KnowBe4
Human error. Conquered.

# Nation-State Hacking 2.0: Why Your Organization is Now at Risk from this Evolving Threat

**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/

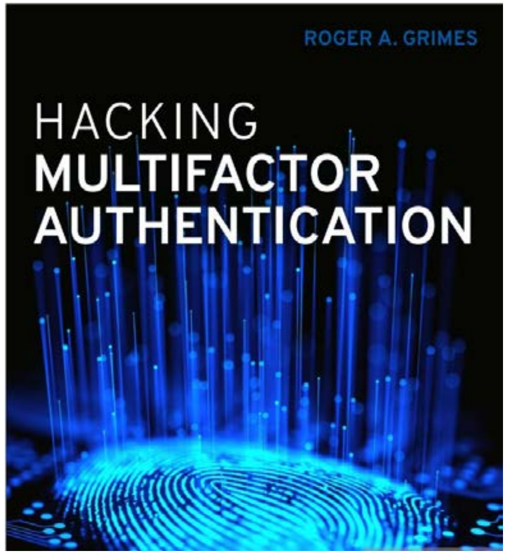
# About Roger

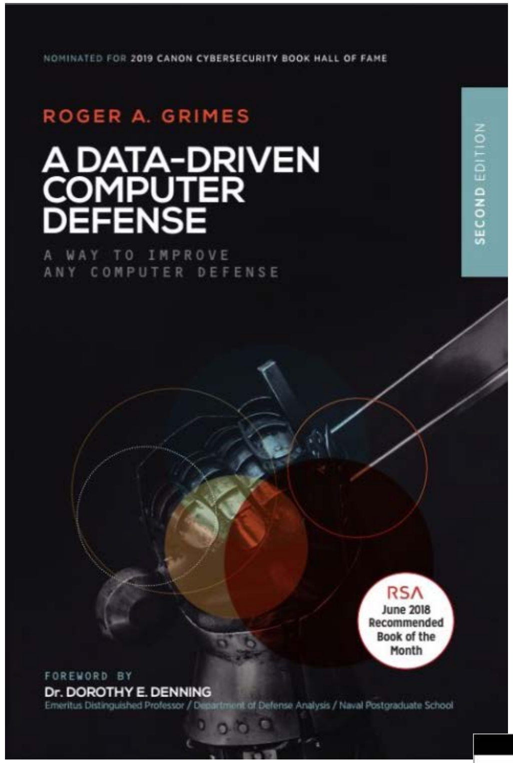
- 30 years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 12 books and over 1,100 magazine articles
-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

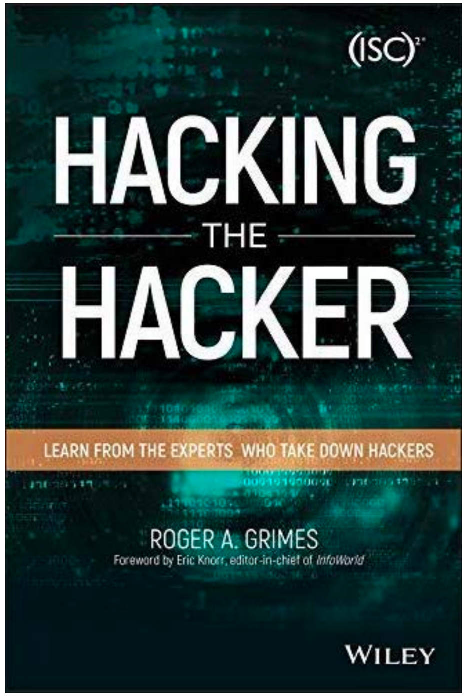
**Certification exams passed include:**

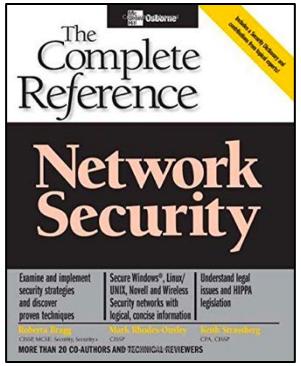
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

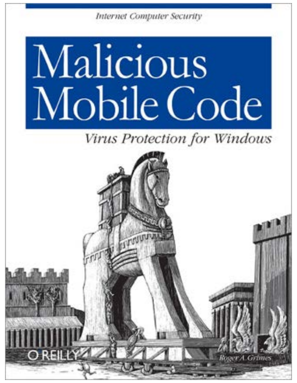
# Roger’s Books

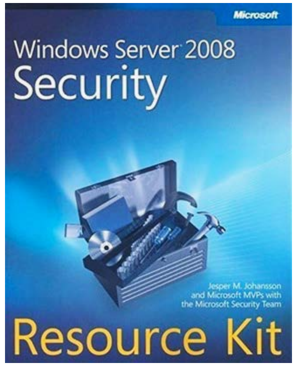


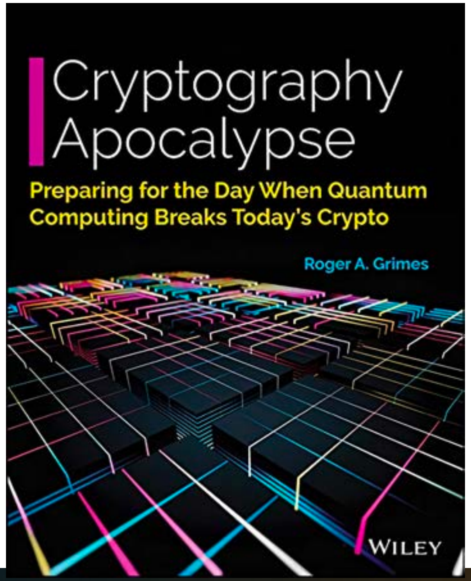


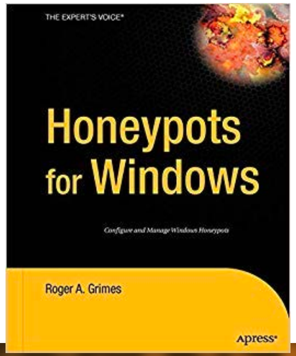

(ISC)²
HACKING
THE
HACKER
LEARN FROM THE EXPERTS WHO TAKE DOWN HACKERS
ROGER A. GRIMES
Foreword by Eric Knorr, editor-in-chief of InfoWorld
WILEY

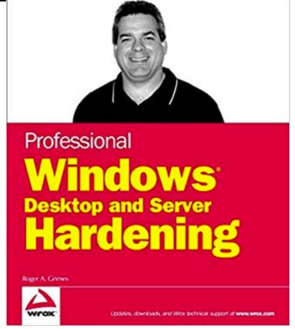


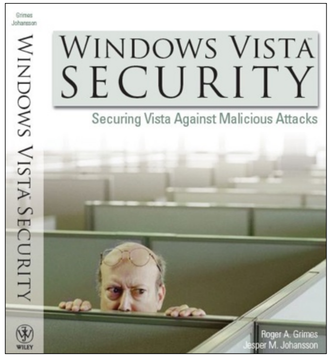


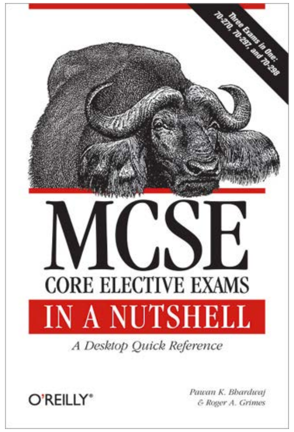


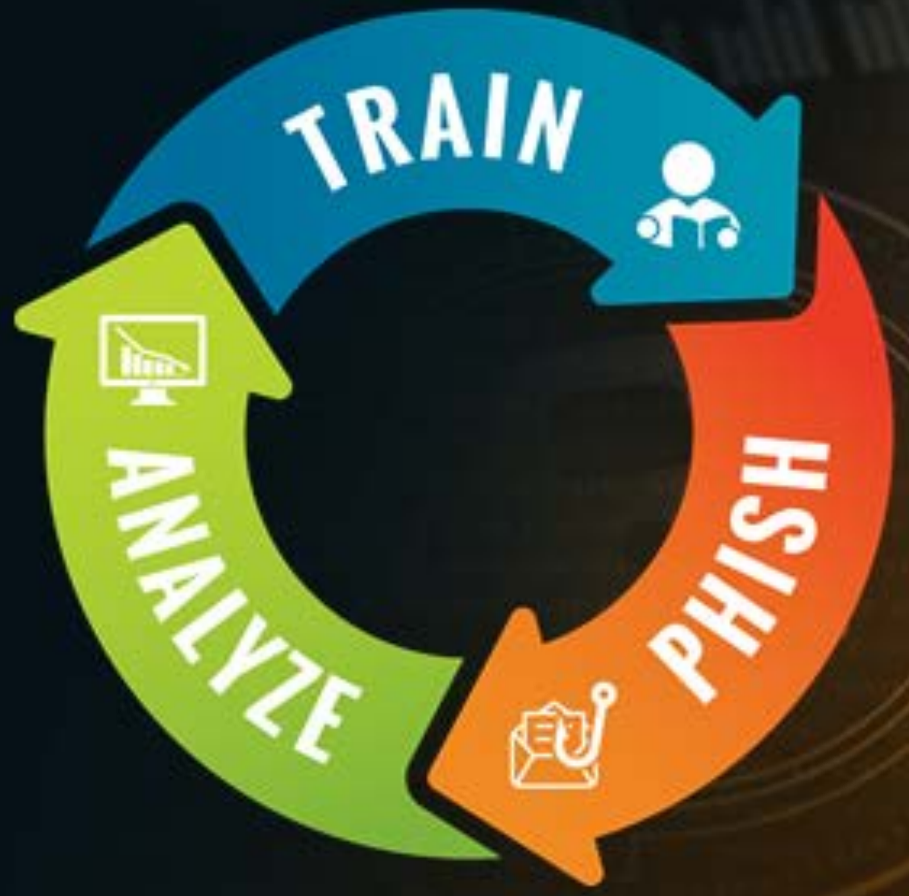

Cryptography
Apocalypse
Preparing for the Day When Quantum
Computing Breaks Today's Crypto
Roger A. Grimes
WILEY











# 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

***This presentation may contain real and/or simulated phishing attacks. The trade names/trademarks of any third parties used in this presentation are solely for illustrative and educational purposes. Trademarks are property of their respective owners and the use or display of any mark does not imply any affiliation with, endorsement by, or association of any kind between such third parties and KnowBe4, if any.***

The bad guys don't care about this and use them anyway to trick you….

# Agenda

- Brief History of Nation-State Attacks
- Why They Are Now Targeting Your Organization
- Mitigating Nation-State Attacks

# Agenda

- Brief History of Nation-State Attacks
- Why They Are Now Targeting Your Organization
- Mitigating Nation-State Attacks

# Nation-State Attackers

Personal Story

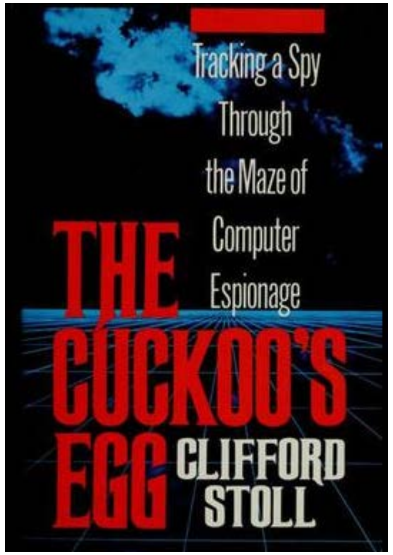
- When I was at pen testing company, the best hacker I knew went to work for the US government
- He worked for a large DC subcontractor (well known employment agency)
- When I asked him what it was like working for the  US government, he said there were thousands of people just like him
- I asked if he was using his great hacking skills to break into places
- He said no
- His job was to train an AI machine who found “zero days” to better recognize when it found an exploitable zero day…and that the computer was much better than he was
- He said they had thousands of 0-day exploits
- He told me that they could break into whatever they needed to at will

# Nation-State Attackers

- Most capable nations have very large teams and agencies dedicated to cyber-related activities
- Many nations, like the US, China, Russia, UK, etc. have tens of thousands of people and billions of dollars dedicated to cyber defenses and attacks
  - In the US: NSA, militaries, CIA, FBI, and 20x more contractors in support of the same
- Many nations likely have dozens to potentially thousands of “zero-day” exploits to use at their disposal
- Today, any nation without offensive cyber capabilities would be at a distinct disadvantage
  - Traditional military war is now known as “kinetic” to differentiate it from cyber activities

# Nation-State Attack History

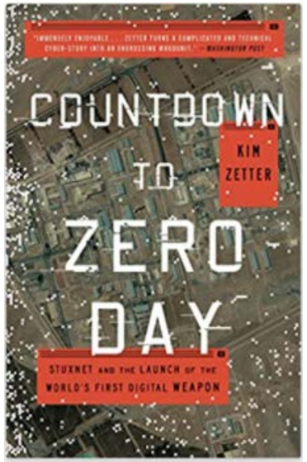
- Been going on as long as computers have been around
- 1989's *Cuckoo's Egg* book– detailed 1986 nation-state attack
  - West German hacker, Markus Hess, stealing info for Russian KGB
  - https://en.wikipedia.org/wiki/The_Cuckoo%27s_Egg_(book)
- 1996 Moonlight Maze
  - Advanced Persistent Threat (APT) attacks
  - Targeted military, contractors, Pentagon, DOE
  - https://en.wikipedia.org/wiki/Moonlight_Maze
- 2003 Titan Rain
  - Targeted defense contractors (e.g. Lockheed Martin, NASA, Sandia National Labs, etc.)
  - https://en.wikipedia.org/wiki/Titan_Rain



# Nation-State Attack History

- 2010 Stuxnet
  - Publicly discovered in 2010, around since 2005
  - Submitted to VirusTotal in 2007, but remained in obscurity until 2010
  - Module malware created to destroy another nation’s nuclear fuel enrichment centrifuges
  - Funded and developed by at least two nation-states and four threat actors
  - Contained at least four 0-days and a bogus Microsoft digital certificate
  - Supposedly did more damage than a nuclear or bunker-busting bomb would have done
  - Related: Duqu, Flame, Gauss
  - Co-opted by regular hackers for their own uses after discovery

  - https://en.wikipedia.org/wiki/Stuxnet
  - Kim Zetter’s Countdown to Zero Day
    - (https://www.amazon.com/Countdown-Zero-Day-Stuxnet-Digital/dp/0770436196)



# Nation-State Attack History

More Recent

- 2012 Saudi Aramco attack
  - Wiped 350K computers
  - https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html
- 2012 Red October
  - Malware program to infect diplomat, scientist, and journalist devices
  - Discovered in 2012, active for 5 years before then
  - https://en.wikipedia.org/wiki/Red_October_(malware)
- 2014 Sony Pictures attack
  - One country did not like what a movie company was producing, so they shut the company down, and released gigabytes of data and embarrassing emails to the world
  - https://en.wikipedia.org/wiki/Sony_Pictures_hack

# Nation-State Attack History

2020

- 2020 Solarwinds attack
  - Supply chain attack, impacted at least 300K companies including many important gov't agencies
  - Hackers modified a "build" process that inserted a remotely-exploitable backdoor hole that was then unknowingly downloaded and used by customers
  - "…the largest and most sophisticated attack the world has ever seen." –MS President Brad Smith
  - https://en.wikipedia.org/wiki/SolarWinds

- The vast, vast majority of nation-state attacks we never hear about

# Attack Summary

## 2021 Microsoft Exchange 0-Day Attacks

- **Publicly announced March 2nd** when Microsoft released 4 emergency patches for Microsoft Exchange 2010, 2013, 2016, and 2019
- First noticed by at least 2 or 3 companies on Jan. 5th and 6th.
  - Later on, first confirmed signs of attack occurred on **Jan. 3rd**
- Some of the involved exploits reported to Microsoft on Jan. 5th
- MS created patches by Feb. 12th for distribution in March
- Impacts hundreds of thousands of organizations worldwide
  - Does not impact Microsoft 365 or Azure Cloud deployments
  - Could impact “hybrid” deployments that still use on-premise Exchange for 2-way password sync and SMTP relay purposes

# Attack Summary

**2021 Microsoft Exchange 0-Day Attacks**

- Involves 4 different actively used MS-Exchange exploits
  - CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065
  - Microsoft also found and patched 3 other related but yet to be exploited holes: CVE-2021-26412, CVE-2021-26854, CVE-2021-27078

- Essentially, if attackers could reach your MS-Exchange servers, they could execute multiple exploits, takeover servers, and use them as a base to take over more of the environment

# Attack Summary

## Exchange Attack Basics – Actively Exploited Vulnerabilities

- **CVE-2021-26855** is a server-side request forgery (SSRF) vulnerability which allows the attackers to get authenticated logon.

- **CVE-2021-26857** is an insecure deserialization vulnerability in the Unified Messaging service. Gives attackers the ability to run code as SYSTEM. This requires administrator permission or another vulnerability to exploit, which is gained by other previously run exploits.

- **CVE-2021-26858** and **CVE-2021-27065** are post-authentication arbitrary file write vulnerabilities.

# Attack Summary

**2021 Microsoft Exchange 0-Day Attacks**

Attackers could:

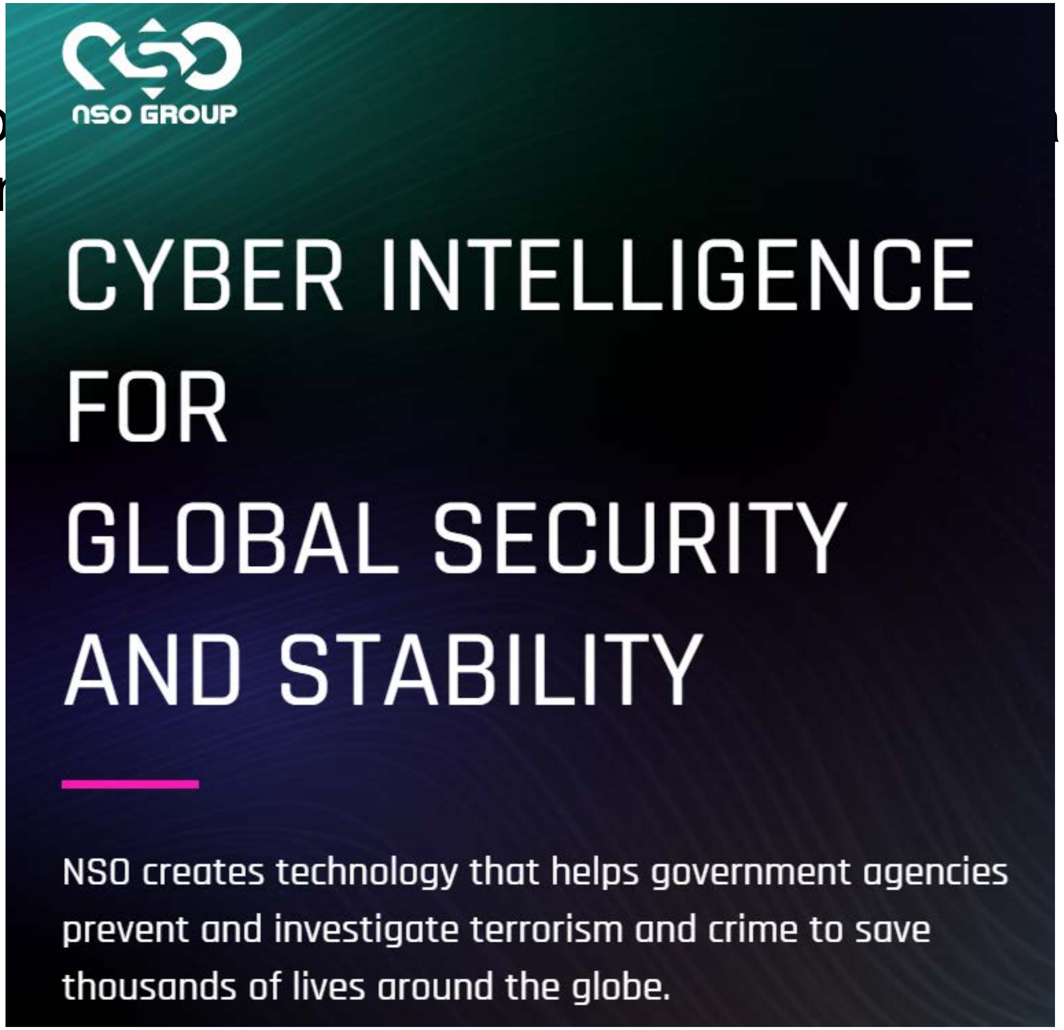
- Completely control exploited boxes
    - Conduct other hacking exploits
- Copy all email
- Dump memory
- Install remotely-accessible web shell(s)
- Execute reverse shells
- Run other exploits
- Access and exploit other reachable computers

# Nation-State Attack History

- Many commercial companies actively advertise their advanced malware and hacking to nations and law enforcement

# Nation-State Attack History

- Many commercial co nced malware and hacking to nations ar
- Like NSO Group



CYBER INTELLIGENCE FOR GLOBAL SECURITY AND STABILITY

NSO creates technology that helps government agencies prevent and investigate terrorism and crime to save thousands of lives around the globe.

# Nation-State Attack History

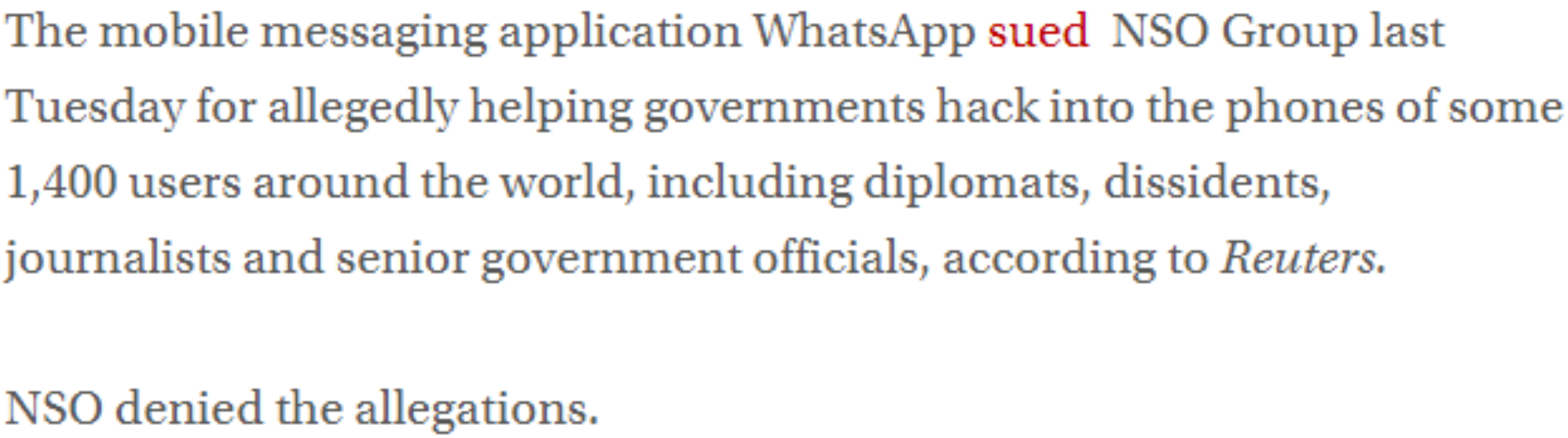
- Citizens and business owners can be targets

<u>Example</u>

- Newspaper runs stories of a murder purportedly aligned to a nation state
- Newspaper owner is sent a text with a picture attached from the leader of that nation
- It contains an exploit that compromises owner’s cell phone
- Confidential and embarrassing owner information and pictures are released to media

# Nation-State Attack History

- Citizens and business owners can be targets



The mobile messaging application WhatsApp sued NSO Group last Tuesday for allegedly helping governments hack into the phones of some 1,400 users around the world, including diplomats, dissidents, journalists and senior government officials, according to *Reuters*.

NSO denied the allegations.

https://www.jns.org/report-israeli-malware-used-to-hack-indian-politicians-phone/

# Nation-State Attack History

<u>Today</u>

- Many groups routinely track malware and activities to various APT threats
  - APT groups known as APT1, Equation Group, Hafnium, Charming Kitten, Larazus, Fancy Bear, etc.
  - The major players know who the major nation-state players are and how they operate

- Who is “good” or “bad” likely depends on who’s country you most support
- There is no digital “Geneva Conventions” covering cyberwarfare, right now
- Many nation-states get away with whatever they can get away with
- Some cyberwarfare attacks have resulted in kinetic responses

# Nation-State Attack History

Summary

- This is to say, nation-state attacks are common and here to stay;
- And have been for decades
- This is the “new” normal if you didn’t already know it existed

- And it’s likely only getting worse
- Why?
- Lots of success and very few to no consequences

# Agenda

- Brief History of Nation-State Attacks
- Why They Are Now Targeting Your Organization
- Mitigating Nation-State Attacks

# What Changed?

## How Are Nation-State Attacks Becoming Worse?

- Who do you think nation-states attack the most?
  - Government and militaries?
  - Infrastructure?
  - Scientist and research facilities?

  Answer:
  - Regular organizations the most, followed by:
  - Software and hardware companies
  - Media, universities, and aid organizations
  - Govt and contractors
  - Citizens related to one of those above
  - Infrastructure (surely to increase in a real cyberwar)

# What Changed?

## How Are Nation-State Attacks Becoming Worse?

- More often attacking non-traditional targets
  - Now can be almost any company
  - If not directly targeted, could be indirectly targeted…might be accidental
  - Might have to compromise everyone to compromise a few

# What Changed?

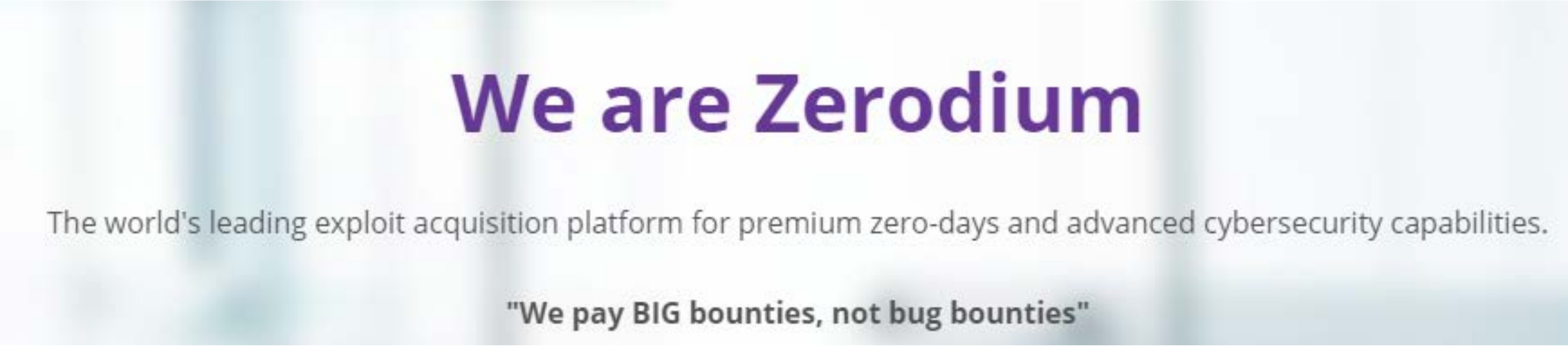
## How Are Nation-State Attacks Becoming Worse?

- Multiple 0-day exploits used more often
- Used to be that 0-days were used sparingly
  - Didn’t want to “burn” them prematurely
  - Didn’t use them if you didn’t need to
  - Didn’t want to bring unneeded attention
  - If you did use them, you used them to break in, insert some other backdoor method, erase evidence of 0-day, and get back out
  - Now they are using them four at a time across thousands of computers and not erasing them

# What Changed?

## How Are Nation-State Attacks Becoming Worse?

- More 0-day exploits being “discovered”, nation-states:
- Find them
- Pay for others to find/create them
- Pay for them at auctions



We are Zerodium

The world's leading exploit acquisition platform for premium zero-days and advanced cybersecurity capabilities.

"We pay BIG bounties, not bug bounties"

# What Changed?

## How Are Nation-State Attacks Becoming Worse?

- More 0-day exploits being “discovered”, nation-states:
- Find them
- Pay for others to find/create them
- Pay for them at auctions
- Secretly insert them into other company’s products
- Pay for them to be intentionally inserted in legitimate company products who are aware that it’s being done
    - If you didn’t know about this you’d probably be shocked at the trusted big names involved

# What Changed?

## How Are Nation-State Attacks Becoming Worse?

More 0-day tools being used

- Most are for eavesdropping/spying
- Second most for exploitation (phones, computers, networks, IoT)
- Remote back doors and control
- Some for devastating damage (wiper, ransomware, Stuxnet, etc.)
- Data exfiltration
- Miscellaneous

# What Changed?

## How Are Nation-State Attacks Becoming Worse?

- Fairly brazen
- Don’t hide that much anymore
- Used to break in, hide, do business, wiped logs, get out
- Now, they just stay
- They don’t care to hide or wipe logs
- When caught, they just stay
- Whatya gonna do about it?

# What Changed?

## How Are Nation-State Attacks Becoming Worse?

- Eavesdropping
- Used to be mostly on government officials or competitive adversaries
- Now often includes journalists, media, CEOs, CISOs
- Opposition figures and aid services
- Often exploit big brand services (e.g. Facebook, Twitter, Whatsapp, etc.) to listen in on their intended targets

# What Changed?

**How Are Nation-State Attacks Becoming Worse?**

- Competitive advantage
- Steal what my competitors are doing and beat them to the punch or offer for cheaper
- Find out what my foreign competitors are doing
- Find out what my foreign competitor’s timelines are
- Find out what my foreign competitor’s loan rates are
- Find out what my foreign competitor’s worries are
- Steal whatever gives a competitive edge

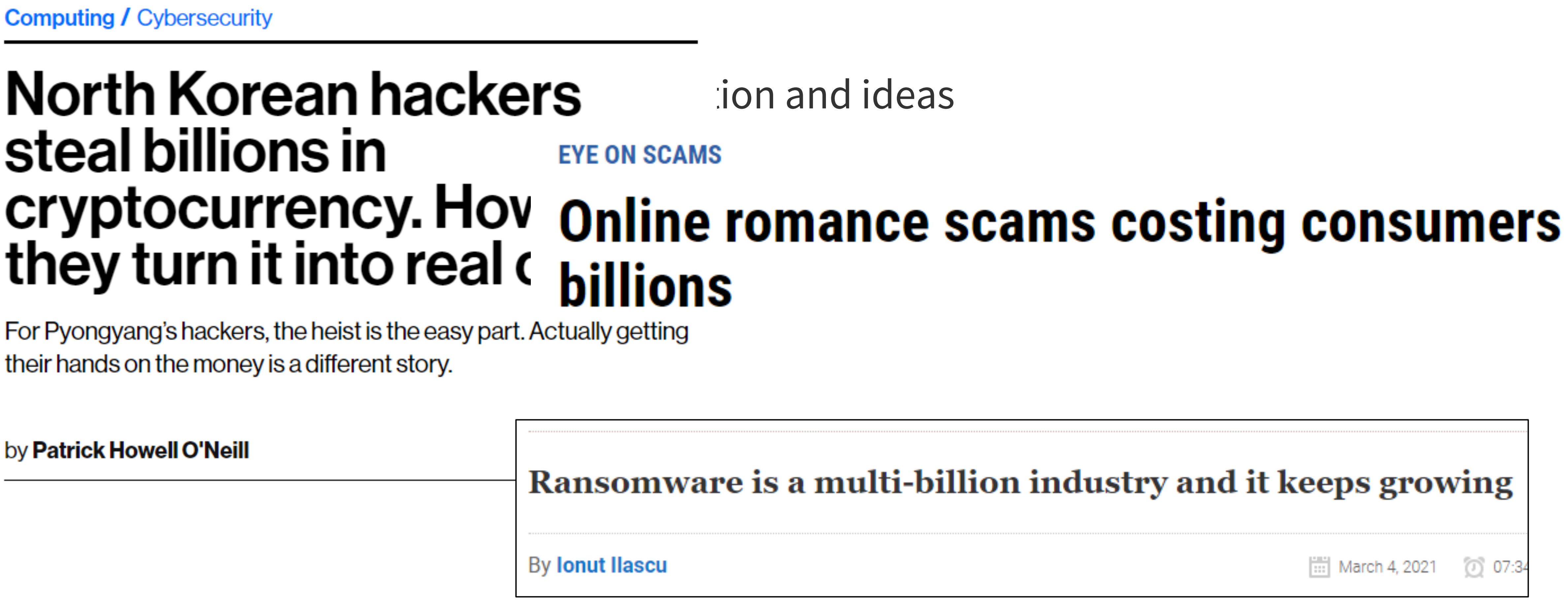
# What Changed?

## How Are Nation-State Attacks Becoming Worse?

- Steal money
- Used to be that they only stole information and ideas
- Now they often steal money and cryptocurrency
- Oftentimes big monetary drivers of their local economy

# What Changed?

## How Are Nation-State Attacks Becoming Worse?



Computing / Cybersecurity

North Korean hackers steal billions in cryptocurrency. Hov they turn it into real c

For Pyongyang's hackers, the heist is the easy part. Actually getting their hands on the money is a different story.

by Patrick Howell O'Neill

ion and ideas

EYE ON SCAMS

Online romance scams costing consumers billions

Ransomware is a multi-billion industry and it keeps growing

By Ionut Ilascu

March 4, 2021 07:34

# What Changed?

## How Are Nation-State Attacks Becoming Worse?

- Disinformation
  - Make your adversary spend time fighting falsehoods
  - Push your agenda
  - Make the press focus on your adversary and not you
  - Confuse the issue
  - Support both sides at once
    - https://www.amazon.com/Manipulated-Inside-Cyberwar-Elections-Distort/dp/1538133504/

Inside the Cyberwar to Hijack Elections and Distort the Truth
MANIPULATED
Theresa Payton

# What Changed?

## How Are Nation-State Attacks Becoming Worse?

- Using Shame and Embarrassment to Achieve their Goals
  - Releasing internal, embarrassing emails and pictures
  - PR Teams to promote break in and publish data
  - Using a counter-offensive strategy as the best defense
  - If your adversary is trying to clean up their mess, they aren’t talking about your mess
  - Trick adversary into publishing bad information, then publicly embarrass

# What Changed?

## How Are Nation-State Attacks Becoming Worse?

- Personal extortion
  - Get you in a compromising situation so you shut-up or do something you would not otherwise do

  - Ex: Nation-state paid trusted journalists for “organic marketing”
  - When revealed, took down dozens of journalists of some of the most trusted magazines and news sites
    - Tried to get me, but I didn’t take the bait

# What Changed?

## How Are Nation-State Attacks Becoming Worse?

- Other Hackers Using Their Tricks
- Stuxnet turned into many other malware programs
- Leaks, intentional and otherwise, turn into vastly more attacks
- APT tools stolen and re-used by other country’s APT programs and regular hackers
    - Ex. EternalBlue (SMB) exploit used by Wannacry ransomware
    - MS-Exchange exploit used by ransomware groups against tens of thousands of unpatched customers

# What Changed?

## How Are Nation-State Attacks Becoming Worse?

### Nation-State Defense vs. Offense Ethical Conflict

- Some nation-state cyber entities are charged with both defense and offense
- Can they really do both best at the same time?
- The NSA is tasked with both offense and defense
- Only 25% of their budget is dedicated to defense
- If they discover a new 0-day, best thing for everyone would be to disclose it to involved vendor and let them patch it ASAP
- They usually don’t do this

# Attack Summary

## Be Prepared

- Nation-State attacks likely to be more prevalent in the future
- Number of attacks increases over time
- All known nation-state cyber budgets are increasing over time

# Agenda

- Brief History of Nation-State Attacks
- Why They Are Now Targeting Your Organization
- Mitigating Nation-State Attacks

# Defenses

**Take It More Seriously**

- If you didn’t before, you must now
- Put nation-state threats in your threat modeling and reports to management
- Prepare like a nation-state could be after you
- Know what is and should be running on your computers
- Know what your legitimate network traffic looks like
- Monitor, monitor, monitor

# Defenses

**Take Social Engineering and Phishing More Seriously**

- Nation-states do sophisticated phishing attacks
- Spear phishing
- Trust third party phishing
- Education: “If email is unexpected and asking you to do something new the sender has never asked you to do before, Stop, Think, Before Doing”
- Is requested action potentially dangerous?
- If so, confirm action request another way

# Defenses

**Argument for the Cloud?**

From a purely patching perspective:

- Software based cloud products seem less risky
- Can be patched, then exploit announced
- On-Premise Exploits – a race against the clock

# Defenses

**Argument for the Cloud?**

- Cloud vendors can more easily notice nation-state attacks
  - Aggregated data and monitoring
  - Have the data of APT attackers and where attacks are coming from
  - Usually stronger and better monitoring
  - Faster and better patching
  - Faster responsiveness to new attacks

# Defenses

## Digital Geneva Conventions Coming?

- United Nations working on globally agreed on cybersecurity and cyberwarfare standards
  - Issued report on March 10, 2021 (5-6 years after starting it)
  - https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf
- Elevates and affirms the authority of international law in cyberspace and the set of norms for responsible behavior
- Sets expectations for responsible nation-state cyber behavior
- Such as don't attack hospitals
- Says to help all nations become cyber-resilient
- French are proposing away forward
  - https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf

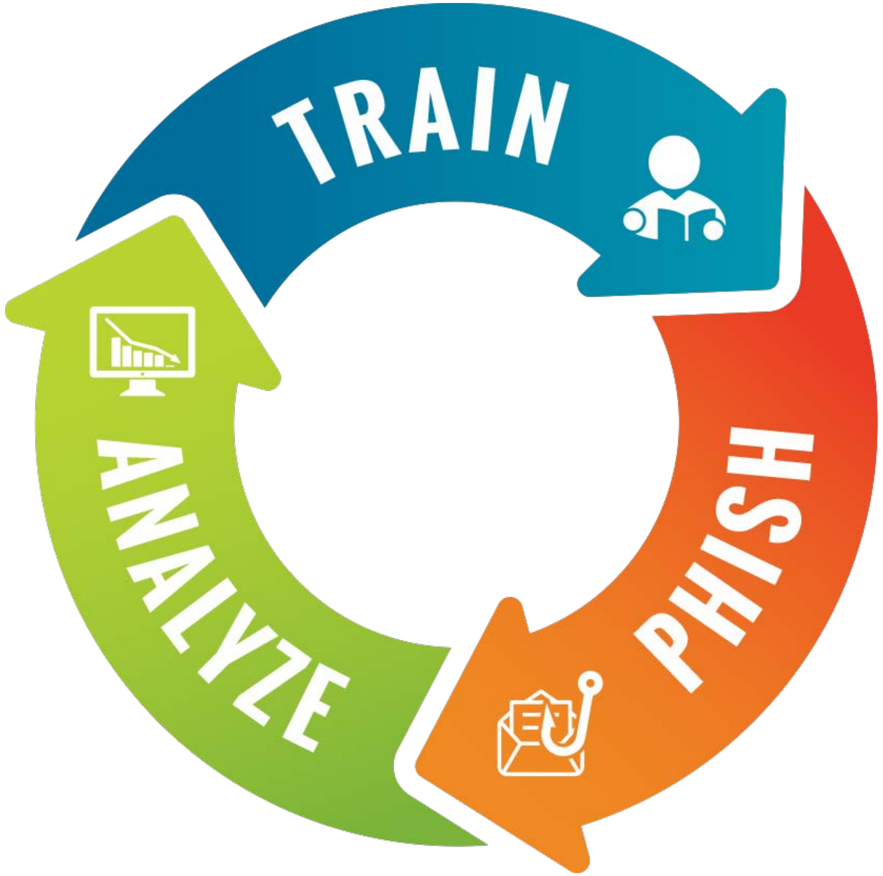
# KnowBe4 Security Awareness Training

**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!

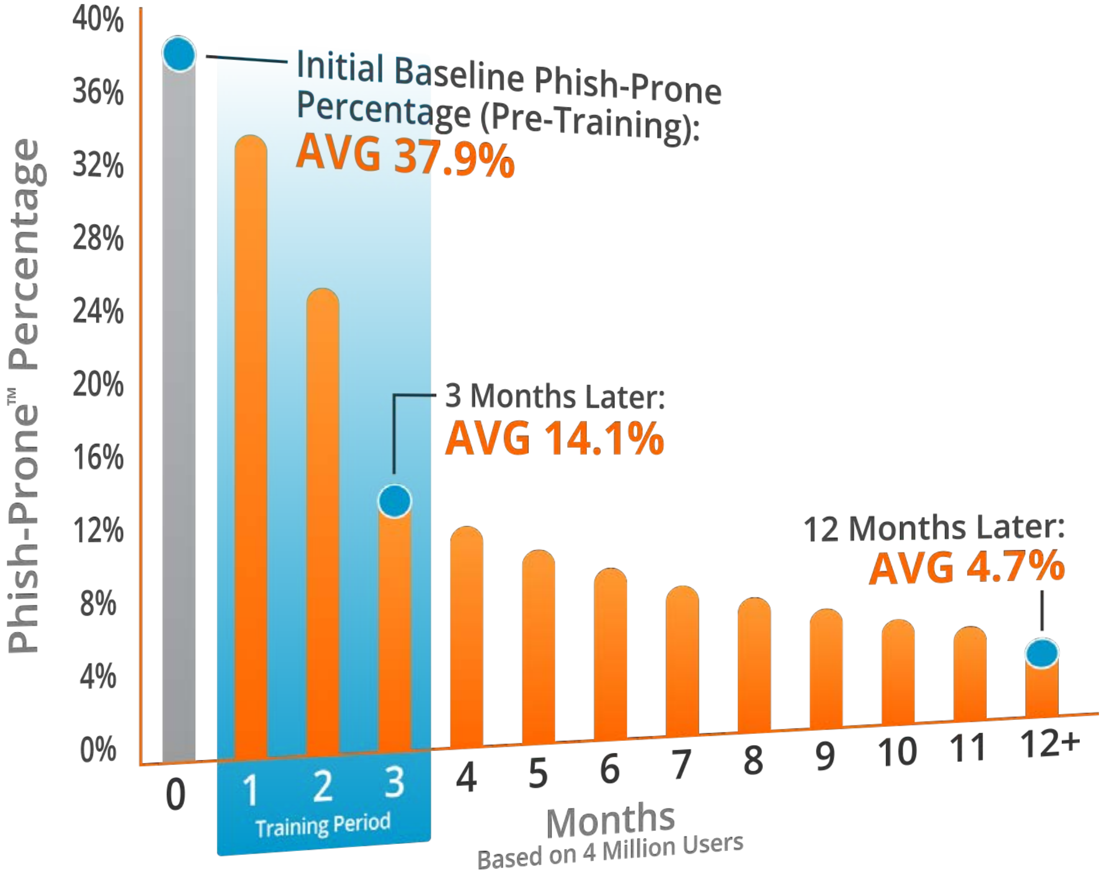


# Generating Industry-Leading Results and ROI

- 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*



*Source: 2020 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 platform prior to the evaluation. Subsequent time periods reflect Phish-Prone percentages for the subset of users who received training with the KnowBe4 platform.*

# Questions?

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

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