

# Simon Whittaker



Me

### CEO & co founder Chair of NI Cyber









## Way back when

- ftp
- HTTPS?
- databases

1	A	Conve	ert Text	to Col	umns Wi	zard - St	tep 1 of 3
1	Contact Name	The If th	Conve	ert Text	to Colun	nns Wiz	ard - Step 2 of 3
2	Maria Anders	Ori	This the p	Conve	ert Text to		
3	Ana Trujillo	Ch	Del		creen lets mn data f		Contact I
4	Antonio Morenc				mn oata n General	2	Maria And
5	Thomas Hardy		V		Text Date: N	<sub>c</sub> 3	Ana Trujill
6	Christina Berglu	Pre	Dat		Do not imp		Antonio M
7	Hanna Moos	1	Dai	Destir	nation:	5	Thomas H
8	Frédérique Cite	2 3 4 5	Co Ma	Data	preview	6	Christina I
9	Martín Sommer	5	An An			. 7	Hanna Mo
10	Laurence Lebih		<u>т</u> н «	Ana		8	Frédérique
11	Elizabeth Lincol				conio M omas H	9	Martín Sor
12	Victoria Ashwor	th				10	Laurence
13	Patricio Simpso	n				11	Elizabeth
14	Francisco Chan	g				12	Victoria A
15	Yang Wang					13	Patricio Si
					N	or	malize [

### EXCEL 2010: Datal

### **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











## Change in motives

• Rise in cybercrime



## Transition

Security testing with tooling

### ULESKA











### Welcome!

Cyber security is born Cybersecurity is born Cyber Security is .....



## Risk transfer



### **Risk transfer**



### Reliance on packages

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



March 31, 2022 · 3 min read





licated



## Other impacts

#### LAPSUS\$

We recruit employees/insider at the following!!!!

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)

- Large software/gaming corporations (Microsoft, Apple, EA, IBN), and other similar)

- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk

If you are not sure if you are needed then send a DM and we will respond!!!!

If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

@lapsusjobs

← 837 • 37.2K 📌 2:37 PM









## 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 MICROSOFT TECH CYBERSECURITY Seven teenagers arrested in connection with the the block Lapsus\$ hacking group Reports surfaced Wednesday indicating a teenager is the group's mastermind By Jay Peters | @jaypeters | Mar 24, 2022, 1 SHARE FBI adds LAPSUS\$ data extortion gang to its "Most Wanted" list Graham Cluley • 9 @gcluley 7:49 pm, March 31, 2022 SEEKING **NEWS** Home War in Ukraine Coronavirus Climate UK World Business Politics Tech Science Health NFORMATION Technology LAPSUS\$ Lapsus\$: Oxford teen accused of being multi-millionaire cybercriminal By Joe Tidy Cyber reporter 3 24 March

### \*\*What should we leak next?\*\*

Anonymous Poll

56% Vodafone source code - around 5000 github repos. 200gb or so compressed

10% Impresa source code and databases.

34% MercadoLibre and MercadoPago source code - 24000 repos

13038 votes

41.9K 💿 01:12

1076 Comments

The above poll will end 03/13/22 00:00 39.5K @



992 Comments

# The rise of Lapsus\$

#### LAPSUS\$

Reply

We recruit employees/insider at the following!!!!

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

#### TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk

If you are not sure if you are needed then send a DM and we will respond!!!!

If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

### @lapsusjobs

### 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] 2022-01-20 18:57:17 C:\Users\[ACCOUNT NAME REDACTED]\Documents\mimikatz\_trunk\x64\hash.txt 2022-01-20 18:58:05 Escalate Privileges hxxps://pastebin.com/7E30i24r by [ACCOUNT NAME REDACTED] 2022-01-20 19:06:43 Escalate Privileges RDP logon by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED] from [SYSTEM NAME REDACTED] 2022-01-20 19:53:31 Escalate Privileges Bing search for Process Hacker by [SYSTEM NAME REDACTED]\[ACCOUNT NAME REDACTED] Move Laterally 2022-01-20 19:55:37 Process Hacker downloaded from Establish Foothold hxxps://objects.githubusercontent.com 2022-01-20 19:55:58 Bing search for Mimikatz by [SYSTEM NAME REDACTED]\[ACCOUNT Establish Foothold NAME REDACTED] 2022-01-20 19:57:07 Mimikatz downloaded from hxxps://github.com by [SYSTEM NAME Escalate Privileges 2022-01-20 20:58:31 RDP disconnect from [SYSTEM NAME REDACTED] by [SYSTEM NAME Escalate Privileges 2022-01-20 23:02:41 First malicious logon by [ACCOUNT NAME REDACTED]@sykes[.]com to Move Laterally 2022-01-21 00:05:15 [ACCOUNT NAME REDACTED]@sykes[.]com accessed Initial Compromise hxps://INTERNAL URL REDACTEDI/personal/[INTERNAL USER NAME REDACTEDI/Documents/Projects/ryk/DomAdmins-LastPass.xlsx via 2022-01-21 05:29:50 Internal Recon [ACCOUNT NAME REDACTED] account created by [ACCOUNT NAME 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 Maintain Presence accounts [ACCOUNT NAME REDACTED]@sykes[.]com and [ACCOUNT 2022-01-21 14:11:38 Last malicious logon by [ACCOUNT NAME REDACTED]@sykes[.]com to Establish Fo Complete N

### LAPSUSS

\$PE

SAMSUNG LEAK IS HERE! Now leaking confidential Samsung source code! Our le... I do enjoy the lies given by Okta. 1. We didn't compromise any laptop? It was a thin client. 2. "Okta detected an unsuccessful attempt to compromise the account of a customer support engineer working for a I'm STILL unsure how its a unsuccessful attempt? Logged in to superuser portal with the ability to reset the Password and MFA of ~95% of clients isn't successful? 4. For a company that supports Zero-Trust. \*Support Engineers\*

APSUSS

seem to have excessive access to Slack? 8.6k channels? (You may want to search AKIA\* on your Slack, rather a bad security practice to store AWS keys in Slack channels 🥪) 5. Support engineers are also able to facilitate the resetting of passwords and MFA factors for users, but are unable to obtain

Uhm? I hope no-one can read passwords? not just support engineers, LOL. - are you implying passwords are stored in

6. You claim a laptop was compromised? In that case what plaintext? \*suspicious IP addresses\* do you have available to report?

7. The potential impact to Okta customers is NOT limited, I'm pretty certain resetting passwords and MFA would result in

complete compromise of many clients systems. 8. If you are committed to transparency how about you hire a firm such as Mandiant and PUBLISH their report? I'm sure it

would be very different to your report :)

SAMSUNG LEAK IS HERE! Now leaking confidential Samsung source code! Our le... a) Notification: In the event of a Security Breach, Okta notifies impacted customers of such Security Breach. Okta cooperates with an impacted customer's reasonable request for information regarding such Security Breach, and Okta provides regular updates on any such Security Breach and the investigative action and corrective action(s) taken.\* -But customers only found out today? Why wait this long?

9. Access Controls. Okta has in place policies, procedures, and

logical controls that are designed: b. Controls to ensure that all Okta personnel who are granted

access to any Customer Data are based on leastprivilege

principles;

kkkkkkkkkkkkkk

1. Security Standards. Okta's ISMP includes adherence to and regular testing of the key controls, systems and procedures of its ISMP to validate that they are properly implemented and effective in addressing the threats and risks identified. Such b) ISO 27001, 27002, 27017 and 27018 certifications; d) SOC2 Type II (or successor standard) audits annually performed by accredited third-party auditors ("Audit

I don't think storing AWS keys within Slack would comply to

any of these standards?

Updated Okta Statement on LAPSUS\$

## **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 todav.



## Technology



# Knowledge & Power



Unsplash @pete\_nuij

## Integrated security



# Thank You

☑ hello@verticalstructure.com