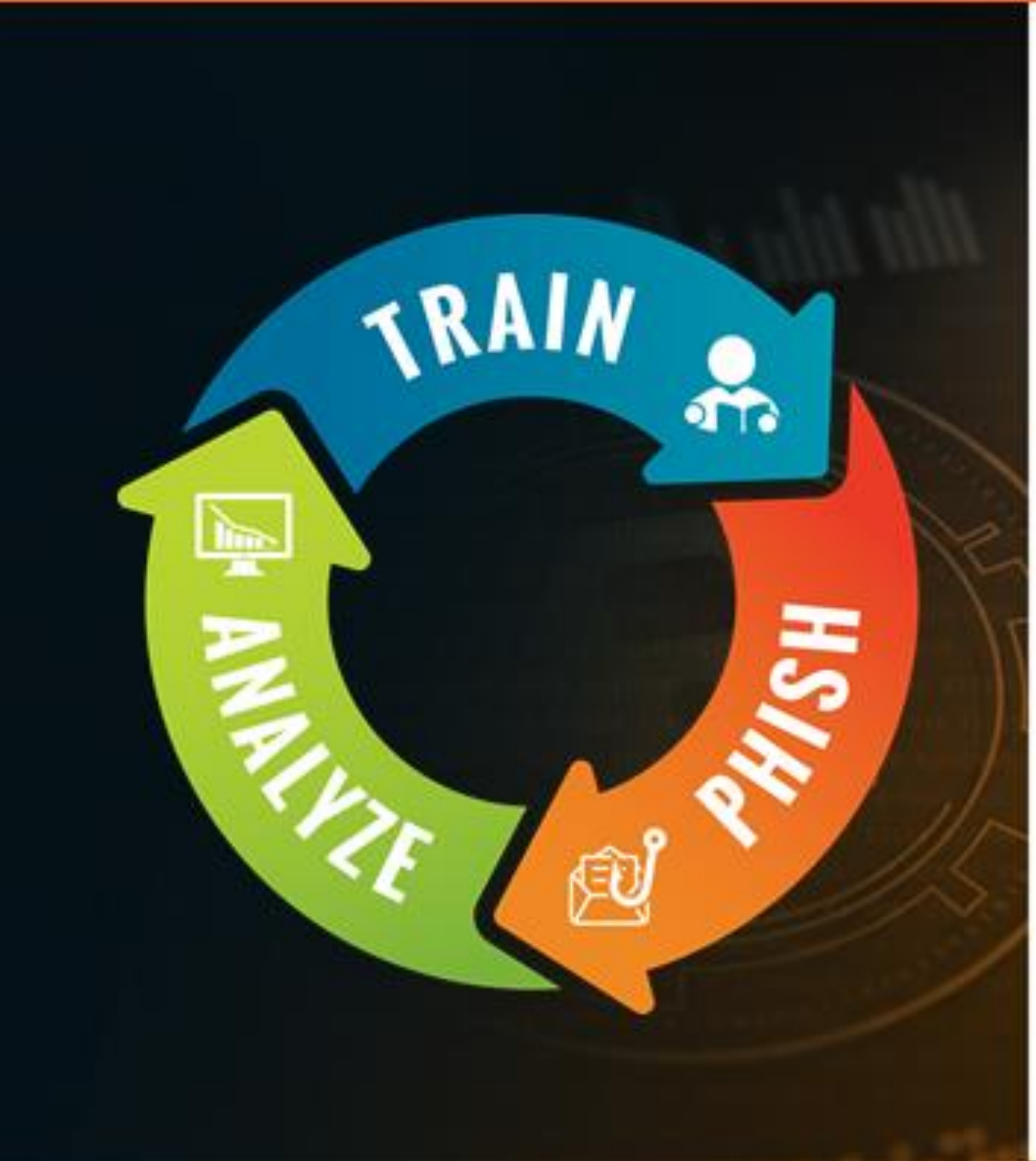
KnowBe4
Human error. Conquered.

The Ransomware Evolution

New Tricks From An Old Trade

Erich Kron
Security Awareness Advocate,
KnowBe4, Inc.



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

Erich Kron

Security Awareness Advocate

About Erich Kron

- CISSP, CISSP-ISSAP, MCITP, ITIL v3, etc…
- Former Security Manager for the US Army 2nd Regional Cyber Center – Western Hemisphere
- Former Director of Member Relations and Services for (ISC)²
- A veteran of IT and Security since the mid 1990's in manufacturing, healthcare and DoD environments

CISSP® | Certified Information Systems Security Professional

CISSP® | Certified Information Systems Security Professional

ISSAP® Architecture

Microsoft® CERTIFIED IT Professional

KnowBe4

Human error. Conquered.

Agenda

- An overview of modern ransomware
- Current attack landscape
- Monetizing the attacks
- Defending ourselves

Agenda

- An overview of modern ransomware
- Current attack landscape
- Monetizing the attacks
- Defending ourselves

2020 Situation Report

KnowBe4
Human error. Conquered.

The First Ransomware

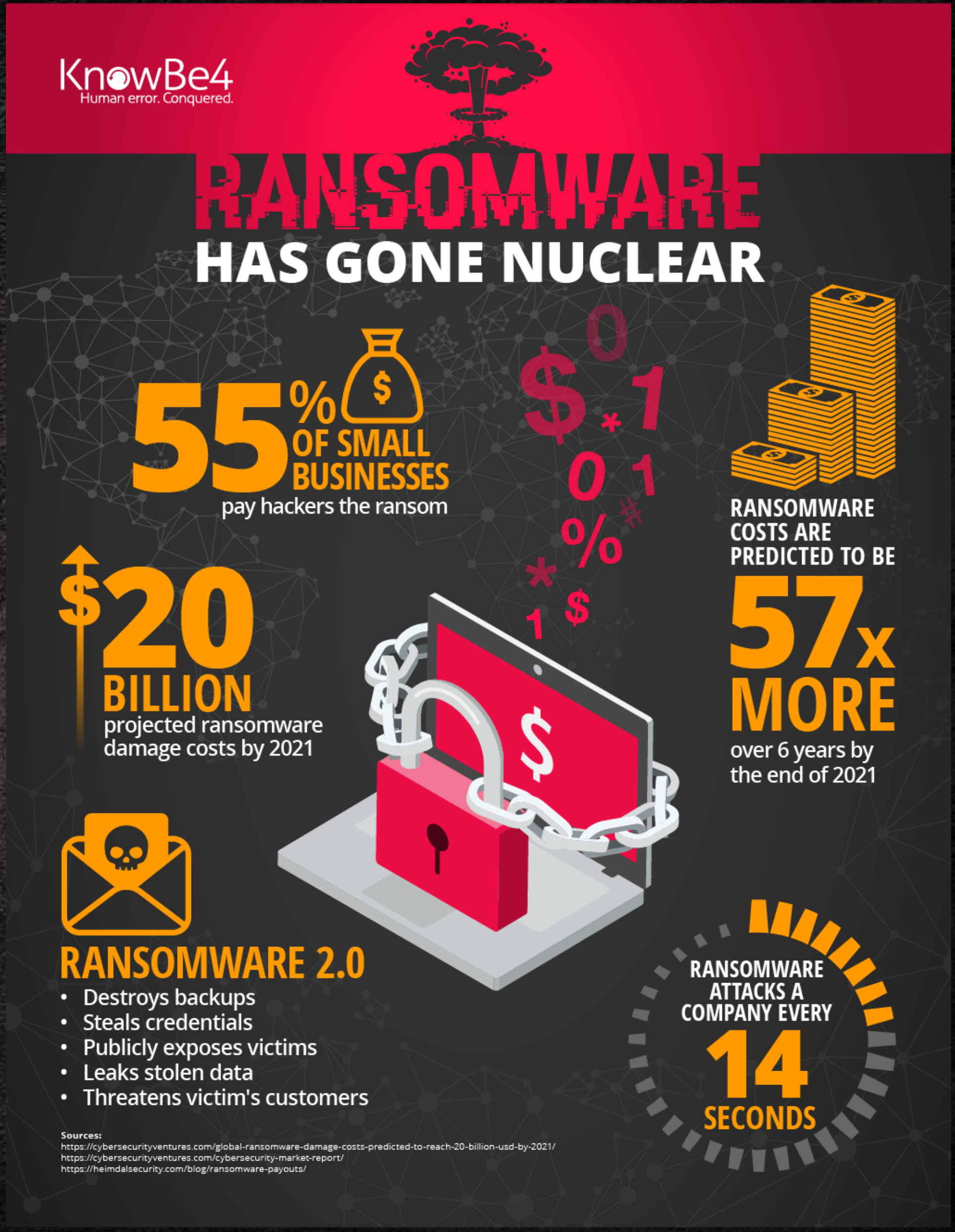
The first ransomware was called AIDS

- It came out in 1989 and was distributed on floppy disk and installed in the DOS AUTEXEC.BAT file
- After 90 reboots, it encrypted the names of the files on the hard disk. The ransom was $189 mailed to a PO Box in Panama
- The author was a doctor and biologist working on AIDS research. When arrested, he said any proceeds were going to help AIDS research

The New Normal in Ransomware

The ransomware game changed in late 2019

- Maze, DoppelPaymer, REvil and others now exfiltrate data and expose it if organizations do not pay the ransom
- This changes how you need to protect yourself against ransomware
- Even if you recover the files, you are looking at a breach due to the exfiltration



KnowBe4
Human error. Conquered.

RANSOMWARE
HAS GONE NUCLEAR

55% OF SMALL BUSINESSES pay hackers the ransom

$20 BILLION projected ransomware damage costs by 2021

RANSOMWARE COSTS ARE PREDICTED TO BE 57x MORE over 6 years by the end of 2021

RANSOMWARE 2.0

- Destroys backups
- Steals credentials
- Publicly exposes victims
- Leaks stolen data
- Threatens victim's customers

RANSOMWARE ATTACKS A COMPANY EVERY 14 SECONDS

Sources:
https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
https://cybersecurityventures.com/cybersecurity-market-report/
https://heimdalsecurity.com/blog/ransomware-payouts/

Agenda

- An overview of modern ransomware
- Current attack landscape
- Monetizing the attacks
- Defending ourselves

Spreading Ransomware

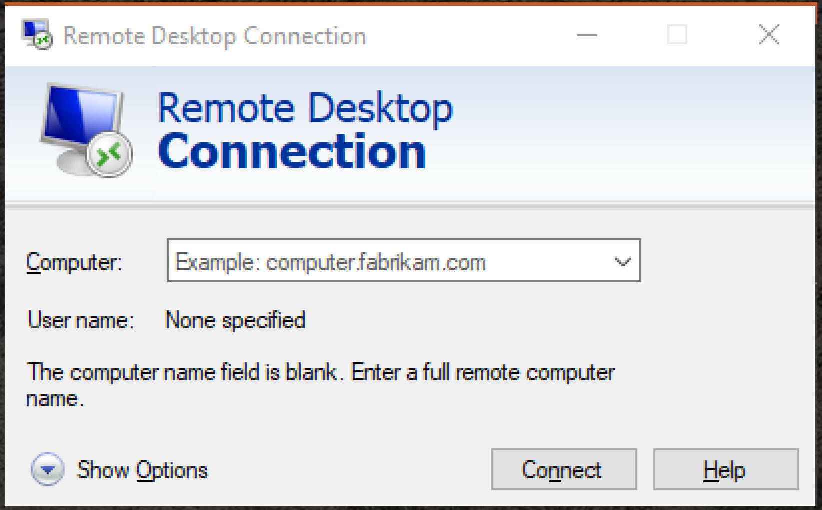
Attackers are not slowing down during this time

- The top two methods of spreading ransomware has consistently been phishing emails and Remote Desktop Protocol (RDP) being available from the internet
- RDP usage has spiked since the COVID-19 pandemic as has phishing attacks

RDP Usage Has Increased

Remote Desktop Protocol (RDP)

- RDP is used to remote access machines at home or in the office.
- Attackers can quickly search for these connections using websites such as Shodan.io or they can scan for them using their own tools



Computer: Example: computer.fabrikam.com

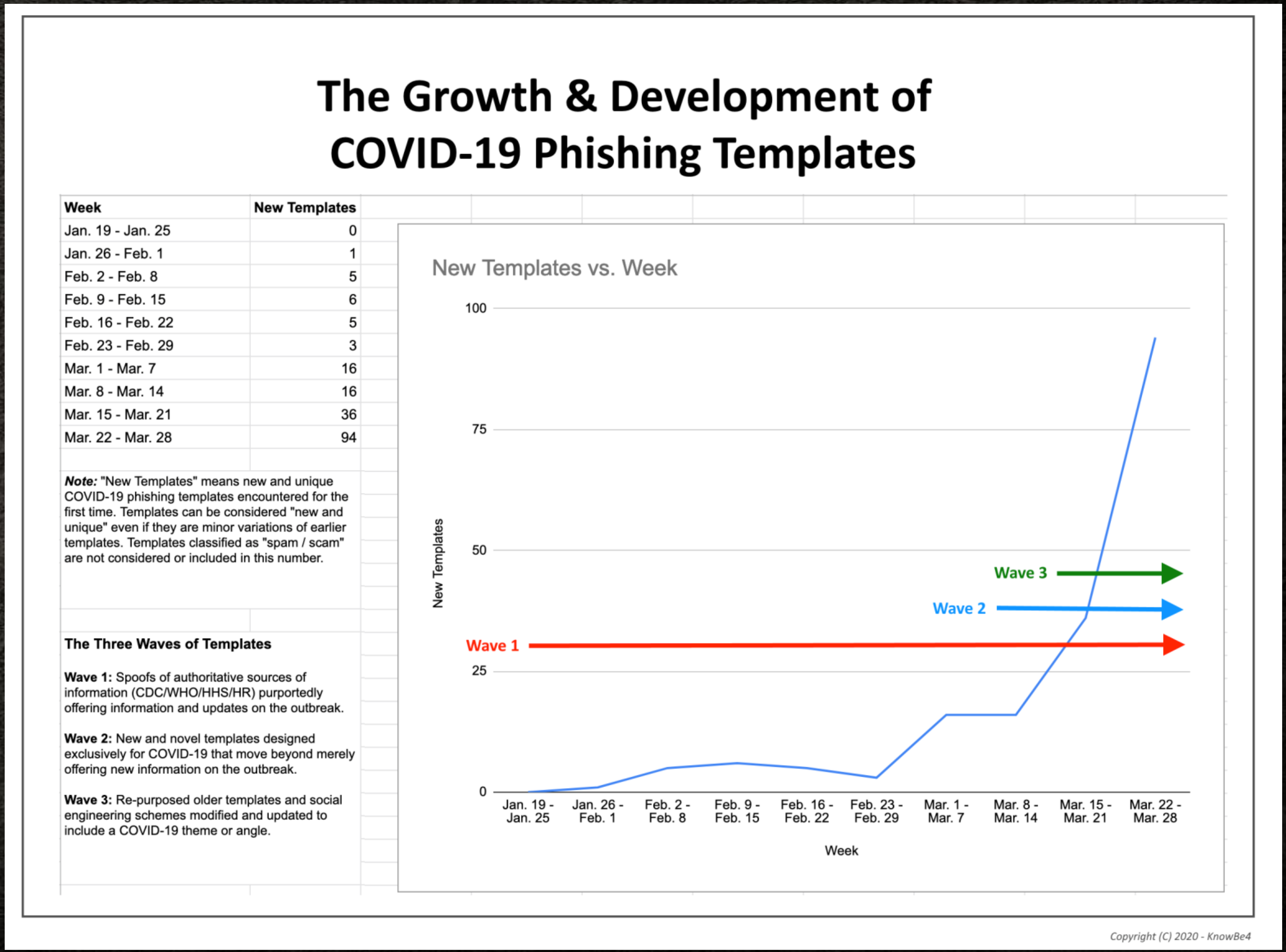
User name: None specified

The computer name field is blank. Enter a full remote computer name.

Overall Phishing Attacks Have Surged

Attacks have really jumped during this time

- Google said it is now blocking 18 Million COVID-19-related emails per day
- We have seen a huge jump in attacks and new phishing templates



The Growth & Development of COVID-19 Phishing Templates

Week	New Templates
Jan. 19 - Jan. 25	0
Jan. 26 - Feb. 1	1
Feb. 2 - Feb. 8	5
Feb. 9 - Feb. 15	6
Feb. 16 - Feb. 22	5
Feb. 23 - Feb. 29	3
Mar. 1 - Mar. 7	16
Mar. 8 - Mar. 14	16
Mar. 15 - Mar. 21	36
Mar. 22 - Mar. 28	94

Note: "New Templates" means new and unique COVID-19 phishing templates encountered for the first time. Templates can be considered "new and unique" even if they are minor variations of earlier templates. Templates classified as "spam / scam" are not considered or included in this number.

The Three Waves of Templates

Wave 1: Spoofs of authoritative sources of information (CDC/WHO/HHS/HR) purportedly offering information and updates on the outbreak.

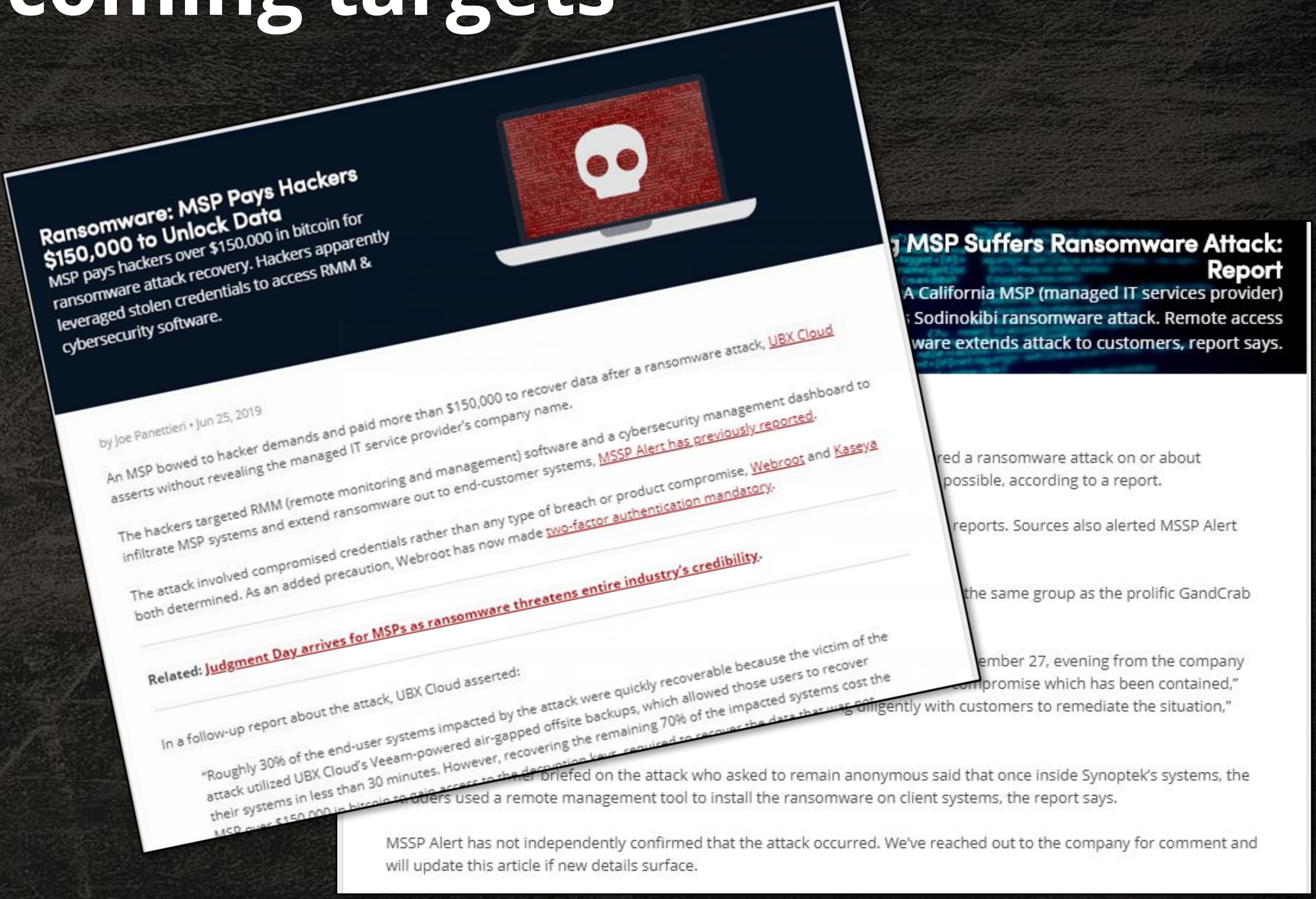
Wave 2: New and novel templates designed exclusively for COVID-19 that move beyond merely offering new information on the outbreak.

Wave 3: Re-purposed older templates and social engineering schemes modified and updated to include a COVID-19 theme or angle.

New Templates vs. Week

MSP/MSSP’s are becoming targets

- MSP/MSSP’s are being targeted heavily as they have access to your systems and data.
- Work with them to ensure you are subscribed to services that help keep your backups offline and in a safe place and that security is a top priority



Ransomware: MSP Pays Hackers $150,000 to Unlock Data

MSP pays hackers over $150,000 in bitcoin for ransomware attack recovery. Hackers apparently leveraged stolen credentials to access RMM & cybersecurity software.

by Joe Panettieri • Jun 25, 2019

An MSP bowed to hacker demands and paid more than $150,000 to recover data after a ransomware attack, UBX Cloud asserts without revealing the managed IT service provider’s company name.

The hackers targeted RMM (remote monitoring and management) software and a cybersecurity management dashboard to infiltrate MSP systems and extend ransomware out to end-customer systems, MSSP Alert has previously reported.

The attack involved compromised credentials rather than any type of breach or product compromise, Webroot and Kaseya both determined. As an added precaution, Webroot has now made two-factor authentication mandatory.

Related: Judgment Day arrives for MSPs as ransomware threatens entire industry’s credibility.

In a follow-up report about the attack, UBX Cloud asserted:

“Roughly 30% of the end-user systems impacted by the attack were quickly recoverable because the victim of the attack utilized UBX Cloud’s Veeam-powered air-gapped offsite backups, which allowed those users to recover their systems in less than 30 minutes. However, recovering the remaining 70% of the impacted systems cost the MSP over $150,000 in bitcoin to gain access to the decryption keys, required to recover the data that was not

MSP Suffers Ransomware Attack: Report

A California MSP (managed IT services provider)

Sodinokibi ransomware attack. Remote access

ware extends attack to customers, report says.

red a ransomware attack on or about

possible, according to a report.

reports. Sources also alerted MSSP Alert

the same group as the prolific GandCrab

ember 27, evening from the company

compromise which has been contained,”

diligently with customers to remediate the situation,”

briefed on the attack who asked to remain anonymous said that once inside Synoptek’s systems, the

ders used a remote management tool to install the ransomware on client systems, the report says.

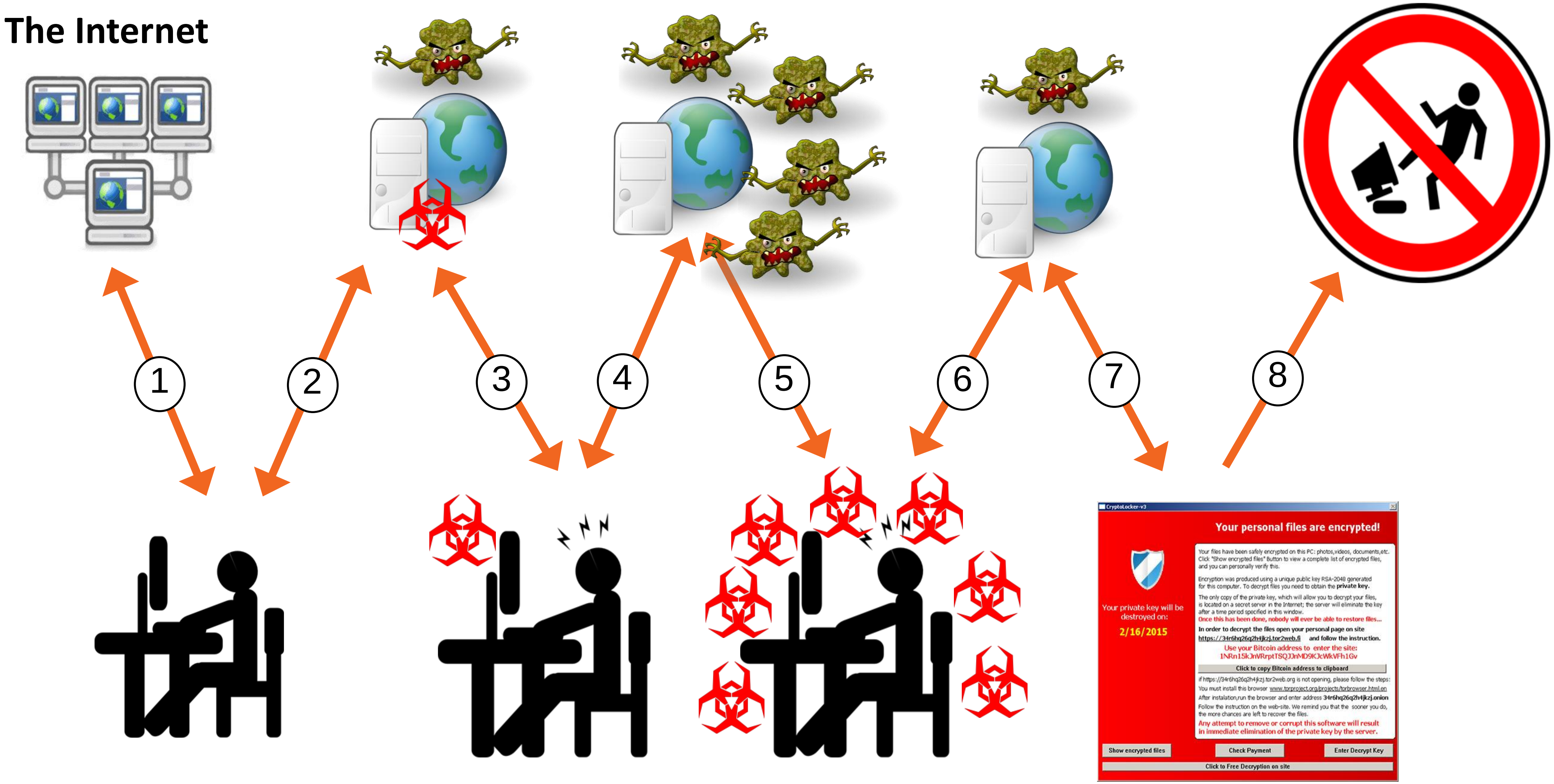
MSSP Alert has not independently confirmed that the attack occurred. We’ve reached out to the company for comment and will update this article if new details surface.

Source: Msspalert.com

The Anatomy of a Ransomware Attack

-- sort of --

The Ransomware Process



Your personal files are encrypted!

Your private key will be destroyed on:

2/16/2015

Your files have been safely encrypted on this PC: photos,videos, documents,etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.
Once this has been done, nobody will ever be able to restore files...

In order to decrypt the files open your personal page on site
https://34r6hq26q2h4jkzj.tor2web.fi and follow the instruction.

Use your Bitcoin address to enter the site:
1NRn15kJnVRrptTSQJJnMD9KJcWkVFh1Gv

Click to copy Bitcoin address to clipboard

if https://34r6hq26q2h4jkzj.tor2web.org is not opening, please follow the steps:
You must install this browser www.torproject.org/projects/torbrowser.html.en
After instalation,run the browser and enter address **34r6hq26q2h4jkzj.onion**
Follow the instruction on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.

Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

Ransomware is Not Taking a Break For COVID-19

Attackers are not slowing down during this time

- Foxconn electronics, Mexico hit with DoppelPaymer ($34mil demand)
- Visser Precision, a defense contractor, hit with DoppelPaymer
- Spanish Hospital hit by Netwalker Ransomware
- U.S. pharmaceutical giant ExecuPharm hit and data published

Ransomware is Not Taking a Break For COVID-19

CryCryptor

- Posed as a Canadian COVID-19 tracing app. It was distributed through two fake websites under the guise of an official COVID-19 tracing app from Health Canada
- Targeted Android devices and encrypted document files plus photos and videos such as .avi, .png and .jpg files
- ESET was able to reverse engineer it and provide a free decryption tool

Ransomware is Not Taking a Break For COVID-19

Evil Corp/WastedLocker

- WastedLocker strain is the latest from from the Evil Corp/Dridex group
- The gang went quiet for a couple of months, then resurfaced with this new strain being spread through phishing
- This strain is completely rewritten and does not share code with their previous ransomware strains and does not exfiltrate files
- It targets high-value servers and backup files and demands ransoms in the millions of dollars

Ransomware is Not Taking a Break For COVID-19

DraftKings/SBTech

- DraftKings merged with SBTech in April, however in the SEC filings it was noted that SBTech was hit with ransomware in late March

- The SBTech online sports and betting platform were down for over a week, taking down customers that used their platform

- The meant a renegotiation of the merger and the creation of a $30 million emergency fund to cover any future costs and litigation fees from the attack

Ransomware is Not Taking a Break For COVID-19

The Red Cross and CyberPeace Institute

- The International Committee of the Red Cross and the CyberPeace Institute issued a joint statement pleading with ransomware attackers to stop attacking organizations and for governments to go after attackers

- Some ransomware gangs said they would stop attacking medical facilities during the pandemic, however other cybercriminals just stepped in and picked up the slack

Ransomware is Not Taking a Break For COVID-19

Grubman, Shire, Meiselas and Sacks

- REvil ransomware exfiltrated data and encrypted files.
- The exfiltrated data, over 750GB worth, is the real threat here as they threaten to release it publicly. They even threaten to have information on President Trump
- Ransom demand is a whopping $42million

Agenda

- An overview of modern ransomware
- Current attack landscape
- Monetizing the attacks
- Defending ourselves

$133K

The Costs of Breaches and Ransomware Attacks

- The **average cost** of a ransomware attack on businesses was **$133,000**

- **75%** of companies infected with ransomware were running **up-to-date** endpoint protection

- **34%** of businesses hit with malware took a **week or more** to regain access to their data.

KnowBe4
Human error. Conquered.

Ransoms are on the rise

- According to Group-IB, from 2018 to 2019, the average ransom demand rose from $6,000 to $84,000 and the attacks rose 40%

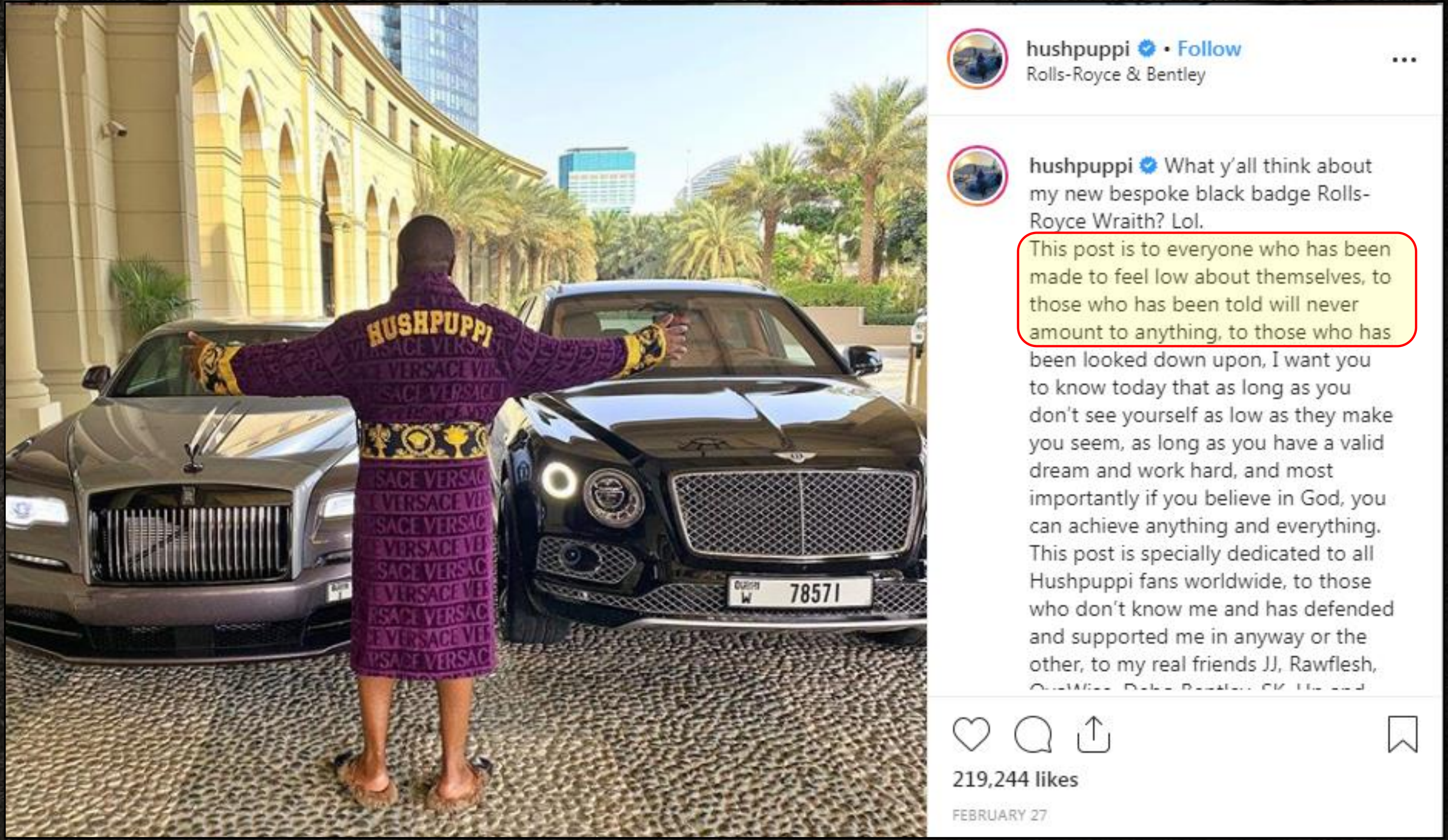
- According to Coveware, the average ransom for the first quarter of 2020 was $111,605

Paying the ransom does not end the ordeal

According to Sophos, the total cost of the average ransomware attack more than doubles if the victim decides to pay the ransom

Why Are They So Hard To Stop?

- These groups are often from outside of areas we can extradite from and they recruit others to do the work
- Many of the money mules think they are doing legit work



hushpuppi • Follow
Rolls-Royce & Bentley

hushpuppi What y'all think about my new bespoke black badge Rolls-Royce Wraith? Lol. This post is to everyone who has been made to feel low about themselves, to those who has been told will never amount to anything, to those who has been looked down upon, I want you to know today that as long as you don't see yourself as low as they make you seem, as long as you have a valid dream and work hard, and most importantly if you believe in God, you can achieve anything and everything. This post is specially dedicated to all Hushpuppi fans worldwide, to those who don't know me and has defended and supported me in anyway or the other, to my real friends JJ, Rawflesh,

219,244 likes

FEBRUARY 27

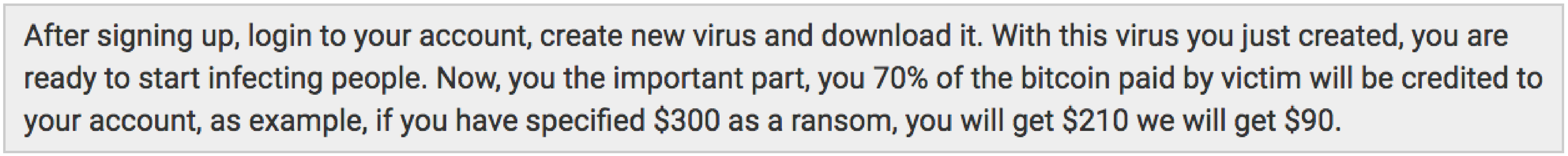
Yeah, Mompha was BEC and finally busted, but many aren't

Ransomware as a Service (RaaS)

Ransomware as a Service

- This is designed to let people that are not technical set up attacks

- Different ways of doing this, for example, Philadelphia is $400, Dot is free with a 50/50 split of profits, Saturn and Cerber RaaS models are free with a 70/30 affiliate/malware developer split



After signing up, login to your account, create new virus and download it. With this virus you just created, you are ready to start infecting people. Now, you the important part, you 70% of the bitcoin paid by victim will be credited to your account, as example, if you have specified $300 as a ransom, you will get $210 we will get $90.

Image Credit : bleepingcomputer.com

Agenda

- An overview of modern ransomware
- Current attack landscape
- Defending ourselves

Do we settle in for the show?

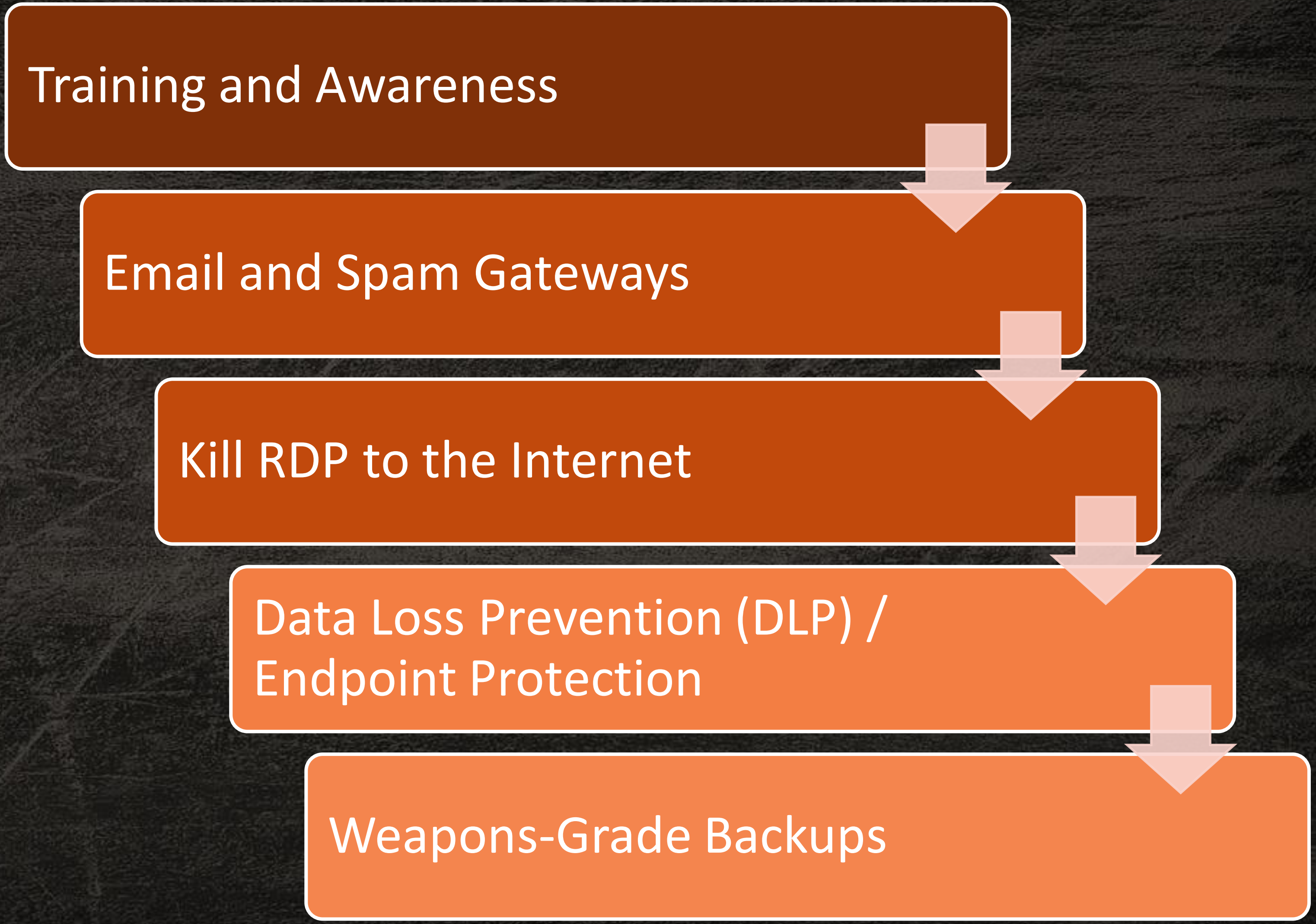
If You Are Not Preparing For a Ransomware Attack, You Are Heading Down A Very Ugly Road, Fast

A Layered Defense

- We know there is no silver bullet to combat any kind of insider threat, it takes layers

- DLP is no longer optional

- Training’s impact is often underestimated, and the method misunderstood



Training and Awareness

Email and Spam Gateways

Kill RDP to the Internet

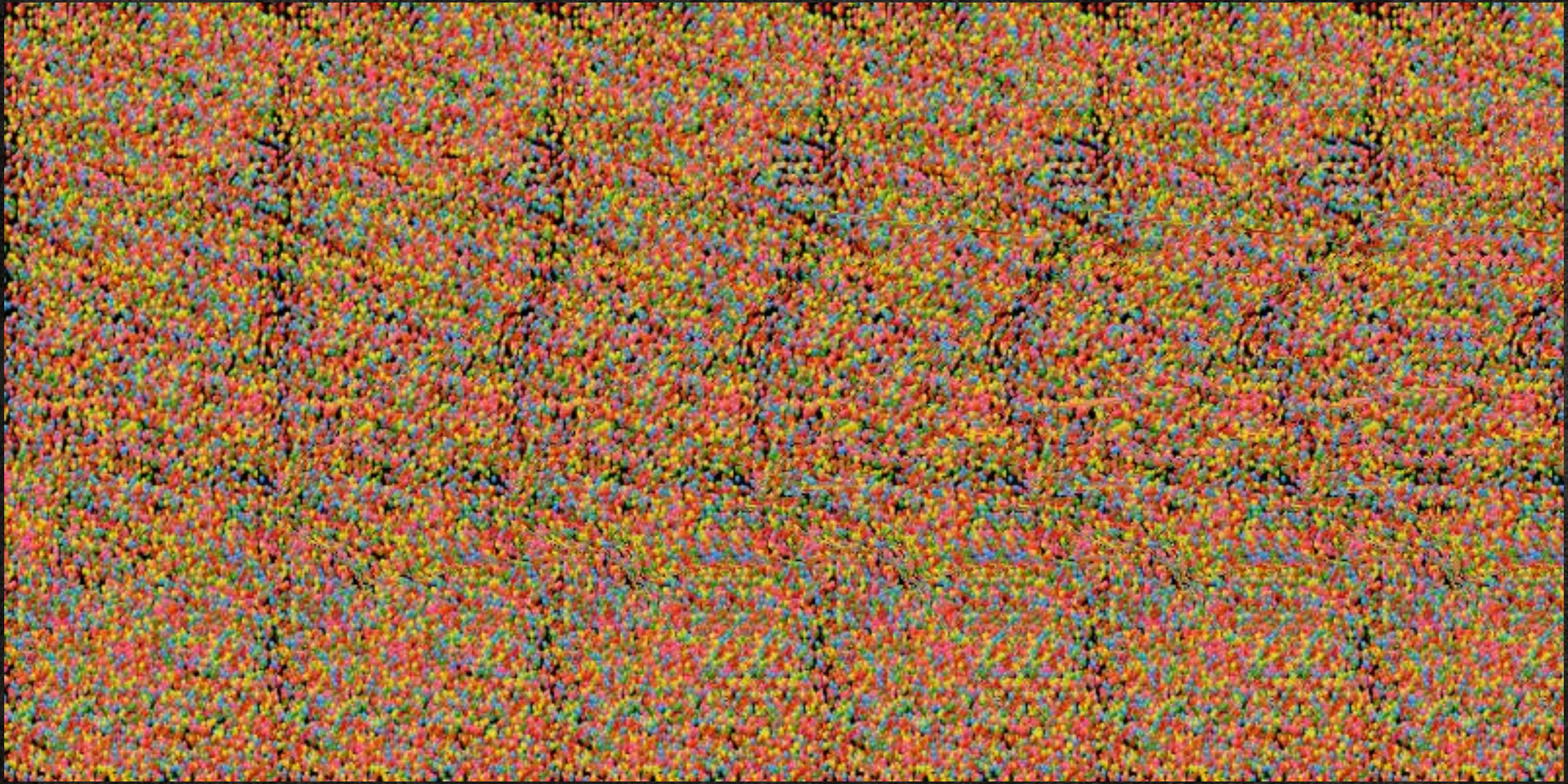
Data Loss Prevention (DLP) / Endpoint Protection

Weapons-Grade Backups

Understanding the root of deception

Our brains’ job to filter, interpret, and present ‘reality’

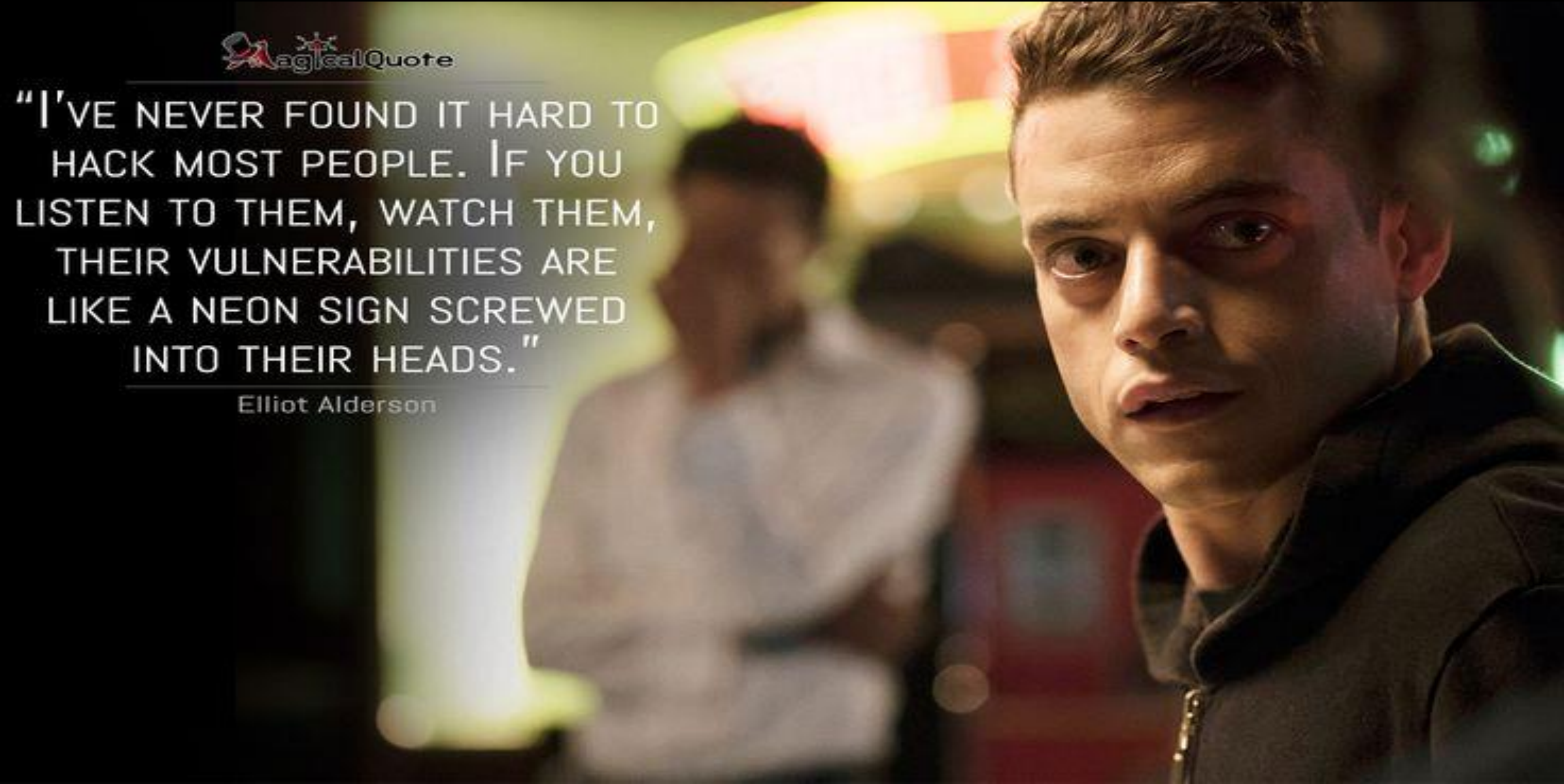
Autostereograms Create the Illusion of 3 Dimensions



There is a shark in ⬅ there (allegedly)

Phot Attribution: By No machine-readable author provided. Fred Hsu assumed (based on copyright claims). - No machine-readable source provided. Own work assumed (based on copyright claims)., CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=75986

All Humans Are Vulnerable



"I'VE NEVER FOUND IT HARD TO HACK MOST PEOPLE. IF YOU LISTEN TO THEM, WATCH THEM, THEIR VULNERABILITIES ARE LIKE A NEON SIGN SCREWED INTO THEIR HEADS."

Elliot Alderson

Social Engineering

Are You Being Manipulated?

-- understand the lures --

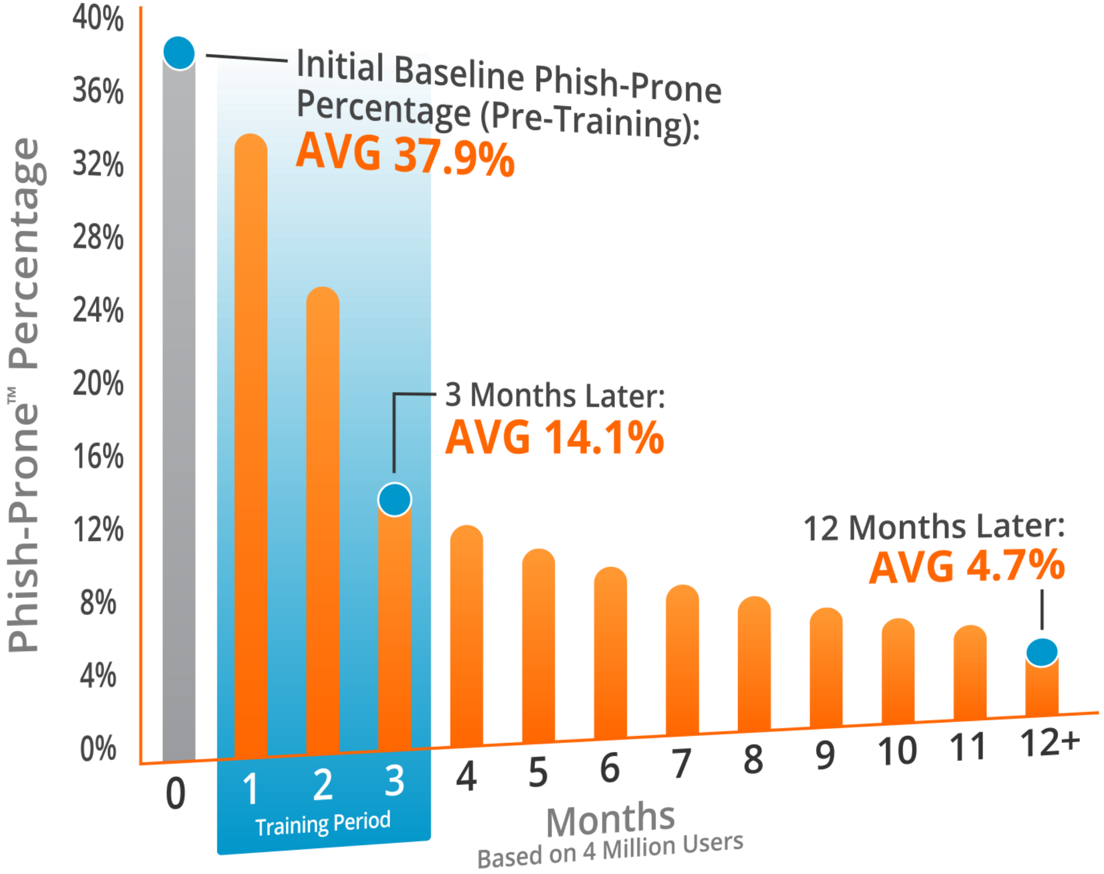
Greed	Curiosity	Self Interest
Urgency	Fear	Helpfulness

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

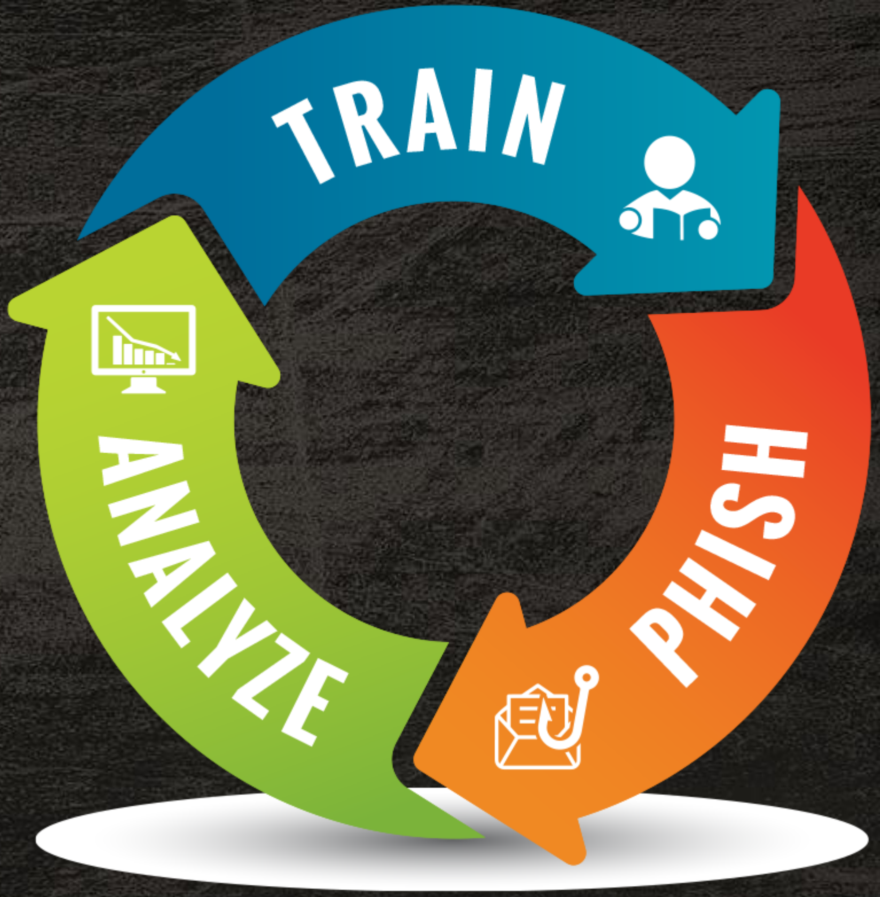
It Takes a Little Planning, But Works

Baseline Testing
We provide baseline testing to assess the Phish-prone™ percentage of your users through a free simulated phishing attack.

Train Your Users
On-demand, interactive, engaging training with common traps, live Kevin Mitnick demos and new scenario-based Danger Zone exercises and educate with ongoing security hints and tips emails.

Phish Your Users
Fully automated simulated phishing attacks, hundreds 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!

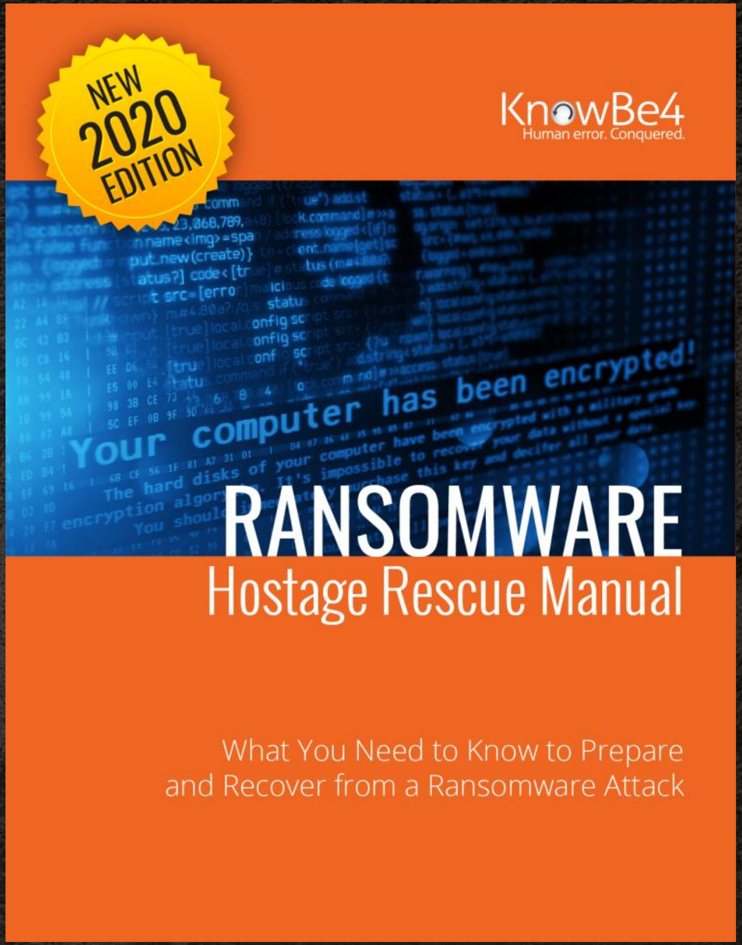


The Ransomware Hostage Rescue Manual

This is a great, free document to help prepare for and recover from ransomware attacks.

Get your free copy of the Ransomware Manual at

https://www.knowbe4.com/ransomware



NEW 2020 EDITION

KnowBe4
Human error. Conquered.

Your computer has been encrypted!

RANSOMWARE
Hostage Rescue Manual

What You Need to Know to Prepare
and Recover from a Ransomware Attack

Thank You!

Erich Kron – Security Awareness Advocate

ErichK@KnowBe4.com | @ErichKron

KnowBe4

Human error. Conquered.

Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com