White Paper

Defending Against the LAPSUS$ Playbook with Deception and the Zscaler Zero Trust Exchange

Introduction

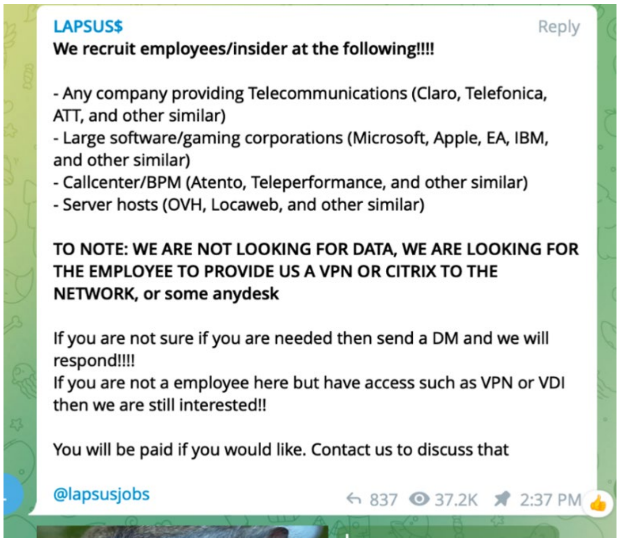
Organizations have embraced multi–factor authentication (MFA) to defend against advanced attacks that use stealthy tactics to bypass defenses. Yet, the LAPSUS$ threat group (a.k.a DEV–0537) has subverted this preventive control using stolen credentials from the dark web and outright buying credentials from employees to compromise identity and use that access to exfiltrate and destroy data while extorting victim organizations.

In this white paper, we look at how sophisticated adversaries use the LAPSUS$ playbook to bypass preventive controls and execute an attack. We then provide guidance on how you can use the Zscaler Zero Trust Exchange—and deception capabilities in particular—to detect such attacks and stop them before they can cause damage.

Deconstructing the LAPSUS$ playbook

LAPSUS$, or DEV-0537, is relentless and methodical in its approach. The threat group invests a lot of time in executing social engineering campaigns to build a detailed picture of its victims. This includes gaining information about employees, organizational hierarchies, and once inside, the organization's crisis response workflows.

Security researchers at Microsoft have observed DEV-0537 and documented some of the TTPs of the group which help us build a picture of its playbook. Here's what that looks like:



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, 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!!

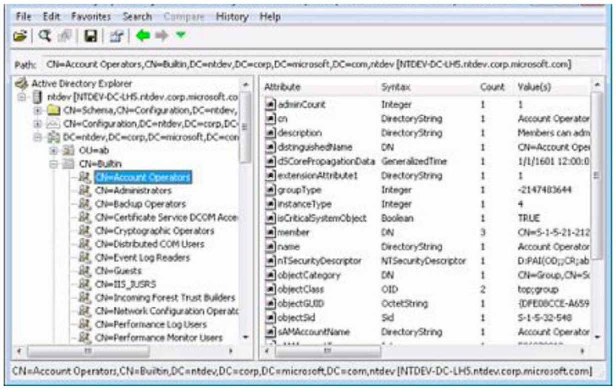
You will be paid if you would like. Contact us to discuss that

@lapsusjobs

837 37.2K 2:37 PM

Initial Access

The LAPSUS$ group uses a variety of tactics to get valid credentials for initial access. These include buying stolen credentials from the dark web, leveraging Redline malware — a password stealer — to procure credentials, and in some cases, purchasing credentials and MFA access from employees of its victims.



Path: CN=Account Operators,CN=Builtin,DC=ntdev,DC=corp,DC=microsoft,DC=com,ntdev [NTDEV-DC-LHS.ntdev.corp.microsoft.com]

Active Directory Explorer
ntdev [NTDEV-DC-LHS.ntdev.corp.microsoft.co
CN=Schema,CN=Configuration,DC=ntdev,
CN=Configuration,DC=ntdev,DC=corp,DC=
DC=ntdev,DC=corp,DC=microsoft,DC=con
OU=ab
CN=Builtin
CN=Account Operators
CN=Administrators
CN=Backup Operators
CN=Certificate Service DCOM Acce
CN=Cryptographic Operators
CN=Distributed COM Users
CN=Event Log Readers
CN=Guests
CN=IIS_IUSRS
CN=Incoming Forest Trust Builders
CN=Network Configuration Operato
CN=Performance Log Users
CN=Performance Monitor Users

Attribute	Syntax	Count	Value(s)
adminCount	Integer	1	1
cn	DirectoryString	1	Account Operator
description	DirectoryString	1	Members can adm
distinguishedName	DN	1	CN=Account Ope
dSCorePropagationData	GeneralizedTime	1	1/1/1601 12:00:0
extensionAttribute1	DirectoryString	1	1
groupType	Integer	1	-2147483644
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	TRUE
member	DN	3	CN=S-1-5-21-212
name	DirectoryString	1	Account Operator
nTSecurityDescriptor	NTSecurityDescriptor	1	D:PAI(OD;;CR;ab
objectCategory	DN	1	CN=Group,CN=S
objectClass	OID	2	top;group
objectGUID	OctetString	1	{DFE0BCCE-A659
objectSid	Sid	1	S-1-5-32-548
sAMAccountName	DirectoryString	1	Account Operator

CN=Account Operators,CN=Builtin,DC=ntdev,DC=corp,DC=microsoft,DC=com,ntdev [NTDEV-DC-LHS.ntdev.corp.microsoft.com]

Internal reconnaissance

Once inside, they use tools like AD explorer to enumerate Active Directory with the objective of finding high-value targets to escalate privileges to.

Privilege Escalation

At this stage of the kill chain, they've been observed to exploit vulnerabilities in collaboration platforms like Confluence, JIRA, and GitLab to get credentials of a privileged account.

Lateral movement

When DEV-0537 owns the desired access level, they move laterally to business applications, information systems, and cloud tenants — their key targets.

Exfiltration and destruction

Once in possession of sensitive information and data, they either delete it or extort the victim organization. As one Microsoft research note observes, "In some cases, DEV-0537 has extorted victims to prevent the release of stolen data, and in others, no extortion attempt was made and DEV-0537 publicly leaked the data they stole."

Kill Chain Phase	Attack Techniques	Zscaler Defense
Initial Access	Uses stolen/purchased credentials to access internet–facing applications like VPNs, RDP, and VDI.	• Reduce your attack surface by hiding applications behind the Zero Trust Exchange so that they are invisible to the internet. • Create decoys of internet–facing applications like VPNs and Citrix servers that attackers are very likely to target. • Extend command–and–control protection to all ports and protocols, including emerging C&C destinations.
Reconnaissance	Uses AD Explorer to enumerate users, computers, and groups.	Create decoy users, user groups, and computers in your Active Directory.
Privilege Escalation	Exploit vulnerabilities in collaboration platforms like Confluence, JIRA, and GitLab to get credentials of a privileged account.	Create decoys of internal apps like Confluence, JIRA, and Gitlab that intercept the use of credentials to access this system.
Privilege Escalation	Uses Mimikatz to extract credentials from memory in Windows. These credentials are then used to access higher privileged accounts.	Plant decoy credentials in Windows memory.
Lateral Movement	Moves laterally to core business applications and cloud environments to gain access to the victim organization's data.	• Prevent exploitation of private applications from compromised users with microsegmentation and full inline inspection of private app traffic. • Plant decoys of internal apps like code repositories, customer databases, business applications, and objects like S3 buckets and AWS keys in your cloud tenants.
Exfiltration	Adversary uses their access to download sensitive data and extort victim.	• Plant decoy files and other sensitive–seeming information on endpoints. • Use data loss prevention to inspect outgoing traffic and evaluate destinations to stop adversaries from stealing sensitive data.

Closing Thoughts

The LAPSUS$ playbook is unique in the sense that it starts from a compromised user. Therefore, the most effective defense against this playbook comprises threat detection approaches that assume breach.

Zero trust and deception strategies both operate on the 'assume breach' principle. Integrated together, they are your most effective defense in instances where an adversary has gained initial access and is now looking to establish a foothold and move laterally.

The Zscaler Zero Trust Exchange is the industry's only security service edge (SSE) platform that features inline application inspection and integrated deception technologies. These features add defense-in-depth to our best-in-class threat prevention and data protection capabilities, maximizing defenses against even the most challenging security threats, such as a compromised user or supply chain attack.

By their very design, deception-based defenses do not trust any user or activity. No one knows that decoys exist in the environment, therefore any interaction with a decoy is a high-confidence indicator of a breach. It doesn't matter how an adversary gained initial access or if they're using AD Explorer to enumerate users or running a scan. A deception alert going off is proof of malicious intent.

This intrinsic high-fidelity, low-false positive property of deception alerts—combined with the threat reduction and mitigation of a layered zero trust defense—make the Zscaler Zero Trust Exchange a pragmatic approach to disrupting the playbooks of LAPSUS$ style threat operators that require rapid response.

Recommendations

- **Initial Access Defense:** Reduce your attack surface by hiding applications behind the Zero Trust Exchange. Plant decoys of vulnerable internet-facing applications like VPN and Citrix servers. LAPSUS$ is known for using these to gain initial access.
- **Stopping Reconnaissance:** LAPSUS$ uses AD Explorer for user enumeration. Protecting Active Directory is extremely difficult. Decoy users, user groups, and computers embedded into your Active Directory are a low-effort approach to detecting and stopping enumeration.
- **Detecting Privilege Escalation:** Deploy decoys of internal apps and lures in system programs like password managers to detect privilege escalation.
- **Stopping Lateral Movement:** Create decoys of business applications like code repositories, customer databases, and servers to intercept the attack and divert it away from the target.
- **Averting exfiltration:** Decoy files detect exfiltration attempts. Data loss prevention inspects outgoing traffic and evaluates destinations to stop adversaries from stealing sensitive data.
- **If you already use ZPA,** configure the conditional access policy to contain attacks and block access to the rest of the environment.

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com