armis

BlueBorne™

PROTECTING THE ENTERPRISE FROM BLUEBORNE

OVERVIEW

The newly discovered BlueBorne attack vector presents a new set of challenges for enterprises and their security teams. BlueBorne cuts across a variety of operating systems that support Bluetooth including Windows, Android, Linux, and iOS. It enables an attacker to install and run malicious code on the affected device without any interaction from the user. It also enables an attacker to intercept, steal, or modify traffic with a Bluetooth pineapple. Attackers can serially repeat this process to spread through an enterprise, invisibly crossing network segments and airgaps at will. Given that BlueBorne applies to unmanaged devices and IoT devices, there will almost certainly be many devices in an enterprise that will be difficult or impossible to patch.

Even though the challenges are significant, enterprises are not defenseless. While traditional security controls may be blind to BlueBorne and similar attacks, Armis introduces a new layer of security that enables enterprises to continuously monitor and automatically protect unmanaged and IoT devices from threats and risk. In this paper, we will delve into how the platform can be applied to the specific challenges of BlueBorne.

THE UNIQUE CHALLENGES OF BLUEBORNE

Before we address the solution, it is important to know what BlueBorne is and what specifically makes it so insidious and hard to control. Some of the challenges are related to the overall landscape of Bluetooth-enabled devices, while others are tied to the technical minutia of the Bluetooth specification itself. However, the most important issue for enterprises, is that BlueBorne introduces an attack vector that exposes a fundamental and unguarded flank in security architectures. An understanding of how these factors come together is essential for understanding the scope and impact of BlueBorne.

Bluetooth: A Sprawling Attack Surface

It is likely not a surprise that there are a great many devices that are Bluetooth enabled - upwards of 8.2 Billion devices[1]. This includes a wide variety of user devices found in the enterprise such as laptops, smartphones, and peripheral devices such as keyboards and headsets. However, Bluetooth is standard in other office devices such as conference phones, TV monitors, speakers. Bluetooth is also often included in IoT devices by default as an always-on, "just connect and it works" option for initial setup and ongoing configuration. This means that everything from thermostats to printers can come with a readily available Bluetooth connection. Whether controlled by end-users or simply installed in the environment itself, enterprises are inundated with Bluetooth devices.

However, the sprawl of devices is just the beginning of the Bluetooth attack surface. The Bluetooth specification itself is massive and complex relative to other protocols. Just as a reference, the Bluetooth specification is over 5 times the size of the Wi-Fi spec. There are several reasons that contribute to the size, but one of the most important is that in many ways Bluetooth recreates its own version of the TCP/IP stack. As a result, the Bluetooth stack is fairly large and complex. And generally speaking, large and complex is a breeding ground for vulnerabilities.

Until recently, Bluetooth had gotten little attention from research community. But with the advent of readily available Bluetooth sniffers, Bluetooth traffic and devices suddenly became much more accessible to attackers, and likewise became a much more interesting area of research. While the initial Armis research into BlueBorne has surfaced vulnerabilities across a variety of operating systems, these are almost certainly the tip of the iceberg.

A BlueBorne Primer

BlueBorne is best described as an attack vector. This vector applies to a variety of operating systems that support Bluetooth including Microsoft Windows, Linux, Google's Android, and Apple's iOS. Since these operating systems each implement Bluetooth slightly differently, the specific vulnerabilities are unique to each operating system. As of the time of writing, Armis researchers have found vulnerabilities that enable Man-in-the-Middle (MITM) techniques against Windows and Android operating systems, and full remote code execution (RCE) against Android, Linux, and iOS. Man-in-the-Middle attacks would allow an attacker to easily intercept and redirect victim traffic, making it easy to steal user credentials and data. Remote code execution, of course, would allow an attacker to do most anything including installing malware or ransomware, infecting additional devices, and routing traffic through the victim device.

Most importantly, these attacks can be launched without any user interaction on the part of the victim user and without the device being put into "discoverable" mode. Unlike typical attacks that would require a user to click a malicious link or open a file, BlueBorne attacks are largely transparent to the user.

Problems with Patching

Of course, patching vulnerable systems is often the first step when responding to a newly discovered threat. However, things are very unlikely to be so easy in terms of BlueBorne. While the various OS vendors have or will provide patches, the nature of unmanaged and IoT devices that support Bluetooth will make them extremely difficult to patch, and outright impossible in some cases.

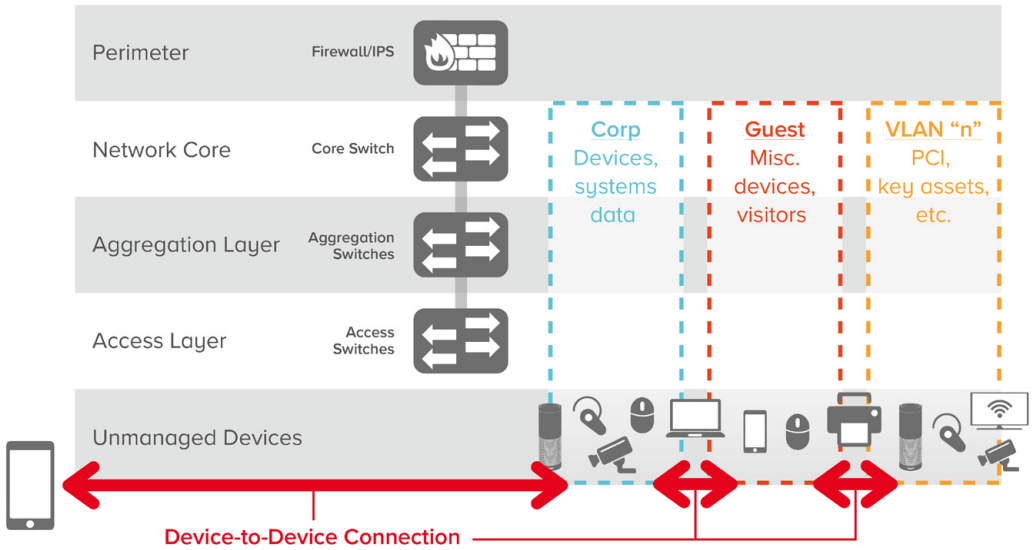
While Windows laptops may be easily updated automatically, other devices are considerably more challenging. Operating system upgrades for smart phones are largely under the control of each phone vendor, but may be delayed, and some older devices may not receive patches. Likewise, users may put off any update simply for matters of convenience. This touches on one of the fundamental issues of unmanaged devices – in many cases the enterprise does not own and is not in control of the device.

Next, many IoT devices rarely receive updates at all. Many of these devices will run one of the virtually innumerable Linux distributions, and in most cases, the operating systems of these devices are never updated. Even in cases where updates are delivered, they often take months for a fix to be delivered, and there is often not an automated way for applying the update. This means that in all likelihood, some devices will be functionally unpatchable and vulnerable devices will persist within the enterprise for months if not years.

Cutting Across Boundaries

We need to consider the impact of BlueBorne to traditional security controls. Access controls such as NAC will likely provide little help since BlueBorne provides a way of compromising valid devices that are allowed to be on the network. Even IoT devices that lack the ability to install a certificate are typically whitelisted. Traditional IPS and firewalls will be bypassed because the attack spreads directly from host to host over Bluetooth. Endpoint controls will naturally not apply to any unmanaged or IoT devices.

Most significantly, BlueBorne provides a method of spreading that cuts across virtually any network segmentation strategy including airgaps. The ability to serially infect and spread directly from device to device allows an attacker to move across VLANs and network segments virtually at will. An initial infection could come from something as little as a delivery man with an infected phone walking in the building. The infection could spread from device to device to create a mesh of compromised hosts and pathways into and out of the network. In its darkest form, BlueBorne can represent an unpatchable threat that can infect and spread without user interaction, and without regard for segmentation or traditional security control.



CONTINUOUS PROTECTION

The BlueBorne attack vector highlights the need for a new layer of security. Many devices are the same devices that will be the most difficult to patch will also lack the ability to run a traditional security agent, putting them beyond the reach of endpoint security controls. Additionally, the ability for the threat to spread directly from device to device means that a threat would be beyond the view of network security controls such as firewalls, IDS/IPS, or malware sandboxes. Likewise, affected devices could likely already be allowed or whitelisted by NAC solutions. In order realistically address this style of threat, organizations will need the ability to bring automated visibility, threat detection, and response capabilities directly the areas where Bluetooth-enabled devices operate. Armis provides this critical layer of defense for unmanaged and IoT devices, and protects the enterprise in the following key areas.

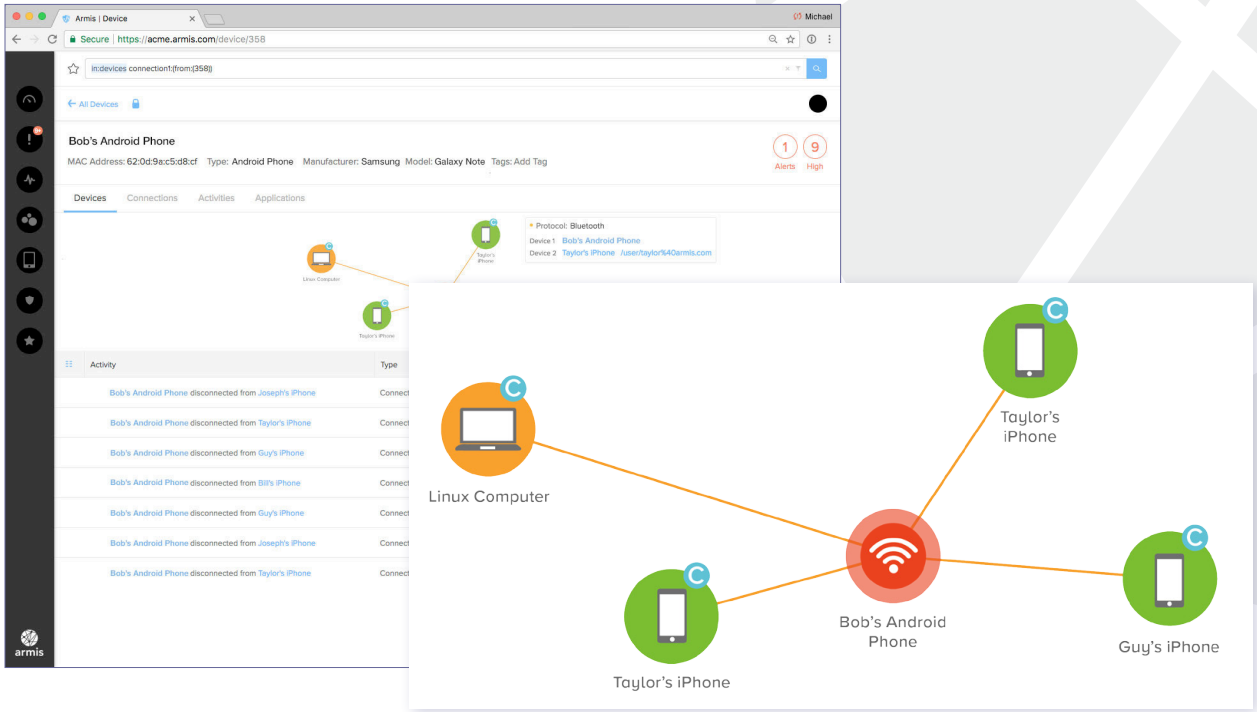
Visibility into the Unmanaged Attack Surface

Most organizations have very little visibility into the behavior of their unmanaged devices. This especially true of how those devices behave in the wireless environment. On the wired side of the network, devices may be limited to access only certain network segments or resources, but visibility into Bluetooth behavior is virtually non-existent. Armis provides a visibility into this layer so that organizations can easily see and monitor all of their devices even without the use of an endpoint agent. Armis lets you discover devices on and off the corporate network.

Armis can deliver this visibility in a few ways depending on the needs and architecture of the environment being protected. First, the Armis solution integrates with the existing wireless infrastructure to collect both WiFi as well as Bluetooth information from the environment. In the vast majority of cases, this allows organizations to gain visibility by leveraging the existing wireless infrastructure and hardware that is already deployed.

With this visibility established, Armis can provide a detailed, live inventory of all devices in the environment. This profile includes traditional devices such as end-user laptops and smart or VOIP phones as well as unmanaged devices and IoT devices. Likewise, staff can see WiFi as well as Bluetooth activity for any and all devices.

Next, the solution provides insight into the type of device that is seen, including its operating system, reputation, version, and more. Given that different operating systems are impacted by BlueBorne differently, staff can use this detailed inventory of devices to quickly understand where they have exposure, and how to correct it.



From Many Network Adapters to One Device

Modern devices often have enormous flexibility in terms of network connectivity, with many devices having network interfaces for WiFi, Bluetooth, and wired traffic. In addition to documenting the environment, Armis is able to see how Bluetooth, WiFi and wired traffic is connected to a single device. This understanding is essential for understanding how a potentially compromised device could impact the network, and ultimately how security teams will need to approach containment.

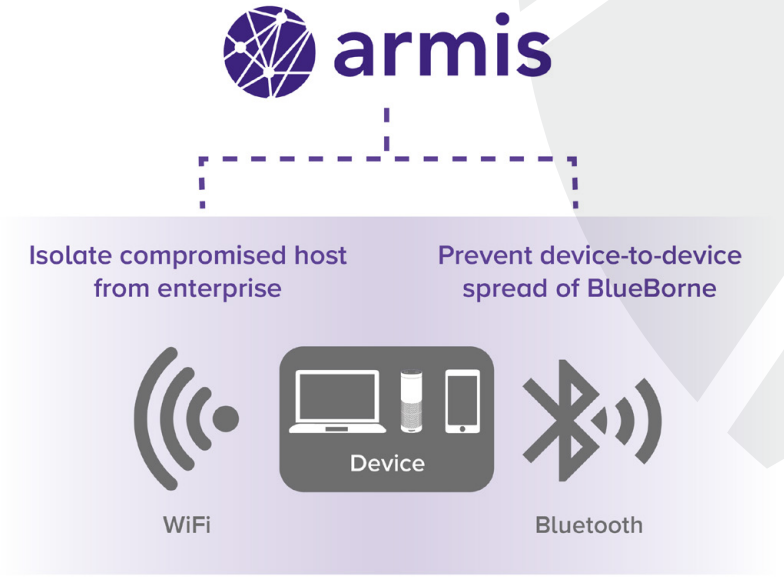
For instance, it is very common for devices to have both WiFi and Bluetooth adapters. Armis can not only automatically see these adapters, but recognize that they are part of the same physical device. While some devices may operate completely wirelessly, others may have a wired connection to the enterprise network as well. Armis also provides the option to integrate with wired network infrastructure such as firewalls, TAP/SPAN infrastructure, and authentication infrastructure to provide a unified view of devices wired and wireless behavior on the network.

This unified view brings the impact of a device into context. While a device may be compromised over the air by BlueBorne, the attacker may use the victim's WiFi or wired connection to spread internally or to access internal assets and applications. On the other hand, a device compromised via BlueBorne could logically be expected to attempt to infect other devices over Bluetooth. This is precisely the behavior that could allow an attacker to use Bluetooth to successively bounce from device to device in order to cross network segments, VLANs, or air gaps. Armis can easily see this behavior, tracking, and revealing the history of a device' s Bluetooth connections, allowing staff to closely monitor those devices for any unusual behavior.

Automated Baselining and Behavior Monitoring

With visibility established and a unified view of each device, Armis next looks for signs of malicious or aberrant behavior. The solution continuously monitors each device to learn its unique behaviors and patterns. This can be incredibly powerful especially for IoT. Unlike end-users, whose behavior can vary from day to day, the behavior of IoT devices tend to be much more predictable. These devices often connect to the same devices over and over, and likewise perform the same tasks repeatedly. This predict-ability makes it easy to see when something is amiss. Armis continually analyzes each device's connections to other devices, and the amount and type of traffic that passes between them.

The solution then can identify any unusual behavior as well as identify the signs of any malicious behaviors. For example, Armis can identify a host that is attempting to scan the environment for new victims or move laterally within the environment. Likewise, staff can quickly spot command-and-control (C&C) from a compromised device to an external server or domain. In other cases, a device may be used as a relay to provide persistence within the network or to siphon data out of the network. This capability is particularly important for mitigating the impact of BlueBorne. BlueBorne's ability to quietly infect devices and jump across segments or airgaps, make it an ideal tool for a cyberattack. Armis automatically identifies these behaviors, and easily shows the progression of an attack and the relationship between all devices impacted by the threat.



Taking Action

Ultimately, security teams are tasked with protecting the enterprise and its assets and information – and this means enforcement. Armis approaches this task in multiple ways. First, the solution enables staff to set and enforce policies in terms of the behaviors that should be allowed for a particular type of device or connection. As covered previously, the Bluetooth protocol is designed to "just work" and often defaults to easy, frictionless connectivity. This means that a Bluetooth-enabled device can potentially connect to a great many other devices, and do any number of things. Yet in reality, those devices should only be allowed to do a very limited number of things in the enterprise. Armis, lets staff create policies to regulate and enforce precisely the connections that should be allowed including what types of traffic and behaviors are sanctioned for that device.

When a threat is detected, Armis can take action to isolate the affected device. For example, a compromised device can be knocked off the wireless network and prevented from making WiFi connections to other devices in the environment to prevent lateral movement or exfiltration of data to an attacker. Likewise, if command-and-control traffic is detected, Armis can trigger the firewall to block the traffic at the network perimeter. This approach allows staff to proactively reduce their attack surface, while instantly responding appropriately to a detected threat.

BEYOND BLUEBORNE

This paper has outlined some of the common ways that Armis can protect organizations from BlueBorne. However, this is merely an introduction and doesn't cover all of the relevant features and capabilities of the Armis solution. Instead, this paper is simply meant to outline the nature of threat and how organizations can adapt their security practice in response.

It is also important to remember that BlueBorne is not simply a finite set of vulnerabilities, but rather an attack vector this is likely to evolve over time. These initial discoveries by Armis researchers impacted all major operating systems, and additional issues will almost certainly be found. The advent of Bluetooth sniffers and attack tools makes Bluetooth not just a theoretical target, but a practical one for attackers as well. We expect this to be a very active area of cybersecurity over the coming months and years and we look forward to sharing new research and defensive capabilities as we evolve over time.

Sources

[1] https://www.bluetooth.com/what-is-bluetooth-technology/where-to-find-it

armis

1.888.452.4011
armis.com