BTB SECURITY

ANALYZED BY:
MATT WILSON
(CISSP, GPEN, GSEC)

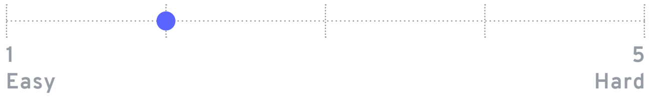
BTB'S INDUSTRY REPORT SCORECARD

UNIT 42 RANSOMWARE
THREAT REPORT, 2021

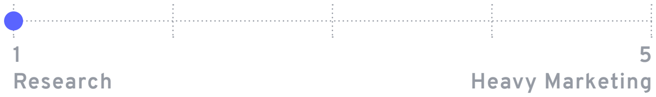
Every year it seems that more and more security vendors are publishing reports on the state of security or on cybersecurity trends. While some of these reports are informative and provide actionable information, too many are thinly disguised marketing pieces or are so dense that getting through them is more challenging than finishing "War and Peace".

With our scorecards we provide a quick review of these reports and call out what you need to know to improve your organization's security posture.

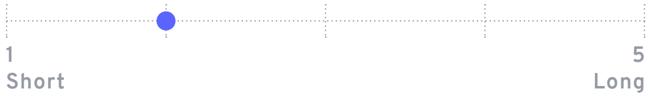
EASE OF READ



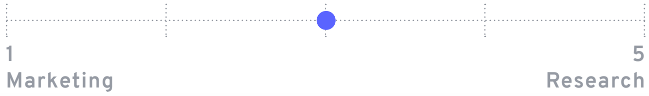
FOCUS



LENGTH: 18 PAGES



MARKETING VS. RESEARCH: 0 CREDITED AUTHORS, BUT UNIT 42 GIVEN CREDIT



OVERALL TRENDS IDENTIFIED

- Both ransomware demands and payments have skyrocketed over the past year.
- The healthcare industry was specifically targeted during the global COVID-19 pandemic.
- "Double extortion" attacks, in which ransomware operators both encrypt and steal data and then threaten to publish it to a leak site on the dark web if the ransom isn't paid, have become much more common.
- There's been a shift from a "spray and pray" strategy to a "stay and play" one: Ransomware attacks are becoming more carefully planned and targeted, with operators spending more time learning about victims' networks in order to maximize an attack's impact and their chances of getting a payment.

BEST OF THE REPORT

- This report is both succinct and current. The statistics it contains will be useful to InfoSec professionals, especially those who need to communicate present-day risks to senior leadership in straightforward terms.
- The 2020 Ransomware Summary Table that appears at the end of the report can serve as a convenient reference, highlighting the most important characteristics of each ransomware family.

> *Compared to 2019, we observed an increase in ransomware incident response cases across several industries in the U.S., Canada, and Europe… Ransomware engagements throughout 2020 were more complex than in prior years, leading to longer, more in-depth breach response times… Additionally, ransomware actors are demanding more money."*
>
> **- VIA UNIT 42 RANSOMWARE THREAT REPORT, 2021**

REPORT HIGHLIGHTS

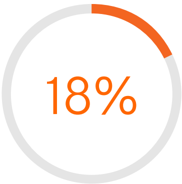
171% GROWTH
IN THE AMOUNT OF THE AVERAGE RANSOM PAID

$847,344
AVERAGE RANSOM DEMAND

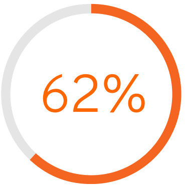
$30 MILLION
HIGHEST RANSOMWARE DEMAND REPORTED

$4.8 MILLION
AVERAGE RANSOM DEMAND IN ATTACKS USING THE MAZE RANSOMWARE VARIANT

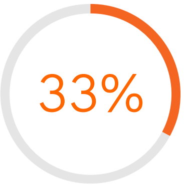
ATTACK METHODS AND VECTORS



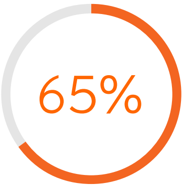
of cyberattacks reported to the FBI involve ransomware



of victims are located in the Americas



of “double extortion” attacks were associated with the NetWalker family



increase in incident response costs for tech companies

BTB’S TAKEAWAY

Palo Alto Networks’ Unit 42 Ransomware Threat Report validates a number of observations that we’ve made in the field. We knew that ransomware attacks were growing in prevalence and severity, but this report includes the hard numbers necessary to back up that statement.

The Ransomware Threat Report also documents the shifting approaches that many of today’s most successful ransomware operators are taking. They’re exploiting virtualized environments and remote desktop protocol (RDP), they’re now targeting Linux systems, and they’re adding on distributed denial-of-service (DDoS) and data exfiltration components to their ransomware attack strategies. Still, they continue to target the organizations and verticals where they believe they’ll have the easiest time getting a payout.

RANSOMWARE OPERATORS PREFER TO GO AFTER SOFT TARGETS

Even as bad actors grow more sophisticated and level up their capabilities, they’re still relying on tried-and-true threat vectors to gain a foothold in the victim’s environment. They’re still launching phishing attacks, they’re still leveraging PowerShell and other native utilities, and they’re still on the lookout for weak credentials.

Through all of our reviews, and our own experiences, we recommend focusing on the following:

- Correct IT Hygiene issues (patching, hardening, backup).
- Measure and improve your security posture. Assessments lead to less expensive and more effective outcomes by prioritizing by risk.
- Train your users, especially executives and board members (**execs and the board are allies**, it’s your responsibility to make them believe).
- Deploy effective monitoring. Make sure whatever solution you’ve deployed is functional, not just by ticking feature-set boxes, but by having the People and Process to support the solution.

BTB SECURITY

LOOK FOR OTHER BTB REPORT SCORECARDS TO CUT THROUGH THE FLUFF AND FIND OUT WHAT YOU NEED TO KNOW TO KEEP YOUR BUSINESS SECURE.