MICROSOLVED,INC.

XP Survival Guide

Staying alive with a target on your back (March 2015)

Reliability. Stability. That is what the Windows XP operation system provided as the IT platform at the Operator Interface, Engineering and Information Management level for a variety of industrial control systems.

You have maximized the useful life of the system. Yet due to circumstances that vary from an imminent plant closing to extended budget cycles, the reliable operation of your plant depends upon an unsupported DCS / ICS and operating system.

What is the cyber risk to such a system? Aside from potential hardware failures, there is a concern for the increased level of vulnerability that is present due to known flaws in Windows XP that could be exploited. This wouldn't be as much concern five years ago, but in 2015 the threat landscape has changed drastically and consideration must be given to how much risk you are accepting with the current security policies and controls in place.

This white paper was written to help you assess and address the cyber risk associated with XP based platforms. We have provided a very pragmatic approach to guide your efforts in exercising "due care" in your specific circumstances.

If you would like to discuss these recommendations with us, we welcome your email or phone call. Please use the contact information at the end of this white paper.

It’s after April 2014 and you are now where you never wanted to be: dependent on Windows XP after all support (including security support) is gone.

You are not alone - but that will be cold comfort if your operational ability is affected by an XP flaw that causes an outage. That could happen as a result of an external attacker, malware, or simply from an internal procedural error that triggers an XP flaw.

This guideline is intended to help you mitigate that risk while you migrate away from XP.

XP – Your Vulnerable Child:

If several members of your family were diagnosed to be uniquely susceptible to an infectious disease, you would take actions to protect them.

You would:

1. Verify that that the diagnosis is true
2. Identify and locate all affected family members
3. Educate the family on the condition
4. Minimize the chance for your susceptible family members to become infected
5. Ensure you detect the initial stages of infection
6. Plan for recovery from the infection

Your XP systems are these unfortunate “family members” in your information infrastructure.

Let’s see what we can do for them using the approach outlined above.

1. Verify that You in Fact Have Unsupported XP

That you have XP is a given. That you must have unsupported XP is not.

There are continued support options for XP available to a select few organizations with special circumstances or deep pockets.

- Users of the "Windows Embedded Industry" version of XP have up to 2019 for extended support.

  See:

  http://www.microsoft.com/windowsembedded/en-us/industry.aspx

  http://en.wikipedia.org/wiki/Windows_Embedded_Industry

- "Custom Support" arrangements are available from Microsoft. They are **expensive** but may make sense in individual cases.

  See:

  http://support.microsoft.com/gp/lifepolicy

  http://www.microsoft.com/en-us/microsoftservices/support.aspx

  http://www.techrepublic.com/blog/european-technology/keeping-xp-on-life-support-will-uk-nhs-drag-it-out-for-another-year/

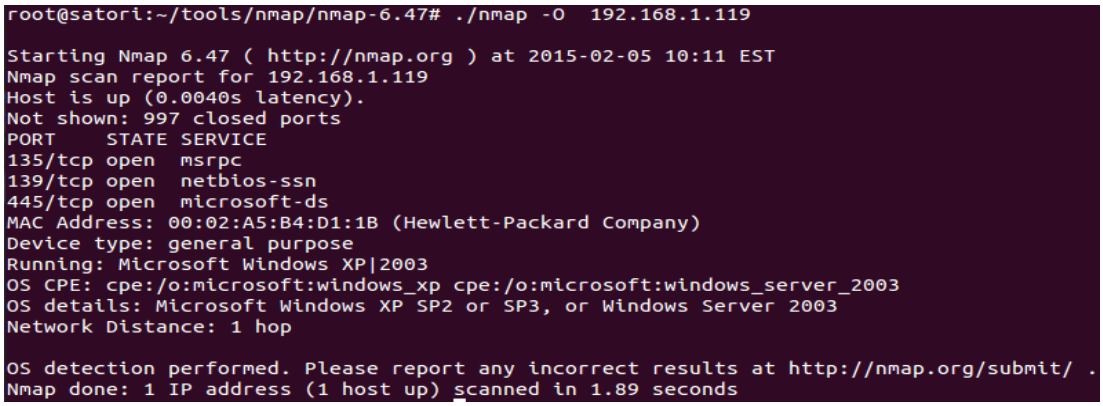
The rest of this guide assumes you unfortunately live in the real world and the options above are not available.

2. Find Your XP Systems

- **Identify**

  Verify that you have an accurate inventory of all your XP systems. Do Internet searches about your ICS devices to determine OS type and consult with your vendors. Be aware that XP can be the underlying embedded OS in many "hidden" devices. You will almost certainly have XP running in places you would not expect.

  If your environment is sufficiently robust, perform active network based assessments using tools like **Nmap** to look for XP signatures. The example below shows the discovery of a system that is running either XP or Windows 2003 server. Either is an issue as XP is already unsupported (April 2014) and Windows 2003 soon will be (June 2015).

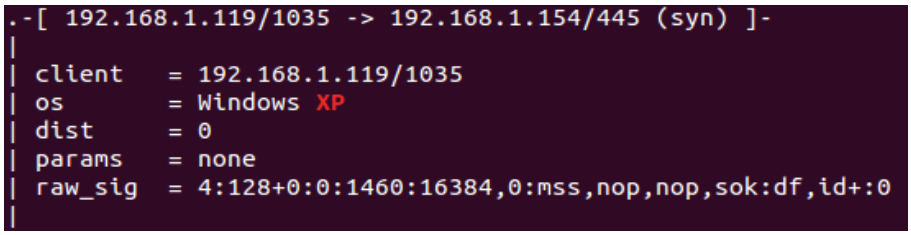


  NOTE: ICS equipment can be sensitive to such scans, and they are often avoided for fear of causing outages.

  If you are concerned about the effects of such active scanning in your ICS environment, consider "passive" OS detection.

  Simply by examining network traffic over time, the existence of XP can be revealed. Where you find one instance, expect more that are not being detected.

  Ethernet hubs or switch ports set up for "port mirroring" can be used to collect traffic for a passive monitor, eliminating any risk to running systems from active scans. Tools like "p0f" and the Nessus "Passive Vulnerability Scanner" can be used to capture relevant information and identify XP systems. Below is an example of a p0f identification of an XP system (192.168.1.119) based solely on network traffic captured passively by tcpdump and then analyzed by p0f.



- **Reduce**

  It is invariably true that in complex environments systems become orphaned, consuming electricity but performing no useful function.

  For some of us, that family-member analogy may be uncomfortably accurate.

  Verify the purpose of all inventoried XP systems and shut down those that are unneeded or whose functionality can be consolidated or moved to a supported environment.

  If a system is a convenience but not a necessity, move it to a network location outside your more sensitive areas.

- **Document**

  Once you have an inventory of needed XP systems, keep it current. All new equipment being introduced into your environment should have its operating system identified and added to the inventory.

See:

http://nmap.org/book/man-os-detection.html "Active" OS detection

http://lcamtuf.coredump.cx/p0f3/ "Passive" OS identification

http://www.tenable.com/products/passive-vulnerability-scanner/features Nessus

http://en.wikipedia.org/wiki/Port_mirroring Obtaining all network traffic passively

http://en.wikipedia.org/wiki/Tcpdump Command line network traffic capture tool

http://en.wikipedia.org/wiki/Wireshark Graphical traffic capture tool

3. Educate Your Employees and Support Vendors

The awareness and training of employees and vendors will do more to protect your environment from the risks of XP and software problems in general than any purely technical control.

- **Awareness**

  Vendors and staff should be made aware of the basics of computer and network security. They must understand that all external interactions that could affect XP systems, such as web browser usage, email usage, FTP, and media from external sources (e.g. USB sticks, smartphones, web downloads, email attachments), are a threat. This has to be re-iterated – it cannot be a one-time sign-off on some document that will be ignored. Frequent awareness messages to ICS and vendor staff can keep the issue alive. Consider deploying information security awareness posters in sensitive locations.

- **Anomaly Reporting**

  All anomalies that are encountered by staff when interacting with computing infrastructure should be reported. Non-disruptive but unusual behaviors are often the first indicators of serious problems, including security breaches. Multiple reports from different ICS locations can alert security staff to broad patterns and give you time to begin effective containment. A formal reporting mechanism used by all ICS staff should be in place and those reports should be consistently reviewed by security staff.

- **Authority**

  Staff should be trained not only to ensure their own correct behaviors, but also to recognize risky behavior in others, particularly vendors. They must all be trained to question – and if necessary, stop – actions that could cause a software disruption. This behavior should be rewarded.

- **Inter-Group Communication**

  IT Security and ICS staff must meet regularly to discuss current security issues. The intent of these meetings is to ensure that concerns from both sides are heard. These discussions should not only deal with XP issues, but should address all issues affecting ICS security. Security staff must understand the practical concerns of the ICS world and ICS staff must understand the reality of the growing information security threat to that world.

Having folks read and then discuss the various analyses of Stuxnet and similar ICS-specific events is probably one of the best ways to raise a common awareness and an understanding of the need for cooperation between groups.

See:

http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

http://www.theregister.co.uk/2014/12/22/hackers_pop_german_steel_mill_wreck_furnace/

http://www.oas.org/cyber/documents/ENISA%20-%20Can%20we%20learn%20from%20SCADA%20security%20incidents%20-%20White%20Paper.pdf (Stresses need for inter-group communication)

4. Minimize the Chance for the Compromise of Remaining Systems

In information security language this is often referred to as reducing your "attack surface". If you have the ability to safely modify your XP systems to make them less susceptible to attack, you should do so.

- **Establish a Security Baseline**
  - **Install all current vendor maintenance**

    Your ICS device vendors may have specific recommendations on bringing their XP-dependent systems to current security maintenance levels. Consult with them before making any changes. If possible, apply all necessary vendor maintenance.

  - **Install Microsoft's XP Service Pack 3 (SP3) and all current security patches**

    If possible, without disrupting service, go to XP Service Pack 3 (SP3) and apply all post-SP3 security patches.

    As of the time of this writing (January 2015), SP3 remains available as well as all XP security patches up to April 2014.

    See:

    http://support.microsoft.com/kb/322389 (SP3)

    https://windowsupdate.microsoft.com (Manual update – IE required)

    http://xdot.tk/ (Tool for manual download of security patches)

    http://answers.microsoft.com/en-us/windows/forum/windows_xp-windows_update/will-there-be-a-final-update-roll-up-aka-sp4-for/01dfac2c-7184-4296-ad0b-bcea20d59e41 (Create a CD with all security maintenance)

    http://www.expertreviews.co.uk/software/1306762/how-to-slipstream-an-xp-disc-with-sp3-and-all-other-updates (additional on CD creation)

  - **Install antivirus and/or malware protection**

    Several antivirus and malware protection vendors continue to provide some support for XP. If you can install an antivirus or malware detection package without disruption, do so. Be aware that traditional antivirus will become increasingly less effective for XP over time.

    See:

http://www.cnet.com/news/still-running-windows-xp-antivirus-products-put-to-the-test/

http://www.techrepublic.com/blog/10-things/10-ways-to-detect-computer-malware/

https://www.malwarebytes.org/ "Malware detection" as opposed to antivirus. Malwarebytes has proved itself useful for XP.

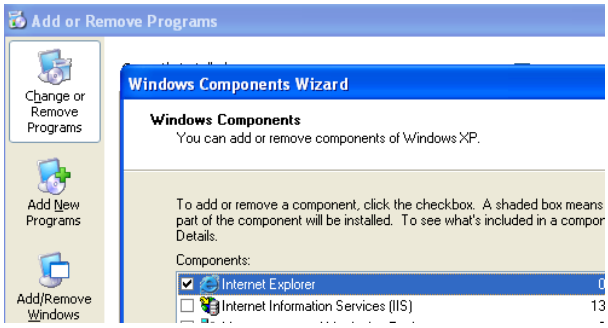
- **Remove Unneeded Software and Disable Unneeded Hardware**

  This should be done on test systems If possible (virtual machines perhaps), and the effect of removals should be evaluated.

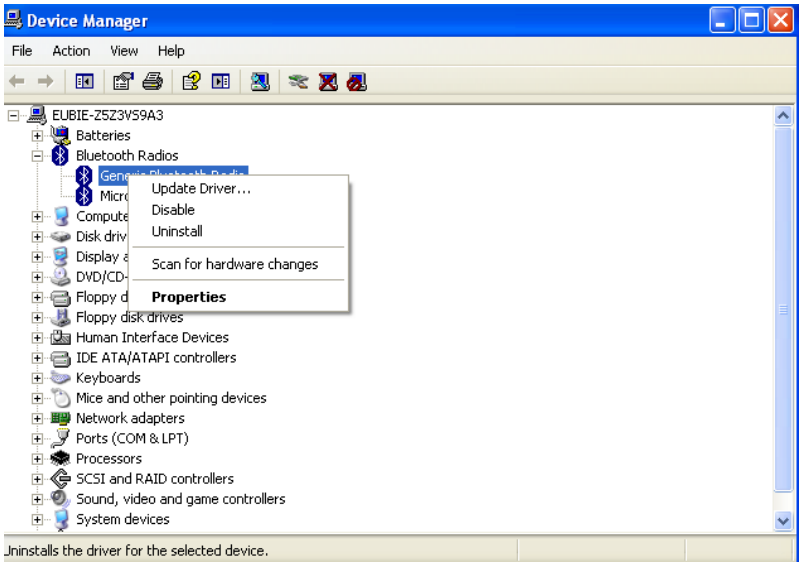
  Remove or disable all unneeded software that allows employees to interact with external systems.

  - Web browsers (see note below on browsers)
  - FTP, telnet, mail, chat and similar clients

  You can remove unneeded programs with "*Control Panel/Add or Remove Programs*". In the example below, Internet Explorer is removed.



  You can disable support for unneeded hardware potentially useful to an attacker with "*My Computer/ Properties/Device Manager*". In the example below, Bluetooth is disabled.



- **If a Browser is Absolutely Required, Use Firefox, Opera or (Possibly) Chrome**

  Internet Explorer is no longer supported on XP and is a chronic source of security problems. The browsers listed above continue to support the most recent version of XP. Firefox with the "Noscript" add-on can further reduce your risk by minimizing the opportunity for malicious content or cross-site scripting vulnerabilities to be exploited. Chrome is feature-rich and for that reason potentially unsuitable in an ICS environment.

  See:

  https://www.mozilla.org (Firefox)

  http://en.wikipedia.org/wiki/NoScript (Limits active content allowed)

  http://www.opera.com (Opera)

  http://www.google.com/chrome/ (Chrome)

- **Limit External Network Exposures**

  The network services offered by your XP instances will be a primary vector for attack and the spread of malware. By reducing the number of such exposures you will significantly reduce your risk.

  Determine the purpose for every network exposure offered by the XP system and if unneeded, remove the software creating the exposure.

  You can check locally at the command line via: *netstat –ano"*

```
C:\Documents and Settings\eubie bundew>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1012
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:1030         0.0.0.0:0              LISTENING       1472
  TCP    192.168.101.130:139    0.0.0.0:0              LISTENING       4
  UDP    0.0.0.0:445            *:*                                    4
  UDP    0.0.0.0:500            *:*                                    760
  UDP    0.0.0.0:1025           *:*                                    1288
  UDP    0.0.0.0:1026           *:*                                    1288
  UDP    0.0.0.0:1034           *:*                                    1288
  UDP    0.0.0.0:4500           *:*                                    760
  UDP    127.0.0.1:123          *:*                                    1188
  UDP    127.0.0.1:1900         *:*                                    1464
  UDP    192.168.101.130:123    *:*                                    1188
  UDP    192.168.101.130:137    *:*                                    4
  UDP    192.168.101.130:138    *:*                                    4
  UDP    192.168.101.130:1900   *:*                                    1464
```

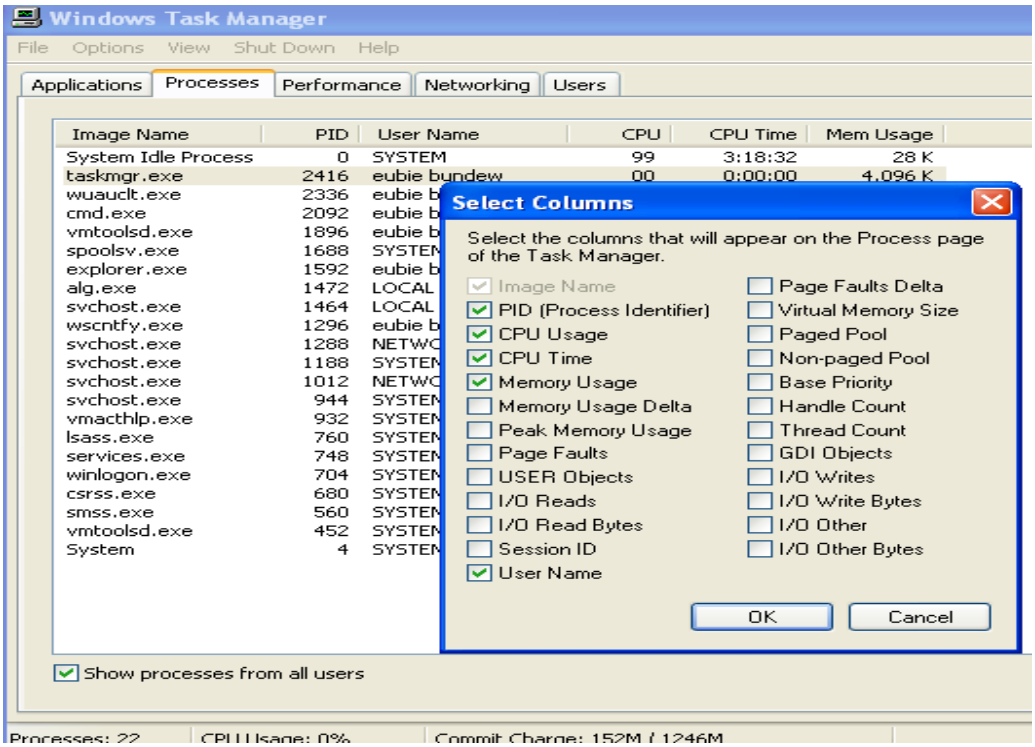
The “process ID” of running programs with network exposures will be listed.

The list of programs associated with those process IDs can be found via: *tasklist/svc*

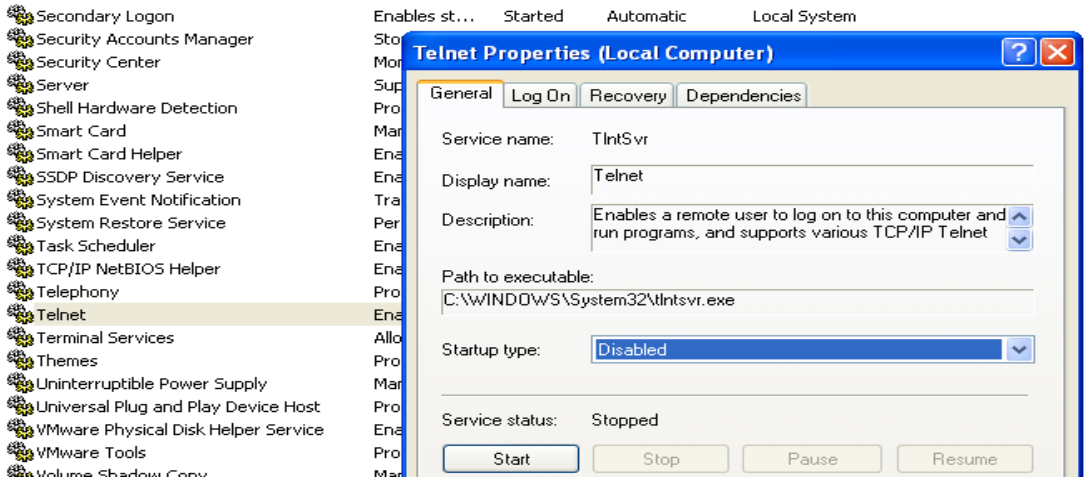
```
C:\Documents and Settings\eubie bundew>tasklist /svc

Image Name                     PID Services
========================= ====== ============================================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       560 N/A
csrss.exe                      680 N/A
winlogon.exe                   704 N/A
services.exe                   748 Eventlog, PlugPlay
lsass.exe                      760 PolicyAgent, ProtectedStorage, SamSs
vmacthlp.exe                   932 VMware Physical Disk Helper Service
svchost.exe                    944 DcomLaunch, TermService
svchost.exe                   1012 RpcSs
svchost.exe                   1188 AudioSrv, BITS, CryptSvc, Dhcp, dmserver,
                                   ERSvc, EventSystem,
                                   FastUserSwitchingCompatibility, helpsvc,
                                   lanmanserver, lanmanworkstation, Netman,
                                   Nla, Schedule, seclogon, SENS, SharedAccess,
                                   ShellHWDetection, srservice, Themes, TrkWks,
                                   W32Time, winmgmt, wscsvc, wuauserv, WZCSVC
svchost.exe                   1288 Dnscache
svchost.exe                   1464 LmHosts, RemoteRegistry, SSDPSRV, WebClient
explorer.exe                  1592 N/A
spoolsv.exe                   1688 Spooler
vmtoolsd.exe                  1896 N/A
vmtoolsd.exe                   452 VMTools
alg.exe                       1472 ALG
wscntfy.exe                   1296 N/A
wuauclt.exe                   2336 N/A
cmd.exe                       2092 N/A
tasklist.exe                  2552 N/A
wmiprvse.exe                  1092 N/A
```

Alternatively, you can use the Windows task manager GUI to identify running processes. Note in the example below that the option to show processes from all users is selected. You can select what values are displayed via the “select columns” options menu.



You can selectively disable unneeded Windows services responsible for those exposures via: *Control Panel / Administrative Tools / Services*. In the example below, the Telnet service is disabled:



- **Use an Onboard Firewall to Restrict Exposures**

  An onboard software firewall is available on all desktop versions of XP.

  Prior to SP2 it is available at: "*Control Panel / Network Connections / Properties / Advanced".*

You can tightly control what TCP/IP service exposures your XP instances offer to the local network and ensure that they are only those needed for required function. You can test those exposures with the netstat command described above or by using port scanning tools like nmap.

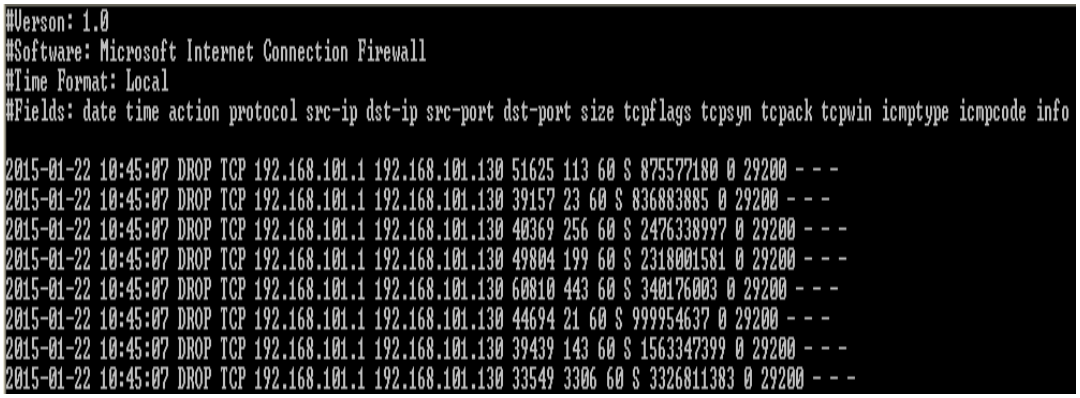
A local log file can be optionally written to by the Windows firewall: C:\Windows\pfirewall.log.

See:

http://ecross.mvps.org/howto/overview-of-the-windows-firewall-security-log-file-in-windows-xp.htm

That log can record all attempts to use network services on your XP system and can be of great aid when tracking down malware.

Below is an example of the Windows XP Firewall Log recording dropped packets from a malicious scan:



Tools exist for "following" such logs and sending information about new entries to a central syslog server.

See:

https://cuit.columbia.edu/cuit/it-security-practices/built-firewalls/turning-windows-xp-firewall-sp1-earlier (XP SP1 or prior)

http://support.microsoft.com/kb/283673 (XP SP2 or later)

http://troy.jdmz.net/syslogwin/ (Syslog for Windows)

Use hardware firewalls where appropriate

If risk justifies the cost, consider deploying hardware ("industrial") firewalls to front-end critical systems. Such firewalls are available from a variety of vendors. They can

be configured to only allow select, approved network traffic from known sources to travel to vulnerable systems. Modern "stateful" firewalls can do further inspection of traffic to ensure allowed traffic is behaving as expected and is not itself being used maliciously. Such firewalls can log to a central repository for analysis and alerting.

See:

http://new.abb.com/network-management/communication-networks/optical-networks/aff650-firewall (ABB AFF 650 firewall)

- **Change Default Vendor Credentials**

  Automated malware and human attackers rely on the common practice of leaving default vendor logins and passwords in place (admin/admin, admin/password, etc.). Vendor documentation (often freely available online with the default listed) may explicitly instruct the installer to change that default, but all too often they do not.

  Google "<your vendor name> default password" for a feel as to how well known those defaults are.

  If at all possible, change those defaults on all your ICS systems, not just XP. Use something complex and unique to your environment. Instruct staff never to store those login credentials in clear text. A hack of the computer on which such credentials are stored opens your whole operation to attack. Various encrypted password storage systems exist. Pick one and use it.

  The same advice applies to SNMP community strings – avoid the defaults of "public" for read access and (much worse but all too common) "private" for write access.

  See:

  http://www.defaultpassword.com/

  http://default-password.info/

  http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

  http://lifehacker.com/5529133/five-best-password-managers

- **Avoid Administrator Account Usage**

  The unnecessary use of the Windows "Administrator" account is the reason why many attacks are successful. A staff member's security error done while logged in as the local admin can immediately allow a malicious web link or file to completely

compromise a system. Software running unnecessarily with "system" privilege that is successfully attacked over the network immediately provides the attacker with full system access.

Ensure staff use non-admin accounts and that all software runs with the least privilege possible.

See:

https://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/windows_security_runas.mspx?mfr=true ("Runas" allows selective use of admin rights)

https://technet.microsoft.com/en-us/library/bb456992.aspx ("Least Privilege" discussion)

- **Segmentation: Network and Business Process Isolation of Your XP Systems**

  This may be the single most effective (read: cost effective) approach you can take in dealing with XP now that you have some idea where it is.

  Multiple regulatory and industry papers advise on this topic, and should be reviewed. But it comes down to this:

  Network Isolation

  Ensure the network segments on which your XP systems reside are as isolated as possible from potential attack sources (e.g. your business network). XP systems should have limited and strictly monitored access from and to the external non-ICS world.

  The onboard and physical firewalls described earlier can help achieve this, but they do not supplant the need for a network architecture that segments your vulnerable systems away from the rest of your enterprise.

  Remote Access

  Staff and vendors who can access your ICS remotely are a particular risk, especially if they are given direct network access over VPN to work with ICS devices from their own personal computers.

  Despite all precautions such user machines are often infected with malware. ICS staff and vendors are also often the direct targets of "phishing" attacks intended to give an attacker control of a laptop that is used for remote access.

ICS systems should ideally be accessed via intermediate "jumphosts" (see the reference diagram below). These jumphosts should be cooperatively configured, maintained and monitored by ICS and ICS-aware security staff. All necessary tools are approved by security staff and stored on the jumphost. File servers enabled with anti-virus can be used to stage the delivery of materials to the ICS environment itself.

Human Isolation

The smallest possible number of staff and support personnel should have access to your ICS XP systems and the systems, networks and media that have access to those systems. Laptops (e.g. contractor laptops) and media used to maintain systems should be strictly limited. A contractor laptop with resident malware can quickly spread that malware throughout your environment.

Staff that do have access should be fully trained as to the risks and know they have the right – and are expected - to enforce the rules. Saying *"You can't do that!"* will NOT get them fired.

Virtualization

If possible, virtualize XP instances and consolidate them on several dedicated, redundant VM servers. Virtualization will not make the XP systems less vulnerable, but it will aid in recovery when the inevitable occurs by allowing quick restore of a VM image.

If virtualization of XP is not possible in production, consider virtualization as a tool for testing your XP remediation.

See:

http://www.vmware.com/products/converter Physical XP to VM conversion

5. Maximize Detection Ability

- **Education**

  As discussed above, educate your staff and vendors.

  Any odd behavior on an ICS computer system should be reported via formal reporting mechanisms.

- **Avoid Information Silos / Turf Battles**

  The friction that often exists between IT Security staff and ICS staff responsible for "keeping the lights on" is a well-known fact. IT people are often seen as dictating security guidelines that simply don't apply in the ICS world. ICS staff is seen as being resistant to basic security considerations that IT sees as fundamental. This causes communication barriers between the staff that can prevent detection of security problems.

  Begin a program now to eliminate any such communication problems in your organization.

- **Centralized Logging and Analysis**

  All systems that can log events should do so to a central log repository. This includes, but is not limited to, ICS XP systems. All firewalls and intrusion detection systems should be logging centrally and those logs should be reviewed by ICS-aware security staff.

  See: http://en.wikipedia.org/wiki/Syslog

- **Honeypot Intrusion Sensors**

  Honeypots have utility within ICS environments as intrusion detection devices. This is distinct from their traditional use as a security research tool for learning attacker behaviors. Honeypots can be deployed internally within ICS environments specifically to **detect intruders or malware that are already active within your environment**. Any interaction with a honeypot crafted to emulate the behavior of an ICS device is immediately suspect and requires immediate investigation. This is a quick, "low noise" approach to detection that can significantly increase your ability to detect problems early on.

  An extension of the honeypot concept is "Honey documents". These are office documents (e.g. spreadsheets, Word documents, etc.) crafted to appear as if they contain sensitive information or even what appear to be ICS-specific application programs. They are instrumented to "call home" when used by the attacker. When

they do, you are alerted to the attacker's presence, what they are interested in and - by source IP address - where they are located.

See:

http://en.wikipedia.org/wiki/Honeypot_computing

http://www.securitytube.net/video/9014 Researcher usage

http://microsolved.com/HoneyPoint-server.html easily-configured ICS "HoneyPoints"

6. Have a Recovery Plan

Plan for Failure. Network segmentation can contain the problem and anomaly detection and reporting can give you an early warning – but you still have to act.

- **Incident Response Plan**

  You should have a formal incident response process in place. ICS and security staff should regularly meet and discuss how they would deal with the operational problems brought on by the failure of a computer system, whether caused by a security incident or a simple software failure. Inter-group communication, containment and remediation strategies required for recovery should be documented and regularly reviewed. Staff at facilities that might be affected by the same event should quickly be made aware.

- **Recovery Materials**

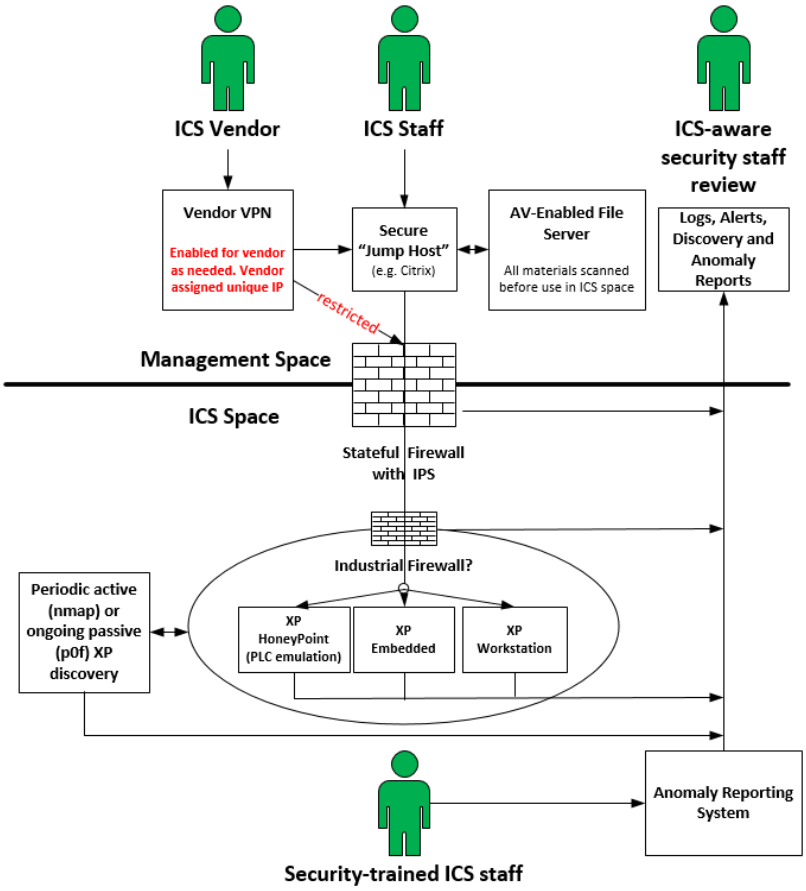
  Make sure all materials required for recovery in your plan are available. That should include all vendor manuals, software installation materials, and any system backups that will be needed. Procedures for using these materials should be documented. Do not assume you will have general Internet access during recovery. Have what you will need locally.

- **Learn and Adapt**

  After recovery, all affected staff should meet and discuss the event and how to plan for similar events in the future. Documentation should be updated and new detection sensors deployed if needed.

Reference Diagram

The diagram below depicts an ICS environment that has implemented the above guidelines.



XP Segmentation and Monitoring

- XP discovery (passive or active) is ongoing
- XP systems patched to the extent possible
- XP systems enabled for external logging where possible
- XP systems in separate network segment if possible
- XP systems have limited and tightly monitored ability to initiate communication out of ICS space.

Only security-trained staff have direct access to equipment. They must know to report all anomalies, *even non-disruptive ones*, as potential security issues

Remote access is by way of secure "jump hosts". Security staff who are aware of both operational and IT security issues cooperate in configuring and managing.

If vendor VPN required, it should ideally be enabled only as needed. Vendors should also use intermediate jumphosts for access. If direct access from vendor VPN laptop to ICS space equipment required, local vendor VPN IP address should be unique by vendor to allow access to be limited and tracked. ICS may be exposed to malware on laptop.

All media – whether physical (e.g. USB stick) or purely electronic – must be evaluated prior to use. ICS staff must enforce this. Antivirus (AV) enabled file server can help.

Industrial firewalls specific to ICS environment used as appropriate to mitigate XP risk. Alerts to security staff.

Stateful firewall at management/ICS boundary is ICS protocol aware and also alerts to security staff.

"HoneyPoints" that emulate XP ICS equipment distributed through environment to capture malware/attacker activity and alert to staff.

ICS staff and Information security staff meet regularly to exchange information and concerns. It is critical that information about potential security issues or practical risks to the operation be discussed and cooperatively resolved.

Summary

The steps described in this document can help minimize the chance for a software event affecting the XP systems that remain within your environment from seriously affecting your operations.

Ultimately you will have to eliminate those systems to reduce risk. Once you have an accurate inventory of XP in your environment, start working with the relevant vendors and look for long-term replacements.

The emphasis should be on long-term. “XP-like” events will happen again…and again. Plan for that. Your replacement systems should have clear, documented upgrade paths that are designed to allow continued, undisturbed operations.

Future proof your operation.

About MicroSolved, Inc.

MSI has more than 20 years of experience working in the ICS/SCADA world. Members of our team have served as OT engineers, designed the penetration testing processes used by the US Department of Energy and other regulators, discovered and analyzed vulnerabilities and worked on incidents deep inside critical infrastructures.

Contact:

info@microsolved.com

http://www.microsolved.com

(614) 351-1237

Sales:

abergen@microsolved.com

(513) 300-0194