Microsoft

Make it tight, protect with might, and try not to hurt anyone

Michael Johnson, MMPC

Topic

In 2012 the MMPC decided to change our approach to potentially unwanted software (PUS)

This presentation talks about how we approached those changes and the changes that we made

Reasons for change

Our mission:

- Protect our customers without interfering with their Windows experience

Internal:

- Researchers were working on PUS cases

Terms

Potentially unwanted software (PUS)

“*behavior [that] may impact the user's privacy, security, or computing experience,*” (MMPC Glossary, 2013)

Categorically speaking:

Adware, BrowserModifier, Dialer, MonitoringTool, Program, RemoteAccess, SettingsModifier, SoftwareBundler, Spyware, and Tool

Malicious software

Backdoor, Constructor, Exploit, HackTool, Joke, PWS, Rogue, Trojan, TrojanClicker, TrojanDownloader, TrojanDropper, TrojanProxy, TrojanSpy, VirTool, Virus and Worm

Theory of change

Realize the need for change
Define what we want to achieve
Understand what we currently do
Assess what we do against our goals
Assess the risks of making changes
Document and communicate
Implement the changes
Measure the results
Define process for making future changes

Realize the need for change

Our detection criteria was not inline with our mission to “protect our customers without interfering with their Windows experience”

We were warning our customers of programs that posed no threat alone but:

- May indicate a security issue
- May have been used my malware on this or some other machine

The PUS research process was not clear.

Define what we want to achieve

Detect only those programs that pose a security risk or interfere with the customer’s Windows experience

Make the PUS research process more accessible to all of the researchers

Understand what we currently do

Documenting what you do, if you have not already

- For us, we already had documents outlining the behaviours that we detected and what their severity was

We had to understand:

- How the researchers used the current documentation
- How they did their research

Assess what we do against our goals

Compare the list of PUS behaviours that we detected against our goal of “protection without interference”

We had to decide if the behaviour was a threat to the customer or only there to inform the customer of a program’s presence

We identified a few more behaviours that we added to our list of criteria

Assess the risks of making changes

We had to answer questions that asked if these changes pose a:

- Risk to Microsoft
- Risk to our customers

Some of these questions were answered by talking to the legal department and they helped us to understand the risk of our changes

Document and communicate

- We documented everything
  - We prepared a PUS course, a series of documents and had trainings
- Communicate internally and externally
  - Ensure one specialized PUS researcher in each of our labs to answer local questions and communicate problems and changes
  - Externally, we have updated our objective criteria page:

    http://www.microsoft.com/security/portal/mmpc/shared/objectivecriteria.aspx

Implement the changes

Comparing all of our past detections against our revised criteria

Rename or remove detection as appropriate

It was done in stages because it was too big a job to do all at once

Measure the results

Internal goals:

- Measuring the number of researchers that add PUS detections
- Researcher satisfaction
- Measure the consistency of PUS conclusions

External:

- Measuring what our customers think of our new approach is more difficult

Define process for making future changes

You may not get it right the first time

It will be easier to make future changes if you have a formal process in place

We have used our process to refine some of our criteria and it was much more streamlined with a formal process in place

What did we change in PUS

Behaviour changes

Category changes

Remediation changes

PUS severity levels - explanation

PUS detections have associated severity levels and default remediation actions with them

Can be applied by category, family, or by variant

Can be assigned by the researcher when they add detection

These severity levels determine how the user is notified and can be used to control what the default actions for remediation are

Severities can be Low, Medium, High or Severe

Default actions can be to Notify the user, Quarantine or Delete

PUS behaviour changes

To achieve our mission of “protection without interference”:

- Removed all behaviours that were at severity levels Moderate or Low, except those related to Adware
- Reclassified remaining behaviours into categories that were more verbose

Redistributed PUS categories

PUS categories contained only Moderate and Low behaviours:

- Tool
- Program
- RemoteAccess

Redistributed PUS examples

Behaviours no longer detected:

- Tool:Win32/Miniftp Configurable FTP server
- Program:Win32/TinyProxy Stand alone configurable proxy
- RemoteAccess:Win32/RealVNC Commercially written remote access tool

Detection signatures removed

Redistributed PUS examples

Behaviours detected as different category:

Program:Win32/FakeAdpro Displays false malware reports. Moved to Rogue category.

RemoteAccess:Win32/SubSeven Hacker-written backdoor. Moved to Backdoor category.

Program:Win32/RegCure System optimization tool that makes misleading claims about system files. Moved to Misleading category.

Detection signatures moved

Active PUS categories

Adware
BrowserModifier
Misleading (new)
MonitoringTool
SoftwareBundler

PUS remediation changes

Previously:

- Behaviours determined severity level

Now:

- Categories determine severity level

As a result:

- Only Adware and SoftwareBundler prompt the customer

PUS remediation changes - example

Old method:

- Exhibits behaviour 1 with severity Low that falls under category Program
- Exhibits behaviour 2 with severity Moderate that falls under category BrowserModifier

Would be classified as a BrowserModifier with severity Moderate

PUS remediation changes - example

New method:

Not exhibiting any detectable behaviours detected

Would be classified as a Clean

PUS remediation changes - example

Old method:

- Exhibits behaviour 3 with severity High and falls under category BrowserModifier
- Exhibits behaviour 4 with severity Low and falls under category Program
- Exhibits behaviour 5 with severity Low and falls under category BrowserModifier

Would be classified as a BrowserModifier with severity High

PUS remediation changes - example

New method:

Exhibits behaviour 3 with that falls under category BrowserModifier

Would be classified as a BrowserModifier with severity High

Easier

Points to remember about change

Making changes:

- Define what you want to achieve before you start
- Understand what you do now
- Documentation is essential

Changes made:

- MMPC removed Low and Moderate PUS behaviours except for Adware category
- Realigned signatures for Tool, Program and RemoteAccess