TLP Clear

New attribution challenges

A case study on emerging threat actors

© Intel 471 Inc. 2023

whoami

- Carlos Borges, cyber threat researcher and intelligence analyst.
- About two years and half hunting adversaries.
- Worked in different industries and roles.
- Contributions to open-source projects.

INTEL471

© Intel 471 Inc. 2023

Agenda

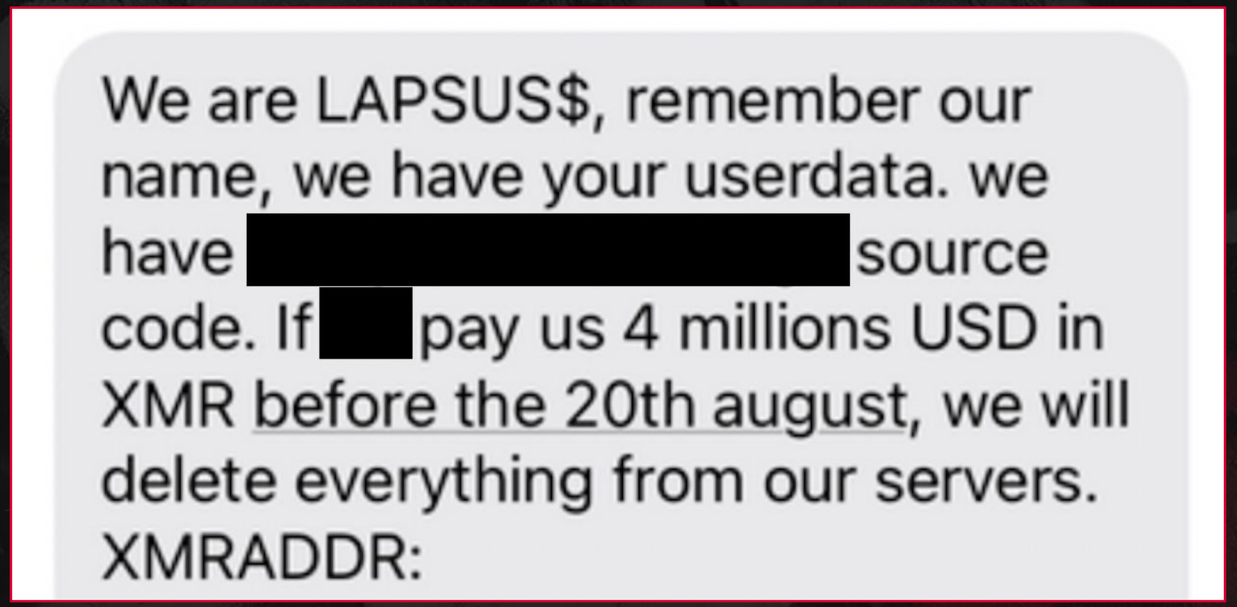
- A quick history about LAPSUS$.
- Campaigns and intrusion clusters.
- Scattered Spider and overlapping clusters.
- What does it matter for us in Brazil?

INTEL471

© Intel 471 Inc. 2023

LAPSUS$

- Breaches impacting Brazilian entities in December 2021.
- The group first appeared about June 2021, but members in the underground operated before that.
- The former self-proclaimed LAPSUS$ leader was a member of another group dubbed “Infinity Recursion”.
- This group specialized in SIM-Swapping and swatting (reporting fake harmful events to trick the police in visiting a target’s address).

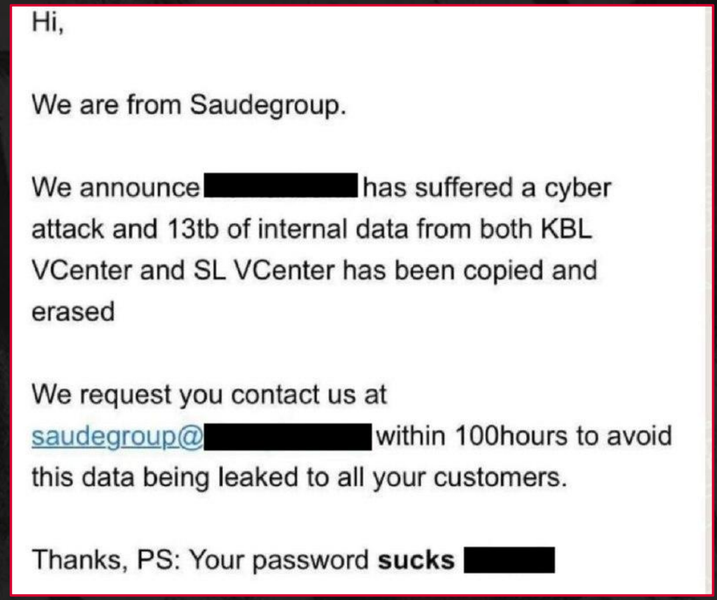


INTEL471

© Intel 471 Inc. 2023

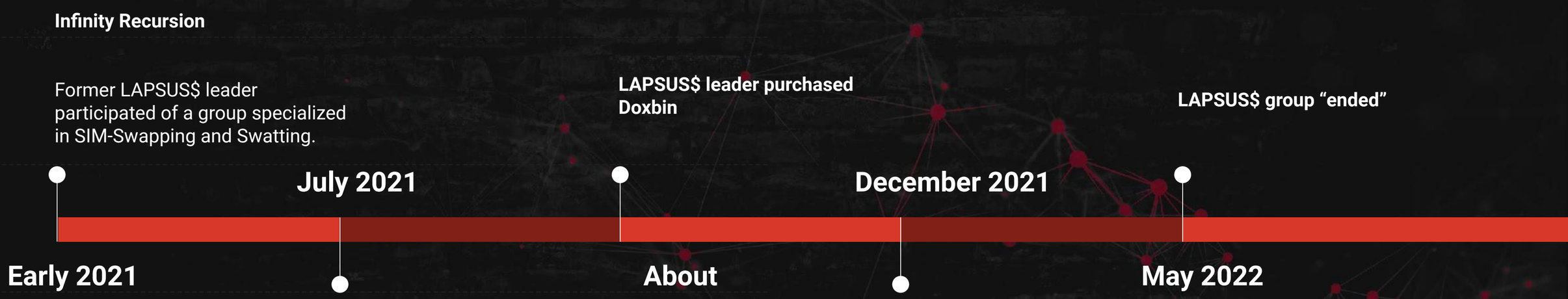
Notable tactics

- Young actors who publicly operated via Telegram.
- Social engineering techniques such as SIM-Swapping, cookies, etc.
- Fast once inside corporate networks and monitored communications.
- Posted offensive messages.
- Okta was one of the victim entities, breached after social engineering a third-party employee working for a BPO provider.



© Intel 471 Inc. 2023

Timeline



© Intel 471 Inc. 2023

Campaigns

> Describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets. Campaigns usually have well defined objectives and may be part of an Intrusion Set.

© Intel 471 Inc. 2023

Intrusion set or cluster

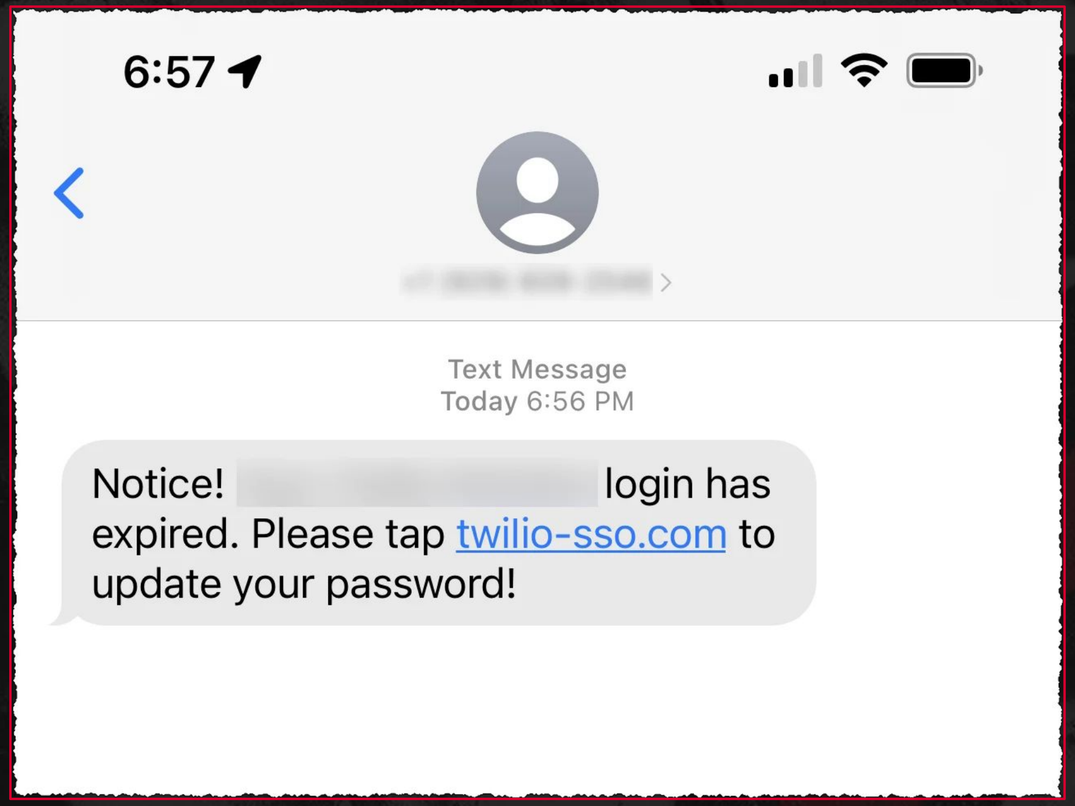
> A grouped set of adversarial behaviors and resources with common properties that is believed to be orchestrated by a single organization. An Intrusion Set may capture multiple Campaigns or other activities that are all tied together by shared attributes indicating a commonly known or unknown Threat Actor.

INTEL471

© Intel 471 Inc. 2023

0ktapus

- Group IB's research alias about a phishing campaign carried by specific actors in the underground about August 2022.
- Targeted customers of identity and access management company Okta.
- Provided details of phishing kits used, stolen login credentials and redacted details of the actors behind it.
- Campaign designed to capture authentication data. Vendors lately published research correlating observed intrusions with 0ktapus.



INTEL471

© Intel 471 Inc. 2023

Scattered Spider

- Crowdstrike’s intrusion cluster with a catchy name sweeps the industry.
- Targeted services providers (BPO), telecommunication and technology companies.
- Reported objectives to perform SIM-Swapping, possibly to compromise cryptocurrency wallets and gain access to other organizations.
- Use of social engineering techniques to impersonate IT staff via phone calls and text messages. Use of remote monitoring and management (RMM) tools.
- Intrusions started about June 2022.

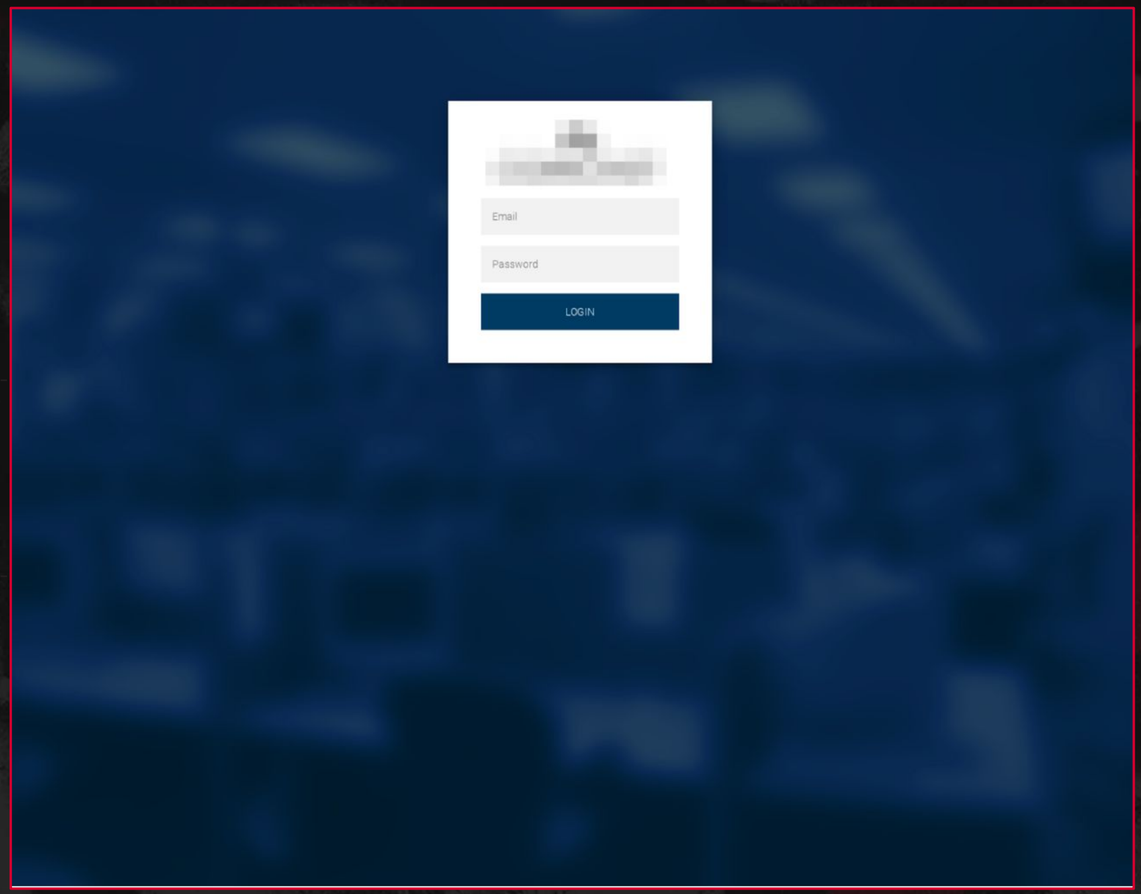
- AnyDesk
- BeAnywhere
- Domotz
- DWservice
- Fixme.it
- Fleetdeck.io
- Itarian Endpoint Manager
- Level.io
- Logmein
- ManageEngine
- N-Able
- Pulseway
- Rport
- Rsocx
- ScreenConnect
- SSH RevShell and RDP Tunnelling via SSH
- Teamviewer
- TrendMicro Basecamp
- Sorillus
- ZeroTier

INTEL471

© Intel 471 Inc. 2023

UNC3944

- Mandiant's intrusion cluster.
- legitimately signed Microsoft drivers were abused as part of a toolkit designed to terminate AV and EDR processes.
- Provided details of phishing kits used in campaigns.
- Intrusions started about March 2022.

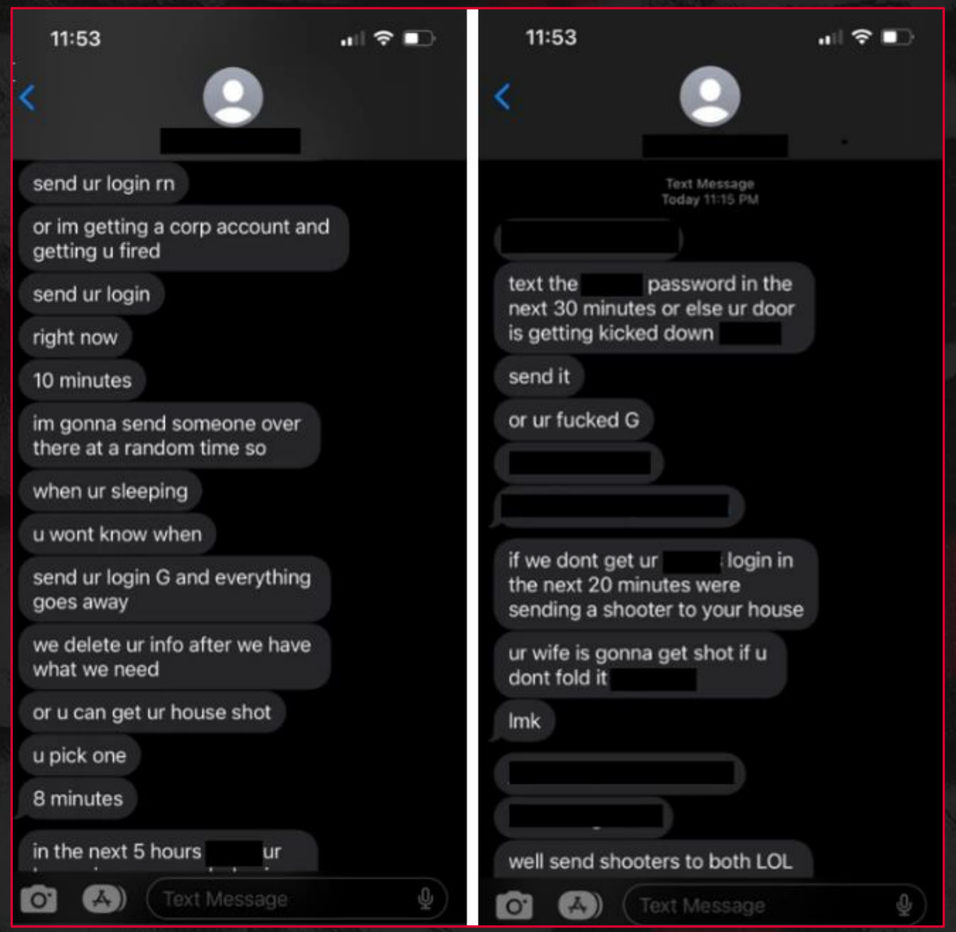


INTEL471

© Intel 471 Inc. 2023

Octo Tempest

- Microsoft's intrusion cluster.
- Evolution from cryptocurrency theft, selling access, extortion and ransomware.
- Indicated affiliation with the AlphV ransomware gang.
- Use of adversary-in-the-middle (AiTM) techniques, social engineering and SIM swapping capabilities.
- Advanced Persistent Teenagers
- Physical threats.



INTEL471

© Intel 471 Inc. 2023

The challenges :)

- Everything is Scattered Spider.

© Intel 471 Inc. 2023

The challenges :)

- Intrusion clusters primary focus is to communicate TTPs rather than the individuals behind it.
- It’s reasonable to talk about a group in the common sense, but semantically speaking intrusions cluster is not a group. Different groups were responsible for breaches replicating similar tradecraft. Actors joined and leave these groups.
- Several other actors are responsible in the attack chain by developing phishing kits, supporting cashout operations, performing typical SIM-Swapping roles such as holders, callers or searchers, etc.
- Companies deeply involved in these investigations reported difficult to track the adversaries due to this dynamic environment where they are operating.
- Clearly communicate overlaps between research.

INTEL471

© Intel 471 Inc. 2023

The Com

- News media outlets published about another “group” dubbed “The Com”.
- This “group” was linked by some sources as the origins of these events.
- There are major and minor groups likely responsible for the breaches.
- The Com is not a specific Discord server nor a Telegram group. It’s a “youth culture phenomenon”.
- Remember LAPSUS$??

INTEL471

© Intel 471 Inc. 2023

Geographically diverse group of individuals, organized in various subgroups, all of whom coordinate through online communication applications such as Discord and Telegram to engage in various types of criminal activity to include corporate intrusions, SIM swapping, cryptocurrency theft, commissioning in real life violence and swatting.

Extracted from a U.S. FBI investigation

INTEL471

© Intel 471 Inc. 2023

Terminology clarification

MONIKERS	ATTRIBUTION TYPE
LAPSUS$	The group's own underground moniker.
0ktapus	Group IB's alias to a campaign operation. Directly associated with specific actors operating in the underground
Scattered Spider, UNC3944, Octo Tempest, Muddled Libra	Crowdstrike, Mandiant, Microsoft and Palo Alto intrusion clusters.
The Com	Reference to "community" and language used by thousands of individuals referring to their culture in communication channels such as Discord, Telegram and forums.
Scatter Swine	Alias given by Okta with details of their internal investigations.

INTEL471

© Intel 471 Inc. 2023

What does it matter for us in BraSil?

- SIM-Swapping attacks (FCC established new rules and last week's Open Gateway announcement).
- SMShing.
- Social engineering and AitM kits.
- Mixing virtual with real world -> Swatting, bricking, shooting.

© Intel 471 Inc. 2023

References

- https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/
- https://www.okta.com/blog/2022/04/okta-concludes-its-investigation-into-the-january-2022-compromise/
- https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_5ol9xlbbnrdn
- https://www.group-ib.com/blog/0ktapus
- https://www.twilio.com/blog/august-2022-social-engineering-attack
- https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/
- https://www.crowdstrike.com/blog/scattered-spider-attempts-to-avoid-detection-with-bring-your-own-vulnerable-driver-tactic/
- https://www.mandiant.com/resources/blog/hunting-attestation-signed-malware
- https://www.mandiant.com/resources/blog/unc3944-sms-phishing-sim-swapping-ransomware
- https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/
- https://www.vice.com/en/article/k7zbma/the-comm-acg-group-linked-to-nationwide-swatting
- https://www.youtube.com/watch?v=2HQoGMG4cWM
- https://www.cisa.gov/news-events/alerts/2023/11/16/fbi-and-cisa-release-advisory-scattered-spider-group
  https://docs.fcc.gov/public/attachments/DOC-398483A1.pdf

INTEL471

© Intel 471 Inc. 2023

Thank you

https://www.linkedin.com/in/carlosavborges

intel471.com