Remsec (Cremes) | !!! ()

Used by the Strider APT group

Provides remote access

Used in cyberespionage campaigns

to compromised hosts and allows

downloading additional software

Contains a module for intercepting

network traffic and keystrokes

2017

DirtyMoe

■ Spreads like a worm, roping

Uses the victim's computing

and mine cryptocurrency

resources to carry out DDoS attacks

victims into a botnet

2018

Moriya

■ Presumably used by APT1

Hides communication

with the C&C server

Provides remote access

to compromised hosts

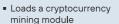
1880

Skidmap

2019







■ Displays fake CPU load data

Scranos



- Injects adware on compromised hosts
- Steals credentials from the browser
- Distributes adware for mobile devices through hacked social media accounts

Drovorub

Used by APT28

2020

 Provides a communication channel with the C&C server

- Can intercept and redirect network traffic
- Changes firewall rules























