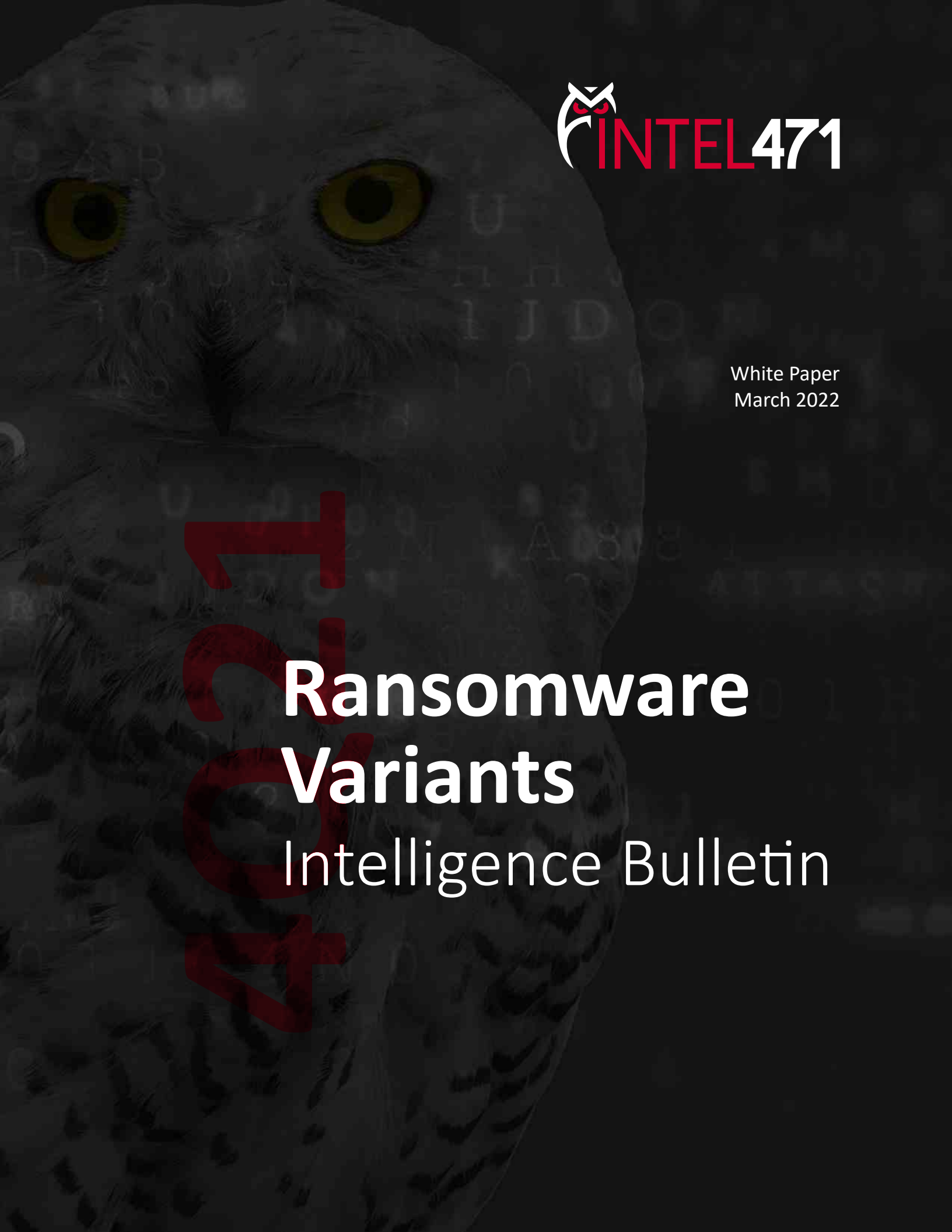


White Paper
March 2022

Ransomware Variants

Intelligence Bulletin

Leading Ransomware Variants for Q4 2021

Key Findings

- **INTEL 471** observed 722 ransomware attacks during the fourth quarter of 2021, an increase of 110 attacks recorded from the third quarter.
- The most prevalent ransomware variants in the fourth quarter of 2021 in descending order were LockBit 2.0, Conti, PYSA and Hive.
- The most-impacted sectors in descending order were consumer and industrial products; manufacturing; professional services and consulting; real estate; life sciences and health care; technology, media and telecommunications; energy, resources and agriculture; public sector; financial services; and nonprofit.
- The most-impacted regions in descending order were North America, Europe, Asia, South America, Oceania, Middle East, Central America and Africa.

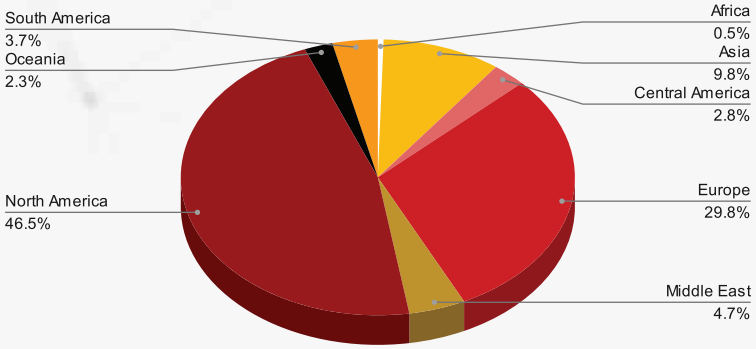
Overview

INTEL 471 reported 34 ransomware variants were used to conduct 722 attacks from October 2021 to December 2021, an increase of 110 and 129 attacks from the third and second quarters of 2021, respectively. The most prevalent ransomware strain in the fourth quarter of 2021 was LockBit 2.0, which was responsible for 29.7% of all reported incidents, followed by Conti at 19%, PYSA at 10.5% and Hive at 10.1%. Other reported variants each accounted for 4.8% or less of the total number of observed ransomware attacks. Intel 471 also captured some initial ransom payment requests sent to victims, of which the average was US $1 million – a drop from our previous report. However, more ransom demands were made public during the fourth quarter of 2021, which increased the number of demands from which the average was taken.

Each recorded ransomware event was sourced from Intel 471 Spot Reports or Breach Reports, which listed impacted entities and domains when available and were tagged with a sector, industry, region and country that aligned to our General Intelligence Requirements (GIR) framework. It is important to highlight that our analysis in this review was based on ransomware variant-related events specifically observed and recorded by Intel 471.

LOCKBIT 2.0

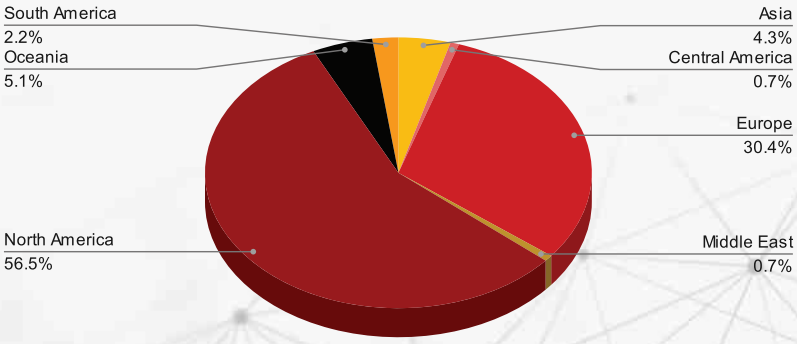
Despite its relatively short period of operation, the LockBit 2.0 ransomware continued to be the most prominent variant in the fourth quarter of 2021. The countries most impacted by LockBit 2.0 from October 2021 to December 2021 in descending order were the U.S. at 41.8% of all recorded LockBit 2.0 attacks, Italy at 6%, Germany at 5.1% and France and Canada at 4% each. LockBit 2.0 allegedly targeted another 39 countries, however, they amounted to less than 2.7% of the total number of ransomware events associated with this variant.



The sectors most impacted by LockBit 2.0 in the fourth quarter of 2021 were consumer and industrial products at 24.6%, followed by professional services and consulting at 22.8%, manufacturing at 16.3% and real estate at 11.6%. The LockBit 2.0 ransomware impacted seven other sectors that equated to less than 6% of the total LockBit 2.0 events. The ransomware also targeted the nonprofit sector, which accounted for 1.8% of LockBit 2.0 attacks and included organizations such as the U.K.-based Educational Recording Agency and the U.S.-based Commission on Economic Opportunity. From the third to fourth quarter of 2021, we observed a slight decrease in the number of attacks that impacted nonprofit organizations. However, analysis of Intel 471 recorded breach events indicated the LockBit 2.0 operators remained relatively consistent in targeting this sector over time.

CONTI

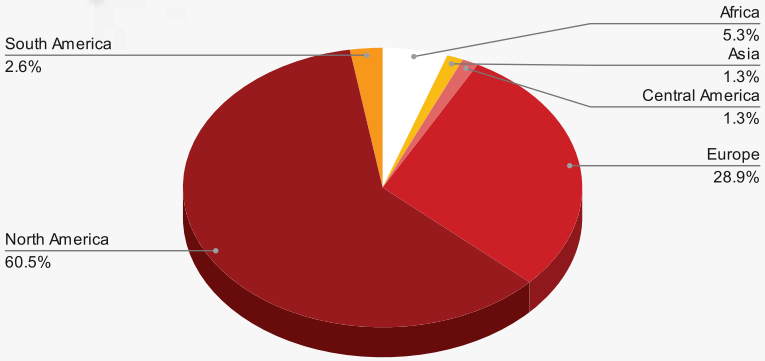
Conti ransomware was the only variant we reported on in all of our published 2021 quarterly ransomware reports. It was the most deployed variant in the second quarter of 2021, dropped to second place in the third quarter of 2021 and remained in second place in the fourth quarter of 2021 but we observed a 48.4% increase in the number of attacks. Countries most impacted by Conti from October 2021 to December 2021 included the U.S. at 50.7% of all recorded Conti attacks, Germany at 8.6%, Italy at 7.2% and Canada and Australia at 5% each. Conti also impacted another 19 locations, each amounting to less than 4% of the total number of Conti incidents. The ransomware variant allegedly was used to target the consumer and industrial products sector in 26.81% of Conti attacks, followed by the manufacturing sector in 21.7%, the professional services and consulting sector in 14.5% and the real estate sector in 9.4%. Other sectors accounted for 7% or less of ransomware events associated with Conti.



During the fourth quarter of 2021, the Conti ransomware gang allegedly compromised the U.S.-based photography products and image sharing company Shutterfly Inc. with a revenue of US $1.96 billion. The attackers allegedly encrypted about 4,000 systems, exfiltrated about 200 GB of sensitive data, shared a complete list of stolen data with Shutterfly as proof of the claim and demanded US $50 million in ransom. The ransomware group also targeted the Australia-based electricity company CS Energy Ltd. with a revenue of US $837.86 million. Looking only at these two named targets that each reported a high revenue, it is likely operators and/or affiliates of Conti ransomware are selective when deciding who to target.

PYSA

PYSA aka “Protect Your System, Amigo” first was observed in December 2019 and is thought to be a version of the Mespinoza ransomware. The sector most impacted by PYSA in the fourth quarter of 2021 was the public sector at 22.4% of all reported PYSA attacks. This included organizations such as South Africa’s Department of Justice and Constitutional Development, the U.S. city Bridgeport, Connecticut, and the U.K.-based Kent County Council. The second most-impacted sectors were consumer and industrial products and life sciences and health care at 17.1% each. The other six sectors accounted for 10% or less of all observed PYSA attacks. The U.S. was the most-impacted country, accounting for 59.2% of all PYSA events reported, followed by the U.K. at 13.1% and then 16 other countries that amounted to nearly 3% each. The marginal difference in the total number of breached entities in the U.S. compared to other countries indicates the U.S. likely was a primary target for attackers leveraging PYSA ransomware.



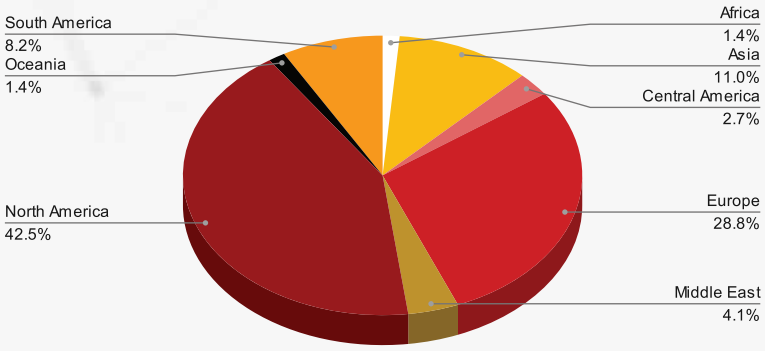
We reported a notable increase of about 22 PYSA attacks from the second to third quarter of 2021. Our analysis for the fourth quarter of 2021 revealed an increase in attacks of about 81% since the second quarter of 2021. From this data, we concluded PYSA was the third most prevalent ransomware strain for the fourth quarter of 2021. When it comes to industries and sectors targeted, questions have been raised regarding the attack ethics of PYSA’s operators. In addition to largely impacting the public sector, attackers leveraging this variant targeted several entities classified as health care providers and services. From October 2021 to December 2021, PYSA ransomware allegedly impacted the Nevada, U.S.-based Las Vegas Cancer Center, the Florida, U.S.-based Ocean View Nursing & Rehabilitation Center, the U.S.-based Florida Heart Associates Pll and the Florida, U.S.-based Electronic Healthcare Systems Inc. This pattern of activity suggests PYSA operators possibly are motivated by disrupting critical services as opposed to targeting large corporate entities for maximum profit.

Methods of delivery, initial access

The PYSA ransomware used a custom Golang proxy binary dubbed ChaChi or Gasket during the course of an infection, which leveraged the domain name system (DNS) communication routine of the Chashell open source tool. This binary had the ability to open a socket secure internet protocol (SOCKS5) proxy or open and execute the Chisel open source tool, which would serve as a transmission control protocol (TCP)-user datagram protocol (UDP) tunnelling application and allow PYSA to execute and exfiltrate data stealthily. The proxy binary and Chisel tool were obfuscated using the open source “gobfuscate” Golang obfuscation tool. Analysis of these tools is fairly challenging and time-consuming since all strings are obfuscated, however, it does make a good identification for Yara rules.

The actual binary PYSA used was observed as an executable ([.]exe) and Python compiled file ([.]pyz).[1] The Python file is relatively simplistic and consists of only 108 lines of code. The run[.]py script contains the following string which will be written to a ransom note: Every byte on your ESXi has been encrypted. This suggests that VMWare ESXi hypervisors were specifically targeted using a Python-based ransomware script. PYSA ransomware uses the extension [.]pysa for infections and the operators ask that victims contact the team via email.

During the fourth quarter of 2021, the sectors most impacted by Hive ransomware were life sciences and health care at 24.6% of all recorded Hive attacks, followed by consumer and industrial products at 20.5%, manufacturing at 13.7% and professional services and consulting at 10.9%. Entities that fell within the other six sectors accounted for less than 6% of all Hive instances. The U.S. remained the most-impacted country in the fourth quarter of 2021 at about 35.6% of all reported Hive attacks. The ransomware variant also was associated with breaches that impacted the U.K., however, it dropped in the overall ranking of impacted countries at 4.1% of recorded Hive events. This was because Hive instances targeting Canada, Italy and Spain increased by 6%, taking them to 6.8% each.



Industries impacted by Hive ransomware included the health care providers and services industry, which equated to 20.5% of attacks from October 2021 to December 2021. We observed a high-profile Hive ransomware attack in the fourth quarter of 2021 against the Italy-based local health care organization Azienda ULSS n. 7 Pedemontana. Hive operators demanded US $3.5 million and shared a complete listing of files exfiltrated from Azienda as proof of the claim. Attackers leveraging the Hive ransomware also targeted the Illinois, U.S.-based Family Christian Health Center with a revenue of US $13.35 million and demanded a ransom of US $600,000. These ransom amounts were large compared to other requests across impacted organizations in the health care industry.

Figure 1: This graphic displays the percentage of variant-specific events per impacted region for the top four most active.

SUMMARY

Ransomware attacks observed in the fourth quarter of 2021 indicated the variants collectively targeted about 234 organizations in October 2021, about 283 in November 2021 and about 205 in December 2021. LockBit 2.0 remained the most impactful ransomware service in the fourth quarter with about 215 attacks. This was only a slight increase of about 5.91% from the third quarter. Following LockBit 2.0, 138 attacks were associated with Conti, about 76 with PYSA and about 73 with Hive. LockBit 2.0 averaged about two attacks per day, while Conti averaged about one per day – the same trend we observed in the third quarter. The least active variants observed were FiveHands, Haron, Payload[.]bin and Thanos, averaging four attacks total from October 2021 to December 2021.

Ransomware Variant Leaders Q4 2021 vs. Q3 2021 Position	
LockBit 2.0 —	Q3 position 1, Q4 same
Conti —	Q3 position 2, Q4 same
PYSA ↑	Q3 position 5, Q4 up 2
Hive —	Q3 position 4, Q4 same

Table 1: This table shows the change in ransomware variant ranks by number of attacks from the third to fourth quarter of 2021.
*Note: These rankings are for illustrative purposes only and the assessment is made from Intel 471 data only.

Attacks impacting the consumer and industrial products sector rose by 22.2% from the third quarter of 2021, making it the most-impacted sector during the fourth quarter. The second most-impacted sector from October 2021 to December 2021 was manufacturing, followed by professional services and consulting. These sectors also were in the top three spots in varying positions for the second and third quarters, indicating no significant difference in the primary impacted sectors over the course of 2021.

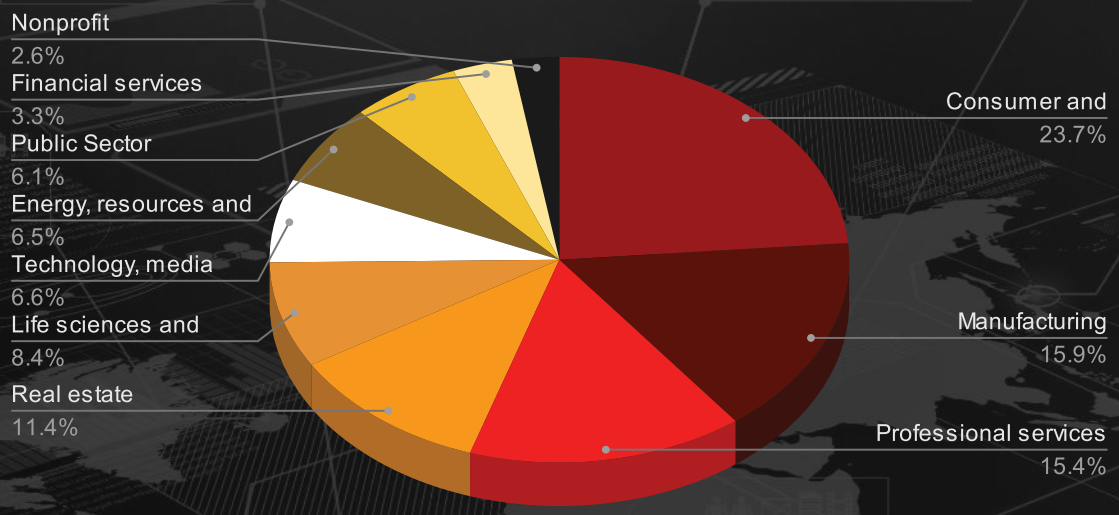


Figure 2: This chart shows a breakdown of sectors and percentage of ransomware attacks observed in the fourth quarter of 2021.

Ransomware operators maintained their pervasiveness during this quarter, including the operators of BlackByte and RagnarLocker, as we noted an increase in the number of attacks associated with each service. However, in the fourth quarter of 2021, we also observed the number of attacks associated with Everest ransomware decreased by nine and the operators and/or affiliates of the service only advertised breach events for four organizations in December 2021.

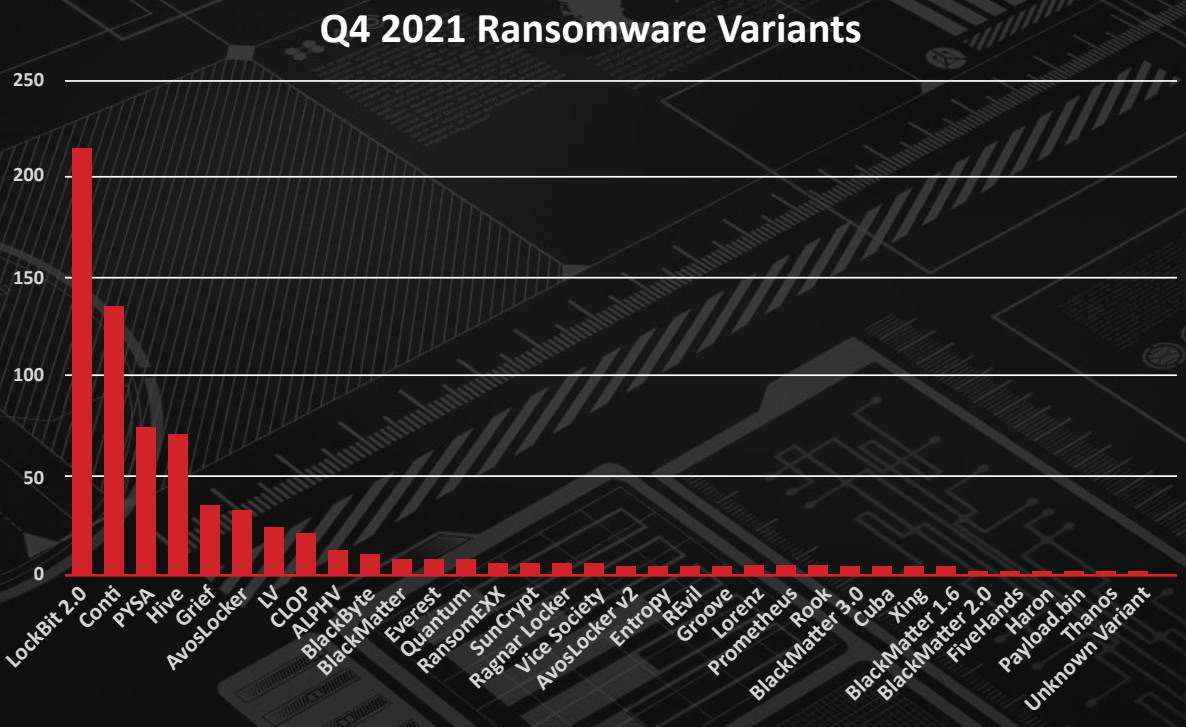


Figure 3: The graph depicts the total number of ransomware events per variant in the fourth quarter of 2021.

The most-impacted region in the fourth quarter of 2021 was North America, amounting to about 52.2% of all reported attacks, followed by Europe at 28.4% and Asia at 8.4%. The number of entities impacted in these regions did not change the leading placement from the previous quarter and likely will not change for the first quarter of 2022. The least-targeted sectors for the fourth quarter of 2021 were the nonprofit and financial services sectors, which was the same placement we observed in the third quarter of 2021.

Ransomware Attacks Per Sector Q4 2021 vs. Q3 2021	
Consumer and industrial products	↑ Up 42
Manufacturing	↓ Down 14
Professional services and consulting	— Same
Real estate	↑ Up 15
Life sciences and health care	↑ Up 27
Technology, media and telecommunications	↓ Down 3
Energy, resources and agriculture	↑ Up 9
Public	↑ Up 13
Financial services	— Same
Nonprofit	↑ Up 11

Table 2: This table depicts the change in ransomware attacks per sector from the third to fourth quarter of 2021.
*Note: These rankings are for illustrative purposes only and the assessment is made from Intel 471 data only.

Although many similarities from the previous quarter were observed in the fourth quarter of 2021, there also were some significant differences. In the third quarter, BlackMatter ransomware was in the top three most prevalent ransomware variants, accounting for 6.9% of all reported ransomware incidents from July 2021 to September 2021. By the fourth quarter, our analysis of attacks attributed to any versions of BlackMatter only accounted for 1.8% of all reported attacks. In early November 2021, we reported the personas affiliated with BlackMatter on the Exploit and XSS underground forums were deactivated and all post threads and individual posts associated with them were deleted. Then, on Nov. 5, 2021, the BlackMatter victim shaming blog and website used for communication with victims went offline. This occurred shortly after the release of BlackMatter 3.0. There is a realistic possibility these events could be due to a fear of law enforcement intervention.

Observations from this report should be seen as an overview of activity highlighted across individual breach events that were correlated to a specific ransomware strain. They are not categorized at the service operator or affiliate level, which would be difficult to ascertain based on information available in breach notifications.

General Intelligence Requirements

1.1.1 Ransomware malware
1.2.2 Ransomware-as-a-service (RaaS)
4.2.3 Compromised personally identifiable information (PII)
4.2.4 Compromised Intellectual Property (IP)
4.2.5 Compromised network or system access
6.1.1 Consumer and industrial products sector
6.1.2 Energy, resources and agriculture sector
6.1.3 Financial services sector
6.1.4 Life sciences and health care sector
6.1.5 Manufacturing sector
6.1.6 Public sector
6.1.7 Real estate sector
6.1.8 Technology, media and telecommunications sector
6.1.9 Professional services and consulting sector
6.1.10 Nonprofit sector
6.2 All geographic regions

Source

[1] 01April2020 CERT FR: Attacks Involving the Mespinoza/PYSA Ransomware
Hxxps[:]//www[.]cert[.]ssi[.]gouv[.]fr/uploads/CERTFR-2020-CTI-003[.]pdf