The New Ransomware Threat: Triple Extortion

Global surge in ransomware attacks hits 102% increase this year compared to the beginning of 2020, and shows no sign of slowing down

- **Number of organizations impacted by ransomware globally has more than doubled in the first half of 2021 compared with 2020**
- **The healthcare and utilities sectors are the most targeted sectors since the beginning of April 2021**
- **Organizations in Asia Pacific are targeted more than any other region**
- **Check Point Research (CPR) warns of new ransomware threat: Triple Extortion**

The FBI confirmed in a statement on Monday that a professional cybercriminal group called DarkSide was responsible for the ransomware attack on the Colonial Pipeline network. DarkSide works in a Ransomware-as-a-Service (RaaS) model, where it leverages a partner program to execute its cyber attacks. This means there is little known at this point about the real actor behind the attack.

DarkSide is known to be part of a trend of ransomware attacks that involve systems rarely seen by the cyber community, like ESXi servers. This has led to suspicions that the ICS network was involved. The ransomware is known to have been deployed in numerous targeted ransomware attacks including other oil and gas companies such as Forbes Energy Services and Gyrodata.

Following other large scale attacks such as the one on the city of Tulsa, and the REvil ransomware that tried to extort Apple, it's clear that ransomware attacks are a major concern globally. Yet, there is a real lack of action by organizations in preparing for incidents or even trying to protect themselves in the first place.

Global Data

CPR reported in March that ransomware attacks had seen a 57% increase in the number of attacks since the beginning of 2021 amid the disclosure of the Microsoft Exchange vulnerabilities. Most recently, Colonial Pipeline, a major US fuel company, was the victim of such an attack and in 2020, according to Cybersecurity Ventures, it is estimated that ransomware cost businesses worldwide around $20 billion – a figure that is nearly 75% higher than in 2019.

Since April, researchers at CPR have seen an average of over 1,000 organizations being impacted by ransomware every week. This follows significant increases in the number of impacted organizations so far in 2021 – 21% in the first trimester of the year and 7% since April so far. These increases have resulted in a staggering 102% overall increase in the number of organizations affected by ransomware compared to the beginning of 2020.

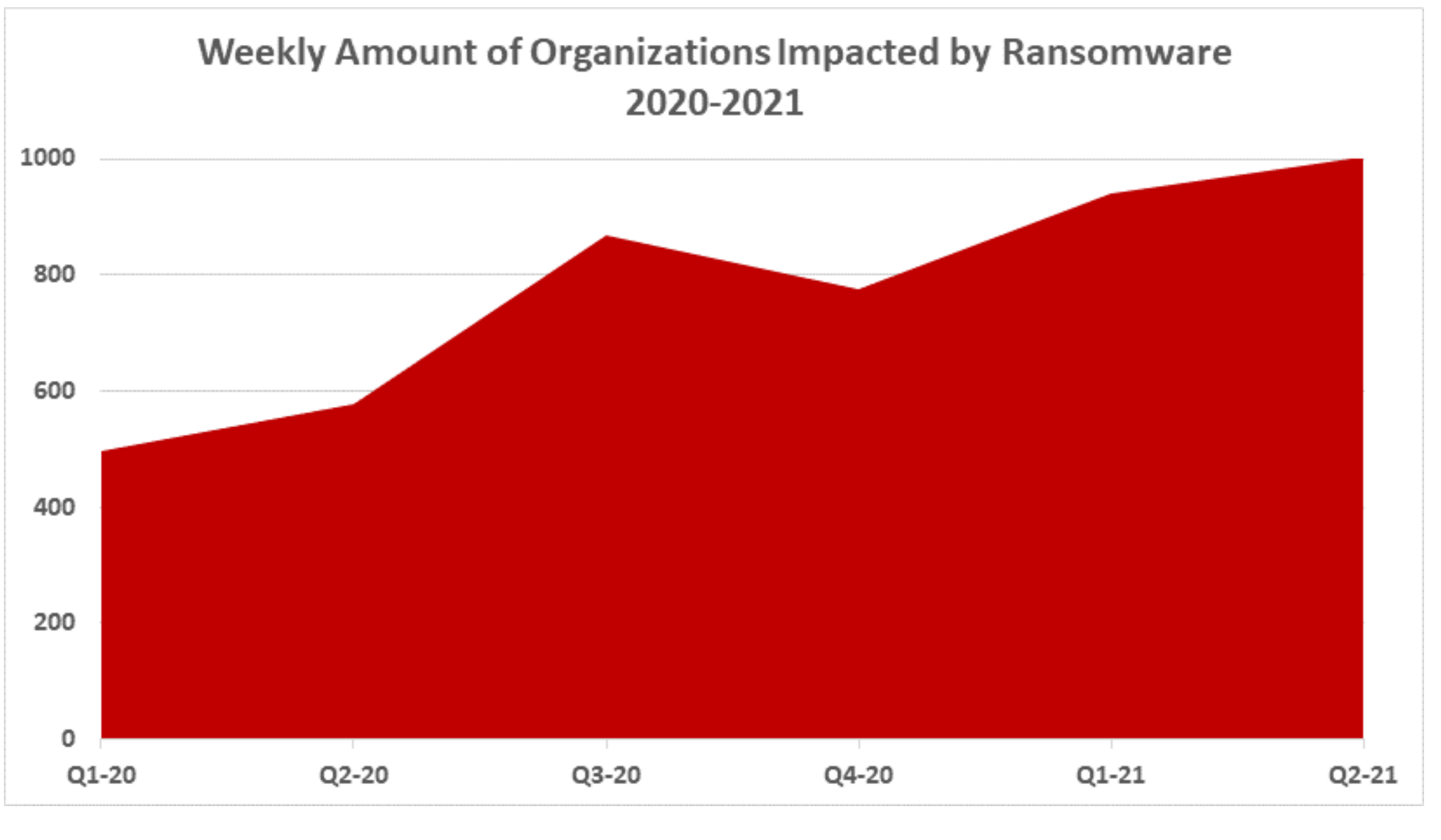

Figure 1: Weekly number of organizations affected by ransomware (2020 – 2021)

Average Weekly Attacks per Organizations by Industry

The industry sectors that are currently experiencing the highest volumes of ransomware attack attempts globally are healthcare, with an average of 109 attacks attempts per organization every week, followed by the utilities' sector with 59 attacks and Insurance/Legal with 34.

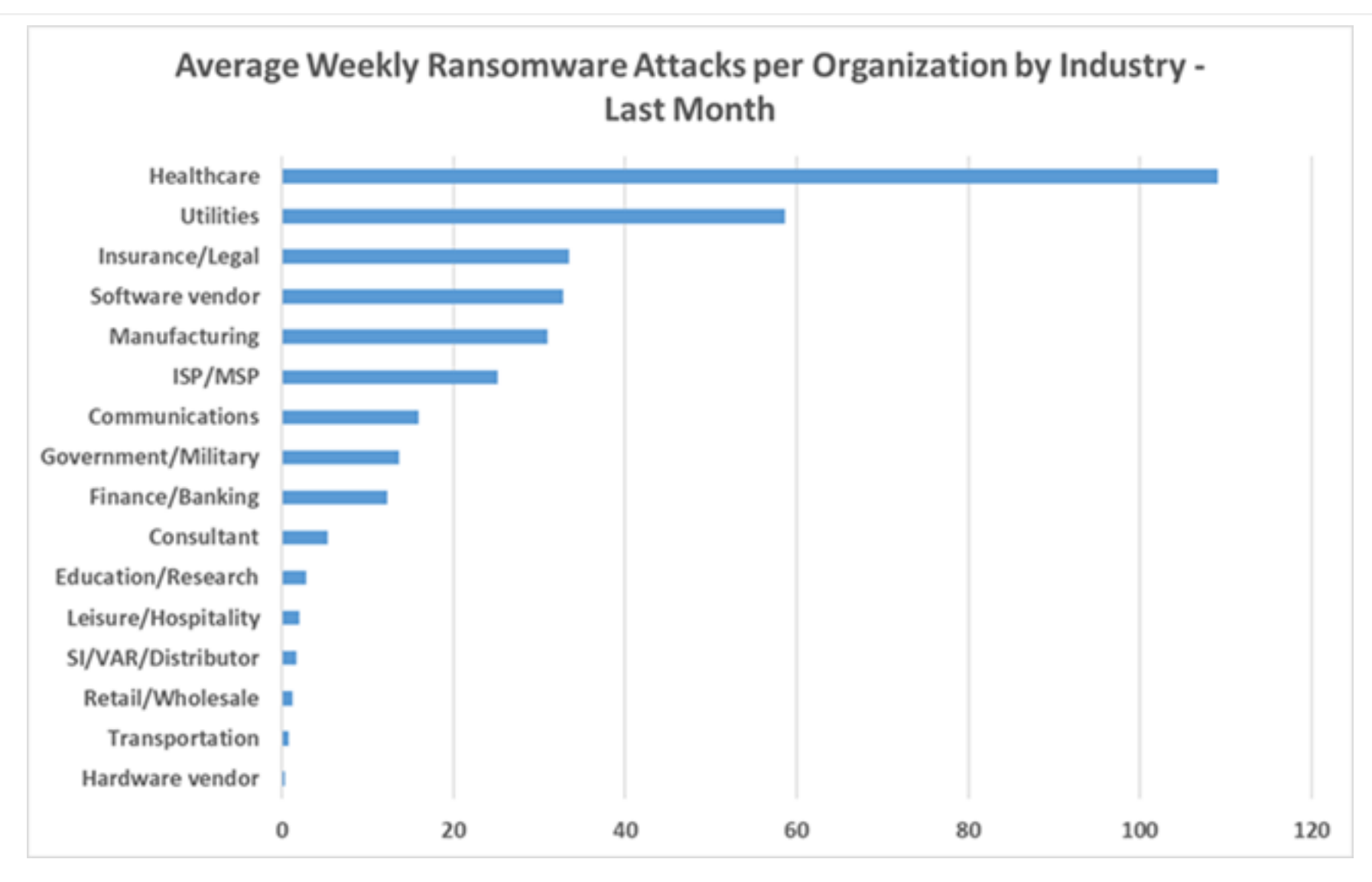

Figure 2: Average number of ransomware attacks per organization per week by industry – April 2021

Geo Data

Ransomware Impact per Region

An organization in Asia Pacific (APAC) currently experiences the highest volume of ransomware attacks. On average, organizations in APAC are attacked 51 times per week. This is a 14% increase compared to the beginning of this year. On the other hand, African organizations have seen the highest increase in attacks, 34%, since April.

On average, a North American organization experiences 29 weekly attacks, European and Latin American companies 14 and African companies each have four weekly attacks per organization.

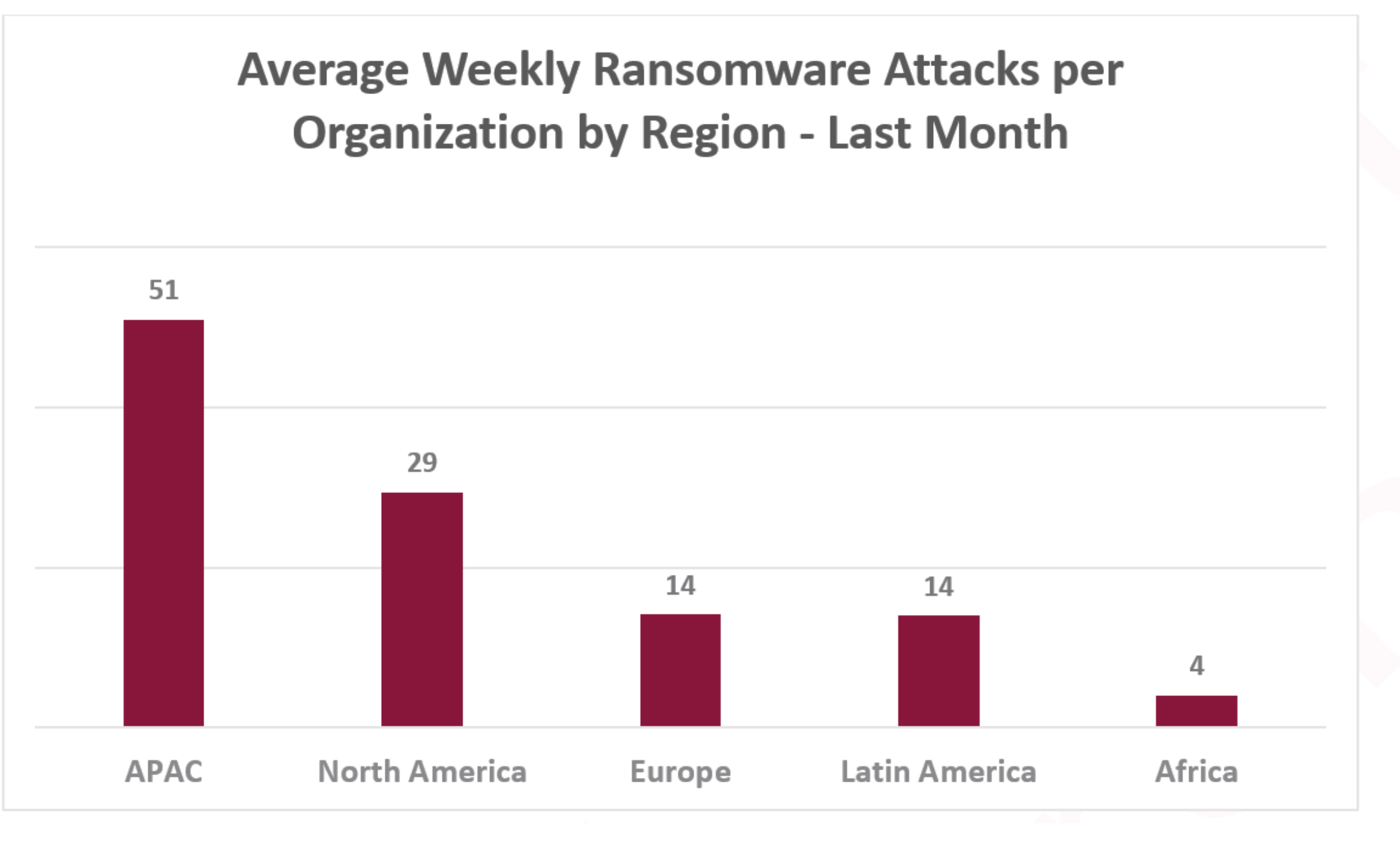

Figure 3: Average weekly number of ransomware attacks per organization by region – April 2021

Top Five Countries with the most Ransomware Attacks

India has seen the most number of attacks attempts per organization, with an average of 213 weekly attacks since the beginning of the year. This is followed by Argentina with 104 per organization, Chile with 103, France 61 and Taiwan 50.

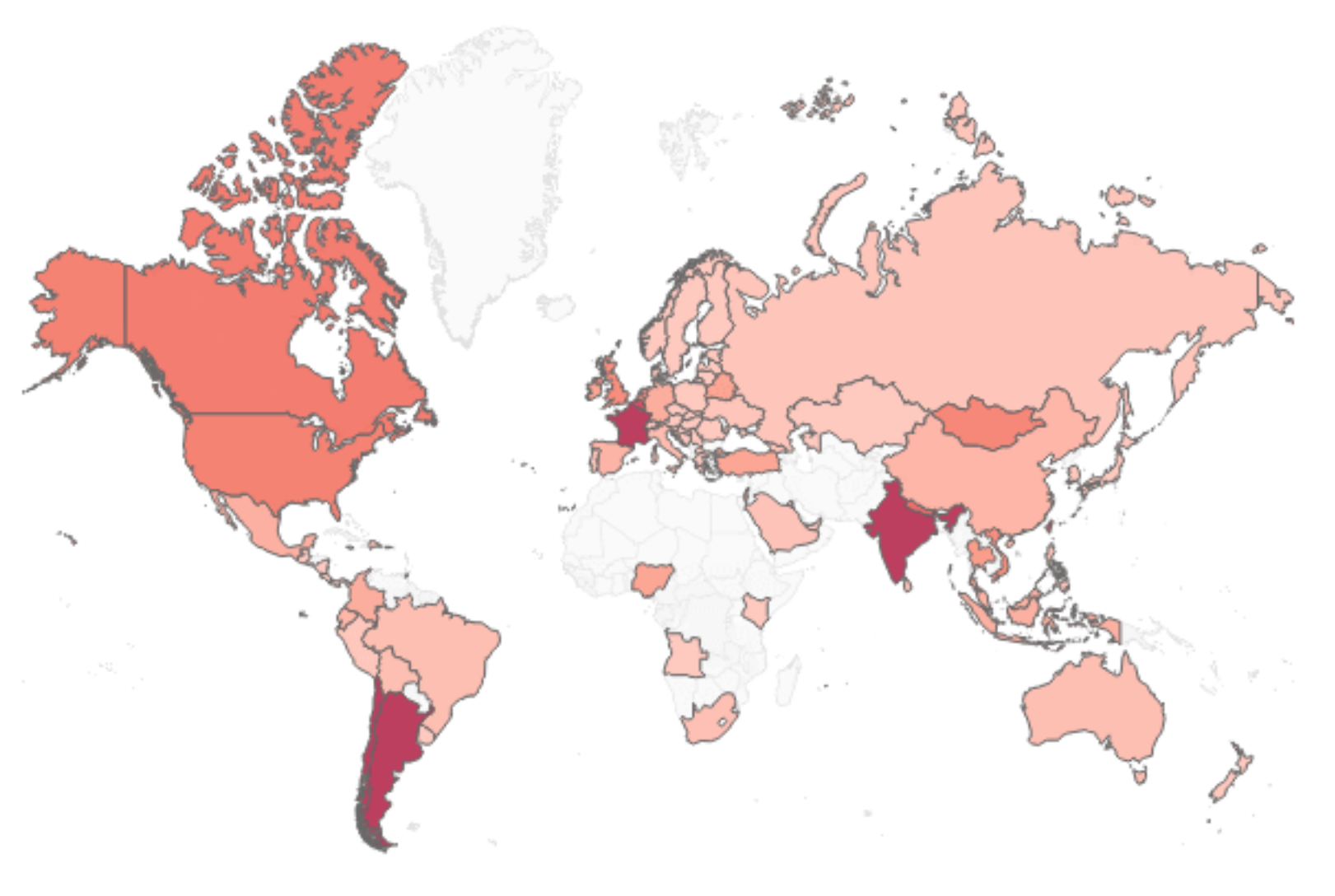

Figure 4: "Heat map" of countries where organizations are most impacted by ransomware since April 2021

Top Industries Attacked per Region in 2021

As the table shows, ransomware attackers are focusing their efforts across all industries globally. While in North America healthcare organizations have suffered the most attacks since the beginning of the year, in Europe utilities 'organizations absorb the most attacks. In APAC, insurance/legal are most impacted, while in LATAM it is the communications industry. In Africa, the financial and banking sector is the most attacked.

Asia Pacific	***Latin America***	***Africa***	***Europe***	***North America***
Insurance/Legal	Communications	Finance/Banking	Utilities	Healthcare
Manufacturing	Manufacturing	Manufacturing	Software vendor	Software vendor
Healthcare	Retail/Wholesale	Retail/Wholesale	Healthcare	Insurance/Legal
ISP/MSP	Finance/Banking	ISP/MSP	ISP/MSP	Education/Research
Government/Military	Government/Military	Government/Military	Government/Military	Government/Military

Triple Extortion Ransomware: The Third-Party Threat

The success of double extortion throughout 2020, most notably since the outburst of the Covid-19 pandemic, is undeniable. While not all incidents – and their results – are disclosed and published, statistics collected during 2020-2021 reflect the prominence of the attack vector. The average ransom payment has increased by 171% in the last year, and is now approximately $310,000. Over 1,000 companies suffered data leakage after refusing to meet ransom demands in 2020, and about 40% of all newly discovered ransomware families incorporated data infiltration into their attack process. As the numbers reflect a golden attack technique, which combines both, a data breach and a ransomware threat, it is clear that attackers are still seeking methods to improve their ransom payment statistics, and their threat efficiency.

Prominent attacks that have taken place at the end of 2020 and the beginning of 2021 point at a new attack chain – essentially an expansion to the double extortion ransomware technique, integrating an additional, unique threat to the process – and we call this Triple Extortion. The first notable case is the Vastaamo clinic attack, which happened in October 2020. Innovative at the time, the 40,000-patient Finnish psychotherapy clinic suffered a yearlong breach that culminated in extensive patient data theft and a ransomware attack. A decent ransom was demanded from the healthcare provider, but surprisingly, smaller sums were also demanded from the patients, who had received the ransom demands individually by email. In those emails, the attackers threatened to publish their therapist session notes. This was the first attack of its kind within the ransomware attacks landscape.

On a wider scale, in February 2021 the REvil ransomware group announced that they had added two stages to their double extortion scheme – DDoS attacks and phone calls to the victim's business partners and the media. The REvil ransomware group, responsible for the distribution of the Sodinokibi ransomware, operates in a ransomware-as-a-service business model. The group now offers DDoS attacks and voice-scrambled VoIP calls to journalists and colleagues as a free service for its affiliates, aimed at applying further pressure on the victim´s company to meet ransom demands within the designated timeframe.

It seems that even when riding the wave of success, threat groups are in constant quest for more innovative and more fruitful business models. We can only assume that creative thinking and a wise analysis of the complex scenario of double extortion ransomware attacks have led to the development of the third extortion technique. Third-party victims, such as company clients, external colleagues and service providers, are heavily influenced, and damaged by data breaches caused by these ransomware attacks, even if their network resources are not targeted directly. Whether further ransom is demanded from them or not, they are powerless in the face of such a threat, and have, a lot to lose should the incident take a wrong turn. Such victims are a natural target for extortion, and might be on the ransomware groups' radar from now on.

Preventing Ransomware

1. **Raise your guard around weekends and holidays–** Most ransomware attacks over the past year took place over weekends and holidays when people are less likely to be watching.
2. **Up-to-date patches–** At the time of the famous WannaCry attack in May 2017, a patch existed for the EternalBlue vulnerability used by WannaCry. This patch was available a month prior to the attack and labeled as "critical" due to its high potential for exploitation. However, many organizations and individuals did not apply the patch in time, resulting in a ransomware outbreak that infected more than 200,000 computers within three days. Keeping computers up-to-date and applying security patches, especially those labeled as critical, can help limit an organization's vulnerability to ransomware attacks.
3. **Anti-Ransomware–** While the previous ransomware prevention steps can help in mitigating an organization's exposure to ransomware threats, they do not provide a perfect protection. Some ransomware operators use well-researched and highly targeted spear phishing emails as their attack vector. These emails may trick even the most diligent employee, resulting in ransomware gaining access to an organization's internal systems. Protecting against this ransomware that "slips through the cracks" requires a specialized security solution. In order to achieve its objective, ransomware must perform certain anomalous actions, such as opening and encrypting large numbers of files. Anti-ransomware solutions monitor programs running on a computer for suspicious behaviors commonly exhibited by ransomware, and if these behaviors are detected, the program can take action to stop encryption before further damage can be done.
4. **Education–** Training users on how to identify and avoid potential ransomware attacks is crucial. Many of the current cyber-attacks start with a targeted email that does not even contain malware, but a socially engineered message that encourages the user to click on a malicious link. User education is often considered one of the most important defenses an organization can deploy.
5. **Ransomware attacks do not start with Ransomware–** Ryuk and other ransomware purchase infection bases in targeted organizations. Security professionals should be aware of **Trickbot, Emotet, Dridex and CobaltStrik** infections within their networks and remove them using threat hunting solutions – as they open the door for Ryuk or other ransomware infections to infiltrate organizations.

The data used in this report was detected by Check Point Threat Prevention's technologies, stored and analyzed in Check Point ThreatCloud. ThreatCloud provides real-time threat intelligence derived from hundreds of millions of sensors worldwide, over networks, endpoints and mobiles. The intelligence is enriched with AI-based engines and exclusive research data from Check Point Research – The Intelligence & Research Arm of Check Point Software Technologies.