REVIEWING AND DEFENDING AGAINST THE LATEST **CYBERSECURITY ATTACKS**

SIKICH®

ABOUT SIKICH

1,000+ TOTAL PERSONNEL

90+ PARTNERS

NATIONWIDE PRESENCE
WITH CLIENTS SERVED
IN 50 STATES

35+ YEARS **SERVICING CLIENTS** AS A FIRM

1 **POSITIVE** AND **COLLABORATIVE** CULTURE

AUDIT, ACCOUNTING, TAX & CONSULTING

- Outsourced Accounting
- Tax Compliance & Planning
- International & Expatriate Tax
- Audit & Assurance
- Employee Benefit Plan & Retirement Plan Audits
- Consulting Services

TECHNOLOGY

- ERP & CRM Software & Consulting
- IT Services
- Cloud & Hosting Services
- Technology Consulting & Projects
- Information Security & Compliance
- Cybersecurity

ADVISORY

- General Business Consulting
- Insurance Services
- Investment Banking*
- Workforce Risk Management
- Regulatory, Quality & Compliance
- Human Capital Management & Payroll Consulting
- Retirement Services
- Marketing & Communications
- Supply Chain
- Transaction Advisory Services
- Wealth Management

SIKICH®

SIKICH.COM

CYBERSECURITY

OUR SECURITY SERVICES

We help customers understand security and compliance risks, how to avoid them and what to do should a security incident occur.

- FORENSIC **INVESTIGATIONS**
- VULNERABILITY **SCANNING**
- COMPLIANCE AND RISK **ASSESSMENTS**
- PENETRATION **TESTING**
- IT **AUDITS**
- REMEDIATION
- SECURITY **AWARENESS TRAINING**

SIKICH®

SIKICH.COM

HOW 2022 IS GOING

PROTECTING AGAINST THE NEWEST CYBERSECURITY THREATS

SIKICH®

SIKICH.COM

INDUSTRIAL CONTROLS UNDER ATTACK

- Industrial control system (ICS)
- Supervisory control and data acquisition (SCADA)
- Devices such as: programmable logic controllers and open platform communication servers
- Impacts mostly medium and large size businesses

SIKICH®

MICROSOFT DYNAMICS GP VULNERABILITY

- Multiple vulnerabilities found this year
- Can lead to confidentiality and integrity issues

Microsoft Dynamics GP Spoofing Vulnerability

CVE-2022-23269

On this page

CVSS 5.4

Security Vulnerability

Released: Feb 8, 2022 Last updated: Feb 25, 2022

Microsoft Dynamics GP Elevation Of Privilege Vulnerability

CVE-2022-23271

On this page

CVSS 6.5

Security Vulnerability

Released: Feb 8, 2022

Microsoft Dynamics GP Elevation Of Privilege Vulnerability

CVE-2022-23272

On this page

CVSS 8.1

Security Vulnerability

Released: Feb 8, 2022

Microsoft Dynamics GP Elevation Of Privilege Vulnerability

CVE-2022-23273

On this page

CVSS 7.1

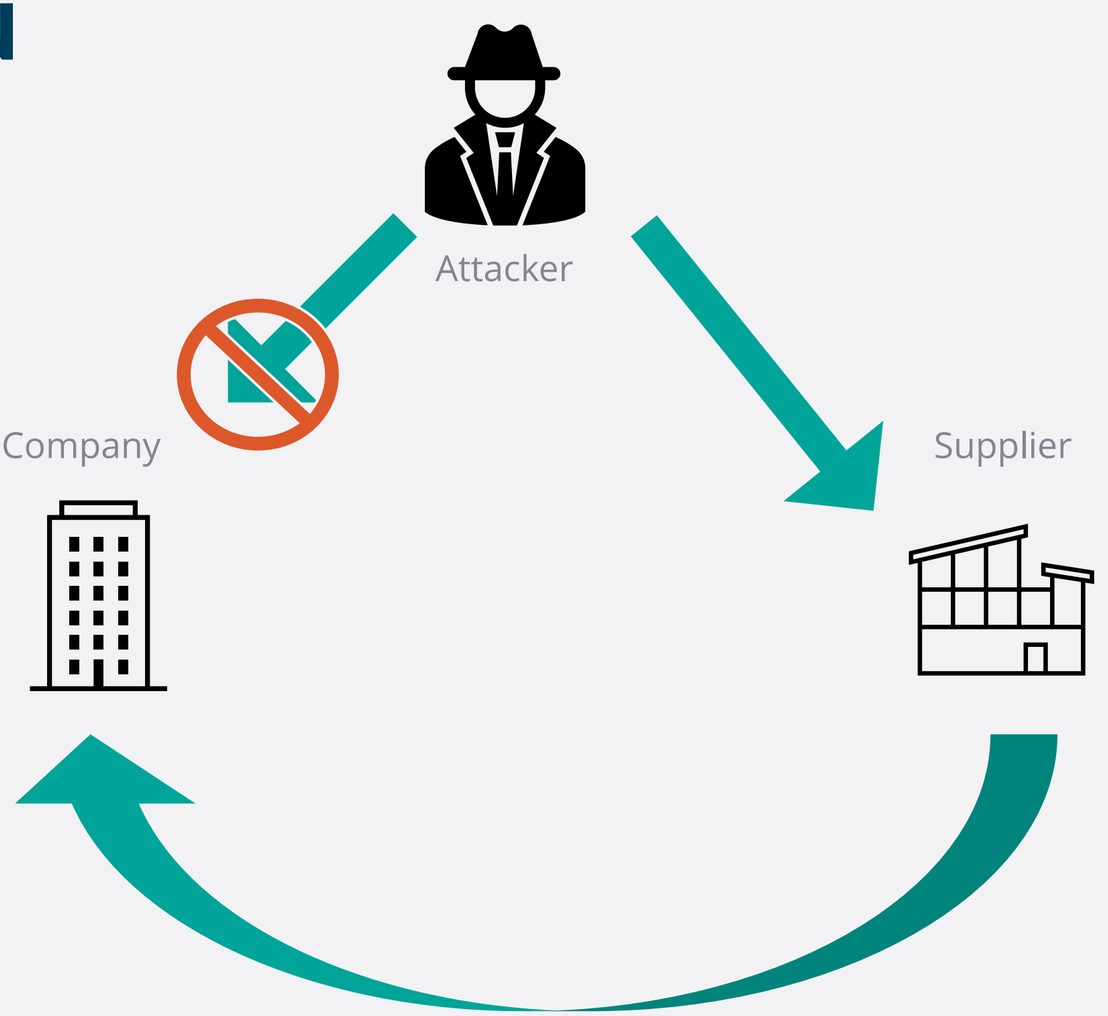
Security Vulnerability

Released: Feb 8, 2022

SIKICH®

SOFTWARE SUPPLY CHAIN ATTACKS

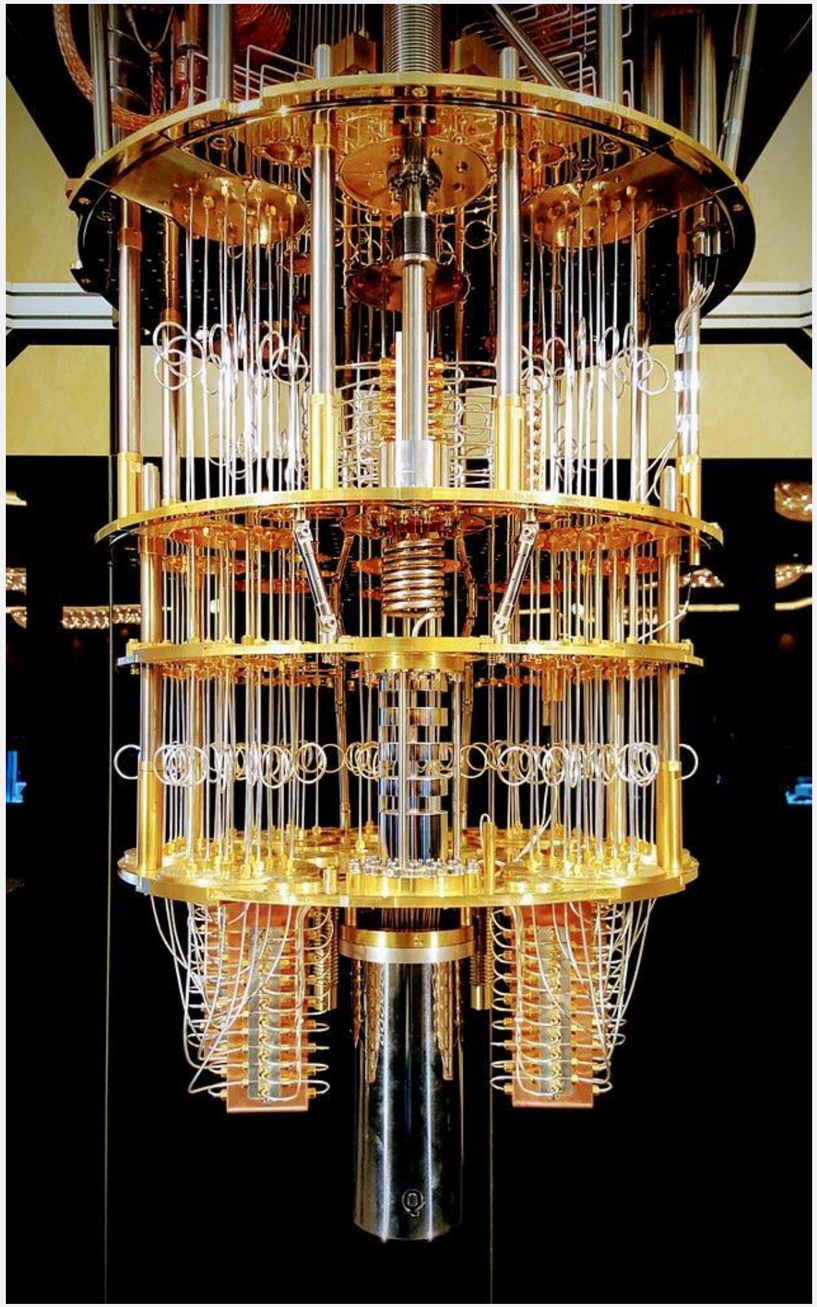
- Goal: gain access to Company
- Attacker finds what software Company uses
- Attacker gains access to Supplier to compromise software
- Compromised software is distributed to Company
- Attacker now has access to Company



SIKICH®

QUANTUM COMPUTING
CYBER ATTACKS

- Can solve problems that are considered “impossible” today
- Threat against public-key encryption
- Researchers are working on “quantum-resistant” cryptography (standard by 2024)



SIKICH®

ADVANCED TACTICS AND TECHNIQUES

PROTECTING AGAINST THE NEWEST CYBERSECURITY THREATS

SIKICH®

SIKICH.COM

POLLING QUESTION:

HAVE YOU EVER USED SITES SUCH AS HTTPS://HAVEIBEENPWNED.COM TO CHECK FOR CREDENTIAL LEAKS?

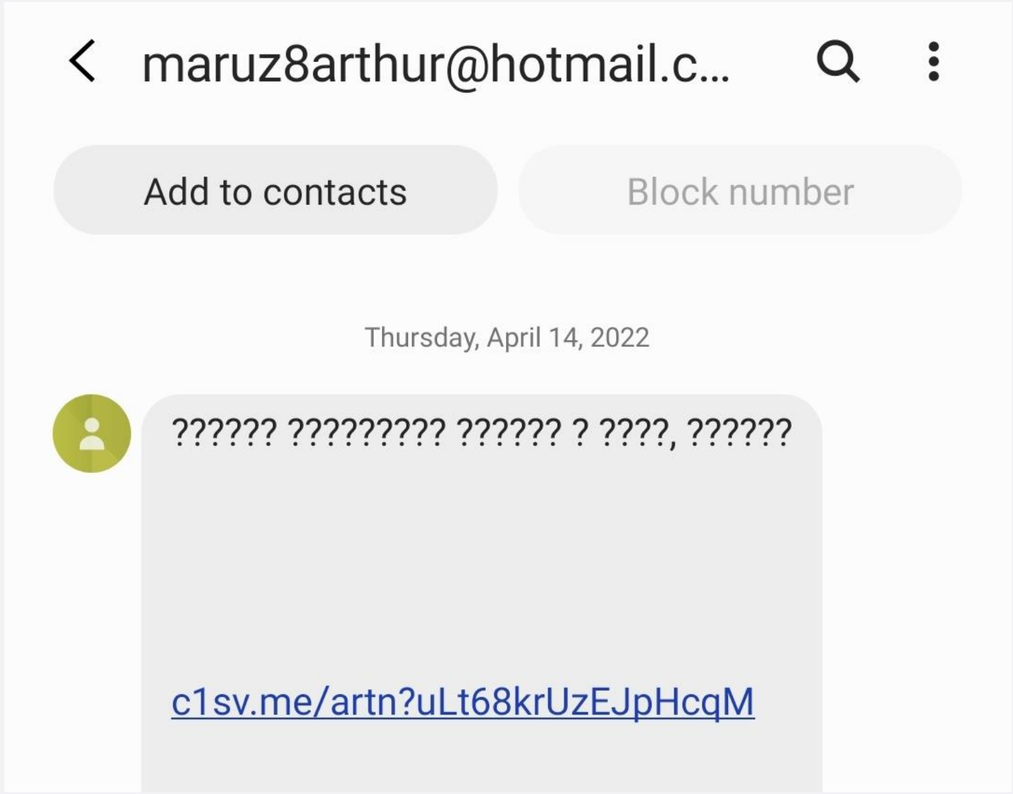
SIKICH®

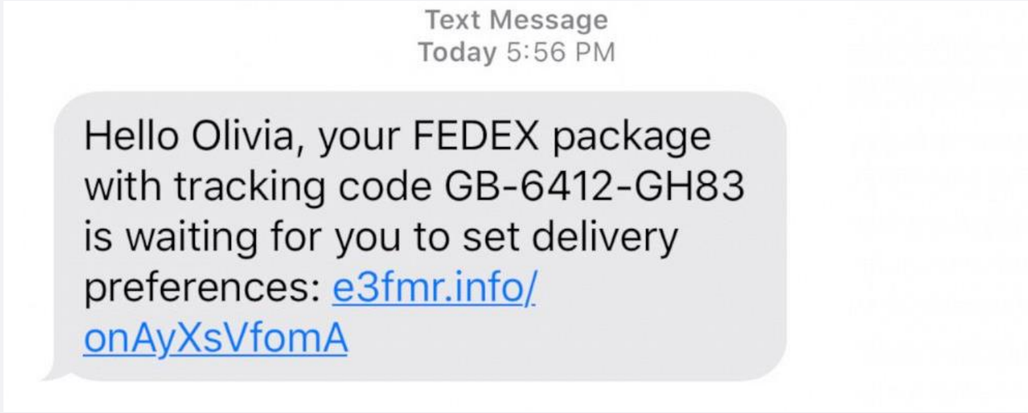
GAINING A FOOTHOLD
WITH COMPROMISED CREDENTIALS

SIKICH®

SMS PHISHING
THE NEW EMAIL PHISHING

- Information about an issue
- Needing you to complete a task
- Asking you to log into a site
- Task needs to be completed quickly
- Includes a link to visit





SIKICH®

SIKICH.COM

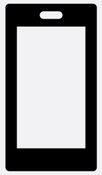
WIDE ARRAY OF THREATS AND ATTACK TECHNIQUES

Phishing Attacks

Virus / Malware

Password Guessing

SMS Attacks



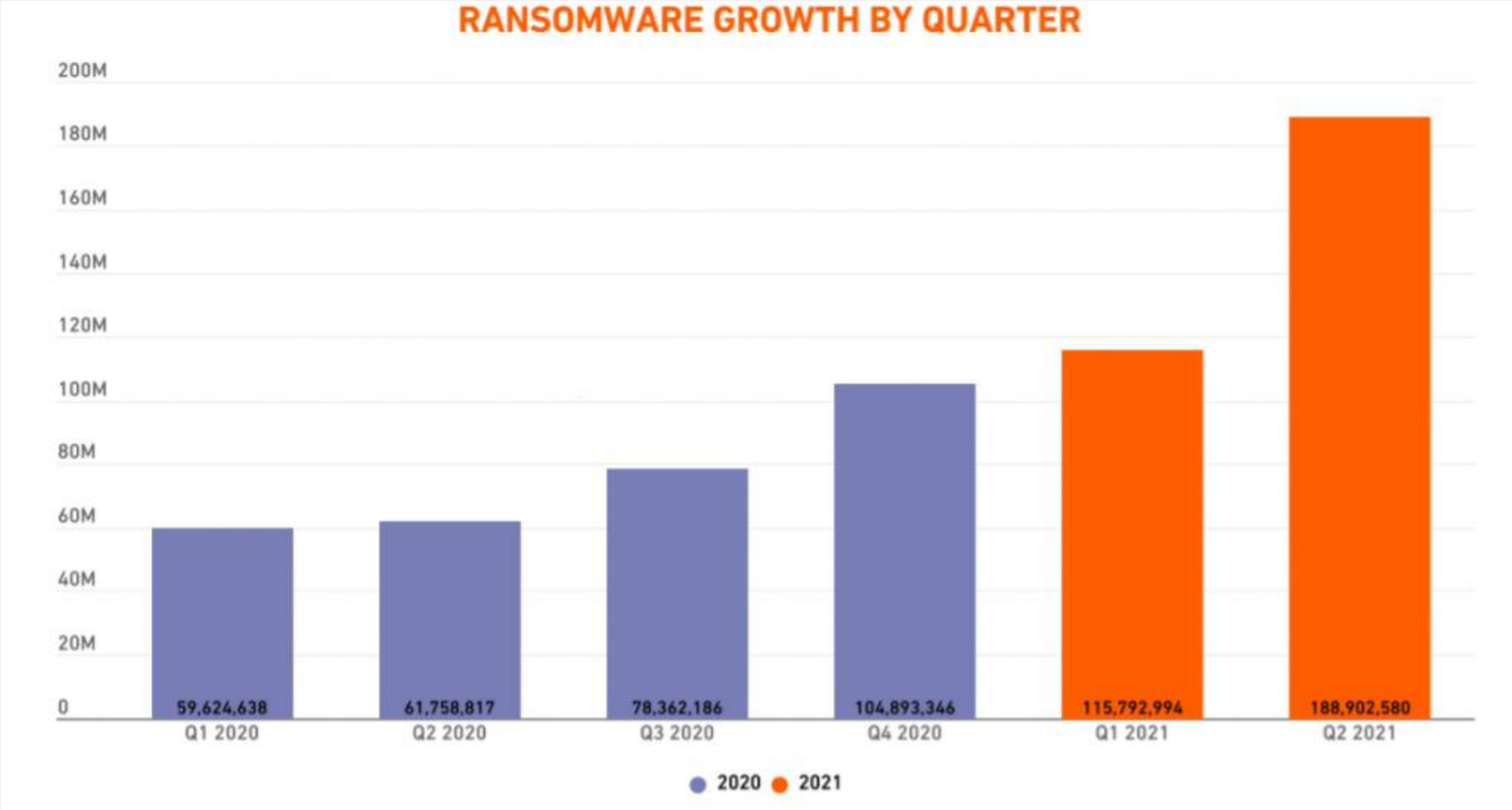
Browser-Based Attacks

Account Takeover

SIKICH®

RANSOMWARE
POST EXPLOITATION

- Offline applications
- Deleted backups
- Ransom demands
- Infected systems
- Shaming sites



SIKICH®

SIKICH.COM

DOING THE BASICS WELL

PROTECTING AGAINST THE NEWEST CYBERSECURITY THREATS

SIKICH®

SIKICH.COM

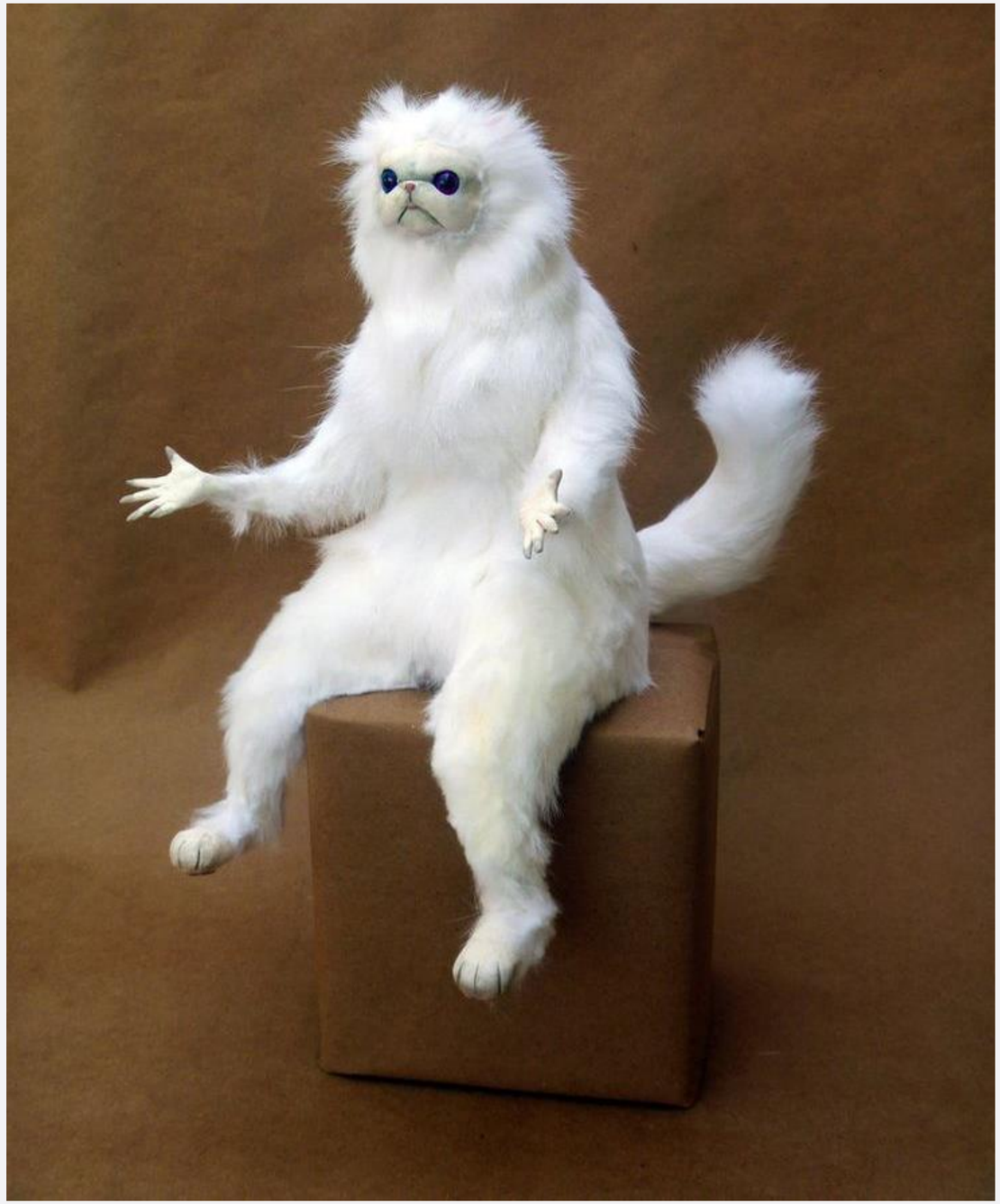
POLLING QUESTION:

HAVE YOU IMPLEMENTED MULTI-FACTOR AUTHENTICATION?

SIKICH®

I WISH
I'D KNOWN...

- That multi-factor authentication was so easy to implement
- That my backups weren't safe from hackers
- That we had so many anti-virus gaps
- How easily they could get admin access after infecting one computer
- That we didn't have hardly any logs



SIKICH®

POLLING QUESTION:

HOW LONG DO YOU THINK IT WOULD TAKE TO CRACK THE PASSWORD
“$ecure P@ssword!”

SIKICH®

TOP CYBERSECURITY CONTROLS YOU ALREADY KNOW ABOUT

- Multi-factor authentication (MFA)
- Commercial anti-virus installed everywhere (workstations and servers)
- Patch management for operating systems, browsers, firewalls
- Passphrases of 15+ characters, and unique passwords per system
- System hardening
- Security awareness training & exercises
- Cyber liability insurance

"5p@rt3n5!"	"flying purple snail gallon"
• Hard to remember • Easy for a computer to guess (48 hours)	• Easy to remember • Hard for a computer to guess (1000s' of years)

SIKICH®

EMERGING SECURITY SOLUTIONS AND STRATEGIES

PROTECTING AGAINST THE NEWEST CYBERSECURITY THREATS

SIKICH®

SIKICH.COM

NEW CYBERSECURITY CONTROL STRATEGIES YOU SHOULD KNOW ABOUT

- Protected backups
  - Immutable backups
  - Offline, in the cloud or behind MFA
- Endpoint detection and response (EDR) applications
  - Provide advanced firewalling, application whitelisting, host intrusion monitoring
- Filtered outbound (egress) traffic to block malware command-and-control
  - Web content filtering (with “uncategorized” set to block)
  - Default-deny for all other protocols

SIKICH®

NEW CYBERSECURITY CONTROL STRATEGIES YOU SHOULD KNOW ABOUT

- Extending workstation management and filtering controls to at-home users
- Logs set to retain six months of history
- Managed security services provider (MSSP) or security information and event management (SIEM) solution
- Periodic testing of security controls
- Testing of systems hosted in the cloud

SIKICH®

HOW CAN SIKICH HELP?

CYBERSECURITY AND IT SOLUTIONS SERVICES

SIKICH®

SIKICH.COM

POLLING QUESTION:

DOES YOUR ORGANIZATION HAVE A CYBERSECURITY PROGRAM?

SIKICH®

HOW CAN SIKICH HELP?

- Compliance assessments
- Risk and network security assessments
- Penetration testing (ethical hacking) to test security posture
- Virtual CISO (vCISO) support
- IT solutions and managed services

SIKICH®

SIKICH.COM

THANK YOU

Dr. Michael Vieau
Michael.Vieau@sikich.com
262.317.8574

Thomas Freeman
Thomas.Freeman@Sikich.com
262.317.8512

LinkedIn: www.linkedin.com/company/sikich
Facebook: www.facebook.com/sikichllp
Twitter: www.twitter.com/sikichllp
Blog: www.sikich.com/insights