How Bitdefender Hypervisor Introspection

Fought Off WannaCry

All Bitdefender customers are safe
from the WannaCry outbreak

Bitdefender®
Hypervisor Introspection

In an intense 24 hours starting May 12, the WannaCryptor (WannaCry) ransomware family infected over 200.000 computers in more than 100 countries, surprising experts and authorities worldwide and claiming victims including Renault, Telefonica Spain, FedEx and over 40 UK Hospitals.

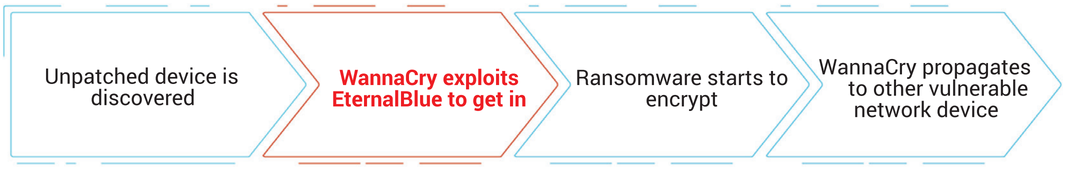
Every infection had two things in common – discovered device with an out-of-date version of Windows and a security solution unable to fend off the attack. Bitdefender customers were protected from WannaCry by a revolutionary new security layer, one developed with the contribution of Citrix, Linux Foundation and Intel.

It is called Hypervisor Introspection, or HVI.

The Godfather of Ransomware

Before looking at the solution, it's important to understand the problem. What made WannaCry so dangerous? Unlike other ransomware waves, WannaCry can spread on the network with no user interaction. It leverages an already known exploit called EternalBlue which gained attackers entry into every unpatched Windows device, and a clear path to blink-of-an-eye proliferation.

Here's how the attack happened, in a nutshell:


Unpatched device is discovered

WannaCry exploits EternalBlue to get in

Ransomware starts to encrypt

WannaCry propagates to other vulnerable network device

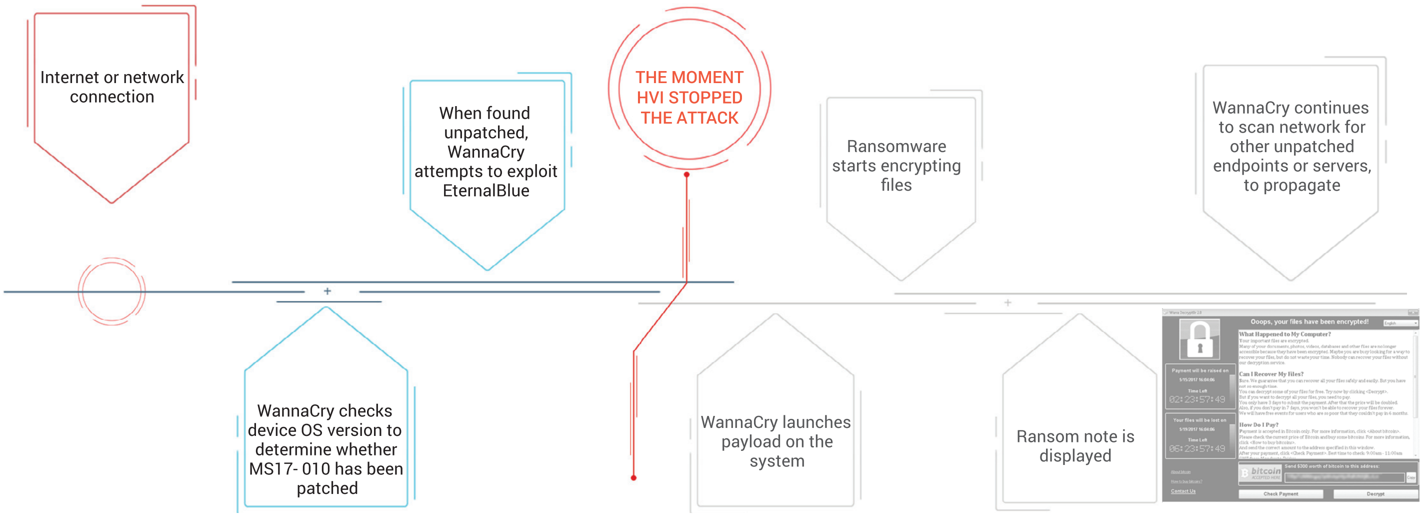
It was enough for the wave to uncover a vulnerable device in a business for it to quickly propagate. Once the first business device was located, WannaCry quickly exploited EternalBlue to deliver the ransomware into the system. Then it started to encrypt the current device, and scanned for new devices to spread to inside the victim' network.

WannaCry is particularly dangerous for businesses because it takes just one infected employee for the attack to quickly spread to the entire network, and sometimes even across countries to other subsidiaries. It also means that attackers could use the vast number of Internet-exposed servers such as webpages, fileshares, and other, to penetrate organizations. The probability to find an unpatched server is higher as admins cannot afford downtime of critical services in order to patch those servers.The final piece that contributed to this massive outbreak is the incredibly wide range of Windows operating systems that shared this vulnerability – everything from Windows 2008 upward.

Bitdefender Hypervisor Introspection Stops WannaCry Infections and Network Propagation

Attacks such as WannaCry can cause temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses incurred to restore systems and files, and devastating effects to an organization's reputation. More targeted attacks can cause even more damage –2016 was a record year, with $4 million in loses estimated per data breach.[1]

Specifically designed to handle attacks, Bitdefender Hypervisor Introspection is a revolutionary new security layer built in collaboration with Citrix that protected its customer infrastructures from the WannaCry wave – **with not a single infection reported**.


Internet or network connection

WannaCry checks device OS version to determine whether MS17- 010 has been patched

When found unpatched, WannaCry attempts to exploit EternalBlue

THE MOMENT HVI STOPPED THE ATTACK

WannaCry launches payload on the system

Ransomware starts encrypting files

Ransom note is displayed

WannaCry continues to scan network for other unpatched endpoints or servers, to propagate

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/15/2017 16:04:06
Time Left
02:23:57:49

Your files will be lost on
5/19/2017 16:04:06
Time Left
06:23:57:49

Send $300 worth of bitcoin to this address:

The figure shows how Bitdefender Hypervisor Introspection stops WannaCry in its early stages, and prevents the next steps of the attack from occurring.

[1] IBM 2016 Cost of Data Breach Study

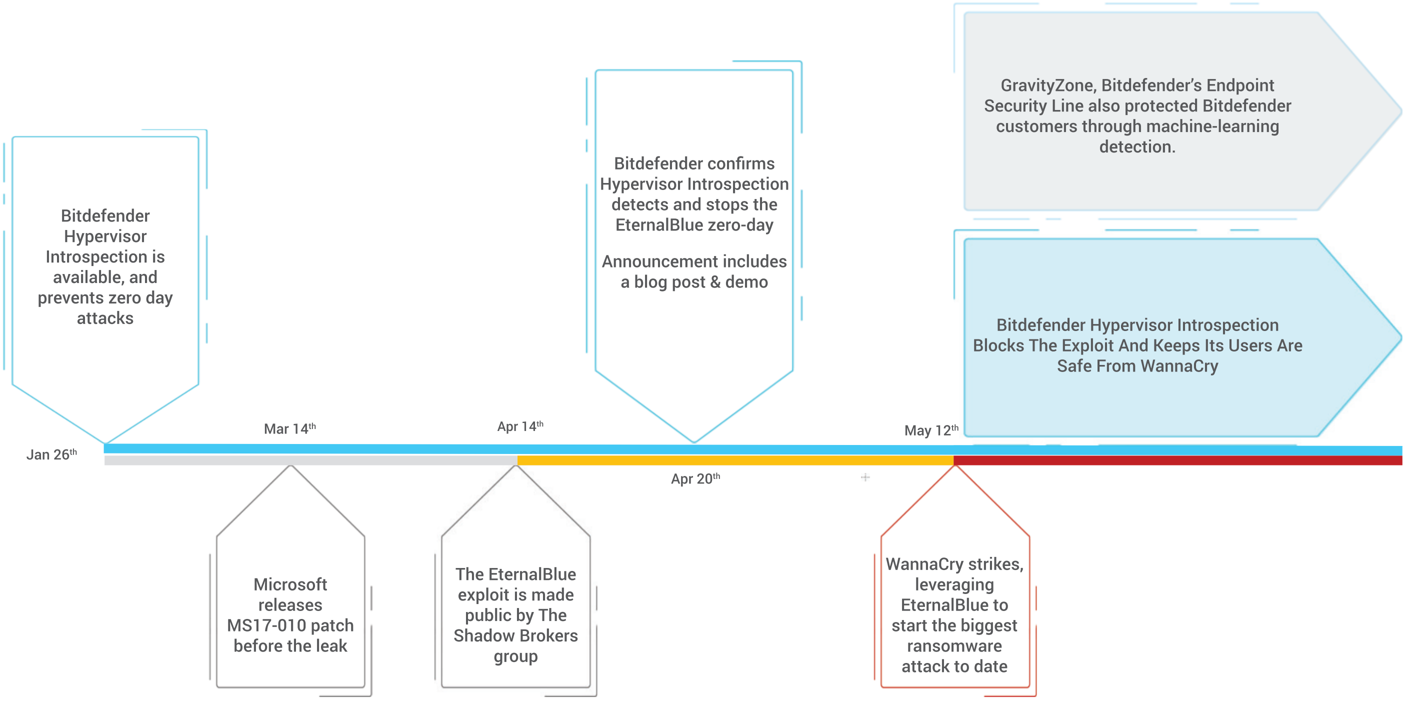
An outside-the-OS solution, Hypervisor introspection has unparalleled visibility into the entire memory stack, where it stopped WannaCry right from the exploit stage. It not only ensured that ransomware didn't start encrypting, but also that **no malicious payload ever made it to the device.**

What's more, by detecting WannaCry's attempt to breach a business and secure the first targeted business workload, Hypervisor Introspection stopped propagation of the attack on the network, ensuring no other workloads of that customer faced any danger.

Protecting Against WannaCry Long Before the Outbreak

WannaCry is just one example of what can happen when a widespread vulnerability meets a cunning exploit kit and a damaging ransomware payload.

The EternalBlue exploit that WannaCry used to spread so quickly had made headlines weeks earlier, when it was discovered by The Shadow Breakers group. Soon after, Bitdefender published a blog post showcasing how Bitdefender Hypervisor Introspection detected and blocked EternalBlue long before anyone foreseeing that an attack such as WannaCry will occur.[2]



Bitdefender Hypervisor Introspection is available, and prevents zero day attacks

Microsoft releases MS17-010 patch before the leak

The EternalBlue exploit is made public by The Shadow Brokers group

Bitdefender confirms Hypervisor Introspection detects and stops the EternalBlue zero-day

Announcement includes a blog post & demo

WannaCry strikes, leveraging EternalBlue to start the biggest ransomware attack to date

Bitdefender Hypervisor Introspection Blocks The Exploit And Keeps Its Users Are Safe From WannaCry

GravityZone, Bitdefender's Endpoint Security Line also protected Bitdefender customers through machine-learning detection.

A figure of how Bitdefender Hypervisor Introspection managed to tackle the attack early on

Hypervisor Introspection is designed to handle advanced exploits such as EternalBlue and even zero-days (exploits that are yet unknown, much harder to detect, and usually used in targeted attacks). At the hypervisor level, it scans raw memory lines – a feat previously deemed impossible, but with an amazing payoff. While kernel-based threats or zero-days can hide from or trick endpoint security tools, they inevitably leave malicious memory traces at the raw memory level, which Hypervisor Introspection picks up clearly.

This means Bitdefender Hypervisor Introspection could prevent the exploitation of the widespread MS17-010 vulnerability **long before it was disclosed and patched by Microsoft.**

[2] businessinsights.bitdefender.com, 'Hypervisor Introspection defeated Eternalblue a priori', Apr 20, 2017

Bitdefender Hypervisor Introspection is the first security solution of its kind, and was achieved through a unique collaboration with Citrix. It taps into XenServer's unique Direct Inspect API to gain insight into the machines it protects, while inserting no agents in them. This makes Hypervisor Introspection immune to attacks, and risks no compromise from kernel-level threats. A truly agentless security layer, it will even protect your other security layers, such as endpoint security, from being compromised by attackers. Bitdefender Hypervisor Introspection works on top of existing security layers and is compatible with every other security vendor.

Bitdefender customers not using Hypervisor Introspection were also protected against the outbreak

Its GravityZone Endpoint Security Solutions prevented the execution of all ransomware variants, by leveraging their machine learning models that are designed specifically to catch never before seen ransomware attacks at pre-execution stage. For this attack wave specifically, a machine learning model at the endpoint, developed by Bitdefender labs in 2013 is able to detect and block all ransomware variants used by WannaCry.

Bitdefender next-generation machine-learning and memory introspection technologies ensure that Enterprises worldwide have always been safe from the WannaCry ransomware mega-attack and the underlying EternalBlue zero-day exploit - AND will be similarly protected from the next such attack.

To learn more about Bitdefender Hypervisor Introspection, visit www.bitdefender.com/hvi

To learn more about Bitdefender's entire business security Line, visit www.bitdefender.com/business

BD-Business-May.19.2017-Tk#CREA-1370
Bitdefender-Business-2017-Whitepaper-WannaCry-c1370-en_EN