Thread by @BillDemirkapi on Thread Reader App – Thread Reader App

threadreaderapp.com/thread/1508527487655067660.html

Thread reader

Tweet Share

Thread by Bill Demirkapi (@BillDemirkapi), Mar 28

> New documents for the Okta breach: I have obtained copies of the Mandiant report detailing the embarrassing Sitel/SYKES breach timeline and the...

Another scary note is the date in the VM used in the screenshot consistently appears to be January 21st, 2022. If this date is correct, this would suggest @okta failed to publicly acknowledge any breach for at least two months. 

LAPSUS$ used off-the-shelf tooling from GitHub for the majority of their attacks. After downloading Process Explorer and Process Hacker, LAPSUS$ bypassed the FireEye

endpoint agent by simply terminating it! 3/N

Intrusion Timeline

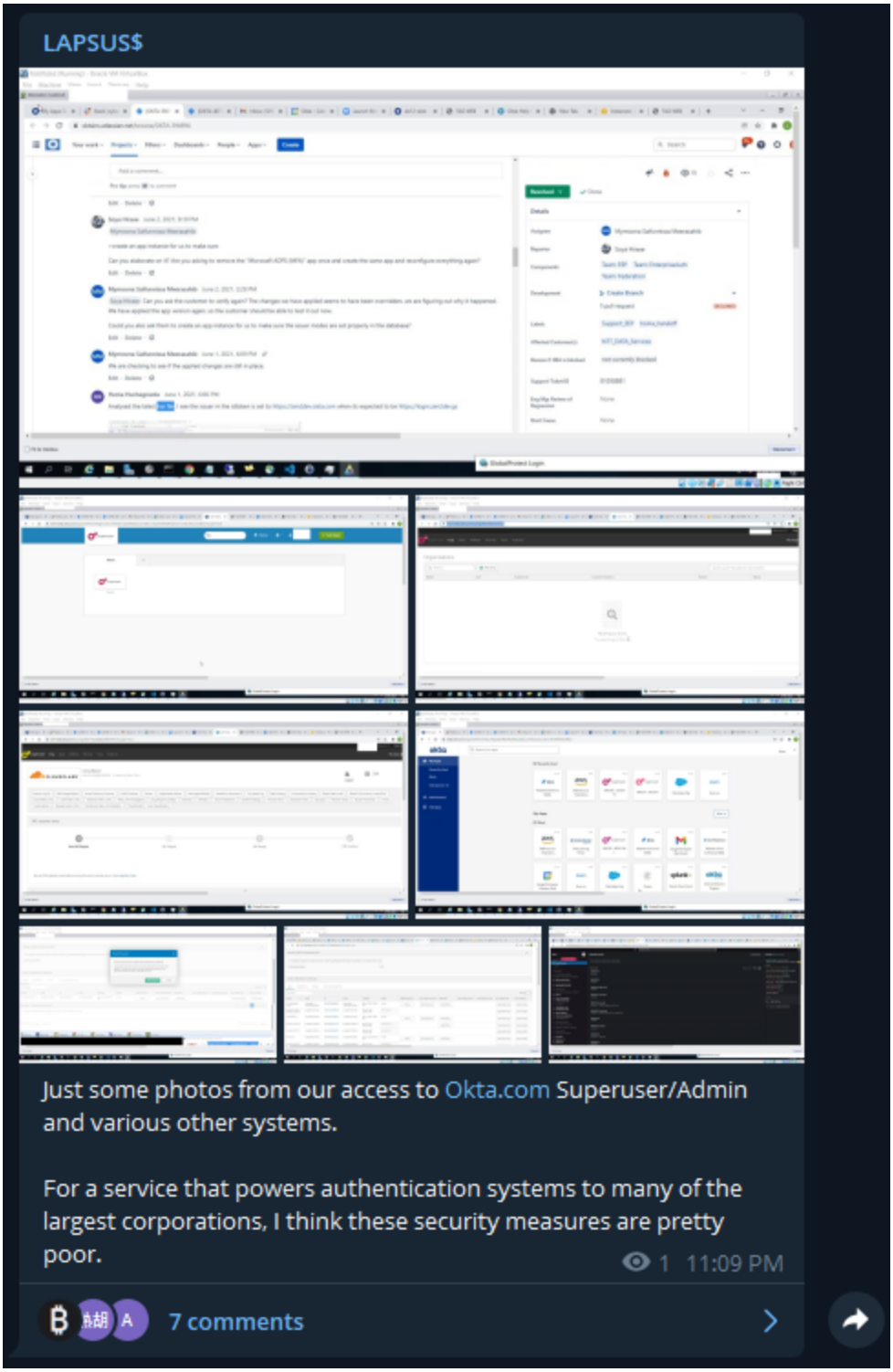
Table 1 lists the major dates, associated events, and the applicable attack phase for the intrusion. All timestamps in this report are in Coordinated Universal Time (UTC), unless otherwise noted. For a detailed description of each attack phase, refer to **Appendix A: Targeted Attack Lifecycle.**

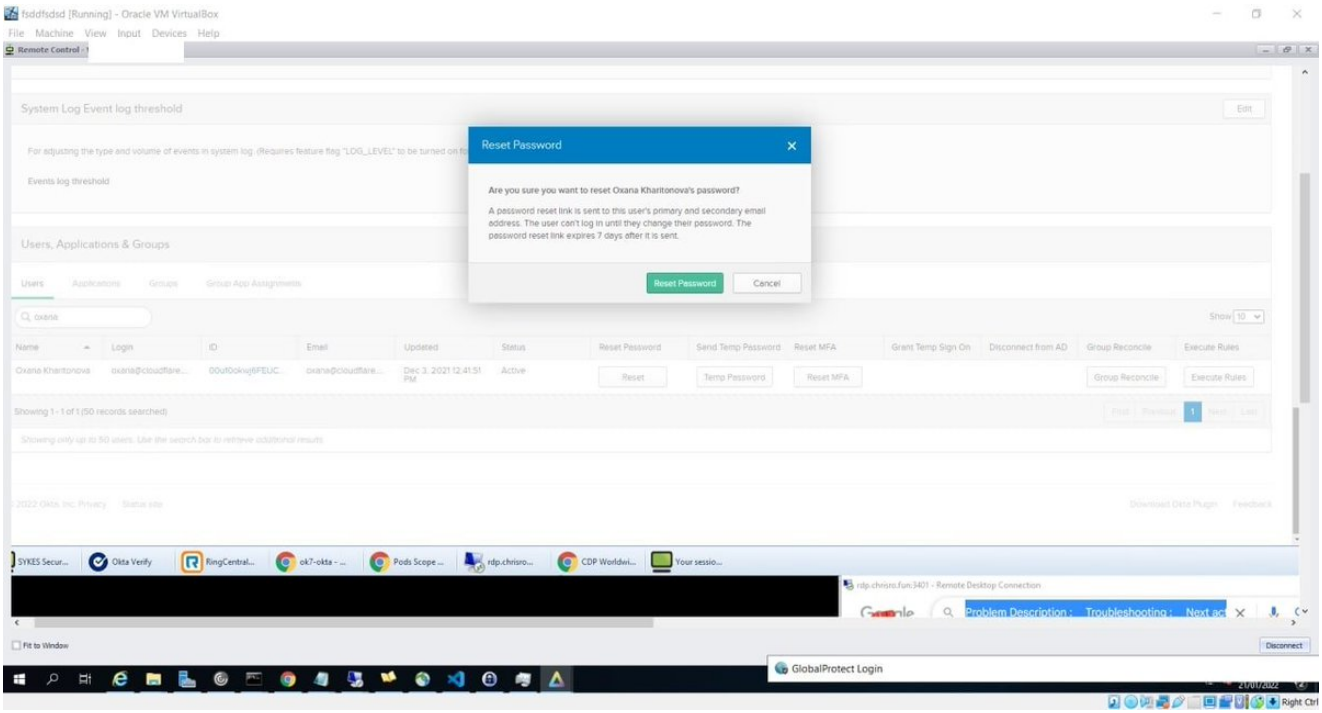
Date (UTC)	Event	Attack Phase
2022-01-16 00:33:23	First logon event from [SYSTEM NAME REDACTED]. Logon to [SYSTEM NAME REDACTED] from [SYSTEM NAME REDACTED] (10.112.137.64)	Initial Compromise
2022-01-19 19:19:47	RDP logon by [ACCOUNT NAME REDACTED] from LOCAL to [SYSTEM NAME REDACTED]	Initial Compromise
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

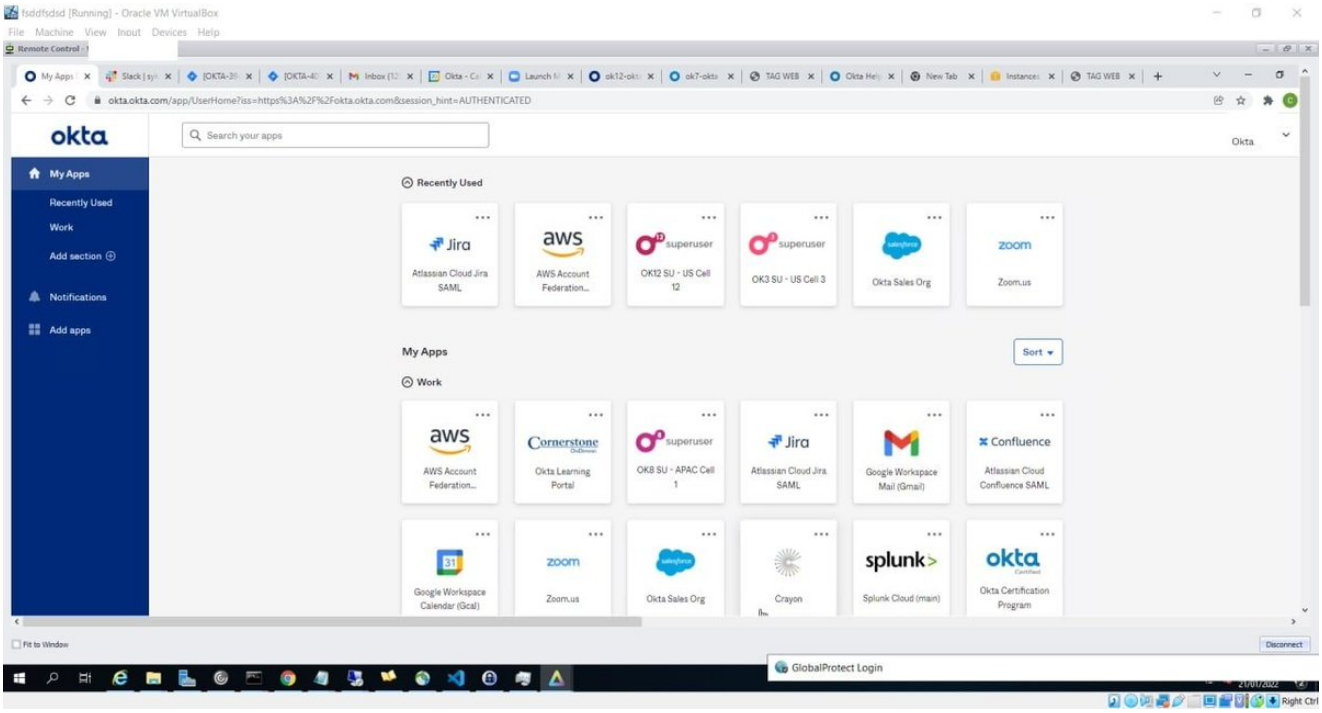
LAPSUS$ was able to create backdoor users in Sitel's environment after retrieving an Excel document conspicuously titled "DomAdmins-LastPass.xlsx" 🤦‍♂️. 5/N

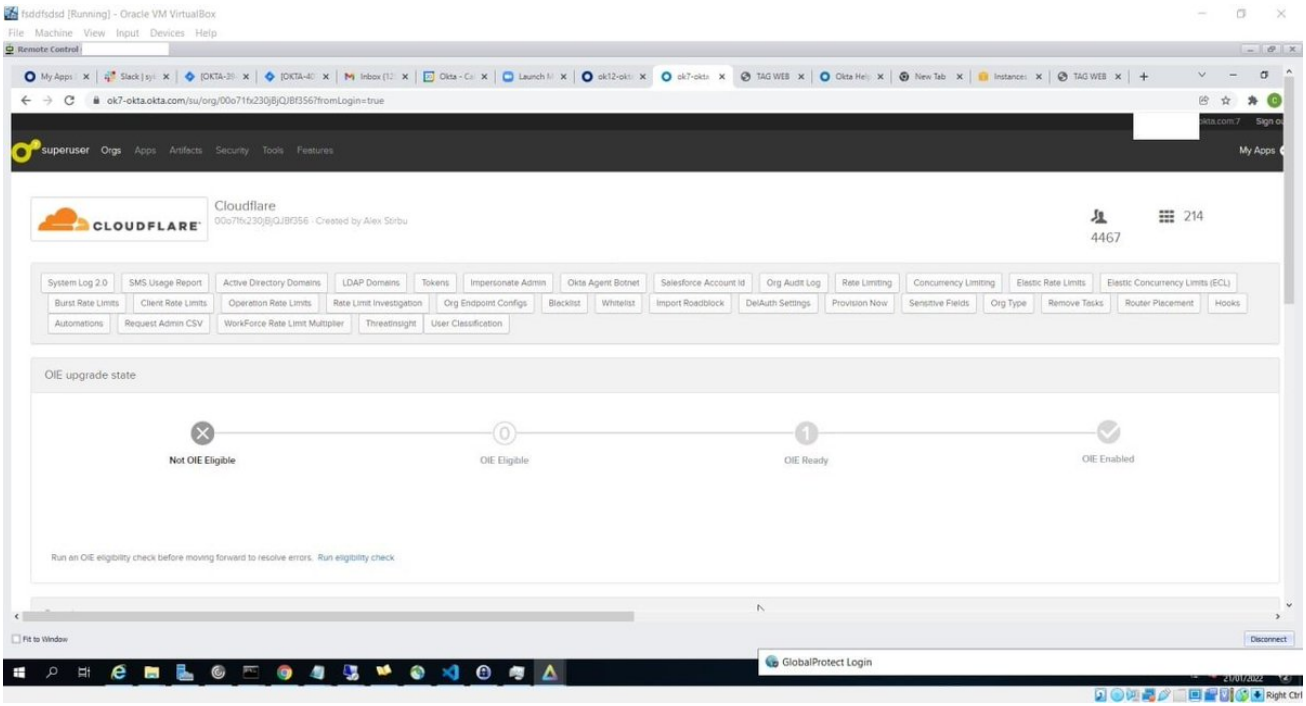
2022-01-20 18:56:00	C:\system.hiv created on [SYSTEM NAME REDACTED]	Escalate Privileges
2022-01-20 18:57:17	C:\Users\[ACCOUNT NAME REDACTED]\Documents\mimikatz_trunk\x64\hash.txt	Escalate Privileges
2022-01-20 18:58:05	hxxps://pastebin.com/7E30i24r by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 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 Foothold
2022-01-21 14:11:38	Last malicious logon by [ACCOUNT NAME REDACTED]@sykes[.]com to O365	Complete Mission

The LAPSUS$ ransomware group has claimed to breach Okta sharing the following images from internal systems.


LAPSUS$
Just some photos from our access to Okta.com Superuser/Admin and various other systems.
For a service that powers authentication systems to many of the largest corporations, I think these security measures are pretty poor.
1 11:09 PM
7 comments


fsddfsdsd [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Remote Control
System Log Event log threshold
Edit
Reset Password
Are you sure you want to reset Oxana Kharitonova's password?
A password reset link is sent to this user's primary and secondary email address. The user can't log in until they change their password. The password reset link expires 7 days after it is sent.
Reset Password
Cancel
Users, Applications & Groups
Users
Applications
Groups
Group App Assignments
oxana
Name
Login
ID
Email
Updated
Status
Reset Password
Send Temp Password
Reset MFA
Grant Temp Sign On
Disconnect from AD
Group Reconcile
Execute Rules
Oxana Kharitonova
oxana@cloudflare...
00ul0okwj6FEUC...
oxana@cloudflare...
Dec 3, 2021 12:41:51 PM
Active
Reset
Temp Password
Reset MFA
Group Reconcile
Execute Rules
Showing 1 - 1 of 1 (50 records searched)
Showing only up to 50 users. Use the search bar to retrieve additional results.
SYKES Secur...
Okta Verify
RingCentral...
ok7-okta - ...
Pods Scope ...
rdp.chrisro...
CDP Worldwi...
Your sessio...
rdp.chrisro.fun:3401 - Remote Desktop Connection
Problem Description : Troubleshooting : Next ac
Fit to Window
Disconnect
GlobalProtect Login
Right Ctrl

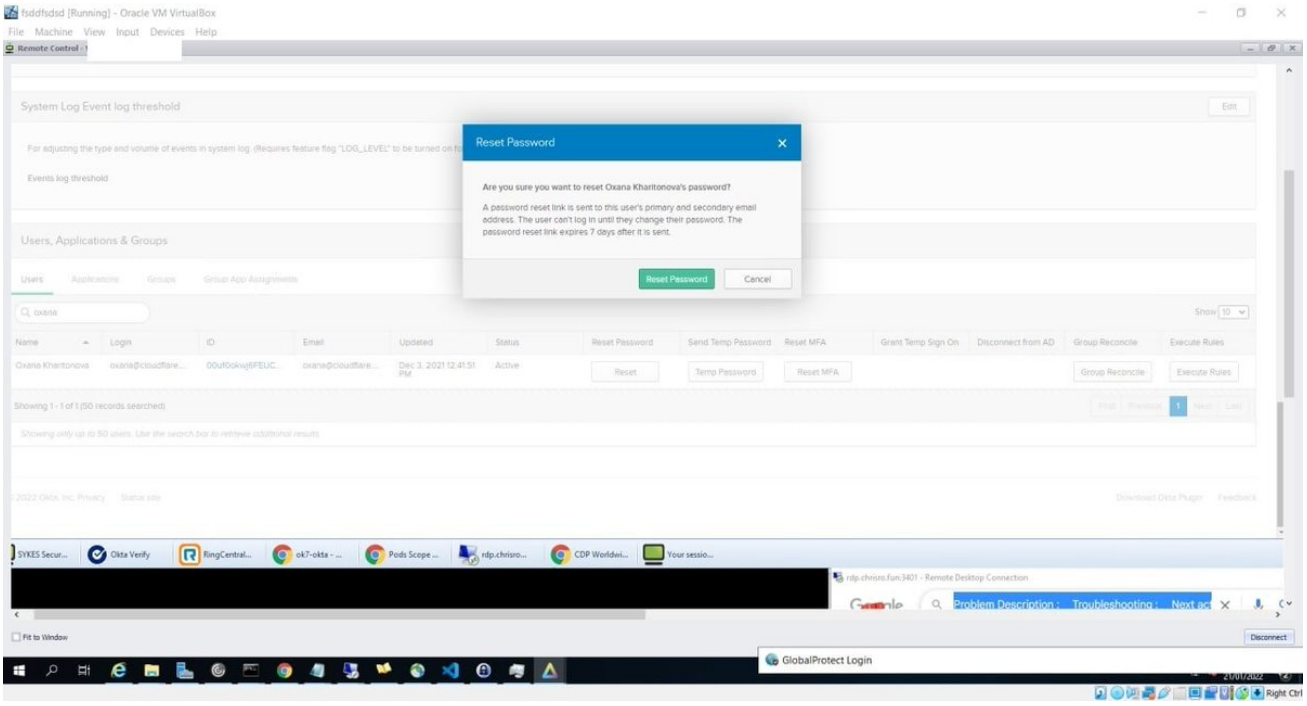

fsddfsdsd [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Remote Control
okta.okta.com/app/UserHome?iss=https%3A%2F%2Fokta.okta.com&session_hint=AUTHENTICATED
okta
Search your apps
Okta
My Apps
Recently Used
Work
Add section
Notifications
Add apps
Recently Used
Atlassian Cloud Jira SAML
AWS Account Federation...
OK12 SU - US Cell 12
OK3 SU - US Cell 3
Okta Sales Org
Zoom.us
My Apps
Sort
Work
AWS Account Federation...
Okta Learning Portal
OK8 SU - APAC Cell 1
Atlassian Cloud Jira SAML
Google Workspace Mail (Gmail)
Atlassian Cloud Confluence SAML
Google Workspace Calendar (Gcal)
Zoom.us
Okta Sales Org
Crayon
Splunk Cloud (main)
Okta Certification Program
Fit to Window
Disconnect
GlobalProtect Login
Right Ctrl

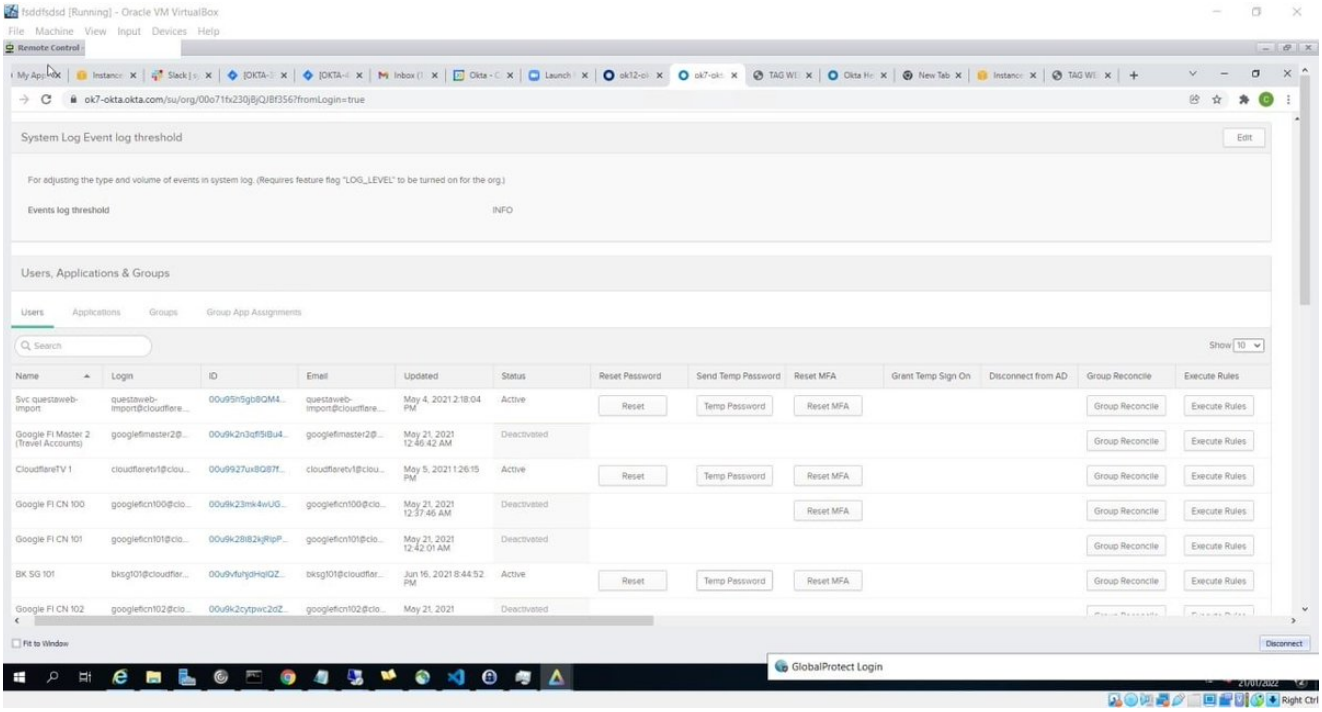


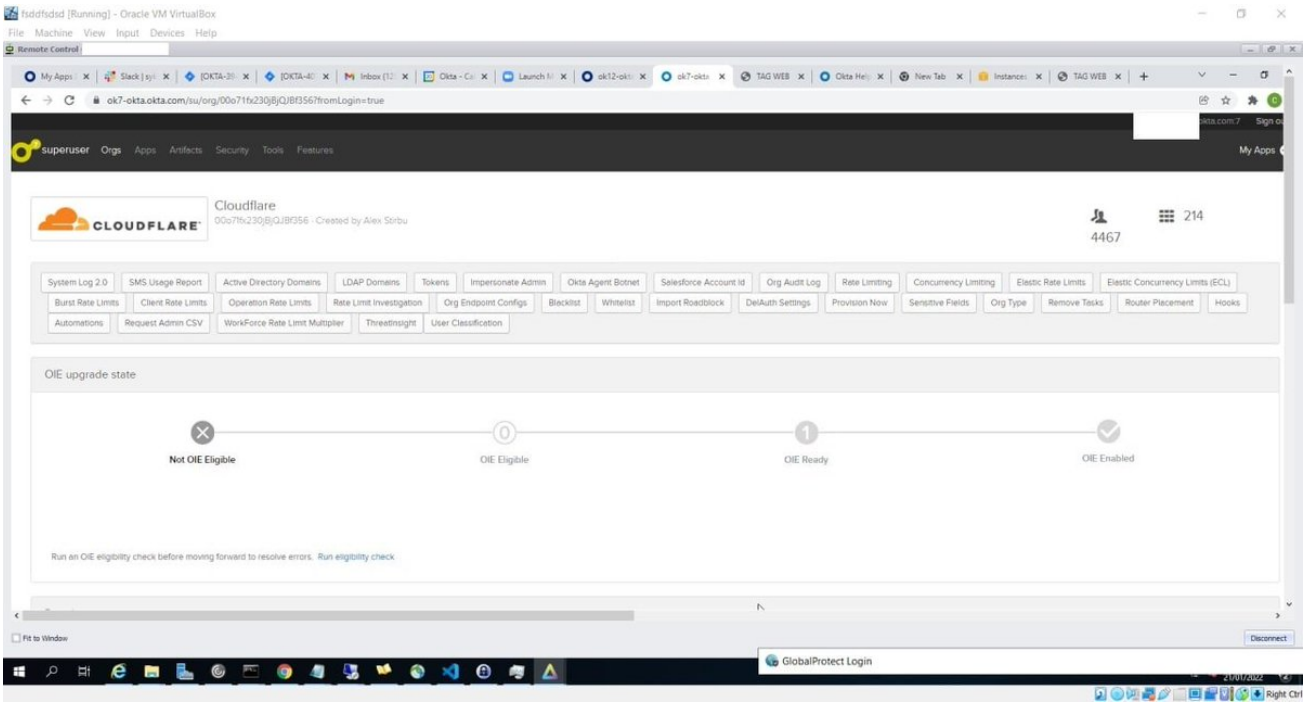
This Thread may be Removed Anytime!

Twitter may remove this content at anytime! Save it as PDF for later use!

The screenshots are very worrisome. In the pictures below, LAPSUS$ appears to have gotten access to the @Cloudflare tenant with the ability to reset employee passwords:







We can see how LAPSUS$ originally began investigating their compromised host on January 19th, 2022. With little regard for OPSEC, LAPSUS$ searched for a CVE-2021-34484 bypass on their compromised host and downloaded the pre-built version from GitHub. 2/N

> https://twitter.com/KLINIX5/status/1451558296872173577

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

Rant about how @Bugcrowd and @Hacker0x01 setup their platforms to let vendors who host private programs abuse researchers. Entirely based on a true story with @Bugcrowd in my case. This is for my #bugbounty friends out there. 1/n

LAPSUS$ finished off their attack by creating a malicious "email transport rule" to forward all mail within Sitel's environment to their own accounts. 6/N docs.microsoft.com/en-

us/exchange…

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 Foothold
2022-01-21 14:11:38	Last malicious logon by [ACCOUNT NAME REDACTED]@sykes[.]com to O365	Complete Mission

New documents for the Okta breach: I have obtained copies of the Mandiant report detailing the embarrassing Sitel/SYKES breach timeline and the methodology of the LAPSUS$ group. 1/N

> https://twitter.com/BillDemirkapi/status/1506107157124722690

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 Foothold
2022-01-21 14:11:38	Last malicious logon by [ACCOUNT NAME REDACTED]@sykes[.]com to O365	Complete Mission

My questions for Okta: You knew that the machine of one of your customer support members was compromised back in January. Why didn't you investigate it? Having the capability to detect an attack is useless if you aren't willing to respond. 7/N

Even when Okta received the Mandiant report in March explicitly detailing the attack, they continued to ignore the obvious signs that their environment was breached until LAPSUS$ shined a spotlight on their inaction. 8/N

For the Sitel Group: Why weren't your customers immediately informed upon the first sign of compromise? Why did your customers have to wait two months to even hear that you were breached? 9/N

Sitel Group serves many more customers than Okta. Often times, for support staff to perform their jobs, they need Administrative privileges into their customer's environment. The attack highlights the increased risk of outsourcing access to your org.'s internal environment. 10/N

Good questions to ask include: Who knows how your sub-processors handle their own security? As we saw in this case, Sitel didn't take the security of their environment very seriously. What can an attacker do if one of your sub-processors becomes compromised? 11/N

Anyone hiring? 😂 12/N

> https://twitter.com/BillDemirkapi/status/1508820739968880640

Would like to clarify some misconceptions I've seen. No, this data is not attorney-client privileged. None of what I shared is from my organization and it was obtained entirely independently. I did not break any NDA/contract. 13/N

• • •