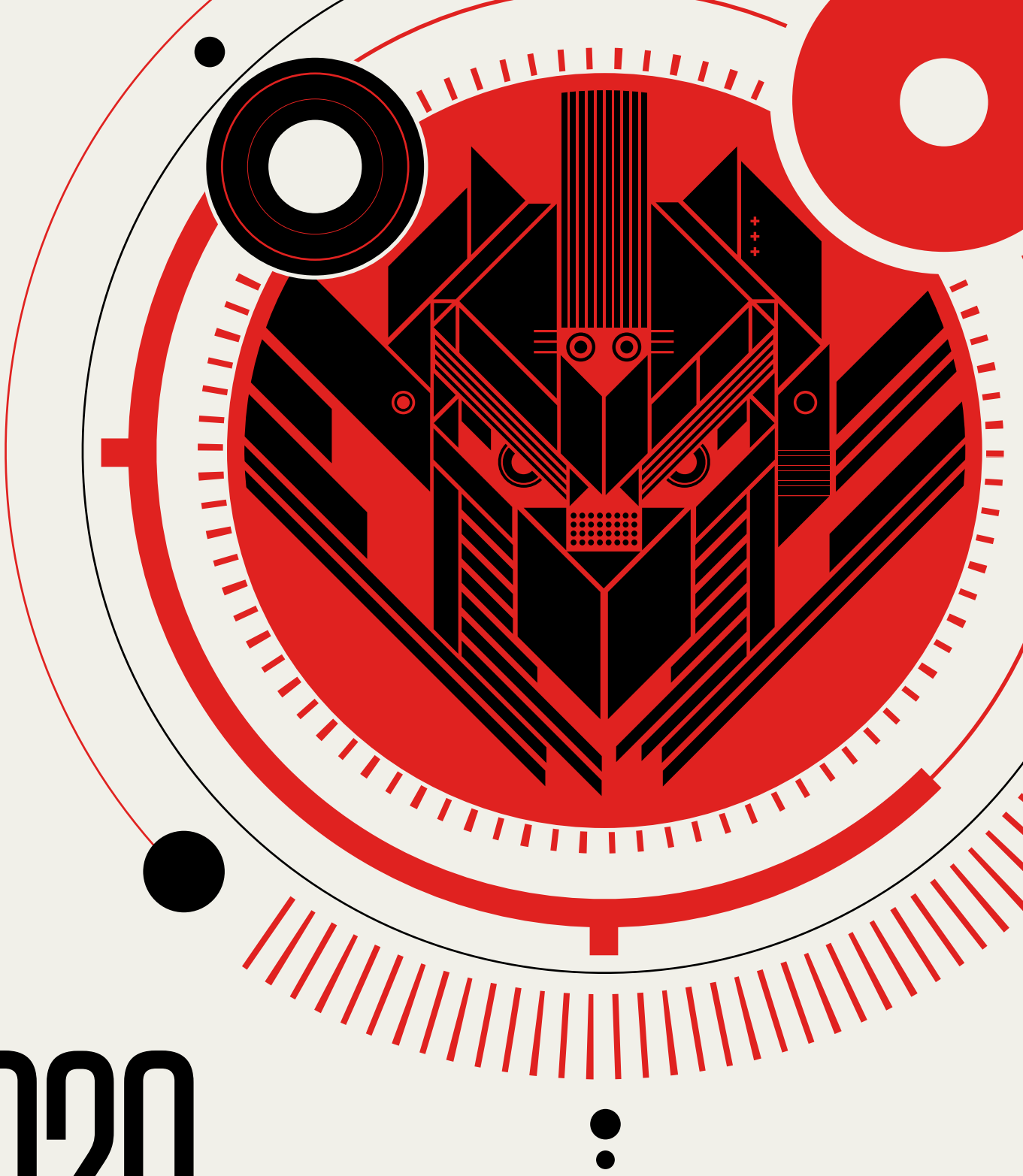

2020 GLOBAL THREAT REPORT

CROWDSTRIKE

FOREWORD

While criminals are relatively predictable in their tendency to always choose the path of least resistance, the activities of nation-states are frequently more relentless and sophisticated — and as a result, more challenging for cyberdefenders.

Those of us who have worked in cybersecurity for many years often start to think we've "seen it all." We haven't. This year's CrowdStrike® Global Threat Report provides clear evidence of that.

Consider the dark turn in cybercrime toward preying on schools, municipal departments and our other chronically understaffed and overburdened public institutions. This is different from targeting large government entities and corporations, many of whom have resigned themselves to being targeted by cyber predators and have the opportunity to try to protect themselves from that onslaught. It's a different matter entirely when the targets are schoolchildren, or just ordinary people trying to go about their daily lives.

This merciless ransomware epidemic will continue, and worsen, as long as the practice remains lucrative, and relatively easy and risk-free. We've developed a platform designed to stop ransomware for our customers, and we've worked hard to make it easy and affordable — even for budget-constrained institutions like our public school systems. As more organizations around the world deploy next-generation platforms like CrowdStrike Falcon® that can prevent these threats, the criminal element will be forced to redirect its efforts elsewhere.

While criminals are relatively predictable in their tendency to always choose the path of least resistance, the activities of nation-states are frequently more relentless and sophisticated — and as a result, more challenging for cyberdefenders. This year's threat report uncovers numerous new tactics, techniques and procedures (TTPs) that state-affiliated threat actors are employing to accomplish their goals. Of concern here is the widening variety of goals these highly capable adversaries may seek to achieve. Along with the more traditional objectives of espionage and surveillance have been added new tasks, such as sowing widespread disruption and discord among individuals, institutions and even whole countries and populations, all in pursuit of political and economic gains.

If there's one thing this year's Global Threat Report really brings home, it's that there's never been a better time to get involved in cybersecurity. The stakes are high, and rising every day. Those that read and share this report are helping to educate themselves and others to better protect themselves and their communities, both at work and at home.

George Kurtz
CrowdStrike CEO and Co-Founder

TABLE OF CONTENTS

INTRODUCTION

From U.S. school districts to asset management firms, from manufacturing to media, ransomware attacks affected multitudes of people. Disruption in 2019 was not punctuated by a single destructive wiper; rather, it was plagued by sustained operations targeting the underpinnings of our society.

A year in cybersecurity is often marked by how disruptive the activity observed was — not just from a destructive standpoint, but also from the perspective of whether day-to-day life was affected. By any such measure, 2019 was an active year. From U.S. school districts to asset management firms, from manufacturing to media, ransomware attacks affected multitudes of people. Disruption in 2019 was not punctuated by a single destructive wiper; rather, it was plagued by sustained operations targeting the underpinnings of our society. The particularly disruptive impact that ransomware had across all sectors is addressed at the beginning of this report, followed by an assessment of additional eCrime threats.

Going into 2019, CrowdStrike Intelligence anticipated that big game hunting (BGH) — targeted, criminally motivated, enterprise-wide ransomware attacks — was expected to continue at least at the 2018 pace. However, what was observed was not just a continuation but an escalation. Ransom demands grew larger. Tactics became more cutthroat. Established criminal organizations like WIZARD SPIDER expanded operations, and affiliates of the ransomware-as-a-service (RaaS) malware developers adopted BGH attacks. In short, the greedy got greedier and the rich got richer.

Other criminal actors took note. Numerous adversaries specializing in the delivery or development of malware benefited from supporting customers or partners conducting BGH operations. Malware-as-a-service (MaaS) developers like VENOM SPIDER introduced ransomware modules. Banking trojans continued to be repurposed for download-as-a-service (DaaS) operations — a trend started by MUMMY SPIDER — used to distribute malware families associated with BGH. Even targeted eCrime appears to be in a state of change, apparent by the recent activity attributed to GRACEFUL SPIDER, an adversary notable for its high-volume spam campaigns and limited use of ransomware.

As in years past, the majority of state-sponsored targeted intrusions appeared to be motivated by traditional intelligence collection needs. Analysis in 2019 revealed a focus by Chinese adversaries on the telecommunications sector, which could support both signals intelligence and further upstream targeting. Content related to

defense, military and government organizations remains a popular lure for targeted intrusion campaigns. Examples of such incidents were seen in the activity of Russian adversaries targeting Ukraine, and the use of defense-themed job and recruitment content by Iran-based IMPERIAL KITTEN and REFINED KITTEN.

While traditional espionage is the primary objective of many state-sponsored actors, adversaries associated with the Democratic People's Republic of Korea (DPRK, aka North Korea) sustained their interest in cryptocurrencies and the targeting of financial services, with identified incidents linked to all five named DPRK-associated adversaries tracked by CrowdStrike. Exact motives remain unconfirmed, but it is possible this interest in financial sector organizations represents additional currency generation operations and/or industrial espionage. Industrial espionage is also a suspected motive for Vietnam's targeting of the automotive sector and China's targeting of healthcare and other sectors, bringing the threat of intellectual property theft back into the spotlight.

In the following sections, the CrowdStrike Intelligence team, the Falcon OverWatch™ managed threat hunting team and the CrowdStrike Services team present selected analysis that highlights the most significant events and trends in the past year of cyber threat activity. This analysis demonstrates how threat intelligence and proactive hunting can provide a deeper understanding of the motives, objectives and activities of these actors — information that can empower swift proactive countermeasures to better defend your valuable data now and in the future.

Numerous adversaries specializing in the delivery or development of malware benefited from supporting customers or partners conducting BGH operations.