



Incident Response Management

Friday, October 28, 2022
11:30AM - 1:00PM

Welcome to BooMUG

CYBERSECURITY NIGHTMARE SCENARIOS

(WITH MORE MEMES!)

FRIDAY, OCTOBER 28, 2022

AGENDA

- CYBERSECURITY SCENARIOS WITH A GROUP DISCUSSION
 - THREE SCENARIOS
 - TWO WILL FOLLOW A SPECIFIC TIMELINE
 - DISCUSSION QUESTIONS TO COVER PREPAREDNESS & RESPONSE

That Ransomware Note Be Like



I WANT TO PLAY A GAME

The Boss's Password List
Taped to the Keyboard -
Colorized 2022

All work and no play makes Jack a dull boy

All work and no play makes Jack a dull boy

All work and no play mmakes Jack a dull boy

v All work and no Play ma es Jack a dull boy

All work and no play makes Jack a dull boy

All work and no ply m^aKes Jack a dull boy

All work and no pllay makes Jack a dull boy

SCENARIO #1

- DAY 1: A PROMINENT MANUFACTURER RELEASES A NOTICE THAT THEIR PRODUCT HAS A VULNERABILITY THAT ALLOWS AUTHENTICATION BYPASS AND REMOTE CODE EXECUTION.
- DAY 5: CISA ISSUES AN ALERT WARNING OF A NEW PHISHING CAMPAIGN THAT USES A MALICIOUS ATTACHMENT TO INSTALL A ROOTKIT AND ESTABLISH CONTROL OF THE VICTIM PC.
- DAY 11: AN EMPLOYEE RECEIVES AN EMAIL STATING IT HAS INFORMATION ATTACHED FOR THE UPCOMING STUDENT LOAN FORGIVENESS PROGRAM. THE ATTACHMENT IS BLANK.
- DAY 14: YOUR ACCOUNTING DEPARTMENT IS CONTACTED ABOUT BLANK INVOICES BEING SENT OUT. LOGS SHOW THE MESSAGE DID NOT COME FROM YOUR ORGANIZATION.


SCENARIO #1 - QUESTIONS

- THERE WERE TWO CYBERSECURITY ALERTS - WOULD YOU RECEIVE THESE ALERTS?
- DOES YOUR COMPANY PROVIDE BASIC SECURITY AWARENESS TRAINING FOR EMPLOYEES?
- DO YOU REGULARLY PERFORM CYBERSECURITY ASSESSMENTS OR PENETRATION TESTS?
- DO YOU HAVE A PATCH MANAGEMENT SYSTEM IN PLACE?
- DO YOU HAVE A PROCESS FOR EMPLOYEES TO REPORT SUSPECTED PHISHING EMAILS?

THE SPOOOOOOOKY NUMBERS


yahoo!financeSign in

[Finance](#)[Watchlists](#)[My Portfolio](#)[Cryptocurrencies](#)[Yahoo Finance Plus](#)[Screeners](#)[Markets](#)[News](#)[Personal Finance](#)[Videos](#)[Yahoo U](#)[...](#)

S&P 500
3,595.13
+6.29 (+0.18%)

Dow 30
29,392.04
+152.85 (+0.52%)

Nasdaq
10,402.90
-23.29 (-0.22%)

Russell 2000
1,675.37
-17.55 (-1.04%)

Crude Oil
88.16
-1.19 (-1.33%)



CISION

Organizations Take an Average of 60 Days to Patch Critical Risk Vulnerabilities

March 7, 2022 · 3 min read



**Russian State Actors When You Go to
Bed Instead of Patching that Zero Day Exploit**

When you use cut-rate
~~exorcists~~
cyber security professionals



THE SPOOOOOOOKY NUMBERS

1. 82% of Data Breaches Are Tied to “Human Element” Related Security Weaknesses



82% of data breaches analyzed by Verizon are linked to “human element” based security weaknesses.

BUT... THERE IS HOPE

Effectiveness of Security Awareness Training

Our own case studies and Results Snapshots have shown persuasive results:

95%

Over a two-year period, a financial institution recorded a 95% reduction in malware and viruses, and a greater awareness of cybersecurity threats.

90%

A college in the Northeastern US reported a significant reduction in malware and viruses, a 90% reduction in successful phishing attacks, significantly fewer support requests, an increase in the number of users reporting incidents and attacks, and a greater awareness of security issues.

89%

An employee benefits organization realized more than an 89% reduction in phishing susceptibility utilizing our assessment and education modules as core components of their security awareness and training program.

80%

Security awareness training helped city government employees reduce average click rates by 80% in one year and avoid a sophisticated wire transfer fraud attack.

SCENARIO #1 – CONT.

- DAY 47: EMPLOYEES CALL THE HELP DESK COMPLAINING OF SLUGGISH COMPUTERS, MOST USERS ARE INSTRUCTED TO REBOOT.
- DAY 50: NETWORK MONITORING BEGINS TO SHOW CRITICAL SYSTEMS OFFLINE, AND USERS REPORT THEY CANNOT ACCESS NETWORK RESOURCES. INVESTIGATION SHOWS SERVERS HAVE FILES RENAMED WITH AN UNKNOWN EXTENSION. RANSOM NOTES ARE ON COMPUTER DESKTOPS ACROSS THE ORGANIZATION.
- DAY 53: DURING YOUR REMEDIATION EFFORTS, YOUR COMPANY'S CLIENTS BEGIN CONTACTING THEIR REPS REGARDING EMAILS STATING YOU HAVE BEEN HACKED AND ACCOMPANIED BY SCREENSHOTS OF PROPRIETARY DATA.

What's the difference between
The Ring and ransomware?



At least in The Ring you get 7 days to stop it.



Ransomware

Your domain joined backup server

SCENARIO #1 – QUESTIONS

- HOW WOULD THIS BE ASSESSED IN YOUR ORGANIZATION?
- WHAT INTERNAL AND EXTERNAL NOTIFICATIONS DO YOU MAKE? TO WHOM?
- DOES YOUR ORGANIZATION HAVE THE CAPABILITIES TO RESTORE THE CRITICAL DATA?
- WHAT ARE YOUR FIRST ACTIONS UPON DISCOVERING THE ENCRYPTED FILES?
- HOW DO YOU PREVENT DATA EXFILTRATION FROM YOUR NETWORK?
- HOW DO YOU PREVENT MALICIOUS ACTORS FROM ENCRYPTING DATA?

SCENARIO #2

- DAY 1: YOUR ORGANIZATION IS RUNNING A VERSION OF MICROSOFT EXCHANGE THAT HAS BEEN OUT OF SUPPORT FOR ONE YEAR.
- DAY 2: A SALESPERSON'S LAPTOP IS STOLEN FROM A COFFEE SHOP. THE LAPTOP CONTAINED SENSITIVE INFORMATION.
- DAY 6: YOUR ACCOUNTS PAYABLE DEPARTMENT IS ABOUT TO WIRE \$50,000 TO ACME CORP. MOMENTS BEFORE EXECUTING THE TRANSFER, THE AP EMPLOYEE RECEIVES NEW ACCOUNT INFORMATION VIA EMAIL. AP UPDATES AND EXECUTES THE TRANSFER.
- DAY 7: YOU REVIEW FIREWALL LOGS AND SEE LARGE VOLUMES OF TRAFFIC LEAVING THE NETWORK FROM THE COMPANY NETWORK PRINTERS.



Phishing Email

End Users



**Unsuspecting end
user**

**Malicious PDF
email attachment**

SCENARIO #2 – QUESTIONS

- DOES YOUR ORGANIZATION HAVE A PROCESS FOR REPLACING HARDWARE OR SOFTWARE BEFORE IT IS “END OF SUPPORT?”
- DOES YOUR ORGANIZATION EMPLOY ANY METHODS TO PROTECT DATA ON DEVICES THAT ARE LOST OR STOLEN?
- DOES YOUR ORGANIZATION USE MULTI-FACTOR AUTHENTICATION (MFA) FOR ACCESS TO EMAIL AND OTHER SYSTEMS?
- DOES YOUR ORGANIZATION MONITOR NETWORK/INTERNET TRAFFIC FOR SUSPICIOUS ACTIVITY?

THE SPOOOOOOOKY NUMBERS

	Currently in use	Planned for acquisition	No plans
Password management / automated reset	62.1%	28.5%	9.4%
Adaptive/risk-based authentication	61.8%	28.7%	9.5%
Two-/multi-factor (2FA/MFA) authentication	56.8%	31.8%	11.4%
Single sign-on (SSO)	53.6%	33.4%	13.0%
Privileged account/access management (PAM)	52.8%	33.7%	13.5%

Source: ISC2

SCENARIO #2 – CONT.

- DAY 8: YOUR EMPLOYEES NOTICE A COMMONLY USED LINK ON THE COMPANY WEBSITE NOW REDIRECTS TO AN UNRELATED WEBSITE.
- DAY 9: USERS BEGIN TO REPORT ACCESS TO NETWORK RESOURCES HAS DEGRADED. DURING TROUBLESHOOTING, YOU FIND AN UNKNOWN PROCESS IS USING 100% OF THE CPU ON ALL SERVERS. UPON INVESTIGATION, YOU FIND OUT THE PROCESS IS RELATED TO A CRYPTOMINING VIRUS.
- DAY 12: THE SECURITY CONSULTANT WITH YOUR CYBER INSURANCE INFORMS YOU THAT EMPLOYEE HR DATA IS FOR SALE ON THE DARK WEB.



You

The Intern

**Your Cryptojacked Server Mining
Bitcoin Until the CPU Melts**

SCENARIO #2 – QUESTIONS

- DOES YOUR ORGANIZATION PERFORM REGULAR PENETRATION TESTING OF COMPANY WEBSITES?
- DOES YOUR ORGANIZATION HAVE PROCESSES TO MANAGE HOW FINANCIAL TRANSACTIONS ARE EXECUTED?
- WHAT IMPACT WOULD THE SALE OF PERSONALLY IDENTIFIABLE INFORMATION (PII) HAVE ON YOUR BUSINESS?
- ARE YOU FAMILIAR WITH THE TERMS, CONDITIONS, REQUIREMENTS, AND COVERAGE PROVIDED BY YOUR CYBERSECURITY INSURANCE?

SCENARIO #3 - REMEDIATION

- SCENARIO #1 CONTINUED
- YOU HAVE IDENTIFIED THE SERVER THAT WAS THE SOURCE OF ENCRYPTION.
- YOU HAVE DISCONNECTED THE SERVER.
- YOU HAVE DISABLED INTERNET ACCESS.
- LET'S DISCUSS THE NEXT STEPS.

That feeling when we finally validate all the ransomware's gone from a client's network



SCENARIO #3 – REMEDIATION PLAN

- DO YOU HAVE ONE?
- WHAT ARE THE FIRST STEPS?
- IS IT REGULARLY REVIEWED AND UPDATED?

SCENARIO #3 – REMEDIATION PLAN

“NO PLAN SURVIVES CONTACT WITH
THE ENEMY” – HELMUTH VON MOLTKE
THE ELDER

“THE PERFECT PLAN IS LIKE
BIGFOOT, EVERYONE KNOWS WHAT IT LOOKS
LIKE, BUT NO ONE HAS SEEN ONE.” –
TIM LEWIS



SCENARIO #3 – REMEDIATION PLAN CONSIDERATIONS

- WHO NEEDS TO BE CONTACTED?
- WHAT RESOURCES DO YOU HAVE AT YOUR DISPOSAL?
- WHAT ARE THE EXPECTATIONS OF THE BUSINESS?
- WHAT LEGAL REQUIREMENTS DO YOU HAVE?
- WHO IS GOING TO FILL WHAT ROLE(S)?

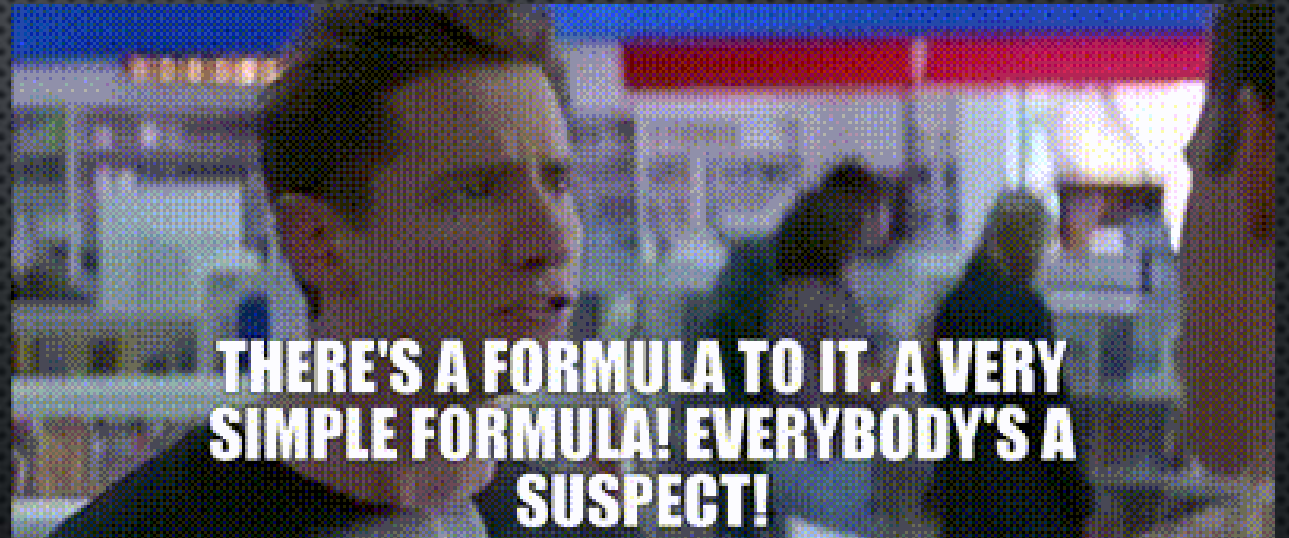
SCENARIO #3 – CLEANUP

- WHERE DO YOU EVEN BEGIN?
- WHEN DO YOU BEGIN?
- HOW DO YOU PREVENT RE-INFECTION?
- WHEN & HOW DO YOU DECIDE WHAT GETS COMPLETELY RE-BUILT?



SCENARIO #3 – CLEAN UP CONSIDERATIONS

- ISOLATE MACHINES UNTIL CONFIRMED CLEAN.
- RESET PASSWORDS PROMPTLY, ESPECIALLY ADMINS.
- BUILD CUSTOM DMZs
- IF IT IS EASIER, RE-IMAGE.
- MONITOR, MONITOR, MONITOR



SCENARIO #3 – LET'S TALK ABOUT YOUR BACKUPS

- DON'T RESTORE FROM A COMPROMISED BACKUP!
- DWELL TIME IS SOMEWHERE BETWEEN 11 & 24 DAYS.
- CONFIRMING AND PROTECTING THE HEALTH OF YOUR BACKUPS IS A TOP PRIORITY.
- KNOW THE TERMS OF ACCESSING OFFSITE BACKUPS BEFORE THEY ARE NEEDED.
- WHATEVER YOUR RPO/RTO IS, IT'S NOT GOING TO BE ENOUGH.



SCENARIO #3 – FINAL THOUGHTS ON REMEDIATION

- THIS IS GOING TO BE A LONG PROCESS.
- THIS IS GOING TO BE AN EXPENSIVE PROCESS.
- THERE ARE NO GUARANTEES THAT IT WILL NOT HAPPEN AGAIN.
- LEARN FROM THE EXPERIENCE.

THANK YOU/QUESTIONS?

- THANK YOU FOR ATTENDING BOOMUG!

TIM LEWIS

TIM.LEWIS@MIRAZON.COM

Boo!

The image features a solid orange background decorated with several stylized orange bat silhouettes in flight. The word "Boo!" is prominently displayed in the center. The letter "B" is a simple, bold black outline. The two "O"s are designed to look like large, staring eyes, each with a thick black outer ring, a white middle ring, and a bright green inner ring surrounding a black pupil. The exclamation mark is a solid black shape.