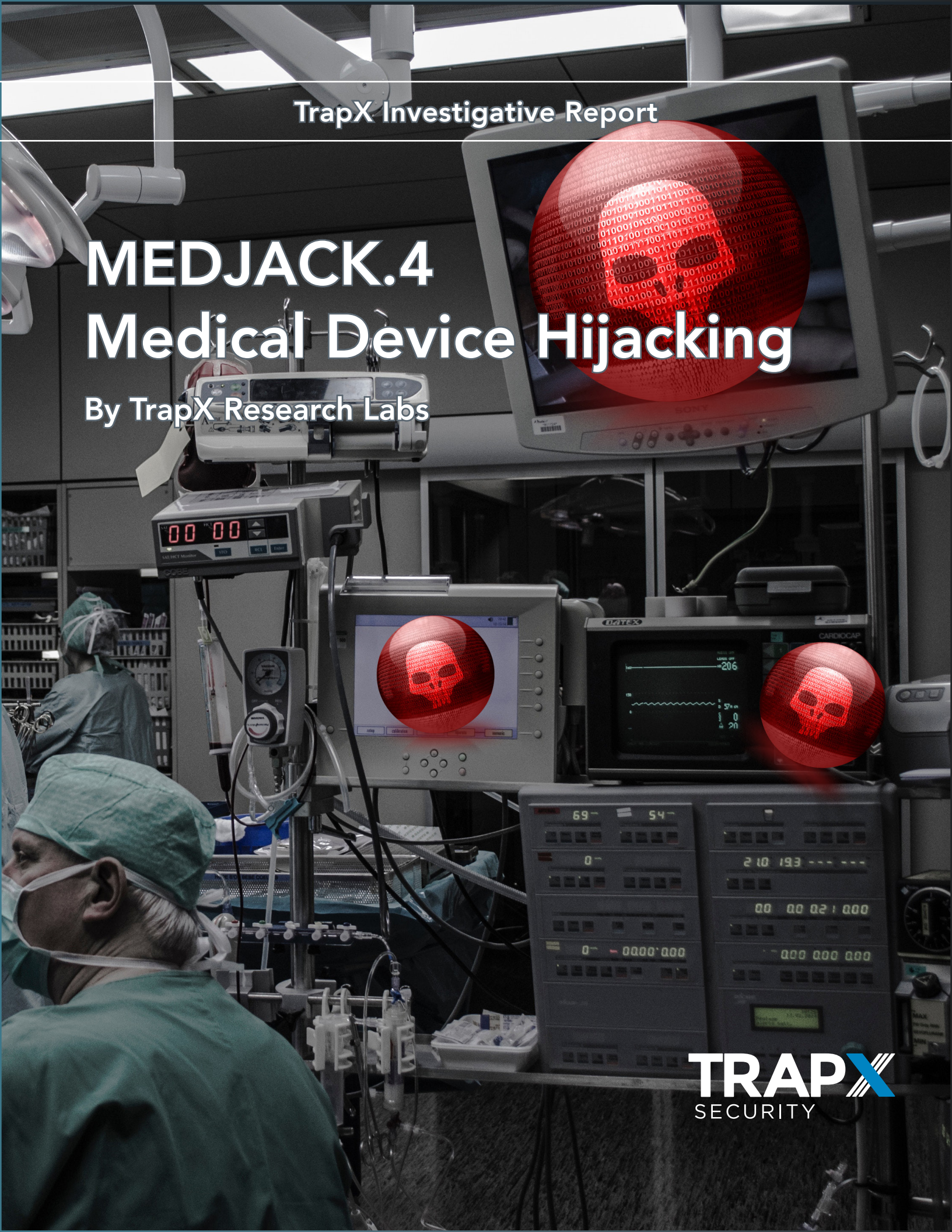
TrapX Investigative Report

# MEDJACK.4 Medical Device Hijacking

By TrapX Research Labs



TRAPX SECURITY

# Contents

# Executive Summary

Over the last six months, the team at TrapX Labs conducted the world's first counter-intelligence cyber-deception operation by creating a fake hospital network and disseminating VPN credentials for it in the Darknet.

In addition, TrapX has been working with several hospitals that have been targets of attacks and helped identify and remediate the attacks.

Extensive data was collected on threat actors targeting healthcare providers and unearthed several cases of MEDJACKING.[1]

This study shows the extent of criminal activities that target healthcare providers, as well as the level of involvement of Russian threat actors.

*"Healthcare networks remain under continuous attack. MEDJACK.4 documents the growing escalation of attacks on healthcare providers to target and exploit medical devices and an increase in sophistication in the techniques used by the attackers."*

**– Ori Bach**
Vice President Products and Marketing of TrapX Security

**This report details:**

- The use of medical device hijacking to steal medical records.
- The broad penetration by threat actors into medical devices located in hospitals.
- The high demand in the Darknet market for healthcare-related information.

**Transforming the hunters into the hunted:**

As part of our counter intelligence efforts at TrapX Labs, we created an entire network for a fictitious healthcare institution including a public website that gave the attackers the feeling that they were dealing with a real healthcare organization. We then exchanged the VPN credentials of this network in the Darknet market. This "fake" hospital served as the ultimate deception to lure, engage and study cyberattackers. As a result, our team at TrapX Labs was able to fully document the attackers' behavior.

1. Medical device hijacking

# The Cyber Security Challenge for Healthcare Today

The healthcare ecosystem today, includes over 900,000 physicians in over 225,000 practices. Their teams include 2,700,000 registered nurses, physician assistants, and medical administrative staff that provide support within their practices and within the many thousands of hospitals in which acute healthcare services are received.

There are also many other important healthcare facilities which are critical to the ecosystem. This includes skilled nursing facilities (SNF), ambulatory surgical centers (Surgi-centers), physical therapists, eye surgery centers, dialysis centers, quick medicine clinics, X-ray/CT-scan centers and many more. The great majority of these facilities are connected electronically and often share common electronic medical record/health systems (EMR/EHR). Ambulatory physicians must move almost transparently between the different electronic systems that make all of this work efficiently. This ecosystem is expected to reach almost 20% of US gross domestic product (GDP) by 2025[2] and is a massive target of choice for cyberattackers.

In 2017 alone, there were 36 breaches that utilized ransomware. This is an increase of over 89% from those reported in 2016[3] . This trend will move aggressively into smaller physician practices and lower-end hospitals and will cause considerable trauma and expense to everyone who doesn't properly protect their healthcare business.

Compliance is still very important for the healthcare community. Data is protected under the Health Insurance and Portability and Accountability Act (HIPAA). In the event of a breach, state requirements for notifications vary. Some states require that you notify the state attorney general if you suffer a breach of more than 1,000 records. The time periods for notification also vary.

2. https://www.advisory.com/daily-briefing/2017/02/16/spending-growth

3. https://www.beckershospitalreview.com/cybersecurity/ransomware-attacks-targeting-us-healthcare-up-89-5-things-to-know.html

# The Medical Device Security Challenge

Medical devices remain black holes to the healthcare staff that must support them. Medical devices go through a complex Food and Drug Administration approval before they can be released to ensure that the standards of manufacturing and product performance meet the 'safe for intended use' guidelines. These products, as approved by the FDA, are essentially closed devices. The cyberdefense team within hospitals cannot install any cyberdefense software on these devices either. Internal software can only be loaded or updated by the device manufacturer.

Furthermore, medical devices cannot be scanned, so understanding the status of potential cyber threats within medical devices is very limited. The healthcare staff would face too much liability if they tampered with the devices to install cybersecurity. Any action might impact the operation of the device in an unpredictable or unknown way. No one in the healthcare system wants to take on that risk. In the final analysis, these medical devices must be managed by the medical device manufacturer's customer support team.

*"It is really easy today for cyberattackers to find and exploit medical devices in any health-care network. As soon as they get past the firewall, the medical devices they find are completely unprotected. The cyberattackers can establish backdoors and exfiltrate patient data. Medical institutions today are very vulnerable to attacks called MEDJACK."*

**– Moshe Ben Simon**
Chief Executive Officer of TrapX Security

Hospitals today install their medical devices "behind the firewall" where they are believed to be secure and protected. We know from all our case studies that this strategy simply doesn't work. Modern attackers and their malware have defeated this strategy in all our case studies over the years.

Malware on medical devices is also very expensive to remove. The healthcare IT team cannot get into these devices. All remediation must be done by the manufacturer or their designated representatives. Almost as soon as they "clean" one machine then they must "re-clean" it again. Many medical devices run outdated operating systems such as Windows 95, Windows 2000, Windows XP or Windows 7. These older operating systems are not updated nor protected against the new wave of cyber threats. The operating systems & machines are getting older and the hackers are getting smarter.

On top of this, there are tens of thousands of medical devices. The list includes diagnostic equipment (PET scanners, CT scanners, MRI machines, etc.), therapeutic equipment (infusion pumps, medical lasers, LASIK surgical machines), life support equipment (heart-lung machines, medical ventilators, extracorporeal membrane oxygenation machines and dialysis machines), and many others that are still vulnerable today.

# MEDJACK.4 - A Functional Overview

## This is the anatomy of a generic medical device hijack attack (MEDJACK)

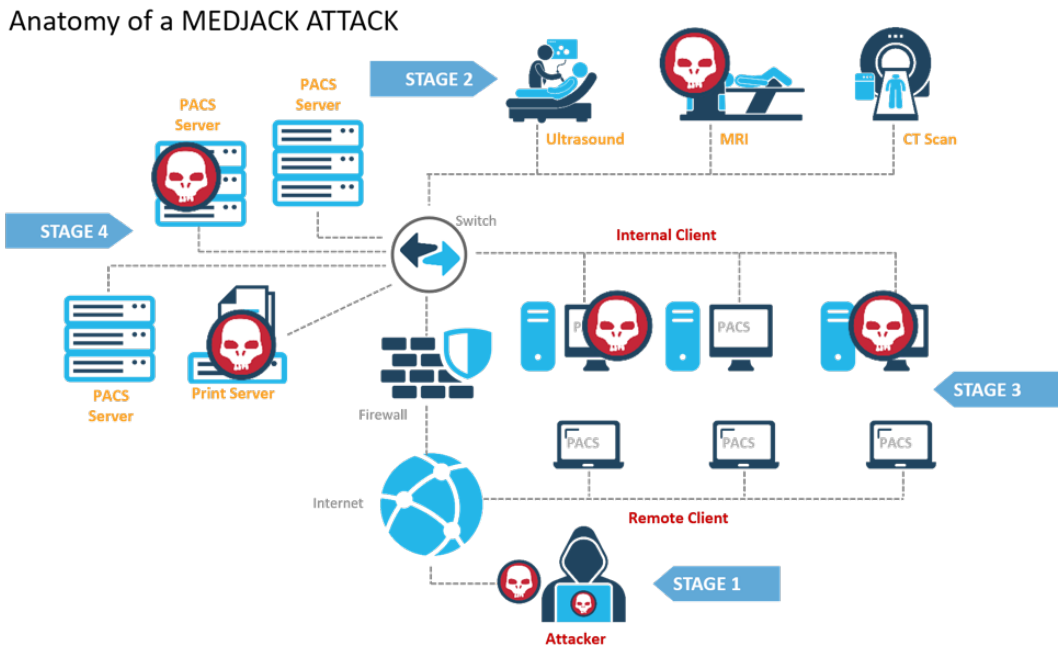
**Stage 1**: Attacker researches target, chooses one or more approaches, then targets and executes attacks, penetrating at least once.

**Stage 2**: Attacker gains foothold in a medical device and cautiously seeks general information and escalation of privileges. Attacker then begins lateral movement.

**Stage 3**: Attacker continues reconnaissance and identifies targets, moves laterally within networks.

**Stage 4**: Attacker engages with chosen targets, exfiltrates confidential patient healthcare data and financial records, cleans up the artifacts of attack as best as possible can and leaves.

**Stage 5**: Attacker leaves a ransomware tool to run in the network to extort funds directly from the healthcare institution.



# Case Study #1

# The Counter-intelligence Operation

## Creating a "fake" healthcare institution & watching it get attacked

**Overview:**

TrapX created a whole entire healthcare provider network including a website and a real, fully-functional IT infrastructure that also contained multiple medical devices.

The goal of creating this healthcare institution was to gain a deeper understanding of attacker tactics and to learn more about their techniques once they penetrate a healthcare organization's network.

The IT infrastructure contained desktop computers, network devices, servers and medical devices. To ensure realism, we also installed various security products like a Firewall, Anti-Virus web filters and other relevant tools. The idea was to give the adversary the feeling that they are attacking a real healthcare organization.

In addition, we deployed our own product DeceptionGrid, and analyzed attacker activities to see every aspect of their operation.

The medical network contained several Traps camouflaged as medical devices - including blood gas analyzers, EMR , PACS , CT scan machines, and X-ray machines.

To keep things interesting for attackers the systems, were loaded with bogus image data, falsified patient data, and several networks of Traps.

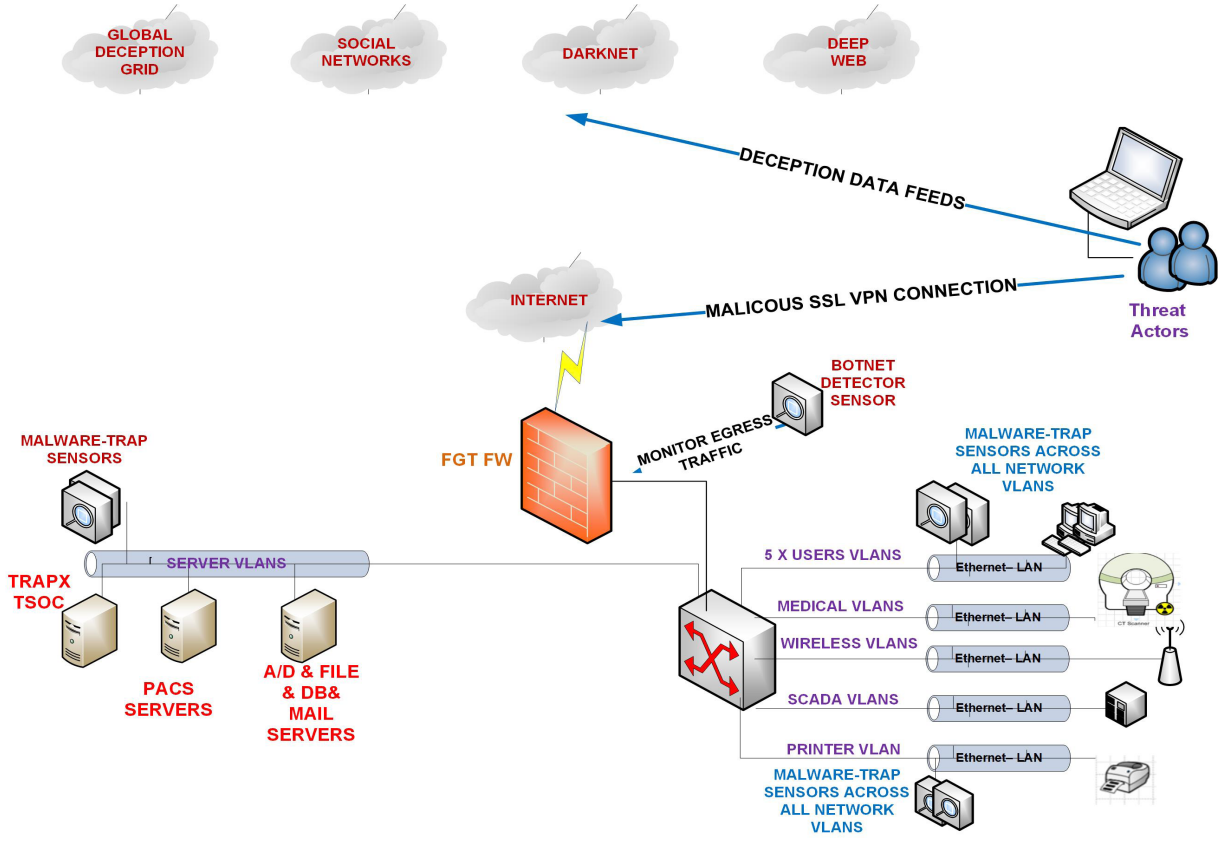
Moreover, we created a website for this fake healthcare institution - just in case the attackers might

try to gather information on the healthcare institution. We named this healthcare institution "Medical Now Group".

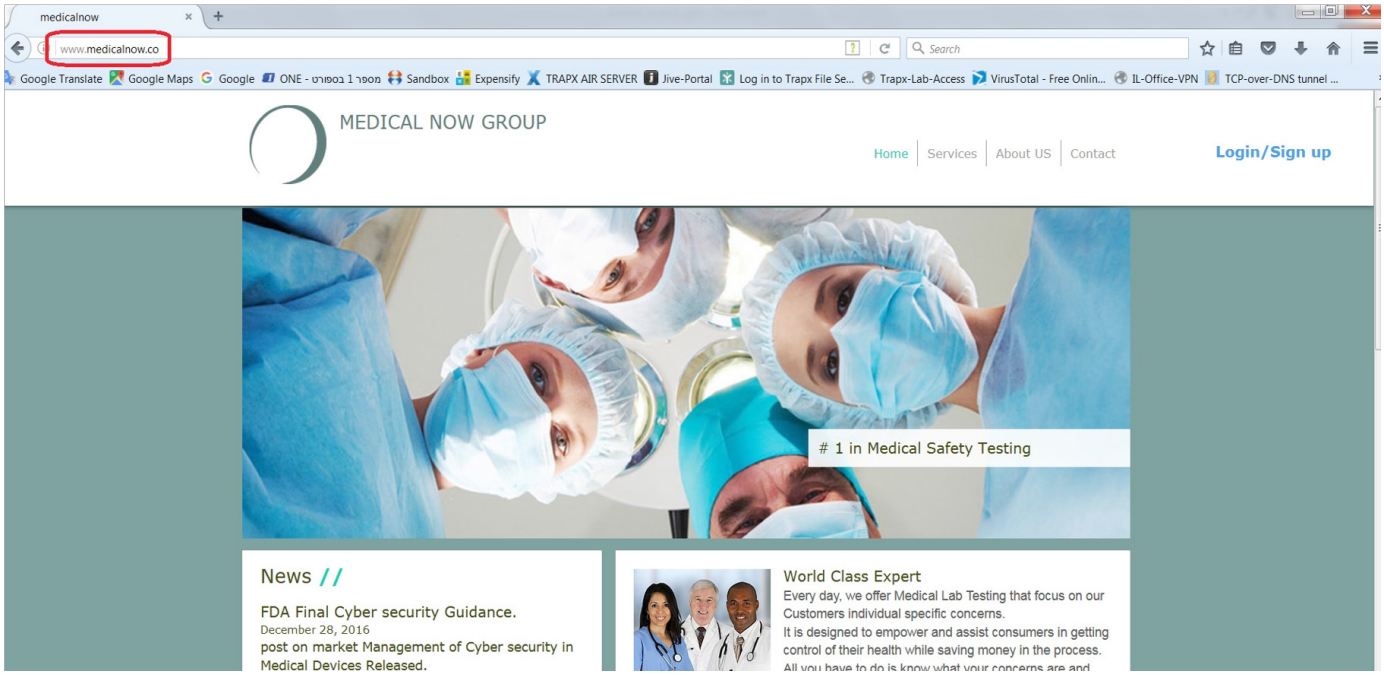
(We also applied traffic analysis on the website to cross-correlate between the IP that accesses the website and the IP that accesses the fake network.) To attract the attackers into the fake network, we created several VPN users that we exchanged in the Darknet with real attackers. We also published part of the access data in several hacking forums that focus on hacking into medical organizations including the Pastebin website.

The VPN user provided remote desktop access to one of the internal desktops. The idea was to simulate a real user access to one of this healthcare institution's desktop via VPN.

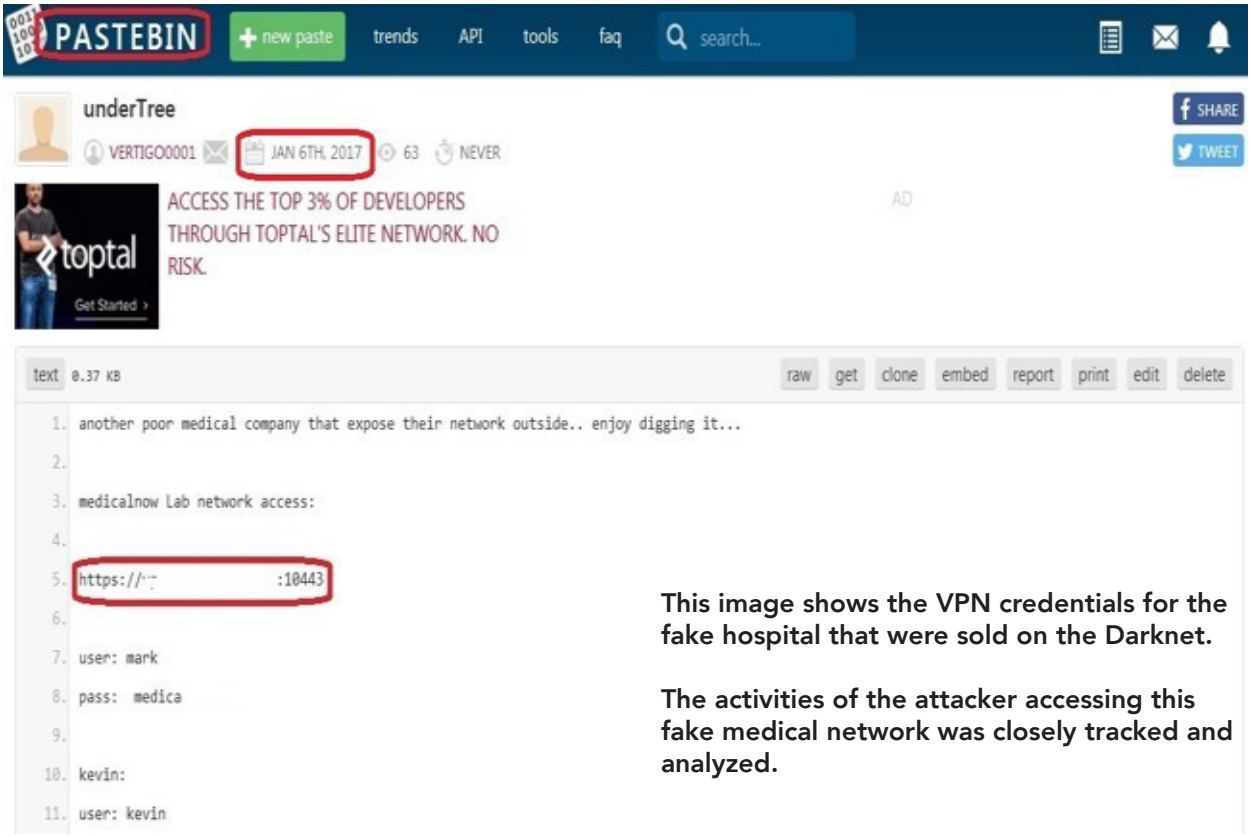
### Step 1: The below diagram illustrates the fake hospital topology



**Step 2: We put together the fake healthcare institution's web site.**




**Step 3: Here is a screenshot from the Pastebin, where we exchanged information with the attackers. Some of the data cannot be displayed as it can expose our research team to dangerous cyber-criminals.**




**This image shows the VPN credentials for the fake hospital that were sold on the Darknet.**

**The activities of the attacker accessing this fake medical network was closely tracked and analyzed.**

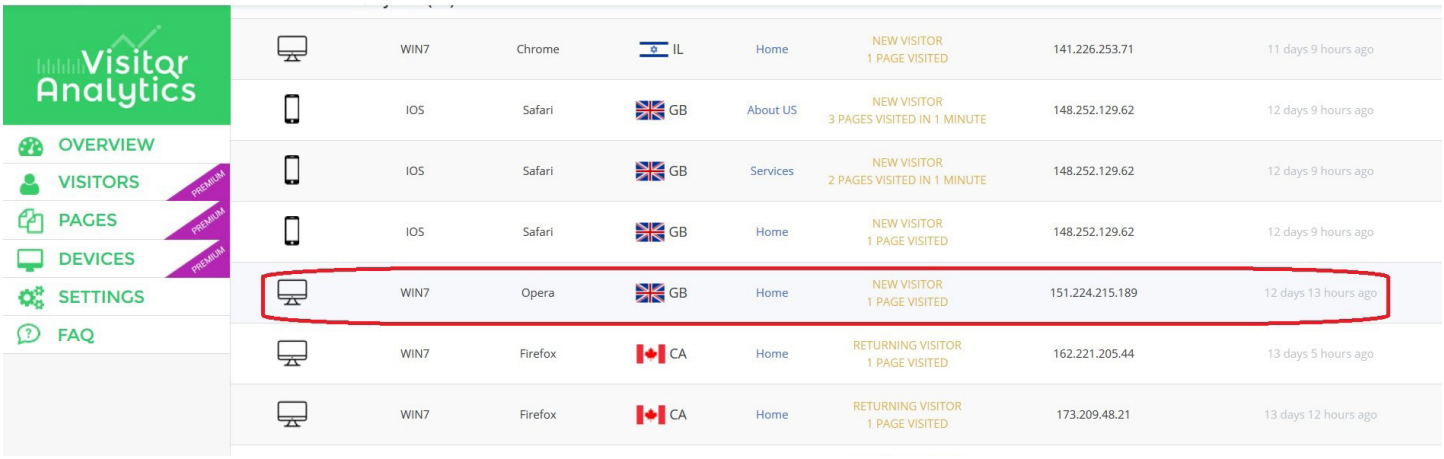
# The Results

It did not take long for the first 'buyer' to use the VPN credentials that we provided.

**Step 1: Below is the screenshot of the VPN access logs that show the attacker's connection using the VPN user "mark".**

| | |
|---|---|
| 1/7/17 8:01:00.000 AM | Jan 7 08:01:00 10.10.20.1 date=2017-01-07 time=08:21:14 devname=FGT80C3910604858 devid=FGT80C3910604858 logid=0101039943 type=event subtype=vpn level=information vd="root" logdesc="SSL VPN new connection" action="ssl-new-con" tunneltype="ssl" tunnelid=0 remip=151.224.215.189 tunnelip=(null) user="N/A" group="N/A" dst_host="N/A" reason="N/A" msg="SSL new connection"<br>host = 10.10.20.1 source = udp:514 sourcetype = syslog |
| 1/7/17 8:01:00.000 AM | Jan 7 08:01:00 10.10.20.1 date=2017-01-07 time=08:21:14 devname=FGT80C3910604858 devid=FGT80C3910604858 logid=0101039943 type=event subtype=vpn level=information vd="root" logdesc="SSL VPN new connection" action="ssl-new-con" tunneltype="ssl" tunnelid=0 remip=151.224.215.189 tunnelip=(null) user="mark" group="N/A" dst_host="N/A" reason="N/A" msg="SSL new connection"<br>host = 10.10.20.1 source = udp:514 sourcetype = syslog |
| 1/7/17 8:01:00.000 AM | Jan 7 08:01:00 10.10.20.1 date=2017-01-07 time=08:21:14 devname=FGT80C3910604858 devid=FGT80C3910604858 logid=0101039943 type=event subtype=vpn level=information vd="root" logdesc="SSL VPN new connection" action="ssl-new-con" tunneltype="ssl" tunnelid=0 remip=151.224.215.189 tunnelip=(null) user="N/A" group="N/A" dst_host="N/A" reason="N/A" msg="SSL new connection"<br>host = 10.10.20.1 source = udp:514 sourcetype = syslog |
| 1/7/17 8:01:00.000 AM | Jan 7 08:01:00 10.10.20.1 date=2017-01-07 time=08:21:13 devname=FGT80C3910604858 devid=FGT80C3910604858 logid=0101039943 type=event subtype=vpn level=information vd="root" logdesc="SSL VPN new connection" action="ssl-new-con" tunneltype="ssl" tunnelid=0 remip=151.224.215.189 tunnelip=(null) user="N/A" group="N/A" dst_host="N/A" reason="N/A" msg="SSL new connection"<br>host = 10.10.20.1 source = udp:514 sourcetype = syslog |
| 1/7/17 8:01:00.000 AM | Jan 7 08:01:00 10.10.20.1 date=2017-01-07 time=08:21:13 devname=FGT80C3910604858 devid=FGT80C3910604858 logid=0101039943 type=event subtype=vpn level=information vd="root" logdesc="SSL VPN new connection" action="ssl-new-con" tunneltype="ssl" tunnelid=0 remip=151.224.215.189 tunnelip=(null) user="N/A" group="N/A" dst_host="N/A" reason="N/A" msg="SSL new connection"<br>host = 10.10.20.1 source = udp:514 sourcetype = syslog |
| 1/7/17 8:00:59.000 AM | Jan 7 08:00:59 10.10.20.1 date=2017-01-07 time=08:21:13 devname=FGT80C3910604858 devid=FGT80C3910604858 logid=0101039943 type=event subtype=vpn level=information vd="root" logdesc="SSL VPN new connection" action="ssl-new-con" tunneltype="ssl" tunnelid=0 remip=151.224.215.189 tunnelip=(null) user="mark" group="N/A" dst_host="N/A" reason="N/A" msg="SSL new connection"<br>host = 10.10.20.1 source = udp:514 sourcetype = syslog |
| 1/7/17 8:00:59.000 AM | Jan 7 08:00:59 10.10.20.1 date=2017-01-07 time=08:21:13 devname=FGT80C3910604858 devid=FGT80C3910604858 logid=0101039943 type=event subtype=vpn level=information vd="root" logdesc="SSL VPN new connection" action="ssl-new-con" tunneltype="ssl" tunnelid=0 remip=151.224.215.189 tunnelip=(null) user="N/A" group="N/A" dst_host="N/A" reason="N/A" msg="SSL new connection"<br>host = 10.10.20.1 source = udp:514 sourcetype = syslog |

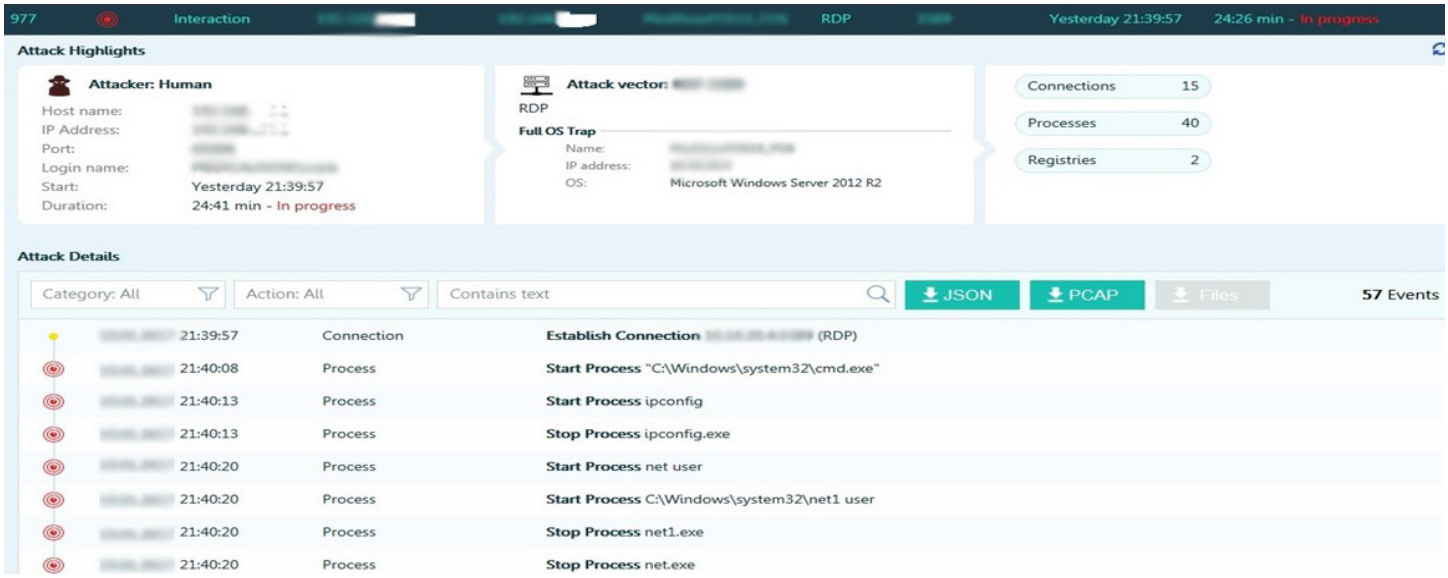
**Step 2. This attacker's IP was also on our fake website. As we correctly predicted, the attacker visited the fake website before penetrating the network to platform early reconnaissance.**




**The attacker's IP address was not flagged as malicious by any of the reputation providers, and we didn't see any past actions that can show malicious activities.**

## Here is the summary of the attacker's activities:

Step 1: Once the attacker landed on the endpoint he quickly disabled the AV software.
Step 2: The attacker started to search for medical data on the endpoints.
Step 3: The attacker was lured by a fake SMB Network Share while trying to access a real share and copied some of the fake data that was on it.
Step 4: The attacker then uploaded part of the "fake data" that he stole using SSL Tunnel access.
Step 5: The attacker performed reconnaissance on the network VLAN he was located in and interacted with several of the Traps.
Step 6: Part of the fake network share contained data that lured the attacker to a Windows server that acted like a full OS decoy, which he accessed via RDP (Remote Desktop Protocol). The attacker tried to download malicious tools to this server with partial success because the web filter blocked some of them. (Screenshot below)




## Conclusions:

During our research, we identified several more attackers that used the VPN credentials and executed classic lateral movement strategies.

The purpose of the lateral movement in over 80% of the cases reported were aimed at finding and stealing medical patients' records.

TrapX has collected additional technical telemetry on the attackers which it has shared with the appropriate entities.

# Case Study #2

# How Hospital Medical Devices Are Transformed Into Internal Staging Points

**Overview:**

The TrapX DeceptionGrid solution was deployed in an American hospital with four state-wide locations.

TrapX decoys were deployed inside the VLANs of the medical device networks and the IT corporate network.

After several hours, when the medical decoys were part of the network and acted as medical devices (from a network perspective,) malware touched a medical device decoy and tried injecting malicious files into it.

The moment the decoy was touched by the attacker, the TrapX platform automatically generated the first high-confidence alert

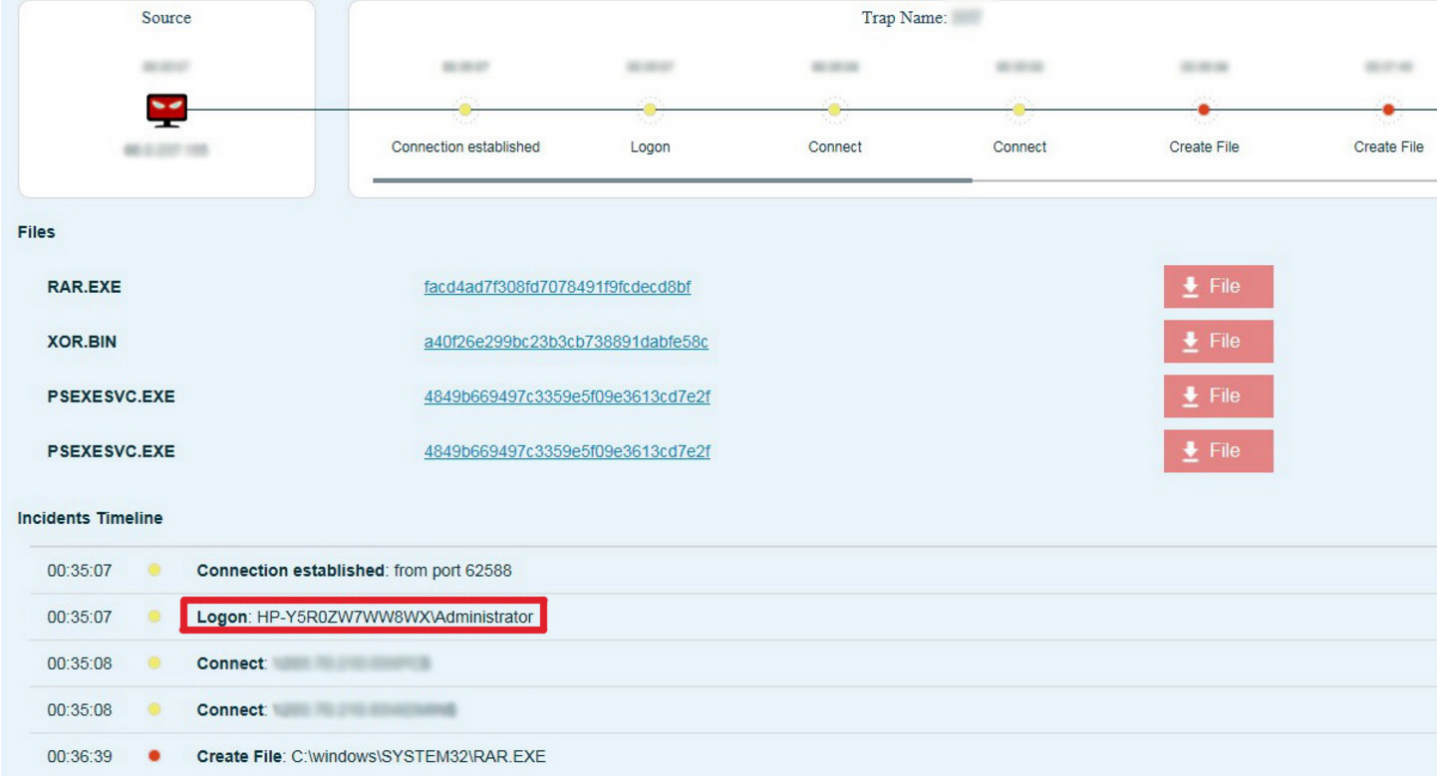
The alert showed:

An MRI device was compromised through an internal IT desktop and began acting as a staging point that allowed the attacker to execute multiple attacks against the hospital's internal network.

The attacker gained administrator access to this medical device using a well-known exploit. (The medical device runs windows XP)

The attacker used this medical device to run more attacks against the network using the "pass-the-hash" attack that leverages the PSEXEC tool and other malicious payloads.

**This screenshot of the TrapX alerts shows the various binaries which infected the trap:**




**Analysis:**

• The pass-the-hash attack injected two malicious payloads. One of them, (RAR.EXE) is a well-known threat from the Win32.Parite.A family. (The second one is unknown to this very day.)

**The threat behavior was as follows:**

• The file was a 32-bit portable executable application. In addition, it was identified as UPX 0.60-3.x.

• The application used the Windows graphical user interface (GUI) subsystem, while the language used was Russian.

• This threat was a polymorphic malware virus that infected .EXE and .SCR files in all of the drives and network shares in the victim's machine.

• The malware virus spread via infected local drives, removable drives, e-mails and network shares.

• The malware virus dropped a UPX packed executable in the user temporary directory and executed it.

• The file was a DLL. The DLL was injected into the EXPLORER.EXE process, thereby keeping the malware resident in memory.

Part of the medical devices had a mapped network share to a central server where medical files are saved (for instance: medical images). The malware attempted to take advantage of this network share and compromised these servers as well, using the same spreading method.

In our case, the malware virus used an administrator account that allowed the attacker to access more medical devices from the same vendor. However, the TrapX DeceptionGrid alert allowed the security team to mitigate the attack quickly and avoid any further damage.

Here's the sandbox analysis link: http://www.trapx.com/wp-content/uploads/2018/03/analysis.pdf

# Case Study #3

# Anatomy of a Medical Device Hijacking

**Overview:**

The TrapX DeceptionGrid solution was deployed in a site of one of the largest hospital networks in the world.

TrapX decoys were deployed inside the VLANs of the medical device networks and the IT corporate network.

Immediately after deployment, malware touched a medical device decoy and tried injecting malicious files into it.

The moment the decoy was touched by the attacker, the TrapX platform automatically generated the first high-confidence alert

**This discovery:**

• The malware specifically targeted medical devices with older operating systems (WinXP or Windows Server 2003).

• The malware also ignored newer 2008-2012 operating systems.

• The primary medical system that was targeted was the PACS image viewer machine[4].

4 Choplin R (1992). "Picture archiving and communication systems: an overview". Radiographics. 12: 127–129.

- The PACS machine has access to a huge repository of medical records and patient images.
- The attacker used a backdoor to establish C&C within a PACS image viewer.

**Analysis:**

Upon a review of forensics and analysis, our security operations team determined that the attacker's malware tools were specifically targeted to older operating systems including Windows XP and Windows Server 2003, which are typical for medical devices. The malware tools were specifically programmed to ignore the newer 2008/2012 operating systems.

The malware Win32.Kido was wrapped and repackaged for delivery. The payload was sophisticated and included anti-VM (sandboxing) and anti-debugging code to avoid detection. The malware scanned the network every three hours to further the spread to other medical devices.

The MD5 File Hash identified was: 378a2915bcec89903faaf5cff2138740 which was attempting to exploit a weak SMB protocol attack.

The malware tool infected systems across the network by exploiting a vulnerability in the Windows service (svchost.exe). Generally, if this vulnerability is successfully exploited, it could allow remote code execution when file sharing is enabled. We noted that the malware could also spread via removable USB drives; meaning it could easily cross firewalls and segmented networks in this manner. The malware attempted to further propagate by using the pass-the-hash technique and also using dictionary attack methods on the affected systems.

PE sections

| Name | Virtual address | Virtual size | Raw size | Entropy | MD5 |
|---|---|---|---|---|---|
| UPX0 | 4096 | 16384 | 0 | 0.00 | d41d8cd98f00b204e9800998ecf8427e |
| UPX1 | 20480 | 90112 | 87552 | 7.80 | d8aba1a456b51bcb836b5fdfb8cd64f3 |
| UPX2 | 110592 | 4096 | 512 | 3.61 | e6a091622f6731108f0a22ebeb9bd38e |

The malware was rewrapped with a UPX packer to hide its internal components.
The TrapX Labs forensics team unpacked the file and uncovered the new MD5 hash: ae538bfa64c71ab338692d60ea709451.

**The malware exposed interesting Windows API functions:**

1. IsDebuggerPresent – Detecting if the malware is running in a debugger.

2. GetProcAddress - Retrieves the address of a function in a DLL loaded into memory.

3. LoadLibrary - Loads a DLL into a process that may not have been loaded when the program started.

4. VirtualAllocEx - A memory-allocation routine that can allocate memory in a remote process. Malware sometimes uses VirtualAllocEx as part of process injection.

**Other characteristics of the malware included:**

1. Propagation - Attempts to clone a copy of itself in a remote computer's ADMIN$ share:

2. The copying is done by using the credentials of the currently logged-in user on the system that the Malware is executed on.

If the above process fails (or the current user doesn't have rights) the Malware will do the following:

1. Enumerate users on the remote system.

2. Use a combination of weak passwords to attempt to login to the remote system.

3. Persistence – Adds itself to the Windows autorun.

4. In subkey: HKCU\Software\Microsoft\Windows\CurrentVersion\Run.

5. Sets value: "<random string>".

6. With data: "rundll32.exe<system folder>\<malware file name>.dll, <malware parameters>".

7. Persistence - it may also load itself as a service that is launched when the netsvcs group is loaded by the system file svchost.exe.

8. Registers itself under the registry key: HKLM\SYSTEM\CurrentControlSet\Services.

9. Remote Scheduled Job – After an infection of a remote system it will create a schedule task job to execute itself.

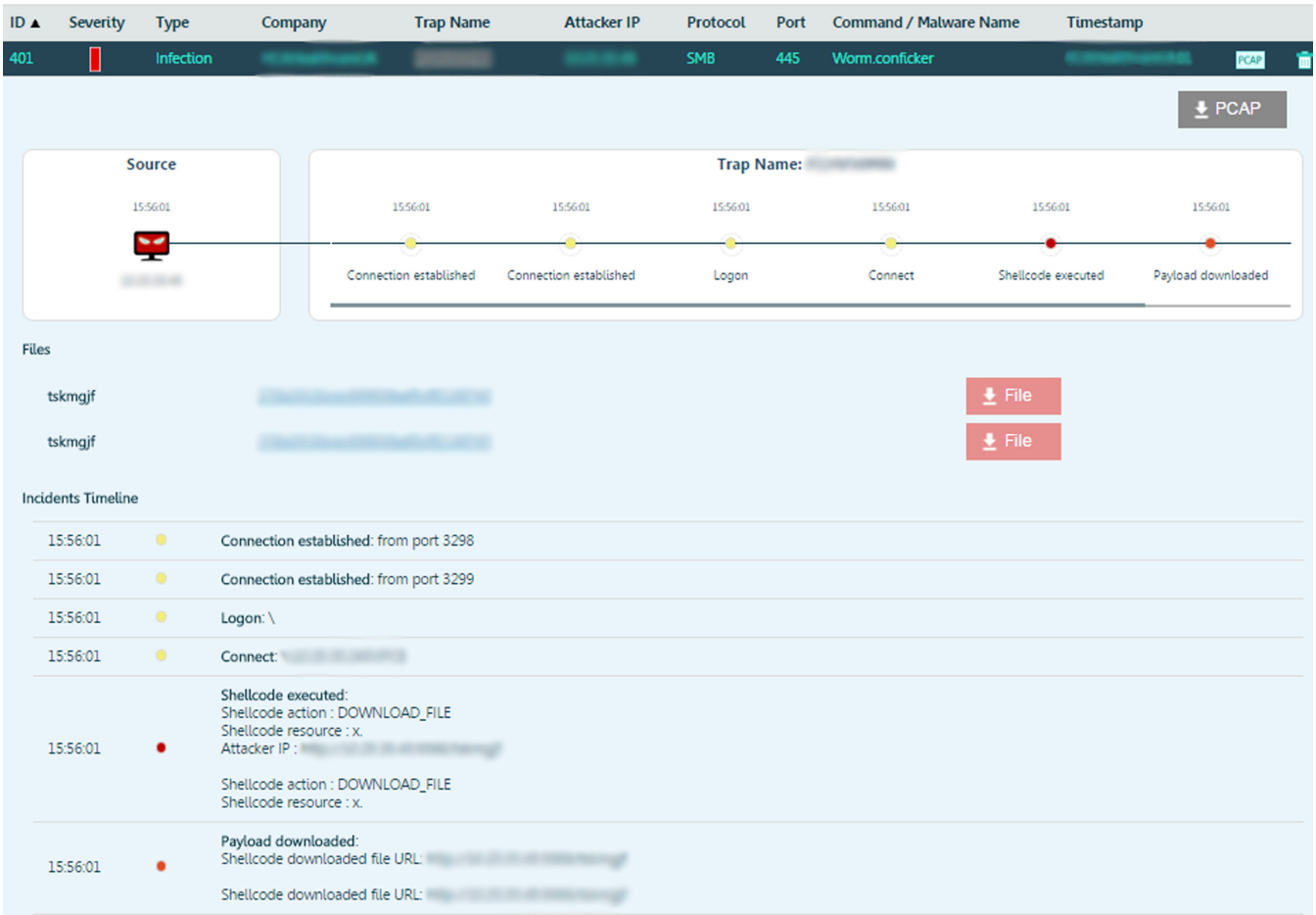
10. Mapped and Removable Drives - may clone a copy of itself in all mapped and removable drives using a random file name.

11. HTTP call back – C&C connection to an external server (IP based connection).

12. An internal desktop which was initially infected also seems to have been used as a C&C server.

13. Resets system restore point - may reset system restore points likely to prevent the victim using system restore.

**The infection screenshot:**




**Remediation:**

The attacker was also controlling the attack from the domain www.andtermsreviewing.ru.

Once identified, the hospital SOC team blocked the domain and subsequently worked with the manufacturers to clear the malware from all devices.

# Case Study #4

# MEDJACKING Traced To International Hacker Involvement

**Overview:**

This case study involved a medium-sized hospital with a little more than 500 beds. This hospital had several layers of security on the perimeter and in their internal network.

The TrapX DeceptionGrid was installed and instantly alerted their SOC team about probes emanating from attacker command and control locations on their radiology medical devices.

The medical system components were as follows: Six of them were located on the same network VLAN where the TrapX medical decoys were installed. Within minutes, we got six infections with the same malicious code. Every single one of the medical machines were compromised and were fully controlled by the same malware. (see the attack visualization below)

All of the medical devices were running windows XP.

These radiology medical devices had safety guidelines that were enforced in order to protect the patients; but when the system was fully controlled by the malware, these safety rules were not enforced. That is what happens when attackers [secretly] manipulate the system.

**Analysis:**

The malware behavior was as follows:

**Indicators:**

1. Search: Enumerates or collects information from a system - checks operating system version.

2. Settings: Tampers with system settings - enumerates system information.

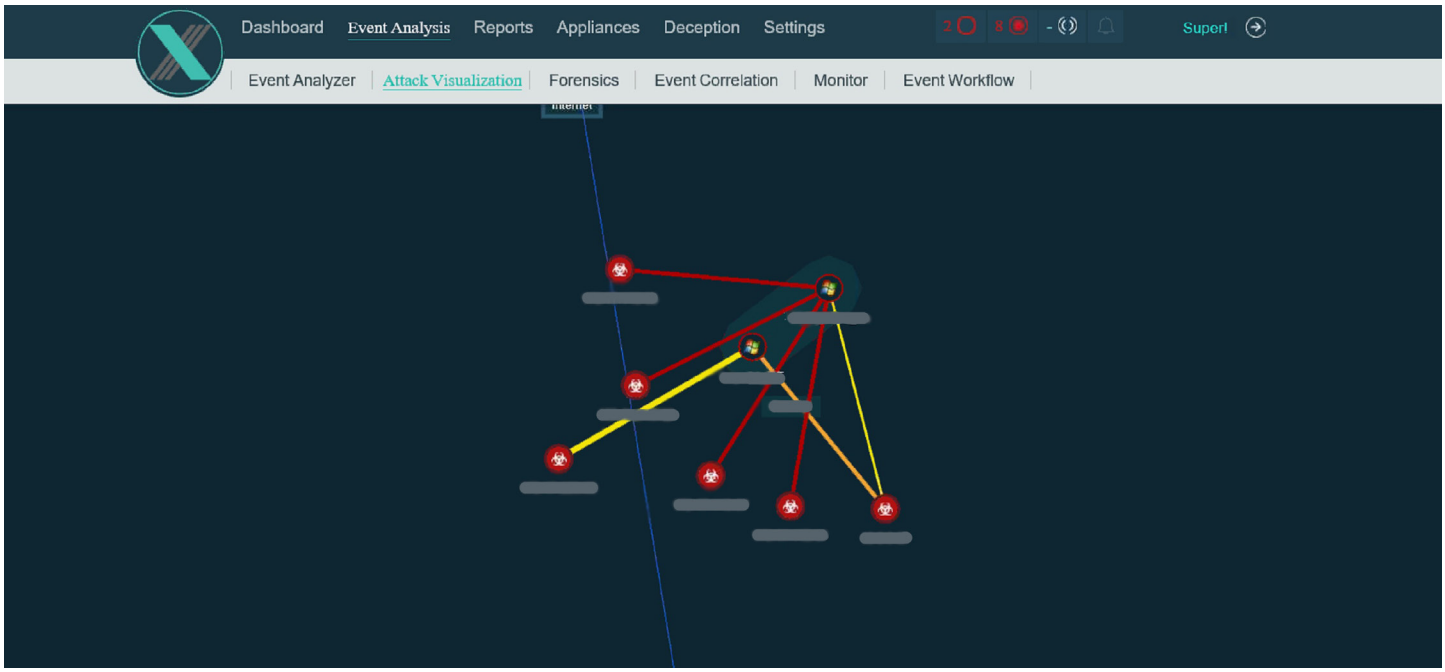
3. Monitor: Able to monitor host activities - tampers with keyboard/mouse status.

4. Execution: Creates other processes or starts other applications - might load additional DLLs and APIs.

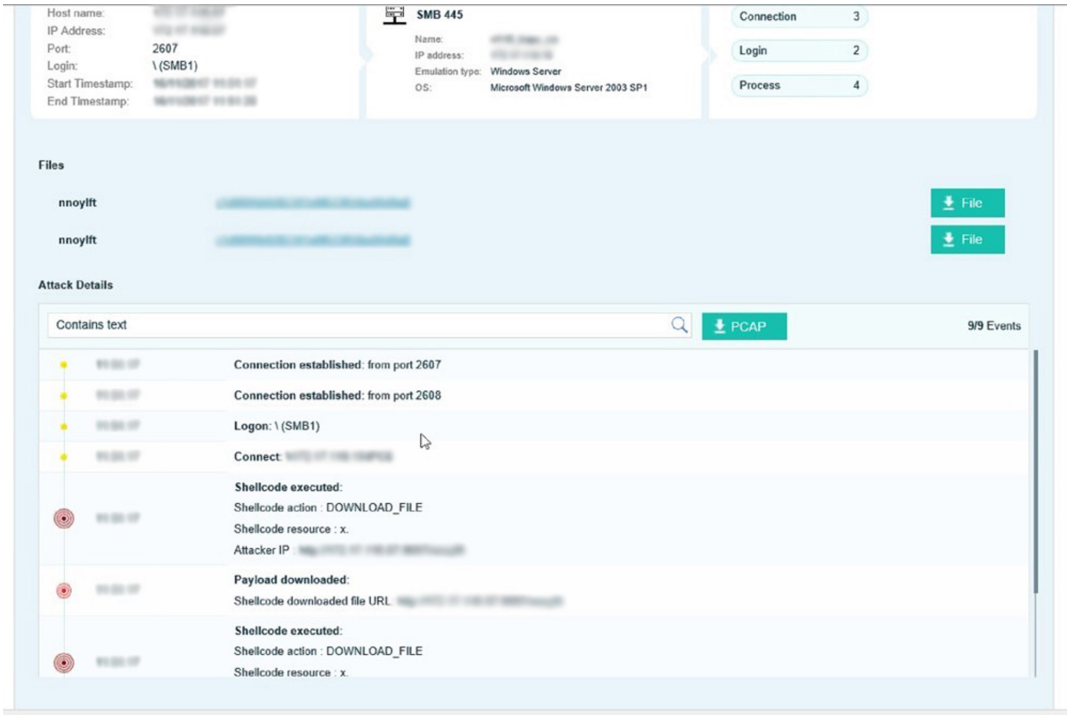
5. Steal: Steals and leaks sensitive information – accesses the clipboard.

6. Spread/infection: using windows SMB vulnerability - spread across the network.

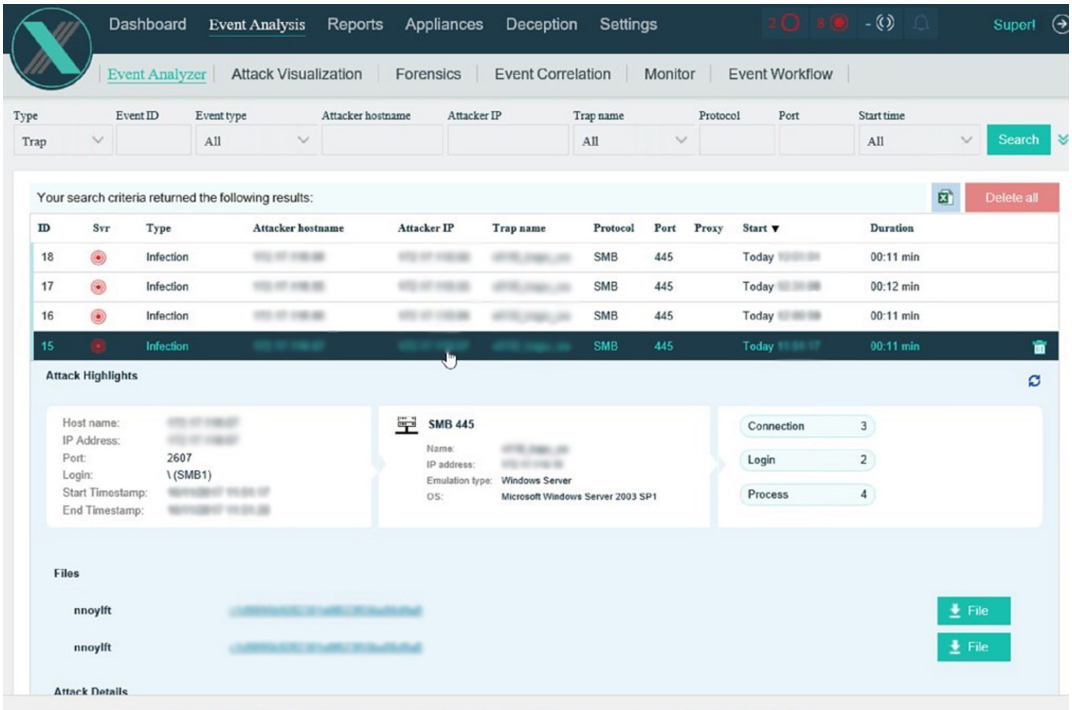
**The TrapX attack visualization tool, demonstrates the malware's lateral movement. Here, we can see the infection stage of two TrapX decoys that were triggered from six different medical machines. The red dots represent infected systems and the windows icons represent traps.**



**Here is a screenshot of a DeceptionGrid alert showing the device with the malicious payload:**




**Here is a screenshot of a DeceptionGrid alert showing another infected device:**



# MEDJACK.4 - Conclusions

The MEDJACK attack vector has the potential to distort or change internal data in medical devices. Based on our investigation and analysis, discussions with the relevant IT teams, hospital staff, and medical device manufacturers, our conclusion is that measurements produced by the devices can usually be manipulated. We have validated this in our simulated attack environment on a blood gas analyzer where we recreated and documented the attack vectors.

**It should also be noted that:**

1. Medical devices are essentially "closed" devices. They must maintain strict compliance with FDA regulations. Medical devices cannot be easily monitored nor is there any real visibility into internal activity by cyberattackers or their malware tools. The extreme vulnerabilities within medical devices render components of the hospital's cybersecurity technology less effective.
2. Medical devices generally have older, embedded processors that are not updated frequently and sometimes never updated.
3. Simpler medical devices are internet of things (IoT) enabled, and are even more difficult to monitor and protect.
4. When the compromise of a medical device is detected, it is tremendously time-consuming to take the device offline, to have the manufacturer completely rebuild the software and then bring it online again. This presents unplanned and unbudgeted financial burdens for hospitals that are already under duress.
5. Even after remediation, most medical devices are exploited again immediately - unless all of the medical devices on the same network are shut down and also remediated. These devices can provide cyberattackers instant access to freshly rebuilt devices.
6. Ransomware has emerged strongly as an attack vector impacting healthcare institutions in 2017 and this trend will continue to rise through 2018.

We have also noted that cyberattackers have evolved their techniques to help mask old / easily detectable malware threats as new malware. This technique of obfuscating malware, rapidly enables attackers to create new malware software. The new malware code is camouflaged, remanufactured, and rendered invisible to detection and defense techniques. This malware can then be deployed again and again to repeatedly attack healthcare institutions.

For these reasons and the convergence of medical devices, IoT connectivity, embedded processors and outdated operating systems, healthcare institutions today remain highly vulnerable. These exploits can be resident within medical devices in hospitals and evade most cyberdefense software for extended periods of time. Cyberdefense software cannot be resident within the medical devices nor can it easily provide visibility to potential attacker activity. The IT teams cannot see any threats.
In fact, these attackers are sitting quietly within the networks and medical devices. They easily steal sensitive data, modify equipment readings and completely disrupt hospital operations.

# Recommendations & Best Practices

Our recommendations for healthcare networks include the use of new best practices and the technologies that support them to keep medical devices clean from cyberattacker exploits.

**Recommendations:**

1. Isolate and remediate groups of medical devices on the same network. If one medical device gets impacted by cyberattacker activity it is likely more medical devices are impacted.

2. Make sure your maintenance contracts include responsibility for the remediation of medical devices impacted by cyber threats. The cost for this can be really expensive for small hospitals and health institutions (unless it is explicitly defined in your medical devices' maintenance agreements.)

3. Make sure you review all of your medical devices and understand their vulnerabilities and system life expectations in terms of cyberdefense. It may be simpler to replace some devices than to upgrade their software. Medical devices often have system lives of five to ten years. The cybersecurity industry however, moves at a much faster pace - in response to escalating cyberattacks.

4. Cybersecurity expenses will most likely increase in your security operations budgets. These cyber threats may not have been anticipated five to ten years ago, but here they are. Your budget for cybersecurity will most likely be higher than it was ten years ago.

5. Hire an outside contractor to do regular, periodic Red Team reviews of your network security and to independently evaluate your medical devices, servers, and endpoints for active compromises. This also supports your risk assessment for your HIPAA compliance.

6. MSSPs that specialize in healthcare can be a good supplement to your inside team. They can also do the regular and necessary audits.

7. Isolate medical devices to the greatest practical extent, ideally behind their own firewalls in a separate network.

8. Network micro-segmentation can help to restrict lateral movement which emanate from within the medical devices.

9. Identify and utilize a technology designed to provide visibility to attackers that have evaded your firewalls and endpoint security but have gained residency and access within your network and sit within your medical devices.

**The right deception technology can provide this capability for your information technology team. Support for emulated medical devices is highly important as these can immediately attract and foil potential attackers.**

# Notice

TrapX Security reports, white papers and legal updates are made available for educational purposes only. It is our intent to provide general information only. Although the information in our reports, white papers and updates is intended to be current and accurate, the information presented herein may not reflect the most current developments or research.

Please note that these materials may be changed, improved, or updated without notice. TrapX Security is not responsible for any errors or omissions in the content of this report or for damages arising from the use of this report under any circumstances.

# Disclaimer

The inclusion of the vendors mentioned within the report is a testimony to the popularity and good reputation of their products within the hospital community and our need to accurately illustrate the MEDJACK.4 attacks.

Medical devices are FDA approved devices and additional software for cyber defense cannot be easily integrated internal to the device especially after the FDA certification and manufacture.

We have worked in strict confidence with healthcare institutions documented in these case studies to identify and remediate current and future cyber attacks. Information released which pertains to specific medical devices is done solely to understand and illustrate the details of the MEDJACK and MEDJACK.4 attack vectors.

Please note some of the information technology, servers, firewalls, networks and medical device equipment were several years old. Notwithstanding the hospital's best intentions, both the information technology and medical devices may not have been maintained or installed in accordance with manufacturer recommendations. Required software updates and improvements to these devices, that may have reduced or eliminated cyber attacks, may not have been installed. Network configurations and firewall set-ups that may have reduced or eliminated cyber attacks, may not be in place. Current best practices may not have been implemented - this is in some cases a subjective determination on the part of the hospital team.

New best practices that utilize advanced threat detection techniques such as deception technology are relatively new to hospitals, and only recently available for commercial deployment.

Finally, we would note that TrapX Labs personnel involved with the cyber security initiatives described herein are not certified or trained by the medical device manufacturer. We do not know if the hospital personnel involved in supporting our efforts during our proof of concept deployments were trained or certified on the equipment.

# About TrapX Security

TrapX Security is the pioneer and leader in cyber deception technology. Their DeceptionGrid solution rapidly detects, deceives, and defeats advanced cyberattacks and human attackers in real-time. The DeceptionGrid also provides automated, highly accurate insight into malicious activity unseen by other types of cyber defenses. By deploying the DeceptionGrid, you can create a proactive security posture, fundamentally halting the progression of an attack while changing the economics of cyberattacks by shifting the cost to the attacker. The TrapX Security customer-base includes Forbes Global 2000 commercial and government customers worldwide in sectors that include defense, healthcare, finance, energy, consumer products, and other key industries. Learn more at www.trapx.com.

## Contact Us

TrapX Security, Inc.,

3031 Tisch Way,

San Jose, CA 95128

+1–855–249–4453

www.trapx.com

For sales: sales@trapx.com

For partners: partners@trapx.com

For support: support@trapx.com

**Trademarks**



## More Information

Visit the TrapX Website: www.trapx.com

Learn more about DeceptionGrid: www.trapx.com/product/

Visit the TrapX blog: www.trapx.com/blog/

Follow TrapX on Twitter: @trapxsecurity

Follow TrapX on LinkedIn: www.linkedin.com/company/trapx

Like TrapX on Facebook: www.facebook.com/TrapX-Security-258804147648401/