BTB SECURITY

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

# BTB'S INDUSTRY REPORT SCORECARD

FIREEYE MANDIANT SERVICES:
M-TRENDS 2021 SPECIAL REPORT


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**

1 Easy — 5 Hard

**FOCUS**

1 Research — 5 Heavy Marketing

**LENGTH:** 83 PAGES

1 Short — 5 Long

**MARKETING VS. RESEARCH:** 0 CREDITED AUTHORS

1 Marketing — 5 Research

## OVERALL TRENDS IDENTIFIED

- **The growing prevalence of double extortion tactics is again confirmed by raw data** (Mandiant calls this "multi-faceted extortion.) Ransomware operators are leveraging their access to client environments to exfiltrate sensitive data and then threatening victims with its public release to further motivate them to comply with their demands.
- **Dwell time in breaches continues to decline,** though the pervasiveness of ransomware attacks – in which creating a sense of urgency and pressuring victims to react quickly are key psychological strategies – is likely contributing to this trend.
- **A relatively small subset of ATT&CK techniques were employed in over 95% of intrusions,** reinforcing the importance of hardening your environment against familiar and well-established threat actions.
- **There's still less ransomware than you might think.** Despite all the buzz that ransomware has generated of late, it accounted for only a small minority of the malware that Mandiant researchers observed, with backdoors making up a far larger portion.
- **Adversaries often target common administrative services** such as Remote Desktop Protocol (RDP), Windows services and Windows command line scripting in "living off the land" techniques, making monitoring such capabilities critical to your cybersecurity posture.

## BEST OF THE REPORT

- This report provides a thoroughly researched perspective on various threat actors and groups as well as their likely motivations and targets, with years' worth of data to support its trend findings and conclusions.
- The authors don't just pile on new buzzwords, but seek to define, explain and support with data their assertion that "multi-faceted extortion" is a significant threat.
- The report's recommendations include both specific elements an organization can adjust (e.g., device configurations) and practical concepts (such as using secure enclaves during ransomware recovery) that, when applied, can truly help security teams better prevent, detect and respond to an incident.

# REPORT HIGHLIGHTS

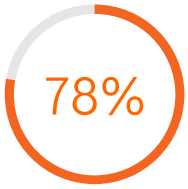
**294**
DISTINCT MALWARE FAMILIES OBSERVED

**59%**
OF INCIDENTS DETECTED BY THE VICTIMS THEMSELVES

**24 DAYS**
MEDIAN DWELL TIME OBSERVED

**5 DAYS**
MEDIAN DWELL TIME IN RANSOMWARE INCIDENTS

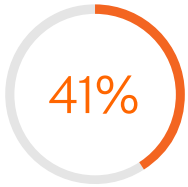
## ATTACK METHODS AND VECTORS




of the malware used is not publicly available


of attacks focused on direct financial gain


of observed malware was ransomware




of observed malware opened a backdoor

# BTB'S TAKEAWAY

At BTB, we review multiple cybersecurity industry studies and research reports on an ongoing basis to compare findings and validate trends. FireEye and Mandiant's new report provides detailed evidence confirming many cybersecurity practitioners' hunches about what's been going on in the threat landscape over the past year. Ransomware continues to make headlines even though it accounts for only a small fraction of the malware that attackers are leveraging to compromise and explore environments. And data exfiltration by ransomware operators is now par for the course, which means that security teams should be responding to every ransomware incident as if it were a confirmed breach. It also means that maintaining comprehensive backups is no longer an adequate strategy to defend against the current ransomware scourge.

At times, the report is a bit self-promotional in tone, with the authors repeatedly patting themselves on the back for naming threat actor groups. Still, it is based on in-depth observations and many years of experience. The report offers well-informed theories to explain the trends the authors are observing. For instance, they postulate that ransomware attacks strategically target verticals like manufacturing where downtime has direct and immediate financial impact. And its recommendations are both detailed and actionable.

### "Living off the land" is common in early stages of ransomware attacks

Today's ransomware attackers continue to leverage native built-in tools like PowerShell, Windows Management Instrumentation (WMI) and command line scripts to cover their tracks as they explore their victim's environment. Privilege management and ongoing security monitoring are must-haves to prevent and detect this activity.

### 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.

### SECURITY IN THE CLOUD REQUIRES ADHERENCE TO FAMILIAR BEST PRACTICES

Maintaining a strong security posture in today's cloud-based and hybrid computing environments demands strong internal access controls, MFA, ongoing monitoring and robust patch and asset management. The basic principles – visibility and awareness – haven't changed.

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.**