



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.

e: rogerg@knowbe4.com

Twitter: [@RogerAGrimes](https://twitter.com/RogerAGrimes)

LinkedIn: <https://www.linkedin.com/in/rogeragrimes/>

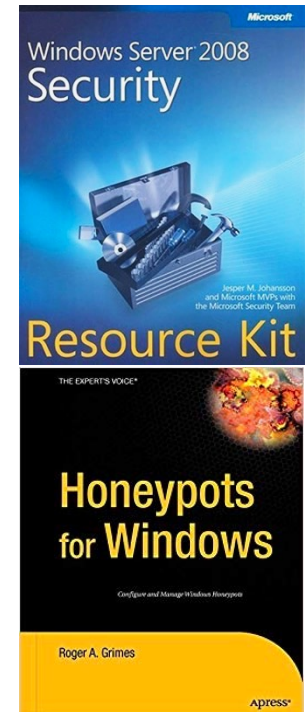
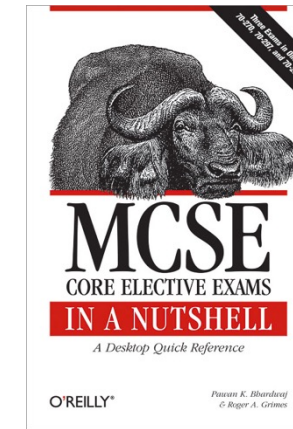
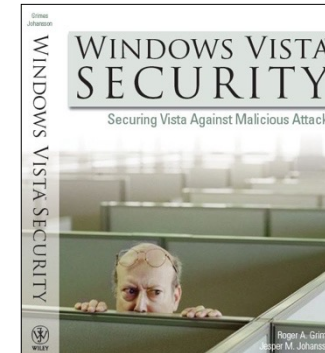
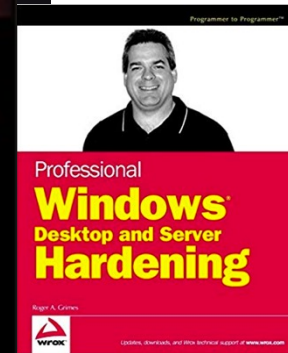
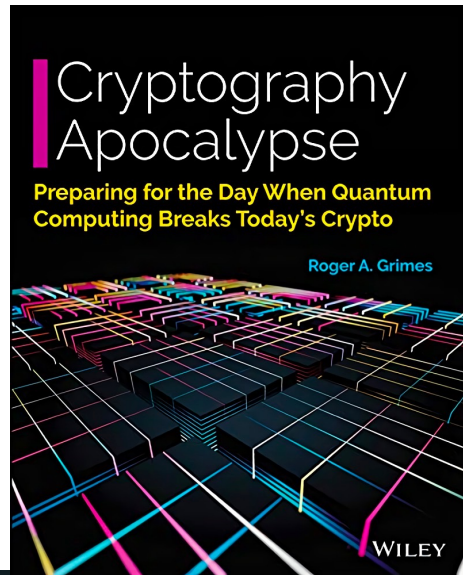
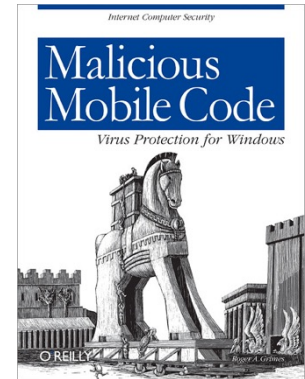
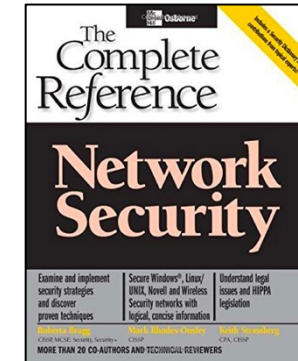
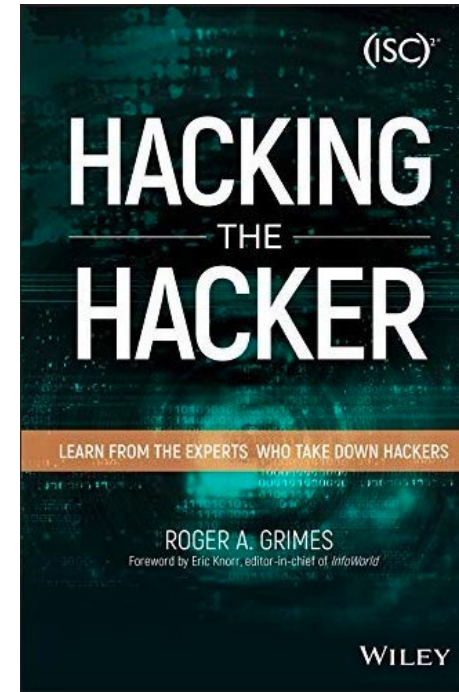
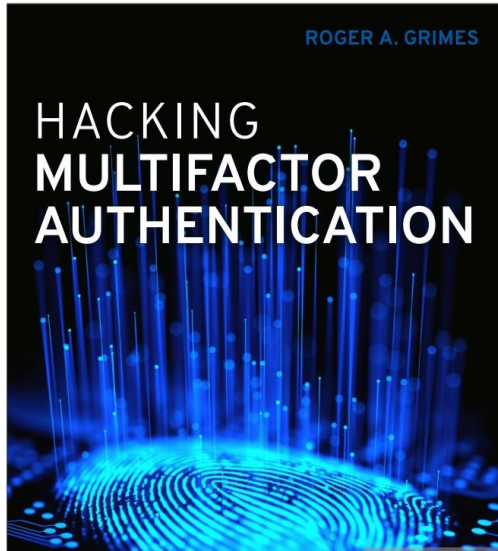
About Roger

- 30 years plus in computer security, 20 years pen testing
- 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 13 books and over 1,300 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 good backups (even offline backups) no longer save you from ransomware
- The policies, technical controls, and education you need to stop ransomware in its tracks
- Official recommendations from the Cybersecurity & Infrastructure Security Agency (CISA)
- How to detect ransomware programs, even those that are highly stealthy
- Incident response

Agenda

- Why good backups (even offline backups) no longer save you from ransomware
- The policies, technical controls, and education you need to stop ransomware in its tracks
- Official recommendations from the Cybersecurity & Infrastructure Security Agency (CISA)
- How to detect ransomware programs, even those that are highly stealthy
- Incident response

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

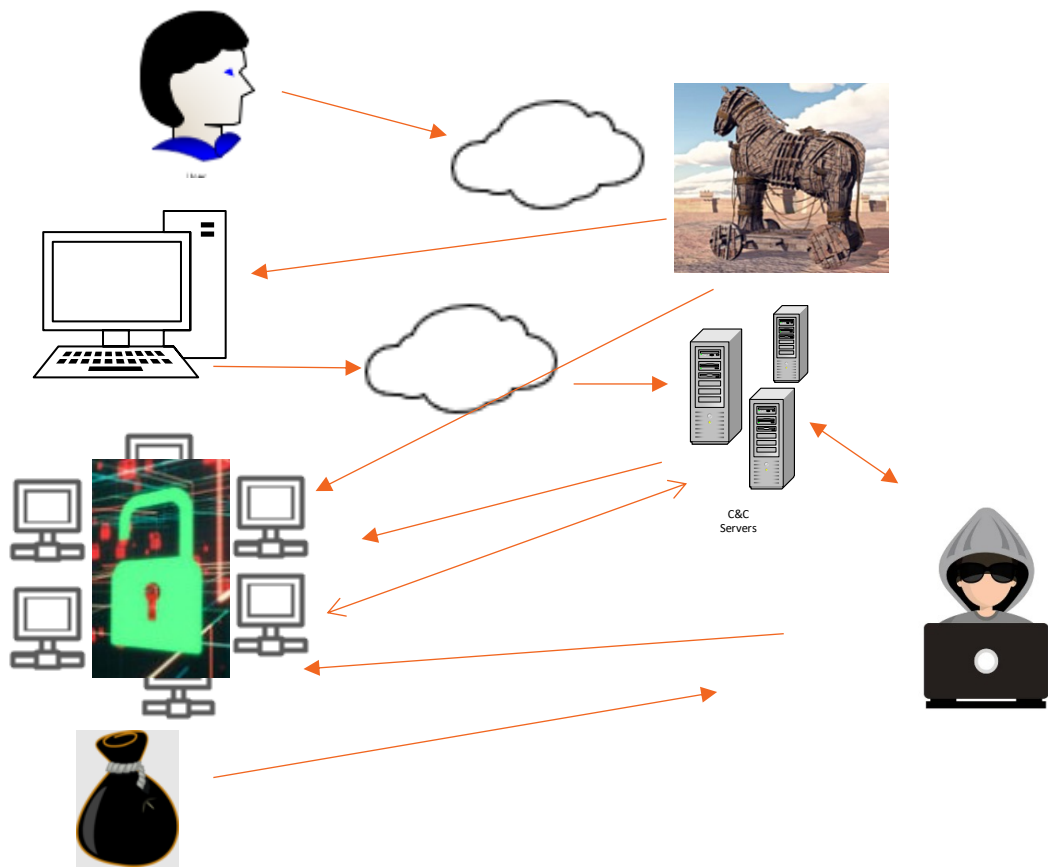
Essentially:

Starting in Nov/Dec 2019:

- 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...

Attacker Workflow

Today's Attacker Workflow



1. Victim tricked into executing "stager" trojan horse program, modifies host system
2. After executing, it immediately downloads updates and additional malware & instructions 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 C&C/hacker about 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 – “Double Extortion”

- 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>

Double Extortion is the Norm

Today's Ransomware Summary – Double Extortion

- Threats to exfiltrate data are over 86% of all ransomware attacks now

Data Exfiltration Remains Prevalent in Cyber Extortion

86% of ransomware cases involve a threat of leaking exfiltrated data. The proportion of companies that succumb to data exfiltration extortion continues to confound and frustrate Coveware and the IR industry at

<https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022>

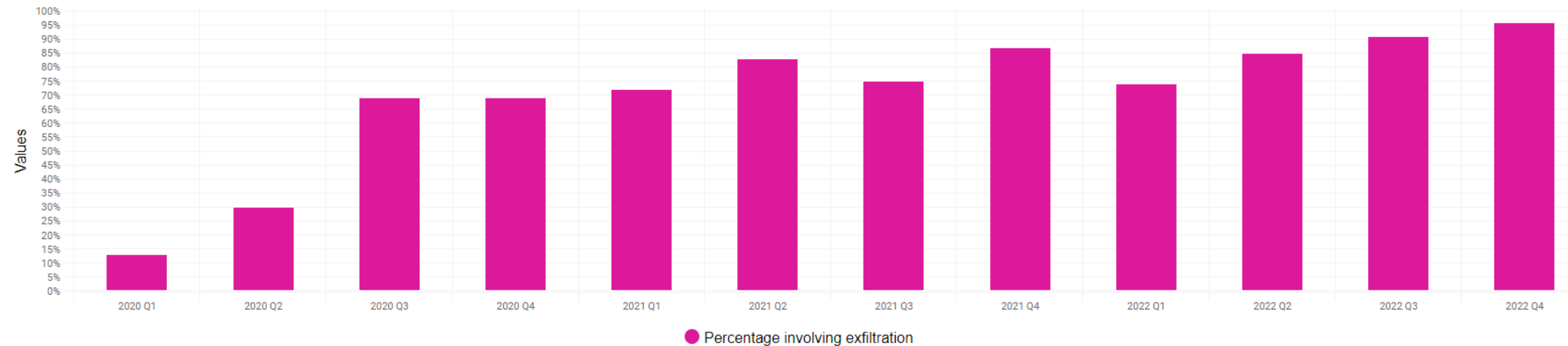
Double Extortion is the Norm

Today's Ransomware Summary – Double Extortion

- Threats to exfiltrate data are over 96% of all ransomware attacks now

Cyber Extortion Incidents with Data Exfiltration

Percentages by quarter



<https://www.beazley.com/en-us/cyber-services-snapshot/latest-trends>

Agenda

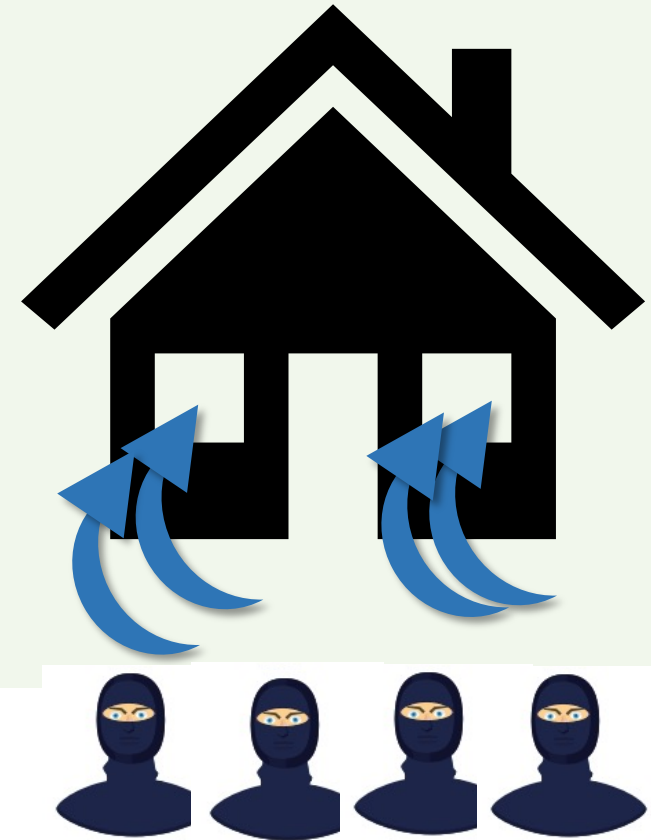
- Why good backups (even offline backups) no longer save you from ransomware
- The policies, technical controls, and education you need to stop ransomware in its tracks
- Official recommendations from the Cybersecurity & Infrastructure Security Agency (CISA)
- How to detect ransomware programs, even those that are highly stealthy
- Incident response

Home Crime Allegory

Houses can be broken into a number of different ways:

- Doors
- Windows
- Garage
- Walls
- Roof
- Etc.

If you want to stop house thieves, you need to mitigate the ways they most likely break-in



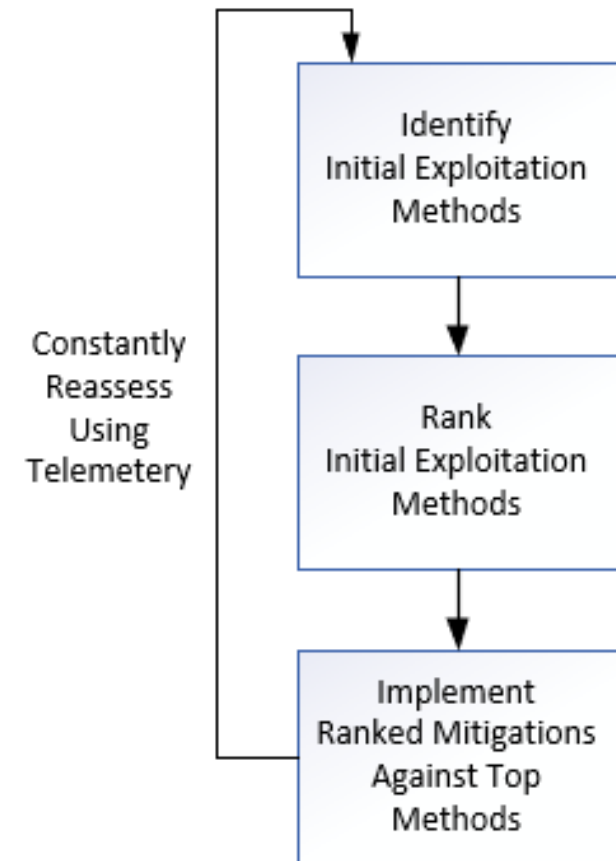
If you want to stop break-ins you need to close the holes thieves use to break-in

Initial Root Access Exploit Methods

How ALL attackers/malware break in

- Social Engineering
- Programming Bug (patch available or not available)
- Authentication Attack
- Malicious Instructions/Scripting
- Human Error/Misconfiguration
- Eavesdropping/MitM
- Side Channel/Information Leak
- Brute Force/Computational
- Data Malformation
- Network Traffic Malformation
- Insider Attack
- 3rd Party Reliance Issue (supply chain/vendor/partner/etc.)
- Physical Attack

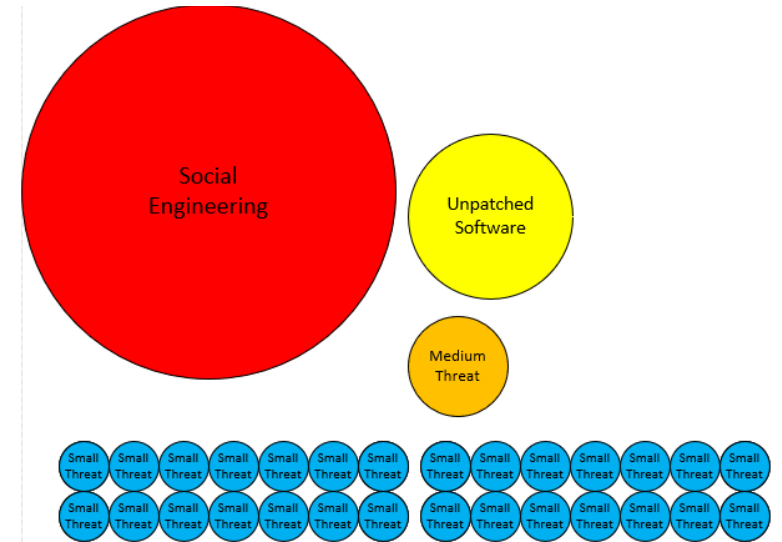
Core Data-Driven Defense Principle



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



How Ransomware Attacks

Top Ransomware Root Exploit Causes (in order)

- Social Engineering
- RDP Attacks
- Unpatched Software
- Password Attacks
- Other

Report Name	<u>Social engineering</u>	<u>Unpatched software</u>	<u>Remote server attack</u>	<u>RDP</u>	<u>Credential Theft</u>	<u>Password Guessing</u>	<u>Third Party</u>	<u>USB</u>	<u>Other</u>
	Coveware Report	30%	18%	-	45%	-	-	-	-
Statista	54%	-	-	20%	10%	-	-	-	-
Forbes magazine article	1st	2nd	-	3rd	-	-	-	-	-
Datto's Report	54%	-	-	20%	10%	21%	-	-	-
Hiscox Cyber Readiness	65%	28%	-	-	39%	19%	34%	-	-
Sophos Report	45%	-	21%	9%	-	-	9%	7%	9%
Averages	50%	23%	21%	24%	20%	20%	22%	7%	7%

Sources:

- Coveware Blog Report (<https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound>)
- Statista (<https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/>)
- Forbes magazine article (<https://www.forbes.com/sites/forbestechcouncil/2021/04/22/six-best-practices-for-ransomware-recovery-and-risk-mitigation/>)
- Datto's Global State of the Channel Ransomware Report (<https://www.datto.com/resources/dattos-2020-global-state-of-the-channel-ransomware-report>)
- Hiscox Cyber Readiness Report 2021 (<https://www.hiscoxgroup.com/sites/group/files/documents/2021-04/Hiscox%20Cyber%20Readiness%20Report%202021.pdf>)
- <https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf>

Best Defenses

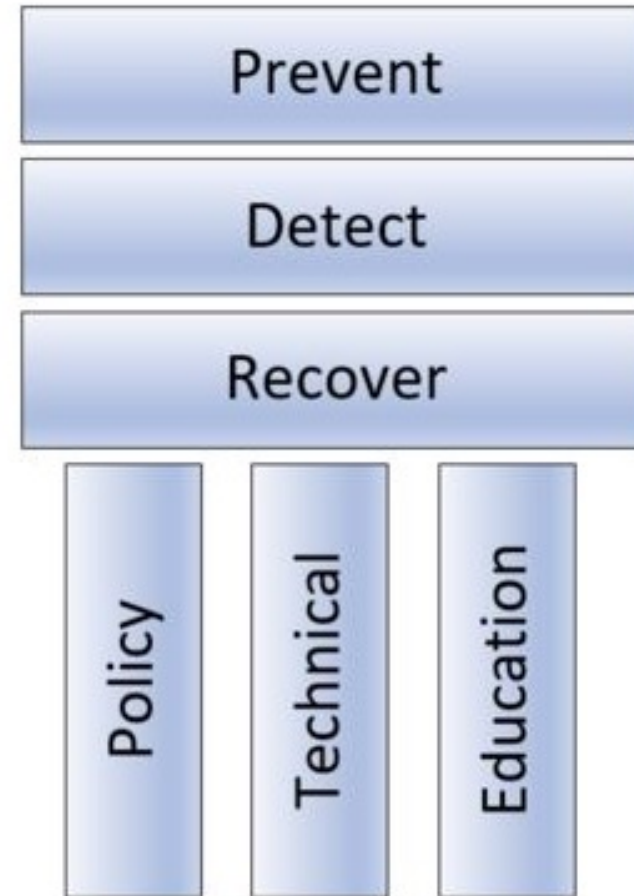
Most Important Critical Defenses

- **Good, thorough, complete system, tested, secure, 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 Defenses for Most Organizations

- **Aggressively Mitigate Social Engineering**
 - Policies, Technical Defenses, Education
 - <https://info.knowbe4.com/comprehensive-anti-phishing-guide>
- **Patch Exploited Software & Firmware**
 - <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- **Use Multifactor Authentication(MFA) When You Can**
 - Use non-phishable MFA where you can
 - <https://www.linkedin.com/pulse/my-list-good-strong-mfa-roger-grimes>
- **Use Different, Non-Guessable/Non-Crackable, Passwords for every website and service where you can't use MFA**
 - 12-char+ fully random or 20-character+ human-created passphrases
 - Use a password manager, <https://blog.knowbe4.com/password-policy-e-book>
- **Teach Everyone How to Spot Rogue URLs**
 - <https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks>
 - <https://info.knowbe4.com/rogue-urls>

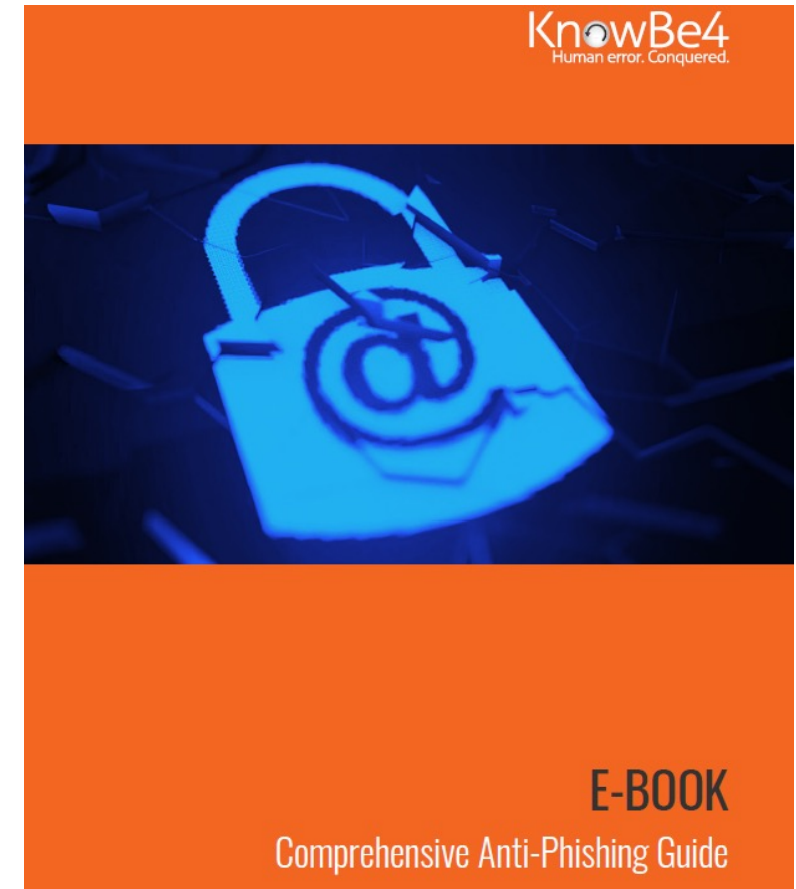
All Anti-Phishing Defenses

Everything You Can Try to Prevent Phishing

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

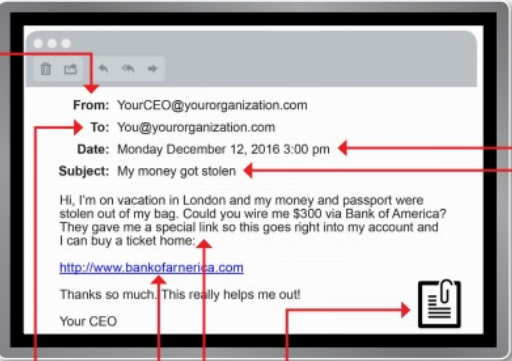


- E-book
 - <https://info.knowbe4.com/comprehensive-anti-phishing-guide>



Give or Get “Red Flags” Training

Social Engineering Red Flags



The infographic shows an email interface with several red flags pointing to specific parts of the message:

- FROM:** Points to the sender's email address: YourCEO@yourorganization.com
- TO:** Points to the recipient's email address: You@yourorganization.com
- DATE:** Points to the date and time: Monday December 12, 2016 3:00 pm
- SUBJECT:** Points to the subject line: My money got stolen
- ATTACHMENTS:** Points to an icon of a document with a checkmark, representing an attachment.
- CONTENT:** Points to the body text of the email.
- HYPERLINKS:** Points to a URL: <http://www.bankofamerica.com>

FROM

- 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.

TO

- 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.

HYPERLINKS

- 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.bankofamerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant or does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?

ATTACHMENTS

- 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 I know?

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

THE RED FLAGS OF ROGUE 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.

Look-a-Like Domains

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

Slight Misspellings

 Microsoftonline
<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%77%6B%6E%6F%77%62%65%63%6F%6D>

Shortened URLs

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

 <https://bit.ly/2SnA7Fnm>

Domain Mismatches

 Human Services .gov
<Despina.Orrantia6731610@gmx.com>

 <https://www.le-blog-qui-assure.com/>

Strange Originating Domains

 MAERSK
<info@onlinealxex.com.pl>

Overly Long URLs

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

 <http://innocentwebsite.com/irs.gov/logon/fasdjkg-sajdkjndfjnbkasldjfbkajsdbfkjbasdf/adsnfjksdngkfdgfgjhfgd/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
52 KB <https://d.pr/free/fjsaeoc>
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

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

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



CYBERSECURITY



INFRASTRUCTURE
SECURITY



EMERGENCY
COMMUNICATIONS



NATIONAL RISK
MANAGEMENT

CISA Recommendations

Cybersecurity and Infrastructure Security Agency (CISA) Example warnings



CYBERSECURITY ADVISORY

#StopRansomware: Royal Ransomware

Release Date: March 02, 2023

Alert Code: AA23-061A

[FTC Reports Scammers Impersonating FTC](#)

01/26/2021 05:17 PM EST

Original release date: January 26, 2021

SUMMARY

Note: This joint Cybersecurity Advisory (CSA) is part of an ongoing [#StopRansomware](#) effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These [#StopRansomware](#) advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all [#StopRansomware](#) advisories and to learn more about other ransomware threats and no-cost resources.

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

CISA #stopransomware

The screenshot shows the CISA #stopransomware website. At the top, there is a navigation bar with the following links: RESOURCES, NEWSROOM, ALERTS, REPORT RANSOMWARE, and CISA.GOV. Below the navigation bar is a search bar. The main content area features three large tiles:

- Lockbit 3.0:** A tile with a glowing padlock icon and the text "#STOPRANSOMWARE LOCKBIT 3.0". It includes logos for CISA, the Department of Justice, and MS-ISAC.
- Ransomware Hit:** A tile with a laptop screen displaying "RANSOMWARE" and the text "HAVE YOU BEEN HIT BY RANSOMWARE?". It includes a "LEARN MORE" button.
- Ransomware Vulnerability Warning Pilot Program:** A tile with the text "RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM" and a CISA logo.

At the bottom of the website, there is a footer with four icons and their corresponding labels: Protection and Response, Services, Public Safety, and Preparation.

CISA Recommendations

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 Address *

Submit

Cancel

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

[Privacy Policy](#) | [Cookie Statement](#) | [Help](#)



CISA Recommendations

CISA Known Exploited Vulnerability Catalog

- Lists software and firmware exploited by real criminals
- You should subscribe: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY



AMERICA'S CYBER DEFENSE AGENCY

Search

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date
CVE-2022-27926	Zimbra	Collaboration (ZCS)	Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability	2023-04-03	Zimbra Collaboration Suite (ZCS) contains a cross-site scripting vulnerability by allowing an endpoint URL to accept parameters without sanitizing.	Apply updates per vendor instructions.	2023-04-24
Notes https://wiki.zimbra.com/wiki/Security_Center							
CVE-2013-3163	Microsoft	Internet Explorer	Microsoft Internet Explorer Memory Corruption Vulnerability	2023-03-30	Microsoft Internet Explorer contains a memory corruption vulnerability that allows remote attackers to execute code or cause a denial of service via a crafted website.	The impacted product is end-of-life and should be disconnected if still in use.	2023-04-20
Notes https://learn.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-055							

CISA Recommendations

Cybersecurity and Infrastructure Security Agency (CISA)

- What does CISA recommend for fighting ransomware?

Actions to take today to mitigate cyber threats from ransomware:

- Prioritize remediating [known exploited vulnerabilities](#).
 - Train users to recognize and report [phishing attempts](#).
 - Enable and enforce [multifactor authentication](#).
- There's a much longer list, but these are the consistent Top 3 they recommend at the top of every ransomware alert



Example taken from: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a>

Agenda

- Why good backups (even offline backups) no longer save you from ransomware
- The policies, technical controls, and education you need to stop ransomware in its tracks
- Official recommendations from the Cybersecurity & Infrastructure Security Agency (CISA)
- How to detect ransomware programs, even those that are highly stealthy
- Incident response

Detecting Ransomware

Traditional Detection

- Extortion messages

Also Unexplained:

- Rogue executables
- Encrypted files
- Elevated group memberships
- Network connections
- Service stoppages
- Very large recent file archives

What happened?

All your important files have been encrypted and all sensitive data was stolen.
The only way to restore your files and keep your data from going public is to contact us.
After a payment has been made you will be given access to decryption software.
As a guarantee we will decrypt 3 files for free.
If you don't contact us within 72 hours the price will be doubled.

Instructions

- Download qTOX messenger from <https://qtox.github.io/>
- Send message to this Tox ID:
3728E933284CE638D06FCF1CBE921096E102508BD370D6D23137D3271EE5733825F63F56805E

Your message should contain your Unique Key: [REDACTED]



ALL YOUR **IMPORTANT FILES** ARE **STOLEN AND ENCRYPTED!**

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquires access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. I attach the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger.

Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.

Detecting Ransomware

Traditional Detection

- Traditional AV programs haven't been great at detecting ransomware

- Endpoint Detection and Response software is much better
 - You should be running one of these

Detecting Ransomware

Anomaly Detection – Different Ideas to Try

- Process Explorer paired with VirusTotal
- Application Control in audit mode

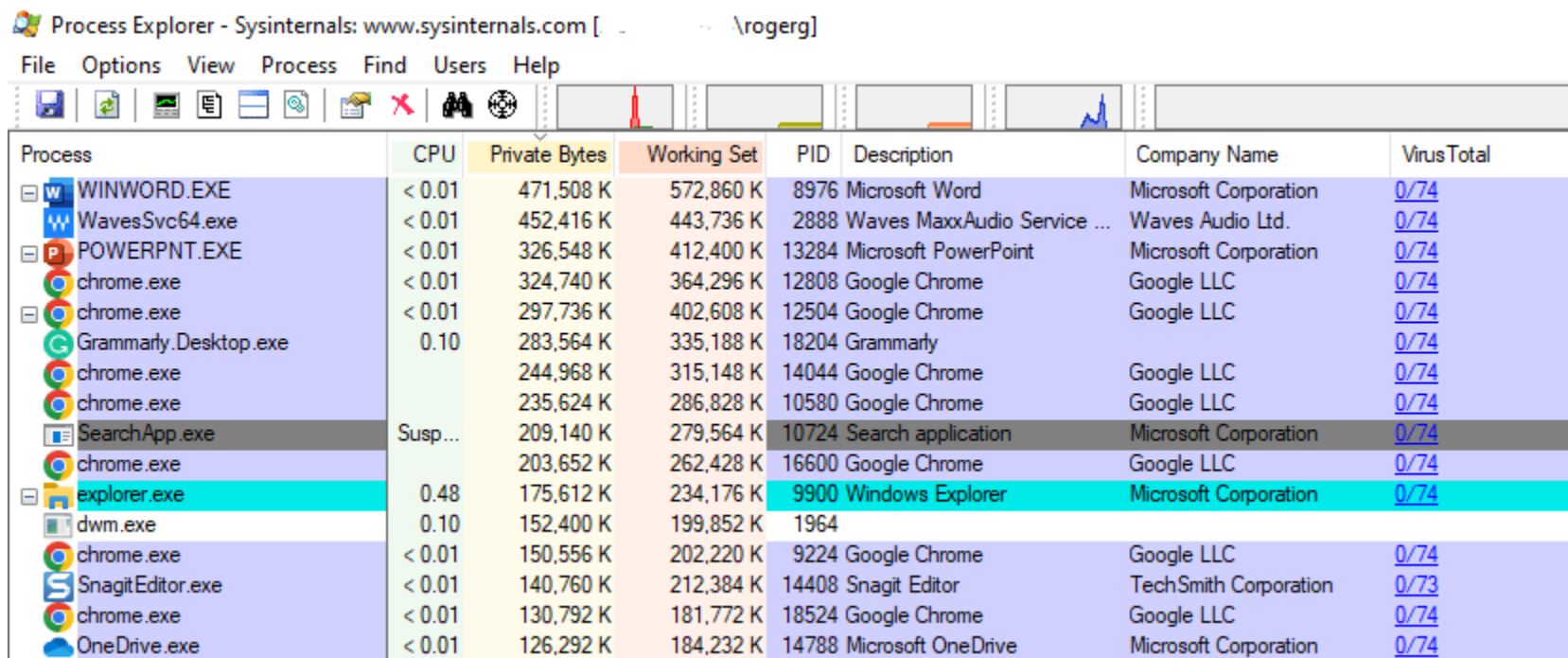
Detecting Ransomware

Process Explorer Paired With VirusTotal

- Process Explorer is a free Microsoft program for showing running executables
 - <https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer>
 - Sadly, only works on Microsoft Windows
- VirusTotal is a free Google web site that runs 70+ AV engines
- Run Process Explorer with VirusTotal option enabled to see if any running executables are flagged as malicious by any AV engine
- Note: Most executables flagged by only 1 AV engine are usually false-positives

Detecting Ransomware

Process Explorer Paired With VirusTotal



Process Explorer - Sysinternals: www.sysinternals.com [...] \rogerg]

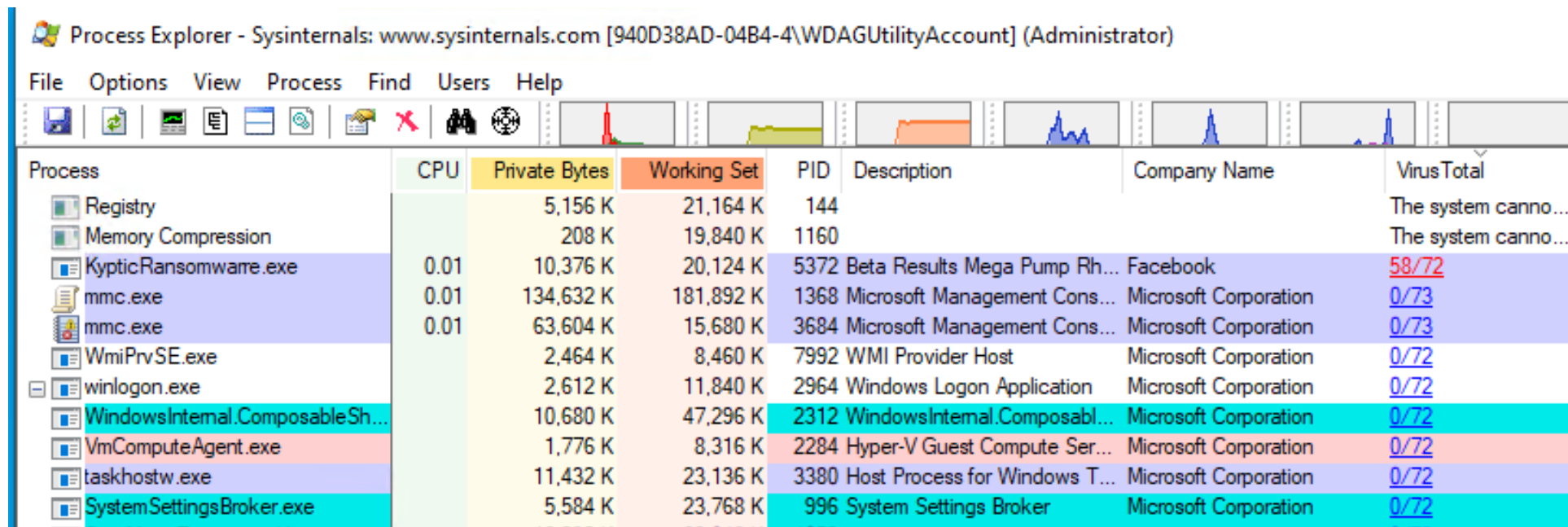
File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
WINWORD.EXE	< 0.01	471,508 K	572,860 K	8976	Microsoft Word	Microsoft Corporation	0/74
WavesSvc64.exe	< 0.01	452,416 K	443,736 K	2888	Waves MaxxAudio Service ...	Waves Audio Ltd.	0/74
POWERPNT.EXE	< 0.01	326,548 K	412,400 K	13284	Microsoft PowerPoint	Microsoft Corporation	0/74
chrome.exe	< 0.01	324,740 K	364,296 K	12808	Google Chrome	Google LLC	0/74
chrome.exe	< 0.01	297,736 K	402,608 K	12504	Google Chrome	Google LLC	0/74
Grammarly.Desktop.exe	0.10	283,564 K	335,188 K	18204	Grammarly		0/74
chrome.exe	< 0.01	244,968 K	315,148 K	14044	Google Chrome	Google LLC	0/74
chrome.exe	< 0.01	235,624 K	286,828 K	10580	Google Chrome	Google LLC	0/74
SearchApp.exe	Susp...	209,140 K	279,564 K	10724	Search application	Microsoft Corporation	0/74
chrome.exe	< 0.01	203,652 K	262,428 K	16600	Google Chrome	Google LLC	0/74
explorer.exe	0.48	175,612 K	234,176 K	9900	Windows Explorer	Microsoft Corporation	0/74
dwm.exe	0.10	152,400 K	199,852 K	1964			
chrome.exe	< 0.01	150,556 K	202,220 K	9224	Google Chrome	Google LLC	0/74
Snagit Editor.exe	< 0.01	140,760 K	212,384 K	14408	Snagit Editor	TechSmith Corporation	0/73
chrome.exe	< 0.01	130,792 K	181,772 K	18524	Google Chrome	Google LLC	0/74
OneDrive.exe	< 0.01	126,292 K	184,232 K	14788	Microsoft OneDrive	Microsoft Corporation	0/74

- <https://www.linkedin.com/pulse/what-should-you-do-suspect-your-computer-hacked-roger-grimes/>

Detecting Ransomware

Process Explorer Paired With VirusTotal



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
Registry		5,156 K	21,164 K	144			The system cannot find the file specified.
Memory Compression		208 K	19,840 K	1160			The system cannot find the file specified.
KypcticRansomwarre.exe	0.01	10,376 K	20,124 K	5372	Beta Results Mega Pump Rh...	Facebook	58/72
mmc.exe	0.01	134,632 K	181,892 K	1368	Microsoft Management Cons...	Microsoft Corporation	0/73
mmc.exe	0.01	63,604 K	15,680 K	3684	Microsoft Management Cons...	Microsoft Corporation	0/73
WmiPrvSE.exe		2,464 K	8,460 K	7992	WMI Provider Host	Microsoft Corporation	0/72
winlogon.exe		2,612 K	11,840 K	2964	Windows Logon Application	Microsoft Corporation	0/72
WindowsInternal.ComposableSh...		10,680 K	47,296 K	2312	WindowsInternal.Composabl...	Microsoft Corporation	0/72
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	0/72
SystemSettingsBroker.exe		5,584 K	23,768 K	996	System Settings Broker	Microsoft Corporation	0/72

- <https://www.linkedin.com/pulse/what-should-you-do-suspect-your-computer-hacked-roger-grimes/>

Detecting Ransomware

Application Control in Audit Mode

- Enable an application control program (e.g., AppLocker, etc.) in audit only mode
- Detect new executables and research

Detecting Ransomware

Determining How Long Malware Dwells and Where

Application Control Programs

- Allows you to block or allow certain 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 Ransomware

Determining How Long Malware Dwells and Where

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 Ransomware

Example Application Control Program Deployment

AppLocker

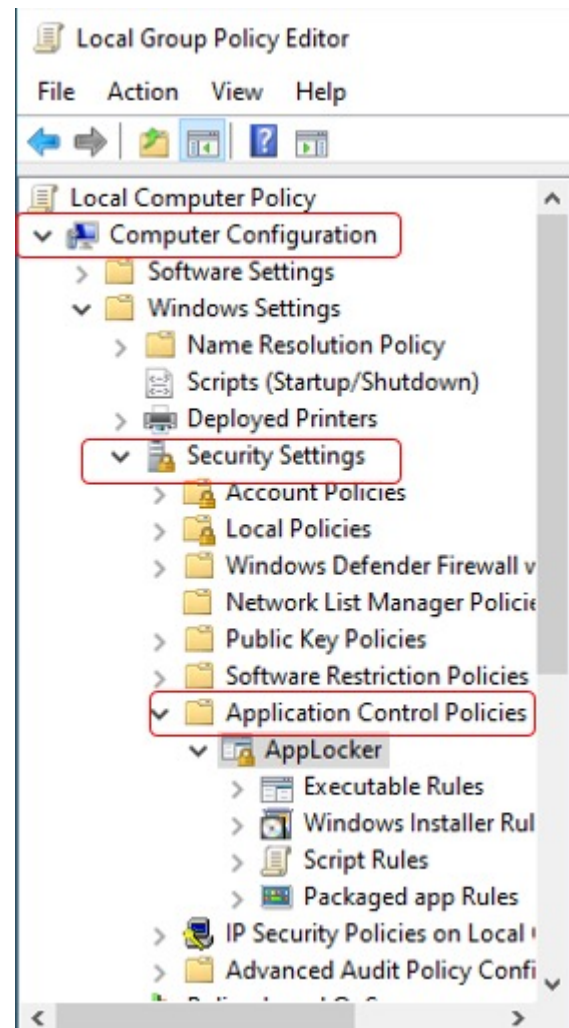
- Been in Microsoft Windows enterprise versions since Windows 7/Windows Server 2008
 - Early related Windows feature was Software Restriction Policies
 - Now called Windows Defender Application Control (WDAC), released in Windows 10
 - WDAC is a far more serious application control program than AppLocker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

Example Application Control Program Deployment

AppLocker

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



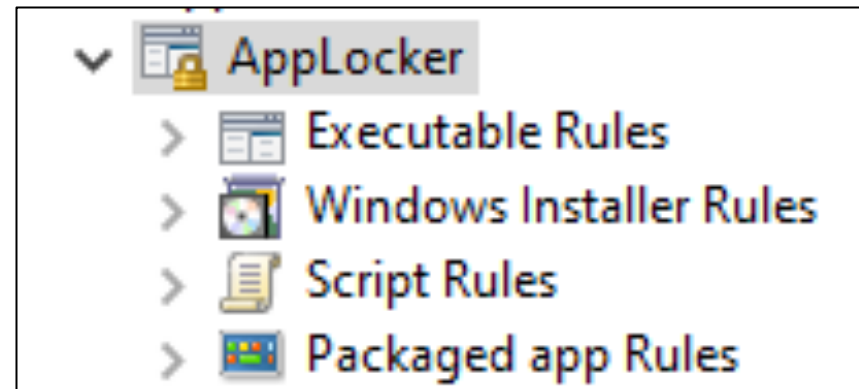
Detecting Ransomware

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 Ransomware

Example Application Control Program Deployment

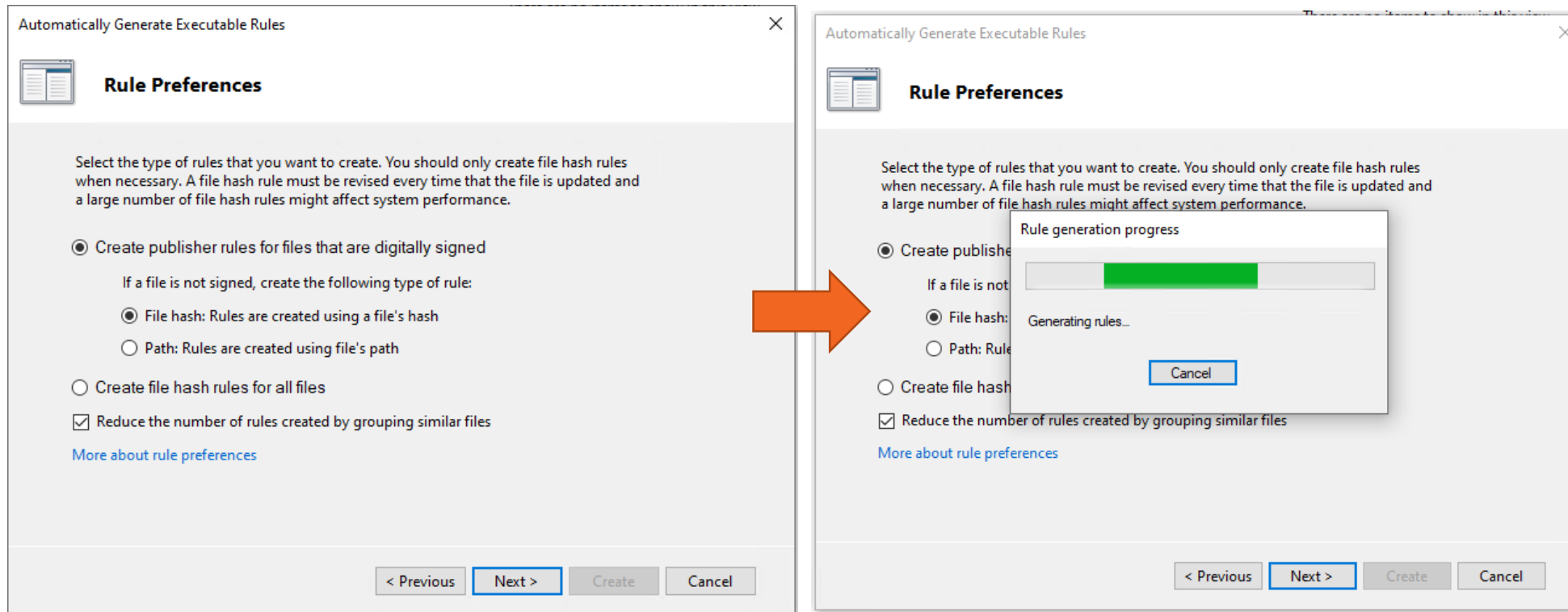
AppLocker

The image shows a sequence of three screenshots illustrating the deployment of AppLocker. The first screenshot shows the 'Local Computer Policy' console with 'AppLocker' selected under 'Application Control Policies'. A context menu is open, and the 'Properties' option is highlighted with a red box. The second screenshot shows the 'AppLocker Properties' dialog box with the 'Enforcement' tab selected. It displays enforcement settings for Executable rules, Windows Installer rules, Script rules, and Packaged app Rules, all set to 'Configured'. The third screenshot shows the 'AppLocker Properties' dialog box with the 'Advanced' tab selected, showing enforcement settings for each rule collection, all set to 'Configured'. An orange arrow points from the 'Enforcement' tab to the 'Advanced' tab.

Detecting Ransomware

Example Application Control Program Deployment

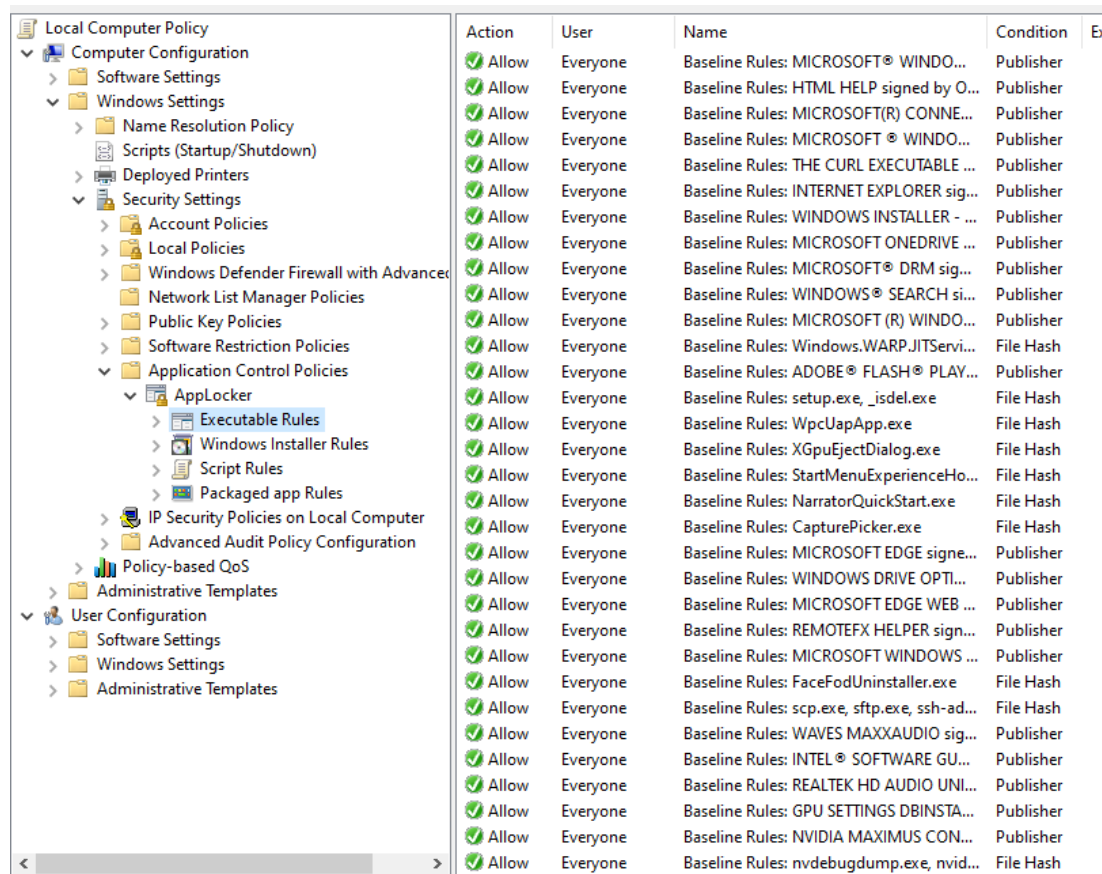
AppLocker



Detecting Ransomware

Example Application Control Program Deployment

AppLocker



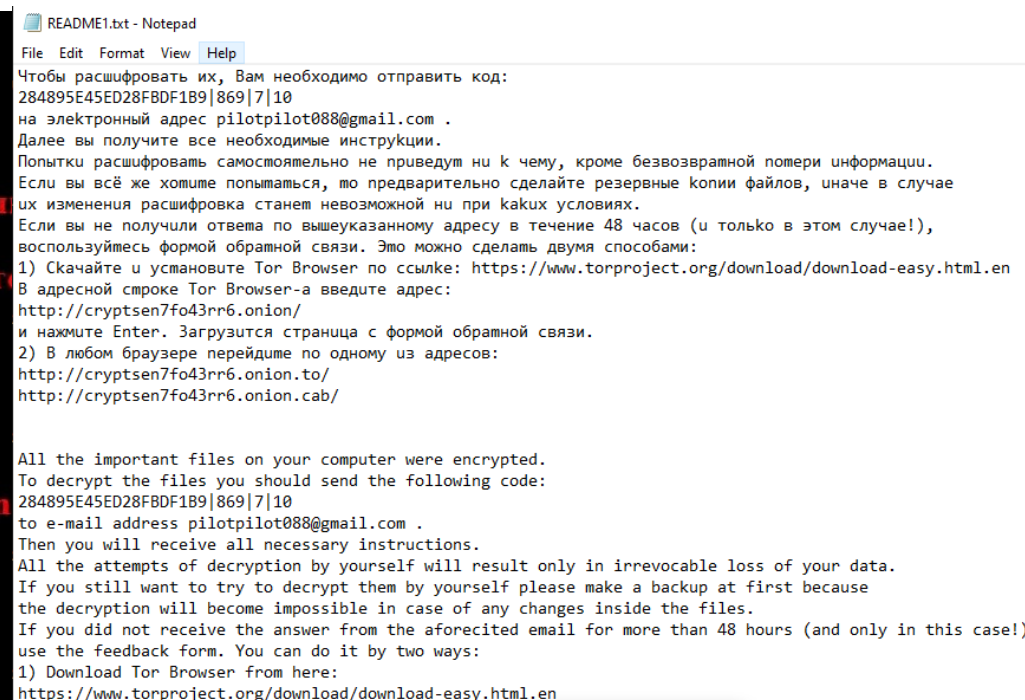
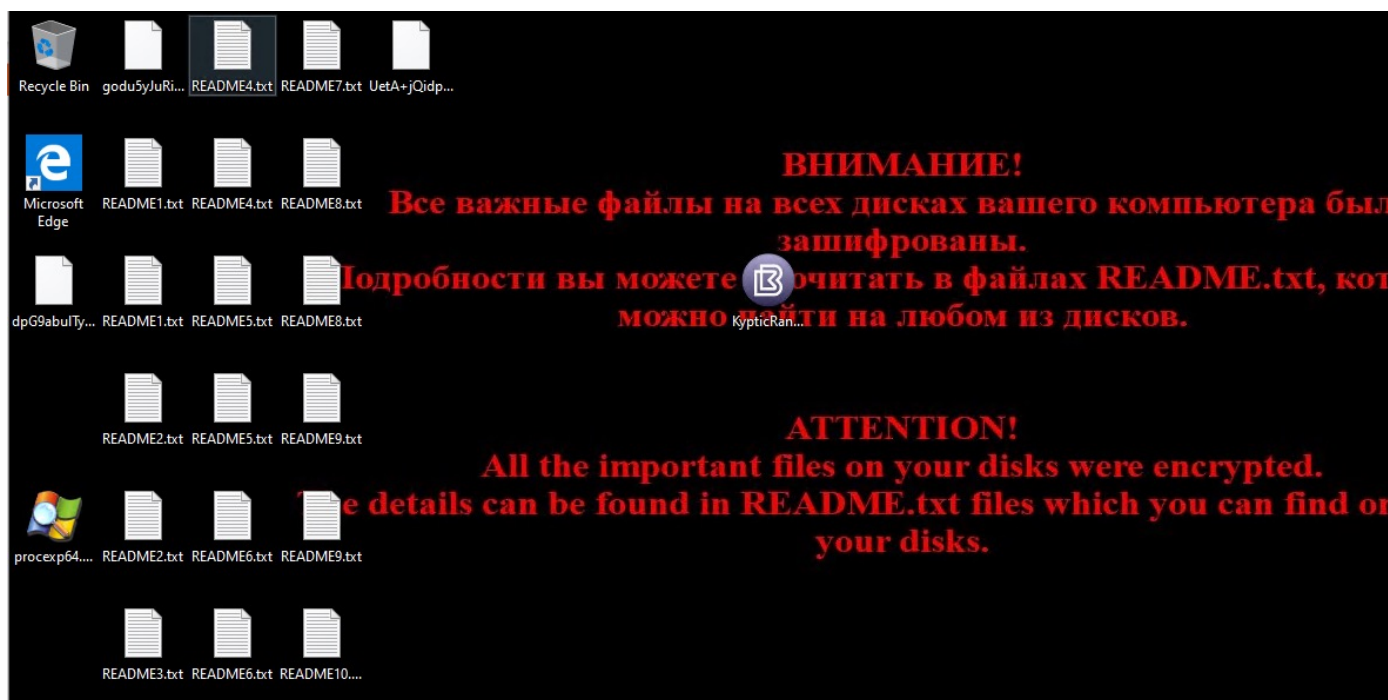
Action	User	Name	Condition
Allow	Everyone	Baseline Rules: MICROSOFT® WINDO...	Publisher
Allow	Everyone	Baseline Rules: HTML HELP signed by O...	Publisher
Allow	Everyone	Baseline Rules: MICROSOFT(R) CONNE...	Publisher
Allow	Everyone	Baseline Rules: MICROSOFT® WINDO...	Publisher
Allow	Everyone	Baseline Rules: THE CURL EXECUTABLE ...	Publisher
Allow	Everyone	Baseline Rules: INTERNET EXPLORER sig...	Publisher
Allow	Everyone	Baseline Rules: WINDOWS INSTALLER - ...	Publisher
Allow	Everyone	Baseline Rules: MICROSOFT ONEDRIVE ...	Publisher
Allow	Everyone	Baseline Rules: MICROSOFT® DRM sig...	Publisher
Allow	Everyone	Baseline Rules: WINDOWS® SEARCH si...	Publisher
Allow	Everyone	Baseline Rules: MICROSOFT (R) WINDO...	Publisher
Allow	Everyone	Baseline Rules: Windows.WARP.JIT Servi...	File Hash
Allow	Everyone	Baseline Rules: ADOBE® FLASH® PLAY...	Publisher
Allow	Everyone	Baseline Rules: setup.exe, _isdcl.exe	File Hash
Allow	Everyone	Baseline Rules: WpcUapApp.exe	File Hash
Allow	Everyone	Baseline Rules: XGpuEjectDialog.exe	File Hash
Allow	Everyone	Baseline Rules: StartMenuExperienceHo...	File Hash
Allow	Everyone	Baseline Rules: NarratorQuickStart.exe	File Hash
Allow	Everyone	Baseline Rules: CapturePicker.exe	File Hash
Allow	Everyone	Baseline Rules: MICROSOFT EDGE signe...	Publisher
Allow	Everyone	Baseline Rules: WINDOWS DRIVE OPTI...	Publisher
Allow	Everyone	Baseline Rules: MICROSOFT EDGE WEB ...	Publisher
Allow	Everyone	Baseline Rules: REMOTEFX HELPER sign...	Publisher
Allow	Everyone	Baseline Rules: MICROSOFT WINDOWS ...	Publisher
Allow	Everyone	Baseline Rules: FaceFodUninstaller.exe	File Hash
Allow	Everyone	Baseline Rules: scp.exe, sftp.exe, ssh-ad...	File Hash
Allow	Everyone	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: GPU SETTINGS DBINSTA...	Publisher
Allow	Everyone	Baseline Rules: NVIDIA MAXIMUS CON...	Publisher
Allow	Everyone	Baseline Rules: nvdebugdump.exe, nvid...	File Hash

Detecting Ransomware

Example Application Control Program Deployment

AppLocker

Malshare Example – When It Executes

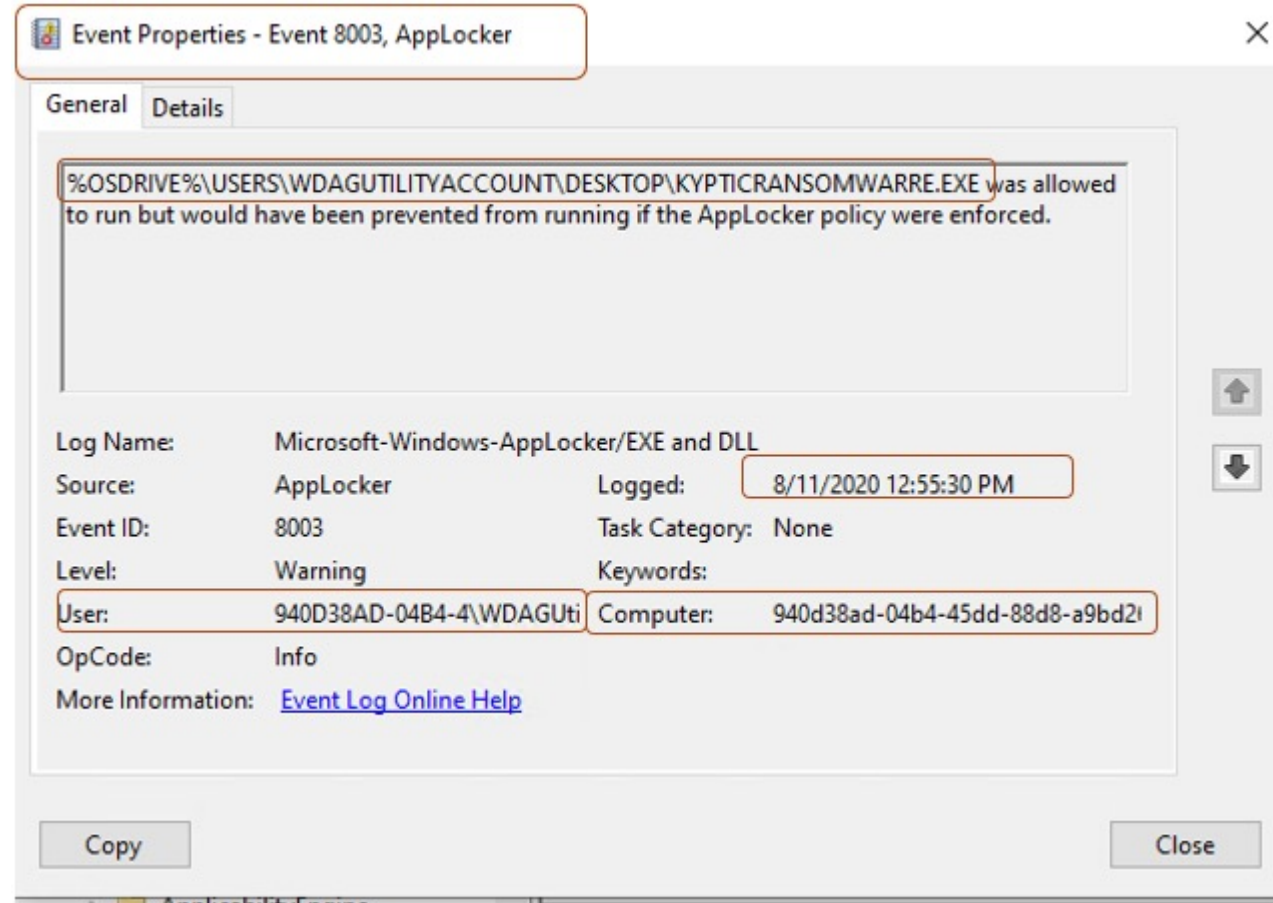


Detecting Ransomware

Example Application Control Program Deployment

AppLocker

Pull all 8003 events to
a centralized database



Agenda

- Why good backups (even offline backups) no longer save you from ransomware
- The policies, technical controls, and education you need to stop ransomware in its tracks
- Official recommendations from the Cybersecurity & Infrastructure Security Agency (CISA)
- How to detect ransomware programs, even those that are highly stealthy
- Incident response

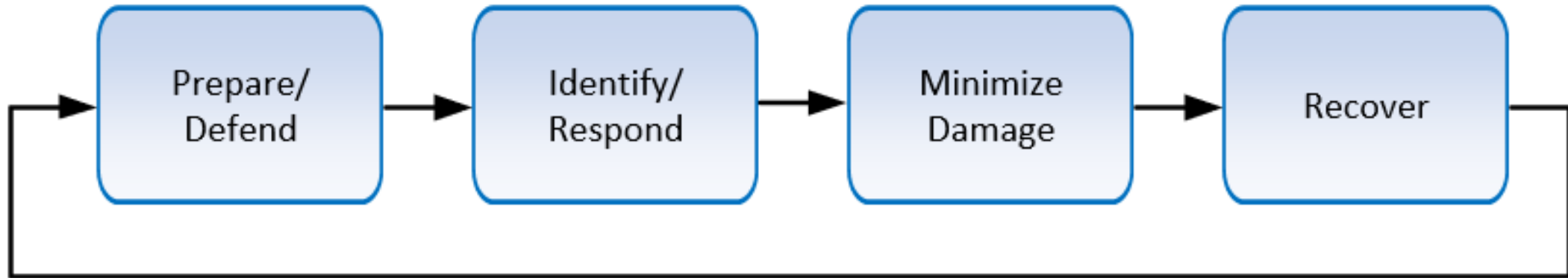
KnowBe4 Ransomware Resources

- **Ransomware Response Step-by-Step Checklist**

<https://www.knowbe4.com/ransomware#ransomwarechecklist>



Ransomware Defense Step-by-Step



Ransomware Response

First Things First

STEP I: Initial Investigation

- a. Determine if it is a real ransomware attack
- b. Determine if more than one device is exploited

If so, continue:

- There are fake “scareware” ransomware attacks
 - **Is it possibly wiperware?**
 - Weird file extensions?
 - Ransom note?
 - Are files really modified?
 - What appears impacted?
-
- Start documentation trail on previously agreed upon wiki

Ransomware Response

Next

STEP 2: Declare Ransomware Event and Start Incident Response

- a. Declare ransomware event
- b. Begin using predefined, alternate communications
- c. Notify team members, senior management and legal

- Notify organization's communications team
- Will need to communicate to staff, customers, regulators, investors, etc.

- Everyone should know their predefined roles and expectations
- Early tasks include looking for more signs of spread
- What is and isn't impacted?
- Legal should communicate with any outside parties
- Don't usually have to involve insurance co's yet unless they help with response

Ransomware Response

Next

STEP 3: Disconnect Network

- a. Disable networking (from network devices, if possible)
- b. Power off devices if wiperware is suspected

Try to stop further:

- Spread
 - Damage
 - Communication to and from ransomware hackers
-
- Disable networking at hubs, switches and routers, if possible
 - Know commands and practice ahead of time
 - Easier to restore network access when needed
 - Know ahead of time what you can and can't disable
 - When in doubt of wiperware vs. ransomware, power-off

Ransomware Response

Next

STEP 4: Determine the Scope of the Exploitation

Check the Following for Signs:

- a. Mapped or shared drives
- b. Cloud-based storage: DropBox, Google Drive, OneDrive, etc.
- c. Network storage devices of any kind
- d. External hard drives
- e. USB storage devices of any kind (USB sticks, memory sticks, attached phones/cameras)
- f. Mapped or shared folders from other computers

Impact

- What locations?
 - What OS's
 - What apps
 - What types of files
 - What isn't impacted?
- If ransom extortion message has a link, don't click it!
 - Could start timer countdown and notify ransomware hackers of new conquest

Ransomware Response

Next

Determine if data or credentials have been stolen

- a. Check logs and DLP software for signs of data leaks
- b. Look for unexpected large archival files (e.g., zip, arc, etc.) containing confidential data that could have been used as staging files
- c. Look for malware, tools and scripts that could have been used to look for and copy data
- d. Of course, one of the most accurate signs of ransomware data theft is a notice from the involved ransomware gang announcing that your data and/or credentials have been stolen

84% or more of ransomware does data exfiltration

Ransomware Response

Next

STEP 5: Limit Initial Damage

- a. Initial investigators should try to stop/reduce any damage they discover, if possible

STEP 6: Gather Team to Share Information

- a. The goal is to make sure the team correctly understands all information, including scope and extent of damage

- No one should assume that everyone knows all the facts
- Share what you know
- Document, document, document
- Share with others and make sure everyone agrees with initial assessment

Ransomware Response

Next

STEP 7: Determine Response

- a. Pay the ransom or not?
- b. Repair or rebuild?
- c. Invite in additional external parties?
- d. Notify regulator bodies, law enforcement, CISA, FBI, etc.?

- If you decide to pay ransom, make sure it is legal to do so
- New or complete rebuild is always the safer choice
- Repair option is usually faster, but riskier
- Senior mgmt. and legal should make these decisions

Ransomware Response

Next

STEP 8: Recover Environment

- a. Repair only or rebuild
- b. Need to preserve evidence?
- c. Use business impact analysis to determine what devices and systems to recover and the associated timing
- d. Restore critical infrastructure first

- Determine what mission-critical apps you need to get back up and working first (should know this ahead of time)
- Know critical dependencies ahead of time (or determine)

Ransomware Response

Next

STEP 8: Recover Environment

- a. Repair only or rebuild
- b. Need to preserve evidence?
- c. Use business impact analysis to determine what devices and systems to recover and the associated timing
- d. Restore critical infrastructure first

- Usually, infrastructure is first before everything else
 - DNS, IP, DHCP, Active Directory
- Get IT security back up and running, then apps
- Start re-enabling needed network ports and pathways
- When in doubt, rebuild

Ransomware Response

Next

STEP 8: Recover Environment

- a. Repair only or rebuild
- b. Need to preserve evidence?
- c. Use business impact analysis to determine what devices and systems to recover and the associated timing
- d. Restore critical infrastructure first

- Clean apps and before running apps or opening network/Internet:
- Reset all possibly compromised passwords

Ransomware Response

Next

STEP 8: Recover Environment

- a. Repair only or rebuild
- b. Need to preserve evidence?
- c. Use business impact analysis to determine what devices and systems to recover and the associated timing
- d. Restore critical infrastructure first

- Preserving evidence
 - If not sure, assume this is necessary
 - Take memory and disk snapshots before modifying existing devices
 - Build new instances on new devices

Ransomware Response

Next

STEP 8: Recover Environment

- a. Repair only or rebuild
- b. Need to preserve evidence?
- c. Use business impact analysis to determine what devices and systems to recover and the associated timing
- d. Restore critical infrastructure first

- Restoring Data
 - From recovered encrypted files with hacker's help or trusted, tested backups?

Ransomware Response

Prevent Next Time

Step 9: Next Steps

Prevent the Next Cyber Attack:

- a. Mitigate social engineering
- b. Patch software
- c. Use multi-factor authentication (MFA) where you can
- d. Use strong, unique passwords
- e. Use antivirus or endpoint detection and response software
- f. Use anti-spam/anti-phishing software
- g. Use data leak prevention (DLP) software
- h. Have a good back up and regularly test

You Are More Likely To Be Hit Again, If:

- You don't determine the initial root cause
- You don't pay the ransom
- You repair versus rebuild
- Don't harden your environment against future attacks

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!

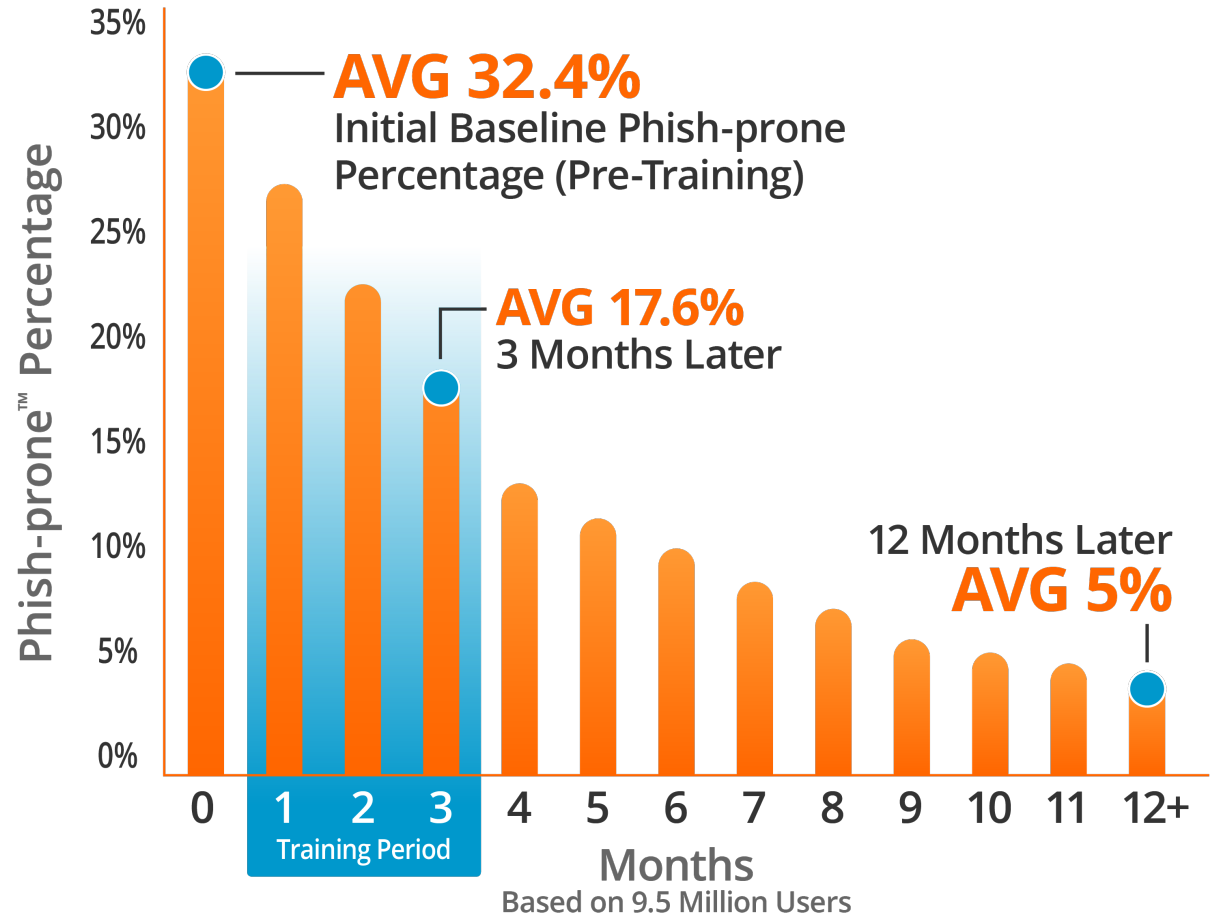


Generating Industry-Leading Results and ROI

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

85% Average Improvement

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



Source: 2022 KnowBe4 Phishing by Industry Benchmarking Report

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 console prior to the evaluation. Subsequent time periods reflect Phish-prone Percentages for the subset of users who received training with the KnowBe4 console.

Questions?

Roger A. Grimes— Data-Driven Defense Evangelist, KnowBe4

rogerg@knowbe4.com

Twitter: [@rogeragrimes](https://twitter.com/rogeragrimes)

<https://www.linkedin.com/in/rogeragrimes/>