Ransomware Protection

Whitepaper

RANSOMWARE AT-A-GLANCE

- Ransomware is a malware that aims at extoring the victims for money
- Ransomwares are often created by criminal gangs with extensive experience and infrastructure
- In 2016 ransomware grew by 400% and costed private individuals and companies several billion USD
- Most ransomwares encrypts the files on the infected computers, but some holds the entire computer as a hostage
- In most cases, once infected and the files are encrypted, there is no way to decrypt the files without paying the ransom fee.
- Most users get infected through emails, but remote attacks and infected websites are also relevant attack vectors.
- Most analysts agree, in 2017 ransomware will evolve to target IoT devices such as Point of Sales systems, ATM machines, Smart TVs, Heating/Climate Control systems and similar.

Introduction

With cybercriminals making billions of dollars from ransom demands, ransomware is unanimously identified as one of the biggest threats businesses face today.

Ironically, the main estimated cost is not the ransom amount but the business downtime it causes[1] – so it is not at all surprising that only one third of businesses believe they will actually recover from a ransomware attack[2].

Clavister together with its technology partner Bitdefender has been closely following the evolution of ransomware, predicting its next steps and introducing techno-logies to handle ransomware specifically.

The best protection if achieved through a combination of educating the end users, infrastructure security such as Next Generation Firewalls and good protection in the form of Endpoint Client software installed on all devices and that follows the user also when leaving the office.

In the following paper, you will learn what you need to know about ransomware, and what technologies Clavister offers, through its partnership with Bitdefender, to uses who wish to protect their business against one of the biggest threats faced today.

WHAT IS RANSOMWARE?

Malware tries to adapt to the surroundings to survive. Some fail, but some thrive, even spreading to become an epidemic. Cyber-threats are no different. In 2015, ransomware caused $350 million3 in damage, living up to its reputation as the most significant menace targeting Internet users and organizations to date. What's more, 3 in 4 security professionals see the re-emergence of ransomware as the greatest new threat to appear in the last 12 months, according to a 2016 BlackHat survey.

Modern ransomware is a type of malware that locks and usually encrypts an operating system until the user pays to regain access. The malware can enter a system through a malicious downloaded file, a vulnerability in a network service or a text message.

Why is it different from traditional malware?

- It doesn't steal victims' information, but rather encrypts it
- It doesn't try to hide itself after files are encrypted because detection won't restore the lost data
- It demands ransom, usually in a virtual currency such as Bitcoins
- It's relatively easy to produce—there are a number of well-documented crypto-libraries

WHAT FORMS DOES IT TAKE?

There are two main types of ransomware in circulation.

Device lockers. *This type of ransomware locks the device screen and displays a full-screen image that blocks access to the device. The message demands payment, but personal files are not encrypted. This type of ransomware is often presented as a message from police and threatens to fine users for alleged online indiscretions or criminal activities.*

Crypto-ranomswares. *File-encryptors are more evolved than lockers, boasting irreversible encryption of personal files and folders such as documents, spreadsheets, pictures and videos.*

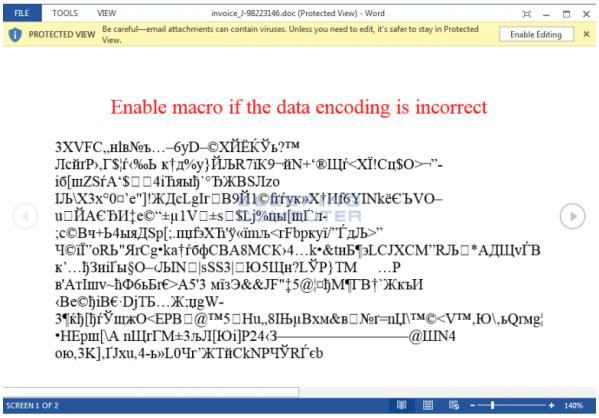
Both types of malware deny access to computer resources, but lockers can be dismantled through various system restore techniques and tools while encryptions can't be easily deciphered, making them more destructive.

WHAT YOU NEED TO KNOW

Clavister and Bitdefender are closely following the evolution of ransomware in 2016, trying to predict its next steps and developing technologies to protect against this major threat.

In the first three months of 2016, spam email with attached files increased by 50%, according to data from Bitdefender Antispam Lab. Similar data is also shown by other analysts.

Partially responsible for the large volumes of infected email attachments is the proliferation of crypto-ransomware. Locky and Petya, two emerging ransomware threats, are aggressively hunting victims via massive spam campaigns spreading Word documents disguised as invoices and Dropbox links to malicious



A Locky-infected document, sent as attachment in a spam email. Once a victim enables the macros, the macros will download an executable from a remote server and execute it. Source blog.knowbe4.com - It's Here. New Locky Ransomware Hidden In Infected Word Files

applications. The two new ransomware proved so prolific that Locky, for example, infected over 400,000 workstations in just a few hours[4].

RANSOMWARE IS DANGEROUSLY EXPANDING ACROSS DEVICES

Windows remains the main victim of ransomware – with variants going through various transformations, as law enforcement and security companies hammered down on some of the most popular and prolific variants, such as CryptoLocker, TorLocker, BitLocker and others.

Bitdefender, supplier of the technology found in the Clavister Endpoint Security Client, currently has a knowledge-base of 2.8 million ransomware samples, and 3 acting technologies to protect Windows systems against this threat.

Ransomware is not only prolific on Windows, but also on Android, Linux and even MacOS. The Android operating system was deemed a likely candidate for the new generation of mobile ransomware, not only because of its staggering 82.2 percent market share in Q2 2015, according to IDC[5], but also because it has more than 1.4 billion 30-day active users globally, according to Google CEO Sundar Pichai[6].

Bitdefender's statistics show the Android SLocker ransomware family accounts for 4.35 percent of all mobile malware reported by infected devices in Q3 2015, and 3.08 percent in Q4 2015.

The newest development in ransomware has been its attack on the Linux operating system. Linux-enabled webservers are at the heart of the Internet, many even hosting dozens of websites. Successful infection could affect more than one victim, so ransom payouts could also increase. One of our 2016 predictions actually involves the evolution of Linux ransomware, making it one the most serious threats to date.

Clavister, together with Bitdefender are also closely following the evolution of Mac ransomware that as of KeRanger, the first ransomware for Mac OSx, is picking up more traction.

HOW DOES CLAVISTER PROTECT BUSINESSES AGAINST RANSOMWARE?

All Clavister Endpoint Security Clients use not one, but two protection layers against ransomware. The two technologies work independently.

Together, they form one of the market's most powerful shields against this ransomware.

To enhance your existing endpoint protection, you can use the ransomware vaccine. It works with any solution you are using.

BLOCKS MOST RANSOMWARE FOUND TODAY

WHY SIMILARITY SIGNATURE-BASED DETECTION?

Signature-based detection is the first line of defense against ransomware attacks. It is not sufficient to protect against this threat, but it nevertheless plays an important role in every business security solution against ransomware.

- **BLOCKS THE EXECUTION OF EVERY KNOWN RANSOMWARE FAMILY.** Detects and blocks every known sample of ransomware from all major and lesser ransomware families.
- **BLOCKS NEW RANSOMWARE VARIANTS FROM KNOWN FAMILY.** Ransomware is polymorphic, creating new copies on each particular device. Clavister identify droppers instead of files, to counter-act this ability.
- **BLOCKS RANSOMWARE WITH BEHAVIOUR SIMILAR TO KNOWN RANSOMWARE FAMILIES.** Thanks to its similarity technology. Clavister can catch previously unknown ransomware, if it's similar in behaviour to known ones.
- **2.8 MILLION NEW RANSOMWARE AND COUNTING.** Bitdefender can detect a total of 2.8 million unique ransomware samples from the last 2 years alone.

HOW IT WORKS

Ransomware is polymorphic – this means that each sample is unique, customized for each victim. This is why signing each sample would not make sense in ransomware's case.

Dropper Signatures

To maximize this traditional detection method, besides the sample, Clavister and Bitdefender also signs the dropper, blocking the attack vector before the ransomware actually reaches your device.

What is the dropper?

During a ransomware attack, the ransomware itself is not the first malicious piece that reaches your device. Whenever you click on the wrong link or file, what is actually downloaded first is a dropper – a small piece of software that acts as a downloader for the actual ransomware piece.

Another advantage of blocking droppers instead of the actual ransomware besides anticipating the infection is that a dropper can be used on multiple devices. So each new victim targeted by that specific dropper that uses Clavister Endpoint Security Client will be completely safe from that ransomware.

Similarity Signatures - Blocking Zero-Day malware based on similarity patterns

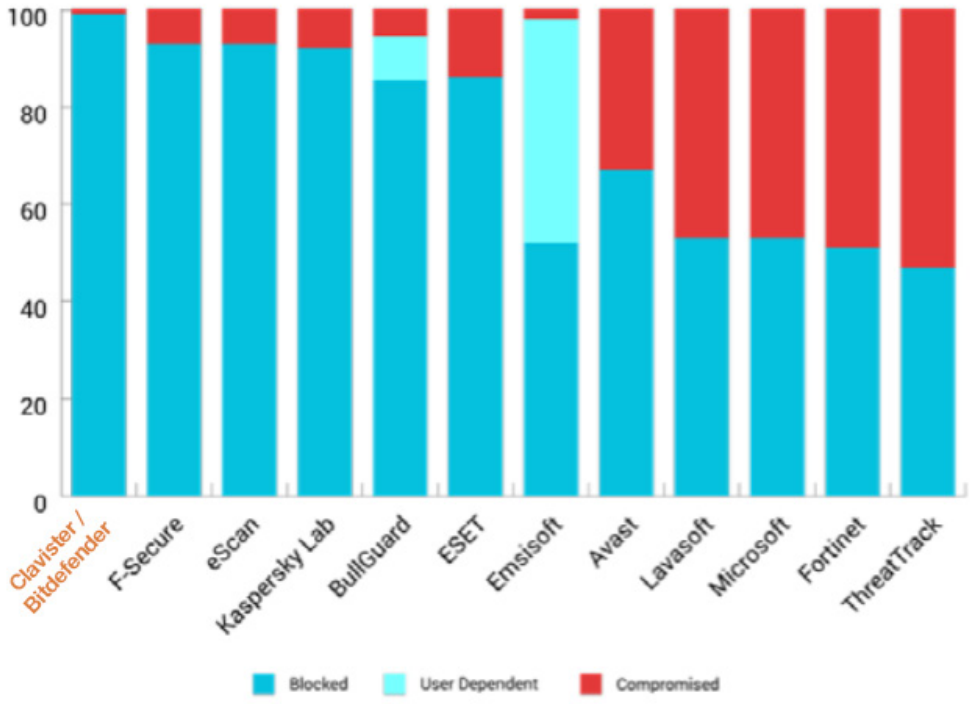
The Clavister Endpoint Security Client can also detect variations that are similar to previously known ransomware, through an internally developed algorithm called simhash. By using simhash, similar ransomware attacks can be blocked, even if the sample was previously unknown.

STOP NEVER-SEEN-BEFORE RANSOMWARE

CLAVISTER AND BITDEFENDER - HIGHEST SCORE AGAINST UNKNOWN THREATS?

The Clavister Endpoint Security Client reaches near-perfect score against new threats, while market average continues to drop The efficiency of the Advanced Threat Control feature can be best demonstrated by Heuristic or Behavioral tests, such as the AV- Comparatives, Proactive Protection Test. The independent report tests leading AV/Antimalware products against new or zero-day malware and ranks their performance based on their ability to block malware samples. Because the threats are new, traditional signatures are useless, so detection relies solely on the heuristic technologies.

In the 2015 test, Clavister/Bitdefender outperformed all other solutions, blocking 99% of the samples, with the nearest competitor blocking 93%. Bitdefender has also scored over 97% in the last 3 years consecutively, with the industry average for this test dropping from 84% to 75% in the same period..



WHY RANSOMWARE ADVANCED THREAT CONTROL?

Since September 2015, Clavister / Bitdefender has extended its proprietary heuristic technology, called ATC, to also detect previously unknown ransomware. The technology uses advanced behavioral models to nd ransomware, even if it has not been signed.

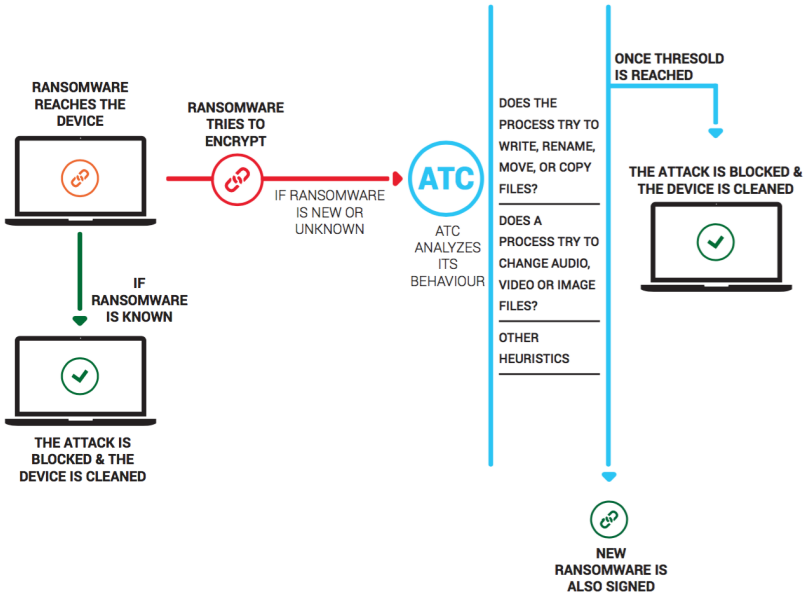
- **INCREDIBLY EFFECTIVE AGAINST NEW BLACK MARKET RANSOMWARE.** Detects new ransomware families that can be purchased and generated through the black market – because they all exhibit similar behavior in essence.
- **DETECTS UNKNOWN** types of ransomware. Ransomware behavior is similar, even if polymorphic. A strong behavioral technology can catch even new variants by using adapted heuristics.
- **WORKS ON COMPLEX BEHAVIOURAL DETECTION.** New variants of ransomware are incredibly easy to make, so signature-based detection cannot keep up. To catch it, a technology needs to track it down by its behavior.
- Uses **RENOWNED ADVANCED THREAT CONTROL (ATC)** technology. ATC has proven an incredibly effective technology in uncovering unknown malware. ATC constantly earns Clavister and Bitdefender top marks in detection by making the difference in uncovering new or unknown malware.
- **PROTECTS AGAINST DIGITALLY SIGNED RANSOMARE.** Even if a ransomware is digitally signed, it will still exhibit malicious behavior, and will be blocked..

HOW THE SOLUTION WORKS

The ATC doesn't need signatures, as it uncovers ransomware simply by its behavior. To determine if a process is ransomware before it gets a chance to hit, ATC watches over all active processes, and marks any suspicious behavior with a score. If a process take several suspicious actions, it will receive a higher score. Once the score passes a threshold, ATC signals other technologies to block the process.

Here are some actions the Clavister Endpoint Security Client looks out for that can indicate ransomware behavior:

DOES THE PROCESS TRY TO WRITE, RENAME, MOVE, OR COPY FILES? A ransomware's single purpose is to encrypt your les. Therefore, the most common actions associated with ransomware are write, rename, move or copy. Bitdefender's ATC constantly checks any program that tries to take one of these actions.



DOES A PROCESS TRY TO CHANGE AUDIO, VIDEO OR IMAGE FILES? Ransomware also targets audio, video or image les. So ATC becomes even more suspicious if a program tries to take one of the actions above on any of these file types.

These are just some examples. Bitdefender Ransomware ATC constantly watches for dozens of actions that can indicate the presence of ransomware.

ATC detection works locally, and does not need a Cloud connection. The technology is autonomous, as ransomware heuristic parameters de ned by the technology work by themselves.

INTELLIGENT AND PROCTIVE APPROACH TO RANSOMWARE

Ransomware is one of the largest threats businesses have ever had to face and a targeted approach is monumental to defend your business against it.

Clavister has not one, but three anti-ransomware layers in its Endpoint Security Client, with more to be added in the near future.

- ATC technology, which offers protection against new forms of ransomware, makes a major contribution in the excellent scores that Bitdefender receives against zero-day threats.
- Clavister Endpoint Security Client has also scored over 97% in the last 3 years consecutively, with the industry average for this test dropping from 84% to 75% in the same time period.
- Clavister Endpoint Security Client can detect a total of 2.8 million unique ransomware samples from the last 2 years alone.

While ransomware remains at large, there is a very fine line between a healthy, trustworthy business and unexpected business downtime that can damage your reputation.

Use the right tools with an intelligent and proactive approach to strengthen your security posture.

In addition to using an intelligent and Proactive endpoint security client like Clavisters, it is also important to look at how the entire organization needs to be protected, this includes using Next Generation Firewalls which capabilities such as stream-based antivirus, web content filtering and application control.

About Clavister
Clavister (NASDAQ: CLAV) is a leading security provider for fixed, mobile and virtual network environments. Its award-winning solutions give enterprises, cloud service providers and telecoms operators the highest levels of protection against threats, with unmatched reliability. Clavister's performance in the security sector was recognized with the Product Quality Leadership Award from Frost & Sullivan. The company was founded in Sweden in 1997, with its solutions available globally through its network of channel partners. To learn more, visit www.clavister.com.

Where to Buy
www.clavister.com/partners

Contact
www.clavister.com/contact

CONNECT . PROTECT

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
■ **Phone:** +46 (0)660 29 92 00 ■ **Fax:** +46 (0)660 122 50 ■ **Web:** www.clavister.com