Weakest in the Herd: EoL Software & a Journey to Secure it

By Aastha Sahni & Anuprita Patankar

Aastha Sahni

Lead CyberSecurity Instructor- Flatiron School

Founder - CyberPreserve Educational Initiative

InfosecGirls NYC Chapter Lead

OWASP NYC Member

Anuprita Patankar

Application Security Engineer, J2 Global

Women of Security(WoSEC)- New Jersey Chapter Lead

Director of Security Awareness: Protect Us Kids foundation

Agenda

- End of Life Philosophy
- Self check: Identify your EoL state
- Is it that time to move on?
- Risk Factors associated with EoL
- Security threats
- Prevention and mitigation strategies

End of life philosophy

- Software change is inevitable with the advancement of hardware, failing to do so the interconnectivity impacts software itself
- Software has become the key in making important business decisions and hardware has been just a commodity
- Good software is hard to build, it takes too long, cost too much and most of the times fails to perform as expected
- Rate of change in technology and software is brutal and unforgiving. It’s difficult to keep up the pace with changing technology

What does End of life (EoL) really mean?

Self check: Identify your EoL state

- What release/version are you on?
- When the current version was implemented?
- How customize your solution is?

- Check vendor software release and upgrade policy for the implemented solution
- How long the currently implemented solution will be supported by the vendor?
- Are you using a niche software product
- Check if your vendor software company has any financial debt to support any resources or research teams

Is it that time to move on?

- You have received a notice from your software vendor
- You are facing difficulty in finding new talent to support your current business systems
- Outdated technology create challenges retaining talented employees
- Technology is failing to meet user functionality experience

Risk Factors associated with EoL

- Compliance
- Lawsuits
- No security Patches and updates
- Higher operational cost
- Reduced performance and productivity
- Risk of hackers, malwares and APTs

Be Aware

Recent examples of EoL software

- Microsoft windows 7
- Python 2
- Windows 2008 & 2008 R2- 1/14/2020
- Exchange 2010- 1/14/2020
- SBS 2011- 1/14/2020

Possible Security Threats to EoL Software

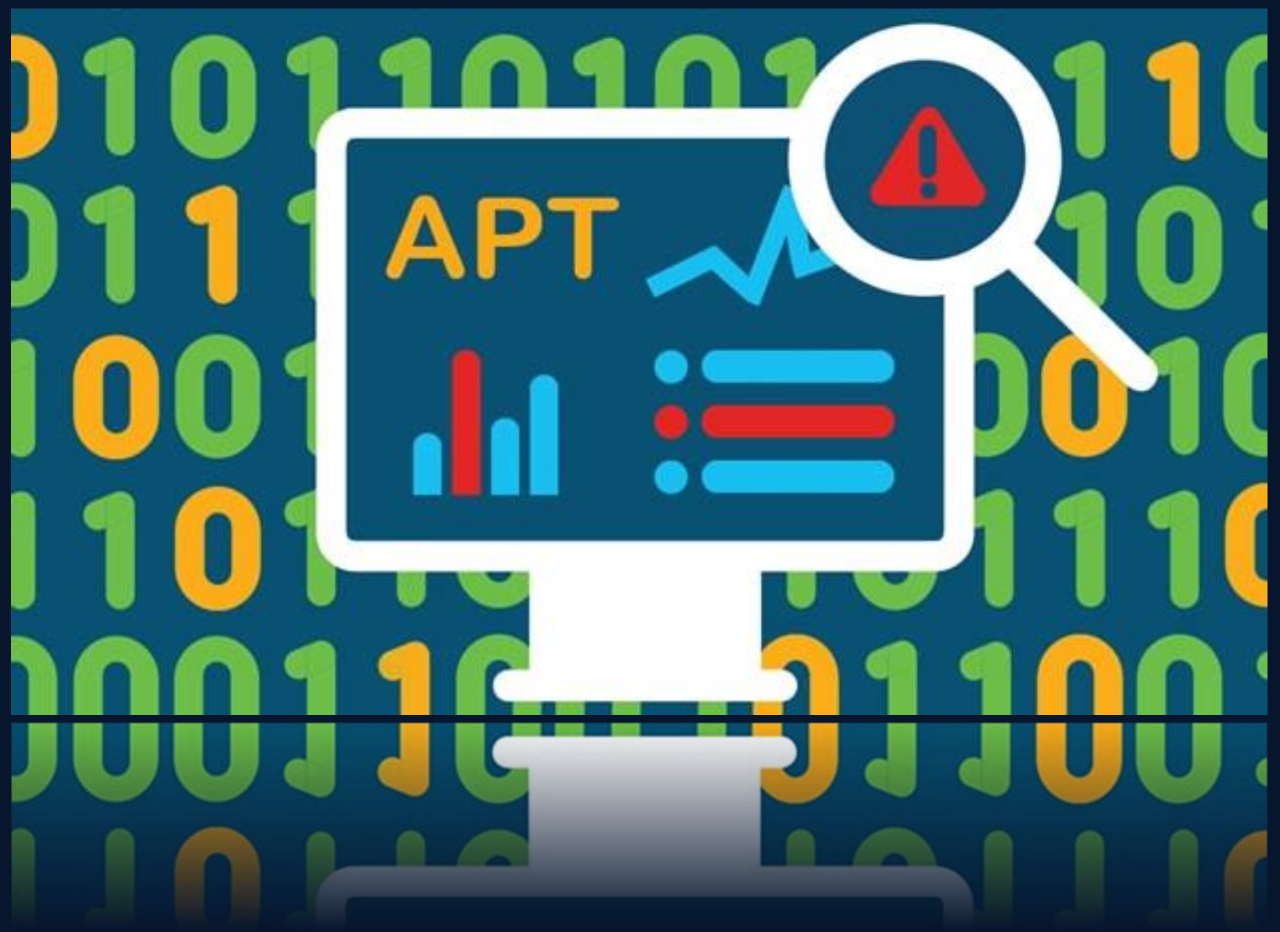
“While Windows XP’s end of life process did not precipitate any major related cyber security events, the scrutiny given to its weakness served as a case study in how preventable vulnerabilities – e.g., ones owing to a system that was not patched in time or to a communications error within the organization – can pave the way for advanced persistent threats, malware delivery and surveillance.”

by TrendMicro

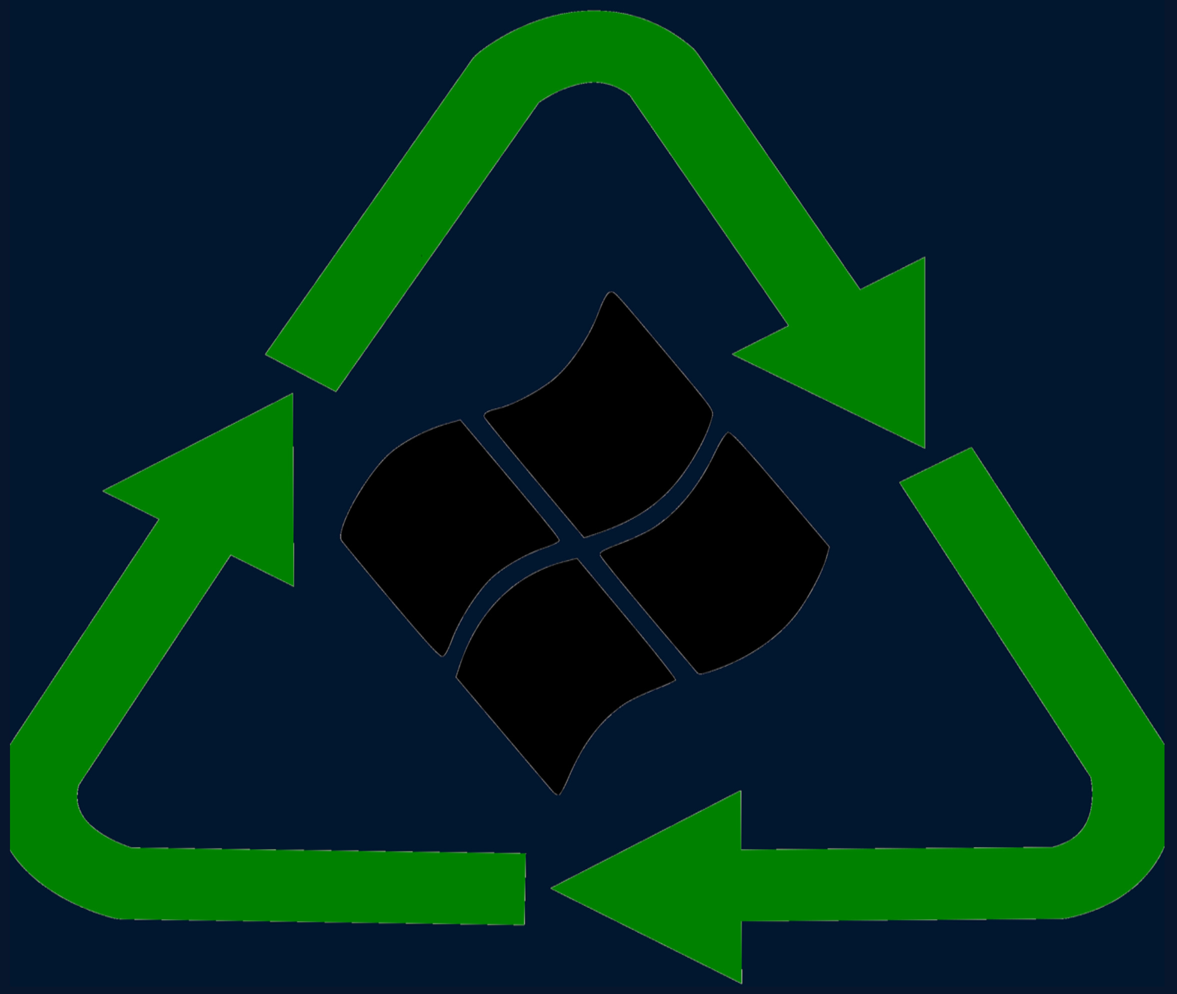
Some Serious Cyber Threats including- APT (Advanced Persistent Threats)

An advanced persistent threat (APT) is a stealthy threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period.In recent times, the term may also refer to non-state sponsored groups conducting large-scale targeted intrusions for specific goals. [1]

APT can be focused on large organizations and cause severe damage.



Prevention and Mitigation of Security Threats Residing on EoL Softwares



- Improved Risk Assessment Planning & Implementation - establish better risk-based programs to eliminate EOL assets.
- Implementing Advance techniques in End Point Detection tools to detect EoL Softwares.
- Include EOLs detection in Inventory management tools.
- Vendors can convert old softwares as free software , such as Windows 7. Free Software Foundation has initiated this campaign to request Microsoft to convert Windows 7 into a free software, so that there is no expiry and it can be written to make changes till the last.

Preparation is Prevention - PDCA

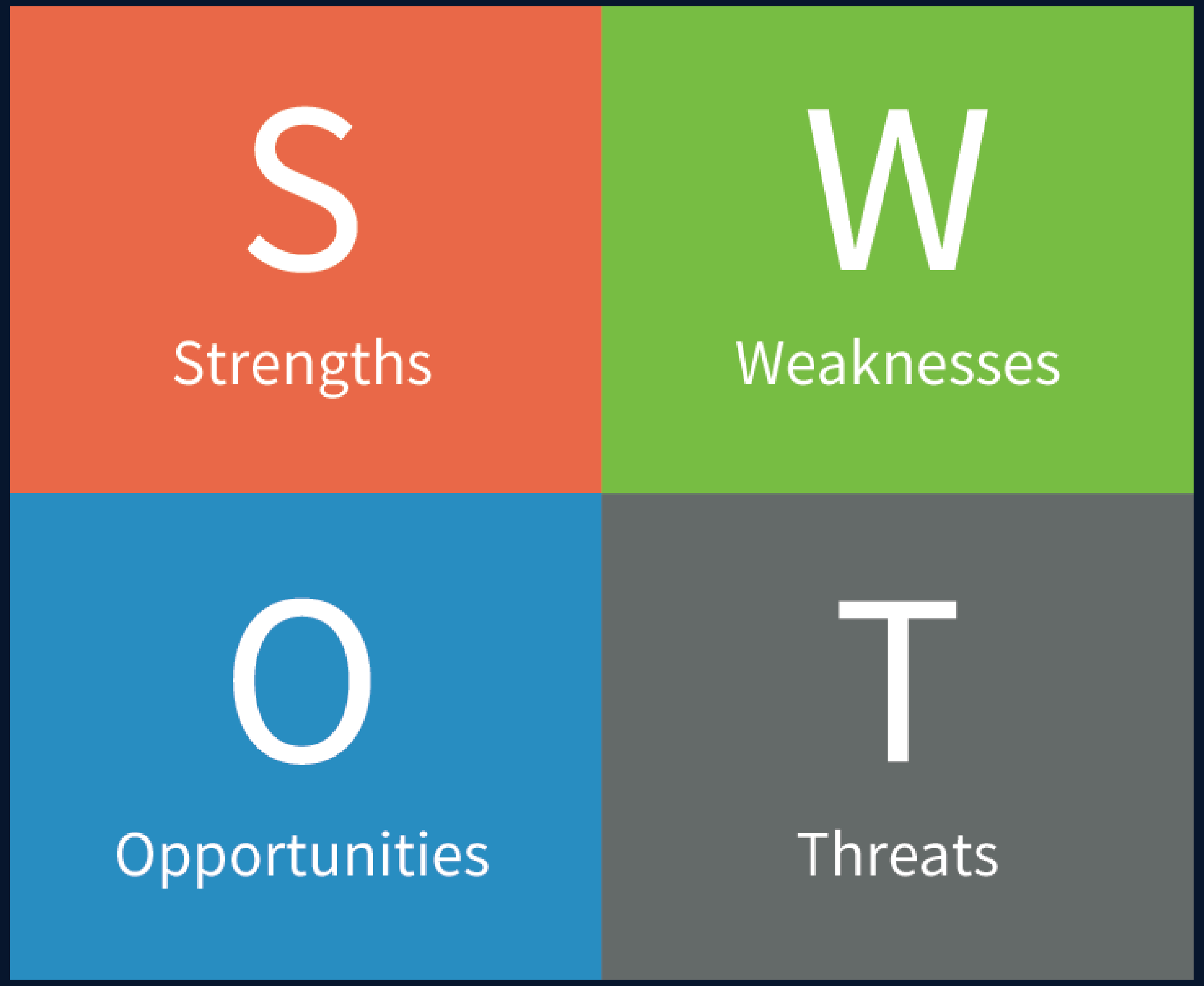
PDCA is a continuous improvement cycle widely used by companies to break out of stagnancy and transition towards continuous growth

Organization can implement EoL Software related improvement strategies in the PDCA approaches in order to ensure continuous improvement

- Plan - Include EoL Software risk assessment as part of Organizations Risk Assessment Plan
- Do - Based on the result of Risk Assessment, take necessary steps to either remove EoLs or update them
- Check - Verify and validate the security controls implemented in Do process are implemented correctly or not
- Repeat - Repeat the process to ensure continued growth and improvement

PLAN
DO
CHECK
ACT

Preparation is Prevention - SWOT Analysis



S Strengths	W Weaknesses
O Opportunities	T Threats

- SWOT Analysis is another technique which helps organizations assess their current situation - it not only talks about the strengths and opportunities but helps organizations to face their weakness and challenges .

- EoL Software detection and mitigation can be included in SWOT analysis. Organizations can then better decide how to deal with these softwares and adapt better approaches which are aligned with their business environment

Upcoming EoL dates for popular software

- Windows: http://windows.microsoft.com/en-ca/windows/lifecycle
- McAfee: http://www.mcafee.com/ca/support/support-eol-software-utilities.aspx
- Citrix: https://www.citrix.com/support/product-lifecycle/product-matrix.html
- Google Chrome: https://www.google.com/chrome/devices/eol.html
- Oracle: http://www.oracle.com/us/support/library/lifetime-support-technology-069183.pdf

REFERENCES

1. https://en.wikipedia.org/wiki/Advanced_persistent_threat#:~:text=An%20advanced%20persistent%20threat%20(APT,undetected%20for%20an%20extended%20period.

1. https://www.mdpi.com/2076-3417/10/11/3874/pdf

1. https://sdtimes.com/softwaredev/report-50-of-companies-dont-have-a-plan-for-python-2-eol/

1. https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

1. https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html

1. https://www.fsf.org/blogs/community/tell-microsoft-to-upcycle-windows-7-set-it-free

1. https://www.doxnet.com/2019/08/2020-signals-end-of-life-for-windows-7-and-other-major-software/

1. https://readwrite.com/2019/10/04/end-of-life-software-keep-it-update-it-or-find-a-new-solution/

1. https://www.doxnet.com/2019/08/2020-signals-end-of-life-for-windows-7-and-other-major-software

1. https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf

Thank you!

You can reach out to us via LinkedIn or Twitter

Anuprita Patankar

LinkedIn: https://linkedin.com/in/anuprita-patankar

Twitter: : @ThisIsAnuprita

Aastha Sahni

LinkedIn: https://www.linkedin.com/in/aastha-sahni/

Twitter:@aastha1891

Website: cyberpreserve.com