RANSOMWARE, PHISHING & CYBERSECURITY SERVICE PROVIDER RISKS

- **June 14, 2022**

DISCLAIMER

The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.

LEARNING OBJECTIVES

UNDERSTAND THE LATEST THREAT DEVELOPMENTS

RECOGNIZE CRITICAL DEPENDENCIES AND RISKS IN OUTSOURCED SERVICE PROVIDER RELATIONSHIPS

LEARN WHERE ORGANIZATIONS CAN FOCUS VALUABLE RISK MITIGATION RESOURCES

DEVELOP AND REFINE A FRAMEWORK OF KNOWLEDGE TO PLAN FUTURE SECURITY EFFORTS

©2021 CliftonLarsonAllen LLP

ABOUT CLA

- CLA creates opportunities for businesses, individuals, and communities through our wealth advisory, outsourcing, audit, tax and consulting services.
- With 7,400 people, more than 120 U.S. locations, and a global affiliation, we promise to know you and help you. Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.

ABOUT NUVODIA

- Nuvodia can provide full range of IT services to your organization – ranging from one-time consulting, to fully outsourced and managed IT solutions.
- Nuvodia specializes in healthcare IT, servicing hospitals, retirement communities, and ambulatory clinics with a variety of services from hosting applications, security services and 24x7 helpdesk.
- Nuvodia is part of the Inland Imaging family of companies, headquartered in Spokane, but serving clients across the United states.

PRESENTERS

Sean Harrell
CEO, Nuvodia

sharrell@nuvodia.com

Javier Young
Principal, Cybersecurity

javier.young@claconnect.com

©2021 CliftonLarsonAllen LLP

CASE STUDIES

RANSOMWARE

WHAT IS RANSOMWARE?

- Cryptolocker, Locky, WannaCry, etc.
- Encrypts all data, holds in "ransom" for $$
  - Data on local machine and on network
- Can affect non-Windows OS (e.g., Mac)

©2021 CliftonLarsonAllen LLP

HOW DOES RANSOMWARE GET INTO BUSINESS NETWORKS?

Insecure Internet Accessible Log-in Prompts

- Outlook Web Access (OWA)
- Citrix Gateway
- Virtual Private Network (VPN)
- Remote Desktop Protocol (RDP)

Email phishing resulting in:

- User opening an infected attachment.
- User downloading malicious payload from a website.

Unpatched systems or mobile devices running outside of organization's firewall.

©2021 CliftonLarsonAllen LLP

RANSOMWARE IN THE NEWS

JBS Foods

- Paid $11 million
- Shutdown operations at beef plants for several days.
- Supply chain disruption.

Colonial Pipeline

- Paid $4.5 million.
- Shutdown operation for several days.
- Caused consumers panic buying gas.

©2021 CliftonLarsonAllen LLP

HOW DO WE MITIGATE?

- Risk assess, classify, and inventory systems
- Perform IT audit/cybersecurity assessments including internal network penetration testing and external network penetration testing – at least annually AND after significant changes
- Review and assess risks related to privileged user accounts (i.e. administrator access)
- Harden network technology and applications against attack
- Continue to enhance and tune network, system and application monitoring and alerting
- Train and test employees frequently (Human Factor)
- Develop a cyber resilience plan and test frequently

©2021 CliftonLarsonAllen LLP

USER EDUCATION AND PHISHING AWARENESS

- Malware typically needs a helper to do its job.
- Educate users on phishing scenarios and consider internal phishing "tests" to gauge employee readiness.
- Tests should familiarize employees with common phishing scenarios as well as teach employees how to identify masked links and spoofed sender addresses.

STRONG USER CONTROLS AND DATA BACKUPS

- Staff should not have local admin rights to their workstations.
- No email, browsing, or general computer use when using admin credentials.
- Network and domain admins should be required to have two sets of credentials.
- Administrators should NOT log into workstations with domain admin rights.
- Attackers are getting smarter and deleting or encrypting online backups; so, organizations should ensure that they have off-line copies of backup and restore files available.
- Backup and restore files should be saved in well secured location.
- Perform a thorough review of file permissions for network file shares.
- Test the restoration of your data

©2021 CliftonLarsonAllen LLP

CASE STUDIES

MICROSOFT EXCHANGE

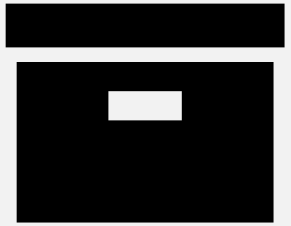
MICROSOFT EXCHANGE

- Exchange
  - Installed on-premise
  - Installed on corporate servers
  - Exchange servers have privileged access in network
- Exchange Online
  - Hosted by Microsoft in Microsoft's cloud
  - Organizations don't have to manage server, only application

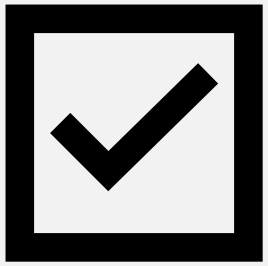
©2021 CliftonLarsonAllen LLP

WHY TARGET EXCHANGE

Conversations



Files



Authorization

©2021 CliftonLarsonAllen LLP

EXCHANGE VULNERABILITY HISTORY

PrivExchange (2019)

Static ViewState Key (2020)

ProxyLogon/Hafnium (2021)

©2021 CliftonLarsonAllen LLP

HAFNIUM (ACCORDING TO MICROSOFT)

Hacking group based out of China

Targets US companies

Operates using Virtual Private Servers (VPS) in US

https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/

TIMELINE

- Jan 5 – Security firm (DEVCORE) notifies Microsoft of vulnerability
- Jan 6 – Security firm (Volexity) notifies Microsoft that it sees hackers exploiting Exchange, going back to as early as Jan 3
- Jan 8 – Microsoft confirms vulnerability
- Jan 27 – Another security firm (Dubex) notifies Microsoft of organizations being hacked by "unknown" Exchange vulnerability

https://krebsonsecurity.com/2021/03/a-basic-timeline-of-the-exchange-mass-hack/

©2021 CliftonLarsonAllen LLP

TIMELINE (CONT.)

Microsoft notifies security firm that patches will be released on March's patch Tuesday (March 9)

Microsoft releases Exchange patches early

26 Feb.

18 Feb.

2 Mar.

Mass exploitation of Exchange vulnerability around the world

https://krebsonsecurity.com/2021/03/a-basic-timeline-of-the-exchange-mass-hack/

©2021 CliftonLarsonAllen LLP

PROXYLOGON VULNERABILITIES

- Four (4) separate vulnerabilities
  - **CVE-2021-26855: Server-Side Request Forgery (SSRF)**
  - CVE-2021-26857: Insecure Deserialization
  - CVE-2021-26858: Arbitrary File Write
  - **CVE-2021-27065: Arbitrary File Write**

MITIGATING CONTROLS

LOGGING AND MONITORING

EGRESS FILTERING

INSTALL PUBLIC-FACING SERVICES IN DMZ

ANTIVIRUS/ENDPOINT CONTROLS

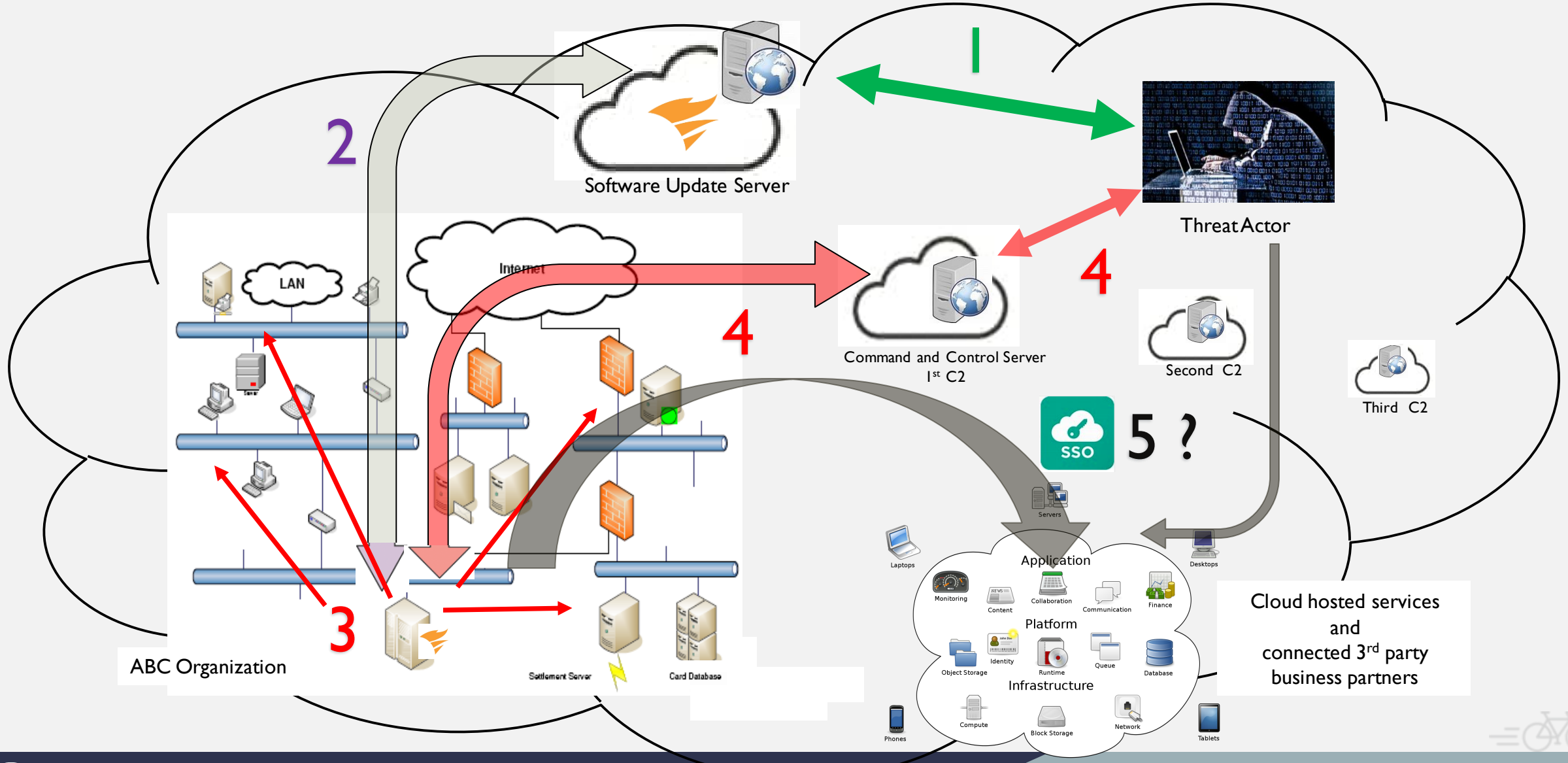
MULTI-FACTOR AUTHENTICATION FOR EMAIL AND REMOTE CONNECTIONS

©2021 CliftonLarsonAllen LLP

CASE STUDIES

SOLARWINDS

PICTURE IN YOUR MIND SOLARWINDS ORION COMPROMISE



©2021 CliftonLarsonAllen LLP

SUMMARY OF SOLARWINDS

1. **SolarWinds (SW) development/update process is compromised**
   - Malware added to plug in component
2. **Customers download and install SW update with back door malware**
   - Legitimate appearing malware installed
3. **Sophisticated malware "scans" location**
   - Gathers information ("where am I")
   - Attacks/disables security tools
4. **Malware "phones home"**
   - Connects to Command and Control Server (C2)
   - Provides recon information and accepts instructions
5. **Some organizations are subject to additional attack activity**
   - Lateral movement/pivoting
   - Privilege escalation
   - Creation of additional/secondary persistence mechanisms

©2021 CliftonLarsonAllen LLP

MICROSOFT TIMELINE

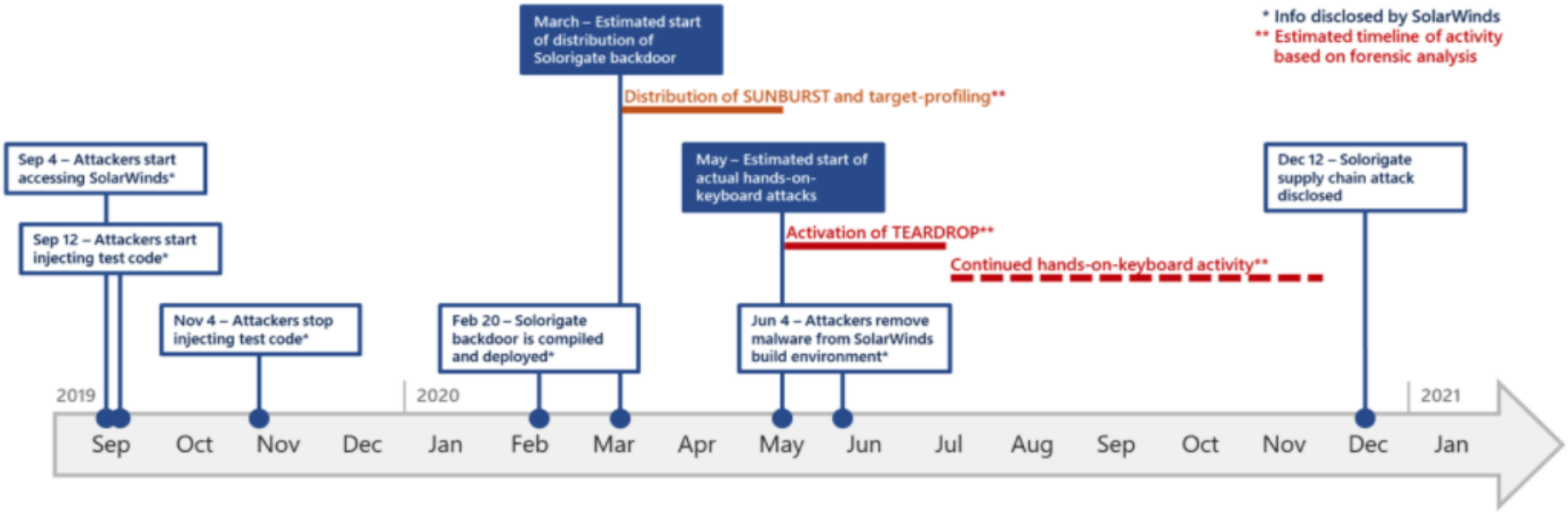


Figure 1. Timeline of the protracted Solorigate attack

https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

©2021 CliftonLarsonAllen LLP

Create Opportunities

UPDATE SUMMARY AS NEW INFORMATION WAS ADDED

1. **Sunspot**
   - Malware designed to compromise software development process (at SolarWinds)
2. **Sunburst**
   - Backdoor inserted by Sunspot
3. **Teardrop**
   - Installed via Sunburst backdoor for additional follow on / focused attacks
4. **Raindrop**
   - Loader that delivers Cobalt Strike
   - NOT delivered by Sunburst
   - Usually delivered/used later in compromise and privilege escalation process
5. Some organizations are subject to additional attack activity
   - Lateral movement/pivoting
   - Privilege escalation
   - Creation of additional/secondary persistence mechanisms
6. Objectives?
   - Espionage?
   - Gather and steal information?
   - Launch point for attack into other trusted systems?
     - Office 365?
     - Other trusted applications/systems?
     - Other trusted organizations?
     - "Golden SAML"

©2021 CliftonLarsonAllen LLP

TAKE-AWAYS

1. Do we use SolarWinds Orion?
   - If ***NO*** → Go to 6
   - If YES → What version?
2. Is our version the affected version (see SW advisory)?
   - If ***NO*** → Go to 6
   - If YES → Continue
3. Have we created a timeline of potential exposure?
4. What logs do we have and how far back in time do they go?
5. What Indicators of Compromise (IOC's) have we searched for?
   - What resources/references have we used to identify known and potential IOC's?
   - Use 3 and 4 to search for IOC's
6. Do we have any third-party service providers with trusted access?
   - Who has remote access into our environment?
   - Who do we push our data out to?
   - Are there any persistent open connections to or from third parties?
7. Repeat 1-5 for those identified in 6

©2021 CliftonLarsonAllen LLP

TAKE-AWAYS

8. "Know What Normal Looks like"
   - Easy to say… challenging to execute
   - Server communication to the outside
   - DNS logs
     - Capture information about a newly-seen, unfamiliar domain in network traffic.
     - Leverage internal data sources and continuous DNS monitoring. Own-network defense is best augmented through visibility of own-network activity and traffic
     - Monitoring for new, unique, or abnormal network connections can identify C2 communication schema.
     - Proper asset classification which identifies specific hosts or host-type (e.g., "server" instead of "end-user client") can further differentiate communication to identify items of concern.
     - Similar classification can also work to identify unusual authentication activity, where servers (such as a SolarWinds Orion device) initiate logons to other clients instead of the reverse.

©2021 CliftonLarsonAllen LLP

https://www.domaintools.com/resources/blog/continuous-eruption-further-analysis-of-the-solarwinds-supply-incident

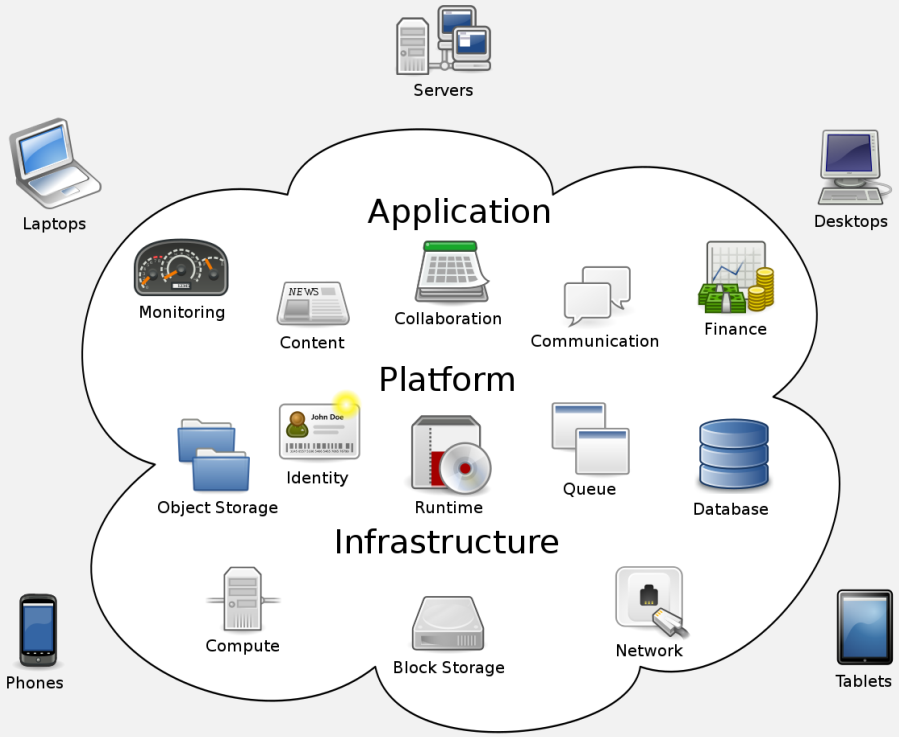
TAKE-AWAYS

9. In-house threat hunting for IOC's

10. In-house changes
    - Privileged accounts and service accounts
    - Critical files and system settings

11. Threat hunting in cloud Infrastructure
    - Mandiant Azure AD Investigator
    - CISA Sparrow
    - MS Azure Security Compass

12. New information is being released regularly…



©2021 CliftonLarsonAllen LLP

BROADER DISCUSSION ON VENDOR MGMT/SUPPLY CHAIN

All software products have bugs/vulnerabilities

Key questions:

What does this software application have access to?

What user account/privileges are given to it?

What is the software vendor doing to provide us a level of comfort that they have done their due diligence?

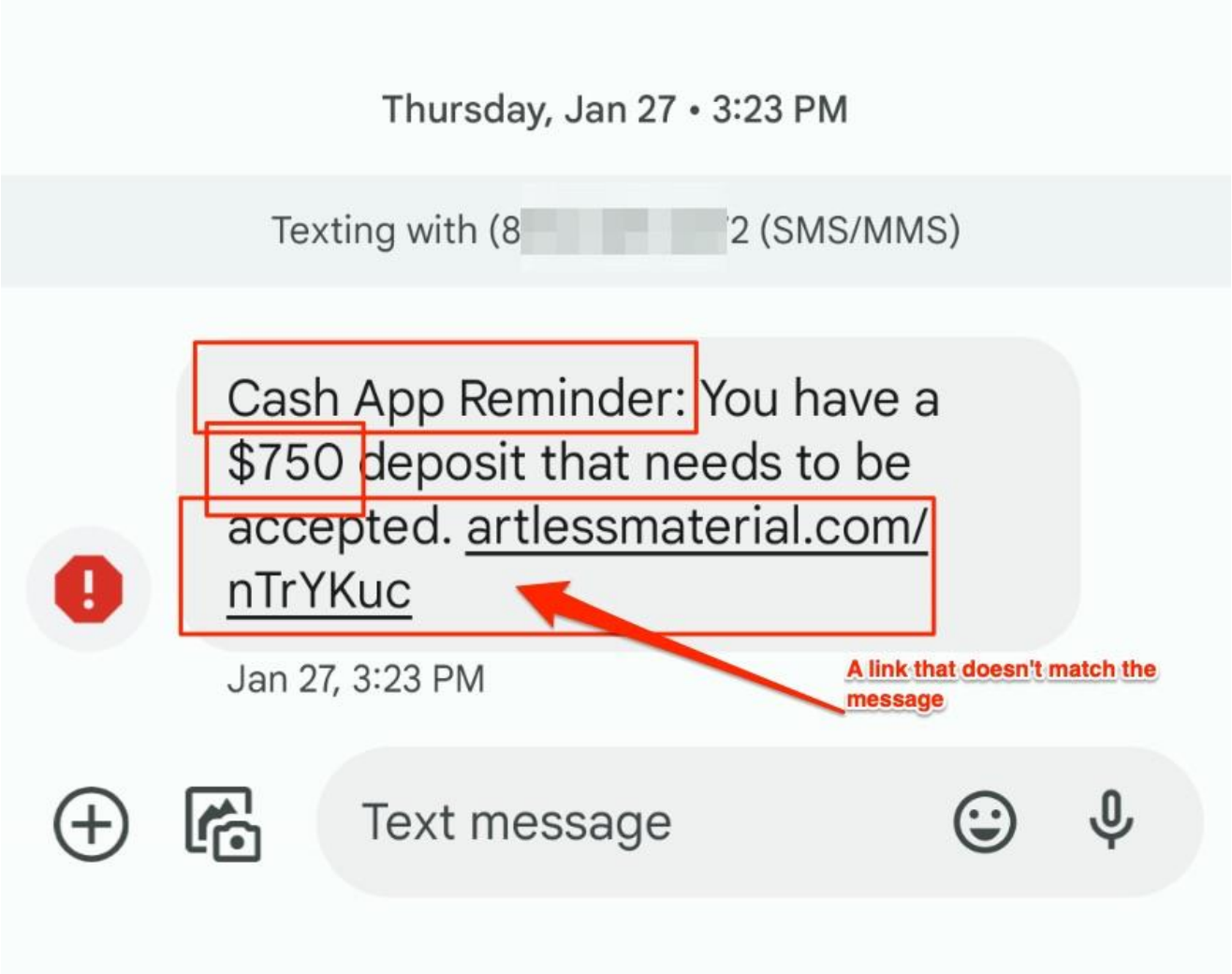
What do we need to do for our due diligence?

©2021 CliftonLarsonAllen LLP

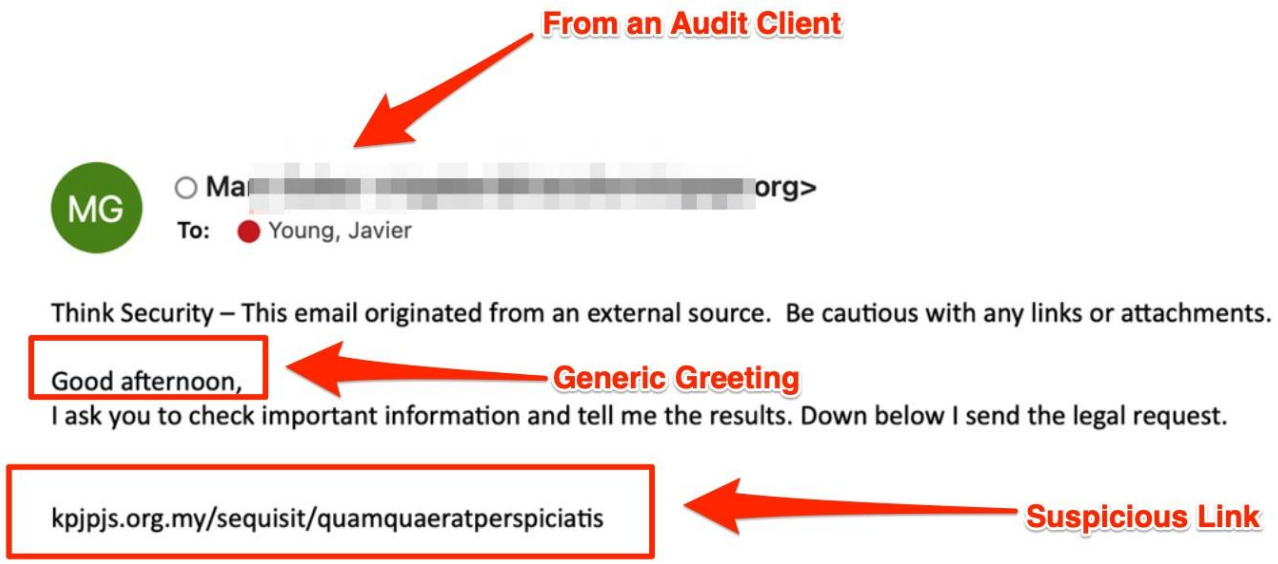
LET'S TALK MORE PHISHING

SOCIAL ENGINEERING

SMS EXAMPLE


Thursday, Jan 27 • 3:23 PM
Texting with (8 2 (SMS/MMS)
Cash App Reminder: You have a $750 deposit that needs to be accepted. artlessmaterial.com/nTrYKuc
Jan 27, 3:23 PM
A link that doesn't match the message
Text message

COMPROMISED EMAIL EXAMPLE



"ACCIDENTAL" EMAIL EXAMPLE

Employee Compensation Adjustment List 1 message

From: [redacted] Dawn

To: [redacted]

November 5, 2020 9:53 AM

Sent to EVERYONE in the company

BJ,

Below is the modified list of employees scheduled to receive out-of-cycle compensation adjustments as we previously discussed. Royce and I discussed and made a few updates.

Employee-Comp-Adjustments-2020-11-05.docx

Please let me know if you have any questions or want to discuss further. These adjustments will start on November 9th.

Regards,

Dawn