KnowBe4
Human error. Conquered.

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/

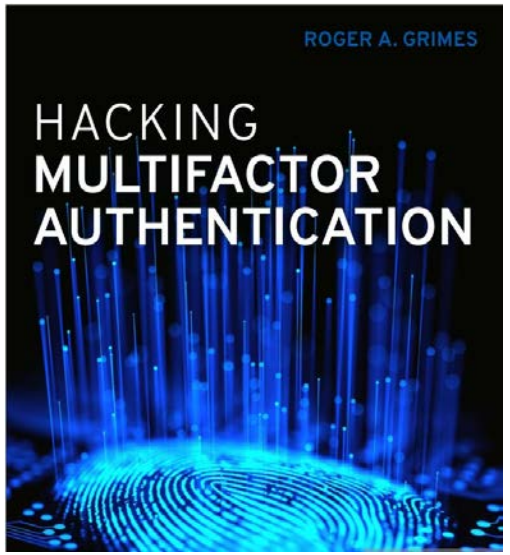
About Roger

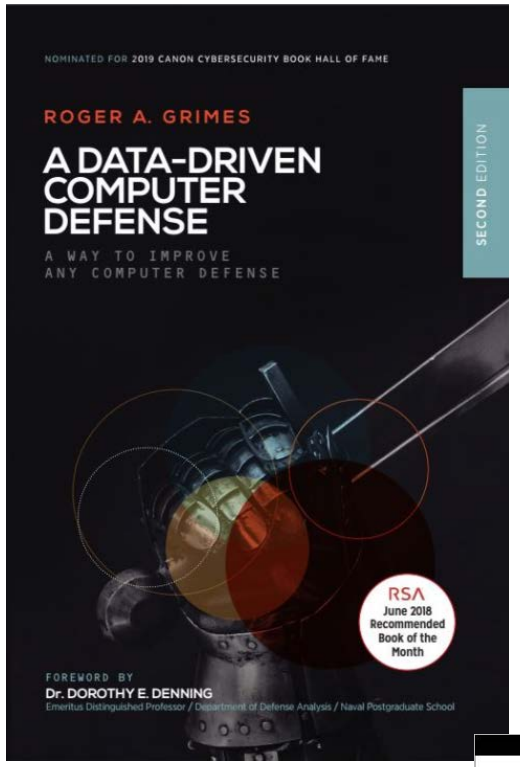
- 30 years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 12 books and over 1,100 magazine articles
- *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)

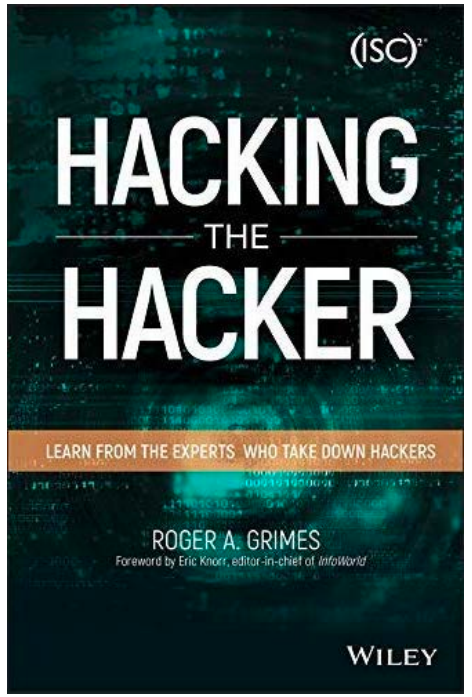
Certification exams passed include:

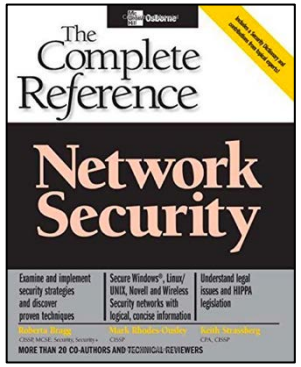
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

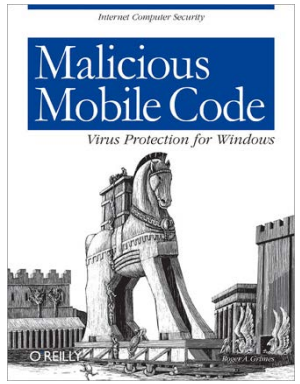
Roger's Books

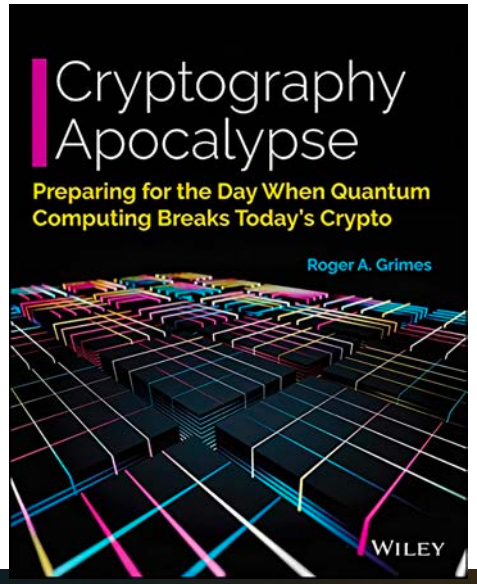


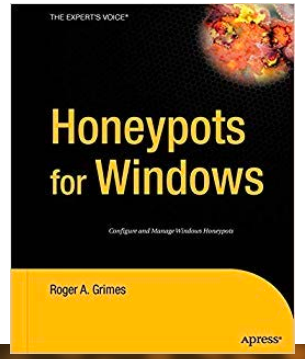


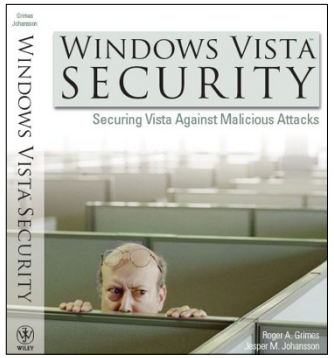


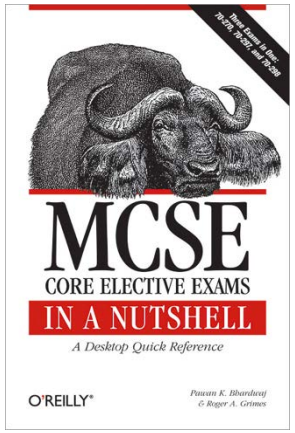


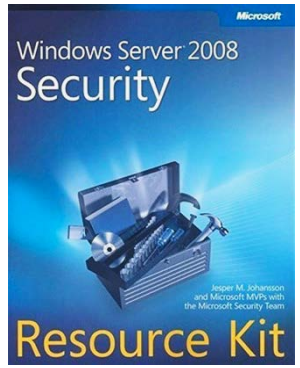












About Us

- 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

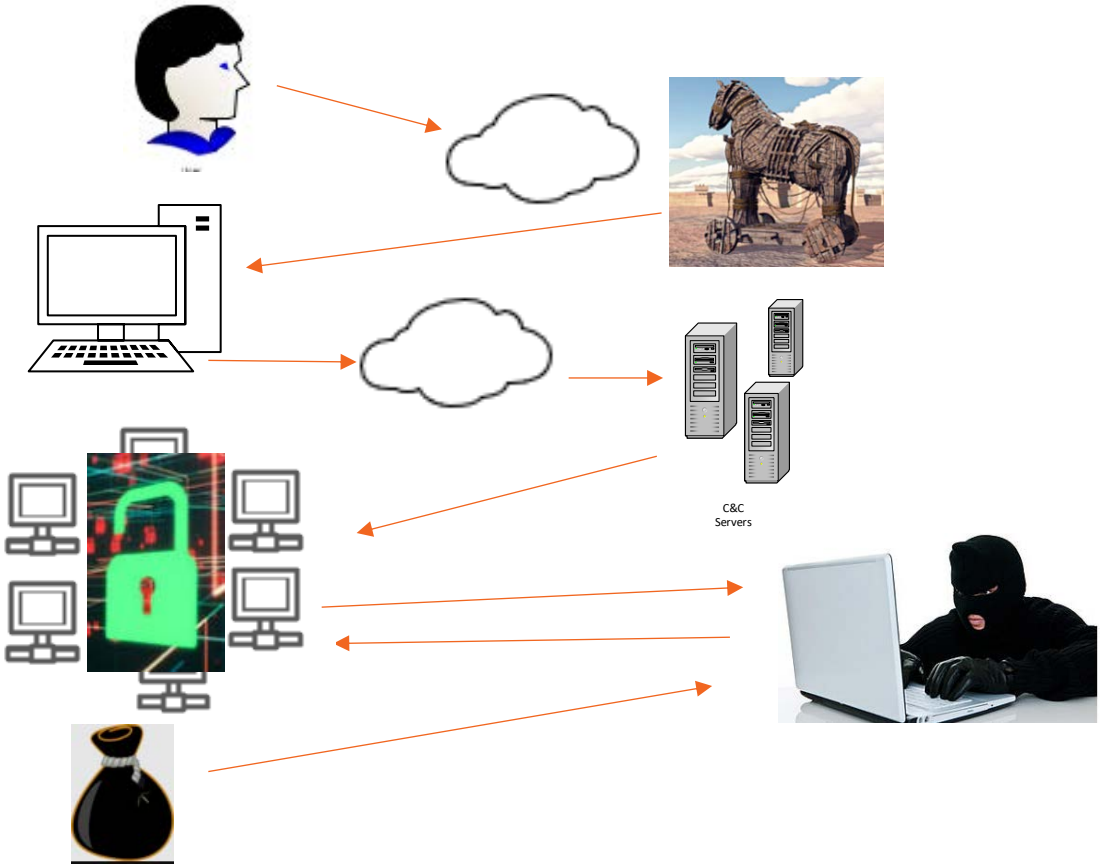
But Ransomware Got More Malicious

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



1. Victim tricked into executing smaller stub, trojan horse "dropper" file
2. 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

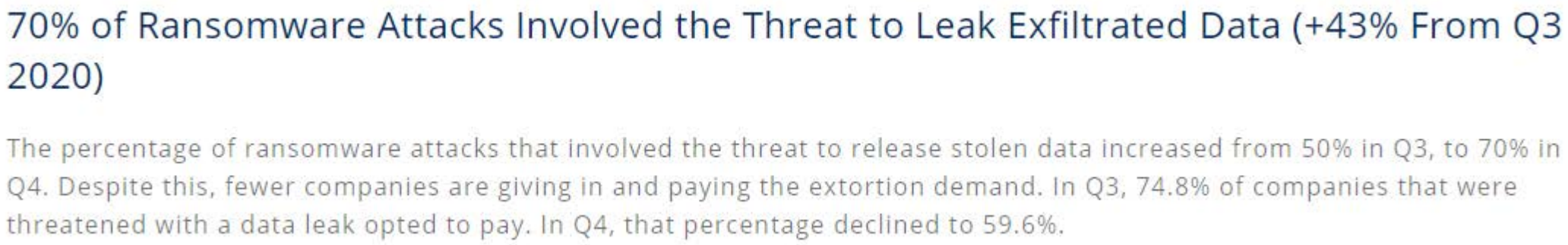
Good luck having a good backup save you!

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



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

CISA Recommendations

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

CISA Recommendations

Cybersecurity and Infrastructure Security Agency (CISA)

Example warning

You are subscribed to National Cyber Awareness System Cur
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

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

FTC Reports Scammers Impersonating FTC

01/26/2021 05:17 PM EST

Original release date: January 26, 2021

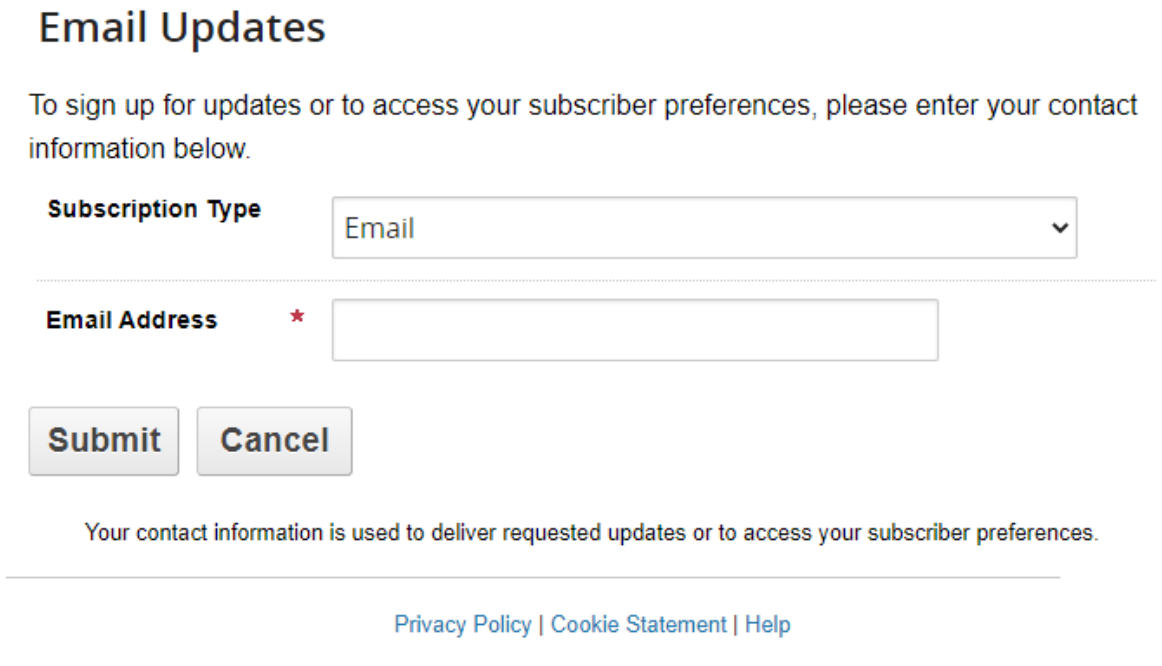
The Federal Trade Commission (FTC) has released information on scammers attempting to impersonate the FTC. The scammers operate an FTC-spoofed website that claims to provide instant cash payments and tries to trick consumers into disclosing their financial information. The real FTC does not require such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

Cybersecurity and Infrastructure Security Agency (CISA)

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



CISA Recommendations

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

CISA Recommendations

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 operatin 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

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

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

CISA Recommendations

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
4. Review and exercise your incident response plan
5. Pay attention to ransomware events and apply lessons learned

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

Agenda

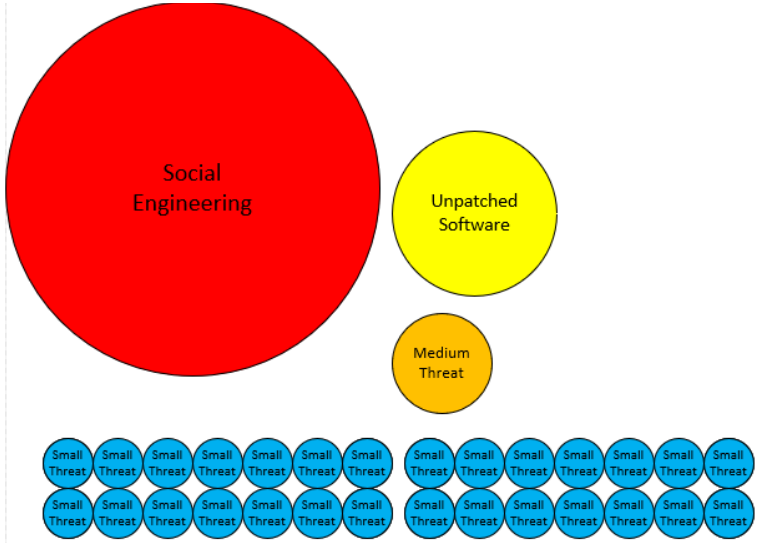
- Why a good backup alone no longer saves you from ransomware
- CISA official recommendations for mitigating ransomware
- Our recommendations
- The policies, technical controls, and education you need to stop ransomware in its tracks
- Incident Response
- How to detect any ransomware program no matter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

Our Recommendations

Risk-Ranking Threats (not all threats are equal)

- Risk-rank likely threats

  If you do that…

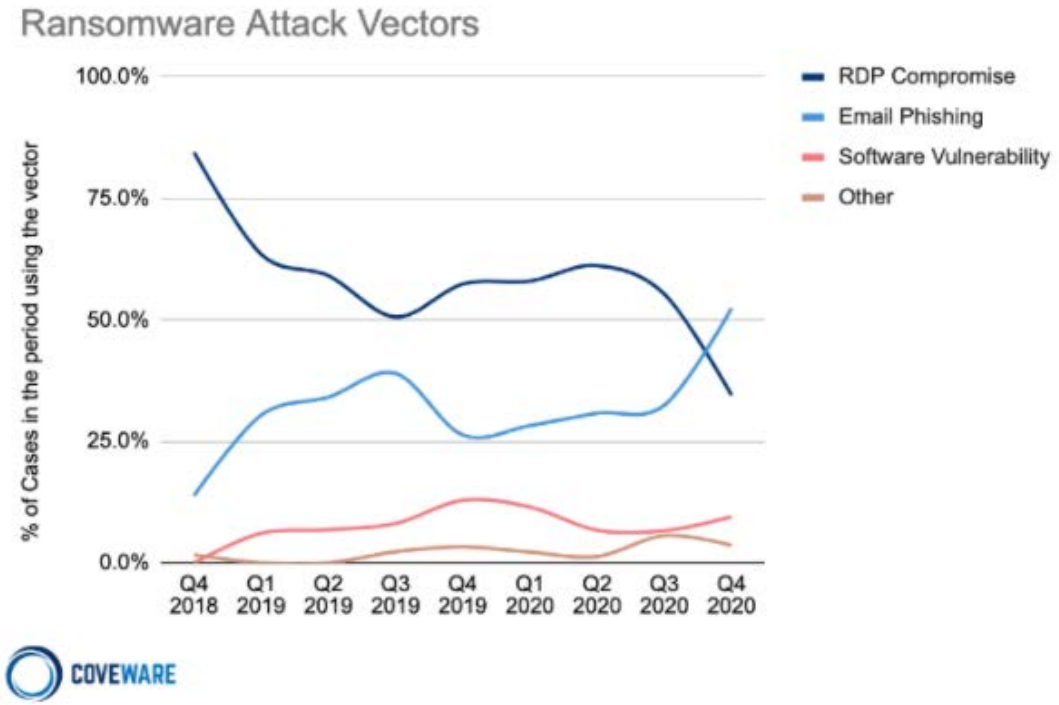


- Majority of all malicious digital breaches are due to social engineering and phishing
- Second most is due to unpatched software
- Everything else added up all together is small part of the risk
- Concentrate your efforts where your prevention efforts will mean the most

Our Recommendations

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

Best Defenses

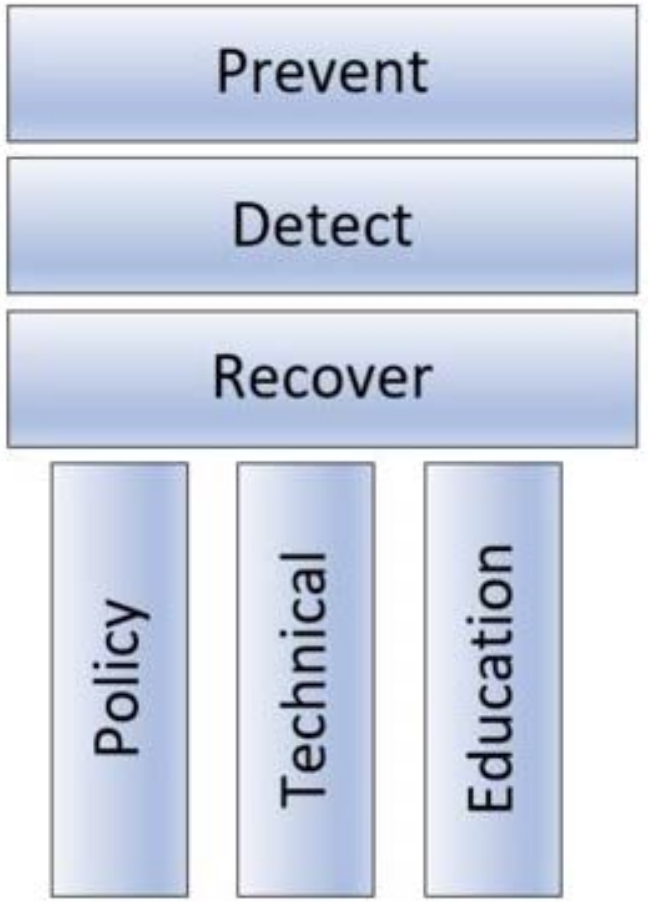
Most Important Critical Defenses

- **Good, thorough, complete system, tested, offline, up-to-date, backup and restore**
  - **Most organizations do not have this**
  - **But in most cases of ransomware, a backup alone will not gain you much**
- **You MUST 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

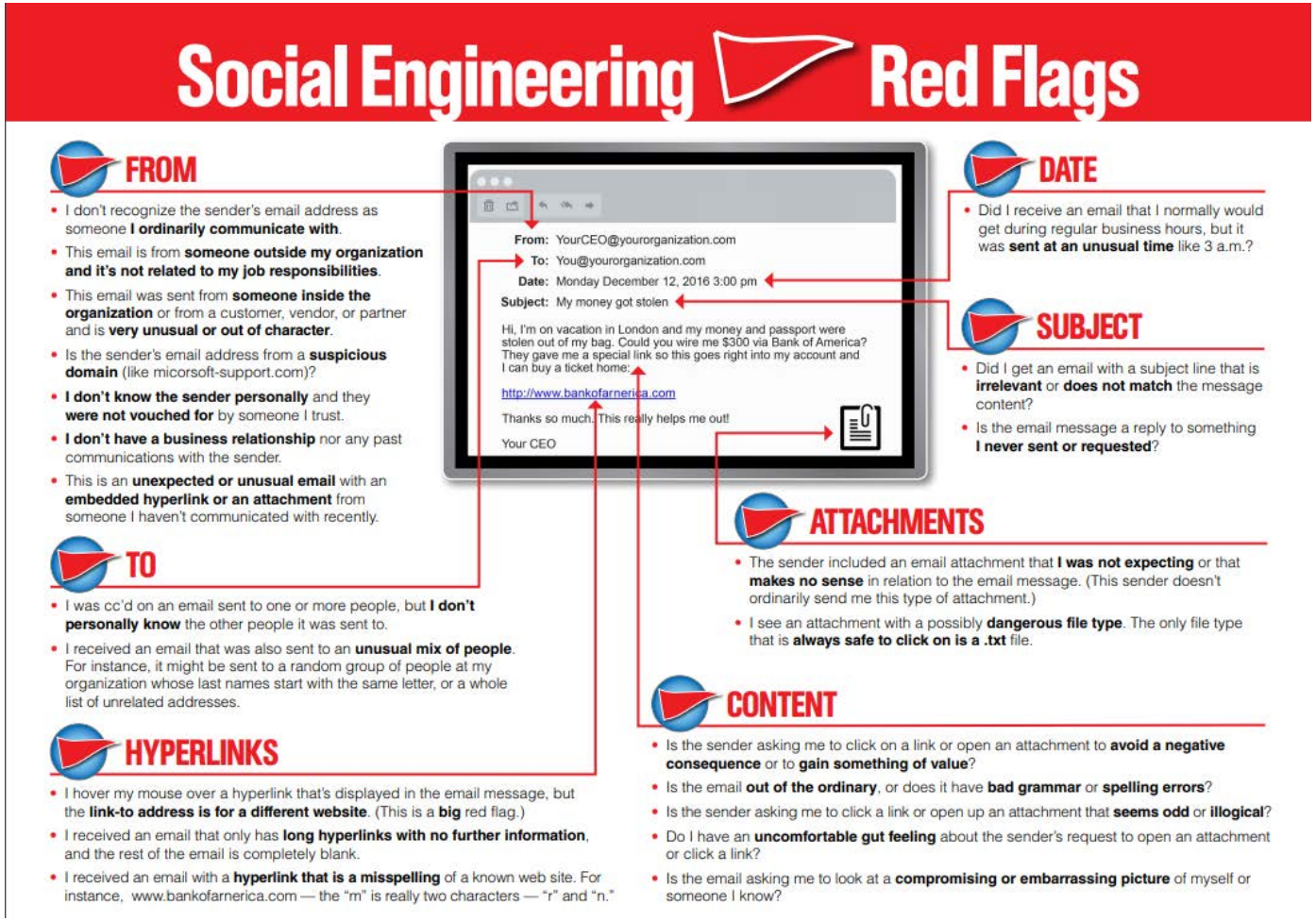
Best Defenses

Top 5 Defenses for Most Organizations

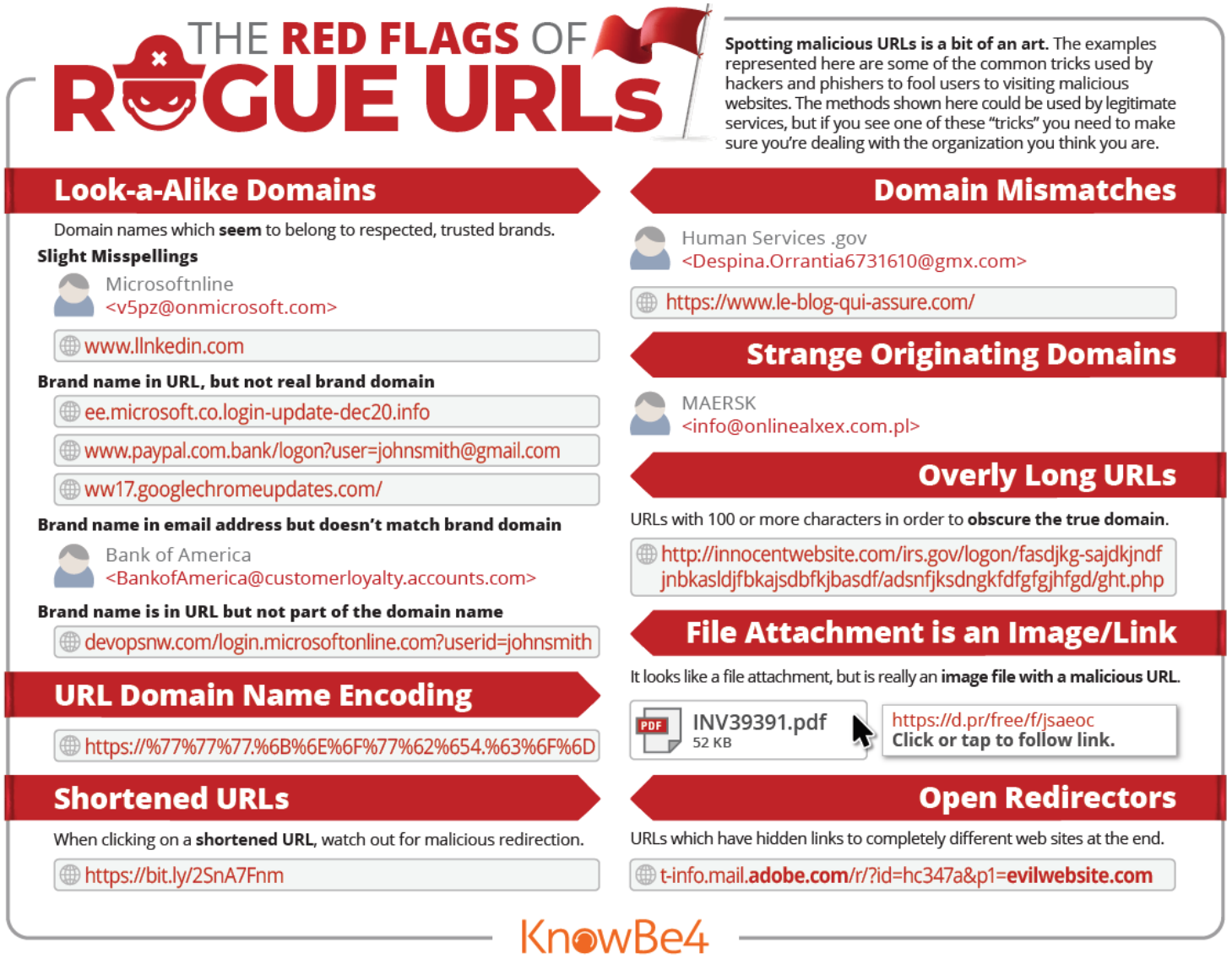
(in order of importance)

- **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



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

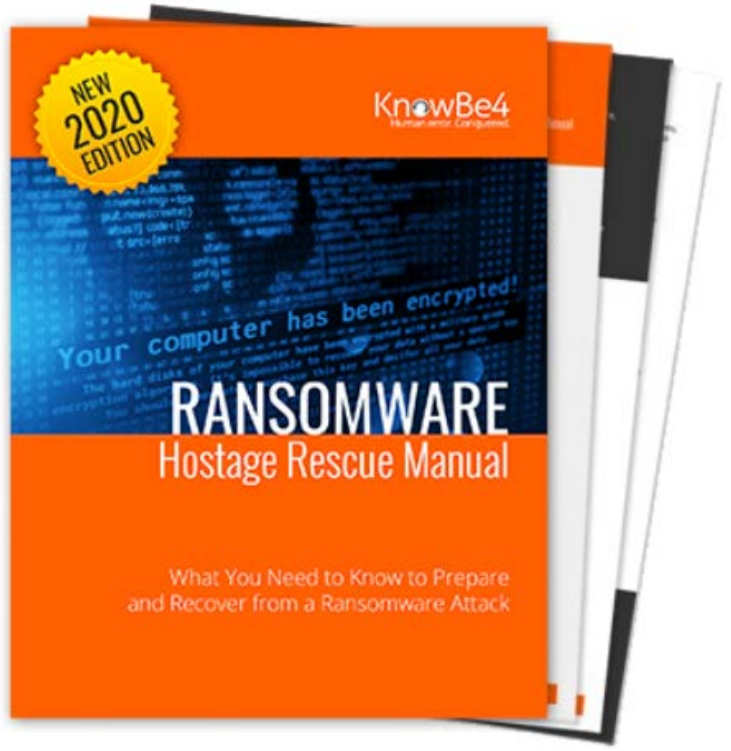


https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks

Best Defenses

KnowBe4 Resources

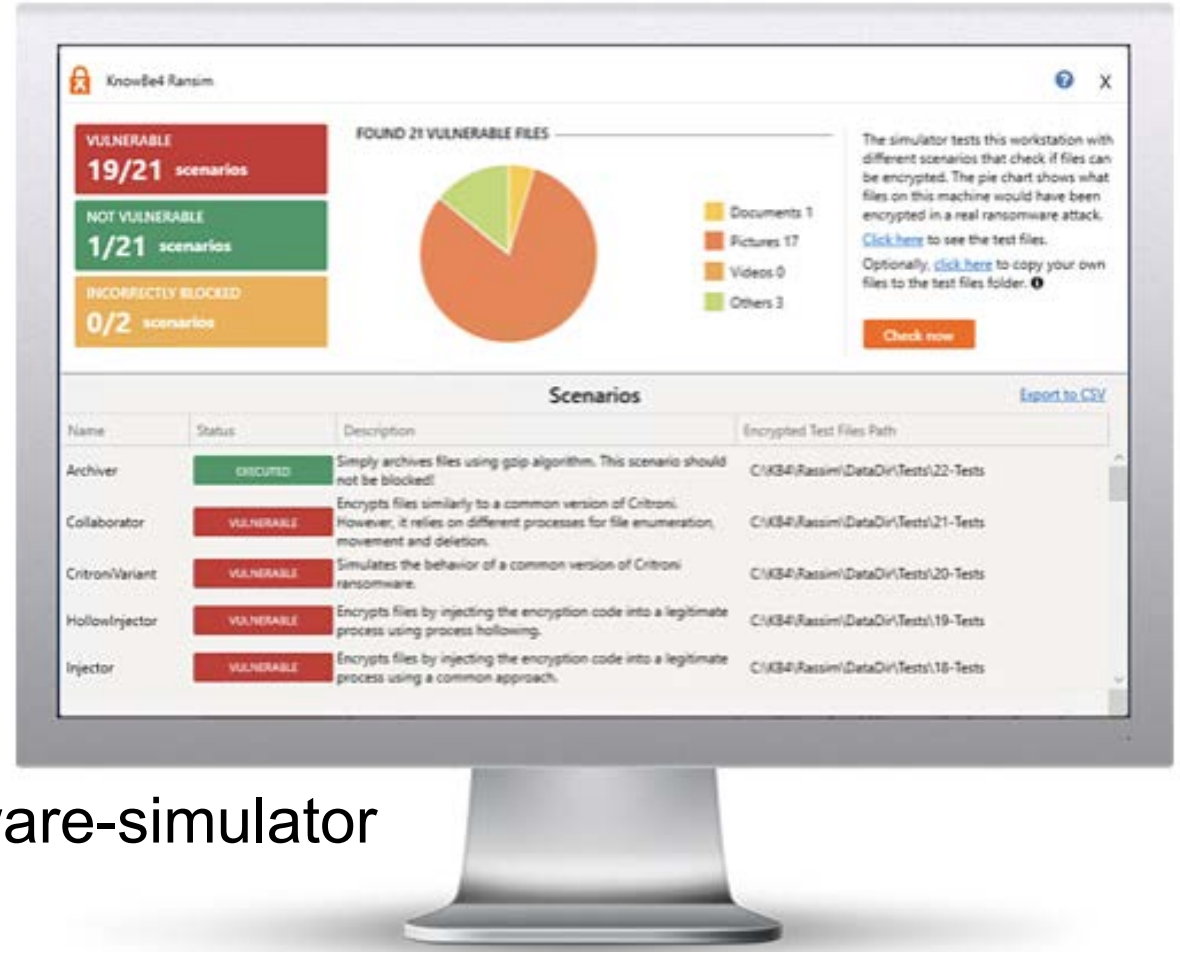
- Ransomware portal
  - https://www.knowbe4.com/ransomware
- Ransomware guide
  - https://info.knowbe4.com/ransomware-hostage-rescue-manual-0
- Ransomware simulator
  - https://www.knowbe4.com/ransomware-simulator



Ransomware Simulator

Ransim

- 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

- 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

Our Recommendations

Response Priorities

- Stop spread
- Stop damage
- Close holes

CISA Recommendations

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

Our Recommendations

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

Our Recommendations

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

Our Recommendations

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)

Our Recommendations

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

Our Recommendations

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

Our Recommendations

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

Detecting Any Malware

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 Any Malware

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 Any Malware

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 Any Malware

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”

Detecting Any Malware

Example Application Control Program Deployment

AppLocker

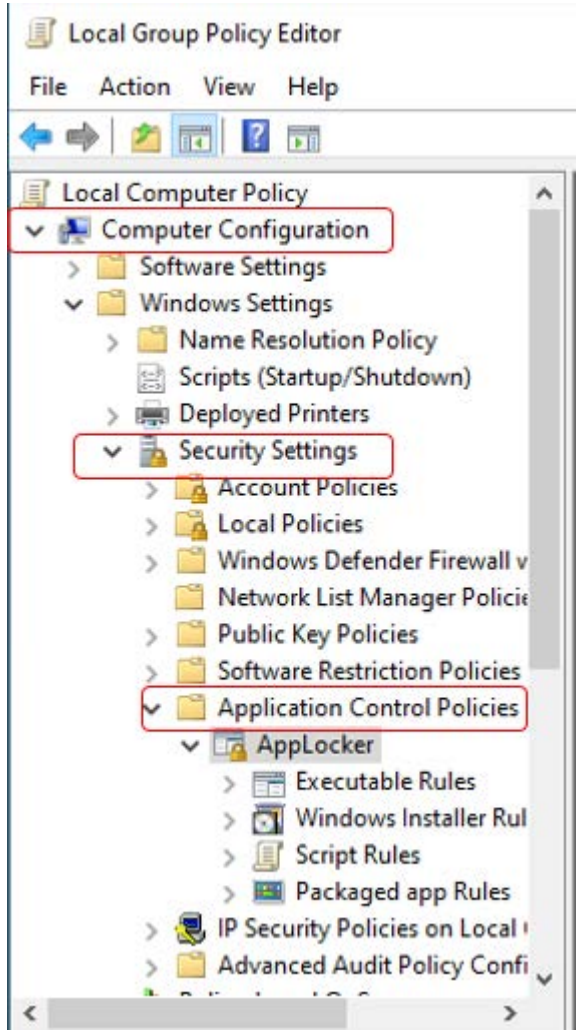
- Been in Microsoft Windows enterprise versions since Windows 7/Windows Server 2008
  - Early related Windows feature was Software Restriction Policies
  - Windows Defender Application Control (WDAC), released in Windows 10
  - WDAC is a far more serious application control program than AppLocker and 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.)

Detecting Any Malware

Example Application Control Program Deployment

AppLocker

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



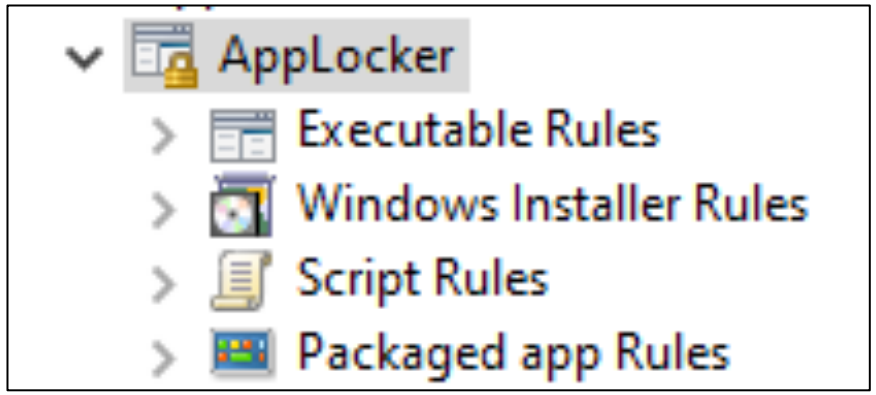
Detecting Any Malware

Example Application Control Program Deployment

AppLocker

AppLocker Rule Categories:

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

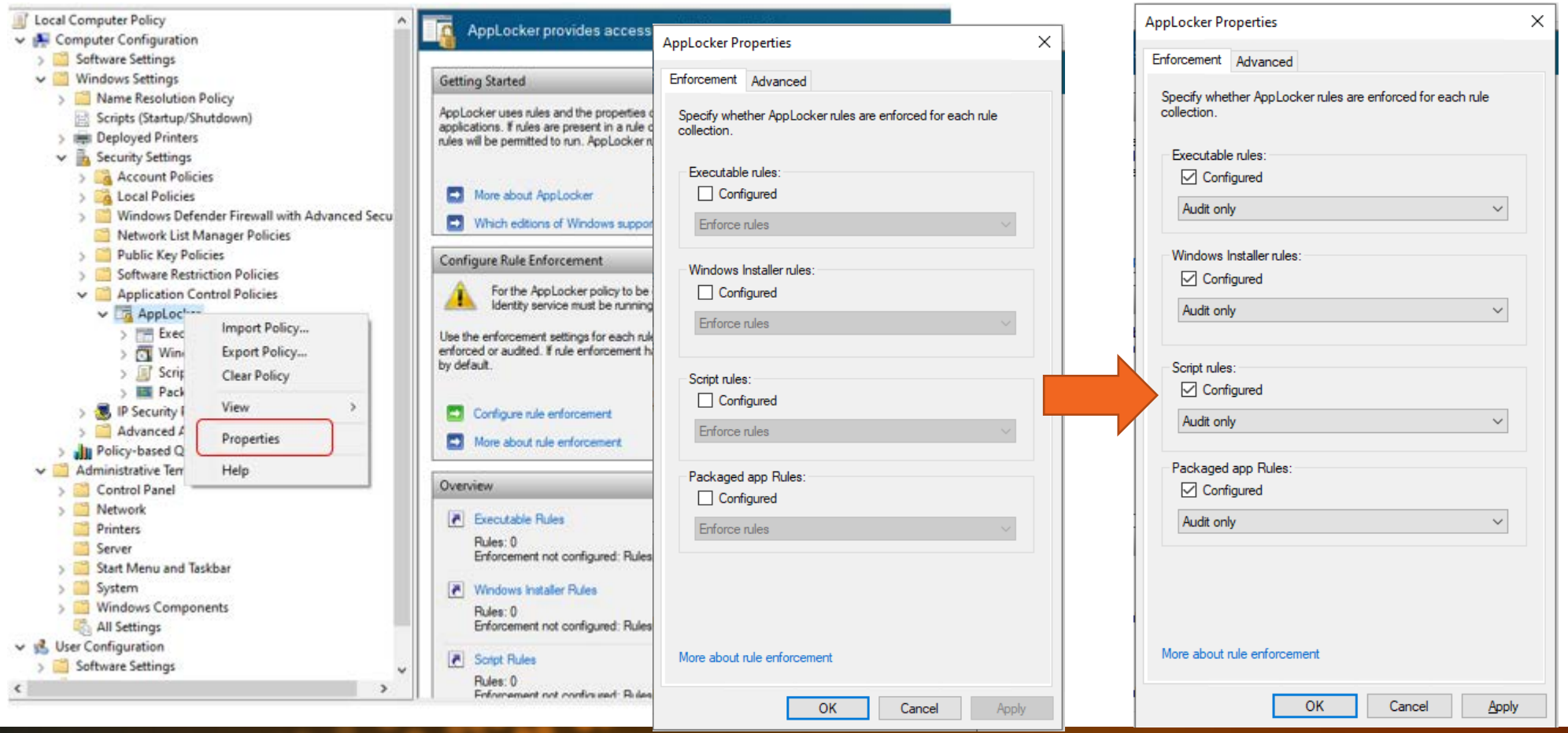


Each can be enabled separately

Detecting Any Malware

Example Application Control Program Deployment

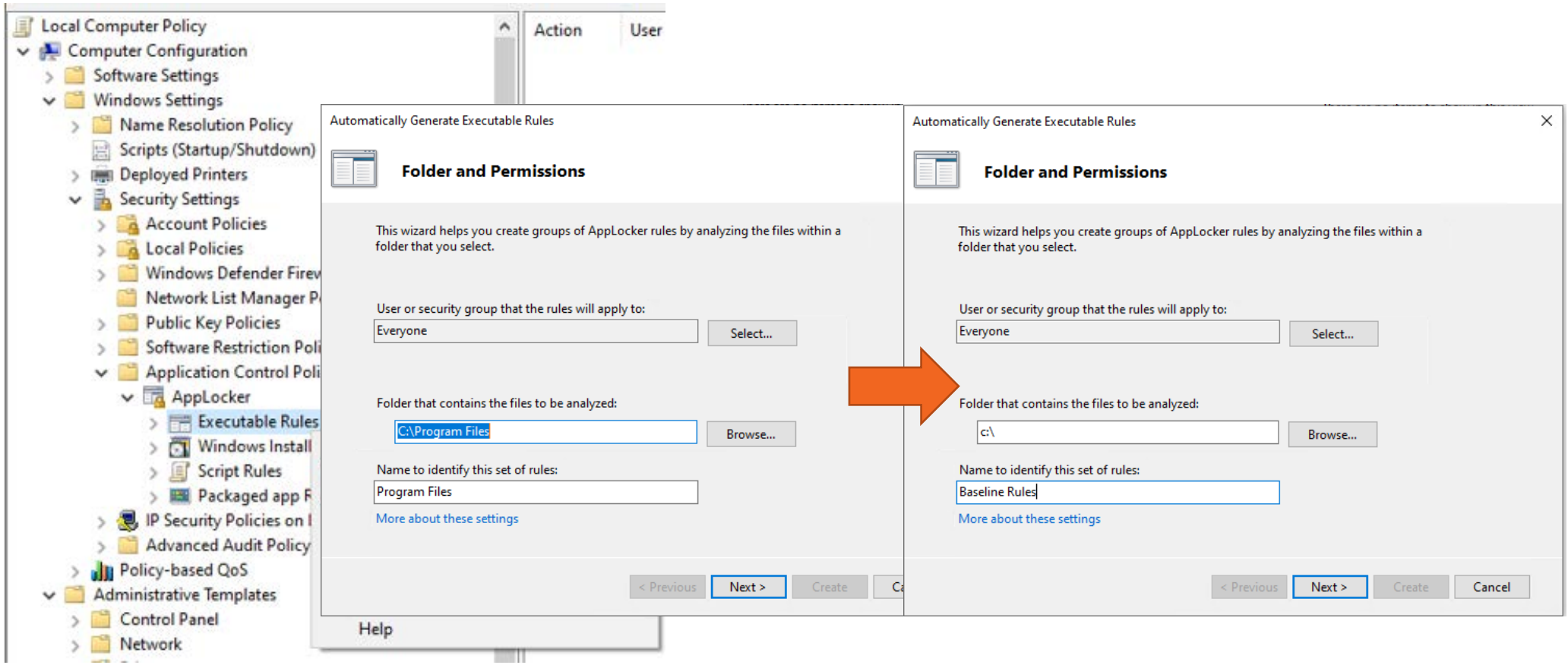
AppLocker



Detecting Any Malware

Example Application Control Program Deployment

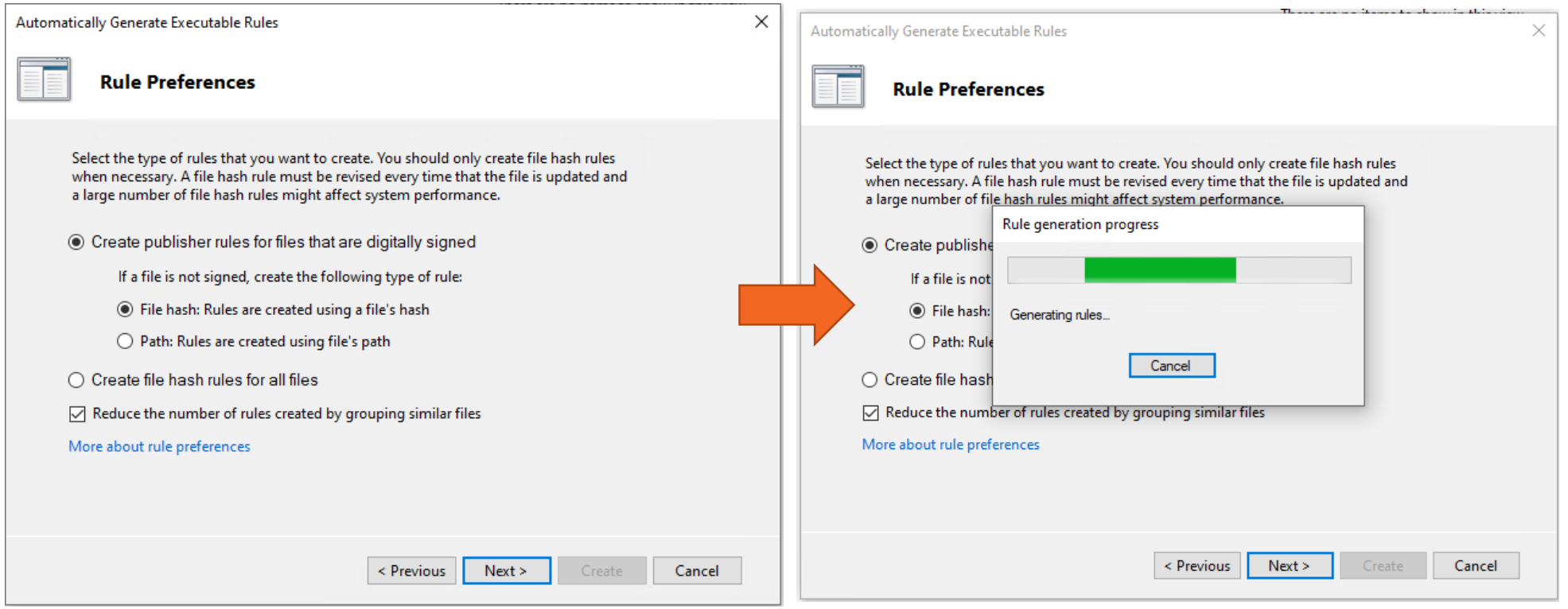
AppLocker



Detecting Any Malware

Example Application Control Program Deployment

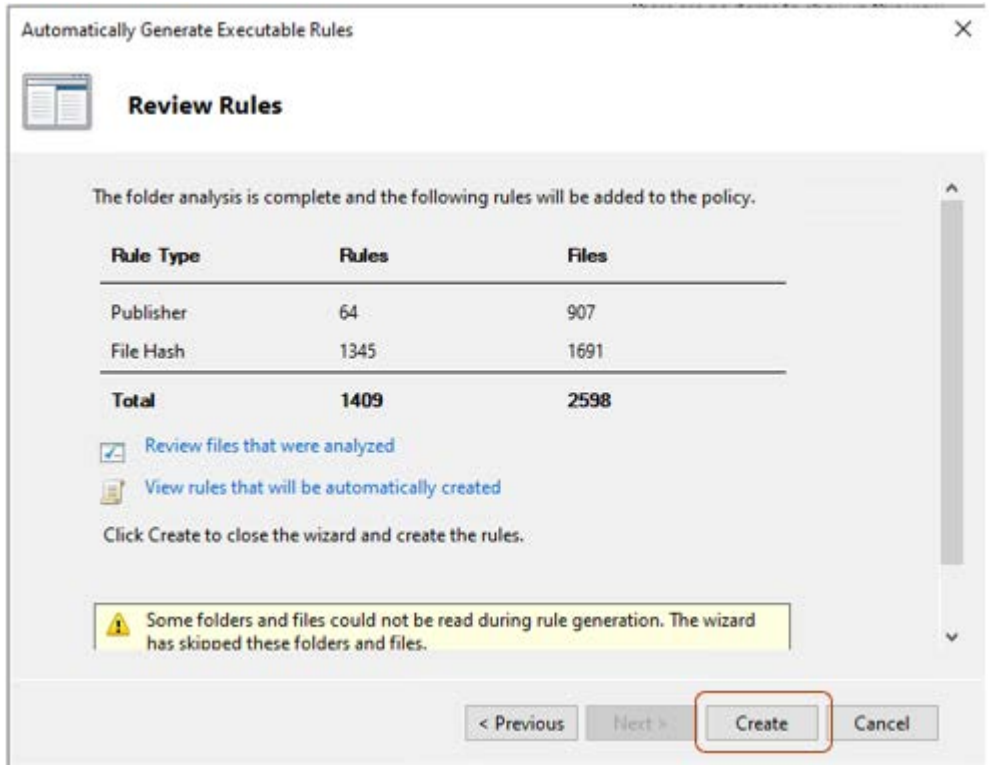
AppLocker



Detecting Any Malware

Example Application Control Program Deployment

AppLocker

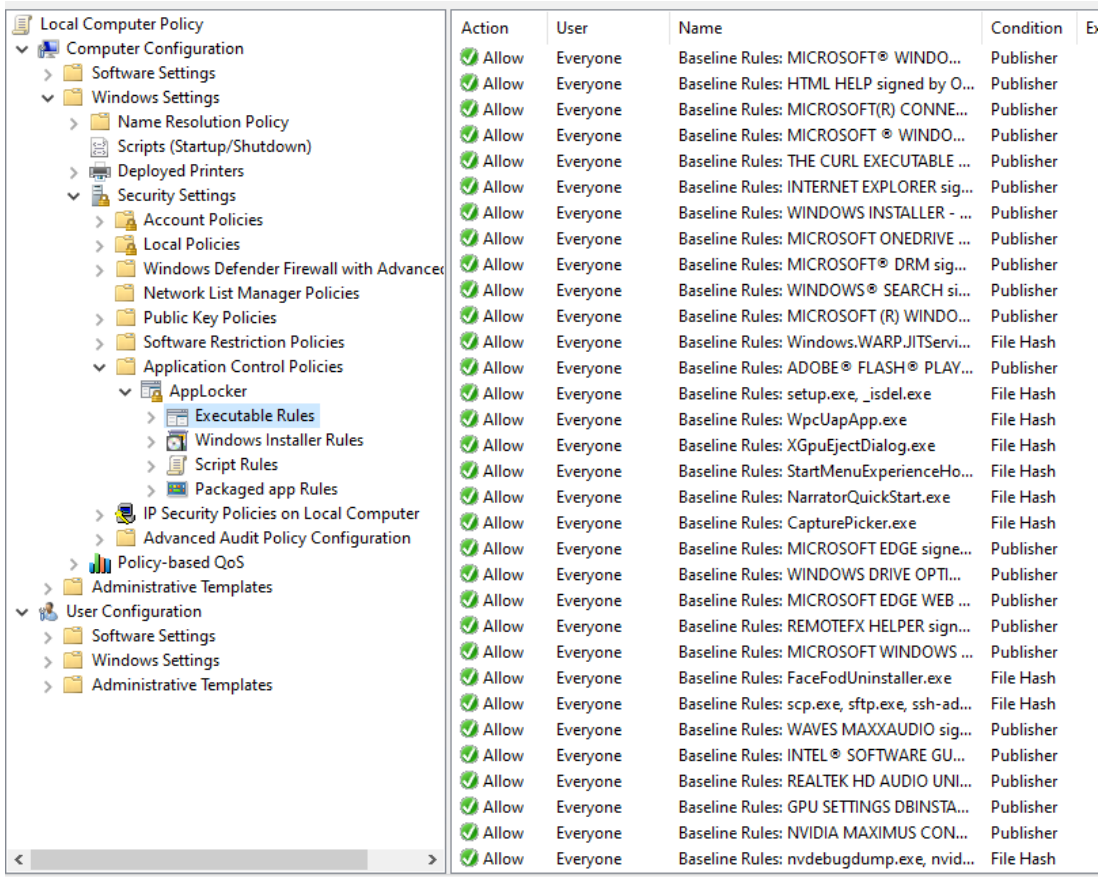


Note: If you enabled enforcement mode you might want to say Yes here.

Detecting Any Malware

Example Application Control Program Deployment

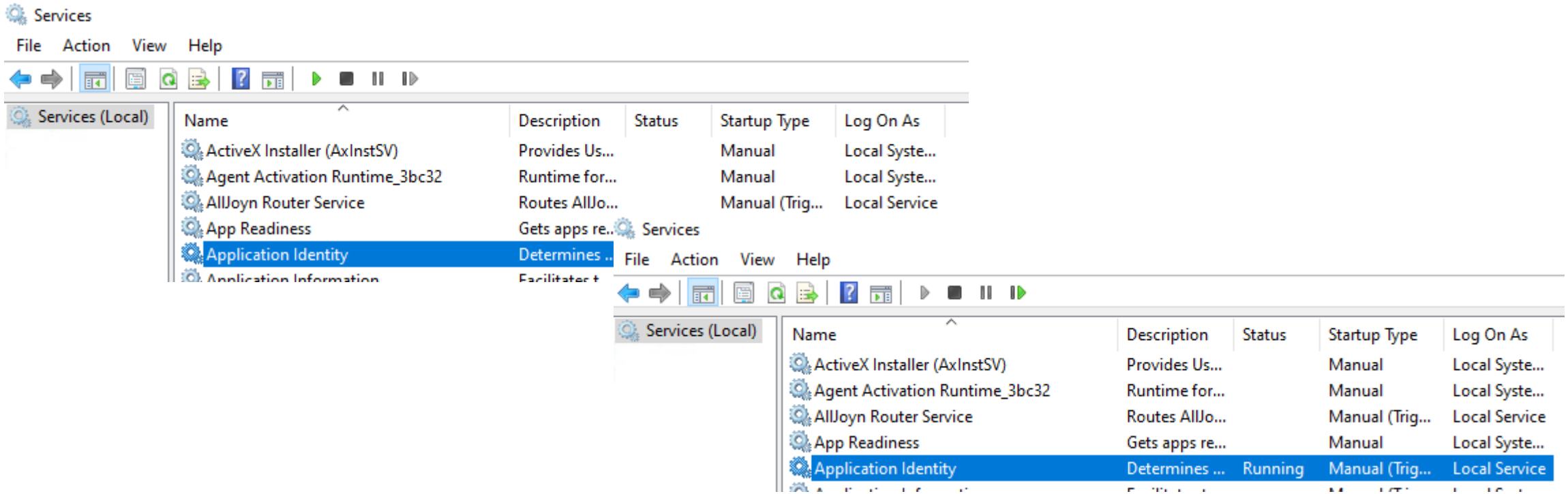
AppLocker



Detecting Any Malware

Example Application Control Program Deployment

AppLocker – Start Application Identity (AppID) service

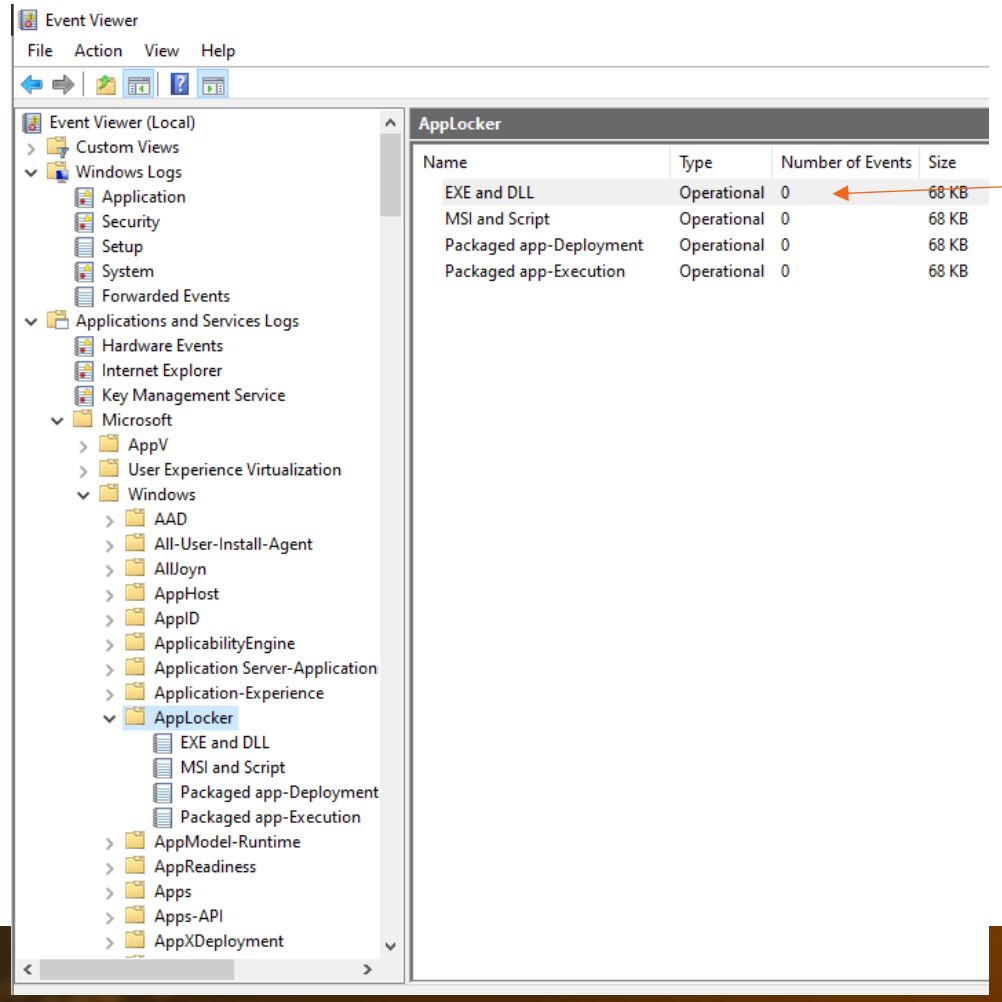


Detecting Any Malware

Example Application Control Program Deployment

AppLocker

Event Viewer



0 logged events

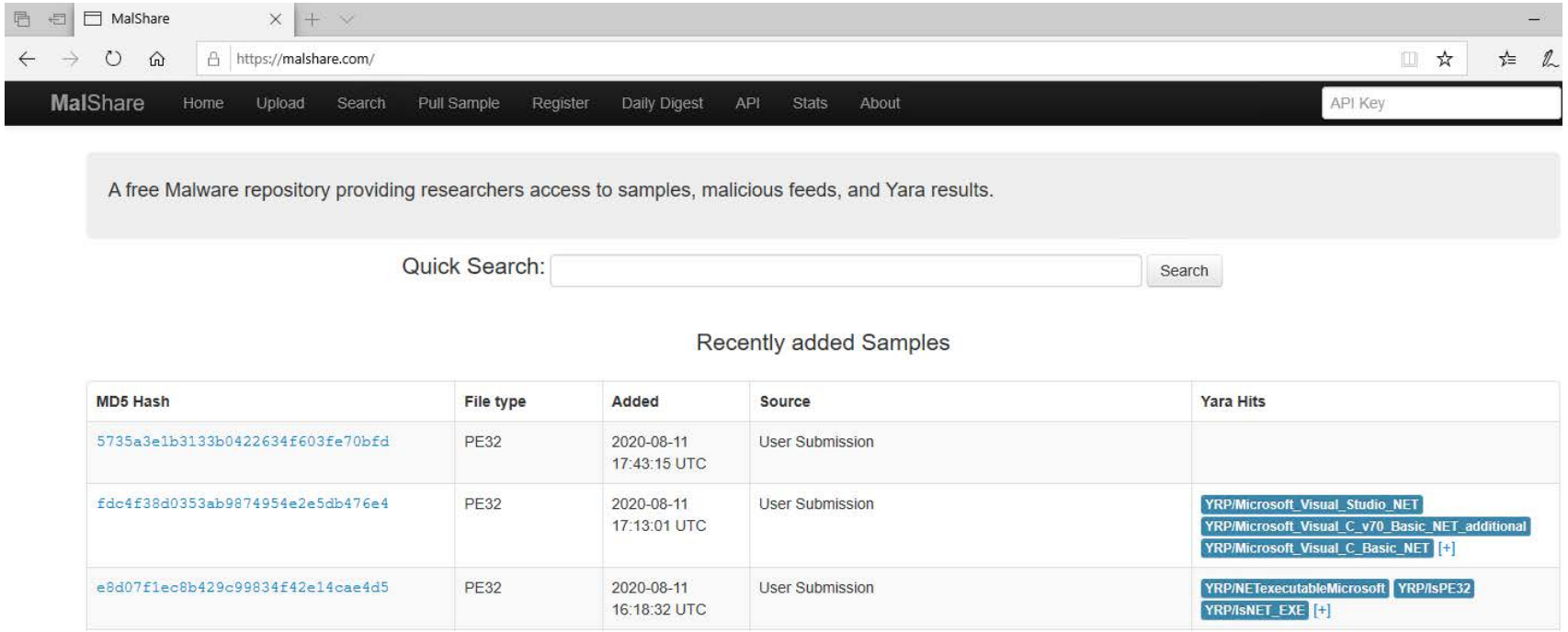
Any execution exceptions to AppLocker's policy will be logged as 8003 events

Detecting Any Malware

Example Application Control Program Deployment

AppLocker

Malshare.com Example

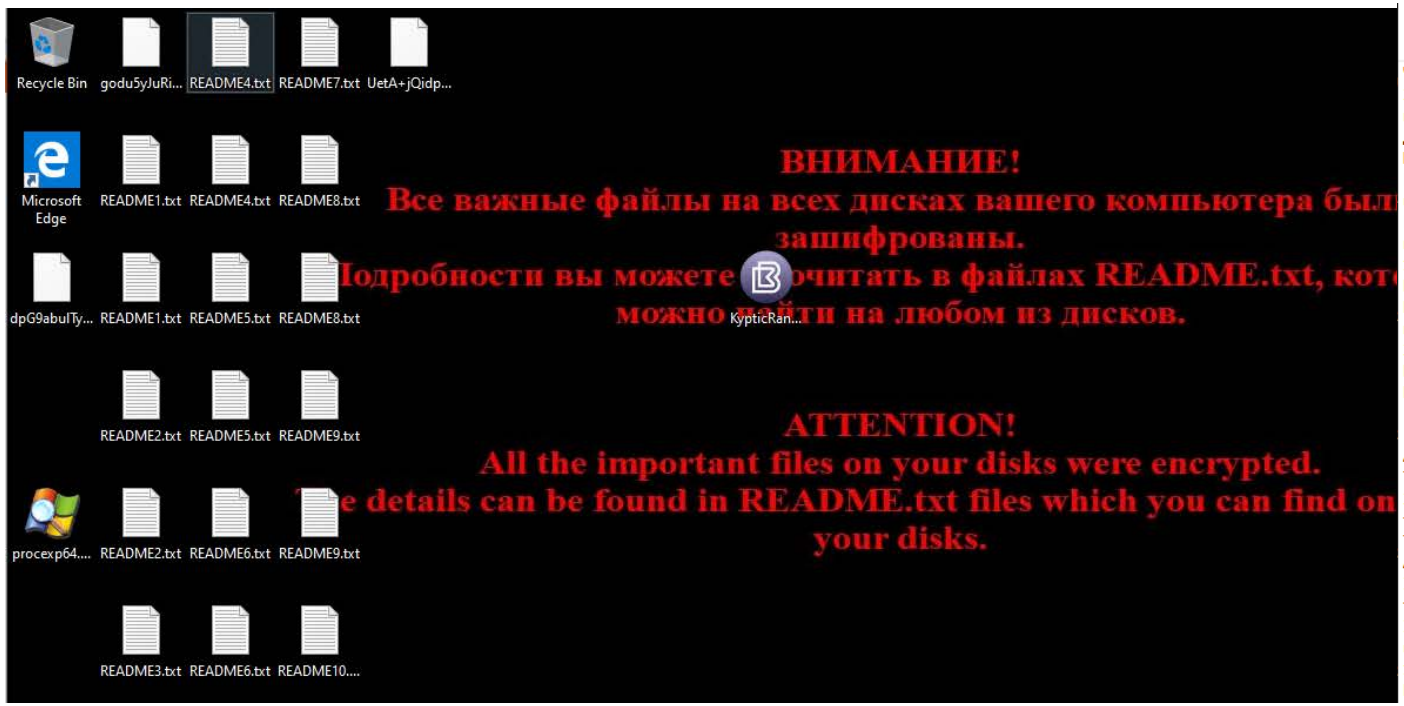


Detecting Any Malware

Example Application Control Program Deployment

AppLocker

Malshare Example – When It Executes



README1.txt - Notepad

File Edit Format View Help

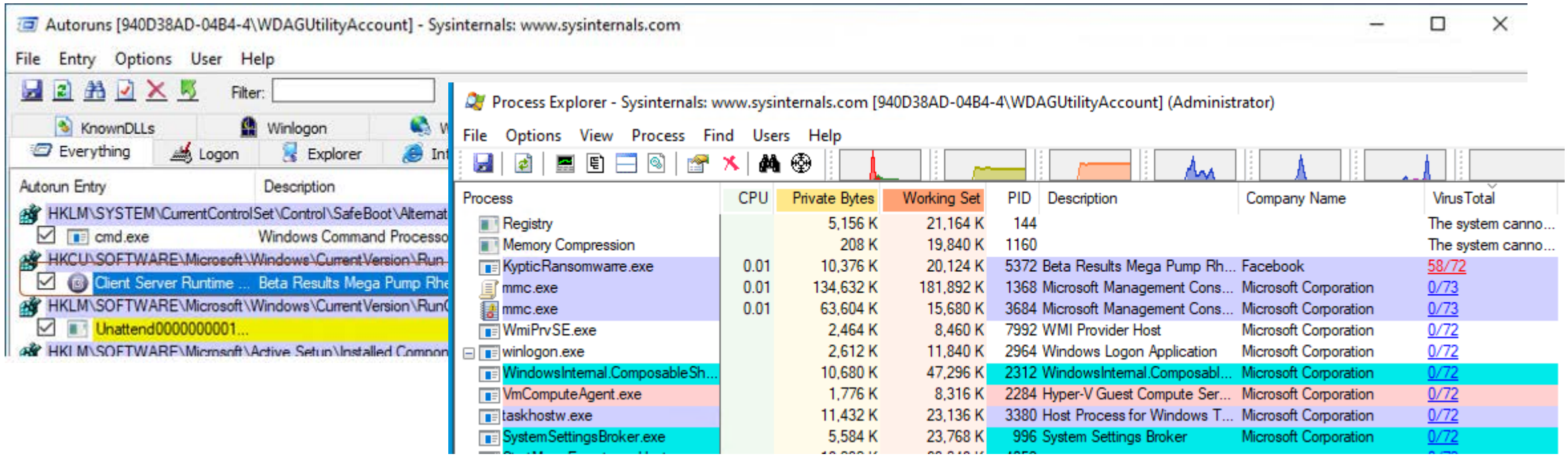
```
Чтобы расшифровать их, Вам необходимо отправить код:
284895E45ED28FBDF1B9|869|7|10
на электронный адрес pilotpilot088@gmail.com .
Далее вы получите все необходимые инструкции.
Попытки расшифровать самостоятельно не приведут ни к чему, кроме безвозвратной потери информации.
Если вы всё же хотите попытаться, то предварительно сделайте резервные копии файлов, иначе в случае
их изменения расшифровка станет невозможной ни при каких условиях.
Если вы не получили ответа по вышеуказанному адресу в течение 48 часов (и только в этом случае!),
воспользуйтесь формой обратной связи. Это можно сделать двумя способами:
1) Скачайте и установите Tor Browser по ссылке: https://www.torproject.org/download/download-easy.html.en
В адресной строке Tor Browser-а введите адрес:
http://cryptsen7fo43rr6.onion/
и нажмите Enter. Загрузится страница с формой обратной связи.
2) В любом браузере перейдите по одному из адресов:
http://cryptsen7fo43rr6.onion.to/
http://cryptsen7fo43rr6.onion.cab/


All the important files on your computer were encrypted.
To decrypt the files you should send the following code:
284895E45ED28FBDF1B9|869|7|10
to e-mail address pilotpilot088@gmail.com .
Then you will receive all necessary instructions.
All the attempts of decryption by yourself will result only in irrevocable loss of your data.
If you still want to try to decrypt them by yourself please make a backup at first because
the decryption will become impossible in case of any changes inside the files.
If you did not receive the answer from the aforecited email for more than 48 hours (and only in this case!)
use the feedback form. You can do it by two ways:
1) Download Tor Browser from here:
https://www.torproject.org/download/download-easy.html.en
```

Detecting Any Malware

Example Application Control Program Deployment

AppLocker

Malshare Example



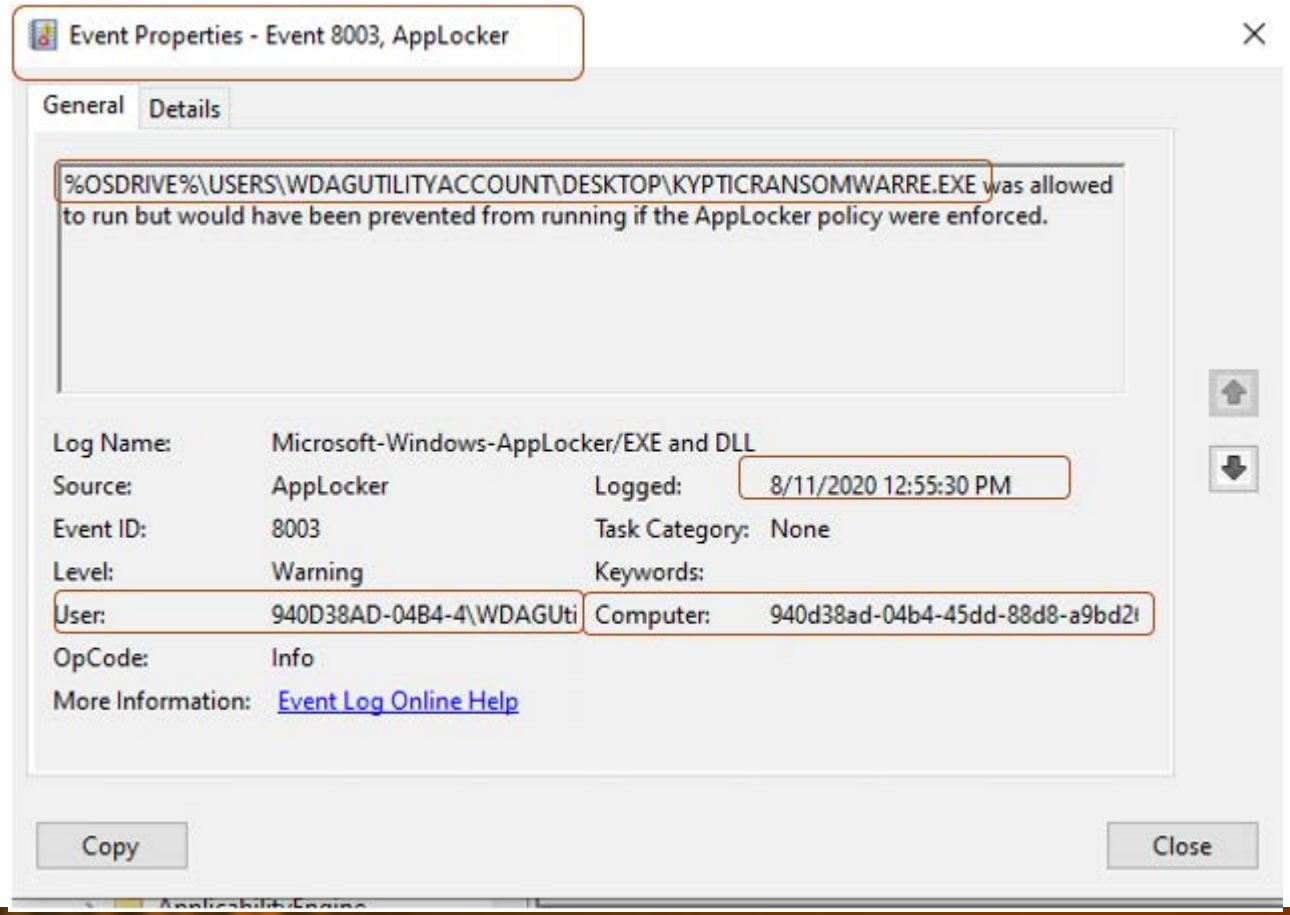
Detecting Any Malware

Example Application Control Program Deployment

AppLocker

Pull all 8003 events to

a centralized database

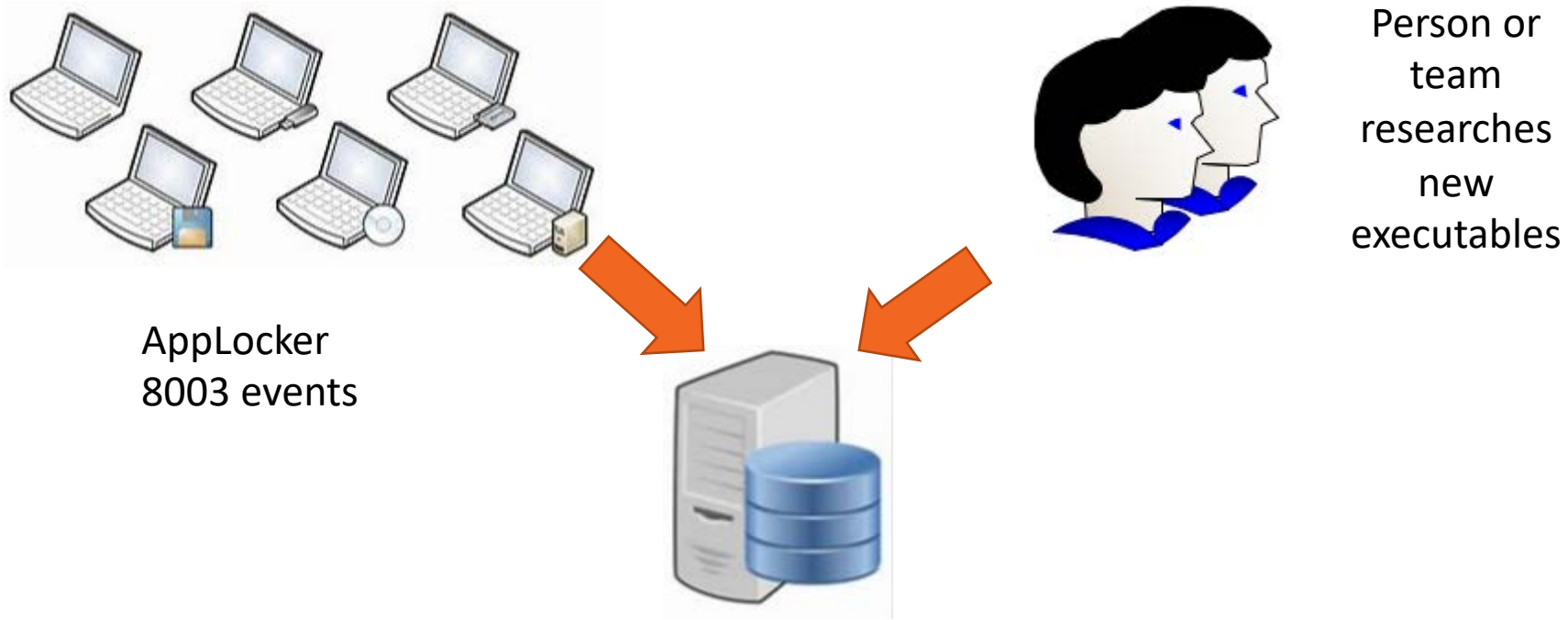


Detecting Any Malware

Example Application Control Program Deployment

Pull all app control new execution events to

a centralized database



Detecting Any Malware

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

Detecting Any Malware

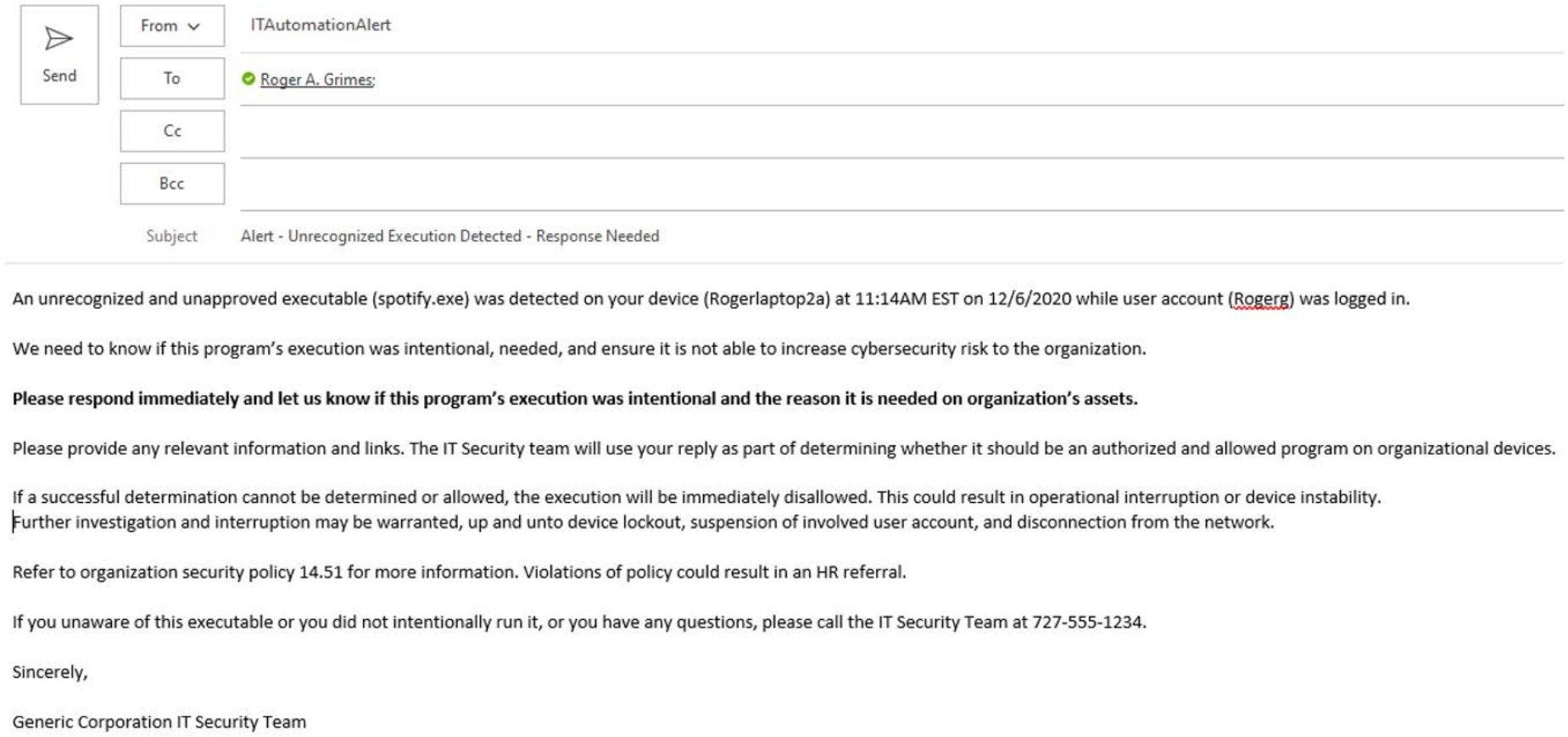
Workflow

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

Detecting Any Malware

Workflow



Send

From ITAutomationAlert

To 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

Detecting Any Malware

Advanced Workflow

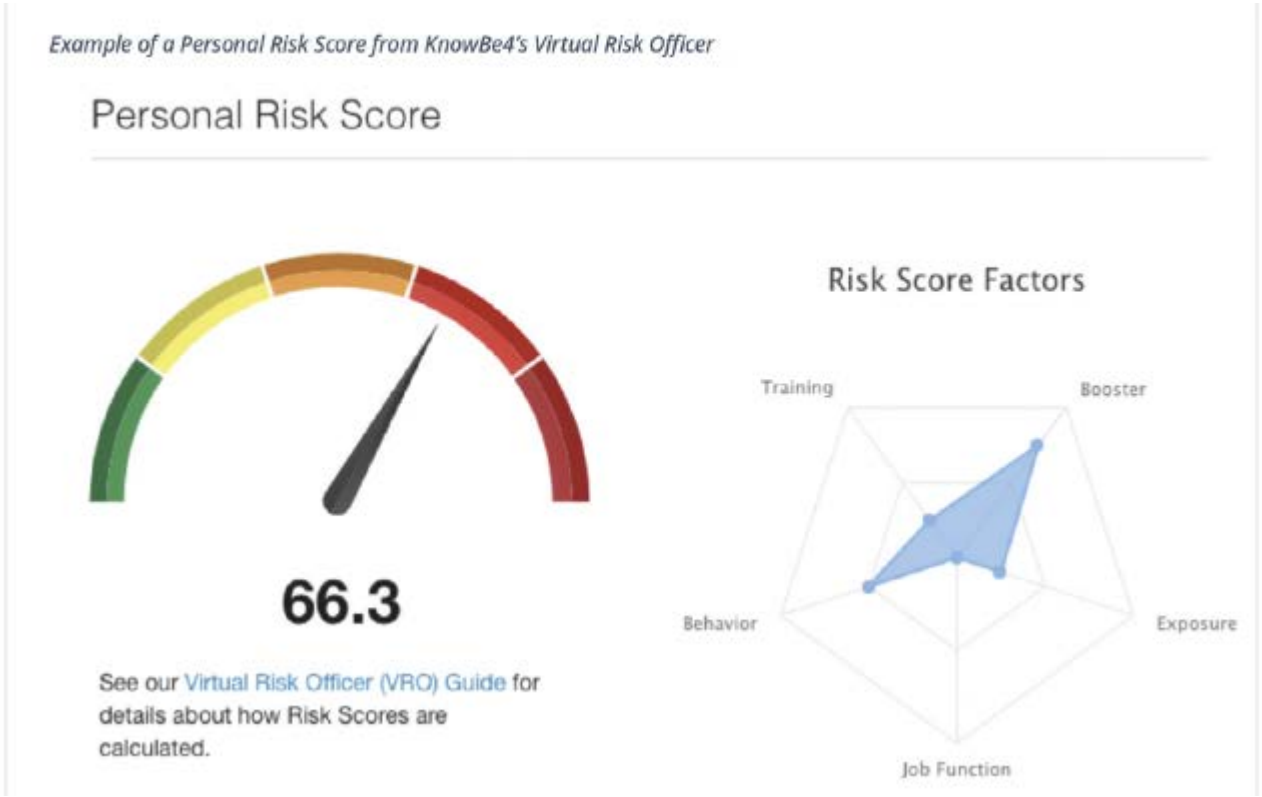
Example advanced automation security workflow

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

Detecting Any Malware

Advanced Workflow – Virtual Risk Officer

Example of a Personal Risk Score from KnowBe4's Virtual Risk Officer



Detecting Any Malware

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™ percentage of your users through a free simulated phishing attack.

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.

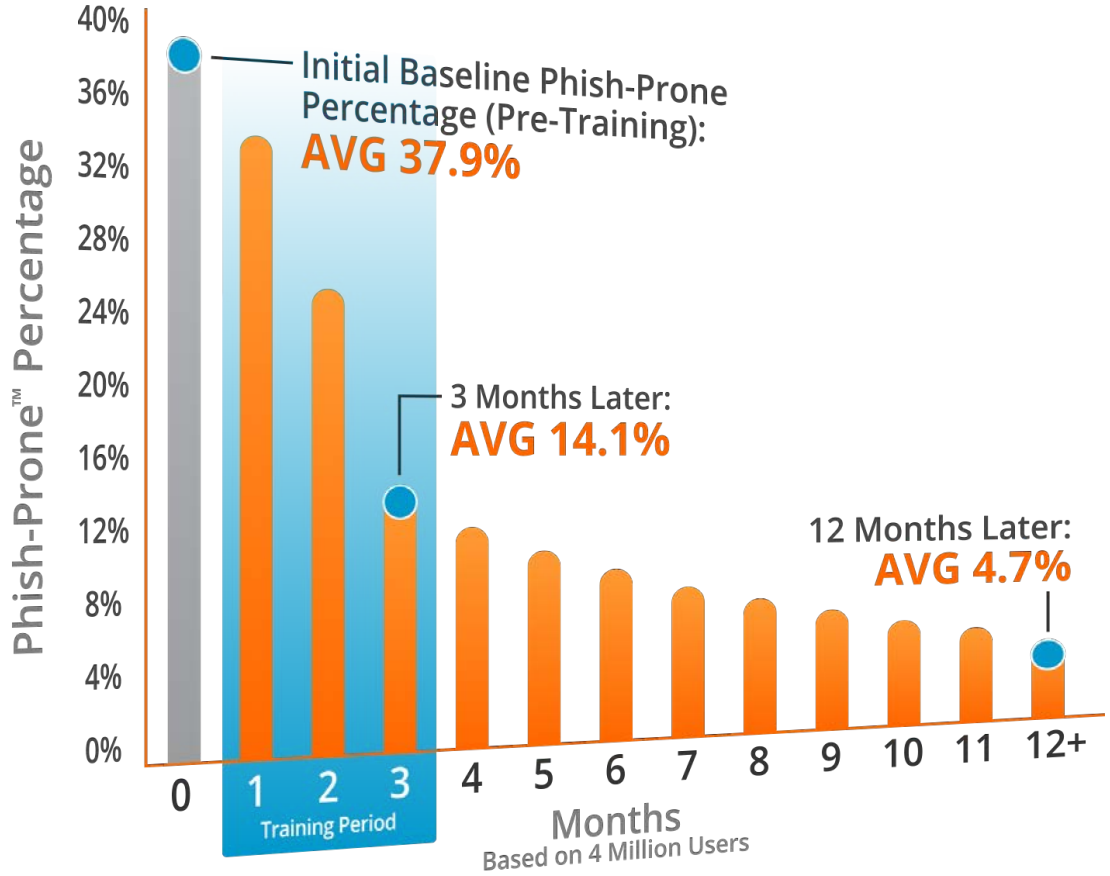
See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!

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/