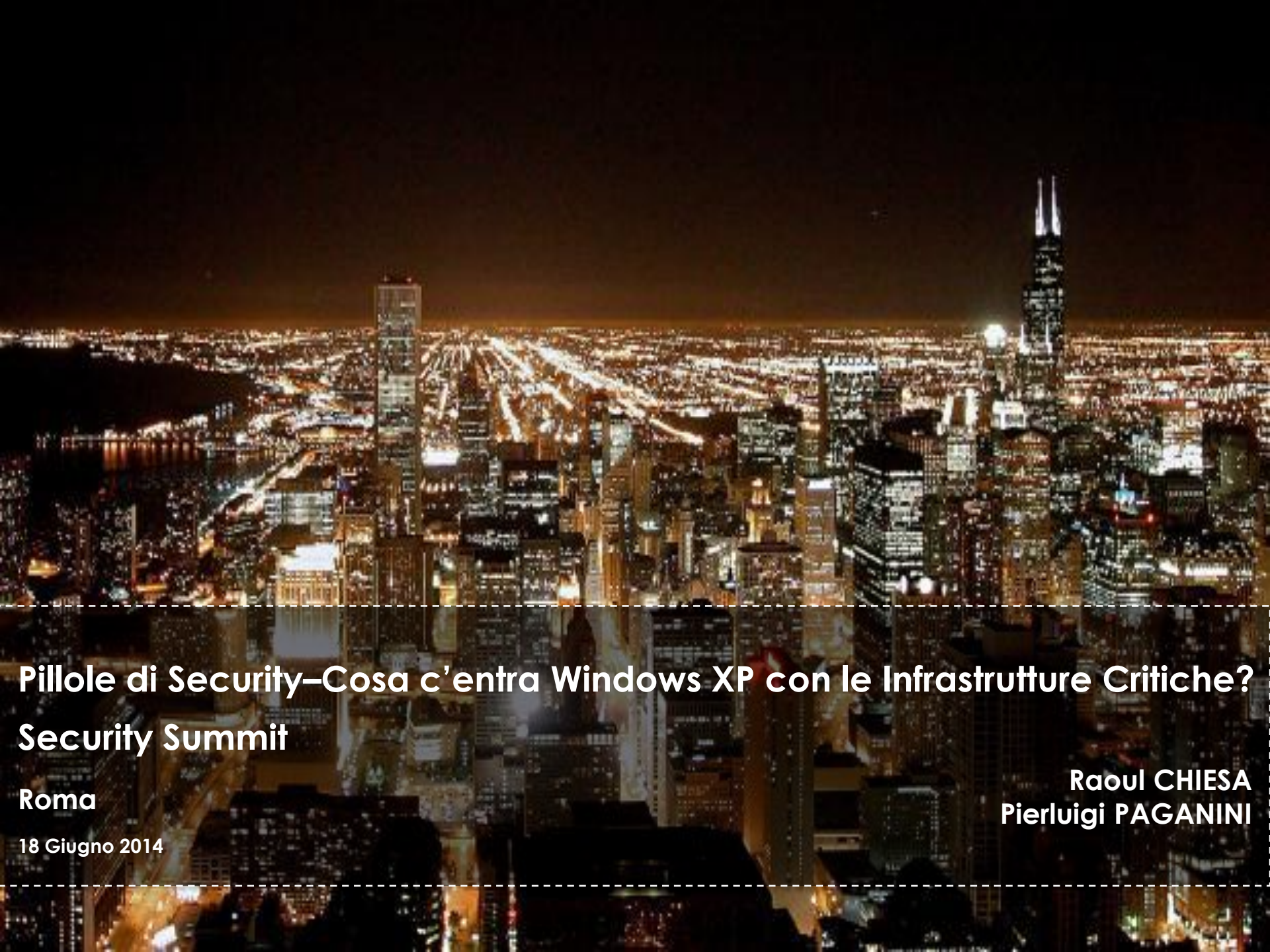


Pillole di Security–Cosa c'entra Windows XP con le Infrastrutture Critiche?

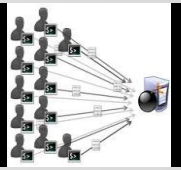
Security Summit

Roma

18 Giugno 2014

Raoul CHIESA
Pierluigi PAGANINI

AGENDA

- Intro 
- XP & Critical Infrastructures 
- Risk analysis 
- Under attack 
- Futher reflections on the attacks 
- Mitigation strategies 
- Conclusions 

AGENDA

- Intro
- XP & Critical Infrastructures
- Risk analysis
- Under attack
- Futher reflections on the attacks
- Mitigation strategies
- Conclusions

Intro

April 8th 2014 - support for WinXP is ended

- *"Security updates patch vulnerabilities that may be exploited by malware and help keep users and their data safer. PCs running Windows XP after April 8, 2014, should not be considered to be protected, and it is important that you migrate to a current supported operating system – such as Windows 8.1 – so you can receive regular security updates to protect their computer from malicious attacks." states Microsoft official announcement.*

- Over 70% Microsoft's security bulletins in 2013 were related to flaw in to Windows XP.

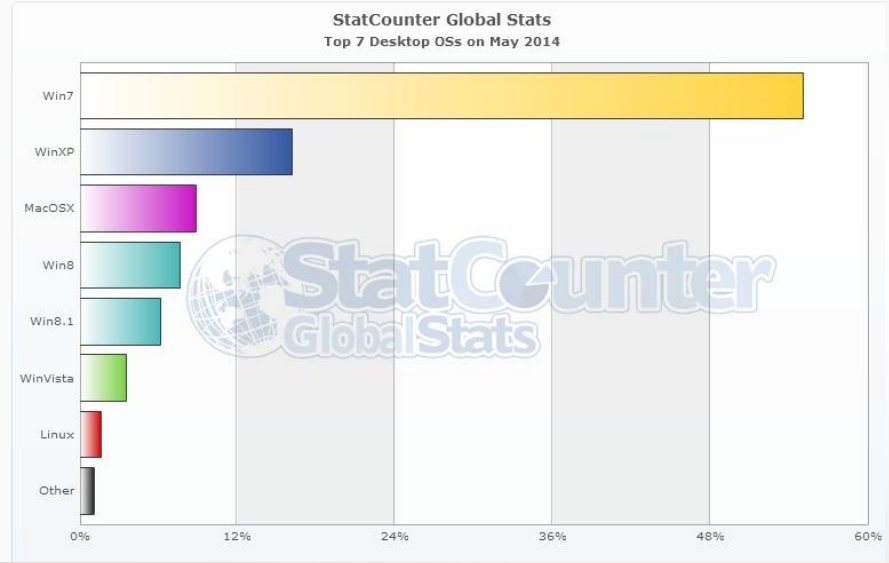
- Windows XP customers could choose to pay for extended support (US$ 100K/year, or migrate a newer OSs like Windows 7 and Windows 8.

- The principal security concerns are related to critical infrastructure where XP replacement is not so simple.

Security experts warn on the possible consequences on Security of Critical Infrastructure

Intro

Statistics – XP support is ended but …



- *Worldwide use of XP has passed from 19,79% to 16,17% in the last 6 months.*
- *In Italy Win XP systems passed from 17,35% (Dec 2013) to 14,14% (May 2014).*
- *In North Korea Win XP systems passed from 47,83% (Dec 2013) to 36,06% (May 2014).*
- *In May 2014 in US percentage of Win XP systems is 12,46, 20,72% in Russian Federation, 25,23% in Iran and 7,22% in UK.*

16,17% of systems worldwide stll use XP OS

Intro

Statistics – XP support is ended but …

- *Microsoft released many different editions of XP specialized for different industries:*
  - ✓ *XP Embedded*
  - ✓ *XP Embedded for Point of Service*
  - ✓ *XP Tablet PC Edition*
  - ✓ *Windows Fundamentals for Legacy PCs*
  - ✓ *XP Professional Blade PC Edition*

- *The above Windows XP edition are used in:*
  - ✓ *Cashpoint (ATM) machines*
  - ✓ *Restaurant and shop payment systems*
  - ✓ *Telecoms systems*
  - ✓ *HMI/SCADA systems*
  - ✓ *Heating and air conditioning systems*
  - ✓ *Elevators*

Windows XP still used in many industries

AGENDA

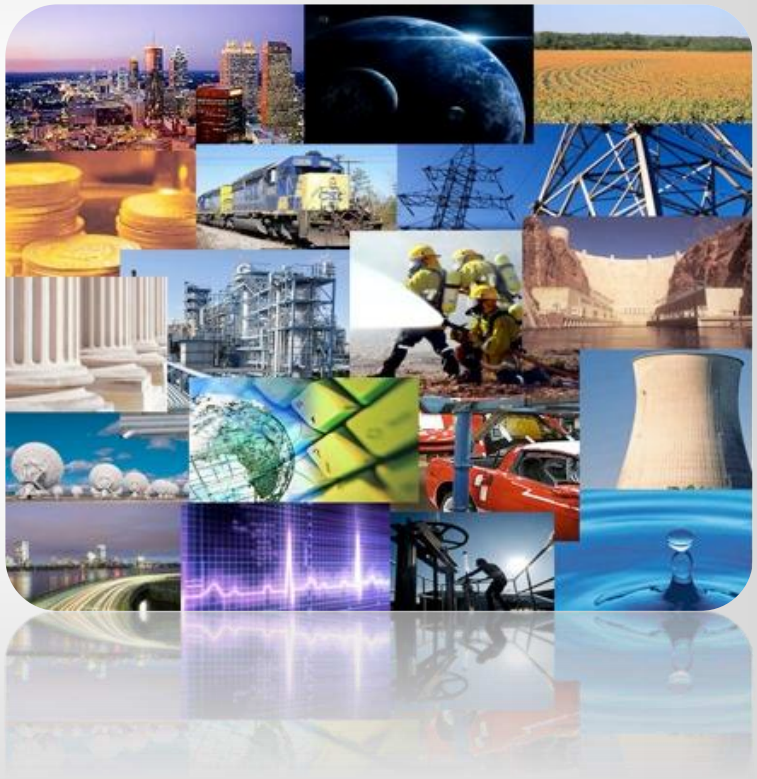
- Intro
- XP & Critical Infrastructures

- Risk analysis
- Under attack
- Futher reflections on the attacks
- Mitigation strategies
- Conclusions

XP & Critical Infrastructures

Where are Win XP implementation?

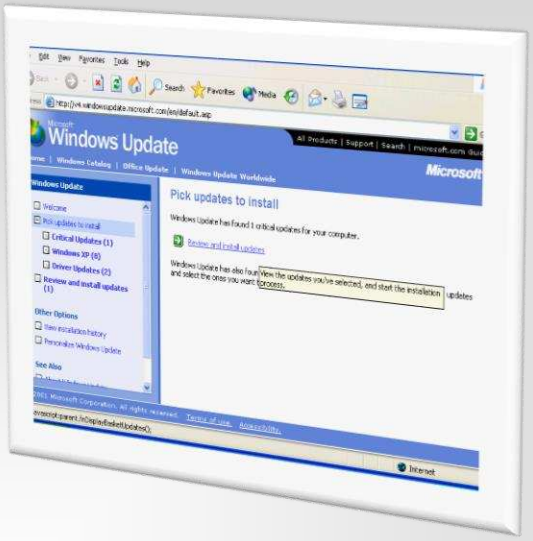
- *Remote Terminal Units used interfaces objects in the physical world to a system by transmitting telemetry data to a master system*
- *Programmable logic controllers connect to sensors in the process and converting sensor signals to digital data.*
- *Human–machine interface applications which are the software or device which presents processed data to a human operator.*
- *Supervisory (computer) systems which gather data on the monitored process and send commands to the SCADA system.*



Windows XP widely adopted in critical environments

XP & Critical Infrastructures

Upgrades for Critical systems perceived as threats



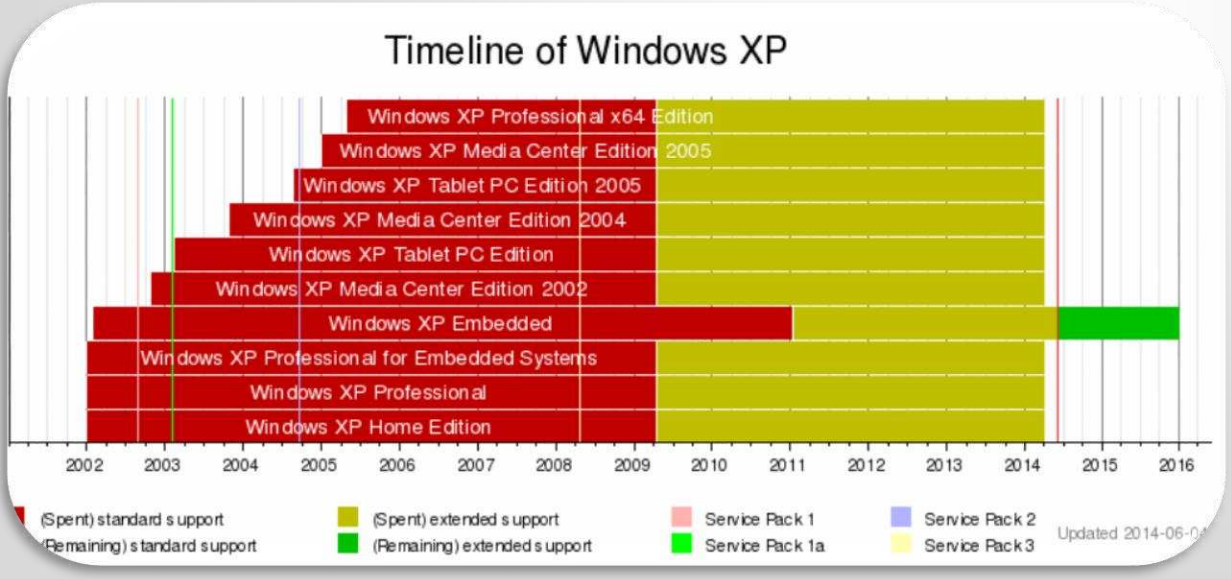
- *Lack of patch mentality is a cultural issue for the ICS/SCADA world.*
- *Between 10 to 20 percent of organizations today actually install patches that their SCADA vendors are releasing.*
- *The likelihood that customers will apply patches to their SCADA systems is low.*
- *Utilities and ICS organizations face risks of power shutdowns if a newly patched system doesn't work correctly.*
- *Many ISC/SCADA software are vulnerable (e.g. presence of vulnerabilities, backdoor in HMI).*
- *Power plant operators prefer to add more monitoring or other defenses to watch for malware and attacks than to change out software*

Effects of Windows XP EoL will be perceived on the long term due to the lack of patch mentality for the ICS/SCADA world.

XP & Critical Infrastructures

Principal technological issues during the XP design timeframe

- *Mobility as assumed a crucial role differently from the past especially for HMI*
- *Technology passed from isolated and proprietary systems into open architectures and standard technologies that are highly interconnected.*
- *Most attacks were designed more to create aggravation target performance, today cyber espionage represents primary concern.*
- *Critical corporate information was often retained in a data center, not on user's devices.*



- *Cyber threats are profoundly changed.*
- *Explosion of state-sponsored hacking and cyber crime*
- *Economy of attacks profoundly changed, in favor of attackers.*

13 years full of changes

XP & Critical Infrastructures

Win XP as attack vector

- The role of Windows XP in the attacks on SCADA systems is to provide a second attack vector.
- A whole range of security issues and system vulnerabilities no more patched have to be added to the problems of software used on these systems.
- In any case, Windows XP Embedded, probably the most used in SCADA systems, will be supported by Microsoft until 2016.

Windows XP widely adopted in critical environments

AGENDA

- Intro
- XP & Critical Infrastructures
- Risk Analysis

- Under attack
- Futher reflections on the attacks
- Mitigation strategies
- Conclusions

Risk analysis

Primary technology risk factors to consider continuing Windows XP use

- *Security updates will no longer be provided leaving Windows XP-based systems vulnerable to exploits and cyber attacks.*
- *Newer versions of IE from 9.0 are not supported, vulnerabilities in older versions will represent major risks going forward.*
- *Organized crime syndicates are developing exploits for unpatched Windows XP systems. In a short time every Windows XP system will be vulnerable.*
- *Criminals reverse reverse-engineer patches for supported operating systems issued by MS and apply the vulnerabilities they found Win XP devices.*
- *Targeted attacks on Win XP systems will increase.*

Risk analysis

Other risk factors to consider continuing Windows XP use

- *Potential liabilities and legal issues related to an APT attack or a data breach.*
- *Cost risks related to potential damages of data breach subsequent to a cyber attack.*
- *Cost risks for supplementary maintenance and mitigation measures.*

Risk analysis

Risks related to Patch Management

- *Increased vulnerability to outside attacks. One way to enhance the security of SCADA is through the application of patches.*
- *Two of the key important issues with patching, at the moment are the failure rate of patches and the lack of patches for SCADA systems.*
- *Applying patches reduces the opportunity for exploitation, but could have a significant effect on the operational behavior.*
- *From a safety point of view, patches and software updates can also be a risk.*

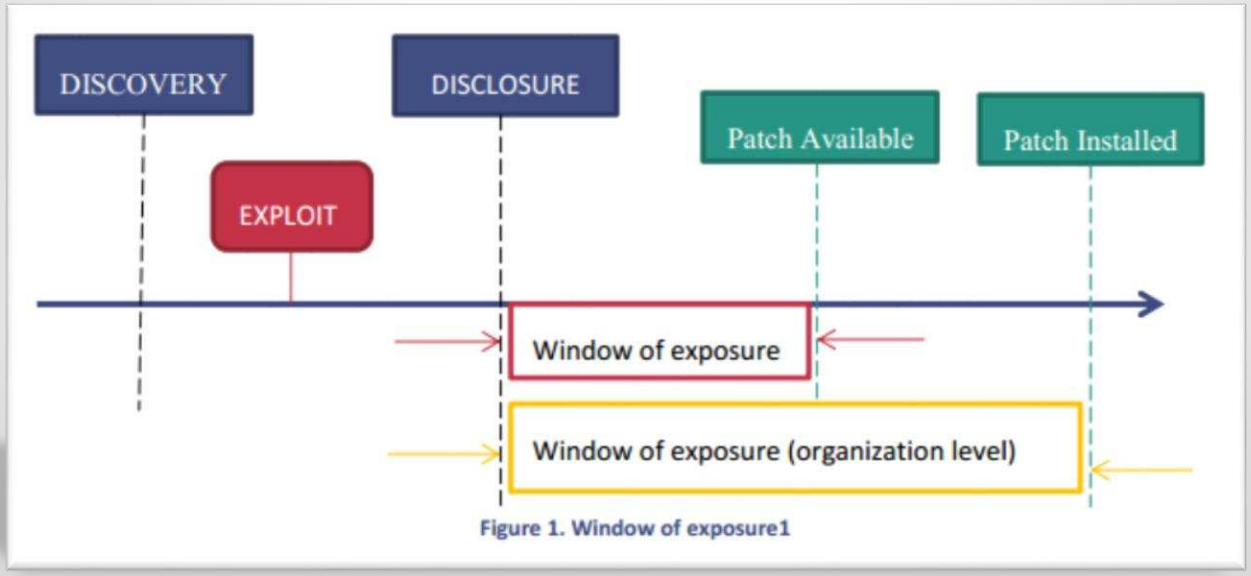


Figure 1. Window of exposure1

Risk analysis

Consequences of Windows XP end of life can be serious if critical infrastructure owners take no actions

- *Breach and data compromise*
- *Affect ability of organizations to comply with standards*
  - *(NERC) North American Electric Reliability Corporation (2013), CIP-007, Systems Security Management*
  - *(NIST) National Institute of Standards and Technology (2005), SP 800-40, Creating a Patch and Vulnerability Management Program*
  - *(NIST) National Institute of Standards and Technology (2011), SP 800-82, Guide to Industrial Control Systems*
  - *ISA/IEC-62443 (Formerly ISA-99)*
- *Financial penalties fined for failure to pass compliance audits or for being in a noncompliant state Operational damages*
- *Damage to corporate brand*
- *Impact on Patch management service contract. Who will be responsible in the event of a failure?*

Risk analysis

Not installing patches … Some organizations deliberately not to install patches on critical systems.

- *Impact on the operational behavior of systems. Some extremely critical systems may have no allowed outage windows available.*
- *Evaluation risks vs benefits.*
- *The software is not supported anymore by the vendor, or the vendor does not exist anymore. In this cases organizations could develop their own patches, but it's complex because OS source code is proprietary.*
- *Organizations prefer to "invest" on alternative controls, like network hardening*

AGENDA

- Intro
- XP & Critical Infrastructures
- Risk Analysis
- Under attack

- Futher reflections on the attacks
- Mitigation strategies
- Conclusions

Under attack

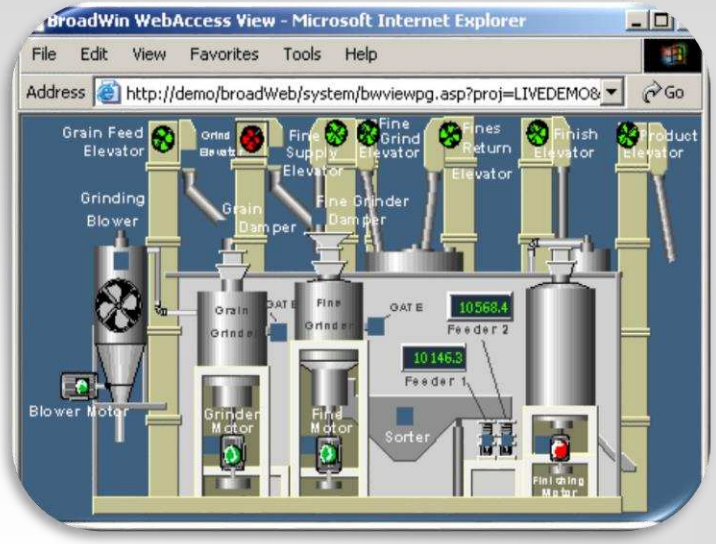
ICS-SCADA under unceasing cyber attacks

- "If ICS is connected to the Internet, it comes with an almost 100% guarantee of its being hacked on the first day" E. Kaspersky
- ISC-CERT reported over 20,000 reports of unauthorized internet access to control systems in the last half of 2012.
- Bad actors wanting to attack a control system can download exploit tools and run them against a target.

The number of cyber attack of cybercriminals, state-sponsored hackers and other bad actors is increasing

Under attack

Risks of exposure for systems on-line



- ICS-SCADA accessible directly from the Internet are exposed to risk of cyber attacks (e.g. probes, brute force attacks, attempts and unauthorized access and scanning).
- In September Kaspersky Lab Team set up a honeypot which pretend to be an industrial system that was successfully breached 422 times.
- Free-available scanning and cataloguing of devices known to be susceptible to emerging vulnerabilities, availability of principal information on the public interface of control systems coupled with a huge quantity of hacking tools, are drastically reducing the level of knowledge required to successfully locate and exploit targets.
- In 2013 ICS-CERT received 181 vulnerability reports from researchers and ICS vendors, 177 were true vulnerabilities, 87 percent were exploitable remotely while the other 13 percent required local access to exploit the flaws.

Under attack

Hacking campaigns targeted XP after EoL
Operation Clandestine Fox

- Early May 2014 FireEye discovered “Operation Clandestine Fox” targeting Windows XP.
- Live attacks exploiting recently discovered IE Remote Code Execution vulnerability (CVE-2014-1776).
- CVE-2014-1776 is the highest profile vulnerability yet to hit Windows XP
- Multiple hacking crews targeted government, energy sector, finance and defense organizations in the US and Europe.
- Microsoft released an emergency, unscheduled patch.

Under attack

Rapid evolution of Hacking campaigns

- Hacking techniques leverage social networking
- Targeted "Spear Phishing" exploiting social media and mobile platforms.
- Malicious Payloads delivered through:
  - ✓ Attachments
  - ✓ IM links
  - ✓ Physically planted peripherals and devices
  - ✓ Watering hole attacks
  - ✓ Mobile devices

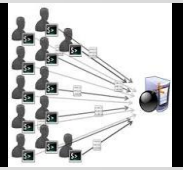
Under attack

Exploitation of targets … not so complex

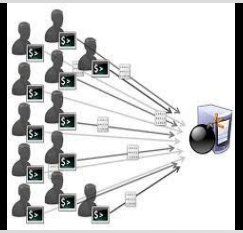
- Legit tools coudl be used to localize and exploit flows in the targets (e.g. Shodan, Google, Metaexploit, Maltego, CORE Impact, Canvas Exploits).
- Terry McCorkle (Boing) and Billy Rios (Google) used serch engine to discover SCADA/ICS systems on Internet. [76 HMI tested, 75 explotable flaws discovered]
  - ✓ +HMI +Download + filetype :(exe,zip,msi)
  - ✓ +HMI +<Vendor Name> +Download
  - ✓ +HMI +<Country Name> +Download
- Underground market offers different services and crimeware-kit that could be used to exploit knonw flaws in XP systems.
- Reverse engineering of malicious agent in the wild.

AGENDA

- Intro
- XP & Critical Infrastructures
- Risk Analysis
- Under attack
- Futher reflections on the attacks



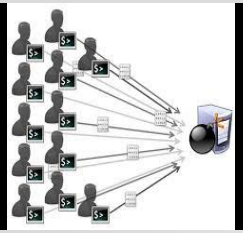
- Mitigation strategies
- Conclusions



Futher reflections on the attacks

XP End of Life - inevitable effects

- Increased interest of state-sponsored actors in research for XP 0-day.
- As collateral effect, bad actors will focus their attention in the exploitation of defense measures adopted to mitigate XP EoL (e.g. industrial firewall)
- Booming of the offer for XP vulnerabilities on the black market.
- Exploit frameworks will acquiring SCADA vulns to create new exploits, surge of interest in XP based systems.
- The number of cyber attacks against Critical Infrastructure will continue to increase, independently from XP EoL.
- Critical System have to share information, increasing of surface of attack.

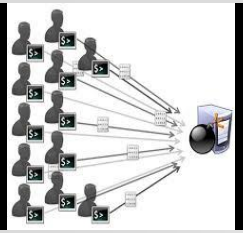


Futher reflections on the attacks

XP End of Life - inevitable effects

- The cost for APT campaign is dramatically dropping [Costin Raiu – Kaspersky Lab].
- Costs collapsed from $100 million [Stuxnet] to just $10,000 [today campaign].
- The dropping for the cost represents an element of serious concerns for cyber security experts because it is lowering the barrier to entry to the global cyber-arms race.

XP eof can further reduce the cost to the organization of a hacking campaign since there are no developments by the defense.

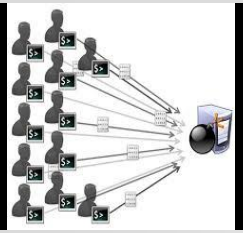


Futher reflections on the attacks

XP End of Life - The opinion of an expert
Luigi Auriemma - ReVuln

A possible attack scenario:

- Attackers can exploit known vulnerabilities in Internet Explorer or known/unknown flaws in ActiveX HMI / SCADA software to take control (e.g. privilege escalation) of the system when victim visits the website of the attacker.
- Possible exploitation of vulnerabilities in HMI/SCADA services to conduct an attack from a machine on the same LAN, or under particular conditions from the Internet.
- Once gained access to the targeted machine the attacker can exploits more bugs no more patched in the operating system for example to increase even more privileges in case he needs it.



Futher reflections on the attacks

XP End of Life - The opinion of an expert

Nations Buying as Hackers Sell Knowledge of Software Flaws

By NICOLE PERLROTH and DAVID E. SANGER

On the tiny Mediterranean island of Malta, two Italian hackers have been searching for bugs — not the island's many beetle varieties, but secret flaws in computer code that governments pay hundreds of thousands of dollars to learn about and exploit.

The hackers, Luigi Auriemma, 32, and Donato Ferrante, 28, sell technical details of such vulnerabilities to countries that want to break into the computer systems of foreign adversaries. The two will not reveal the clients of their company, ReVuln, but big buyers of services like theirs include the National Security Agency — which seeks the flaws for America's growing arsenal of cyberweapons — and American adversaries like the Revolutionary Guards of Iran.

All over the world, from South Africa to South Korea, business is booming in what hackers call "zero days," the coding flaws in software like Microsoft Windows that can give a buyer unfettered access to a computer and any business, agency or individual dependent on one.

Just a few years ago, hackers like Mr. Auriemma and Mr. Ferrante would have sold the knowl-

Continued on Page 14

- Exploitation of not updated OS as attack vector.
- The reversing engineering of security patches for SCADA is a privileged way to use bug fixes recently released in situations where vendors have ended the support.
- Patch reverse engineering effective also in case personnel of critical systems haven't applied the upgrades due to stability problems.
- Regarding XP EoL it could be observed a contradictory effect on zero-day market, zero-days prices could not be affected because attackers could simply get a proof-of-concept exploit public available and reuse it.

AGENDA

- Intro
- XP & Critical Infrastructures
- Risk Analysis
- Under attack
- Futher reflections on the attacks
- Mitigation strategies

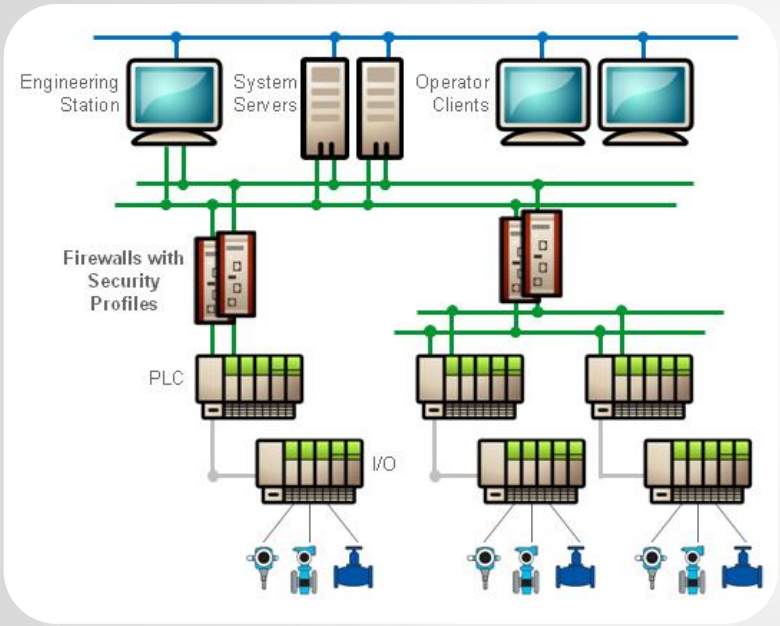
- Conclusions

Mitigation Strategies

- Replace with more recent Oss (e.g. Windows 7). Almost all SCADA application and libraries/packages that run on XP will run on Window 7.
- Virtualization is an inexpensive method of preserving the state of a PC at a snapshot in time.
- Redundancy of critical systems. Price of systems being so low, provisioning a spare SCADA PC is both cost effective and easy to do, but spare will not be identical to production machines.
- Using innovative, non-signature based Host Intrusion Prevention and OS hardening
- Using Host Intrusion Detection and File Integrity Monitoring capabilities that include system, services, file and application checks, as well as real-time
- Isolate from outside critical components. Take care of possible vector of attacks (e.g. network, USB, mobile devices)

Mitigation Strategies

Industrial Firewalls



- Industrial Firewalls Are an Easy Way to Protect Your Applications
- Industrial firewalls could be considered an immediate and cost effective security solution.
- Can be deployed into live networks without disrupting production
- Simple to install and configure
- Designed implementing security for industrial development from the ground up, including being appropriately ruggedized and certified

AGENDA

- Intro
- XP & Critical Infrastructures
- Risk Analysis
- Under attack
- Futher reflections on the attacks
- Mitigation strategies
- Conclusions

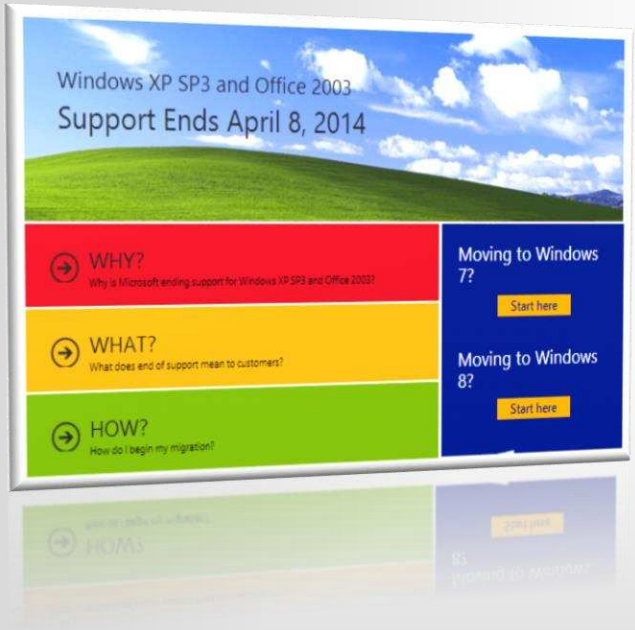
Conclusions

Resuming

- *As Microsoft Trustworthy Computing director Tim Rains pointed out, the company's own security updates for supported operating systems such as Windows 7 and Windows 8 involuntarily provide attackers with intelligence about flaws in older operating systems*
- *There's certainly a possibility that some flaws in Win XP OS that were already known, but that haven't been exploited yet, will be targeted in a number of attacks.*
- *Reverse-engineering a patch for other OS versions could help the design of exploits for an unannounced vulnerability.*
- *End users and OEMs have been slow to react. This creates a major opportunity for HMI software and services suppliers to sell upgrades.*
- *Organizations managing critical system could decide to pay for a MS Custom Support.*

Conclusions

What could happen in the next months?



- *XP EoL will have a significant impact on both defense and offense perspectives.*
- *Windows XP in the attacks on critical infrastructure provides a second attack vector.*
- *Attackers will increase the number of offensives against systems not updated.*
- *Cost of attacks on XP systems fall down lowering the barrier to entry to the global cyber-arms race.*
- *Be aware of possible actions of independent hackers or hacktivits.*
- *Critical System will need to share information even more increasing of surface of attack.*
- *Security Emergence as Business opportunity.*


Thank you

Conclusions

Raoul Chiesa

About Raoul "Nobody" Chiesa:
Founder, President @ Security Brokers SCpA, Security Evangelist, Security Advisor, Journalist and books writer.

Security expert with over 25 years experience in the field. Certified OSSTMM International Trainer, OPST, OPSA at **ISECOM**.

Member of **ENISA PSG** – Permanent Stakeholder's Group (2010-2015)

Special Advisor on Cybercrime and Hacker's Profiling at the United Nations Interregional Crime & Justice Research Institute (**UNICRI**)

Italian manager for the European chapter of the Anti-Phishing Working Group (**APWG.EU**)

Founder, Steering Committee & Technical Committee at Italian Information Security Association (**CLUSIT**)

Member of the Board at **ISECOM**

Member of the Board at **OWASP**, Italian Chapter

Raoul Chiesa

President Security Brokers SCpA

rc@security-brokers.com

www. security-brokers.com

Conclusions

Pierluigi Paganini

About Pierluigi Paganini:
Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, he is also a member of the advisory council for The European Centre for Information Policy and Security (ECIPS), Security Evangelist, Security Analyst and Freelance Writer.
Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness lead Pierluigi to find the security blog "Security Affairs" named a Top National Security Resource for US.
Pierluigi is a member of the DarkReading Editorial team and he isregular contributor for some major publications in the cyber security field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines.
Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin", coming soon the new book "Spy attack: comeaziende, servizi segreti e hacker possono violare la nostra privacy"

Ing. Pierluigi Paganini

Chief Information Security Officer Bit4id

ppa@bit4id.com

www.bit4id.com

Founder Security Affairs

http://securityaffairs.co/wordpress

pierluigi.paganini@securityaffairs.co