SEPI©

For Healthcare ITAM & Security Challenges

Innovative Hardware Asset Risk Management

February 24



Questions our healthcare customers ask themselves

- ? Are all my assets listed?
- Where are my assets located?
- Output the and the second s
- Output Are my assets verified and can I trust them?
- Where are my regulatory compliance gaps?



Hardware assets security concerns





2

Visibility and validation of **all Hardware Assets** including:

O Peripheral devices

1

○ (MAC-less devices)

O Hardware BOM

Hardware Zero Trust Control access to the enterprise through granular policy enforcement & hardware identity validation



3

Rogue Device Mitigation (RDM) of spoofed,

manipulated devices, and hidden implants



Detection of Hardware Manipulation within the supply chain

4

Hardware attack tools are gaining popularity

- O Every physical asset is an exposure
- Uncontrolled assets are an entry point for malware/ransomware payloads
- Uncontrolled assets are an exit door for sensitive data leakage
- Uncontrolled asset provide a permanent
 foothold for threat actors in the organization:
 MiTM, Data manipulation etc.



Demonstrated value to IT operation

- Existing CMDB, CMMS and NAC performance boost
- Visibility across inventory, shadow and rogue assets
- Reduced hardware clutter and better budget spending



Uninterrupted streamlined operations

Case study

BAPTIST HEALTH



Baptist deployment highlights

- More than 27,500 hosts and 544 network switches
- More than 635K connected assets
- Conline Sepio Cloud deployment
- Periodic reporting
- **Attack surface reduction**

COVID-19 VBC POP HEALTH ANALYTICS/AI CYBERSECURITY FINANCE/REVENUE CYCLE INTEROPERABILITY & HIE CLINICAL IT IMAGING

CYBERSECURITY

CISO Michael Erickson Discusses Implementation of HAC-1 Solution

Michael Erickson, CISO of the Louisville, Ky.-based Baptist Health, sat down with Healthcare Innovation to discuss the implementation of the Rockville, Md.-based Sepio Systems' HAC-1 solution

Janette Wider

Can you discuss how the implementation of the HAC-1 solution went at Baptist Health?

Sepio's HAC-1 solution went very simply for Baptist, actually, and we were surprised by that. A lot of times when we work with technology companies, especially those that are more innovative, it can be quite an implementation challenge. In this case, we were pleasantly surprised that the system is very lightweight, very sophisticated, but installs rather easily along with our other threat detection types of tools. **What is the most challenging**

What is the most challenging aspect of cybersecurity in hospitals today?

We're looking at the term zero trust quite closely right now, and I'm sure your readers are thinking about that strategy as well. For us, zero trust is difficult in an organization that serves the public. We want people to come and spend time in our organization to heal and be comforted. When we look at IT assets, we have to think about not just the activity of the devices that are coming into our organization, but the existence of those devices. So, working on visibility, working on understanding down to the peripheral level, the wireless level, and wired devices.

Understanding what's in our facilities at any given time is a is a big challenge and that's why we have invested in the Sepio product. It has given us a much more robust dataset than we've had previously with other vulnerability management tools.

SEPI

Attack study



Peripheral asset attacks

Way In



0x8A,0xC6,0x22,... http://URL... cmd /c netsh wlan show profiles "+NetName+"...



Depending on attacker's "style" and prior knowledge of the target, they will either:

- O Use HID emulation for binary payload
- "Send" the target PC to a pre-known/prepared web URL to download the payload
- Act as a Network Interface and inject the payload into the PC
- O Use USB Proxy MiTM attacks

Way Out







- O Exfiltrate the data directly to the attack tool
- O Use an integrated Wi-Fi to remotely extract
- Connect to the internet and exfiltrate the data
 "invisibly" such as adding comments on youtube
- Use continuous and invisible remote shell into corporate PCs

Network asset - MiTM & 802.1x bypassing

- Unmanaged switch & uncontrolled (MiTM) hardware are completely invisible to NAC and IDS/IPS
- O Any device that is connected poses a risk-
 - Spoof to be a legitimate device and send traffic into the network
 - Intercept/manipulate traffic between a legitimate asset and the network
 - Invisibly infect/attack a legitimate asset without being flagged
 - Create as **invisible and continuous** foothold in the infrastructure



Avoiding existing technologies blind spots



Friend or Foe?







Same MAC





MAC:00D085045802

MAC:00D085045802



Same Ports





| 👁 Zenmap | | | | | | | | | - | | × |
|-----------------------------|----------------------------|---|---|--|---|--|--------------------------------------|---------------------------|--------|------|---------|
| Sc <u>a</u> n <u>T</u> ools | <u>P</u> rofile <u>H</u> e | lp | | | | | | | | | |
| arget: 192 | 2.168.10.46 | | | Profile: | Intense s | can | | | \sim | Scan | Cancel |
| ommand: | nmap -T4 -A | -v 192.168.10.46 | | | | | | | | | |
| Hosts | Services | Nmap Output | Ports / Hosts | Topology H | ost Details | Scans | | | | | |
| S 4 Host | | nmap -T4 -A -v | 192.168.10.46 | | | | | | | ~ 1 | Details |
| | | NSE: Script Initiating I Completed NS Initiating I Completed NS Initiating I Completed NS Initiating I Completed AS Initiating I Completed AS Initiating I Scanning 192 Discovered o Discovered o Discovered o Discovered o Completed SS Initiating S | Pre-scanni SE at 10:15 SE at 10:15 SE at 10:15 SE at 10:15 SE at 10:15 SE at 10:15 STARP Ping Sci 2.168.10.46 RP Ping Scar arallel DNS SYN Stealth 2.168.10.46 open port 4 open port 5 Syn Stealth 5 Service scar | <pre>rg. 5 6 7 8 8 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9</pre> | psed psed psed n of 1 ho of 1 hos s] 92.168.10 92.168.10 192.168.10 192.168.11 192.168.11 192.168.12 | apsed (1 st. at 1 t. at 10 .46 46 .46 0.46 .46 elapsed | total hosts 0:15 1:15, 0.07s e | ;) :lapsed . ports) | | | |

| 👁 Zenmap | | | - | | × | | | | | | | |
|---------------------|-------------------|---|---|--------|---------|--|--|--|--|--|--|--|
| Sc <u>an T</u> ools | s <u>P</u> rofile | Help | | | | | | | | | | |
| Target: 19 | 2.168.10.46 | V Profile: Intense scan | \sim | Scan | Cancel | | | | | | | |
| Command: | nmap -T4 | -A -v 192.168.10.46 | | | | | | | | | | |
| Hosts | Services | Nmap Output Ports / Hosts Topology Host Details Scans | Nmap Output Ports / Hosts Topology Host Details Scans | | | | | | | | | |
| OS 4 Host | | nmap -T4 -A -v 192.168.10.46 | | ~ | Details | | | | | | | |
| | | <pre>Starting Nmap 7.91 (https://nmap.org) at 2023-04-18 10:15 Jerusalem Dayl NSE: Loaded 153 scripts for scanning. Initiating NSE at 10:15 Completed NSE at 10:15, 0.00s elapsed Initiating PP ing Scan at 10:15 Scanning 192.168.10.46 [1 port] Completed ASE at 10:15, 0.00s elapsed (1 total hosts) Initiating Parallel DNS resolution of 1 host. at 10:15, 0.07s elapsed Initiating SVN Stealth Scan at 10:15 Scanning 192.168.10.46 [1000 ports] Discovered open port 43/tcp on 192.168.10.46 Discovered open port 63/tcp on 192.168.10.46 Discovered open port 53/tcp on 192.168.10.46 Discovered open port 53/tcp on 192.168.10.46 Completed SVN Stealth Scan at 10:15</pre> | light | t Time | | | | | | | | |

Same Traffic





| 0 | | | | | Traffic Log - | Network Threat Prot | ection Logs | | | | <u>E</u> |
|---|-----------|----------|-----------|----------|------------------------------|---------------------|-------------|------------------|-----------------|------------------|----------|
| File Edit View Filter | Action H | rip . | | | | | | | | | |
| Date and | Action | Severity | Direction | Protocol | Source Nost | Source MAC | Source Port | Destination Host | Destination NAC | Destination Port | Applic |
| O22/11/2013 8:07. | . Allowed | 5 | Incoming | 009 | 192.140.0.55 | 7C-05-07-91-D | 5353 | 224.0.0.251 | 01-00-58-00+0 | \$353 | |
| 022/11/2013 8:07. | . Allowed | 5 | Incoming | ICF | 192.148.0.111 | A0-83-CC-4E-C | 52514 | 214.2.48.149 | 00-09-08-09-0 | 20 | D:\Pro |
| 22/11/2013 8:08. | . Allowed | 5 | Incoming | 100 | 192.168.0.53 | 70-08-07-91-0 | 1900 | 239.255.255.250 | 01-00-58-78-8 | 1900 | |
| 22/11/2013 8:08. | . Allowed | 5 | Incoming | TCP | 192.148.0.70 | 00-50-56-88-7 | 58498 | 192.160.0.117 | 00-00-29-99-9 | 443 | D:\Pro |
| D22/11/2013 8:08. | . Allowed | 5 | Incoming | 059 | 192.148.0.56 | 00-07-22-29-5 | 137 | 192.140.0.127 | TT-TT-TT-T | 137 | C:\Win |
| D22/11/2013 8:06. | . Allowed | 3 | Incoming | 009 | 192.148.0.63 | 00-07-FE-FD-E | 137 | 192.168.0.127 | TT-TT-TT-TT-T | 137 | C:\Win |
| D22/11/2013 8:08. | . Allowed | 5 | Incoming | 3CP | 192.168.0.111 | A0-83-CC-4E-C | 52015 | 216.2.40.149 | 00-09-07-09-0 | 80 | D:\Pro |
| D22/11/2013 8:08. | . Allowed | 5 | Incoming | TCP | 192.148.0.111 | 20-83-CC-4E-C | 52816 | 216.2.40.149 | 00-09-07-09-0 | 80 | Dt\Pro |
| 22/11/2013 8:08. | . Allowed | 5 | Outgoing | TCP | 192.148.0.117 | 00-00-29-99-9 | 42301 | 192.168.0.310 | 00-00-29-28-4 | 8014 | C:\Win |
| 22/11/2013 8:08. | . Allowed | 5 | Incoming | TCP | 192.148.0.111 | A0-83-CC-48-C | 82817 | 216.2.48.149 | 00-09-07-09-0 | =0 | D:\Pro |
| D22/11/2013 8:00. | . Bilowed | . 5 | Incening | 157 | 182.148.0.111 | 30-53-CC-4E-C | 32318 | 214.2.42.143 | 00-09-0F-09-0 | 80 | Dr\Pro |
| D 22/11/2013 8:08. | . Allowed | 5 | Incoming | 000 | 192.148.0.51 | 84-85-27-17-B | 50144 | 239.235.255.250 | 01-00-5E-7F-F | 1900 | 100000 |
| Daz/11/2013 8:08. | . Allowed | 5 | Incoming | 009 | 192.148.0.57 | 00-23-18-C3-F | 137 | 192.140.0.127 | TT-ET-FT-TT-T | 137 | C:\Win |
| D22/11/2015 8:08. | . Allowed | 5 | Incening | 009 | 192.148.0.57 | 00-23-18-C3-F | 60248 | 224.0.0.252 | 01-00-52-00-0 | 5355 | C:\Win |
| D22/11/2013 8:08. | . Allowed | 5 | Incoming | 57 | 192.148.0.55 | 7C-08-07-91-D | 115 | 224.0.0.22 | 01-00-M-00-0 | ITA | |
| D22/11/2013 8:08. | . Allowed | 5 | Incoming | TOP | 192.148.0.55 | 10-05-07-91-0 | 51452 | 224.0.0.252 | 01-00-58-00-0 | \$355 | C:\Win |
| D22/11/2013 8:08. | . Allowed | 3 | Incoming | ICP | 192.148.0.111 | A0-83-CC-4E-C | 52019 | 216.2.60.149 | 00-09-05-09-0 | 80 | D:\Pro |
| D22/11/2013 0:08. | . Allowed | 5 | Incoming | ICF | 192.148.0.111 | A0-83-CC-48-C | 82820 | 216.2.48.149 | 00-09-08-09-0 | 80 | D:\Pro |
| D22/11/2013 8:08. | . Allowed | 5 | Incoming | 105 | 192.148.0.111 | A0-83-CC-4E-C | 82821 | 214.2.40.149 | 00-09-07-09-0 | 80 | D:\Pro |
| 22/11/2013 8:08. | . Allowed | 5 | Incoming | TCP | 192.148.0.111 | A0-83-CC-4E-C | 52822 | 216.2.40.149 | 00-09-07-09-0 | 20 | D:\Pro |
| 22/11/2013 8:08. | . Allowed | 5 | Outgoing | TCP | 192.148.0.117 | 00-00-29-99-9 | 42303 | 192.148.0.110 | 00-00-29-28-4 | #016 | C:\Win |
| D22/11/2013 8:08. | . Allowed | 3 | Incending | ICF | 192.148.0.111 | A0-83-CC-4E-C | 52824 | 214.2.48.149 | 00-09-07-09-0 | 10 | D:\Pro |
| 22/11/2013 8:09. | . Allowed | 5 | Outgoing | TCP | 192.168.0.117 | 00-00-29-99-9 | 02304 | 192.160.0.310 | 00-00-29-28-4 | 8016 | C:\Win |
| D22/11/2013 8:09. | . Allowed | 5 | Incoming | TCP | 192.148.0.111 | A0-83-CC-4E-C | 52825 | 216.2.48.149 | 00-09-05-09-0 | 80 | D:\Pro |
| D22/11/2013 8:09. | . Allowed | 5 | Incoming | ICP | 192.148.0.111 | A0-83-CC-46-C | 52826 | 216.2.48.149 | 00-09-07-09-0 | 80 | D:\Pro |
| D22/11/2013 8:09. | . Allowed | 5 | Incoming | 17 | 192.148.0.64 | E0-69-95-FA-3 | NA. | 224.0.0.22 | 01-00-58-00-0 | NA | |
| D22/11/2013 8:09. | . Allowed | 5 | Incoming | 107 | 192.168.0.64 | E0-69-95-FA-3 | 52124 | 224.0.0.252 | 01-00-55-00-0 | \$358 | C:\Win |
| 22/11/2013 8:09. | . Allowed | 5 | Incoming | UDP | 192.168.0.64 | E0-69-95-FA-3 | 137 | 192.140.0.127 | TT-TT-TT-TT-T | 137 | C:\Win |
| Constant of the state of the state of the | | | | | and the second second second | | | | | | |

| 0 | | | | Traffic Log - I | Network Threat Prot | ection Logs | | | | 12. |
|-----------------------------|-------------|-------------|----------|--|---------------------|-------------|------------------|------------------------|------------------|----------|
| File Edit View Filter Actio | n Help | | | | | | | | | |
| Date and Act | ion Severit | y Direction | Protocol | Source Nost | Source MAC | Source Port | Destination Nost | Destination NAC | Destination Port | Applic |
| 322/11/2013 8:07 All | oved 5 | Incoming | 009 | 192.148.0.55 | 7C-05-07-91-D | 5353 | 224.0.0.251 | 01+00-58-00+0 | \$353 | |
| 022/11/2013 8:07 All | oved 5 | Incoming | SCE | 192.148.0.111 | A0-83-00-48-0 | 52514 | 214.2.48.149 | 00-09-08-09-0 | =0 | D:\Pro |
| 22/11/2013 8:08 All | oved 5 | Incoming | 100 | 192.168.0.53 | 70-08-07-91-0 | 1900 | 239.255.255.250 | 01-00-52-78-8 | 1900 | |
| 022/11/2013 8:08 All | oved 5 | Incoming | TCP | 192.148.0.70 | 00-50-56-56-7 | 58498 | 192.160.0.117 | 00-00-29-99-9 | 443 | D:\Pro |
| 022/11/2013 8:08 All | oved 5 | Incoming | 009 | 192.148.0.56 | 00-07-22-29-5 | 137 | 192.140.0.127 | TT-ET-TT-T | 137 | C:\Win |
| 222/11/2013 8:06 All | owed 3 | Incoming | 00F | 192.148.0.83 | 00-07-FE-FD-E | 137 | 192.168.0.127 | TT-TT-TT-TT-T | 137 | C:\Win |
| 022/11/2013 8:08 All | oved 5 | Incoming | TCP | 192.168.0.111 | A0-83-CC-4E-C | 52015 | 216.2.40.149 | 00-09-02-09-0 | 80 | D:\Pro |
| 022/11/2013 8:08 All | oved 5 | Incoming | TCP | 192.148.0.111 | A0-83-CC-4E-C | 52816 | 216.2.40.149 | 00-09-07-09-0 | 80 | Dt\Pro |
| 22/11/2013 8:00 All | oved 5 | Outgoing | TCP | 192.148.0.117 | 00-00-29-99-9 | 42301 | 192.148.0.310 | 00-00-29-28-4 | 8014 | C:\Win |
| 022/11/2013 8:08 All | oved 5 | Incoming | ICF | 192.148.0.111 | A0-83-00-48-0 | 82817 | 216.2.48.149 | 00-09-07-09-0 | 10 | D:\Pro |
| 022/11/2013 8:88 NIL | oved 5 | Incening | SCP | 182.149.0.111 | 30-83-CC-4E-C | 32318 | 214.2.42.149 | 00-08-0 7 -08-0 | 80 | Dr\Pro |
| 22/11/2013 8:08 All | oved 5 | Incoming | 100 | 197.148.0.51 | 84-85-27-17-B | 50144 | 239.235.255.250 | 01-00-5K-7F-F | 1900 | |
| 022/11/2013 8:08 All | oved 5 | Incoming | 009 | 192.148.0.57 | 00-23-18-C3-F | 137 | 192.140.0.127 | TT-ET-TT-TT-T | 137 | C:\Win |
| 022/11/2013 8:08 All | oved 5 | Incoming | 009 | 192.148.0.57 | 00-23-18-C3-F | 60048 | 224.0.0.252 | 01-00-58-00-0 | 5355 | C:\Win |
| 22/11/2013 8:08 All | oved 5 | Incoming | 57 | 192.148.0.55 | 70-08-07-91-0 | 115 | 224.0.0.22 | 01-00-M-00-0 | ITA | |
| 022/11/2013 8:08 All | oved 5 | Incoming | TOP | 192.148.0.55 | 10-05-07-91-0 | 51452 | 224.0.0.252 | 01-00-58-00-0 | \$355 | C:\Win |
| 022/11/2013 8:08 All | oved 5 | Incoming | ICP | 192.148.0.111 | A0-83-CC-4E-C | 52019 | 216.2.60.149 | 00-09-07-09-0 | 80 | Dr\Pro |
| 022/11/2013 8:08 All | oved 5 | Incoming | ICF | 192.148.0.111 | A0-83-00-48-0 | 82820 | 216.2.48.149 | 00-09-07-09-0 | 10 | D:\Pro |
| 22/11/2013 8:08 All | oved 5 | Incoming | TCP | 192.168.0.111 | A0-83-CC-48-C | 82821 | 214.2.40.149 | 00-09-07-09-0 | 80 | D:\Pro |
| 022/11/2013 8:08 All | oved 5 | Incoming | TCP | 192.148.0.111 | A0-83-CC-4E-C | 52822 | 216.2.40.149 | 00-09-07-09-0 | 20 | D:\Pro |
| 22/11/2013 8:08 All | oved 5 | Outgoing | TCP | 192.148.0.117 | 00-00-29-99-9 | 42303 | 192.148.0.110 | 00-00-29-28-4 | 8014 | C:\Win |
| 022/11/2013 8:00 All | owed 3 | Incending | ICF | 192.148.0.111 | A0-83-CC-48-C | 52824 | 216.2.68.149 | 00-09-07-09-0 | 10 | D:\Pro |
| 22/11/2013 8:09 All | oved 5 | Outgoing | TCP | 192.168.0.117 | 00-00-29-99-9 | 42304 | 192.148.0.110 | 00-00-29-28-4 | 8016 | C:\Win |
| 022/11/2013 8:09 All | oved 5 | Incoming | TCP | 192.148.0.111 | A0-83-CC-4E-C | 52525 | 216.2.48.149 | 00-09-07-09-0 | 80 | D:\Pro |
| 022/11/2013 8:09 All | oved 5 | Incoming | TCP | 192.148.0.111 | A0-83-CC-48-C | 52826 | 216.2.68.149 | 00-09-07-09-0 | 80 | D:\Pro |
| 022/11/2013 8:09 All | oved 5 | Incoming | 17 | 192.148.0.64 | E0-69-95-FA-3 | NA. | 224.0.0.22 | 01-00-58-00-0 | NA | |
| 022/11/2013 8:09 All | oved 5 | Incoming | 107 | 182.168.0.64 | E0-69-95-FA-3 | 52124 | 224.0.0.252 | 01-00-5E-00-0 | \$353 | C:\Win |
| 022/11/2013 8:09 Bit | oved 5 | Incoming | TOP | 192.168.0.64 | E0-69-95-FA-3 | 137 | 192.140.0.127 | TT-TT-TT-TT-T | 137 | C:\Win v |
| | | 1 | | Street St | | | | | | |

Different Asset DNA!













Sepio's trafficless solution avoids cumbersome deployments and privacy issues, vertical, type and protocol indifferent, at any scale, without effecting the network performance.



Sepio's enhanced visibility provides unmatched rogue device mitigation, while supporting USB entitlement at scale.





Go beyond legacy NAC solutions

Embrace Sepio's Zero Trust Hardware Access (ZTHA) to augment your ZTNA initiatives across all your assets (IT/IoT/OT).

Establish trust validate assets, enforce regulatory compliance with a single low TCO solution.

Sepio's unique approach





SEPIO

Asset DNA provides a single source of truth, focusing on EXISTENCE – rather than ACTIVITY.

With our patented technology, we now harness a new data source – physical layer to accurately identify and classify your assets.

Introducing Asset DNA







Sepio's proven value for healthcare



Who benefits from our data?

SIEM/SOAR

- Instant alerts when unwanted or rogue devices are connected, eliminating unnecessary noise
- Contextual information, i.e., asset location, expedites response time to prevent crises
- Publicly recognized asset vulnerability module (OSINT and proprietary) for an immediate mitigation

Security team

- Understand what needs attention with actionable data
- Enforce organization policies and establish trust at the asset level
- Greater ROI by radically improving the efficacy of existing tools

ITAM & CMDB

- Reduce complexity with a consolidated source of asset visibility across all environments
- Reduce hardware clutter
- Ensure operational efficiency of assets

CAASM

- Augment existing data sources
- Validate security controls
- Remediate issues

Architecture and Deployment aspects





SEPIO

Sepio agent deployment options

Fixed agent

Session based





Typical Customer Journey

Workshop with extended team

Identify key use cases – endpoint or network

PoV – installs in hours; standard duration up to 2 weeks Develop deployment and integration plan Present business case for approval



Deployment process



SEPIO

Sepio's Asset Risk Management solution

| \bigcirc | Visibility Overview | | | | | | ¢, 2 |
|--|----------------------------------|---------------------------------|---------------------------------------|-------------------------------|----------------------|--|------------|
| Visibility ** Assets Visibility | ිද් 93690 Assets Total | 0 465 New Hosts | © 6510 26 _{Hosts} New | 87180 Network Total | 0 439 New | Recent Visible Risks Assets (188) Hosts (8) Network (24) Camera | 0 |
| Control Center Reports | Online Assets Risk | Assets Distribution | 29 | 523 | Sort By: High Risk 👻 | Communication - Switches Extreme Networks | (6) |
| Logs 랴 Settings | High | 🛱 Printer | 96 | | 6510 | Communication - C3750X Switch Cisco Systems | |
| | 38 | Random MAC address | 59 1 | | | Cisco Systems CAC Card Reader Realtek Semiconductor Corp. | 1) |
| | Medium | ස් Attack Tool | Attack Tool Access Point Access Point | | | RTL8188EUS 802.11n Wireless Network Adapter Realtek Semiconductor Corp. | 1) |
| | 1306 | 🗐 Keyboard | 9 0 | | | RTL8153 Gigabit Ethernet Adapter Realtek Semiconductor Corp. | (1) |
| | (| Smartphone | 0 10 0 1 4 | | | Keyboard K120 Logitech, Inc. | 1) |
| | 92384 | 🙏 USB Hub | 0 10 0 | | | Hub Hub | (1) |
| | | [™] ⊕ IoT - Healthcare | () 1 () 0 | | | Hub | |

Additional video resources

- https://www.youtube.com/watch?v=kv8_YzFQ4OY&list=PLIhAGMBWwGmex8Fk5w4PbbFNZH7O0nE0q&index=5
- https://www.youtube.com/watch?v=CCiUqsyf-H8&list=PLIhAGMBWwGmfe-wUejNyOzTpiadr715m6
- https://www.youtube.com/watch?v=bJPfINfYumc
- https://www.youtube.com/watch?v=A3Lf16GfGGE&list=PLIhAGMBWwGmdlt7aRfTc0C07N_1kA49p4&index=7





See what you've been missing