

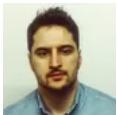
The malware that usually installs ransomware and you need to remove right away

zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/



[Home Innovation Security](#)

If you see any of these malware strains on your enterprise networks, stop everything you're doing and audit all systems.



Written by [Catalin Cimpanu, Contributor](#) on Nov. 19, 2020

-
-
-
-
-

Image: Lina White

Gone are the days when ransomware groups operated by launching mass email spam campaigns in the hopes of infecting random users across the internet.

Today, ransomware operators have evolved from a niche of clumsy malware gangs into a series of complex cybercrime cartels with the skills, tools, and budgets of government-sponsored hacking groups.

Nowadays, ransomware gangs rely on multi-level partnerships with other cybercrime operations. Called "**initial access brokers**," these groups operate as the supply chain of the criminal underground, providing ransomware gangs (and others) with access to large collections of compromised systems.

Consisting of hacked RDP endpoints, backdoored networking devices, and malware-infected computers, these systems allow ransomware gangs to easily gain access to corporate networks, escalate their access, and encrypt files to demand huge ransoms.

These initial access brokers are a crucial part of the cybercrime scene. Today, three types of brokers stand out as the sources of most ransomware attacks:

- **Sellers of compromised RDP endpoints:** Cybercrime gangs are currently carrying out brute-force attacks against workstations or servers configured for remote RDP access that have also been left exposed on the internet with weak credentials. These systems are later sold on so-called "RDP shops" from where ransomware gangs often select systems they believe might be located inside the network of a high-value target.
- **Sellers of hacked networking devices:** Cybercrime gangs are also using exploits for publicly known vulnerabilities to take control of a company's networking equipment, such as VPN servers, firewalls, or other edge devices. Access to these devices and the internal networks they protect/connect is sold on hacking forums or to ransomware gangs directly.
- **Sellers of computers already infected with malware:** Many of today's malware botnets will often comb through the computers they infect for systems on corporate networks and then sell access to these high-value systems to other cybercrime operations, including ransomware gangs.

Protecting against these three types of initial access vectors is often the easiest way of avoiding ransomware.

However, while safeguarding against the first two typically involves practicing good password policies and keeping equipment updated, the third vector is harder to protect against.


This is because malware botnet operators often rely on social engineering to trick users into installing malware on their systems themselves, even if computers are running up-to-date software.

This article focuses on the known malware strains that have been used over the past two years to install ransomware.

Compiled with the help of security researchers from [Advanced Intelligence](#), [Binary Defense](#), and [Sophos](#), the list below should serve as a "code red" moment for any organization.

Once any of these malware strains are detected, system administrators should drop everything, take systems offline, and audit and remove the malware as a top priority.

ZDNet will keep the list up to date going forward.

 r-emotet.png

Emotet is considered today's biggest malware botnet.

There are few cases where Emotet has dealt with ransomware gangs directly, but many ransomware infections have been traced back to initial Emotet infections.

Usually, Emotet sold access to its infected systems to other malware gangs, which later sold their own access to ransomware gangs.

Today, the most common ransomware infection chain linked back to Emotet is: **Emotet—Trickbot—Ryuk**


 r-trickbot.png

Trickbot is a malware botnet and cybercrime similar to Emotet. Trickbot infects its own victims but is also known to buy access to Emotet-infected systems in order to boost its numbers.

Over the past two years, security researchers have seen Trickbot sell access to its systems to cybercrime gangs that later deployed Ryuk, and later the Conti ransomware.

Trickbot—Conti

Trickbot—Ryuk

 r-bazar.png

BazarLoader is currently considered to be a modular backdoor developed by a group with links or that spun off from the main Trickbot gang. Either way, regardless of how they came to be, the group is following Trickbot's model and has already partnered with ransomware gangs to provide access to the systems they infect.

Currently, BazarLoader has been seen as the origin point for infections with the Ryuk ransomware [1, 2, 3].

BazarLoader—Ryuk

 r-qbot.png

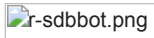
QakBot, Pinkslipbot, Qbot, or Quakbot is sometimes referred inside the infosec community as the "slower" Emotet because it usually does what Emotet does, but a few months later.

With the Emotet gang allowing its systems to be used to deploy ransomware, QakBot has also recently partnered with different ransomware gangs. First with MegaCortex, then with ProLock, and currently with the Egregor ransomware gang.

QakBot—MegaCortex

QakBot—ProLock

QakBot—Egregor

r-sdbbot.png

SDBBot is a malware strain operated by a cybercrime group referred to as TA505.

It's not a common malware strain but has been seen as the origin point of incidents where the Clop ransomware was deployed.


SDBBot—Clop

 r-dridex.png

Dridex is yet another banking trojan gang that has reorganized as a "malware downloader," following the examples set by Emotet and Trickbot in 2017.

While in the past Dridex botnet has used spam campaigns to distribute the Locky ransomware to random users across the internet, for the past few years, they are also using computers they have infected to drop either BitPaymer or the DoppelPaymer ransomware strains for more targeted attacks against high-value targets.

Dridex—BitPaymer
Dridex—DoppelPaymer

 r-zloader.png

A late arrival to the "install ransomware" game, Zloader is catching up fast and has already established partnerships with the operators of Egregor and Ryuk ransomware strains.

If there's one malware operation that has the ability and connections to expand, this is it.

Zloader—Egregor

Zloader—Ryuk

 r-buer.png

Buer, or Buer Loader, is a malware operation that launched late last year, but has already established a reputation and connections in the cybercrime underground to partner with ransomware groups.

Per Sophos, some incidents where the Ryuk ransomware has been discovered have been linked back to Buer infections days before.


Buer—Ryuk

 r-phorpiex.png

Phorpiex, or Trik, is one of the smaller malware botnets, but not less dangerous.

Infections with the Avaddon ransomware seen earlier this year have been linked to Phorpiex. Although neither Avaddon nor Phorpiex are common names, they should be treated with the same level of attention as Emotet, Trickbot, and the others.

Phorpiex—Avaddon

 r-cobalt.png

CobaltStrike is not a malware botnet. It's actually a penetration testing tool developed for cyber-security researchers that is also often abused by malware gangs.

Companies don't get "infected" with CobaltStrike. However, many ransomware gangs deploy CobaltStrike components as part of their intrusions.

The tool is often used as a way to control multiple systems inside an internal network and as a precursor to the actual ransomware attack.

Many of the infection chains listed above are actually **[MalwareBotnet]—CobaltStrike—[Ransomware]**, with CobaltStrike usually serving as the most common intermediary bridging the two.

We included CobaltStrike on our list at the request of our sources, who consider it as dangerous as a de-facto malware strain. If you see it on your network and you're not running a penetration test, then stop everything you're doing, take systems offline, and audit everything for an attack's entry point.

The FBI's most wanted cybercriminals
