Ransomware Monitoring

Trends and Insights in November-December 2023

18 January 2024

TLP: CLEAR
Disclosure is not limited

Clipeus Intelligence OU
Estonian Business Registration: 16862531
Harju maakond, Tallinn, Kesklinna linnaosa, Ahtri tn 12, 15551

Scope and Methodology

OSINT Monitoring

Data collection via monitoring of leak sites without actor engagement

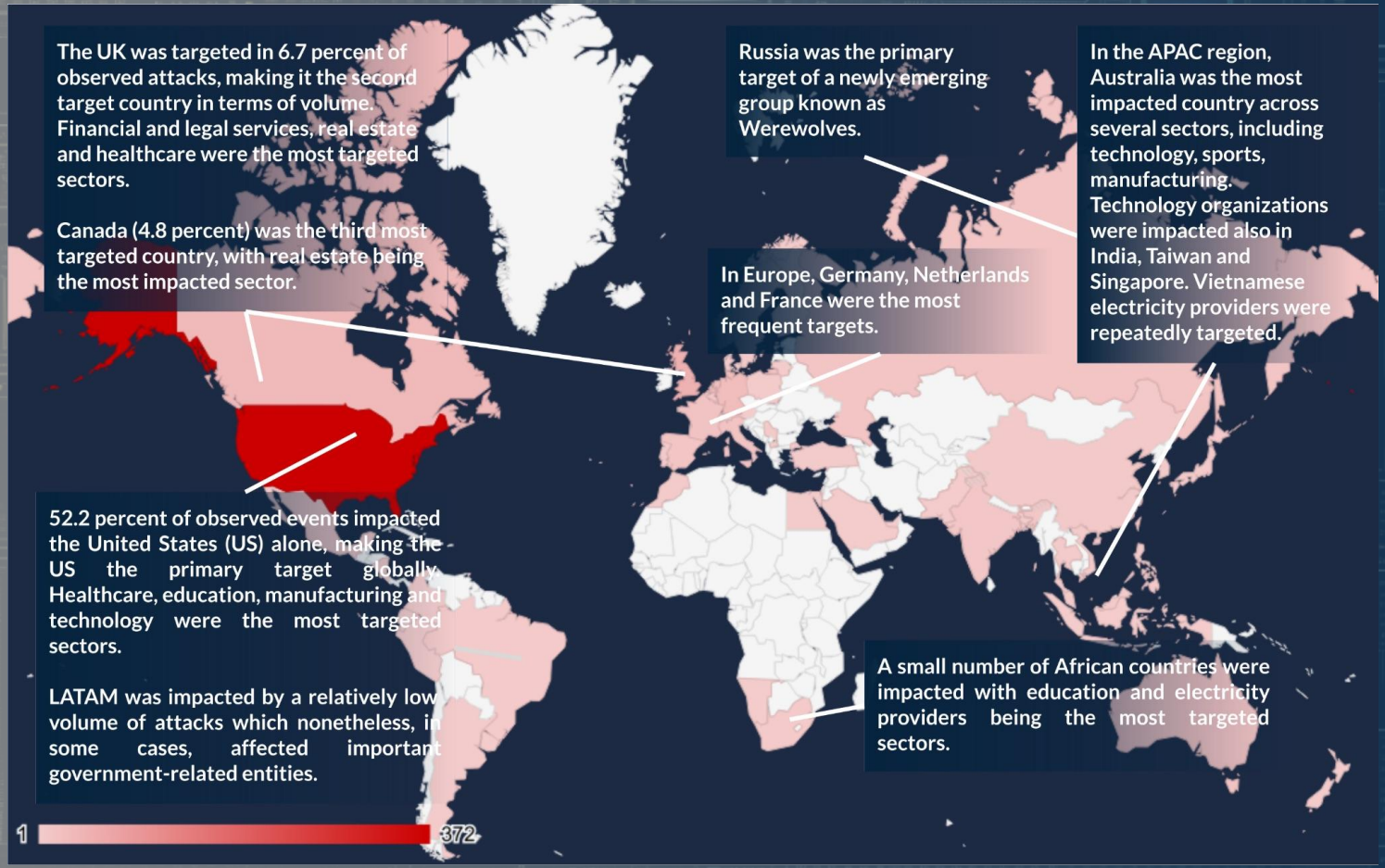
Curated

We collect with automation but validate and enrich data with human intelligence

Time Scope

Our scope goes from November 1, 2023 (when we began our operations) to December 31, 2023

Summary


The UK was targeted in 6.7 percent of observed attacks, making it the second target country in terms of volume. Financial and legal services, real estate and healthcare were the most targeted sectors.
Canada (4.8 percent) was the third most targeted country, with real estate being the most impacted sector.
Russia was the primary target of a newly emerging group known as Werewolves.
In the APAC region, Australia was the most impacted country across several sectors, including technology, sports, manufacturing. Technology organizations were impacted also in India, Taiwan and Singapore. Vietnamese electricity providers were repeatedly targeted.
In Europe, Germany, Netherlands and France were the most frequent targets.
52.2 percent of observed events impacted the United States (US) alone, making the US the primary target globally. Healthcare, education, manufacturing and technology were the most targeted sectors.
LATAM was impacted by a relatively low volume of attacks which nonetheless, in some cases, affected important government-related entities.
A small number of African countries were impacted with education and electricity providers being the most targeted sectors.
1
372

Ransomware Actors

Most Active Ransomware Operations By Volume Of Attacks

Claimed Victims: 152

Claimed Victims: 122

Claimed Victims: 62

Victimology

Monitoring Figures By Impacted Sector

Manufacturing: 75 Events

The industrial sector and manufacturing were globally impacted. Attacks were observed across a wide range of segments, from appliance and machinery manufacturing to food and small consumer goods.

Technology: 67 Events

Technology companies were extensively targeted. Sensitive attacks involved semiconductor companies, as well as developers of software employed by government and digital identity service providers.

Healthcare: 65 Events

Healthcare service providers, including private and state-owned hospitals, pharmaceutical, and diagnostics companies, became a primary target. Data breaches may lead to the leakage of restricted Personally Identifiable Information (PII).

Educational organizations (53 events) and **legal service providers** (32) were also extensively targeted globally with significant potential ramifications in terms of PII leaks.

Critical Infrastructure, Public Services, Government

Public utility services, including healthcare, telecommunications, education, and government, came heavily under attack of ransomware operators for the large amount of data they hold and the sensitivity of their public function, enabling cybercriminals to put significant pressure on the victims.

When it comes to critical infrastructure, telecommunications and government, the raging geopolitical conflicts have an impact on cybercrime. In this respect, ransomware operations became partially instrumental to nation state agendas.

December 10: **LockBit** claimed to have compromised a major branch of the government in a LATAM country

November 29-December 4: **LockBit** and **BlackCat** hit a government-owned organizations of two countries in APAC, including an electricity supplier

December 13: **Akira** claimed the hack of technology companies providing sensitive services to a NAM government

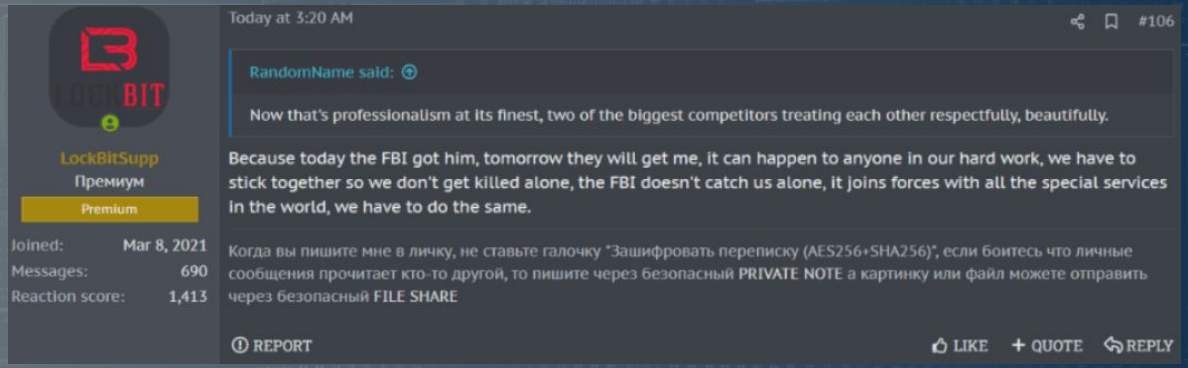
December 13-21: **Akira** claimed the compromise of telecommunication companies in two African countries

Geopolitics and Cybercrime

North America and Western Europe

BlackCat's and LockBit's operations show alignment with Russia, with increased coordination following the US-led seizure of the BlackCat leak site in December 2023.

The coordination raises concerns in the United States and Western Europe, especially regarding public utilities, government, military, and critical infrastructure. BlackCat claimed the hack of a strategic communication provider for Western governments on December 27, supporting this assessment.



Geopolitics and Cybercrime

Russia

A newly Russian-speaking group known as Werewolves has emerged throughout 2023. The actor historically engaged in targeting Russia, Belarus and some Balkan countries such as Serbia and Macedonia.

While intelligence concerning this actor is still limited, there is an apparent anti-Russian focus in their targeting. Werewolves targeted entities in several sectors, including critical infrastructure and telecommunications.

WEREWOLVES
group

Geopolitics and Cybercrime

Middle East

In the Middle East, the Toufan group, believed to be Iran-linked, has consistently targeted Israel during the last two months of 2023. Such events have a clear political connotation.

Impacted organizations include telecommunications, critical infrastructure, government and public utility services.

Cyber Toufan Operations - Backup - سايبر طوفان الأقصى

#IsraelLeaks - Day 27 - Leak #1 –[illegible]td. ([illegible].com) -

#OpCyberToufan #OpIsrael

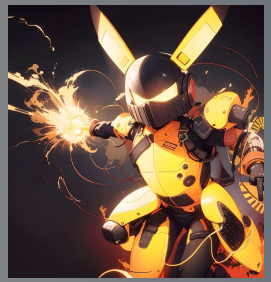
Ransomware and Trojans

Recent Trojan Developments and Ransomware

RATs and backdoors may serve as access brokers for ransomware infection. Particularly in the aftermath of the US-led offensive on the Qbot infrastructure (August 2023), new developments in the trojan landscape have been observed.

8base ransomware operators were observed deploying the Phobos ransomware via Smokeloader and alongside information stealers such as LummaC2 and RedLine.

The Carbanak backdoor resurfaced in November 2023. The malware was observed in conjunction with the deployment of ransomware.



PikaBot has been slowly emerging as a primary alternative to Qbot, paving the way to a potential prospective employment in ransomware infection chain. Yet, in October and early December 2023, there were already indications of a resurgence of Qbot after the August 2023 setback.

The Defense Side

Attack Surface Management

- Ensuring vulnerability and patch management is always crucial to control the attack surface, especially concerning internet-facing assets. During the examined timeframe, cybercriminals were observed targeting specific vulnerabilities as entry points for deploying ransomware.
- "CitrixBleed" (CVE-2023-4966) impacting Citrix NetScaler ADC and NetScaler Gateway was extensively leveraged by LockBit as well as other ransomware operation groups.
- HelloKitty and TellYouThePass targeted Apache ActiveMQ instances vulnerable to CVE-2023-46604.
- Vulnerabilities impacting Qlik Sense (CVE-2023-41266, CVE-2023-41265, and CVE-2023-48365) were chained in attacks related to Cactus ransomware.
- Vulnerabilities such as CVE-2023-34362 (MOVEit) and CVE-2023-27532 (Veeam) have been historically leveraged for ransomware attacks - Cl0p specifically - and require particular attention.

The Defense Side

Security Begins With The User

- User behavior is critical for cybersecurity. Anti-phishing training is essential to protect organizations from ransomware threats. Such efforts help staff to serve as a first line of defense by appropriately handling unusual messages via emails or social media as primary vectors of phishing attacks.
- Enforcement of strong credentials and secure handling of credentials is also critical to reduce the risk of unauthorized access.
- Caution in handling online resources is equally important. NCC Group reports that, beginning in November 2023, new samples of the Carbanak backdoor - also observed in conjunction with ransomware - were distributed via a watering-hole like technique. Cybercriminals set up impersonation sites for popular software such as HubSpot, Veeam and Xero.

The document has been prepared by Clipeus Intelligence based on collection and analysis of open source intelligence and publicly available information. The document has been prepared respecting the criteria of legality and privacy policies presented on the company's website. No engagement with any threat actor was conducted.

Clipeus Intelligence is committed to the betterment of communities and of the security ecosystem. In this spirit, intelligence is always shared with jurisdictionally-competent law enforcement whenever the company encounters information of potential illicit or criminal relevance.

Ransomware victim names were not reported, even if they were already disclosed via press or other online sources. For questions, reach out to info@clipeusintelligence.com, or visit our website www.clipeusintelligence.com.

Clipeus Intelligence OU (registration: 16862531)

Harju maakond, Tallinn, Kesklinna linnaosa, Ahtri tn 12, 15551