LockBit, Conti, and BlackCat Lead Pack Amid Rise in Active RaaS and Extortion Groups: Ransomware in Q1 2022

trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022

Ransomware actors were off to a running start in 2022, ramping up their activity as more gangs joined the fray. Using data from ransomware-as-a-service (RaaS) and extortion groups' leak sites, Trend Micro's open-source intelligence (OSINT) research, and the Trend Micro™ Smart Protection Network™, we mapped out the ransomware threat landscape of the first quarter (from Jan. 1 to March 31) of 2022. We tracked ransomware activity with a focus on the malicious actor groups behind the three ransomware families that pulled in the highest numbers of successful attacks during this period: the notorious LockBit and Conti, and the rising player BlackCat.

Ransomware threats post year-on-year growth

Our telemetry showed that during this three-month span, we detected and blocked a total of 4,439,903 ransomware threats across email, URL, and file layers. This is a 36.6% increase in overall ransomware threats from the previous quarter (the fourth quarter of 2021), and a

4.3% year-on-year rise (from the first quarter of 2021).

The number of RaaS and extortion groups grew by 63.2% in the first quarter of 2022 over the same period the previous year, an increase that inevitably led to more organizations falling prey to ransomware activity. According to the ransomware groups’ leak sites, which recorded attacks on successfully compromised organizations that refused to pay the ransom, ransomware victims rose by 29.2% year-on-year.

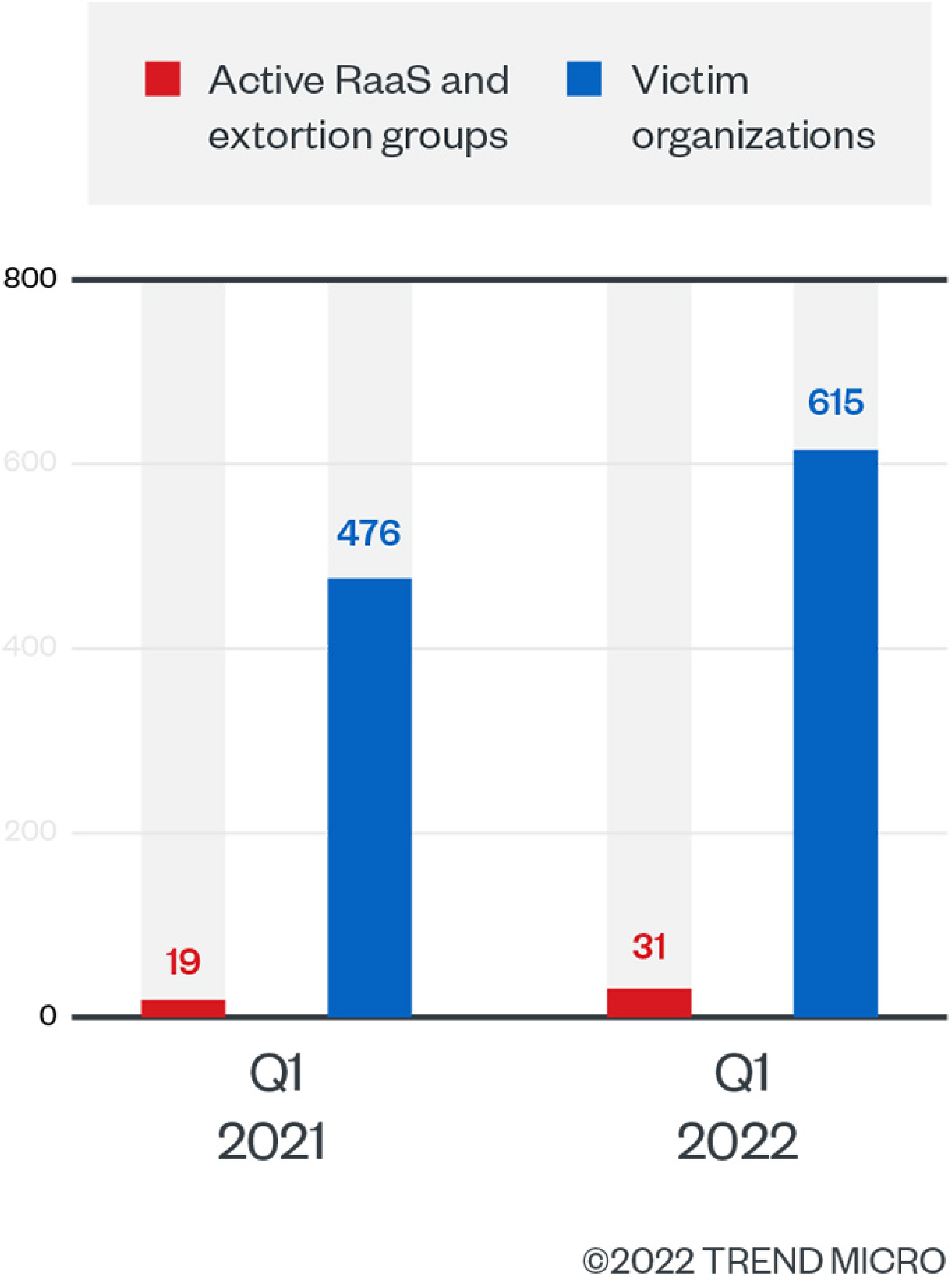


Figure 1. The numbers of active RaaS and extortion groups and of victim organizations of successful ransomware attacks in the first quarter of 2021 and the first quarter of 2022
Source: RaaS and extortion groups' leak sites

LockBit, Conti, and BlackCat's for-hire attacks prevail

The three ransomware families that laid claim to the highest numbers of successful attacks in the first quarter of 2022 were all widely known for operating under the RaaS model. Based on data from the leak sites of their operators, 35.8% of these attacks were attributed to LockBit, while 19% belonged to Conti and 9.6% to BlackCat.

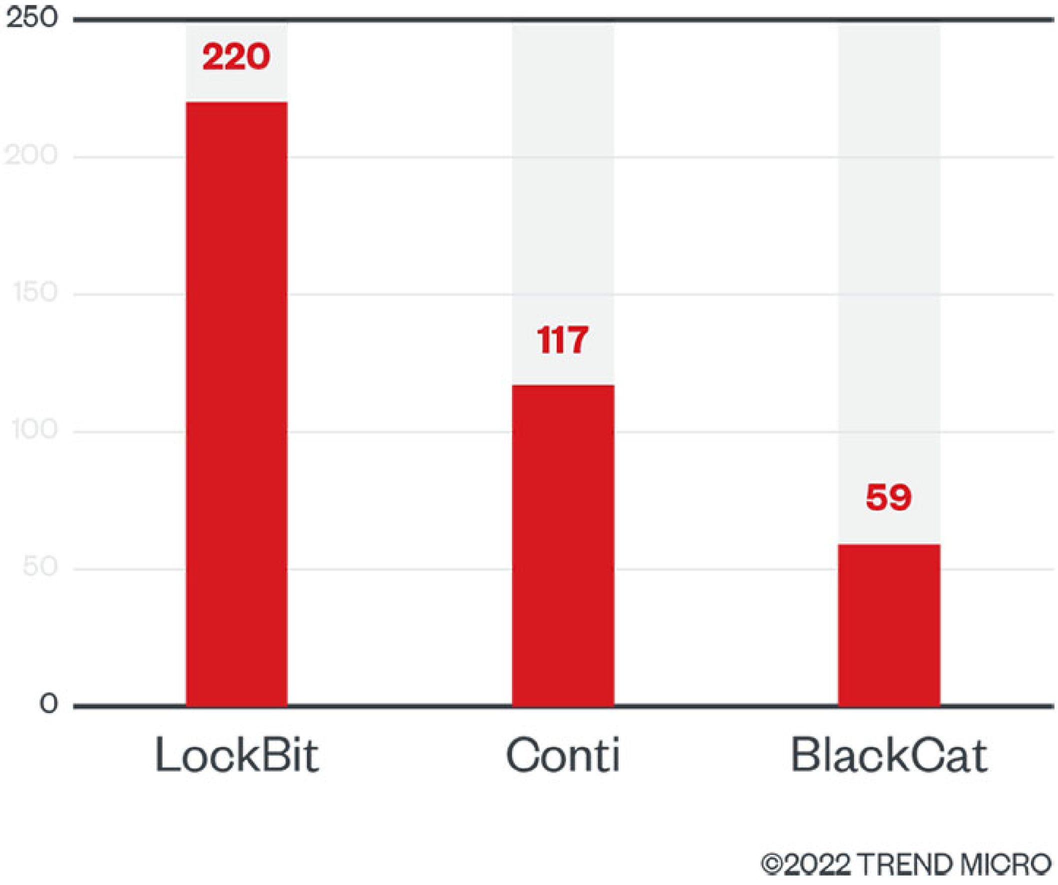


Figure 2. The top three ransomware families used in successful RaaS and extortion attacks in terms of victim organizations in the first quarter of 2022
Source: RaaS and extortion groups' leak sites

Based on our ransomware data, which tracked detections of ransomware attempts to compromise organizations, LockBit and Conti were among the top 10 families detected in the entire first quarter of 2022. Meanwhile, BlackCat was among the top 10 ransomware families detected in February and March 2022.

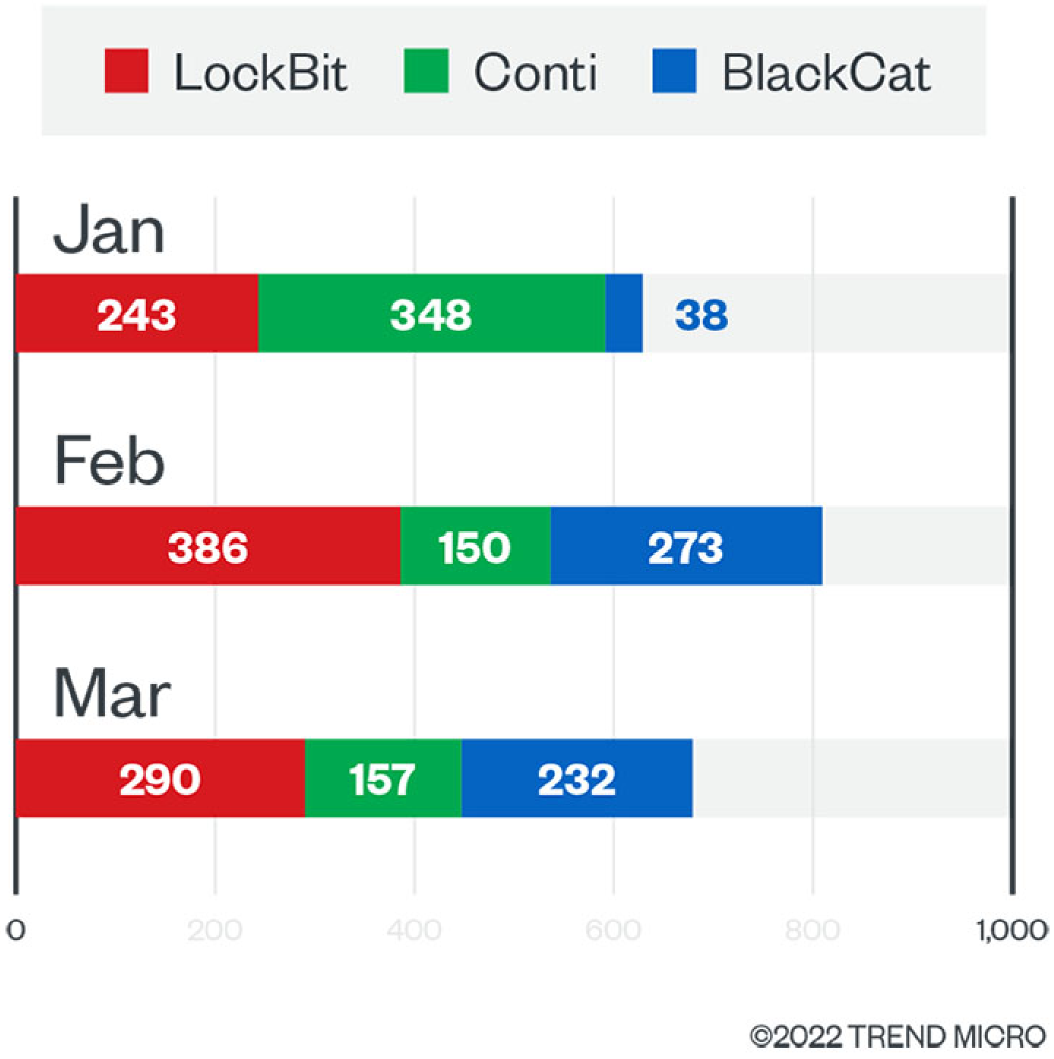


Figure 3. The numbers of ransomware file detections of LockBit, Conti, and BlackCat in machines in each month of the first quarter of 2022
Source: Trend Micro™ Smart Protection Network™

Of the three, only Conti was among the top active ransomware families in the first quarter of 2021, based on RaaS and extortion groups' leak sites. In fact, Conti was first among them in that period, racking up a victim count of 105. The Federal Bureau of Investigation (FBI) estimates that the group behind Conti, which Trend Micro tracks as Water Goblin, has amassed more than 1,000 victims and payouts amounting to over US$150 million as of January 2022, making it one of the costliest ransomware families ever documented.

RaaS providers like LockBit, detections of which were at their highest in the first quarter of 2022 in February, have become an even more formidable threat since incorporating double extortion in their playbooks. Under double extortion, ransomware actors not only encrypt their victims' data and demand payment in exchange for restoration of access, but they also put additional pressure on victims by threatening to release the data if the ransom is not paid. LockBit operators relied on this tactic after they took credit for an attack on France's Ministry of Justice in January 2022, threatening to publish sensitive ministry data on the dark web upon failure of payment.

Relative to Conti and LockBit, BlackCat (aka AlphaVM, AlphaV, or ALPHV) is a newcomer; it was first reported in November 2021 by researchers from MalwareHunterTeam. But what sets it apart from many other RaaS operators is its use of triple extortion, a tactic where ransomware actors threaten to launch distributed denial-of-service (DDoS) attacks on their victims' infrastructure on top of leaking their data unless the ransom is paid. BlackCat demands millions of US dollars in bitcoin or monero from its victims. It is shaping up to be a major contender in the underground marketplace, thanks to its generous payouts to its RaaS affiliates, who can earn as much as 90% of paid ransoms.

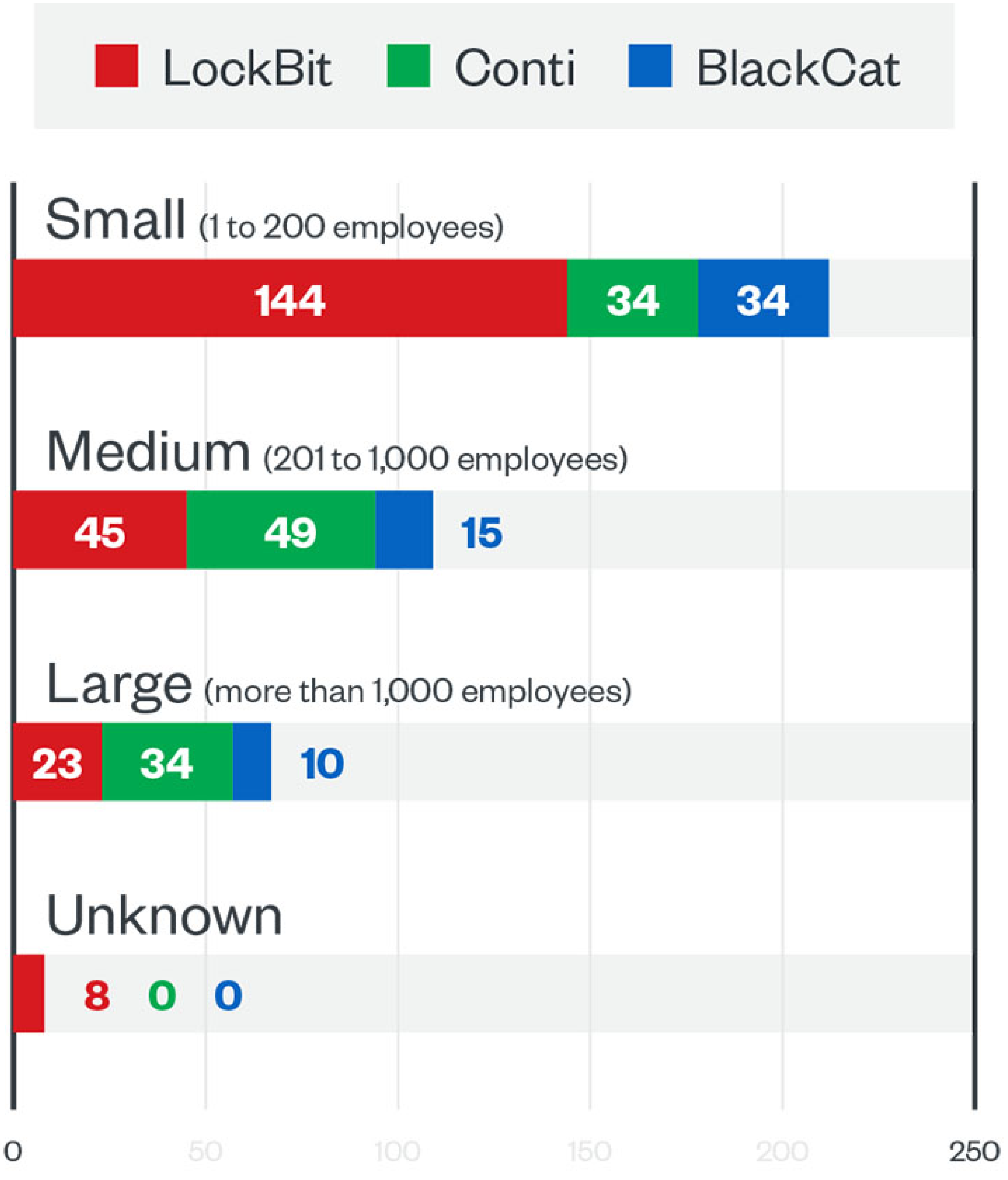
BlackCat, which our detections showed was most active in the first quarter of 2022 in February, has successfully compromised at least 60 organizations around the world as of March. BlackCat is also notable for being the first professional ransomware family to be written in Rust. This is a major selling point for BlackCat, as Rust is considered a more secure programming language that is capable of concurrent processing. As a cross-platform language, Rust also makes it easier for threat actors to tailor malware to different operating systems like Windows and Linux.

Ransomware attackers set their sights on small and medium-size businesses

Small businesses are often subjected to a huge volume of cyberattacks because malicious actors believe that they have fewer resources to counter cyberthreats, while medium-size ones make compelling targets because they possess comparatively valuable assets.

According to its leak site data, Conti staged attacks primarily on medium-size organizations (with 201 to 1,000 employees), accounting for 41.9% of its successful attacks in the first quarter of 2022, with the rest of its attacks evenly split between small businesses (with at most 200 employees) and large enterprises (with more than 1,000 employees).

In contrast, 65.5% of LockBit's successful attacks in the first quarter of 2022 affected small businesses, followed by medium-size companies at 20.5% and large enterprises at 10.5%. Similarly, BlackCat victimized mostly small businesses in the first quarter of 2022, making up 57.6% of its successful attacks, with medium-size organizations and large enterprises constituting 25.4% and 17%, respectively.



©2022 TREND MICRO

Figure 4. The distribution by organization size of LockBit, Conti, and BlackCat's successful attacks in terms of victim organizations in the first quarter of 2022
Source: LockBit, Conti, and BlackCat's leak sites, and Trend Micro's OSINT research

Government, finance, and manufacturing industries grapple with onslaught of attacks

Our telemetry showed that government agencies and financial companies consistently ranked in the top three industries in terms of ransomware file detections from January to March 2022, followed by organizations in the manufacturing and fast-moving consumer goods (FMCG) industries. Ransomware actors continued to beset government organizations, which also contended with high quantities of ransomware detections in the fourth quarter of 2021.

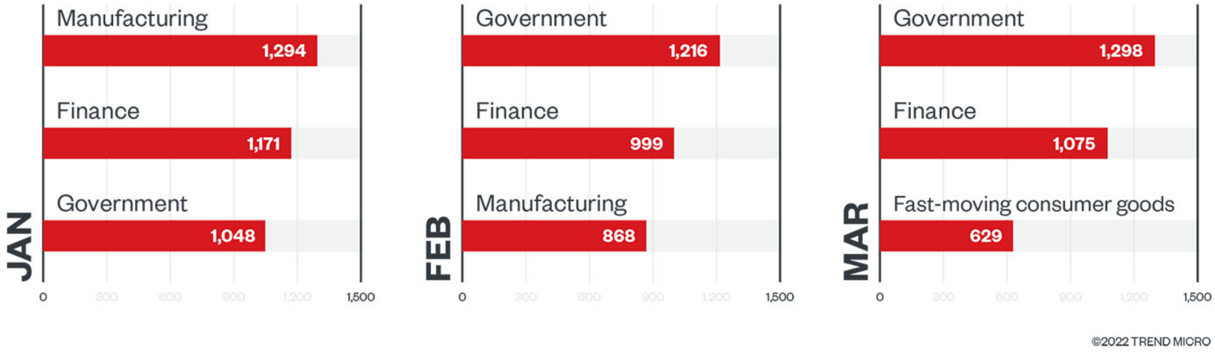
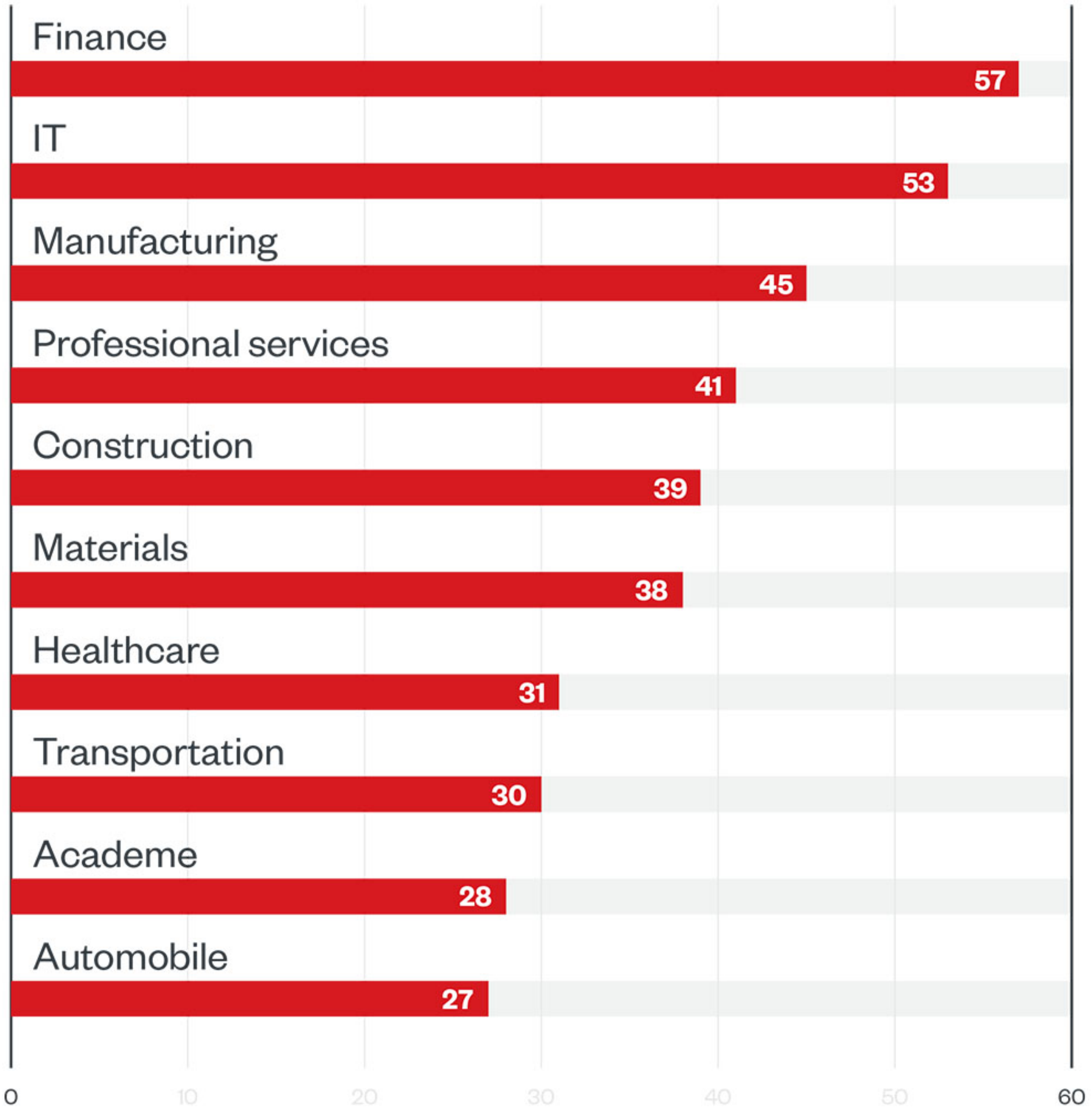


Figure 5. The top three industries in terms of ransomware file detections in machines in each month of the first quarter of 2022
Source: Trend Micro Smart Protection Network

Organizations in finance and IT remained common targets of RaaS and extortion groups. In a repeat of the first quarter of last year, ransomware groups' leak sites showed that these two industries sustained the most attacks in the first quarter of 2022. Ransomware groups have typically been drawn to financial companies not only for their valuable data, but also because their attack surface continues to expand as a result of increased connectivity and a more distributed workforce.



©2022 TREND MICRO

Figure 6. The top 10 industries affected by successful RaaS and extortion attacks in terms of victim organizations in the first quarter of 2022
Source: RaaS and extortion groups' leak sites, and Trend Micro's OSINT research

Our detections were more or less consistent with our findings from ransomware groups' leak sites, where financial organizations bore the brunt — 12.7% — of LockBit's successful attacks in the first quarter of 2022. The construction and manufacturing industries each made up 9.5% of LockBit's victim count in the same period. This count included one of the world's largest tire manufacturers, which LockBit compromised in February.

Industry	Victim count

Finance	28
Construction	21
Manufacturing	21
IT	16
Professional services	16
Others	118
Total	**220**

Table 1. The top industries affected by LockBit’s successful attacks in terms of victim organizations in the first quarter of 2022
Source: LockBit’s leak site and Trend Micro’s OSINT research

In comparison, Conti’s victims in the first quarter of 2022 were more varied: 12.8% of them were involved in manufacturing, with materials and professional services companies running close behind at 10.3% and 8.5%, respectively. One notable Conti attack occurred in January, against a Taiwanese electronics company that supplies components to the likes of Apple, Dell, and Tesla. Fortunately, only noncritical systems were affected, but the company’s high-profile clientele gives an idea of how ransomware attacks have the potential to also affect a victim’s big-name clients.

Industry	Victim count
Manufacturing	15
Materials	12
Professional services	10
Construction	9
IT	8
Others	63
Total	**117**

Table 2. The top industries affected by Conti’s successful attacks in terms of victim organizations in the first quarter of 2022
Source: Conti’s leak site and Trend Micro’s OSINT research

Organizations in the professional services industry were hit hardest by BlackCat in the first quarter of 2022, as they were the victims in 13.6% of its successful attacks. Additionally, the finance and legal services industries each experienced 10.2% of BlackCat's successful attacks. One organization that fell victim to BlackCat's activity was a Swiss aviation business, which suffered a data leak in February that included the company's internal memos and information on job applicants.

Industry	Victim count
Professional services	8
Finance	6
Legal services	6
Apparel and fashion	5
Materials	5
Others	29
Total	**59**

Table 3. The top industries affected by BlackCat's successful attacks in terms of victim organizations in the first quarter of 2022
Source: BlackCat's leak site and Trend Micro's OSINT research

Ransomware takes a toll on organizations in Europe and North America

Our investigation into RaaS and extortion groups' leak sites showed that the US still topped the list of countries that suffered the most RaaS and extortion attacks, but many European countries were also affected.

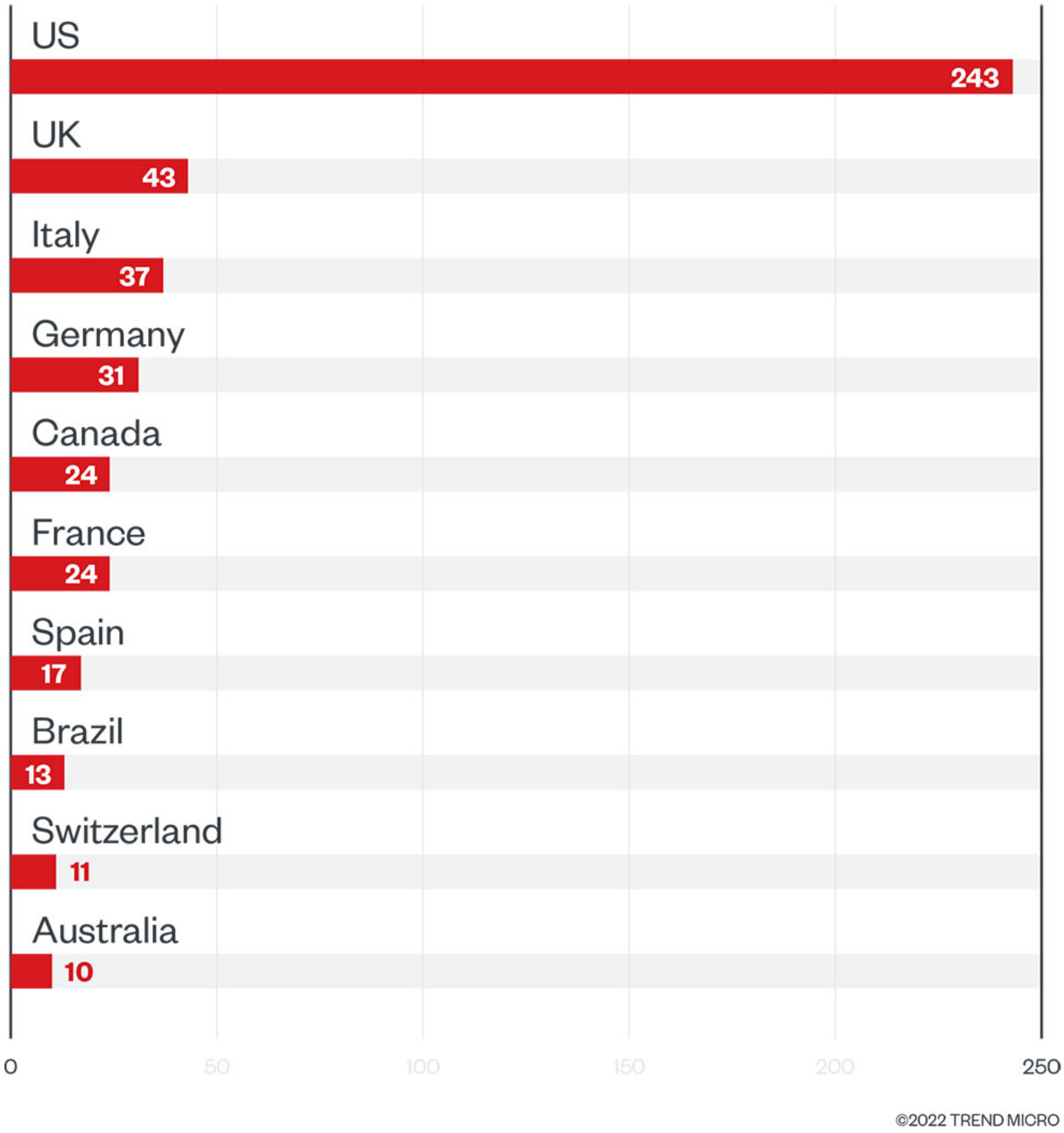


Figure 7. The top 10 countries affected by successful RaaS and extortion attacks in terms of victim organizations in the first quarter of 2022
Source: RaaS and extortion groups' leak sites, and Trend Micro's OSINT research

The bulk — 40.5% — of LockBit's victims in the first quarter of 2022 were organizations located in Europe, followed by those in North America at 34.1% and those in Asia-Pacific at 10.9%. In particular, the US, Italy, and France experienced the most LockBit attacks. Even though most of LockBit's victims were based in Europe, the FBI noted in February that LockBit's latest known version, LockBit 2.0, was designed to identify and exclude Eastern European organizations from its attacks. LockBit's previous version also had an automated vetting process that screened out systems in Russia and countries belonging to the Commonwealth of Independent States, possibly as a means of avoiding prosecution in these countries.

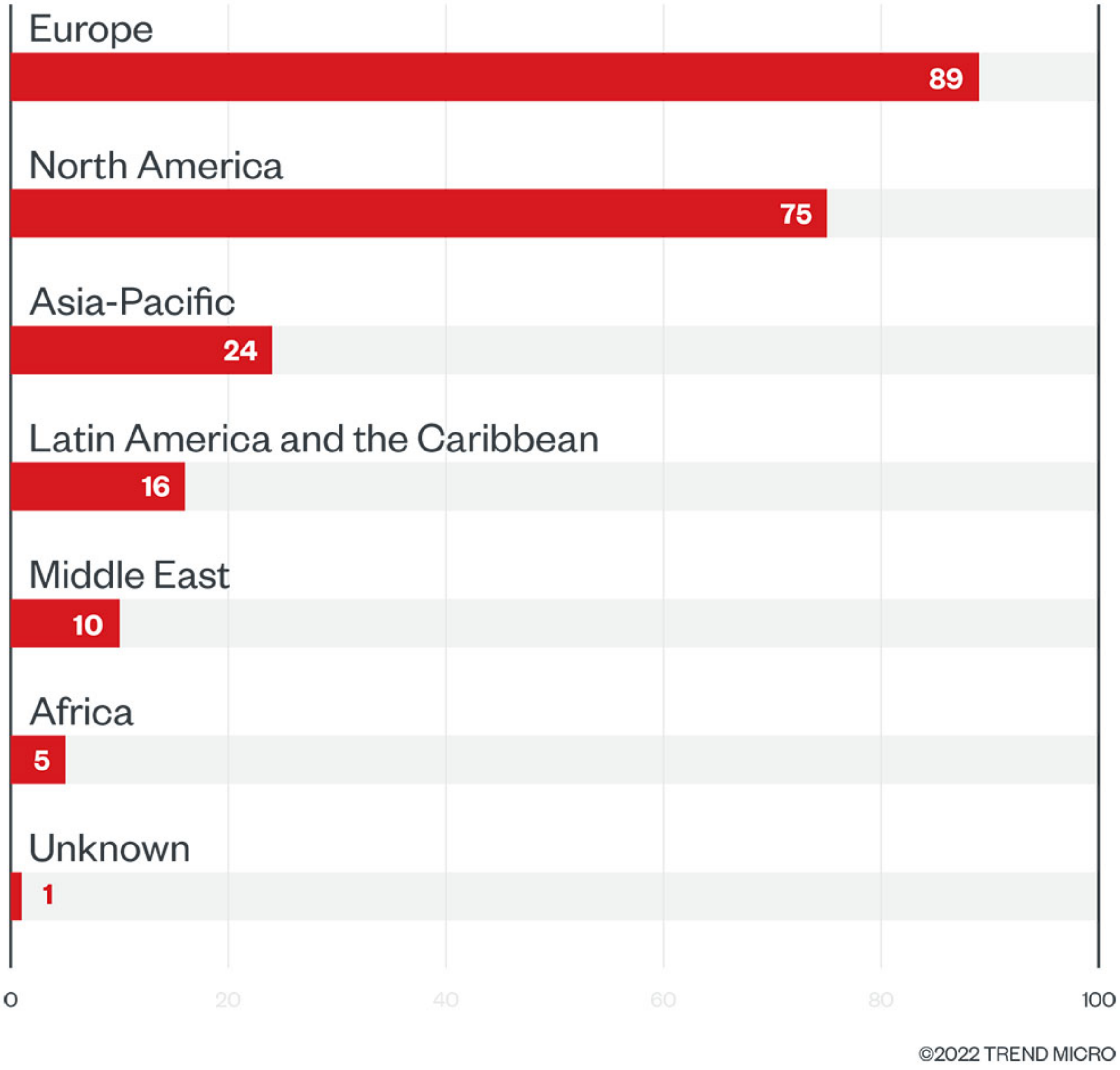


Figure 8. The top regions affected by LockBit’s successful attacks in terms of victim organizations in the first quarter of 2022
Source: LockBit’s leak site and Trend Micro’s OSINT research

In February, Conti, which has many members located in Russia, weighed in on the Russia-Ukraine conflict and expressed its intent to retaliate against anyone who would stage cyberattacks on Russia. This might explain, in part, the regional distribution of its activity in the first quarter of 2022: Organizations in North America were the most affected by its successful attacks, making up 49.6% of its victims, whereas those in Europe accounted for 41.9% and those in the Asia-Pacific region made up 6%. Most of Conti's victims were in the US, Germany, and the UK.

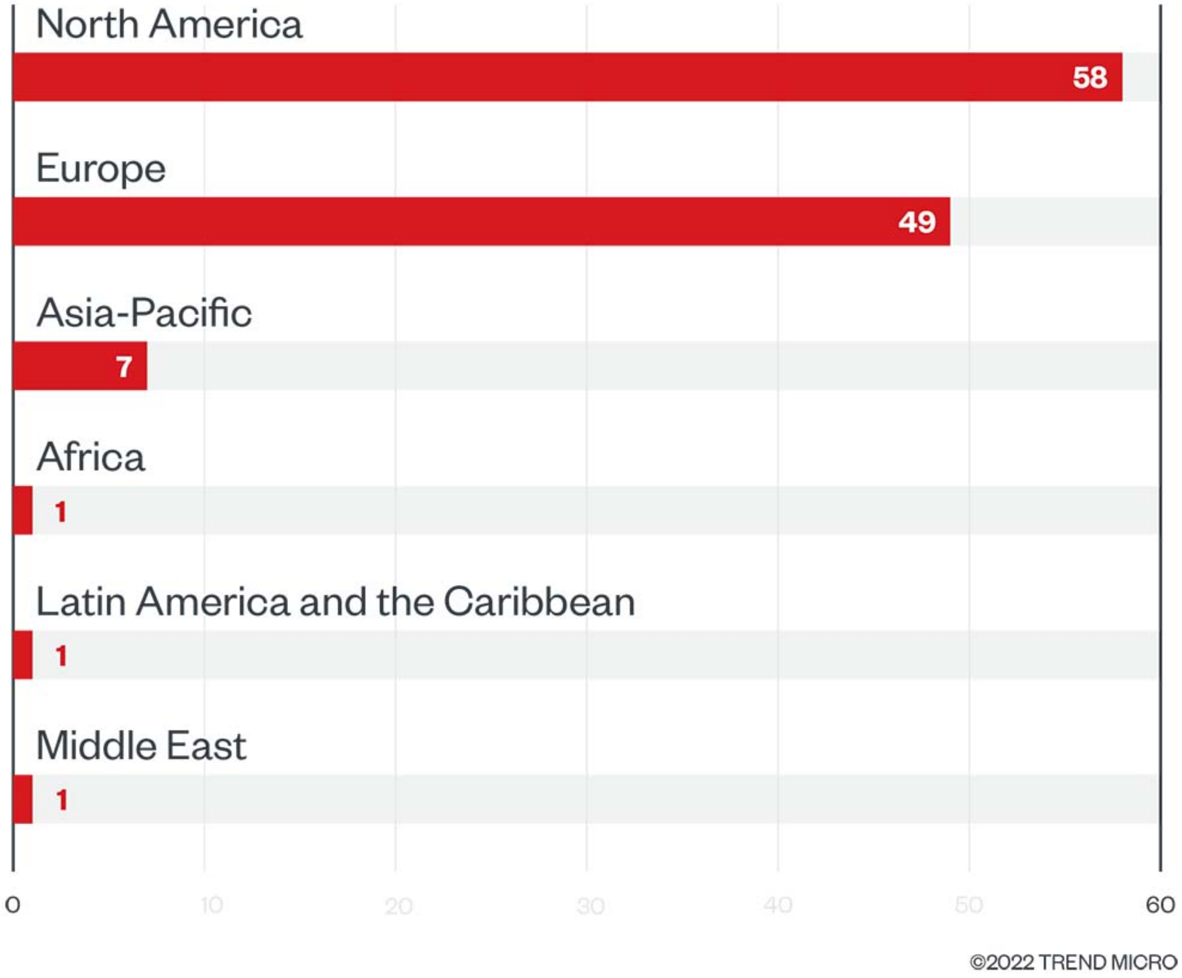


Figure 9. The top regions affected by Conti's successful attacks in terms of victim organizations in the first quarter of 2022
Source: Conti's leak site and Trend Micro's OSINT research

Like Conti, BlackCat focused its activity in the first quarter of 2022 on victims located in North America, where 50.8% of its successful attacks took place. Its victims in Europe and Asia-Pacific accounted for 25.4% and 18.6%, respectively. More specifically, it homed in on targets in the US and Italy. In the first quarter of 2022, BlackCat was responsible for headline-making attacks on prominent European companies, including a German fuel distribution firm and an Italian high-end fashion brand.

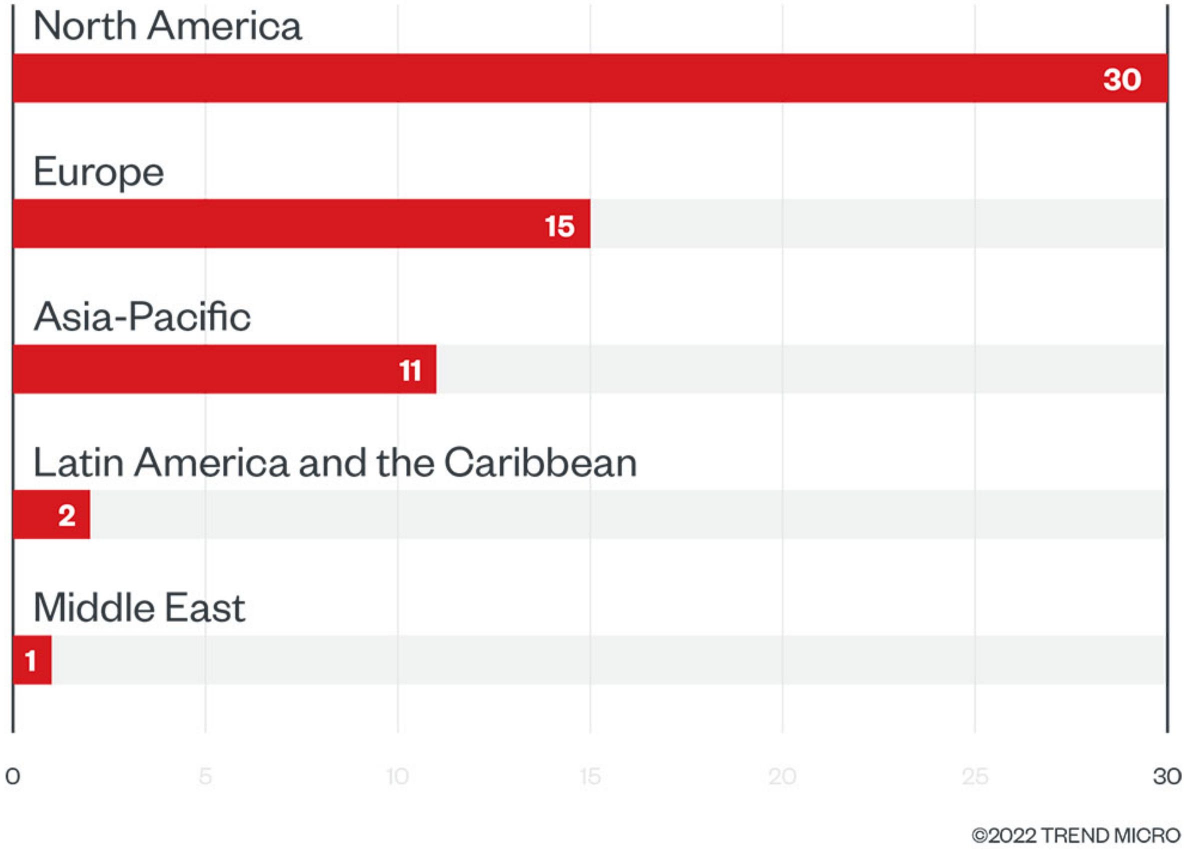


Figure 10. The top regions affected by BlackCat's successful attacks in terms of victim organizations in the first quarter of 2022
Source: BlackCat's leak site and Trend Micro's OSINT research

Security solutions and practices safeguard organizations against ransomware attacks

Ransomware remains a major threat to businesses of all sizes, which must contend with malicious actors wielding an arsenal of increasingly sophisticated tools and techniques. Organizations can mitigate the risk of ransomware attacks that could compromise their data by following these recommended security practices:

- **Enable multifactor authentication**. Organizations should have policies in place that require employees who access or store company data on their devices to enable multifactor authentication, so that any sensitive information in these devices cannot be easily accessed.
- **Back up data**. As much as possible, organizations should follow the “3-2-1 rule” to protect their important files: Create at least three backup copies in two different file formats, with one of those copies stored off-site.

- **Keep systems up to date**. Organizations should update all of their applications, operating systems, and other software as soon as patches are released by vendors and developers. Doing so can help prevent ransomware actors from exploiting vulnerabilities to gain access to organizations' systems.
- **Verify emails before opening them**. Organizations should train their employees to avoid downloading attachments or clicking on embedded links in emails from senders they do not recognize, as malicious actors bank on these as means to install ransomware.
- **Follow established security frameworks**. Organizations can develop cybersecurity strategies based on the security frameworks created by the Center of Internet Security (CIS) and the National Institute of Standards and Technology (NIST). The security measures and best practices laid out in these frameworks can serve as a guide for organizations' security teams as they design their own threat mitigation plans.

Organizations can augment their cybersecurity infrastructure with multilayered detection and response solutions that can anticipate and respond to ransomware movements before operators can carry out an attack. One such solution is Trend Micro Vision One™, which is equipped with extended detection and response (XDR) capabilities that gather and automatically correlate data across multiple security layers — including email, endpoints, servers, cloud workloads, and networks — to avert ransomware attack attempts.

Organizations can also benefit from solutions with network detection and response (NDR) capabilities, which can give them greater visibility over their network traffic. Among these solutions is Trend Micro Network One™, which provides security teams with the critical network telemetry they need to form a clearer picture of their environment, accelerate their response, and prevent future attacks.

The supplementary data sheet for this report, including data from RaaS and extortion groups' leak sites, Trend Micro's OSINT research, and the Trend Micro Smart Protection Network, can be downloaded here.

With contributions by Matsugaya Shingo

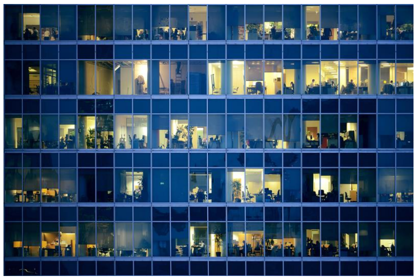
HIDE

Like it? Add this infographic to your site:
1. Click on the box below.   2. Press Ctrl+A to select all.   3. Press Ctrl+C to copy.   4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Ransomware By The Numbers, Ransomware, Cybercrime, By The Numbers
This report delves into the ransomware threat landscape of the first quarter of 2022, with a focus on the three most successful ransomware families and the types of industries and organizations that were affected by their attacks.

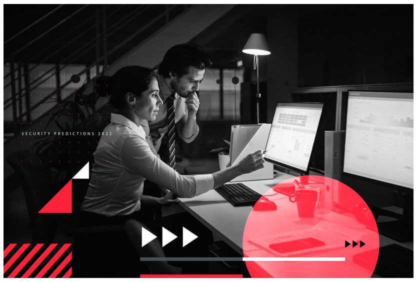
2021 Midyear Cybersecurity Report



In the first half of this year, cybersecurity strongholds were surrounded by cybercriminals waiting to pounce at the sight of even the slightest crack in defenses to ravage valuable assets.

View the report

Trend Micro Security Predictions for 2022: Toward a New Momentum



In 2022, decision-makers will have to contend with threats old and new bearing down on the increasingly interconnected and perimeterless environments that define the postpandemic workplace.

View the 2022 Trend Micro Security Predictions