Bitdefender®

WHAT YOU NEED TO KNOW ABOUT RANSOMWARE

AND HOW BITDEFENDER HELPS YOU STAY SAFE

With cybercriminals making millions – if not 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].

Bitdefender has been closely following the evolution of ransomware, predicting its next steps and introducing technologies to handle ransomware specifically.

In the following paper, you will learn what you need to know about ransomware, and what technologies Bitdefender uses to protect your business against one of the biggest threats it faces today.

1 http://www.prnewswire.com/news-releases/report-identifies-ransomwares-biggest-cost-to-be-business-downtime-300236505.html

2 https://www.hotforsecurity.com/blog/only-38-of-businesses-believe-they-will-recover-from-a-ransomware-attack-13625.html

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 million[3] 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.

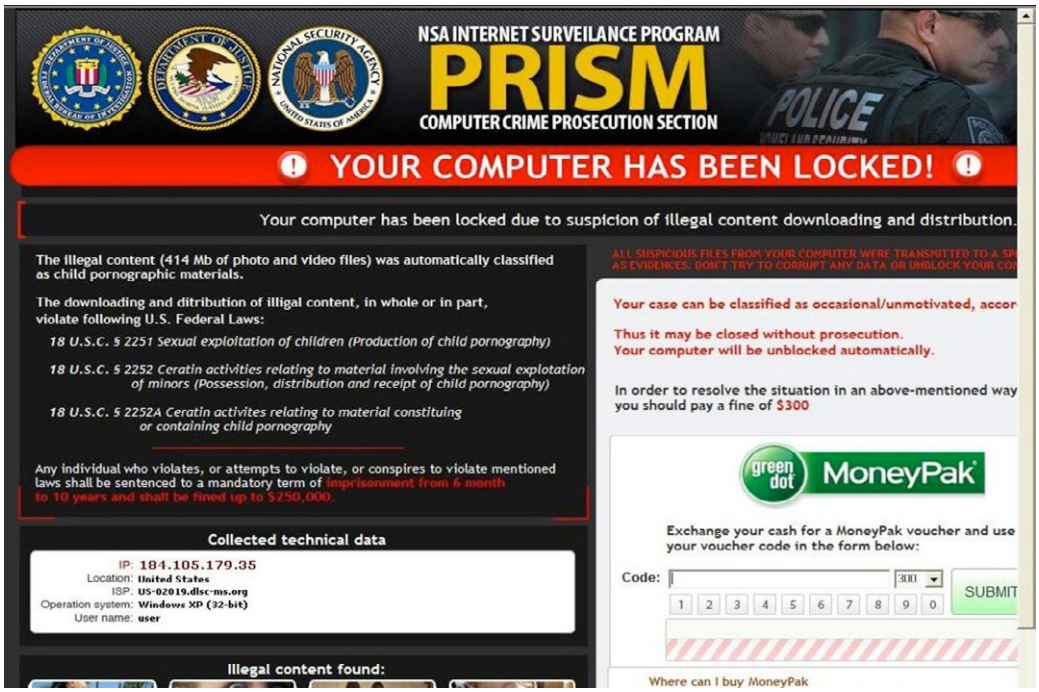
Why is it different from traditional malware?

- 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
- It's relatively easy to produce—there are a number of well-documented crypto-libraries

WHAT FORM DOES IT TAKE?

There are two main types of ransomware in circulation.

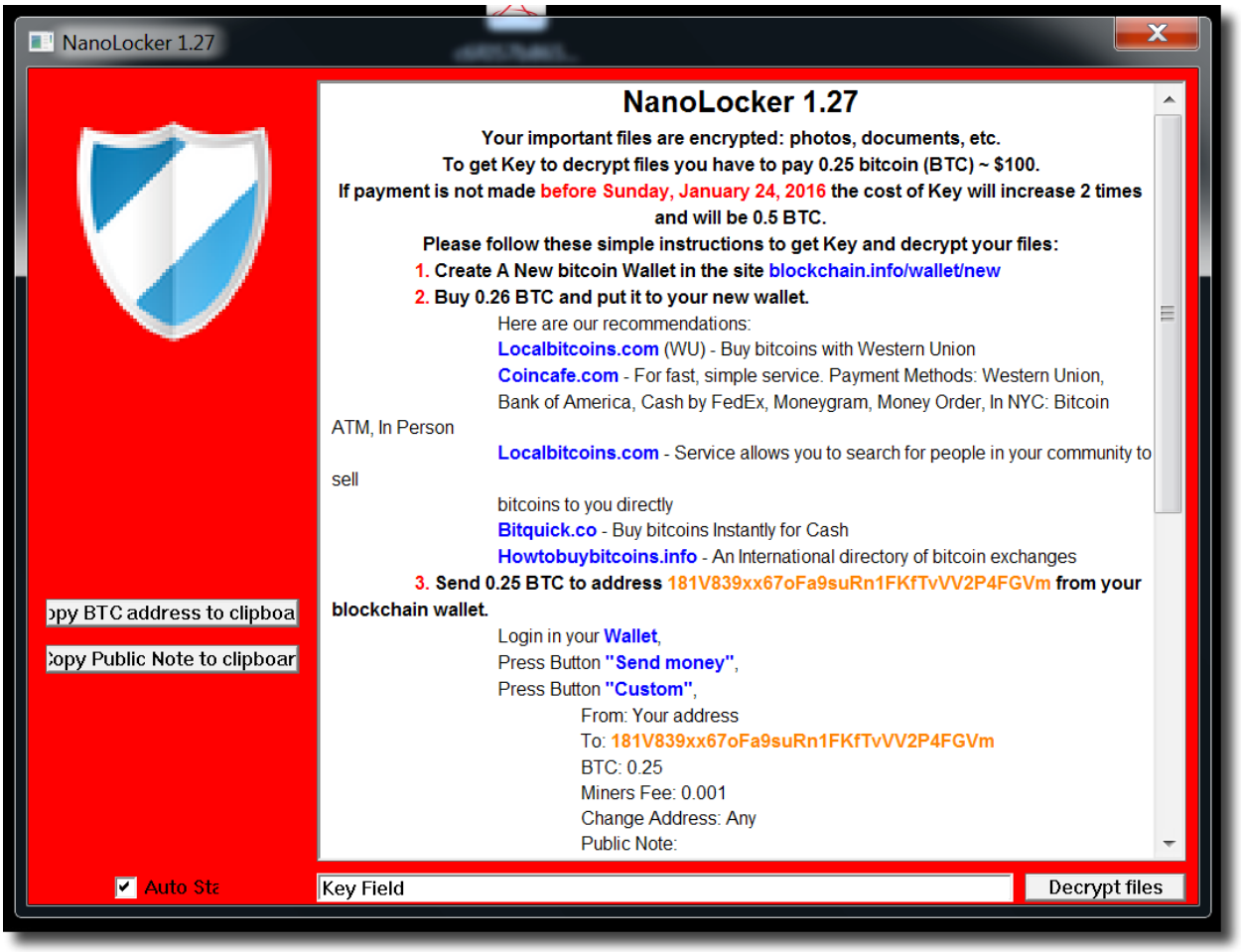
Device lockers. This type of ransomware locks the device screen and displays a full-screen image that blocks access to the device. The message demands payment, but personal files are not encrypted. This type of ransomware is often presented as a message from police and threatens to fine users for alleged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



Source: theregister.co.uk - Hackers giving up on crypto ransomware. Now they just lock up device, hope you pay

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

3 http://download.bitdefender.com/resources/files/News/CaseStudies/study/59/Bitdefender-Ransomware-A-Victim-Perspective.pdf



Source: blog.malwareclipboard.com – Nanolocker Ransomware Analysis

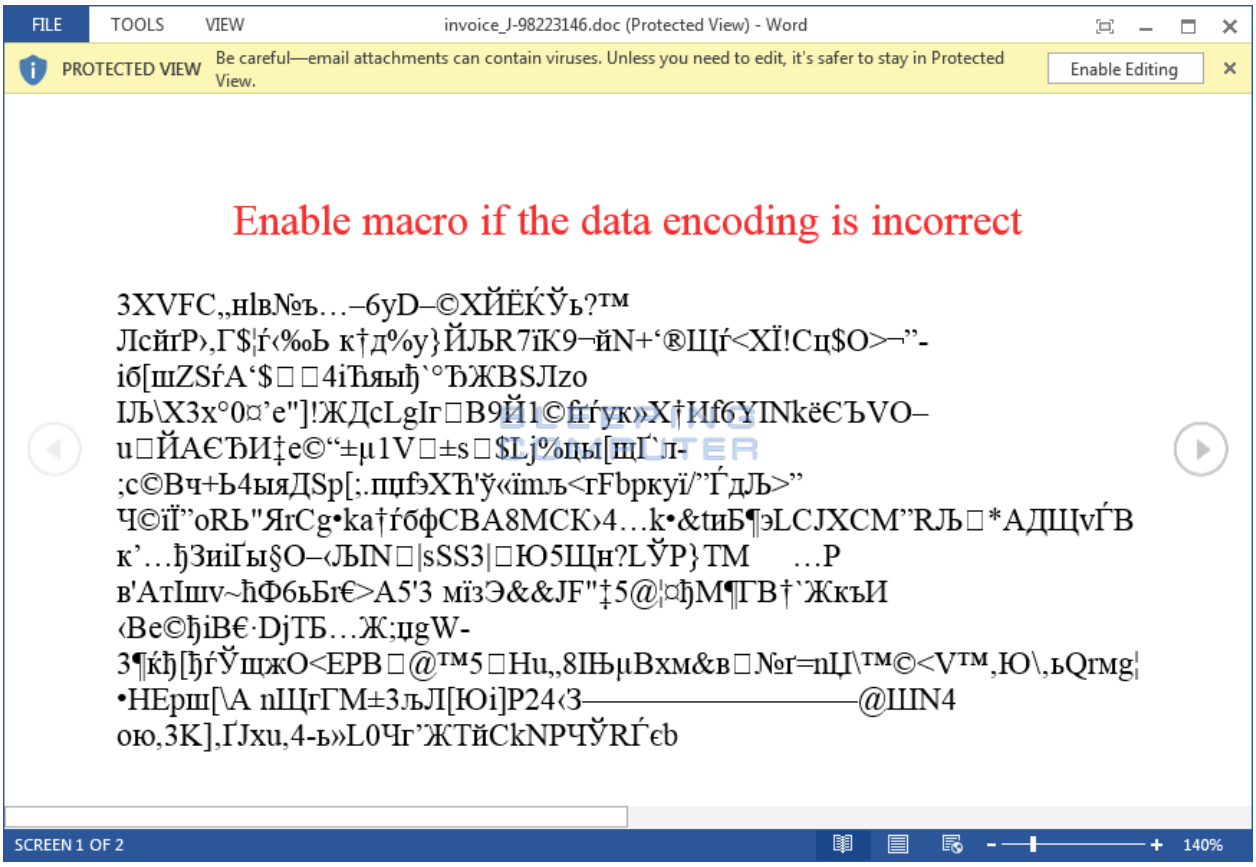
Both types of malware deny access to computer resources, but lockers can be dismantled through various system restore techniques and tools while encryptions can't be easily deciphered, making them more destructive.

WHAT YOU NEED TO KNOW

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

4 https://blog.knowbe4.com/its-here.-new-ransomware-hidden-in-infected-word-files



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

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 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 own 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.

Bitdefender is the first security vendor to release a decryption tool for Linux ransomware victims – free of charge. Bitdefender researchers were able to find cracks in the encryption algorithms used to lock the files of Linux.Encoder encryption.

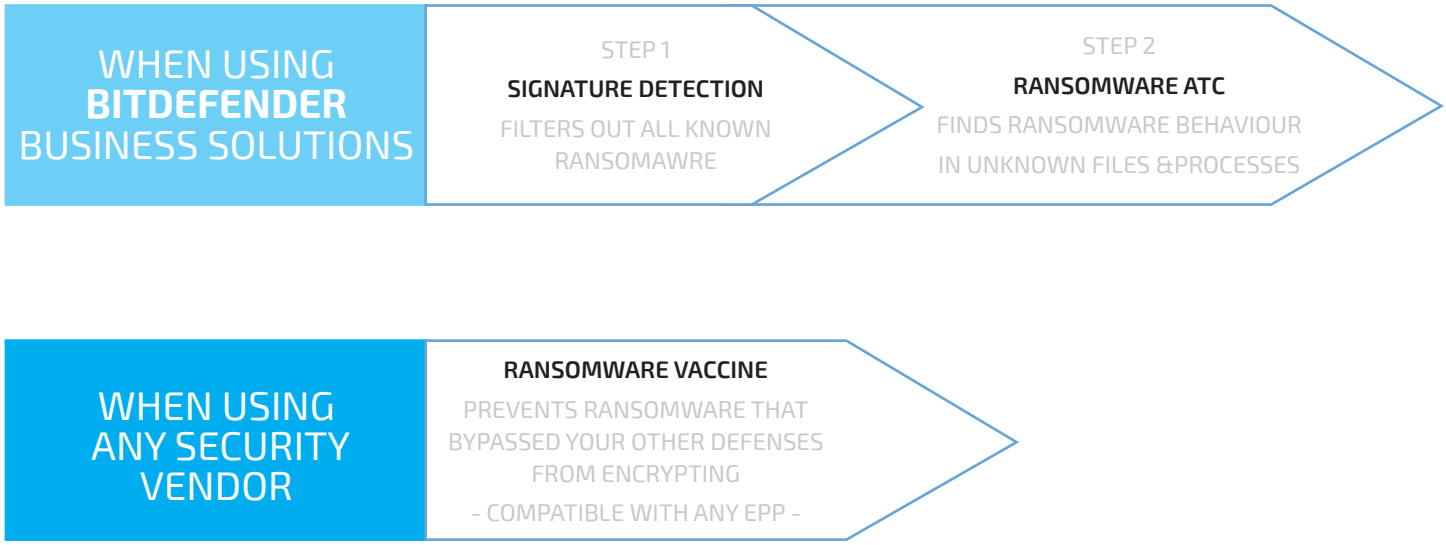
5 http://www.idc.com/prodserv/smartphone-os-market-share.jsp
6 http://techcrunch.com/2015/09/29/android-now-has-1-4bn-30-day-active-devices-globally/

Bitdefender is also closely following the evolution of Mac ransomware. In December 2015, Bitdefender CTO Bogdan Dumitru, announced he was expecting the emergence of the first Mac ransomware sometime in 2016[7]. Three months later, a team of researchers at Palo Alto Network discovered KeRanger, a ransomware infection inside a popular BitTorrent client for Apple's OS X software. This is the first ransomware detected on Mac OS.

HOW DOES BITDEFENDER PROTECT BUSINESSES AGAINST RANSOMWARE?

All Bitdefender business products 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.



7 http://businessinsights.bitdefender.com/predictions-for-2016

SIMILARITY SIGNATURE-BASED DETECTION

BLOCKS MOST RANSOMWARE FOUND TODAY

Integrated in all GravityZone solutions

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. Bitdefender signs droppers instead of files, to counter-act this ability.

BLOCKS RANSOMWARE WITH BEHAVIOUR SIMILAR TO KNOWN RANSOMWARE FAMILIES. Thanks to its similarity technology, Bitdefender 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, 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 Bitdefender will be completely safe from that ransomware.

Similarity Signatures

Bitdefender can also detect samples that are very 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.

RANSOMWARE ATC

UNCOVERS NEVER-BEFORE-SEEN RANSOMWARE

Built on top of Bitdefender's notorious ATC behavioural technology.

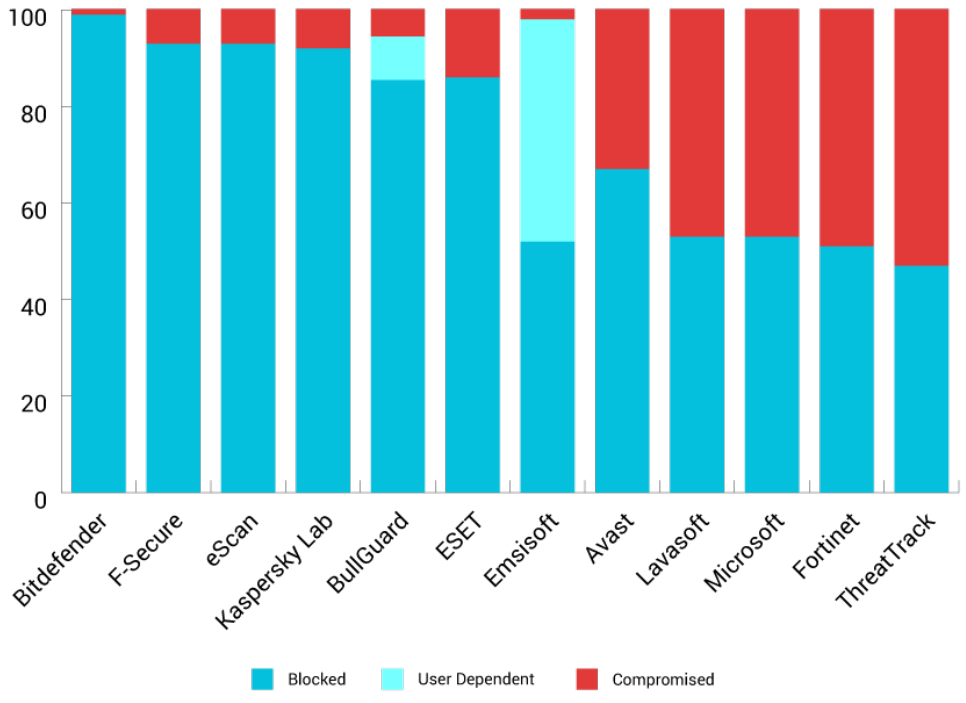
Integrated in all GravityZone solutions

BITDEFENDER – HIGHEST SCORE AGAINST UNKNOWN THREATS

Bitdefender reaches near-perfect score against new threats, while market average continues to drop

The efficiency of Bitdefender Advanced Threat Control 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, 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.



AV-Comparatives, Behavioral/Heuristic Detection Test, 2015

WHY RANSOMWARE ATC?

Since September 2015, Bitdefender has extended its proprietary heuristic technology, called ATC, to also detect previously unknown ransomware. The technology uses advanced behavioral models to find 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.

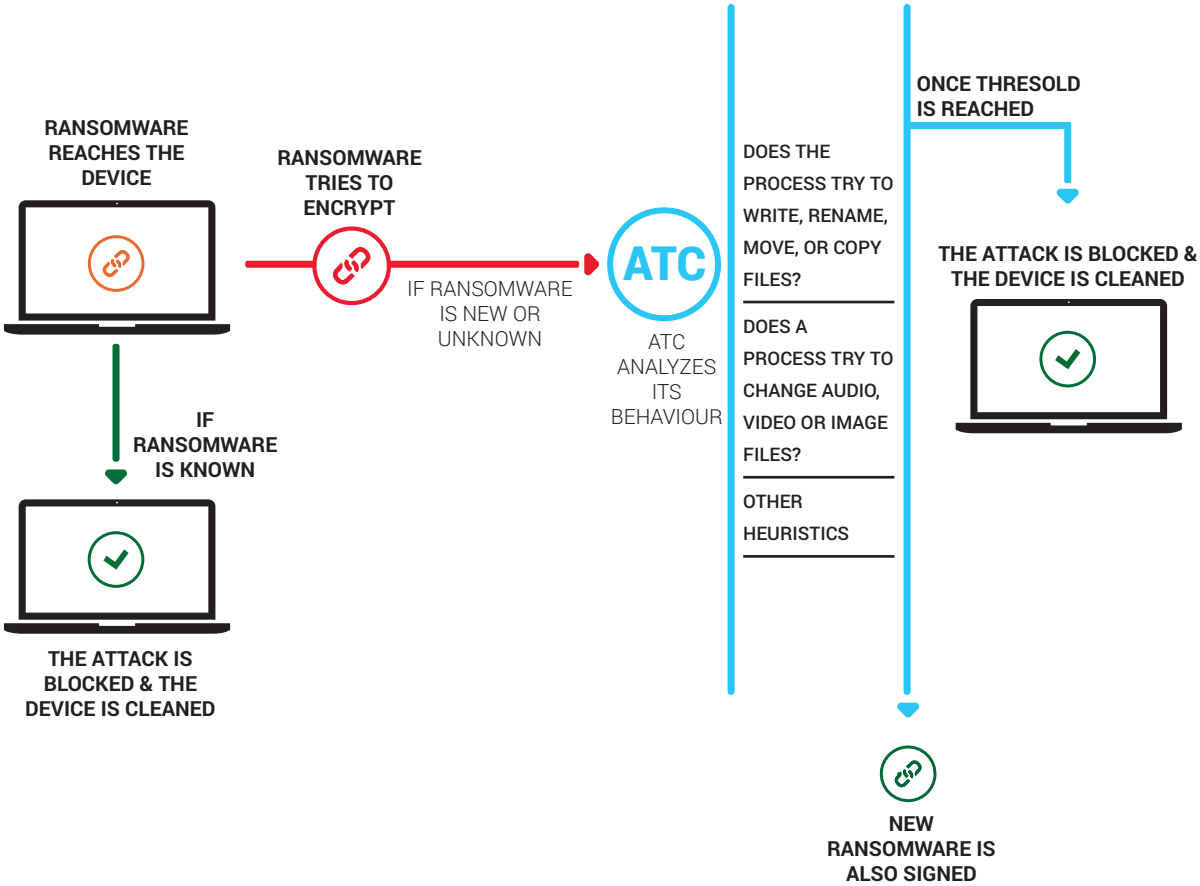
WORKS ON COMPLEX BEHAVIOURAL DETECTION. New variants of ransomware are incredibly easy to make, so signature-based detection cannot keep up. To catch it, a technology needs to track it down by its behavior.

Uses our RENOWNED ATC technology. ATC has proven an incredibly effective technology in uncovering unknown malware. ATC constantly earns 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 Bitdefender 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 files. 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 files. 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 defined by the technology work by themselves.

As ransomware continues to evolve, Bitdefender constantly improves its heuristics, and adds new ones, to constantly stay ahead of ransomware.

ANTI-RANSOMWARE VACCINE

PREVENTS EXISTING RANSOMWARE FROM ENCRYPTING

WHY ANTI-RANSOMWARE VACCINE?

Despite security vendors' efforts, ransomware sometimes manages to slip by the defenses. Bitdefender Anti-Ransomware Vaccine is a last line of defense against ransomware – if your security solution did not detect or block this threat, the vaccine manages to trick it into not encrypting your files. The technology is integrated in Bitdefender business line, and it is also available free of charge to be run together with any other endpoint security solution on the market. For it to work, it needs to be installed before the infection takes place.

PREVENTIVE ANTI-RANSOMWARE DEFENSE. The solution acts as a vaccine that blocks known ransomware patterns from encrypting your system.

WORKS FOR KNOWN AND EVEN SOME UNKNOWN RANSOMWARE. Bitdefender's Anti-Ransomware Vaccine can even halt new ransomware with familiar patterns, which are using unknown droppers.

COMPATIBLE WITH YOUR SECURITY SOLUTION. Bitdefender's Anti-Ransomware Vaccine works with any endpoint protection you might be using, offering a final safety net in case your other security layers fail.

LAST LINE OF DEFENSE. Bitdefender Anti-Ransomware Vaccine is a final layer of protection for ransomware that bypassed all your other security filters.

ZERO ADDITIONAL PERFORMANCE IMPACT. The technology is carefully built to not strain your endpoint performance.

HOW THE SOLUTION WORKS

Bitdefender's Anti-Ransomware Vaccine works by exploiting flaws in the ransomware's method of spreading, and manages to stop it from encrypting, in case the malware already penetrated your device. The solution works in combination with any existing endpoint protection, and acts as a last line of defense against ransomware that manages to slip by the other protection layers, even if the dropper is unknown.

Bitdefender's Anti-Ransomware Vaccine is currently available as a free download from Bitdefender Labs
https://labs.bitdefender.com/2016/03/combination-crypto-ransomware-vaccine-released/

BITDEFENDER
THE TARGETED 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.

- Bitdefender has not one, but three anti-ransomware layers in its business solutions, 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. 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 time period.
- Bitdefender can detect a total of 2.8 million unique ransomware samples from the last 2 years alone.
- We are the first security vendor to release a decryption tool for Linux ransomware victims – free of charge. Bitdefender researchers were able to find cracks in the encryption algorithms used to lock the files of Linux.Encoder encryption.

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 set of tools to thicken that line.

Bitdefender delivers security technology in more than 100 countries through a cutting-edge network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced market-leading technologies for businesses and consumers and is one of the top security providers in virtualization and cloud technologies. Bitdefender has matched its award-winning technologies with sales alliances and partnerships and has strengthened its global market position through strategic alliances with some of the world's leading virtualization and cloud technology providers.

BD-Business-Sep.13.2016-Tk#:
Bitdefender-Business-2015-Whitepaper-AntiRansomware-c279-en_EN