

## A Master Class on IT Security

Roger Grimes Teaches Ransomware Mitigation

> Roger A. Grimes Data-Driven Security Evangelist rogerg@knowbe4.com



### Roger A. Grimes

Data-Driven Defense Evangelist KnowBe4, Inc.

Twitter: @RogerAGrimes LinkedIn: https://www.linkedin.com/in/rogeragrimes/

### **About Roger**

- 30 years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 12 books and over 1,100 magazine articles
- InfoWorld and CSO weekly security columnist 2005 -2019
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

#### **Certification exams passed include:**

- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

### **Roger's Books**

#### HACKING MULTIFACTOR AUTHENTICATION



### Cryptography Apocalypse Preparing for the Day When Quantum Computing Breaks Today's Crypto





**Apress** 





Windows Server 2008 Security





#### ELECTIVE EXAMS NUTSHELI A Desktop Quick Reference O'REILLY'

Pawan K. Bbardwaj & Roger A. Grimes

KnowBe4



### About Us

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- Winner of numerous industry awards







# Agenda

- Why a good backup alone no longer saves you from ransomware
- CISA official recommendations for mitigating ransomware
- Our recommendations
- The policies, technical controls, and education you need to stop ransomware in its tracks
- Incident response
- How to detect any ransomware program no matter how secretive it is



# Agenda

- Why a good backup alone no longer saves you from ransomware
- CISA official recommendations for mitigating ransomware
- Our recommendations
- The policies, technical controls, and education you need to stop ransomware in its tracks
- Incident response
- How to detect any ransomware program no matter how secretive it is



## When A Good Backup Saved You

### **Traditional Ransomware**

- Main actions start as soon as malware is executed
- Spreads (possibly)
- Encrypts files and folders
- Asked for ransom to provide decryption keys



## **But Ransomware Got More Malicious**

Essentially:

- Ransomware crooks got tired of victims saying no
- They realized the access they had was the hacker "gold" and that they could do anything
- Encrypting data and holding it for hostage was the least of the victims worries now...



## What Ransomware Looks Like Now

### Today's Ransomware Workflow



- Victim tricked into executing smaller stub, trojan horse "dropper" file
- After executing, stub immediately downloads additional malware from C&C servers
- 3. Updates itself to keep ahead of AV/EDR detection, new payloads, spreads
- 4. Collects as many passwords as it can
- 5. Notifies ransomware gang of new intrusion
- 6. Dwells (sometimes up to 8 to 12 months)
- 7. Hackers come in, assess and analyze target
- 8. Steal whatever they want
- 9. Launch encryption and ask for ransom

## What Ransomware Looks Like Now

### Today's Ransomware

- Hacker gang often surveys compromised network
- Researches victim organization
- Determines how much ransom to charge based on victim org's ability to pay
- Determines crown jewels of organization
- Exfiltrates data, emails, passwords, etc.
- Encrypts the crown jewels and causes as much critical service disruption as possible
- Says if you don't pay, I release the crown jewels to hackers, competitors, and the Internet



### **More Malicious Ransomware**

Today's Ransomware Summary - Nuclear Badness

- Steals Intellectual Property/Data
- Steals Every Credential It Can Business, Employee, Personal, Customer
- Threatens Victim's Employees and Customers
- Uses Stolen Data to Spear Phish Partners and Customers
- Does Public Shaming

Good luck having a good backup save you!

1-hour webinar on this subject: https://info.knowbe4.com/nuclear-ransomware



### **More Malicious Ransomware**

#### Today's Ransomware Summary - Nuclear Badness

• Threats to exfiltrate data are over 70% of all ransomware attacks now

## 70% of Ransomware Attacks Involved the Threat to Leak Exfiltrated Data (+43% From Q3 2020)

The percentage of ransomware attacks that involved the threat to release stolen data increased from 50% in Q3, to 70% in Q4. Despite this, fewer companies are giving in and paying the extortion demand. In Q3, 74.8% of companies that were threatened with a data leak opted to pay. In Q4, that percentage declined to 59.6%.

https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020#exfil



# Agenda

- Why a good backup alone no longer saves you from ransomware
- CISA official recommendations for mitigating ransomware
- Our recommendations
- The policies, technical controls, and education you need to stop ransomware in its tracks
- Incident Response
- How to detect any ransomware program no matter how secretive it is

### **Cybersecurity and Infrastructure Security Agency (CISA)**

- Primary US gov't organization to protect our cyber assets, networks, devices, and Internet to reduce cybersecurity risk
- https://www.cisa.gov
- Collection of previous organizations (like US-CERT)
- Announces new vulnerabilities and threats
- Shares information
  - Ex. Indicators of Compromise (IOC)
- Recommends mitigations











### Cybersecurity and Infrastructure Security Agency (CISA)

### Example warning



DEFEND TODAY, SECURE TOMORROW

You are subscribed to National Cyber Awareness System Curi Security Agency. This information has recently been updated

#### **CISA Malware Analysis on Supernova**

01/27/2021 07:43 AM EST

Original release date: January 27, 2021

CISA has released a malware analysis report on Supernova m The report contains indicators of compromise (IOCs) and ana of the SolarWinds supply chain attack described in Alert AA2



#### FTC Reports Scammers Impersonating FTC

01/26/2021 05:17 PM EST

#### Original release date: January 26, 2021

The Federal Trade Commission (FTC) has released information on scammers attempting to impersonate the FTC. The scammers operate an FTC-spoofed website that claims to provide instant cash payments and tries to trick consumers into disclosing their financial information. The real FTC does not require such information and scammers can use this information to steal consumers' money and identities.

CISA encourages consumers to review the FTC blog post and CISA's Security Tips on Avoiding Social Engineering and Phishing Attacks and Preventing and Responding to Identity Theft.

CISA encourages users and administrators to review Malware Analysis Report MAR-10319053-1.v1 and the SolarWinds advisory for more information on Supernova.





TURE

Cybersecurity and Infrastructure Security Agency (CISA)

- You should subscribe to their alerts:
- https://public.govdelivery.com/accounts/USDHSCISA/subscriber/new

#### **Email Updates**

To sign up for updates or to access your subscriber preferences, please enter your contact information below.

Subscription Type	Email	~
Email Address *		
Submit Cancel		



Your contact information is used to deliver requested updates or to access your subscriber preferences.

Privacy Policy | Cookie Statement | Help



### Cybersecurity and Infrastructure Security Agency (CISA)

### **Quick Links**

CISA Insights Combating Cyber Crime Coordinated Vulnerability Disclosure Cyber Essentials Cyber Incident Response Cyber Safety Cyber Resource Hub Supply Chain Compromise Cybersecurity Governance Cybersecurity Insurance Cybersecurity Training & Exercises Detection and Prevention Education EO 13800 Deliverables

Ransomware Guidance and Resources Cyber Hygiene Services Information Sharing Protecting Critical Infrastructure Securing Federal Networks Shop Safely

https://www.cisa.gov/ransomware



### Cybersecurity and Infrastructure Security Agency (CISA)

Primary recommendations

#### What are some mitigations against ransomware?

CISA recommends the following precautions to protect users against the threat of ransomware:

- Update software and operating systems with the latest patches. Outdated applications and operating of most attacks.
- Never click on links or open attachments in unsolicited emails.
- · Back up data on a regular basis. Keep it on a separate device and store it offline.
- Follow safe practices when using devices that connect to the Internet. Read Good Security Habits for

From https://www.cisa.gov/ransomware

#### Ransomware

Ransomware Alerts and Statements

Ransomware Fact Sheets and Infographics

**Ransomware Guides and Services** 

Ransomware Reference Materials for K-12 School and School District IT Staff

Ransomware Reference Materials for K-12

Ransomware Reference Materials for Parents, Teachers, and School Administrators

Ransomware Reference Materials for Students

Ransomware Trainings and Webinars



Cybersecurity and Infrastructure Security Agency (CISA)

Primary Prevention recommendations

### Actions for Today – Make Sure You're Not Tomorrow's Headline:

- 1. Backup your data, system images, and configurations and keep the backups offline
- 2. Update and patch systems
- 3. Make sure your security solutions are up to date
- Review and exercise your incident response plan
- 5. Pay attention to ransomware events and apply lessons learned

From https://www.cisa.gov/ransomware



# Agenda

- Why a good backup alone no longer saves you from ransomware
- CISA official recommendations for mitigating ransomware
- Our recommendations
- The policies, technical controls, and education you need to stop ransomware in its tracks
- Incident Response
- How to detect any ransomware program no matter how secretive it is



Risk-Ranking Threats (not all threats are equal)

 Risk-rank likely threats If you do that...



- Majority of all malicious digital breaches are due to social engineering and phishing
- Second most is due to unpatched software
- Everything else added up all together is small part of the risk
- Concentrate your efforts where your prevention efforts will mean the most



#### Top Ransomware Vectors in 2021

- Email/Phishing
- Unpatched software
- RDP/Weak Passwords
- USB key and other minority causes



https://blog.knowbe4.com/heads-up-email-phishing-is-now-the-top-ransomware-attack-vector





Most Important Critical Defenses

- Good, <u>thorough</u>, <u>complete</u> <u>system</u>, <u>tested</u>, <u>offline</u>, <u>up-to-date</u>, backup and restore
  - Most organizations do not have this
  - But in most cases of ransomware, a backup alone will not gain you much
- You <u>MUST</u> stop ransomware from accessing your environment in the first place!
  - Everything else must be secondary to these two defenses



### **Best Defenses**

### **General Defense Methods**

- Policies
- Technical Controls
  - Anti-Malware Software
  - Anti-Spam/Phishing
  - Content Filtering
- Security Awareness Training



https://blog.knowbe4.com/the-three-pillars-of-the-three-computer-security-pillars



### **Best Defenses**

Top 5 Defenses for Most Organizations

(in order of importance)

- Focus on mitigating Social Engineering
- Patch Internet-accessible software
- Use non-guessable passwords/multifactor authentication
  - Different passwords for every website and service

### Teach Users How to Spot Rogue URLs

- https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks
- https://info.knowbe4.com/rogue-urls

### Use Least-Permissive Permissions



### Give "Red Flags" Training

### Social Engineering **Red Flags**

前四

C 1000 / 146

I can buy a ticket home:

Your CEO

http://www.bankofarnerica.com



- I don't recognize the sender's email address as someone I ordinarily communicate with.
- This email is from someone outside my organization and it's not related to my job responsibilities.
- · This email was sent from someone inside the organization or from a customer, vendor, or partner and is very unusual or out of character.
- · Is the sender's email address from a suspicious domain (like micorsoft-support.com)?
- I don't know the sender personally and they were not vouched for by someone I trust.
- I don't have a business relationship nor any past communications with the sender.
- · This is an unexpected or unusual email with an embedded hyperlink or an attachment from someone I haven't communicated with recently.



- . I was cc'd on an email sent to one or more people, but I don't personally know the other people it was sent to.
- . I received an email that was also sent to an unusual mix of people. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.



- . I hover my mouse over a hyperlink that's displayed in the email message, but the link-to address is for a different website. (This is a big red flag.)
- · I received an email that only has long hyperlinks with no further information. and the rest of the email is completely blank.
- . I received an email with a hyperlink that is a misspelling of a known web site. For instance, www.bankofarnerica.com - the "m" is really two characters - "r" and "n."



- · The sender included an email attachment that I was not expecting or that makes no sense in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- · I see an attachment with a possibly dangerous file type. The only file type that is always safe to click on is a .txt file.

#### CONTENT

- Is the sender asking me to click on a link or open an attachment to avoid a negative consequence or to gain something of value?
- Is the email out of the ordinary, or does it have bad grammar or spelling errors?
- Is the sender asking me to click a link or open up an attachment that seems odd or illogical?
- · Do I have an uncomfortable gut feeling about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a compromising or embarrassing picture of myself or someone | know?

#### https://blog.knowbe4.com/share-the-red-flags-of-social-engineering-infographic-with-your-employees



# REGUE URLS

Spotting malicious URLs is a bit of an art. The examples represented here are some of the common tricks used by hackers and phishers to fool users to visiting malicious websites. The methods shown here could be used by legitimate services, but if you see one of these "tricks" you need to make sure you're dealing with the organization you think you are.

#### **Domain Mismatches**

#### Look-a-Alike Domains

Domain names which seem to belong to respected, trusted brands.

#### Slight Misspellings

Microsoftnline <v5pz@onmicrosoft.com>

#### www.llnkedin.com

Brand name in URL, but not real brand domain

ee.microsoft.co.login-update-dec20.info

www.paypal.com.bank/logon?user=johnsmith@gmail.com

ww17.googlechromeupdates.com/

Brand name in email address but doesn't match brand domain

Bank of America <BankofAmerica@customerloyalty.accounts.com>

#### Brand name is in URL but not part of the domain name

devopsnw.com/login.microsoftonline.com?userid=johnsmith

#### **URL Domain Name Encoding**

https://%77%77%77%6B%6E%6F%77%62%654.%63%6F%6D

#### Shortened URLs

When clicking on a shortened URL, watch out for malicious redirection.

https://bit.ly/2SnA7Fnm



<Despina.Orrantia6731610@gmx.com>

Human Services .gov

#### **Strange Originating Domains**

MAERSK

#### <info@onlinealxex.com.pl>

#### **Overly Long URLs**

URLs with 100 or more characters in order to obscure the true domain.

ttp://innocentwebsite.com/irs.gov/logon/fasdjkg-sajdkjndf inbkasldifbkajsdbfkjbasdf/adsnfjksdngkfdfgfgjhfgd/ght.php

#### File Attachment is an Image/Link

It looks like a file attachment, but is really an image file with a malicious URL.

INV39391.pdf https://d.pr/free/f/jsaeoc Click or tap to follow link.

#### **Open Redirectors**

URLs which have hidden links to completely different web sites at the end.

#### t-info.mail.adobe.com/r/?id=hc347a&p1=evilwebsite.com

KnowBe4

PDF

52 KB

https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks



### **Best Defenses**

### KnowBe4 Resources

- Ransomware portal
  - https://www.knowbe4.com/ransomware
- Ransomware guide
  - https://info.knowbe4.com/ransomware-hostage-rescue-manual-0
- Ransomware simulator
  - https://www.knowbe4.com/ransomware-simulator





### **Ransomware Simulator**

#### <u>Ransim</u>

- Simulates over a dozen common ransomware programs
- Is not real ransomware, does not use your files
- Tests your current defenses



https://www.knowbe4.com/ransomware-simulator



## **All Anti-Phishing Defenses**

### Everything You Can Try to Prevent Phishing

- Policies, Education
- Secure Desktops, secure configurations, not logged in as admin all the time
- Anti-Phishing filters
- AV/EDR
- Detonation sandboxes for URLs and file attachments
- SPF, DKIM, DMARC (https://info.knowbe4.com/dmarc-spf-dkim-webinar)
- Whitelisting, blacklisting, gray listing, reputation filters
- Application Control Programs
- Etc.



## **All Anti-Phishing Defenses**

### **Everything You Can Try to Prevent Phishing**

- Webinar
  - https://info.knowbe4.com/webinar-stay-out-of-the-net

#### **ON-DEMAND WEBINAR**

### Stay out of the Net: Your Ultimate Guide to Phishing Mitigation



E-BOOK Comprehensive Anti-Phishing Guide

- E-book
  - https://www.knowbe4.com/hubfs/Comprehensive-Phishing-Guide.pdf



# Agenda

- Why a good backup alone no longer saves you from ransomware
- CISA official recommendations for mitigating ransomware
- Our recommendations
- The policies, technical controls, and education you need to stop ransomware in its tracks
- Incident Response
- How to detect any ransomware program no matter how secretive it is



### **Response Priorities**

- Stop spread
- Stop damage
- Close holes



#### Cybersecurity and Infrastructure Security Agency (CISA)

Primary Incident Response recommendations

### Actions to Recover If Impacted - Don't Let a Bad Day Get Worse:

- 1. Ask for help! Contact CISA, the FBI, or the Secret Service
- 2. Work with an experienced advisor to help recover from a cyber attack
- 3. Isolate the infected systems and phase your return to operations
- 4. Review the connections of any business relationships (customers, partners, vendors) that touch your network
- 5. Apply business impact assessment findings to prioritize recovery

From https://www.cisa.gov/ransomware



### **Response Recommendations**

- Practice your ransomware response plan
  - You have one of those, right?
- Notify management
- Get legal involved, let legal make all outside calls
- Freeze Internet access
- Call insurance company if you have cybersecurity insurance
- Call in experts
- Identify ransomware strain
- Decide ahead of time if you will pay the ransom



### **Data Exfiltration Considerations**

- Not all ransomware gangs claiming to have exfiltrated data really have
- So ask for verification
- Verify it was deleted as promised before you pay all of the ransom



#### **Negotiation Considerations**

- Talk to someone who knows the ransomware gang to understand how negotiations should go
- Never pay all up front
  - Ask for proof that decipher kill will work
- Consider using professional ransomware negotiator
- Ex: Coveware (www.coveware.com)



#### **Response Recommendations**

**Public Relations Response** 

- Have a ransomware PR plan already in place
- Have a PR team that will work with you already in place and practiced
- PR to employees
- PR to customers
- PR to investors (if it applies)
- PR to public



### Inviting Others to Help

- Getting CISA involved is great
- Getting other authorities like the FBI and Secret Service can be great
- But recognize they can easily take over what you do and how you do it
- They can seize your involved assets for a long time
- They are usually very helpful, but don't lose sight that when you get them involved there is a chance you lose control of your own response
- Let mgmt. and legal make the decision to get any outside entity involved



### **Cybersecurity Insurance**

- I'm a big fan
- Fairly low cost for the financial risk it covers
- Make sure the policy doesn't include social engineering exclusions
- Clarify ahead of time who is ultimately in charge of the response and who makes the "ransom" decision
- Call insurance company's incident response person/team ahead of time to establish a relationship and document procedures



# Agenda

- Why a good backup alone no longer saves you from ransomware
- CISA official recommendations for mitigating ransomware
- Our recommendations
- The policies, technical controls, and education you need to stop ransomware in its tracks
- How to detect any ransomware program no matter how secretive it is



#### **Determining Where Malware Is**

### **Biggest Risk**

- When malware is undetected
  - Called dwell time
- When undetected, malware and hackers can be doing anything
- Risk increases over time
- Average ransomware dwells from 8 months to a year without being detected



### **Detecting Malware**

### Summary

- Use an application control program in monitor/audit-only mode
  - Or any program that can detect brand new, previously unknown, executions
- Create a snapshot rule baseline from a clean image
- Detect and report on newly executed programs
- Copy new execution log events to centralized database
- Research any and all new executions immediately
- Create reports and security workflows from this info



#### **Detecting Malware**

**Application Control Programs** 

- Allows you to whitelist and blacklist executables and other programs
- Most allow monitoring/audit-only modes versus blocking/enforcement modes
- Most can build rules by "snapshotting" a system
- Most write events to security logs when new executions not on baseline occur



#### **Detecting Malware**

**Application Control Program Examples** 

- AppLocker and Windows Defender Application Control on Microsoft Windows
- Most major AV programs have a version
- Commercial versions: Beyond Trust, Carbon Black, Tripwire, Cisco, Ivanti
- Open source versions: SE Linux, AppArmor, Fapolicyd
- NIST SP 800-167 "Guide to Application Whitelisting"



Example Application Control Program Deployment

- Been in Microsoft Windows enterprise versions since Windows 7/Windows Server 2008
  - Early related Windows feature was Software Restriction Policies
  - Windows Defender Application Control (WDAC), released in Windows 10
  - WDAC is a far more serious application control program than AppLocker and takes much more planning and administration to run
  - AppLocker does not promise a true security boundary, WDAC does
  - For our purposes, AppLocker is good enough
- Stand-alone, Group Policy, MDM (e.g. InTune, etc.)



Example Application Control Program Deployment

- Run Gpedit.msc
- Computer Configuration\Windows Settings\Security Settings\
- Application Control Policies





Example Application Control Program Deployment

AppLocker

AppLocker Rule Categories:

- Executable Rules
- Windows Installer Rules
- Script Rules
- Packaged app Rules (Modern apps)

AppLocker
 Executable Rules
 Windows Installer Rules
 Script Rules
 Packaged app Rules

Each can be enabled separately



#### **Example Application Control Program Deployment**

A I I	Local Computer Policy	Appl ocker provides access			AppLocker Properties X
ADDI OCKER	V 👫 Computer Configuration	- A Appendice provides access	AppLocker Properties X		
, appeoener	> Software Settings	Dente and the			Enforcement Advanced
	<ul> <li>Windows Settings</li> <li>Name Recelution Policy</li> </ul>	Getting Started	Enforcement Advanced		Specify whether Appliacker niles are enforced for each nile
	Scripts (Startup/Shutdown)	AppLocker uses rules and the properties of applications. If rules are present in a rule of	Specify whether AppLocker rules are enforced for each rule collection.		collection.
	> Ib Security Settings	rules will be permitted to run. AppLocker n			Executable rules:
	> Account Policies		Executable rules:		
	> 🙀 Local Policies	More about AppLocker	Configured		
	> Windows Defender Firewall with Advanced Secu Network List Manager Policies	Which editions of Windows support	Enforce rules $\sim$		Audit only ~
	> 2 Public Key Policies	Configure Rule Enforcement			Windows Installer rules:
	Software Restriction Policies		Windows Installer rules:		Configured
	Application Control Policies	For the AppLocker policy to be Identity service must be supping	Configured		
	V AppLoc Impart Policy		Enforce rules 🗸		Audit only
	> The Export Policy	Use the enforcement settings for each rul enforced or audited. If rule enforcement h by default.			
					Script rules:
	Pack Clear Policy		Script rules:		Configured
	> 🕄 IP Security I View >	Configure rule enforcement			
	> Advanced A Deposition		Enforce rules 🗸 🗸		Audit only
	Policy-based Q     Properties     Administrative Terr     Help	More about rule enforcement			
			Packaged app Rules:		Packaged app Rules:
	> 🧾 Control Panel	Overview	Configured		Configured
	> Network	Executable Rules			Audit only V
	Printers Secure	Rules: 0	Enforce rules		
	Start Menu and Tarkhar	Enforcement not configured: Rules			
	System	Windows Installer Pules			
	> 🛄 Windows Components	Bules: 0			
	🍓 All Settings	Enforcement not configured: Rules			
	✓ ss User Configuration	III Const Dates	More about rule enforcement		More about rule enforcement
	> Software Settings 🗸 🗸	Diani 0	Hore about the different		
	د >	Enforcement out configured Rides			
			OK Cancel Apply		OK Cancel <u>A</u> pply

#### **Example Application Control Program Deployment**

AppLocker	<ul> <li>Local Computer Policy</li> <li>Computer Configuration</li> <li>Software Settings</li> <li>Windows Settings</li> </ul>	Action User		
	> 🔛 Name Resolution Policy	Automatically Generate Executable Rules	Automatically Generate Executable Rules	×
	Scripts (Startup/Shutdown)  Deployed Printers  Security Settings	Folder and Permissions	Folder and Permissions	
	> CACcount Policies	This wizard helps you create groups of AppLocker rules by analyzing the files within a folder that you select.	This wizard helps you create groups of AppLocker rules by analyzing the files within a folder that you select.	
	Windows Defender Firev     Windows Defender Firev     Windows List Manager Pi     Windows Defender Firev     Windows Defender Firev	User or security group that the rules will apply to:	User or security group that the rules will apply to:	
	<ul> <li>Software Restriction Poli</li> <li>Application Control Poli</li> <li>Appl ocker</li> </ul>			
	> F Executable Rules > T Windows Install	Folder that contains the files to be analyzed:           C:\Program Files         Browse	Folder that contains the files to be analyzed: c:\ Browse	
	> 🧾 Script Rules > 🧱 Packaged app F	Name to identify this set of rules: Program Files	Name to identify this set of rules: Baseline Rules	
	> (1) IP Security Policies on I > 2 Advanced Audit Policy	More about these settings	More about these settings	
	Policy-based QoS     Administrative Templates	< Previous Next > Create	Ca <pre>Ca</pre> <pre>Create</pre> Ca	ncel
	> Control Panel > Control Panel	Help		

### **Example Application Control Program Deployment**

Automatically Generate Executable Rules	X Automatically Generate Executable Rules ×
Rule Preferences	Rule Preferences
<ul> <li>Select the type of rules that you want to create. You should only create file hash rules when necessary. A file hash rule must be revised every time that the file is updated and a large number of file hash rules might affect system performance.</li> <li>Create publisher rules for files that are digitally signed If a file is not signed, create the following type of rule: <ul> <li>File hash: Rules are created using a file's hash</li> <li>Path: Rules are created using file's path</li> </ul> </li> <li>Create file hash rules for all files</li> </ul>	Select the type of rules that you want to create. You should only create file hash rules when necessary. A file hash rule must be revised every time that the file is updated and a large number of file hash rules might affect system performance.
Reduce the number of rules created by grouping similar files	Reduce the number of rules created by grouping similar files
< Previous Next > Create Cancel	<pre></pre>



### **Example Application Control Program Deployment**

tomatically Generate Execu	table Rules		×	
The folder analysis is	esemplete and the followin	e o deco 20 ha a dela da a tha a clian	^	AppLocker
Rule Type	Rules	Files		The default rules are currently not in the rule list for this rule collection. When creating rules, it is recommended that you also create the default rules to ensure that important system
Publisher	64	907		files will be allowed to run.
File Hash	1345	1691		Do you want to create the default rules now?
Total	1409	2598		
Review files the	at were analyzed			Yes No
View rules that	will be automatically crea	ted		
Click Create to close	e the wizard and create the	rules.		
Some folders a has skipped th	ind files could not be read ese folders and files.	during rule generation. The wizard	v	Note: If you enabled enforcement mode
		< Previous Next > Create	Cancel	you might want to say les here.



#### **Example Application Control Program Deployment**

✓       Computer Configuration       ✓       Allow       Everyone       Baseline Rules: MICROSOFT® WINDO       Publisher         ✓       Mindows Settings       ✓       Allow       Everyone       Baseline Rules: MICROSOFT® WINDO       Publisher         ✓       Mindows Settings       ✓       Allow       Everyone       Baseline Rules: MICROSOFT® WINDO       Publisher         ✓       Scripts (Startup/Shutdown)       ✓       Allow       Everyone       Baseline Rules: MICROSOFT® WINDO       Publisher         ✓       Scrupts (Startup/Shutdown)       ✓       Allow       Everyone       Baseline Rules: MICROSOFT® WINDO       Publisher         ✓       Maccount Policies       ✓       Allow       Everyone       Baseline Rules: MICROSOFT® UNDOW       Publisher         ✓       Mindows Defender Firewall with Advancer       ✓       Allow       Everyone       Baseline Rules: MICROSOFT® DNB Sig       Publisher         ✓       Motows Installer Rules       Microsos Defender Firewall with Advancer       ✓       ✓       Allow       Everyone       Baseline Rules: MICROSOFT® DNB Sig       Publisher         ✓       Motows Installer Rules       ✓       Allow       Everyone       Baseline Rules: MICROSOFT® DNB Sig       Publisher         ✓	Local Computer Policy	Action	User	Name	Condition	Б
<ul> <li>Software Settings</li> <li>Windows Settings</li> <li>Windows Settings</li> <li>Allow Everyone</li> <li>Allow Everyone</li> <li>Baseline Rules: HTML HELP signed by O Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT(R) CONNE Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT WINDO Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT Policise</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) WINDO Publisher</li> <li>Allow Ever</li></ul>	🗸 👰 Computer Configuration	M Allow	Everyone	Baseline Rules: MICROSOFT® WINDO	Publisher	
<ul> <li>Windows Settings</li> <li>Mame Resolution Policy</li> <li>Scripts (Startup/Shutdown)</li> <li>Deployed Printers</li> <li>Scripts (Startup/Shutdown)</li> <li>Catalantian and the settings</li> <li>Allow Everyone</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT(R) CONNE</li> <li>Publisher</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) CONNE</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT BINSTALLER</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) CONNE</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) CONNE</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) CONNE</li> <li>Publisher</li> <li>Allow Ever</li></ul>	> 🚞 Software Settings	Allow	Everyone	Baseline Rules: HTML HELP signed by O	Publisher	
Name Resolution Policy       Scripts (Startup/Shutdown)       Publisher       Publisher         Mame Resolution Policy       Allow       Everyone       Baseline Rules: MICROSOFT © WINDO       Publisher         Publisker       Allow       Everyone       Baseline Rules: INTERNET EXPLORER sig       Publisher         Allow       Everyone       Baseline Rules: WINDOWS INSTALLER       Publisher         Mindows Defender Firewall with Advanced       Allow       Everyone       Baseline Rules: WICROSOFT © DRM sig       Publisher         Mindows Defender Firewall with Advanced       Allow       Everyone       Baseline Rules: WICROSOFT (R) WINDO       Publisher         Mindows Defender Firewall with Advanced       Allow       Everyone       Baseline Rules: WICROSOFT (R) WINDO       Publisher         Mindows Defender Firewall with Advanced       Allow       Everyone       Baseline Rules: WICROSOFT (R) WINDO       Publisher         Mindows Defender Firewall with Advanced       Allow       Everyone       Baseline Rules: WICROSOFT (R) WINDO       Publisher         Mindows Defender Firewall with Advanced       Allow       Everyone       Baseline Rules: WinDOWS © SEARCH si       Publisher         Mallow       Everyone       Baseline Rules: WinDOWS © SEARCH si       Publisher       Publisher         Mindows Defender	✓	Allow	Everyone	Baseline Rules: MICROSOFT(R) CONNE	Publisher	
<ul> <li>Scripts (Startup/Shutdown)</li> <li>More Deployed Printers</li> <li>Security Settings</li> <li>Account Policies</li> <li>Account Policies</li> <li>Account Policies</li> <li>Allow Everyone</li> <li>Baseline Rules: INTERNET EXPLORER sig Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: WINDOWS INSTALLER Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: WINDOWS SEARCH si Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) WINDO Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: StartMenuExperienceHo File Hash</li> <li>Allow Everyone</li> <li>Baseline Rules: StartMenuExperienceHo File Hash</li> <li>Allow Everyone</li> <li>Baseline Rules: StartMenuExperienceHo File Hash</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT EDEE signe Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT EDE KEE Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT EDE Signe Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT EDE KEE Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT ED</li></ul>	> Particular Sector Policy	Allow	Everyone	Baseline Rules: MICROSOFT @ WINDO	Publisher	
<ul> <li>         Deployed Printers         Security Settings         Security Policies on Local Computer         Security Policy Securi</li></ul>	Scripts (Startup/Shutdown)	Allow	Everyone	Baseline Rules' THE CURLEXECUTABLE	Publisher	
<ul> <li>Security Settings</li> <li>Security Settings</li> <li>Account Policies</li> <li>Windows Defender Firewall with Advanced</li> <li>Windows Defender Firewall with Advanced</li> <li>Allow Everyone</li> <li>Public Key Policies</li> <li>Public Key Policies</li> <li>Public Key Policies</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) WINDOW. Publisher</li> <li>Public Key Policies</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) WINDOW. Publisher</li> <li>Public Key Policies</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) WINDO Publisher</li> <li>Application Control Policies</li> <li>Application Control Policies</li> <li>Application Control Policies</li> <li>Application Control Policies</li> <li>Allow Everyone</li> <li>Baseline Rules: Windows.WARP JITServi Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: ADOBE® FLASH® PLAY Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: StattMenuExperimetho File Hash</li> <li>Allow Everyone</li> <li>Baseline Rules: StattMenuExperimetho File Hash</li> <li>Allow Everyone</li> <li>Baseline Rules: NartatorQuickStatt.exe</li> <li>He Hash</li> <li>Allow Everyone</li> <li>Baseline Rules: NartatorQuickStatt.exe</li> <li>He Hash</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT EDGE signe</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT EDGE were</li> <li>Allow Everyone</li></ul>	> 📺 Deployed Printers	Allow	Everyone	Baseline Rules: INTERNET EXPLORER sig.	Publisher	
<ul> <li>Account Policies</li> <li>Local Policies</li> <li>Windows Defender Firewall with Advances</li> <li>Network List Manager Policies</li> <li>Public Key Policies</li> <li>Software Restriction Policies</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT © DRN Windows. WARP JITServi</li> <li>Publisher</li> <li>Public Key Policies</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) WINDO</li> <li>Publisher</li> <li>Public Key Policies</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) WINDO</li> <li>Publisher</li> <li>Public Key Policies</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) WINDO</li> <li>Publisher</li> <li>Public Key Policies</li> <li>Allow Everyone</li> <li>Baseline Rules: WINDOWS SEARCH si</li> <li>Publisher</li> <li>Public Key Policies</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) WINDO</li> <li>Publisher</li> <li>Publisher</li></ul>	Security Settings	Allow	Everyone	Baseline Rules: WINDOWS INSTALLER -	Publisher	
<ul> <li>Local Policies</li> <li>Windows Defender Firewall with Advancet</li> <li>Windows Defender Firewall with Advancet</li> <li>Network List Manager Policies</li> <li>Public Key Policies</li> <li>Software Restriction Policies</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT © DRM sig Publisher</li> <li>Software Restriction Policies</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) WINDO Publisher</li> <li>Software Restriction Policies</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) WINDO Publisher</li> <li>Software Restriction Policies</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) WINDO Publisher</li> <li>Appl.cocker</li> <li>Allow Everyone</li> <li>Baseline Rules: ADOBE © FLASH © PLAY Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: setup.exe, _isdel.exe</li> <li>File Hash</li> <li>Software Settings</li> <li>Advanced Audit Policy Configuration</li> <li>Advanistrative Templates</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT EDGE Signe</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT EDGE WEB</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT WINDOWS</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline</li></ul>	Account Policies		Everyone	Baseline Rules: MICROSOFT ONEDRIVE	Publisher	
<ul> <li>Windows Defender Pirewail with Advanced</li> <li>Allow</li> <li>Everyone</li> <li>Baseline Rules: Windows 9 SEARCH si</li> <li>Publick Rey Policies</li> <li>Software Restriction Policies</li> <li>Application Control Policies</li> <li>Allow</li> <li>Everyone</li> <li>Baseline Rules: Windows Mathematics Windows WARP.JITServi</li> <li>File Hash</li> <li>Allow</li> <li>Everyone</li> <li>Baseline Rules: StartMenuExperienceHo</li> <li>File Hash</li> <li>Allow</li> <li>Everyone</li> <li>Baseline Rules: MICROSOFT EDGE signe</li> <li>Allow</li> <li>Everyone</li> <li>Baseline Rules: MICROSOFT EDGE WEB</li> <li>Publisher</li> <li>Allow</li> <li>Everyone</li> <li>Baseline Rules: MICROSOFT EDGE WEB</li> <li>Publisher</li> <li>Allow</li> <li>Everyone</li> <li>Baseline Rules: MICROSOFT WINDOWS</li> <li>Publisher</li> <li>Allow</li> <li>Everyone</li> <li>Baseline Rules: MICROS</li></ul>	Local Policies		Evenyone	Baseline Rules: MICROSOFT® DRM sig	Dublisher	
<ul> <li>Network Exist Manager Policies</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) WINDO</li> <li>Public Key Policies</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) WINDO</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT (R) WINDO</li> <li>Policitation Control Policies</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT EDGE signe</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT EDGE WEB</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT WINDOWS DRIVE OPTI</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT EDGE WEB</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: State MICROSOFT WINDOWS</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: State MICROSOFT WINDOWS</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: State MICROSOFT WINDOWS</li> <li>Publis</li></ul>	Windows Derender Firewall with Advanced Network List Manager Delision	Allow	Evenyone	Baseline Rules: WINDOWS® SEARCH si	Dublisher	
<ul> <li>Allow Everyone Baseline Rules: Windows.WARP.JITServi File Hash</li> <li>Allow Everyone Baseline Rules: Windows.WARP.JITServi File Hash</li> <li>Allow Everyone Baseline Rules: ADOBE® FLASH® PLAY Publisher</li> <li>Mindows Installer Rules</li> <li>Mindows Installer Rules</li> <li>Mindows Installer Rules</li> <li>Script Rules</li> <l< td=""><td>Dublic Key Policies</td><td>Allow</td><td>Evenyone</td><td>Baseline Rules: MICROSOFT (R) WINDO</td><td>Dublisher</td><td></td></l<></ul>	Dublic Key Policies	Allow	Evenyone	Baseline Rules: MICROSOFT (R) WINDO	Dublisher	
<ul> <li>Allow Everyone Baseline Rules: ADOBE® FLASH® PLAY Publisher</li> <li>Allow Everyone Baseline Rules: setup.exe, jsdel.exe</li> <li>Allow Everyone Baseline Rules: StartMenuExperienceHo File Hash</li> <li>Allow Everyone Baseline Rules: MICROSOFT EDGE signe Publisher</li> <li>Allow Everyone Baseline Rules: MICROSOFT EDGE signe Publisher</li> <li>Allow Everyone Baseline Rules: MICROSOFT EDGE Signe Publisher</li> <li>Allow Everyone Baseline Rules: MICROSOFT EDGE WEB Publisher</li> <li>Allow Everyone Baseline Rules: StartMenuExperienceHo File Hash</li> <li>Allow Everyone Baseline Rules: MICROSOFT EDGE Signe Publisher</li> <li>Allow Everyone Baseline Rules: MICROSOFT EDGE WEB Publisher</li> <li>Allow Everyone Baseline Rules: MICROSOFT EDGE WEB Publisher</li> <li>Allow Everyone Baseline Rules: StartMenuExperienceHo File Hash</li> <li>Allow Everyone Baseline Rules: MICROSOFT EDGE WEB Publisher</li> <li>Allow Everyone Baseline Rules: MICROSOFT EDGE WEB Publisher</li> <li>Allow Everyone Baseline Rules: MICROSOFT WINDOWS Publisher</li> <li>Allow Everyone Baseline Rules: Start Heller Start.</li> <li>Allow Everyone Baseline Rules: Start Heller Start.</li> <li>Allow Everyone Baseline Rules: MICROSOFT WINDOWS Publisher</li> <li>Allow Everyone Baseline Rules: MICROSOFT WINDOWS Publisher</li> <li>Allow Everyone Baseline Rules: Start Heller Start.</li> <li>Allow Everyone Baseline Rules: Start MAXAUDIO Sign Publisher</li> &lt;</ul>	Software Restriction Policies	Allow	Everyone	Baseline Rules: Windows WARP IITServi	File Hash	
<ul> <li>AppLocker</li> <li>AppLocker</li> <li>AppLocker</li> <li>Allow</li> <li>Evecutable Rules</li> <li>Windows Installer Rules</li> <li>Script Rules</li> <li>Script</li></ul>	Application Control Policies	Allow	Everyone	Baseline Rules: ADOBE® ELASH® PLAV	Publisher	
<ul> <li>Figure Configuration</li> <li>Configuration</li> <li>C</li></ul>	✓ ☐ AppLocker	Allow	Everyone	Baseline Rules: setup.exeisdel.exe	File Hash	
<ul> <li>Windows Installer Rules</li> <li>Script Rules</li> <li>Script Rules</li> <li>Script Rules</li> <li>Packaged app Rules</li> <li>Packaged app Rules</li> <li>Policy-based QoS</li> <li>Advanced Audit Policy Configuration</li> <li>Advanced Audit Policy Configuration</li> <li>Policy-based QoS</li> <li>Administrative Templates</li> <li>Software Settings</li> <li>Mindows Settings</li> <li>Administrative Templates</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT EDGE WEB Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT EDGE WEB Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT WINDOWS DRIVE OPT Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT WINDOWS DRIVE OPT Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT WINDOWS Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: Section Baseline Rules: Sector Windows Settings</li> <li>Allow Everyone</li> <li>Baseline Rules: Sector Windows Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: Sector Windows</li></ul>	> 🗮 Executable Rules	Allow	Everyone	Baseline Rules: WpcUapApp.exe	File Hash	
<ul> <li>Script Rules</li> <li>Script Rules</li> <li>Packaged app Rules</li> <li>Packaged Rules</li> <li>Packa</li></ul>	> 🔄 Windows Installer Rules	Allow	Everyone	Baseline Rules: XGpuEiectDialog.exe	File Hash	
<ul> <li>Packaged app Rules</li> <li>Packaged Packaged Packaged</li></ul>	> 🧾 Script Rules	Allow	Everyone	Baseline Rules: StartMenuExperienceHo	File Hash	
<ul> <li>IP Security Policies on Local Computer</li> <li>Advanced Audit Policy Configuration</li> <li>Advanced Audit Policy Configuration</li> <li>Policy-based QoS</li> <li>Administrative Templates</li> <li>Software Settings</li> <li>Mindows Settings</li> <li>Administrative Templates</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT EDGE Signe</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT EDGE WEB</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT HEDE Signe</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT WINDOWS DRIVE OPTI</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: REMOTEFX HELPER Sign</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: Settings</li> <li>Publisher</li> </ul>	> 📟 Packaged app Rules	Allow	Everyone	Baseline Rules: NarratorOuickStart.exe	File Hash	
<ul> <li>Advanced Audit Policy Configuration</li> <li>Policy-based QoS</li> <li>Administrative Templates</li> <li>Software Settings</li> <li>Minows Settings</li> <li>Administrative Templates</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT EDGE Signe</li> <li>Publisher</li> <li>Publisher</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT EDGE WEB</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT USE OF WEB</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT USE WEB</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: REMOTEFX HELPER sign</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: Software Settings</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: Software Settings</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: Software Settings</li> <li>Publisher</li> <li>Publisher</li> <li>Publisher</li> <li>Publisher</li> <li>Publisher</li> <li>Publisher</li> <li>Publisher</li> </ul>	> 뢿 IP Security Policies on Local Computer	Allow	Everyone	Baseline Rules: CapturePicker.exe	File Hash	
<ul> <li>Jin Policy-based QoS</li> <li>Administrative Templates</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Administrative Templates</li> <li>Allow Everyone Baseline Rules: MICROSOFT EDGE WEB Publisher</li> <li>Allow Everyone Baseline Rules: MICROSOFT WINDOWS Publisher</li> <li>Allow Everyone Baseline Rules: Settings</li> </ul>	> Advanced Audit Policy Configuration	Allow	Everyone	Baseline Rules: MICROSOFT EDGE signe	Publisher	
<ul> <li>Administrative Templates</li> <li>Administrative Templates</li> <li>User Configuration</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Allow Everyone</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT EDGE WEB Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: MICROSOFT WINDOWS Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: FaceFodUninstaller.exe</li> <li>Hash</li> <li>Allow Everyone</li> <li>Baseline Rules: Sep.exe, sftp.exe, ssh-ad</li> <li>File Hash</li> <li>Allow Everyone</li> <li>Baseline Rules: NAVES MAXXAUDIO sig</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: Software Settings</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: INTEL © SOFTWARE GU</li> <li>Publisher</li> </ul>	> Policy-based QoS	Allow	Everyone	Baseline Rules: WINDOWS DRIVE OPTI	Publisher	
<ul> <li>User Configuration</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Administrative Templates</li> <li>Allow Everyone</li> <li>Baseline Rules: REMOTEFX HELPER sign</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: Settings</li> <li>Publisher</li> <li>Allow Everyone</li> <li>Baseline Rules: INTEL® SOFTWARE GU</li> <li>Publisher</li> </ul>	> 🦰 Administrative Templates	Allow	Everyone	Baseline Rules: MICROSOFT EDGE WEB	Publisher	
<ul> <li>Software Settings</li> <li>Windows Settings</li> <li>Administrative Templates</li> <li>Administrative Templates</li> <li>Allow Everyone Baseline Rules: FaceFodUninstaller.exe File Hash</li> <li>Allow Everyone Baseline Rules: sp.exe, sftp.exe, ssh-ad File Hash</li> <li>Allow Everyone Baseline Rules: SoFTWARE GU Publisher</li> <li>Allow Everyone Baseline Rules: SoFTWARE GU Publisher</li> </ul>	V 🔥 User Configuration	Allow	Everyone	Baseline Rules: REMOTEEX HELPER sign	Publisher	
<ul> <li>Windows Settings</li> <li>Administrative Templates</li> <li>Allow Everyone Baseline Rules: FaceFodUninstaller.exe File Hash</li> <li>Allow Everyone Baseline Rules: scp.exe, sftp.exe, ssh-ad File Hash</li> <li>Allow Everyone Baseline Rules: INTEL® SOFTWARE GU Publisher</li> </ul>	> Software Settings	Allow	Everyone	Baseline Rules: MICROSOFT WINDOWS	Publisher	
Administrative lemplates       Allow       Everyone       Baseline Rules: scp.exe, sftp.exe, ssh-ad       File Hash         Allow       Everyone       Baseline Rules: wAVES MAXXAUDIO sig       File Hash         Allow       Everyone       Baseline Rules: WAVES MAXXAUDIO sig       Publisher         Allow       Everyone       Baseline Rules: INTEL® SOFTWARE GU       Publisher	Windows Settings	Allow	Everyone	Baseline Rules: FaceFodUninstaller.exe	File Hash	
Allow Everyone Baseline Rules: WAVES MAXXAUDIO sig Publisher     Allow Everyone Baseline Rules: INTEL® SOFTWARE GU Publisher	Administrative lemplates	Allow	Everyone	Baseline Rules: scn.exe. sftn.exe. ssh-ad	File Hash	
Allow Everyone Baseline Rules: INTEL® SOFTWARE GU Publisher		Allow	Evenyone	Baseline Rules: WAVES MAXXAUDIO sig	Publisher	
		Allow	Everyone	Baseline Rules: INTEL® SOFTWARE GU	Publisher	
Allow Everyone Baseline Rules: REALTEK HD AUDIO UNI Publisher		Allow	Everyone	Baseline Rules: REALTEK HD AUDIO UNI	Publisher	
Allow Everyone Raseline Rules (RUI SETTINGS DRINSTA Dublicher		M Allow	Everyone	Baseline Rules: GPU SETTINGS DRINSTA	Publisher	
Allow Everyone Baseline Rules: NVID/A MXIMUS CON Dublisher		Allow	Everyone	Baseline Rules: NVIDIA MAXIMUS CON	Publisher	
Set and the Everyone Baseline Rules: nydehunding everyone Field the Set and		Allow	Everyone	Baseline Rules: nydebugdump.exe. nyid	File Hash	



#### **Example Application Control Program Deployment**

### AppLocker – Start Application Identity (AppID) service





#### **Example Application Control Program Deployment**

AppLocker Event Viewer





### Example Application Control Program Deployment

AppLocker

#### Malshare.com Example

MalShare × + · · ·				
ひ 命 https://malshare.com/				
IShare Home Upload Search F	Pull Sample Regi	ster Daily Digest	API Stats About	API Key
A free Malware repository providing	researchers acce	ess to samples, ma	licious feeds, and Yara results.	
Q	uick Search:			Search
		Re	cently added Samples	
MD5 Hach	File fune	Added	Source	Vara Llife
5735a3e1b3133b0422634f603fe70bfd	PE32	2020-08-11 17:43:15 UTC	User Submission	Jara nus
fdc4f38d0353ab9874954e2e5db476e4	PE32	2020-08-11 17:13:01 UTC	User Submission	YRP/Microsoft_Visual_Studio_NET YRP/Microsoft_Visual_C_v70_Basic_NET_additional YRP/Microsoft Visual_C_Basic_NET [+]
e8d07f1ec8b429c99834f42e14cae4d5	PE32	2020-08-11	User Submission	YRP/NETexecutableMicrosoft YRP/IsPE32

YRP/ISNET\_EXE [+]

16:18:32 UTC



### **Example Application Control Program Deployment**

AppLocker

### Malshare Example – When It Executes



### **Example Application Control Program Deployment**

AppLocker

#### Malshare Example

Autoruns [940D38AD-04B4	4-4\WDAGUtilityAccount] - Sys	sinternals: www.sysinternals.com					<del>,</del>	
File Entry Options User	Help							
	Filter:	Process Explorer - Sysinternals: v	www.sysi	internals.com [9	40D38AD-04B4	-4\WDAGUtilitvAccount] (Adminis	trator)	
S KnownDLLs	🔮 Winlogon 🛛 🔍 V	File Ontions View Process Fi	nd Use	ers Help				
🖾 Everything 🛛 🏄 Logo	n 💈 Explorer 🥭 Int		× 4				A	
Autorun Entry	Description	Process	CPU	Private Bytes	Working Set	PID Description	Company Name	VirusTotal
HKLM\SYSTEM\CurrentCor	trolSet\Control\SafeBoot\Alternat	Registry		5,156 K	21,164 K	144		The system canno
M Cmd.exe	Windows Command Processo	Memory Compression		208 K	19,840 K	1160		The system canno
HKCU\SOFTWARE\Microso	oft\Windows\CurrentVersion\Run	Kyptic Ransomwarre.exe	0.01	10,376 K	20,124 K	5372 Beta Results Mega Pump Rh	Facebook	<u>58/72</u>
Client Server Runtime	e Beta Results Mega Pump Rhe	🗐 mmc.exe	0.01	134,632 K	181,892 K	1368 Microsoft Management Cons	. Microsoft Corporation	<u>0/73</u>
HKLM\SOFTWARE\Microso	oft\Windows\CurrentVersion\Run(	mmc.exe	0.01	63,604 K	15,680 K	3684 Microsoft Management Cons	. Microsoft Corporation	<u>0/73</u>
Unattend000000000	1	WmiPrvSE.exe		2,464 K	8,460 K	7992 WMI Provider Host	Microsoft Corporation	<u>0/72</u>
HKI M\SOFTWARE\Micmso	htt\Active Setun\Installed Compon	🖃 📻 winlogon.exe		2,612 K	11,840 K	2964 Windows Logon Application	Microsoft Corporation	<u>0/72</u>
		WindowsInternal.ComposableSh		10,680 K	47,296 K	2312 WindowsInternal.Composabl	Microsoft Corporation	<u>0/72</u>
		VmComputeAgent.exe		1,776 K	8,316 K	2284 Hyper-V Guest Compute Ser	Microsoft Corporation	0/72
		taskhostw.exe		11,432 K	23,136 K	3380 Host Process for Windows T	. Microsoft Corporation	<u>0/72</u>
		System Settings Broker.exe		5,584 K	23,768 K	996 System Settings Broker	Microsoft Corporation	<u>0/72</u>
				40.000.14	00.010.14	1050		0.000



### **Example Application Control Program Deployment**

AppLocker Pull all 8003 events to

a centralized database

			DANICOMMANDE EVE	
to run but would h	ave been prevented from run	ning if the AppL	ocker policy were enforced.	
		3		
				4
Log Name:	Microsoft-Windows-AppLoc	ker/EXE and DLI	<u> </u>	
Source:	AppLocker	Logged:	8/11/2020 12:55:30 PM	4
Event ID:	8003	Task Category:	None	
Level:	Warning	Keywords:		
User:	940D38AD-04B4-4\WDAGUti	Computer:	940d38ad-04b4-45dd-88d8-a9bd2l	
OpCode:	Info			
More Information:	Event Log Online Help			



**Example Application Control Program Deployment** 

Pull all app control new execution events to a centralized database





### **Workflow**

Every time new executable is detected:

- Research any new executable
- Use automation for mitigation when you can
- Contact user for unexplainable executions
- Develop security workflows

### <u>Workflow</u>

Example automation security workflow

- New executable identified
- Submit to Virus Total/AV for analysis
- Run in "detonation sandbox" to see effects of execution
- Send email to end user involved
- Resolve as benign or malicious

### **Workflow**

$\triangleright$	From ~	ITAutomationAlert
Send	То	Roger A. Grimes:
	Cc	
	Bcc	
	Subject	Alert - Unrecognized Execution Detected - Response Needed

An unrecognized and unapproved executable (spotify.exe) was detected on your device (Rogerlaptop2a) at 11:14AM EST on 12/6/2020 while user account (Rogerg) was logged in.

We need to know if this program's execution was intentional, needed, and ensure it is not able to increase cybersecurity risk to the organization.

Please respond immediately and let us know if this program's execution was intentional and the reason it is needed on organization's assets.

Please provide any relevant information and links. The IT Security team will use your reply as part of determining whether it should be an authorized and allowed program on organizational devices.

If a successful determination cannot be determined or allowed, the execution will be immediately disallowed. This could result in operational interruption or device instability. Further investigation and interruption may be warranted, up and unto device lockout, suspension of involved user account, and disconnection from the network.

Refer to organization security policy 14.51 for more information. Violations of policy could result in an HR referral.

If you unaware of this executable or you did not intentionally run it, or you have any questions, please call the IT Security Team at 727-555-1234.

Sincerely,

Generic Corporation IT Security Team

### Advanced Workflow

Example advanced automation security workflow

- Assign a risk score to workstations, devices, and users detected with new executables
- Track risk scores over time
  - Per user, device, and overall organization

### <u>Advanced Workflow – Virtual Risk Officer</u>



### **Workflows**

### Security workflows

 Tie back to how malware got in the first place and modify your preventative training and defenses as needed

### **KnowBe4 Security Awareness Training**

#### Baseline Testing

We provide baseline testing to assess the Phish-Prone<sup>™</sup> percentage of your users through a free simulated phishing attack.

#### Real Train Your Users

The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

#### **?** Phish Your Users

Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

#### See the Results

Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!





### **Generating Industry-Leading Results and ROI**

- Reduced Malware Infections
- Reduced Data Loss
- Reduced Potential Cyber-theft
- Increased User Productivity
- Users Have Security Top of Mind

## 87% Average Improvement

Across all industries and sizes from baseline testing to one year or more of ongoing training and testing

Note: The initial Phish-Prone percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 platform prior to the evaluation. Subsequent time periods reflect Phish-Prone percentages for the subset of users who received training with the KnowBe4 platform.



Source: 2020 KnowBe4 Phishing by Industry Benchmarking Report



# **Questions?**

### Roger A. Grimes– Data-Driven Defense Evangelist, KnowBe4

rogerg@knowbe4.com Twitter: @rogeragrimes https://www.linkedin.com/in/rogeragrimes/