EBOOK

Gartner
COOL
VENDOR
2020

Raspberry Pi – A Friend or Foe?
Cyber Physical Security Challenges

RASPBERRY PI & TODAY'S WORLD

The Raspberry Pi is a small (credit card-like size), inexpensive, portable computer that connects to real-world objects. It contains all the basics of any computer including a processor, memory and graphics processor. As such, it is capable of doing everything one would expect a regular computer to do such as browse the internet, play high definition videos, create spreadsheets, word processing and more. With its computer-functioning capabilities, the Raspberry Pi was intended to be used for ethical purposes, which it is still used for. It can, however – through a payload – be instructed to carry out malicious, clandestine activity, thus making it a Rogue Device.

With the world currently focusing on health risks, cybersecurity is taking a backseat in almost every industry; public and private. The global economy has been severely impacted by COVID-19, causing businesses to suffer; a cyberattack will only exacerbate the situation. As such, it is imperative – now, more than ever – to address the security risks associated with the Raspberry Pi, whether the intentions of its usage are moral or not, since this device has the ability to carry out perilous cyberattacks. Mitigating an attack is wiser than dealing with the consequences of one.

SECURITY CHALLENGES OF RASPBERRY PI

1 | PoisonTap

PoisonTap is built for Raspberry Pi and produces a cascading effect by exploiting the existing trust in various mechanisms of a machine and network to produce a snowball effect of information exfiltration, network access and installation of semi-permanent backdoors. The risks of PoisonTap are explored below:

A. Emulate an Ethernet device over USB.

This results in the computer thinking that it is dealing with local LAN traffic, which is automatically prioritised over internet traffic. This allows the attacker to hijack all internet traffic to and from the machine, despite being a low priority, by giving it an IP address.

B. Siphons and stores HTTP cookies.

Cookies and sessions from the web browser are siphoned and stored, which often contain login details of the person who uses the browser. Every iframe HTTP request to a site that is made, the HTTP cookies are sent from the browser to the "public IP" – hijacked by PoisonTap – which swiftly logs the cookies/ authentication information.

C. Installs web-based backdoors.

PoisonTap allows a malicious actor to install a persistent web-based backdoor in HTTP cache for hundreds of domains and common JavaScript CDN URLs, all with access to the user's cookies via cache poisoning. As a result, attackers can, at any point, connect back to the backdoored machines and perform requests across any origin that has the backdoor implemented.

D. Exposes the system's internal router.

The internal router can be exposed since PoisonTap makes it accessible remotely via outbound WebSocket and DNS rebinding. The internal router often provides greater security for systems on the network and an attack puts that security at risk, especially since it can lead to other attacks on the router which the perpetrators may have never to do prior, such as authentication vulnerabilities.

2 | P4wnP1

P4wnP1 is a highly customizable USB attack platform for the Raspberry Pi Zero or Raspberry Pi Zero W that allows one to connect the device into a host computer – as a HID or network interface – and carry out various actions, which will be expanded on below.

A. Mouse/Keyboard emulation.

With output capabilities, the device can act as a mouse or keyboard and trigger payloads that can cause a range of attacks including a data breach, malware installation and cookie harvesting. Since P4wnP1 allows the Raspberry Pi to emulate a mouse or a keyboard, security software will recognize it has a genuine HID, thus raising no alarms.

B. HID covert channel – backdoor.

Attackers can obtain remote shell access through a reverse shell to bridge an air-gapped target. From this, the perpetrator can upload and run PowerShell scripts which will allow the attacker to remotely manage computers from the command line or access data stores. As such, firewalls will not protect the target from an attack.

C. HID cover channel – frontdoor.

Bad actors can gain access to a custom shell on P4wnP1 from a restricted Windows host, tunnelled through a raw HID device with low footprint. Again, this can be used to upload and run PowerShell scripts directly into memory of the PowerShell process running on the target.

D. Cookie harvesting.

P4wnP1 can allow for cookie harvesting which might provide attackers with sensitive, personal information, thus resulting in a data breach. Depending on whose information is obtained, it can be useful in carrying out further attacks. Moreover, the Pi can store the information using a PowerShell script.

E. Man-in-the-middle (MiTM) attack.

When connecting the Raspberry Pi device to a router, P4wnP1 can convince it to route all internet-bound traffic through the Raspberry Pi by altering its MAC address. With precisely placed packets, the perpetrator can sniff the private traffic between two hosts, potentially allowing information to be unlawfully accessed by manipulating the communication between the two parties.

F. WiFi hotspot.

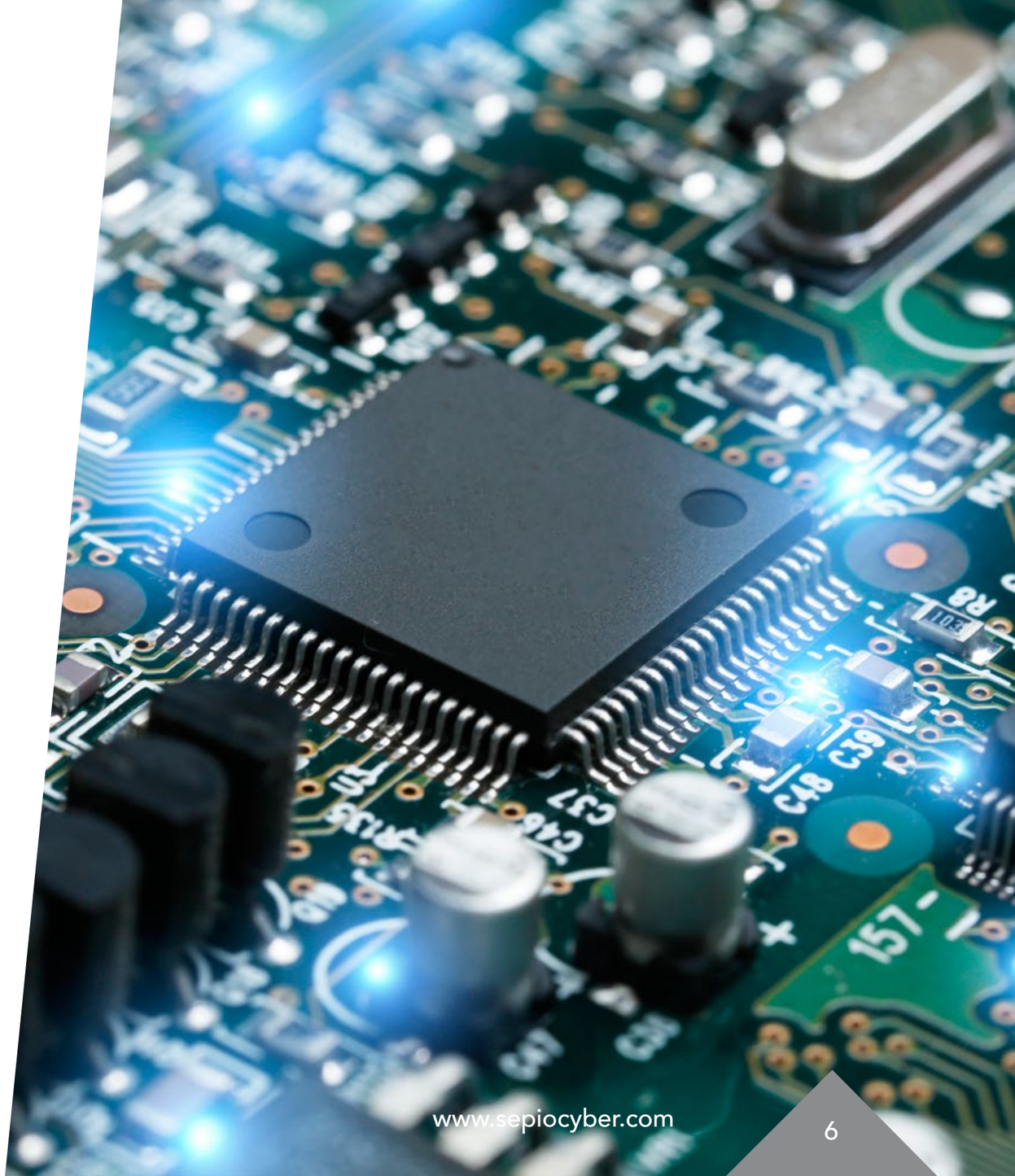
The Raspberry Pi Zero W has a built-in WiFi unit which allows it to start a Bluetooth hotspot. This can provide benefits in that the device can operate as a small, portable WiFi source. However, it provides SSH access, which allows an attacker to control various servers remotely.

This threat is especially prevalent to today's current situation whereby many organizations have resorted to Work From Home policies, which can mean employees are using public WiFi hotspots, not knowing who configured it, or who else is using it.

3 | Bypassing NAC

NAC software supports network visibility and access management through policy enforcement on devices and users of corporate networks. To bypass, an attacker must access a device that has already been authenticated. In other words, a genuine device must be spoofed, which can be done with a Raspberry Pi.

The authenticated device is used to log into the network which then smuggles network packets from the Raspberry Pi by overwriting the MAC address, making it seem as if the packets are originating from the genuine, authenticated device. From here, the attacker has access to the organization's network and can, consequently, move laterally through it. This can allow for a variety of potential attacks such as a data breach, malware installation or Advanced Persistent Threat (APT) attack.



4 | Advanced Persistent Threat (APT) attack

An APT, which can be carried out with a Raspberry Pi, is one of the greatest threats to an organization due to the sophisticated, specific nature of the attack. The clandestine essence of APT thus means that the targets are frequently government agencies or critical infrastructure providers since an attack on these sectors can often cause a risk to national security. With this type of motivation, APTs are usually affiliated with nation state or state-sponsored actors, in addition to the fact that these attacks need strong capabilities to be carried out.

APTs allow the attacker to go deep into the target's network and do so unnoticed for long periods of time using advanced hacking methods. State secrets, confidential data and government officials' personal information can be acquired through an APT attack for the purposes of sabotage or even terrorism.

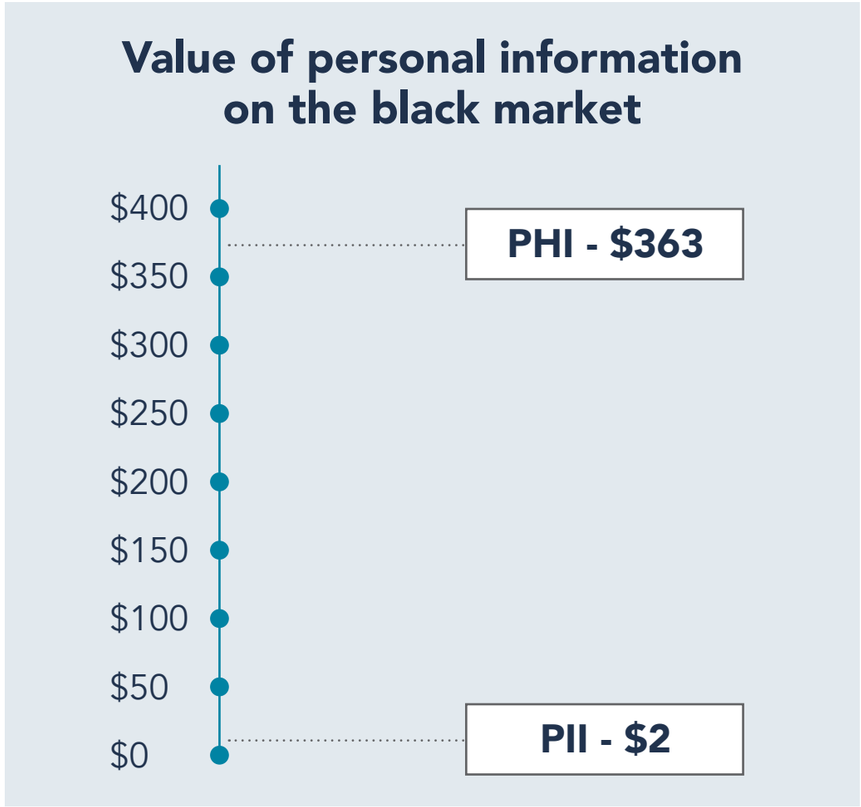
Cyberwarfare is growing in prevalence due to nations' economies, infrastructure, trade, business, communication, transport and more increasingly relying on IT and IT-enabled services. An attack on any sector can cause serious damages, not only to the direct target. Cyberwarfare is also cheaper and more immediate than traditional warfare, with less risk to human life – especially on the attacker's side – and can allow smaller, weaker states to impose substantial damage on a strong adversary that would otherwise not be possible. By harming a strong adversary, smaller states have the potential to become powers in asymmetric warfare.

As a result, APTs are an appealing attack method for those with sabotage as a motive.

5 | Ventilators

Due to its computer-like capabilities, the Raspberry Pi device can control a medical ventilator by setting the air pressure, opening and closing valves and regulating whether a patient needs full or partial breathing assistance. Since a ventilator has relatively low demands, the Raspberry Pi Zero is the ideal device to power it, especially since it is inexpensive and portable. Additionally, the company producing Raspberry Pi builds to stock, rather than to order, meaning that the products are constantly on hand, which is essential during a pandemic.

However, having computer-controlled ventilators means that there are more entry points for an attacker to target the healthcare industry, which is already the most frequently targeted industry. The data held by healthcare facilities is known as Personal Health Information (PHI) and sells for 100x more than Personally Identifiable Information (PII) on the black market. Moreover, the healthcare industry is widely known to forgo cybersecurity in order to provide more efficient services to patients. Due to the often-critical nature of the industry, security features are viewed as a hindrance, rather than an aid.



6 | Characteristics

One of the greatest risks of a Raspberry Pi device is its clandestine nature. Physically, the size of the device is small enough to be imbedded inside peripherals or placed on the network and therefore it goes unnoticed to the human eye.

Furthermore, the device, when used as a USB attack tool, is recognized by security software solutions as a legitimate HID device, thereby raising no alarms. When acting as a network implant, the device sits on the Physical Layer – Layer 1 – which these security software solutions do not cover, hence the device goes completely undetected and, again, no security concerns are raised.

This is, arguably, the greatest risk.

> **“The device, when used as a USB attack tool, is recognized by security software solutions as a legitimate HID device, thereby raising no alarms”**

HAC-1 SOLUTION

Many times, enterprises' IT and security teams struggle in providing complete and accurate visibility into their hardware assets, especially in today's extremely challenging IT/OT/IoT environment. This is due to the fact that often, there is a lack of visibility, which leads to a weakened policy enforcement of hardware access. This may result in security accidents, such as ransomware attacks, data leakage, etc.

In order to address this challenge, ultimate visibility into your Hardware assets is required, regardless of their characteristics and the interface used for connection as attackers. Moreover, it is important to be practical and adjust to the dynamic Cyber security defenses put in place to block them, as well as take advantage of the "blind" spots – mainly through USB Human Interface Device (HID) emulating devices or Physical layer network implants.

In addition to the deep visibility layer, a comprehensive policy enforcement mechanism recommends on best practice policy and allows the administrator to define a strict, or more granular, set of rules for the system to enforce.

Sepio Systems is the leader in the Rogue Device Mitigation (RDM) market and is disrupting the cybersecurity industry by uncovering hidden hardware attacks operating over network and USB interfaces. SepioPrime, which orchestrates Sepio's solution, identifies, detects and handles all peripherals; no device goes unmanaged.

The only company in the world to undertake Physical Layer fingerprinting, Sepio Systems calculates a digital fingerprint using the device descriptors of all connected peripherals and compares them against a known set of malicious devices, automatically blocking any attacks. With Machine Learning, the software analyses device behavior to identify abnormalities, such as a mouse acting as a keyboard.

HAC-1 - VISIBILITY & SECURITY OF HARDWARE ASSETS

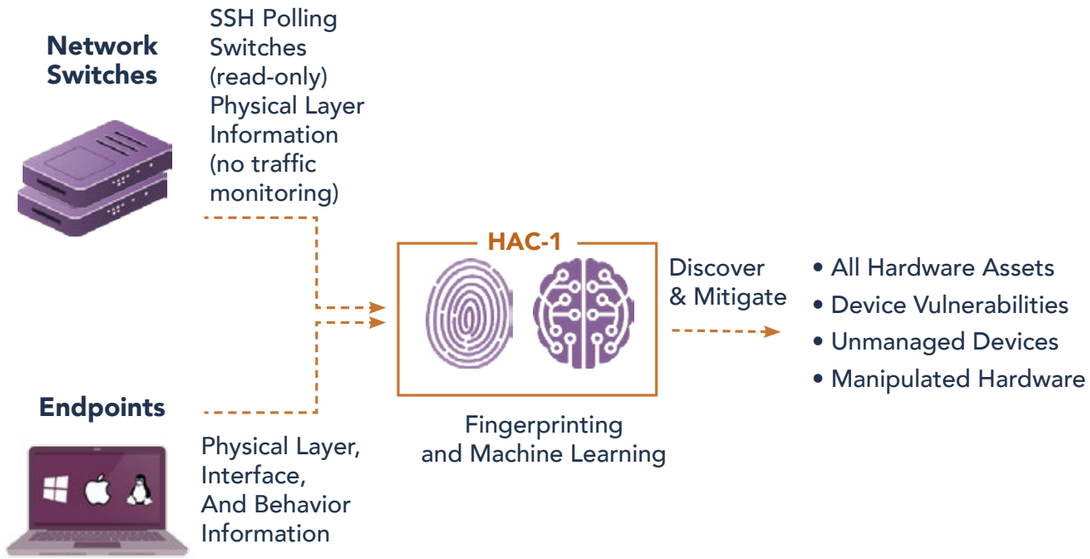
Main Benefits:

Complete Visibility of all Hardware Assets: With all devices and anomalies detected, enterprises benefit from a greater overall cybersecurity posture. Gaining full visibility of all hardware devices from endpoint peripherals to connected devices (IT/OT/IoT), Sepio uses unique physical layer hardware fingerprinting technology and data augmentation from endpoints and networks.

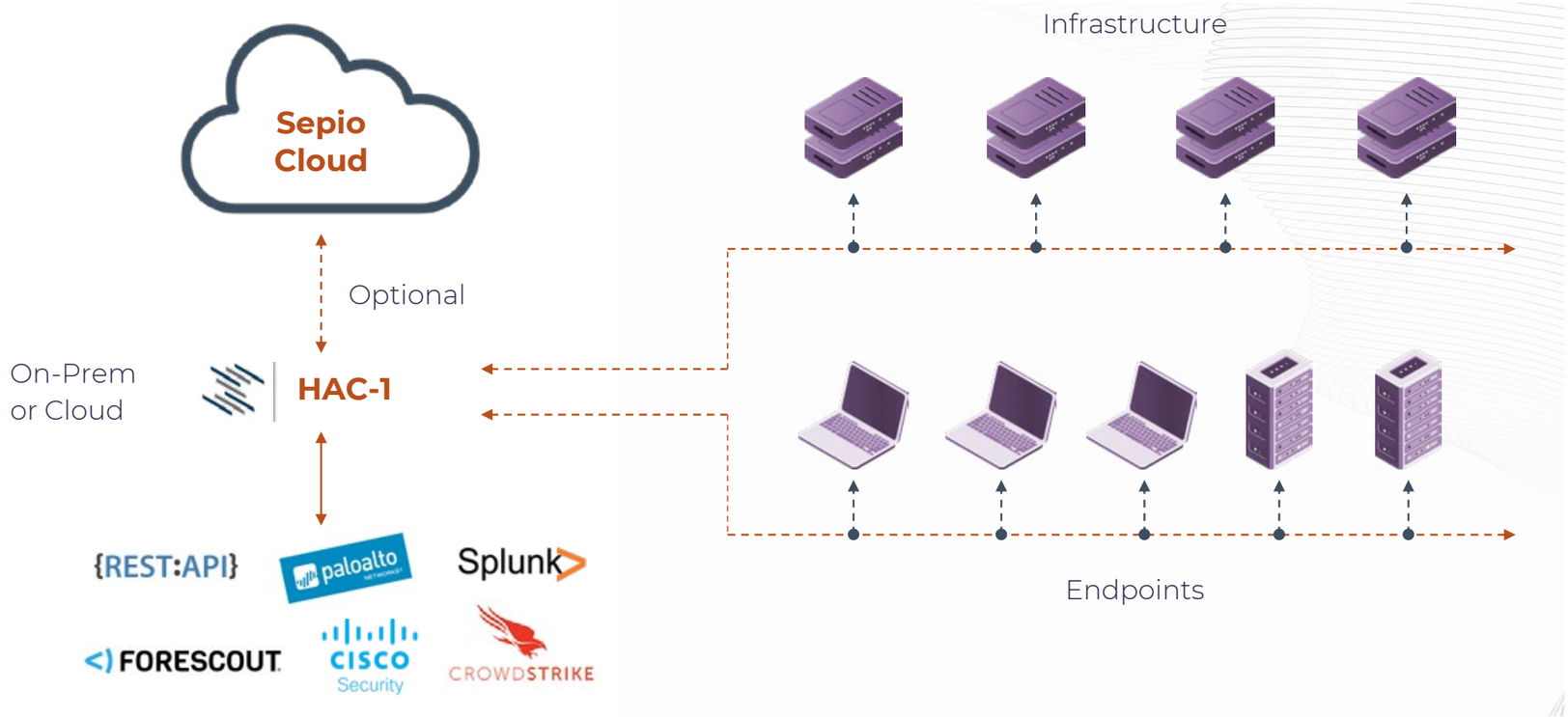
Full Control through Predefined Policies: Enterprise-wide policies enable compliance, regulation and best practices. With predefined templates and no baselining or whitelisting, and no requirement for a clean environment start, Sepio provides a fast and easy setup.

Rogue Device Mitigation (RDM): Threat mitigation upon discovery of rogue or threatening devices. Integrations with existing security platforms such as NACs and SOARs for mitigation and remediation enhancements.

How It Works



System Architecture



SUMMARY

Despite the Raspberry Pi offering advantageous uses, the risks associated with the device are too precarious to ignore. Additionally, the unethical use of these devices is increasing due to its low price, ease of use, and various capabilities. Additionally, these factors mean that no industry, sector or organization is free from the threat of a Raspberry Pi-enabled attack. Moreover, organizations do not have sufficient detection capabilities and, currently, can only reduce the damage of an attack once it has been carried out, rather than mitigate the chances of it occurring in the first place.

Visit us at **www.sepio.systems** to find out more about our solution and the risks of the Raspberry Pi. Here, you can contact our sales team to further discuss the usage and benefits of Sepio Systems. Additionally, we provide demos to give a visual representation of how our solution works once deployed. Please do not hesitate to reach out to us with any questions or inquiries.

We are also available on:

Linkedin >>

https://www.linkedin.com/company/sepio-systems/

Facebook >>

https://www.facebook.com/cybersepiosystems/

Twitter >>

https://twitter.com/sepiosys

<< LEARN MORE >>