VerticalStructure

# Security stories

Simon Whittaker

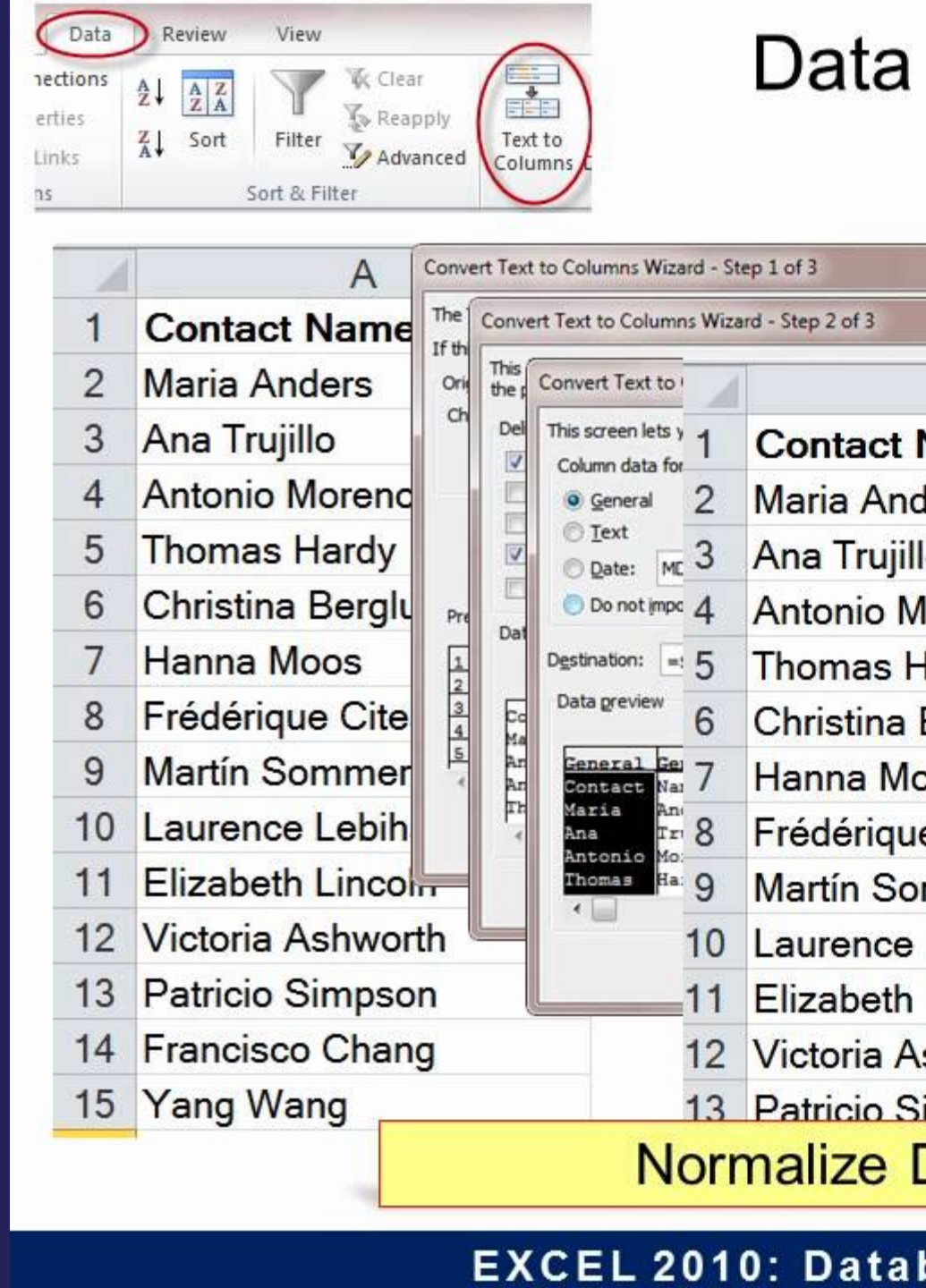
# Me

## CEO & co founder
## Chair of NI Cyber


@gwenking Unsplash

# Way back when

- ftp
- HTTPS?
- databases



# Securing the outside

- Firewall to protect outside
- Software running internally
- No way anyone could get in!
- In house support

The past

# Development

- A million passwords
- Write everything yourself, each time
- Username and passwords in the database.


# Bad actors

Unsplash @vademann

verticalstructure.com


Unsplash Art Rachen

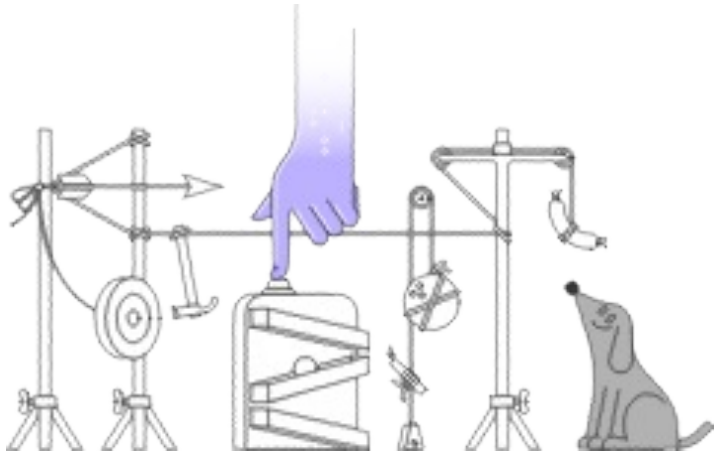
# Change in motives

- Rise in cybercrime

# Transition

## Security testing with tooling

ULESKA



Azure Security Center

# Engagement


paloalto
NETWORKS


CODE42


CROWDSTRIKE


McAfee


Infoblox
NEXT LEVEL NETWORKING


LexisNexis
RISK SOLUTIONS


Secureworks


DARKTRACE


GENERALI
GLOBAL ASSISTANCE
IDENTITY & CYBER PROTECTION


HACKTHEBOX

# Welcome!

Cyber security is born

Cybersecurity is born

Cyber Security is .....


# Risk transfer

Vertical Structure

verticalstructure.com

# Risk transfer

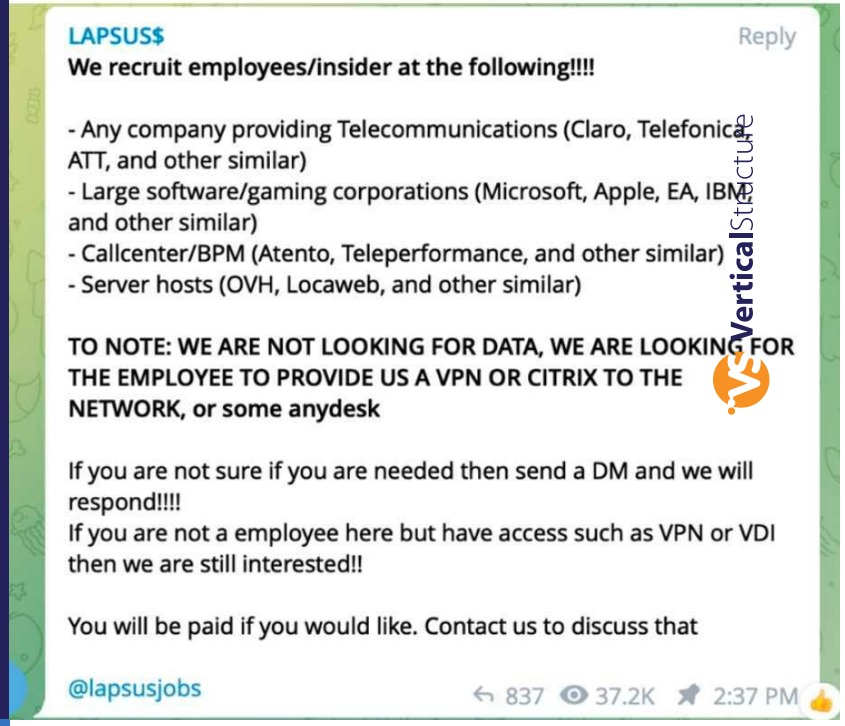
# Reliance on packages

## Spring4Shell Detection: New Java Vulnerability Follows in the Footsteps of Notorious Log4j

WRITTEN BY
**Anastasiia Yevdokimova**

March 31, 2022 · 3 min read


# Other impacts



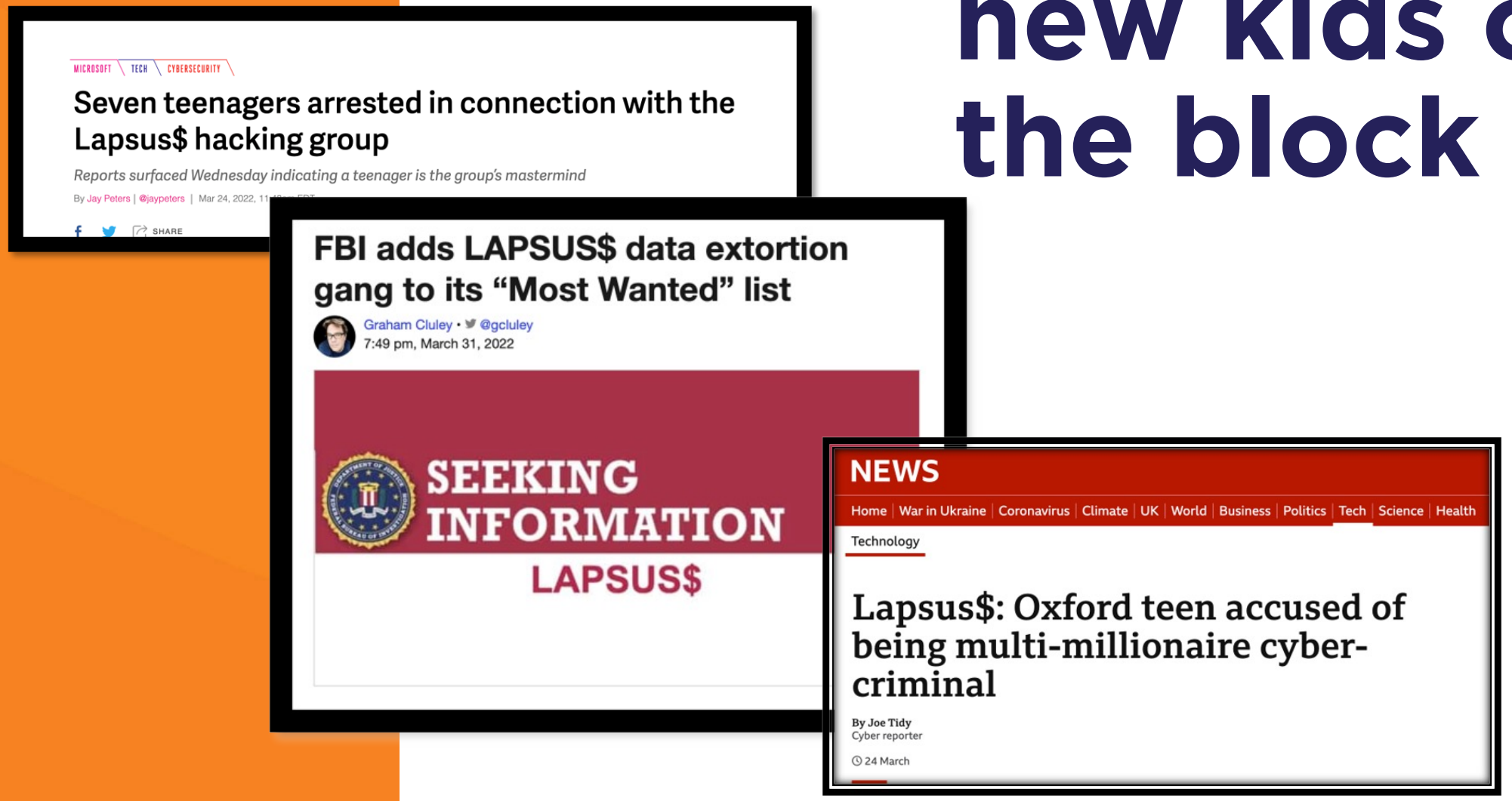

Unsplash engin akyurt

# Reliance on third parties

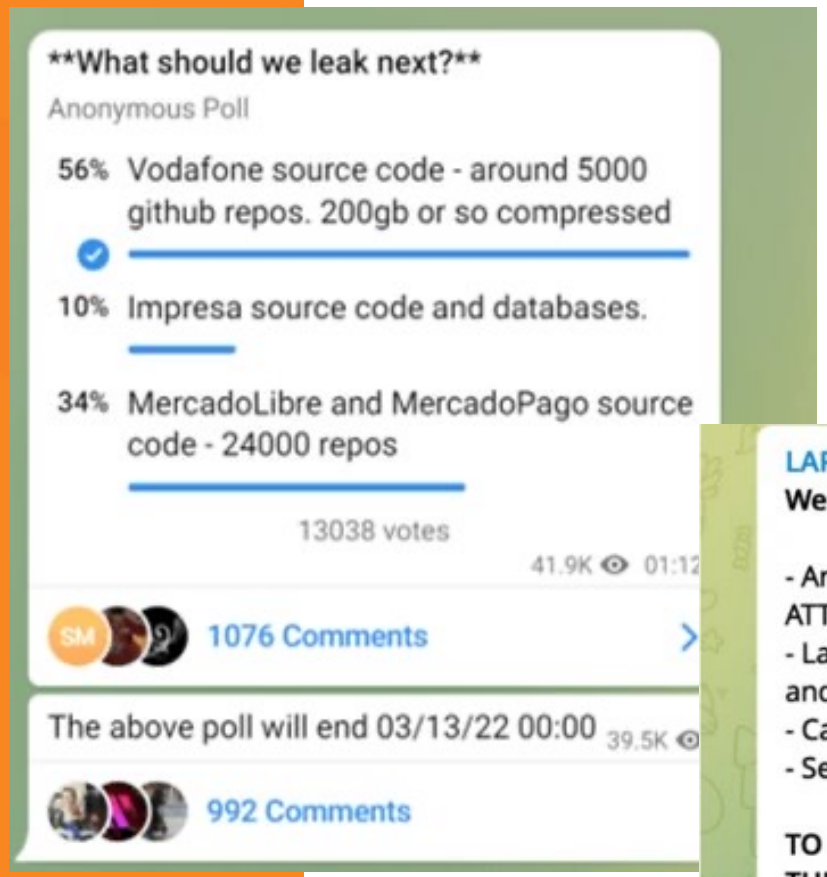
# The power of a devious person

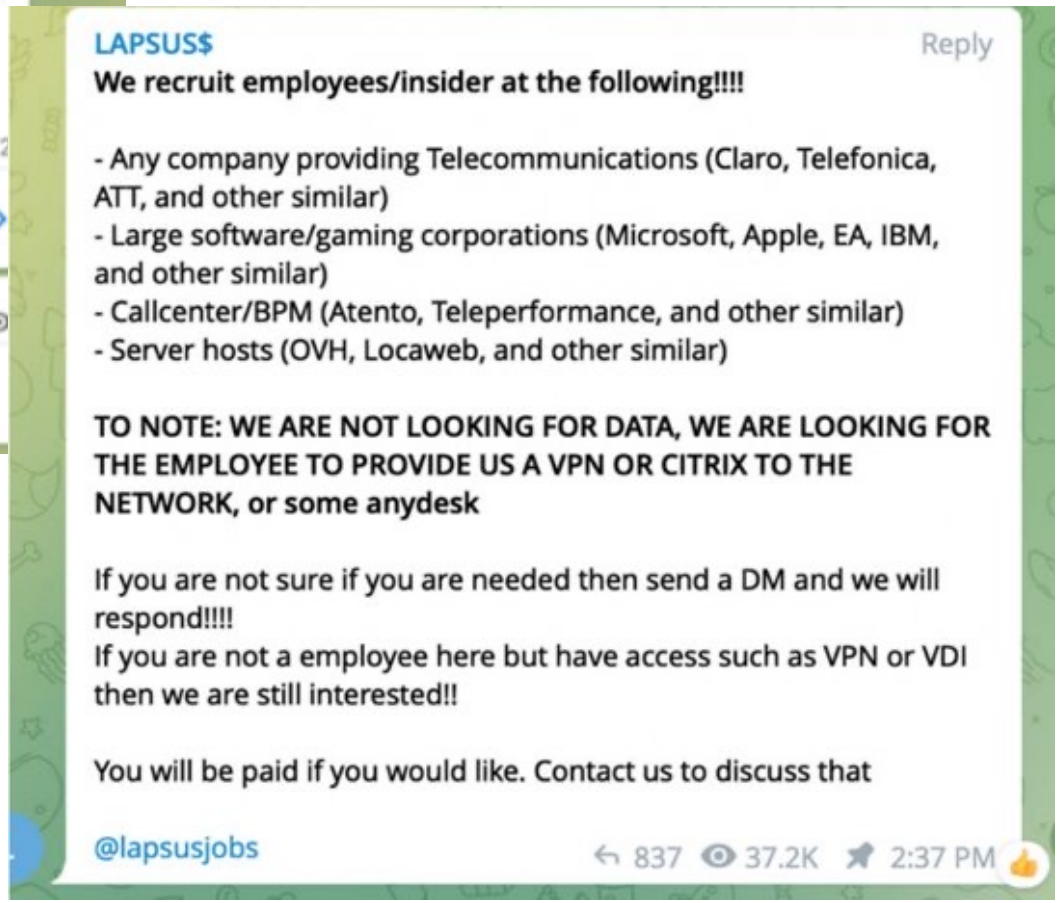
The actor has been observed then **joining** the organization's crisis communication calls and internal discussion boards (Slack, Teams, conference calls, and others) to **understand** the incident response workflow and their corresponding response. It is assessed this provides DEV-0537 **insight into the victim's state of mind**, their **knowledge** of the intrusion, and a **venue** to initiate extortion demands. Notably, DEV-0537 has been observed joining incident response bridges within targeted organizations responding to destructive actions.

# Lapsus$ - new kids on the block



# The rise of Lapsus$



# Timeline of OKTA


**Intrusion Timeline**

Table 1 lists the major dates, associated events, and the applicable attack phase for the intrusion. All timestamps in this report are in Coordinated Universal Time (UTC), unless otherwise noted. For a detailed description of each attack phase, refer to **Appendix A: Targeted Attack Lifecycle.**

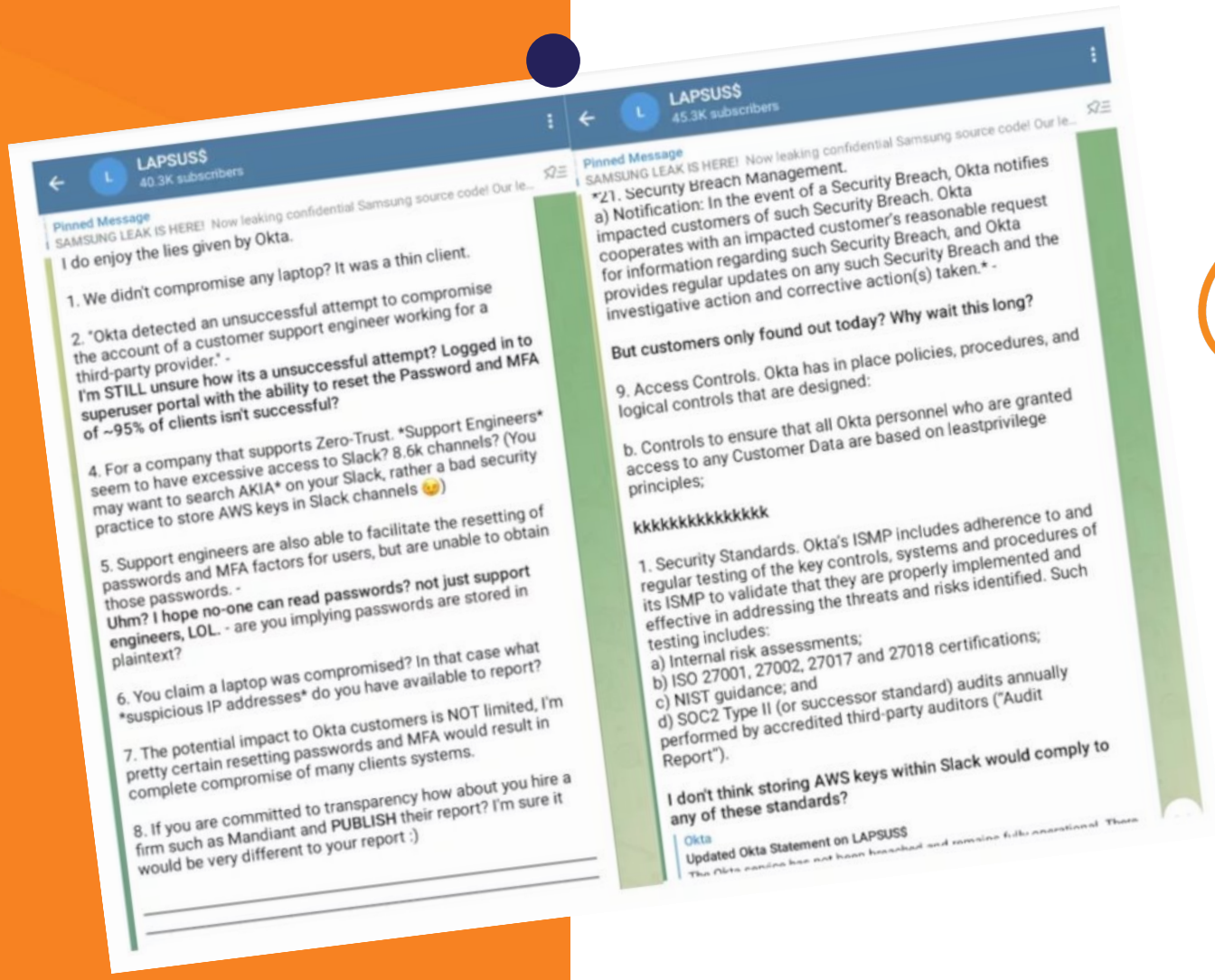
| Date (UTC) | Event | Attack Phase |
|---|---|---|
| 2022-01-16 00:33:23 | First logon event from [SYSTEM NAME REDACTED]. Logon to [SYSTEM NAME REDACTED] from [SYSTEM NAME REDACTED] (10.112.137.64) | Initial Compromise |
| 2022-01-19 19:19:47 | RDP logon by [ACCOUNT NAME REDACTED] from LOCAL to [SYSTEM NAME REDACTED] | Initial Compromise |
| 2022-01-19 19:45:39 | Bing search for Privilege escalation tools on Github by [ACCOUNT NAME REDACTED] | Escalate Privileges |
| 2022-01 19:47:58 | UserProfileSvcEop.exe downloaded from hxxps://github.com by [ACCOUNT NAME REDACTED] | Escalate Privileges |
| 2022-01-20 18:31:19 | Account [ACCOUNT NAME REDACTED] created on [SYSTEM NAME REDACTED] | Maintain Presence |
| 2022-01-20 18:32:32 | RDP logon by [ACCOUNT NAME REDACTED] from LOCAL to [SYSTEM NAME REDACTED] | Move Laterally |
| 2022-01-20 18:39:43 | Bing search for Process Explorer by [ACCOUNT NAME REDACTED] | Internal Recon |
| 2022-01-20 18:40:04 | Process Explorer executed by [ACCOUNT NAME REDACTED] | Internal Recon |
| 2022-01-20 18:43:51 | Bing search for Process Hacker by [ACCOUNT NAME REDACTED] | Establish Foothold |
| 2022-01-20 18:44:01 | Process Hacker downloaded from hxxps://github.com by [ACCOUNT NAME REDACTED] | Establish Foothold |
| 2022-01-20 18:44:17 | Process Hacker execution by [ACCOUNT NAME REDACTED] | Establish Foothold |
| 2022-01-20 18:46:22 | FireEye Endpoint Agent service terminated on [SYSTEM NAME REDACTED] | Establish Foothold |
| 2022-01-20 18:46:55 | Bing search for Mimikatz by [ACCOUNT NAME REDACTED] | Escalate Privileges |
| 2022-01-20 18:48:28 | Mimikatz downloaded from hxxps://github.com by [ACCOUNT NAME REDACTED] | Escalate Privileges |
| 2022-01-20 18:50:10 | Mimikatz executed by [ACCOUNT NAME REDACTED] on [SYSTEM NAME REDACTED] | Escalate Privileges |
| 2022-01-20 18:55:29 | C:\Windows\System32\sam.hiv created on [SYSTEM NAME REDACTED] | Escalate Privileges |
| 2022-01-20 18:55:41 | C:\sam.hiv created on [SYSTEM NAME REDACTED] | Escalate Privileges |

| | | |
|---|---|---|
| 2022-01-20 18:56:00 | C:\system.hiv created on [SYSTEM NAME REDACTED] | Escalate Privileges |
| 2022-01-20 18:57:17 | C:\Users\[ACCOUNT NAME REDACTED]\Documents\mimikatz_trunk\x64\hash.txt | Escalate Privileges |
| 2022-01-20 18:58:05 | hxxps://pastebin.com/7E30i24r by [ACCOUNT NAME REDACTED] | Escalate Privileges |
| 2022-01-20 19:06:43 | RDP logon by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED] from [SYSTEM NAME REDACTED] | Move Laterally |
| 2022-01-20 19:53:31 | Bing search for Process Hacker by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED] | Establish Foothold |
| 2022-01-20 19:55:37 | Process Hacker downloaded from hxxps://objects.githubusercontent.com | Establish Foothold |
| 2022-01-20 19:55:58 | Bing search for Mimikatz by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED] | Escalate Privileges |
| 2022-01-20 19:57:07 | Mimikatz downloaded from hxxps://github.com by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED] | Escalate Privileges |
| 2022-01-20 20:58:31 | RDP disconnect from [SYSTEM NAME REDACTED] by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED] | Move Laterally |
| 2022-01-20 23:02:41 | First malicious logon by [ACCOUNT NAME REDACTED]@sykes[.]com to O365 | Initial Compromise |
| 2022-01-21 00:05:15 | [ACCOUNT NAME REDACTED]@sykes[.]com accessed hxxps://[INTERNAL URL REDACTED]/personal/[INTERNAL USER NAME REDACTED]/Documents/Projects/ryk/DomAdmins-LastPass.xlsx via SecureLink | Internal Recon |
| 2022-01-21 05:29:50 | [ACCOUNT NAME REDACTED] account created by [ACCOUNT NAME REDACTED]@sykes[.]com | Maintain Presence |
| 2022-01-21 05:29:51 | [ACCOUNT NAME REDACTED] added to TenantAdmins group by [ACCOUNT NAME REDACTED]@sykes[.]com | Maintain Presence |
| 2022-01-21 05:39:13 | Malicious Email Transport rule to forward to BCC all mail to the accounts [ACCOUNT NAME REDACTED]@sykes[.]com and [ACCOUNT NAME REDACTED] | Establish Fo |
| 2022-01-21 14:11:38 | Last malicious logon by [ACCOUNT NAME REDACTED]@sykes[.]com to O365 | Complete M |



VerticalStructure

verticalstructure.com




# OKTA's Response

In January, we did not know the extent of the Sitel issue – only that we detected and prevented an account takeover attempt and that Sitel had retained a third party forensic firm to investigate. At that time, we didn't recognize that there was a risk to Okta and our customers. We should have more actively and forcefully compelled information from Sitel. In light of the evidence that we have gathered in the last week, it is clear that we would have made a different decision if we had been in possession of all of the facts that we have today.

# Technology

# Knowledge & Power

Unsplash @pete_nuij

# Integrated security

Unsplash engin akyurt

# Thank You

hello@verticalstructure.com