RANSOMWARE'S GLOBAL IMPACT:

MORE RESPONSIVE THREAT INTELLIGENCE IS NEEDED

Abstract

The ransomware threat landscape has grown significantly in the past several years. A holistic understanding of the modern threat environment is needed to enable companies to determine what is required to enhance technical capabilities and strategies.

Phil Wheeler

Telos Advanced Cyber Analytics Product Management

Telos Corporation

Telos®

RANSOMWARE'S GLOBAL IMPACT:
More Responsive Threat Intelligence Is Needed

INTRODUCTION

The ransomware threat landscape has grown significantly in the past several years. In 2021 there was a total of US$623.3 million ransomware attacks, an increase of over 202% from the US$206.4 million attacks in 2018. For reference, approximately 1 million ransomware attacks –occurred every twelve hours in 2021. This surge in ransomware attacks demonstrates just how volatile the threat environment is for corporations around the globe.

Considering the rapidly increasing threat that ransomware poses to the global economy and corporate operations, this report will discuss the global threat landscape, the evolution of ransomware-as-a-service, predicted future costs, and illuminate where companies fall short. The goal of this report is to assist cybersecurity specialists in better understanding the threat environment and identify innovative techniques to effectively mitigate these risks.

THE GLOBAL THREAT LANDSCAPE

Cybercriminals around the world are employing ransomware for monetary gain without regard for the impact to the global economy and companies targeted. In 2021, 66% of global organizations were targeted by ransomware, in comparison to 37% the year prior. Cybercriminals' development of the Ransomware-as-a-Service (RaaS) model has significantly expanded the ability of cybercriminal groups to employ ransomware at a global scale.

66% of organizations were hit by ransomware in 2021,
up from 37% in 2020.
Sophos, The State of Ransomware 2022

Between 2021 and 2022, there has been a 57% increase in cyberattacks, with 59% of companies targeted reporting a noted increase in attack complexity. Along with the increased volume of ransomware attacks, there has been a 300% increase in ransom

demands over $1 million USD. The manufacturing industry in particular was hardest hit, with industry-wide ransoms averaging US$2 million.

In response to the increased volume of attacks, companies have started to develop more robust recovery plans. Almost every company that experienced a ransomware attack in 2021 successfully recovered at least some of their data, primarily through use of data backups. Additionally, analysis shows that paying ransom demands is an ineffective solution for data recovery; on average, only 4% of victims that capitulated to demands recovered all of their data, with the majority only recovering about 60%.

Ransomware-as-a-Service (RaaS)

RaaS is a business model wherein ransomware operators develop and launch ransomware attacks at the behest of affiliates who pay for the service. Through RaaS, cybercriminals have developed a profitable business model that has vastly increased accessibility for various actors that otherwise may not have the technical know-how to employ such attacks. RaaS has enabled the large-scale employment of ransomware, further task-saturating cybersecurity teams around the globe now faced with defending against the high volume of attacks.

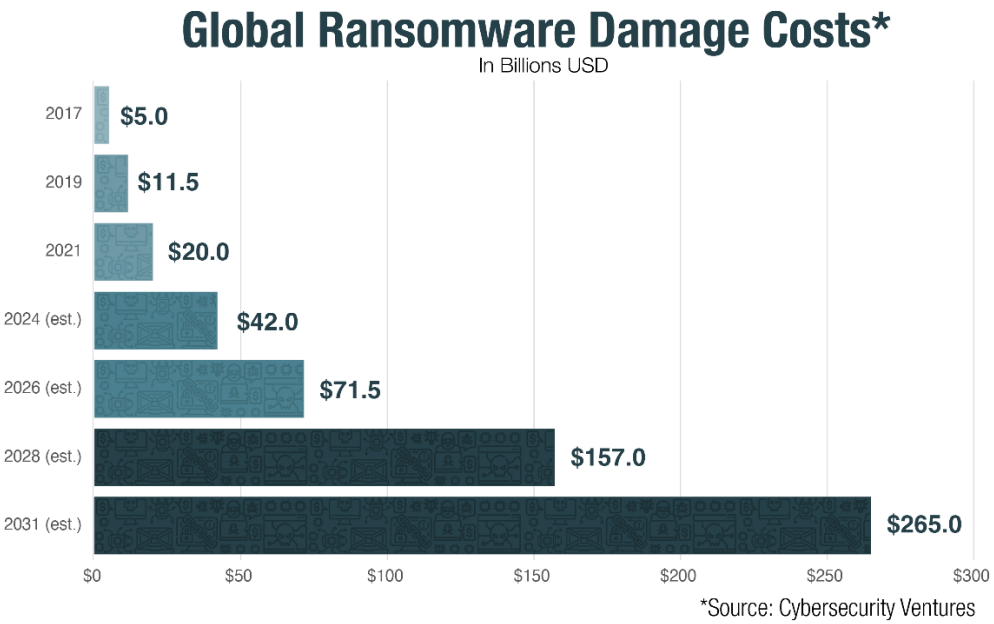
There are four revenue models traditionally associated with RaaS:

1. Monthly subscription at a flat fee.
2. Monthly subscription, with a percentage of profits (usually 20-30%) additionally going to the developer.
3. One-time fee with no profit sharing.
4. Pure profit sharing.

More elaborate RaaS platforms provide customer-specific dashboards where clients can track payments, view the status of infections, and any other pertinent information associated with their targets.

Future Cost

The RaaS market has become an established and extremely competitive market. Similar to legitimate businesses, RaaS operators have developed marketing campaigns and published white papers, blogs, and other marketing products. In turn, between 2019 and 2021, there was an approximately 200% increase in monetary gain due to criminal ransomware attacks, from US$11.5 billion to US$20 billion USD.

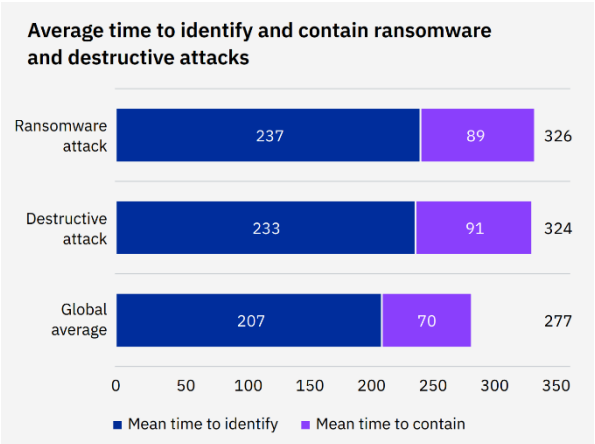


The pace and volume of ransomware attacks shows no sign of slowing. Between 2020 and 2022, the total annual cost of ransomware attacks globally has increased by approximately 200%. Ransomware attack volume continues to grow at a similar pace; global cost in 2031 could reach an estimated US$265 billion.

Where Enterprises Fall Short

Traditionally, cybersecurity has been an afterthought for many corporations; however, COVID-19 and the vast increase of cyber-criminal activity has shifted the paradigm. This new outlook has enabled greater budgets and resources for cybersecurity. According to a 2022 study, 88% of companies believe they have adequate budgets and resources to effectively manage the threat landscape. Yet, ransomware attacks still take, on average, 326 days to identify and contain.

Cybercriminals' ability to outpace corporate efforts through rapid development of threat vectors prevents cybersecurity specialists from adequately mitigating threats. Obfuscation techniques are used to hide the true intent of ransomware employed by cybercriminals to infect a target's network. Identifying these threats in real time is a challenge for companies around the globe. In an



Source: IBM Cost of a Data Breach Report 2022

attempt to combat such techniques, companies rely on behavioral analytics internal to infrastructure to flag suspicious activity; however, such strategies take time and create latency in identifying threats.

The threat intelligence industry needs to develop methods to illuminate hacker ecosystems in a timelier manner and prevent threats before network access is gained. One way to do this is to utilize external behavioral analytics, allowing for proactive targeting of unknown threat vectors and significantly decreasing the identification timeline.

Conclusion

Ransomware is an expanding and increasingly effective threat employed by cybercriminals around the globe. By gaining a holistic understanding of the modern threat environment, companies can begin to determine what is required to enhance technical capabilities and strategies. The threat intelligence industry's shift toward analytics external of the customer's infrastructure enables rapid threat identification and the ability to contextualize the threat environment in real time.

A holistic understanding of the modern threat environment enables companies to determine what is required to enhance technical capabilities and strategies.

Works Cited

Baker, K. (2022, February 7). *Ransomware as a Service (RaaS) Explained*. Retrieved from Crowdstrike: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

Braue, D. (2022, June 2). *Global Ransomware Damage Costs Predicted to Exceed $265 Billion By 2031*. Retrieved from Cybercrime Magazine: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

(2022). *Cost of a Data Breach Report 2022.* IBM Security.

(2022). *Mid-Year Update: 2022 SonicWall Cyber Threat Report.* Sonicwall.

(2022). *The State of Ransomware 2022.* Sophos.

Version 1.1
November 2022