CROWDSTRIKE

# CROWDSTRIKE SERVICES CYBER FRONT LINES REPORT

## INCIDENT RESPONSE AND PROACTIVE SERVICES FROM 2020 AND INSIGHTS THAT MATTER FOR 2021

# TABLE OF CONTENTS

# FOREWORD

**Welcome to the latest edition of the CrowdStrike® Services Cyber Front Lines Report!**

In the year since our last report was published, a pandemic has changed not only cybersecurity practices globally, but also our jobs as defenders in the digital space. Our jobs as defenders are more complicated, require more advanced skills and are more important now than ever. Moving from a traditional corporate IT stack to a global "work from anywhere" workforce in a few short weeks was truly a remarkable undertaking for many organizations, and the adversaries took notice. Attackers — both eCrime and state-sponsored — continued to quickly adapt to broad industry changes in an effort to leapfrog legacy defenses, deploy new ransomware and execute data extortion attacks. They persisted in exploiting the path of least resistance, facilitated by the increased attack surface created by the remote workforce, preying on victims' emotions and corporate vulnerabilities.

We learned the basic cybersecurity principles we've always advocated remain critical: asset inventory, vulnerability management, multifactor authentication, network segmentation, system backup and recovery, and more. Our Services mission has always been focused on helping organizations train for, react to and remediate a breach quickly and effectively to allow them to get back to business faster. In light of the events of 2020, we have organized our responders into "Front-Line Teams" that have a stronger and more defined focus on each of these essential areas:

- **Incident Response (IR):** Rapid response, containment and investigation with digital forensics and root cause analysis
- **Endpoint Recovery Services:** Containment of active threats, recovery and remediation with speed and surgical precision
- **Falcon Complete™:** Continuous 24/7/365 managed detection, response and remediation, backed by up to $1M Breach Prevention Warranty

This report outlines trends we've identified in the data we collect from hundreds of engagements, along with key themes we've observed, to enable you to better protect your organization. I encourage you to review it from your perspective — in a similar situation, what would you, your teams and your organizational leadership do? Perhaps more importantly, how would you fare? Identifying your vulnerabilities, becoming more aware and educating yourself is half the battle.

We know attackers will continue to refine their techniques and strengthen their skills to evade security, monetize their access and/or reach their ultimate objective. The year 2020 saw more intrusions than ever before, larger ransomware demands and little opportunity for organizations to improve their security posture while keeping pace with the chaos brought on by the global pandemic. Corporate defenders are spread thin, and adversaries are well organized and better funded than ever, making it much more difficult to detect and respond to threats.

All is not lost though. CrowdStrike is steadfastly helping our customers move from simply reacting to breaches days or weeks after the fact to continuous monitoring, detection, response and optimization. We are glad you trust us to provide you with the support you need to safeguard your critical assets, especially in these uncertain times. We appreciate your confidence and thank you for your partnership.

One team, one fight.

Shawn Henry

**Shawn Henry**
CrowdStrike, President of Services and Chief Security Officer

# EXECUTIVE SUMMARY

The CrowdStrike Services Cyber Front Lines report brings together the insights and observations of dedicated CrowdStrike team members from all corners of the globe, who work tirelessly to help organizations defend against and recover from intrusions every day. Not only does the report provide a clear picture of how adversaries are adapting to today's realities, it also includes concrete recommendations that you can implement in your organization today to improve your cybersecurity readiness.

The findings and trends in this report are derived from data points and insights collected from a wide variety of incident response (IR) engagements and proactive services activities over the past 12 months. Key findings from these metrics include:

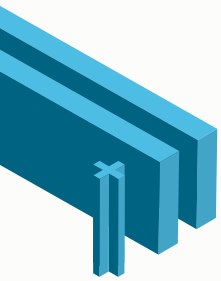
- **The volume and velocity of financially motivated attacks are staggering.** Financially motivated attacks represented 63% of CrowdStrike Services cases over the past year, with 81% of financially motivated attacks involving the deployment of ransomware or a precursor to ransomware activities.

- **Buying technology alone is not enough — configuration, coverage and management matters.** In at least 30% of incident response engagements, CrowdStrike observed the organization's antivirus solutions were either incorrectly configured with weak prevention settings or not fully deployed across the environment, which may have been a factor in the threat actor gaining and maintaining access.

- **Intrusions should not be thought of as a one-time event.** The Services team looked at organizations that experienced an intrusion and then leveraged CrowdStrike to manage their endpoint protection and remediation efforts moving forward. Crowdstrike identified that 68% of those organizations experienced another intrusion attempt, which was prevented.

- **Shifting to continuous monitoring and response changes the game.** Rather than thinking of intrusion response as a one-off emergency activity, mature organizations plan for real-time, continuous monitoring and response. CrowdStrike's Falcon Complete managed service offering reduced the average time to detect, investigate and remediate from a total of 162 hours — nearly seven days — to less than one hour for customers.

- **Outside counsel is playing a bigger role in the incident response process.** Outside counsel retained CrowdStrike to advise its clients in 49% of the incidents investigated in 2020.



**The volume and velocity of financially motivated attacks are staggering.**

In addition to these findings, CrowdStrike's incident responders identified a number of key themes in 2020. Organizations should be mindful of the following:

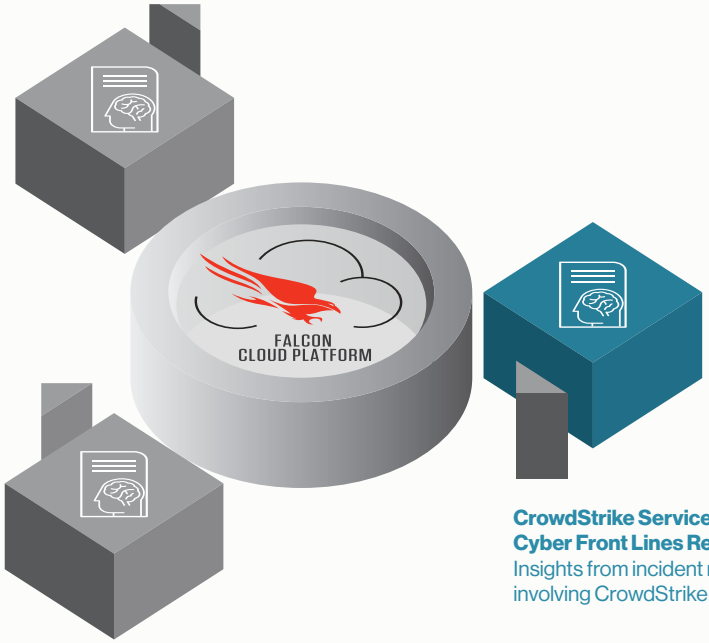
- **Widespread remote work has broad-reaching effects on cybersecurity.** Networks around the world were turned inside-out as office workers became remote workers, with dramatic effects on how attackers target organizations and how defenders must react.
- **Ransomware actors have learned new tricks.** Not content with just encrypting data for extortion, eCrime actors are increasingly destroying and/or threatening to leak data, as they target ever larger ransom payments.
- **Cloud infrastructure requires special attention from defenders.** The global pandemic accelerated digital transformation — including cloud adoption — for many organizations, and attackers took advantage of this attack surface. Defending the cloud requires additional planning and focus beyond traditional on-premises networks.
- **Weaknesses in public-facing applications and services are increasingly dangerous.** CrowdStrike observed significant increases in attackers targeting public-facing applications and services in 2020. Defenders must continue to be vigilant to ensure no exterior gaps exist for an adversary to use as an initial foothold.
- **State-sponsored adversaries leave smaller footprints.** While eCrime actors got most of the headlines in 2020, state-sponsored adversaries remained active across a wide range of sectors. Detecting and stopping these sophisticated intrusions requires a well coordinated and holistic response.
- **Organizations focused on driving key security enhancements can stop the next breach.** An intrusion can happen to any organization — how you respond and learn from prior incidents can make a significant difference on the impact of the next breach.

Organizations that heed the observations and recommendations in this report will see significant improvements in their ability to defend against many of the common types of attacks. CrowdStrike is here to help, providing highly skilled cybersecurity professionals who partner with clients, ensuring that the adversaries are defeated and any damage is quickly remediated.

# A UNIQUE PERSPECTIVE

## CROWDSTRIKE'S POWERFUL REPORTS ARE ENABLED BY POWERFUL INSIGHTS

**Falcon OverWatch Threat Hunting Report**
Insights gained from proactive threat hunting conducted in customer environments where the CrowdStrike Falcon platform is deployed




**CrowdStrike Global Threat Report**
Global cyber threat intelligence and insights

**CrowdStrike Services Cyber Front Lines Report**
Insights from incident response engagements involving CrowdStrike Services

CrowdStrike provides a unique perspective when assessing the state of cyber threats, given the company's industry-leading expertise in threat intelligence, managed services and professional services, combined with the power of the massive, cloud-native CrowdStrike Falcon® platform for endpoint and cloud protection. These distinct areas of expertise are represented in three annual publications, each highlighting the contributions and assessments of individual CrowdStrike teams:

- **CrowdStrike Global Threat Report**
- **Falcon OverWatch Threat Hunting Report**
- **CrowdStrike Services Cyber Front Lines Report**

The CrowdStrike Global Threat Report combines CrowdStrike's comprehensive global observations with real-world case studies to deliver deep insights on modern adversaries and their tactics, techniques and procedures (TTPs). The Falcon OverWatch Threat Hunting Report presents observations from the Falcon OverWatch™ team as they hunt adversaries. This CrowdStrike Services Cyber Front Lines Report documents the real-world experience gained from the Services team as they respond to incidents and breaches. With such a comprehensive and holistic view of the threat landscape, CrowdStrike can provide specific guidance on the actions organizations can take to improve their security posture.

# KEY FINDINGS: DEMOGRAPHICS AND METRICS

In keeping with the format of last year's CrowdStrike Services Cyber Front Lines Report, this year's edition reflects data derived from CrowdStrike Services incident response, managed services and proactive services engagements over 2020. The real-world observations and analysis presented in this report should prove both compelling and practical, as well as the recommendations you can implement within your organization to improve your cybersecurity readiness. The organizations assisted by CrowdStrike during 2020 spanned 15 industry sectors, resided in 34 countries, and varied in size from large global organizations to regionally focused small/mid-sized businesses (SMBs). Of note, CrowdStrike served 25% of the Fortune 100 and 9% of the Global 100 organizations in 2020.

Figure 1 depicts the breakdown of organizations by industry within the dataset leveraged for this report.

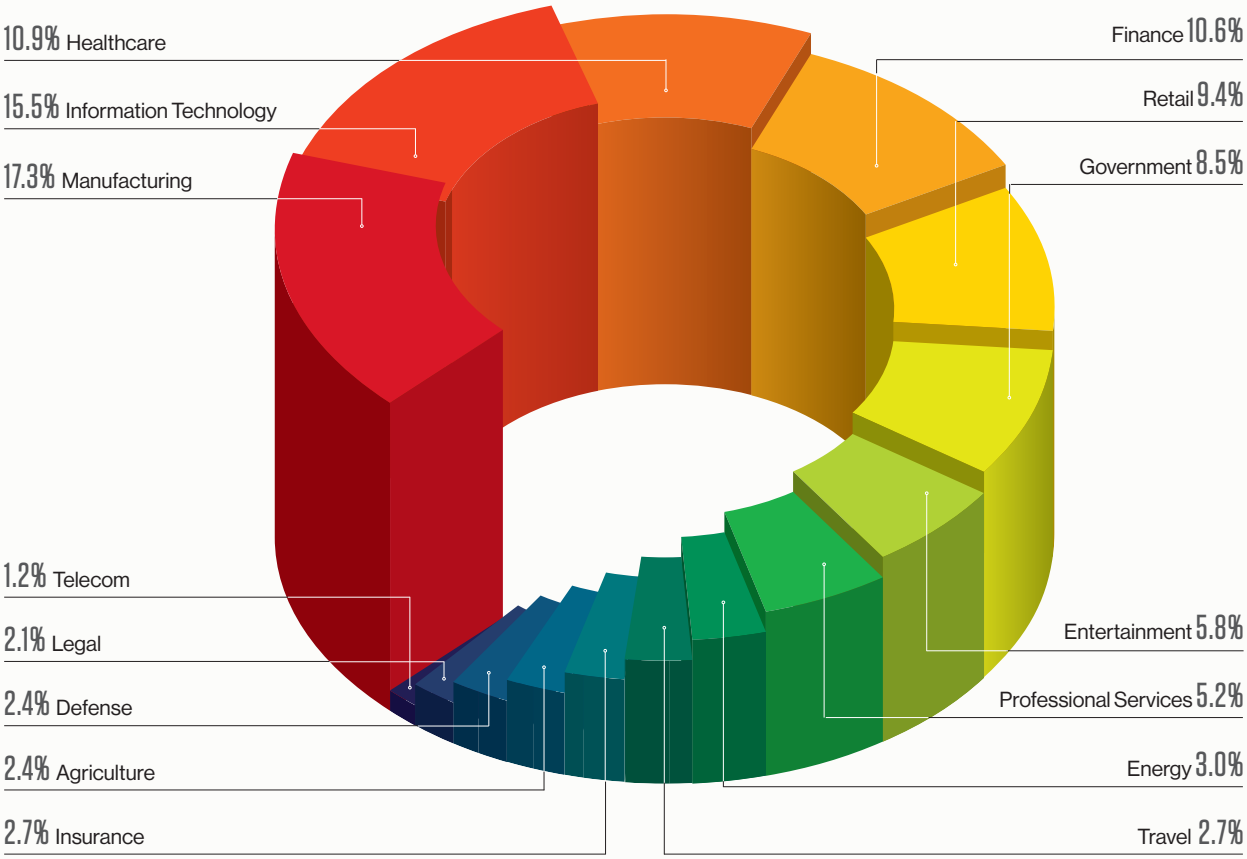



**Figure 1. Organizations that CrowdStrike assisted in 2020 by industry sector**

## ORGANIZATIONS ASSISTED BY CROWDSTRIKE IN 2020

**15**
Industry Sectors

**34**
Countries

**25**
Fortune 100 Companies

**9**
Global 100 Organizations

While the demographics of the organizations supported and the incidents investigated evolve year to year, one thing has remained constant: Cyber adversaries continue to be both relentless and innovative in their efforts to find gaps in your organization's infrastructure and exploit them. While adversary motives vary, in 2020 financially motivated eCrime attacks far outnumber any others by volume — representing 63% of CrowdStrike's incident response engagements. eCrime adversaries operate in both targeted and opportunistic ways, leaving no organization — regardless of structure, size, industry or location — immune from attacks.

As with reports in years past, this report offers statistics and anecdotes that provide unique visibility into the adversaries and trends the CrowdStrike Services team is seeing from the front lines of working with organizations. Based on the numbers derived from Services engagements, the following trends have been observed.

## THE VOLUME AND VELOCITY OF FINANCIALLY MOTIVATED ATTACKS IS STAGGERING

Sixty-three percent of incidents investigated in 2020 involved financially motivated threat actors. These attacks ranged from ransomware targeting organizations of all shapes and sizes, to unauthorized financial transactions in regionally focused SMBs, all the way to large global enterprises. Among the financially motivated eCrime attacks, 81% involved ransomware. The other 19% included eCrime attacks such as point-of-sale intrusions, ecommerce website attacks, business email compromise and cryptocurrency mining.

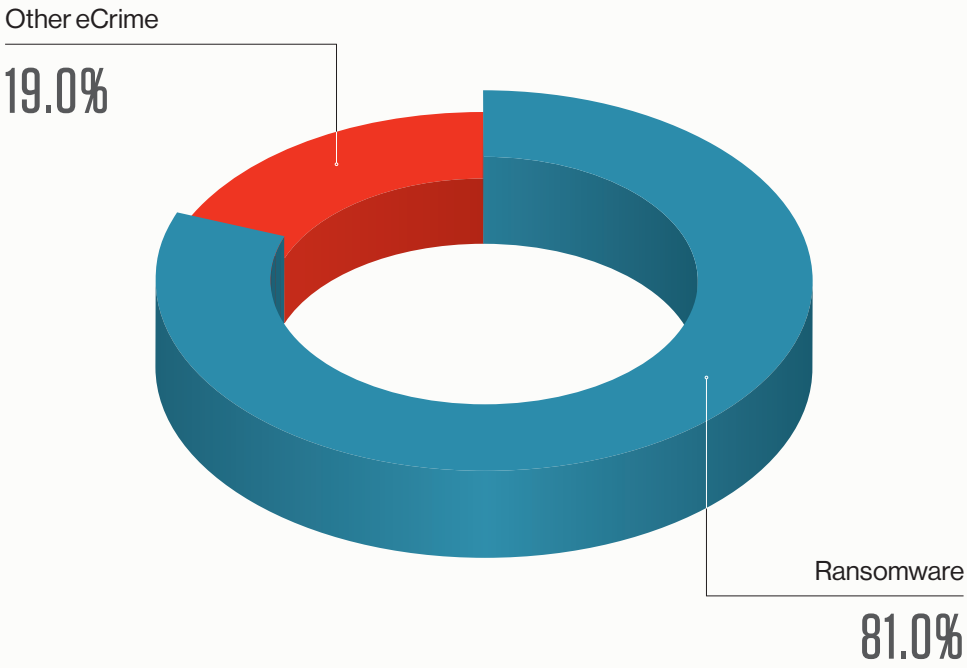



**Figure 2. Ransomware involved in financially motivated eCrime attacks in 2020**

## THREAT ACTORS ARE UPPING THEIR GAME WITH MALWARE THAT EVADES TRADITIONAL ANTIVIRUS

As ransoms often continue to exceed seven figures and eCrime generally becomes more lucrative, threat actors have additional capital and continue to mature their organization to raise their game. What used to be smaller-scale business operations have become big businesses generating exponential growth in revenue. With this, threat actors are investing more into the development and deployment of techniques that evade antivirus countermeasures. Antivirus solutions failed to provide protection in 40% of the incidents CrowdStrike responded to in 2020 in which either malware was undetected or a portion of the attack sequence was missed by antivirus tools. And in 30% of incidents, antivirus or endpoint detection and response (EDR) tools were not fully deployed, were improperly configured or were not supported on the operating system. This data highlights why it is important to protect your organization with next-generation antivirus solutions that leverage the cloud for scalability and use modern techniques including machine learning and behavioral detection to identify advanced threats. It also emphasizes the need to not just buy a security product, but actually invest in ensuring comprehensive coverage in your environment and proper configuration, tuning and integrating it into your security operations program to mitigate even the most sophisticated attacks.

# AT A GLANCE

Here are a few additional data points that reveal insights into the more successful attack techniques, as well as some benchmarks for defenders.

**Self-identification of a breach** is when an organization proactively identified a breach without notification from a third party such as law enforcement. While victims self-identified a breach in 69% of cases, in 14% the breach was identified due to the execution of ransomware. Please note this is the first year that ransomware execution is being tracked as its own category.

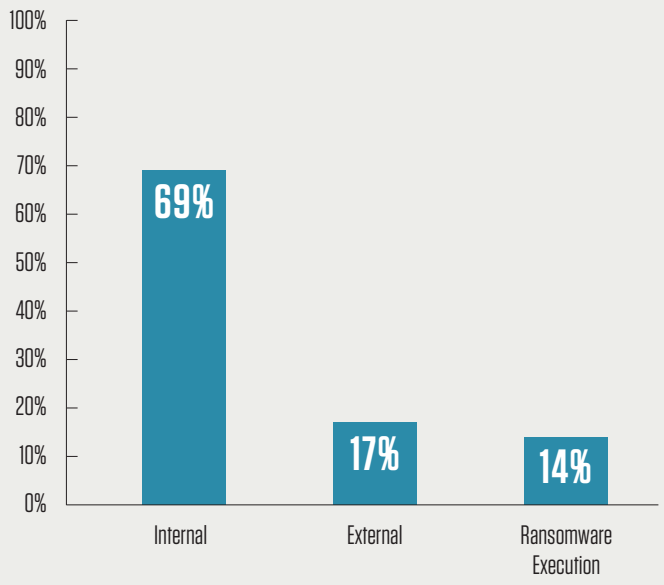



**Figure 3. Method by which intrusions were detected in 2020**

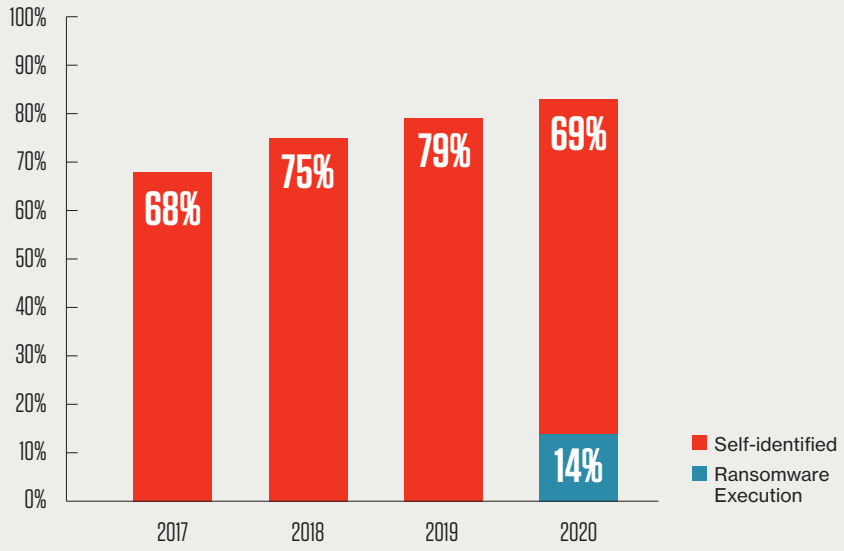



**Figure 4. Organizations that self-identified a breach, 2017-2020**

**Dwell time** — the time an adversary has unfettered access to a compromised system — is down slightly from 95 days in 2019 but still remains quite high, at 79 days in 2020. Some organizations are getting faster at identifying a breach within one week, but CrowdStrike also observed a slight increase in the percentage of cases with dwell times greater than six months. It is worth noting that the average dwell time for ransomware attacks was 45 days in 2020, but in 26% of the ransomware cases CrowdStrike observed, the dwell time was just a single day, and in 48% it was less than one week.

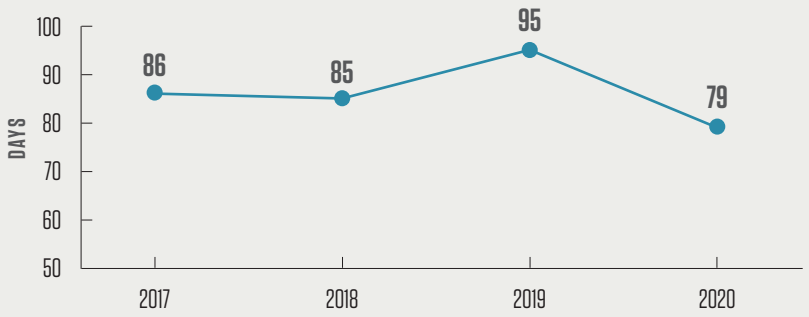



**Figure 5. Average dwell time of attackers, 2017-2020**

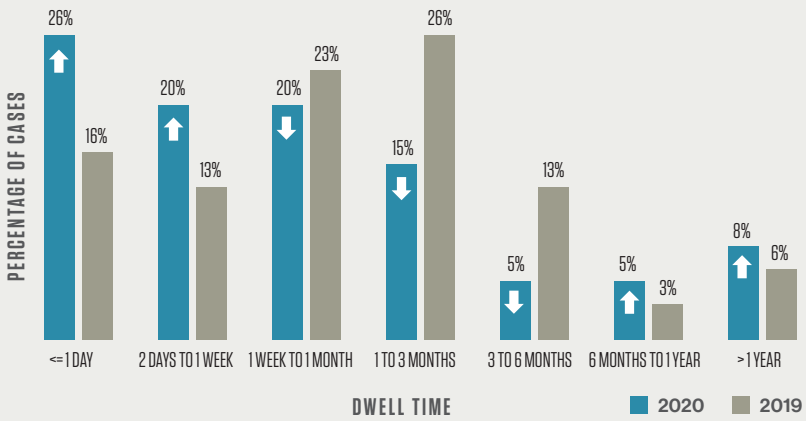



**Figure 6. Change in dwell time from 2019 to 2020**

Adversaries are increasing their use of **malware-free** attack techniques, although malware is still frequently used.

| | Malware Only | Malware Free | Both |
|---|---|---|---|
| 2020 | 42% | 24% | 33% |
| 2019 | 49% | 22% | 29% |

**Table 1. Use of malware-free attack techniques, 2019 vs. 2020**

Drilling into malware-free techniques shows a high prevalence of attacks against user accounts as well as use of hands-on-keyboard techniques — essentially unchanged from 2019.

| Top 5 MITRE ATT&CK® Techniques 2020 |
|---|
| Credential Dumping |
| PowerShell |
| Scripting |
| Command-Line Interface |
| Account Discovery |

**Table 2. Top malware-free attack techniques in 2020**

**68%**

**OF ORGANIZATIONS STUDIED POST-IR ENCOUNTERED ANOTHER SOPHISTICATED INTRUSION ATTEMPT WITHIN THE NEXT 12 MONTHS**

## INTRUSIONS SHOULD NOT BE THOUGHT OF AS A ONE-TIME EVENT

Organizations that engage a professional services firm for incident response are often eager to get the experience behind them and move on with business as usual. Completion of an incident response, however, represents a critical opportunity to drive improvements in people, process, technology and cybersecurity maturity that should not be overlooked. Ignoring this opportunity to mature leaves organizations exposed to the next intrusion, which is rarely far down the road.

CrowdStrike examined data from organizations that engaged incident response services and later opted to engage CrowdStrike for fully managed endpoint protection through the Falcon Complete service. Of these organizations, 68% encountered and stopped another sophisticated intrusion attempt within the next 12 months.

It is tempting to think of intrusions as a lightning strike — a blinding flash that is unlikely to strike the same place twice. Unfortunately, intrusion attempts are rarely a one-time event. Organizations that do not take the opportunity to apply lessons learned and to better prepare for their next encounter with an adversary may well suffer attacks that result in additional data loss, ransom demands, extortion or other monetary losses requiring costly legal fees, response services and perhaps even future business interruption.

## CONTINUOUS MONITORING AND RESPONSE CHANGES THE GAME

The key metric in effectively dealing with ongoing and recurring attacks is the time it takes to remediate. Effective response and remediation of a threat first requires detecting the threat, then performing the necessary investigation to scope and understand it, and finally taking the needed actions to remediate the threat. Of course, while the defenders are executing this playbook, adversaries are not standing still. The fastest player wins this race.

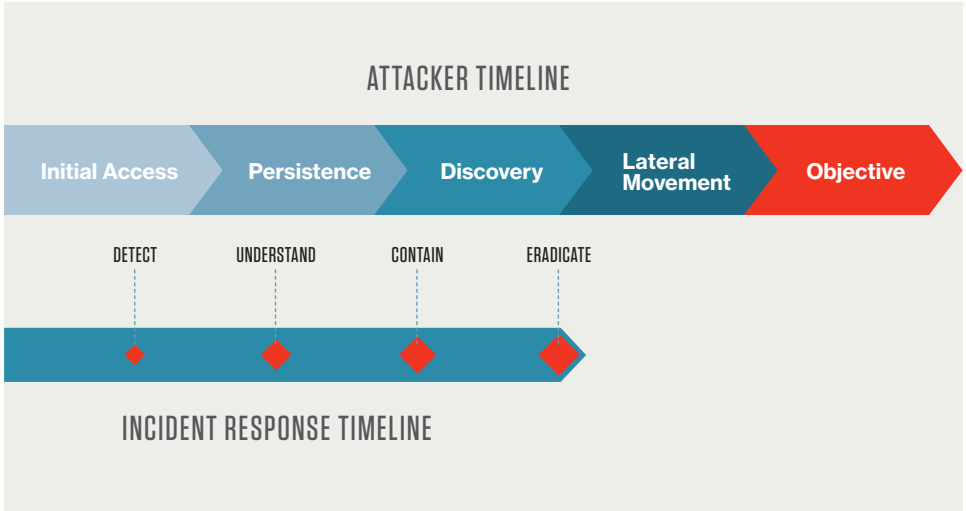



**Figure 7. The Incident Response Race: First to the goal line wins!**

CrowdStrike maintains a strong focus on acting quickly to stop a breach, clean up malicious artifacts and help organizations get back to business quickly. CrowdStrike encourages organizations to strive to meet the 1-10-60 rule, where security teams demonstrate the ability to detect threats within the first minute of an intrusion, investigate and understand the threat within 10 minutes, and contain and eradicate the threat within 60 minutes.

In 2020, CrowdStrike introduced its Endpoint Recovery Services (ERS), specifically designed to help customers bring their core business operations back quickly while minimizing the risk of the attacker's foothold within the environment. While traditional incident response focuses on understanding an attacker's activity and determining root cause, ERS focuses on quickly removing malware and other artifacts from infected systems, blocking malicious activity and closing holes so the attackers cannot get back in. CrowdStrike is seeing more organizations combine Incident Response Services with ERS, which provides a powerful combination of detailed root cause and impact (often demanded by cyber insurers and outside counsel) along with fast and effective recovery. For more information, read this CrowdStrike white paper, **"Intelligence-led Rapid Recovery."**

Of course, the fastest way to handle intrusions is not to have one in the first place. The most effective security teams handle intrusion attempts in near real time, as they happen. At CrowdStrike, this is called "continuous monitoring and response" — and this mindset shifts the balance of power strongly in favor of the defender. Continuous monitoring and response requires a 24/7/365 security operations center (SOC) team that is empowered with the advanced technology and mature processes needed to quickly and effectively handle all kinds of cyber threats.

The CrowdStrike Falcon Complete team was created around this notion of continuous monitoring and response, and the team has built and optimized its operations to deliver security operations excellence for their global customer base.

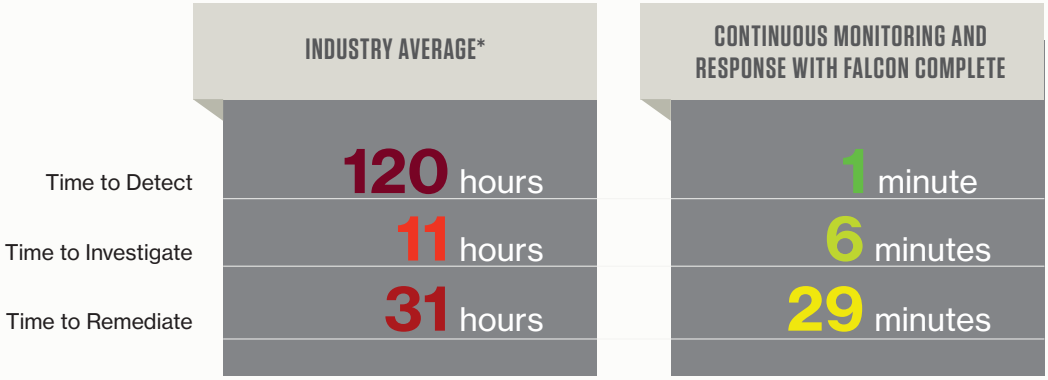



**Figure 8. Industry average time to detect, investigate and remediate vs. Falcon Complete, 2020**

Shifting SOC tactics from incident response to continuous monitoring and response is key to stopping breaches in 2021 and beyond. CrowdStrike encourages all organizations to examine their own response times and look for opportunities to lower these metrics, turning the tables on the adversaries.

*Source: CrowdStrike 2019 Global Security Attitude Survey

**49%**

**OF INCIDENT RESPONSE SERVICES ENGAGEMENTS WERE BROUGHT TO CROWDSTRIKE SERVICES BY OUTSIDE COUNSEL**

## OUTSIDE COUNSEL IS PLAYING A BIGGER ROLE IN THE INCIDENT RESPONSE PROCESS

As organizations become more mature and understand the risks associated with breaches, they are careful that sensitive information about an incident does not fall into the wrong hands or, if released, does not potentially increase the liability they face. When dealing with a data breach, it is becoming best practices to engage the incident response partner through outside counsel. When handling a cyber event, work performed in order to gather information for the purpose of assisting an attorney in rendering legal advice may be protected under attorney-client privilege and/or work product doctrine, preventing it from being open to discovery in a lawsuit. Attorney-client privilege is designed to protect confidential communication between attorneys and their clients, and the work product doctrine precludes disclosure of materials created at the direction of counsel specifically in preparation for litigation.

In 2020, outside counsel engaged CrowdStrike Services to advise its clients in 49% of investigations. This trend has increased globally and will likely continue over the next several years. While the same legal constructs do not exist in every country, multinational organizations that conduct business in the United States or other jurisdictions may want to consult outside legal counsel at the outset of an incident response to determine how best to engage an investigation firm.

Preserving attorney-client privilege and work product protections during incident response and recovery engagements is no small task. If you are interested in understanding more about engaging CrowdStrike Services through outside counsel for your next cyber investigation and incident recovery, read this paper developed by CrowdStrike Services in conjunction with representatives from an IT technical services firm and a forensic accounting firm: **Intelligence-led Rapid Recovery.**

# KEY THEMES

As CrowdStrike's teams of experts engage with clients around the world to contain and eradicate threats and drive more mature cybersecurity practices, patterns emerge. In addition to the findings already discussed, the CrowdStrike Services team identified a number of key themes from the work performed across all customer engagements over the past year. This next section dives deep into the top six key themes from 2020.

**56%**
**OF SURVEY RESPONDENTS REPORTED WORKING FROM HOME MORE OFTEN**

**60%**
**OF SURVEY RESPONDENTS ARE USING PERSONAL DEVICES WHILE WORKING REMOTELY***

## THEME 1: SECURITY IN SWEATPANTS: HOW WIDESPREAD REMOTE WORK CHANGES SECURITY

The year 2020 brought quick and decisive digital transformations across industries in response to remote work requirements. During this "Great Pivot," many organizations effectively turned their networks inside out to allow employees to work from anywhere. This pivot also accelerated both the ongoing adoption of cloud technologies and the organizational support for hybrid working environments. Some organizations accomplished several years' worth of digital transformation in a matter of weeks. As a result, CrowdStrike saw more organizations seeking to move away from traditional on-premises cybersecurity solutions and toward cloud-centric architectures. For these organizations especially, identity management and workload security — including endpoints, cloud workloads, mobile devices, etc. — are crucially important.

### NETWORKS TURNED INSIDE OUT

The operational and architectural pivot to a work-from-anywhere model occurred under extreme time and operational pressures, resulting in significant changes to operations and even network configurations themselves. Suddenly, organizational perimeters dramatically changed as employees began accessing network resources from new locations, and in some cases, with new devices. This pivot also forced organizations to change some of their own operations. For instance, many companies that did not previously permit remote access to corporate networks, like virtual private networks (VPNs), suddenly found that they needed to enable these technologies to support a fully remote workforce.

*Source: CrowdStrike 2020 Work Security Index Survey

Despite the best efforts of the technology teams that implemented these changes, attackers have consistently capitalized on new opportunities arising from security gaps or unintentional configuration errors. In 2020, CrowdStrike Services responded to multiple cases in which the transition to remote operations resulted in unauthorized remote access to internal systems. In some of these cases, companies had adjusted configurations on corporate laptops to allow expanded use of VPN and RDP, but did not implement best practices to restrict activity to approved internal IP addresses or require the use of multifactor authentication.

**Attackers have consistently capitalized on new opportunities arising from security gaps or unintentional configuration errors.**

## TARGETS NEW AND OLD

Individual users remain a significant target of opportunity for attackers seeking to infiltrate organizations. However, the move to "work from anywhere" has expanded the potential methods that attackers can employ to exploit users. CrowdStrike continues to observe attackers leveraging remote access credentials to gain access to target environments. Conversely, the pivot to remote work highlights the difficulty that many security teams face in administering and patching systems when users are not required to connect to the domain with a VPN.

Meanwhile, attackers also continue to exploit vulnerabilities that existed before widespread remote work. Organizations that lack robust system configuration controls have faced challenges in applying patches, deploying security updates and performing standard maintenance activities for devices. CrowdStrike has worked with organizations that experienced attacks stemming from initial access gained through vulnerabilities in publicly exposed systems and applications.

## SECURITY AFTER THE GREAT PIVOT

In this work-from-anywhere landscape, security teams must remain vigilant in performing the fundamentals of cybersecurity. Organizations that migrate to cloud-centric architectures must become more focused on implementing effective identity and device-based access controls, steering access controls toward a posture of Zero Trust. All employees who participate in information security — from leadership to supporting team members — must clearly understand their roles and be ready to perform them, especially under these high-stakes conditions as organizations continue to transition to work from anywhere.

CrowdStrike recommends the following practices:

- **Survey your battlefield.** For security teams operating in this new environment, visibility and speed are critical for blocking attackers that have the capability and intent to steal data and disrupt operations. As organizations increasingly support work-from-anywhere operations, security teams must establish consistent visibility into on-premises and cloud environments and must proactively address potential vulnerabilities before they can be leveraged by attackers.

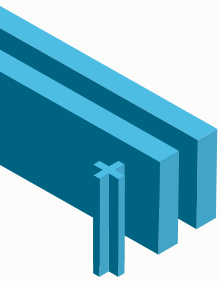
- Local and cloud-hosted applications should be consistently patched, and business-critical applications should be carefully monitored and maintained.
- Security teams should reinforce their understanding of externally facing devices by performing routine vulnerability and asset management scans.
- All perimeter devices — including network DMZs, jump servers, and web and email servers — should be treated as high-risk systems and subjected to security reviews equivalent to critical systems on the network.
- Security and infrastructure teams should ensure that externally facing systems are hardened by closing unnecessary ports and network services, applying strict firewall policies and properly segmenting networks.
- Access control policies should be applied and security teams should monitor for unauthorized attempts to access networks, such as through brute-force vulnerability exploitation or similar techniques.
- Security teams should be able to readily discover cloud assets, detect misconfigurations and quickly perform remediation in their cloud environments.

- **Establish Zero Trust controls for critical systems and data.** CrowdStrike continues to observe attackers focusing their attention on identity-based attacks, with diverse adversaries leveraging compromised or weak credentials to evade detection and access “crown jewels” and critical systems. The concept of Zero Trust security addresses the problem of access exploitation by continuously vetting access requests to locally or cloud-hosted assets. While implementing Zero Trust may sound like a daunting task, focusing on the fundamentals and closing the biggest gaps in your environment with Zero Trust principles have the most immediate impact and can be achieved in a short amount of time. Organizations can achieve quick time-to-value with Zero Trust by focusing on privileged or over-privileged accounts, building a baseline of behavior based on access, and putting in prevention or conditional access in high-risk authentication scenarios (e.g., RDP access to Domain Controller, and service account RDP). Zero Trust may also include installing multifactor authentication on all systems that hold sensitive data or support key operations, enforcing least-privilege access on sensitive systems, and reducing the size of network zones through micro-segmentation. Zero Trust security typically also involves real-time monitoring, both of potential misuse of sensitive credentials and of suspicious system or data access patterns.

- **Don’t forget about controlling access and data within your cloud environments.** Organizations that leverage cloud or hybrid environments should control and monitor access to these environments through a cloud access security broker (CASB). Regardless of network architecture, organizations should provide their security teams with tools to monitor both user access patterns and the movement of sensitive data. Ultimately,

organizations should reevaluate all default access controls, removing trusted sources and require all connections to be authenticated, authorized and encrypted.

- **Test your operations with tailored exercises.** Even if an organization's move to "work from anywhere" has been relatively smooth, the pivot has likely introduced subtle but significant changes to baseline security posture and response processes. For many companies, long-held assumptions about security processes and workflows may no longer be true — at least not in the way they were once understood. CrowdStrike has seen organizations gain significant value through remote exercises. Remotely hosted red team/blue team exercises highlight new operational challenges — and opportunities — for SOC teams responding to red team attacks. Remote tabletop exercises provide both technical and management teams with crucial opportunities to rehearse incident response activities while all participants — including executives — are limited to virtual interactions. The lessons learned through these proactive engagements pay significant dividends by keeping incident response and management teams alert to evolving threats, nimble in their response, and savvy regarding how organizational processes should evolve to meet current needs.



**BGH ransomware variants have multiplied, evolved and become more sophisticated, with their proliferation going virtually unimpeded by legacy endpoint security tools.**

## THEME 2: RANSOMWARE ACTORS EVOLVE THEIR OPERATIONS

In 2020, CrowdStrike Services observed the continued evolution and proliferation of eCrime adversaries engaging in big game hunting (BGH) ransomware techniques. BGH was first observed by CrowdStrike in 2016 with the introduction of BOSS SPIDER's Samas (aka SamSam) ransomware. In the years that followed, BGH ransomware variants have multiplied, evolved and become more sophisticated, with their proliferation going virtually unimpeded by legacy endpoint security tools. The year 2020 was marked by the trend continuing at an accelerated rate. The advancements by eCrime actors include refinement and application of high-pressure extortion tactics on victim organizations and the sharing or copying of new techniques among different ransomware groups, in addition to a marked increase in the number of ransomware variants. These advancements all but ensure that ransomware will remain a popular method for eCrime actors to monetize breaches in the foreseeable future.

### RANSOMWARE ACTORS INCREASE PRESSURE

CrowdStrike Services observed eCrime adversaries utilizing various techniques to increase pressure on victim organizations to pay their extortion. While in previous years ransomware eCrime adversaries were rarely observed exfiltrating data, 2020 witnessed a widespread adoption of ransomware with data-leak extortion tactics among multiple eCrime groups. This method involves both encrypting a victim organization's environment and also exfiltrating data with the threat to leak it if the extortion demand is not paid. This tactic was initially observed by CrowdStrike

Intelligence with OUTLAW SPIDER in May 2019. However, it was not until November 2019, when TWISTED SPIDER adopted this technique, that it became a catalyst for multiple other eCrime actors, many of which have created dedicated leak sites to threaten exfiltration and distribute data. CrowdStrike Intelligence performed research on known dedicated leak sites beginning in November 2019. The results of this analysis depict growth throughout 2020 in terms of the number of leak sites and the number of victim entities with data published on the leak sites.

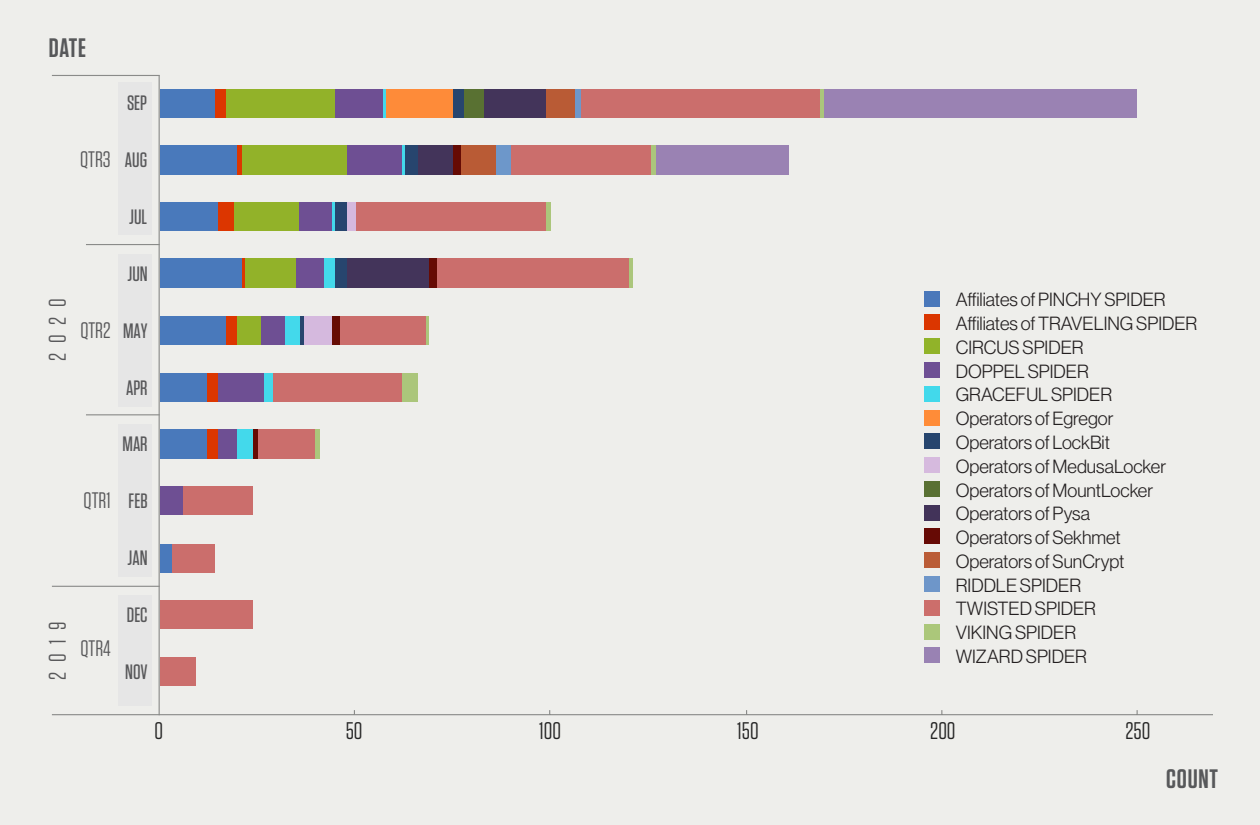



**Figure 9. Number of times that eCrime adversary groups were observed publishing exfiltrated data on dedicated leak sites, Nov. 2019-Sept. 2020**

In engagements involving eCrime adversaries that use ransomware with data-leak extortion, CrowdStrike Services is regularly asked to perform incident response investigations to assist stakeholders by identifying data that was accessed and exfiltrated by threat actors. Frequently, CrowdStrike Services is able to identify the data exfiltrated prior to publication by the eCrime adversary, thereby giving stakeholders an opportunity to prepare.

Not only has the number of eCrime dedicated leak sites grown, threat actors have also become more sophisticated in their methods of leaking the data. In general, eCrime adversaries will leak exfiltrated data slowly, saving what they perceive to be the most sensitive data for last in an effort to increase pressure on the victim organization to

pay the extortion, rather than posting all of the exfiltrated data at once. PINCHY SPIDER's dedicated leak site frequently holds auctions to sell exfiltrated data. Others, such as DOPPEL SPIDER's leak site, utilize a countdown timer that triggers an increase in the ransom demand upon each expiration. CARBON SPIDER's leak site automatically releases data on a pre-set timer, with the least sensitive data leaked first and the most sensitive leaked last. There are also significant differences in the amount of data exfiltrated by threat actors. CrowdStrike Services has observed DOPPEL SPIDER frequently exfiltrating only tens of gigabytes, while others — such as TRAVELING SPIDER and affiliates associated with Nemty X ransomware — exfiltrate hundreds of gigabytes of data or more from victim organizations.

In addition to ransomware with data-leak extortion, CrowdStrike Services has identified additional tactics by eCrime adversaries to increase pressure on the victim to pay the ransom. During several recent incidents, the eCrime adversaries, after deploying ransomware to the victim organization's environment, have utilized stolen credentials to gain access to the victim organization's email instance to send extortion-related emails to users demanding payment to prevent exfiltrated data from being leaked. In other instances, the eCrime adversaries have called and harassed employees of a victim organization following ransomware deployment. Finally, CrowdStrike also observed threat actors increase pressure for payment with credible threats of distributed denial-of-service (DDoS) attacks if ransom payment is not received.

## ECRIME ADVERSARIES COLLABORATE

CrowdStrike has observed formal collaboration among eCrime adversaries as well as shared tactics. In June 2020, the self-named "Maze Cartel" was created when TWISTED SPIDER, VIKING SPIDER and the operators of LockBit ransomware entered into an apparent collaborative business arrangement. After this occurred, leaks associated with VIKING SPIDER's Ragnar Locker began appearing on TWISTED SPIDER's dedicated leak site and Maze ransomware began deploying ransomware using common virtualization software, a tactic originally pioneered by VIKING SPIDER.

In addition to formal collaboration, CrowdStrike Services has observed new tactics used and spread among eCrime actors. One such tactic was the development and deployment of an ELF ransomware binary that can be deployed to ESXi hosts for the purpose of encrypting virtual systems. This tactic was initially observed being used by SPRITE SPIDER's Defray777 ransomware in August 2020 and was quickly adopted by CARBON SPIDER, which utilized a similar tactic weeks later. In addition, multiple eCrime adversaries share common exfiltration techniques. CrowdStrike has observed multiple eCrime adversaries exfiltrating data through MegaSync as well as Rclone, an open-source computer program.

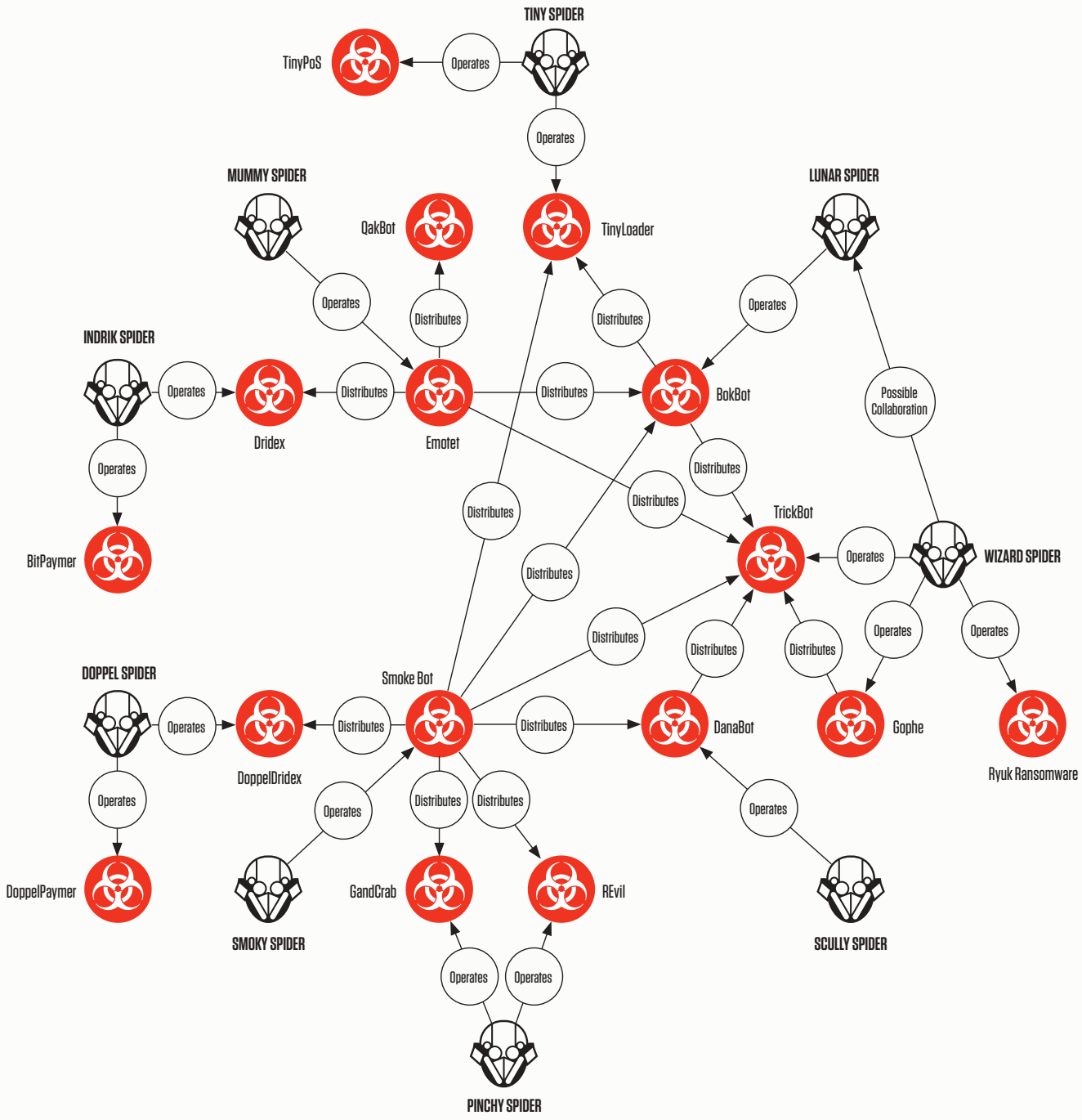



**Figure 10. Mapping of observed relationships between eCrime adversaries by CrowdStrike Intelligence**

## WHAT TO EXPECT NEXT

Over the last several years, eCrime adversaries that engage in BGH ransomware have advanced rapidly in terms of their capabilities and sophistication. It is reasonable to expect that this trend will continue at an accelerated rate with the same goal in mind — to apply as much pressure as possible to organizations to pay ever-larger extortion demands. CrowdStrike expects that eCrime adversaries will continue to refine their data-leak extortion ransomware tactics, develop increasingly sophisticated exfiltration tooling that can be deployed widely, and automate data exfiltration by searching for, identifying and exfiltrating sensitive data by keyword.

Lastly, CrowdStrike expects eCrime adversaries to continue pursuing targets of opportunity. Frequently, these are SMBs that rely heavily on legacy antivirus to protect them, but many large organizations are being hit frequently, as threat actors see a higher return on investment when targeting an organization that may have stronger defenses but is also likely to pay a higher ransom demand.

**Ransomware with data extortion remains a lucrative tactic for eCrime adversaries to monetize their presence in a victim organization's network.**

## WHAT CAN BE DONE?

Why is ransomware so prevalent in 2020? In short, ransomware with data extortion remains a lucrative tactic for eCrime adversaries to monetize their presence in a victim organization's network. Fueled by increasingly larger ransom demands, eCrime adversaries continue to develop tactics and tools that allow them to slip past legacy antivirus virtually unnoticed. Following a ransomware incident, many organizations may find that they do not have adequate backups, or that their backups became encrypted, and they have few options but to pay the ransom. In addition, some cyber insurance companies, during cost-benefit analysis, may find that paying the ransom is a less costly option than rebuilding systems and incurring credit monitoring and legal fees due to the disclosure of regulated data by an eCrime adversary.

CrowdStrike recommends the following practices:

- **Build a bulletproof backup strategy.** When it comes to ransomware, how you've configured your backups is critical. Attackers often delete backups before deploying ransomware so you are more inclined to pay. Some steps to consider include purchasing an immutable backup solution, using separate non-domain accounts with multifactor authentication to administer your backup solution, retaining multiple copies of data on different media with one of them being off-site, keeping at least one copy of your backups offline or on an otherwise air-gapped network, and closely monitoring your backup solution for evidence of data exfiltration, whether it's on-premises or in the cloud. eCrime adversaries have publicly boasted about utilizing cloud backups for data exfiltration, and CrowdStrike recommends taking steps to prevent threat actors from accessing cloud backup infrastructure in the event of a compromise. This can involve using non-domain accounts for cloud management and multifactor authentication.

- **Use multifactor authentication.** Organizations can improve their security posture by enabling multifactor authentication on all public-facing employee services and portals as well as restricting internet-facing protocols such as RDP and Server Message Block. This will inhibit unauthorized access to the organization's environment.

- **Implement next-generation endpoint protection.** Organizations can improve their security posture by utilizing advanced endpoint protection across their environment. The agent should leverage machine learning to identify anomalies and perform heuristic analysis, in addition to conducting antivirus and anti-malware activities in real time. The agent should be capable of detection and prevention, allow for remote network containment of assets pending investigation and/or remediation, and detect unmanaged assets within the corporate environment.

- **Utilize a privileged account management solution.** Organizations can improve their security posture by implementing privileged account management (PAM) that securely containerizes and rotates credentials of privileged accounts such as local or domain administrators, service accounts and database accounts. The PAM should rotate credentials no longer than every eight hours and be capable of alerting if credential reuse is attempted after their expiration, thereby inhibiting threat actor activity.

- **Know when to ask for help.** In some instances, organizations become aware of threat actor activity within their environment but may lack the visibility to address the problem or the right intelligence to understand the nature of the threat. Getting educated about the latest threats and knowing when to ask for help by activating an incident response team or retainer, such as those offered by CrowdStrike Services, may allow for detection and remediation before the threat actor is able to deploy ransomware or exfiltrate data from the environment.

## THEME 3: ADVERSARIES HAVE THEIR HEADS IN THE CLOUD

In many organizations, the adoption of cloud infrastructure had happened to some degree prior to the global pandemic. While the pandemic certainly accelerated the move to the cloud for many organizations, with some electing to go all-in on cloud, other organizations continue to test the waters and gradually move certain services or capabilities into various cloud platforms. CrowdStrike is even seeing some early cloud adopters moving from legacy cloud deployments to new architectures in the hope of gaining improvements in scalability, maintenance and security. No matter where you are in your cloud journey, managing the security posture of cloud environments can play a critical role in preventing a breach.

One trend CrowdStrike saw in 2020 involved threat actors targeting cloud infrastructure slated for retirement or simply neglected for various reasons. This vulnerability likely stemmed from infrastructure no longer receiving security configuration updates and regular maintenance. Unfortunately, security controls like monitoring, expanded logging, security architecture/planning and posture remediation no longer occurred in these environments.

Unfortunately, CrowdStrike encountered cases where neglected cloud infrastructure still contained critical business data and systems. As such, attacks led to sensitive data leaks requiring costly investigation and reporting obligations. Additionally, some attacks on abandoned cloud environments resulted in impactful service outages, since they still provided critical services that hadn't been fully transitioned to new infrastructure. Moreover, the triage, containment and recovery from the incident in these environments had a tremendous negative impact on some organizations as these activities disrupted the release of a key feature launch in one case and delayed M&A activities in another.

Not only did the Services team see cloud infrastructure as a target of attacks in 2020, the cloud also served as a vehicle to launch attacks. Over the past year, threat actors leveraged common cloud services, like Microsoft Azure, and data storage syncing services, like MEGA, to exfiltrate data and proxy network traffic. A lack of outbound restrictions coupled with a lack of workload protection enabled threat actors to interact with local services over proxies to IP addresses in the cloud. This gave attackers additional time to interrogate systems and exfiltrate data from services ranging from partner-operated web-based APIs to databases to custom network services — all while appearing to originate from inside the victim's network and barely leaving a trace on local file systems.

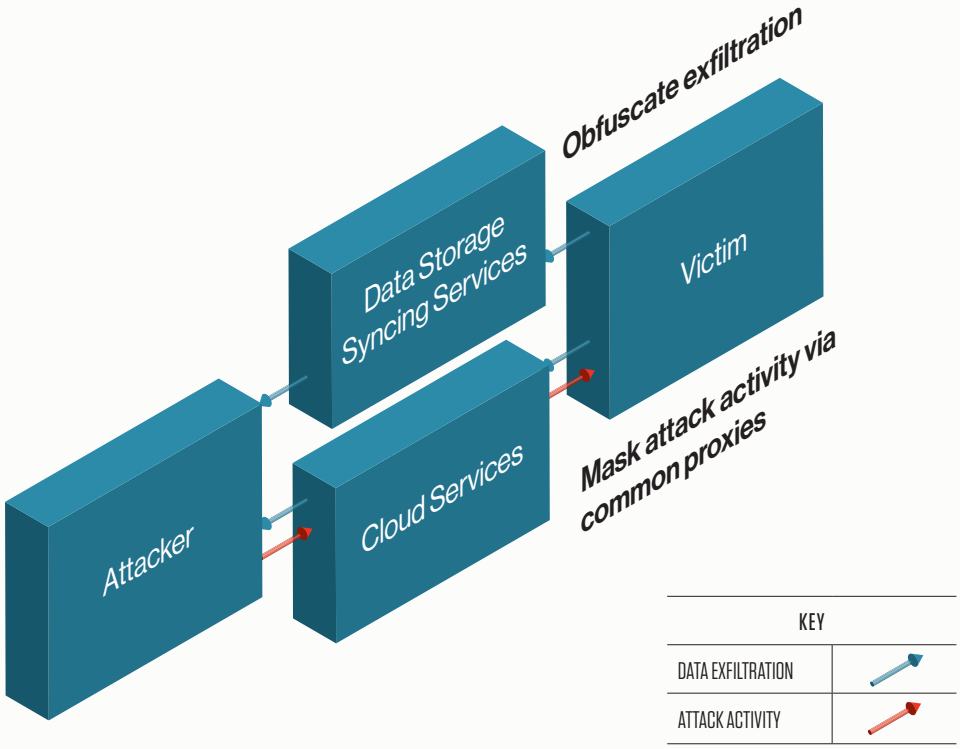



**Figure 11. Attackers leverage common cloud services to obfuscate malicious activity**

## WHAT CAN I DO TO PROTECT MY CLOUD ENVIRONMENT?

The cloud introduces new wrinkles to proper protection that don't all translate exactly from a traditional on-premises data center model. Security teams should keep the following firmly in mind as they strive to remain grounded in best practices.

- **Enable runtime protection and obtain real-time visibility.** You can't protect what you don't have visibility into — even if you have plans to decommission the infrastructure. Central to securing your cloud infrastructure to prevent a breach is runtime protection and visibility provided by cloud workload protection (CWP). It remains critical to protect your workloads with next-generation endpoint protection, including servers, workstations and mobile devices, regardless of whether they reside in an on-premises data center or virtual cluster, or hosted in the cloud.

- **Eliminate configuration errors.** The most common root cause of cloud intrusions continues to be human errors and omissions introduced during common administrative activities. It's important to set up new infrastructure with default patterns that make secure operations easy to adopt. One way to do this is to use a cloud account factory to create new sub-accounts and subscriptions easily. This strategy ensures that new accounts are set up in a predictable manner, eliminating common sources of human error. Also, make sure to set up roles and network security groups that keep developers and operators from needing to build their own security profiles and accidentally do it poorly.

- **Leverage a cloud security posture management (CSPM) solution.** Ensure your cloud account factory includes enabling detailed logging and a CSPM — like CrowdStrike's Falcon Horizon™ — with alerting to responsible parties including cloud operations and SOC teams. Actively seek out unmanaged cloud subscriptions, and when found, don't assume it's managed by someone else. Instead, ensure that responsible parties are identified and motivated to either decommission any shadow IT cloud environments or bring them under full management along with your CSPM. Then use your CSPM on all infrastructure up until the day the account or subscription is fully decommissioned to ensure that operations teams have continuous visibility.

# THEME 4: WATCH FOR WEAKNESSES WITH PUBLIC-FACING APPLICATIONS AND SERVICES

In order for state-sponsored or criminally motivated adversaries to launch an attack, they must gain initial access to an environment. In 2020, CrowdStrike Services observed adversaries exploiting public-facing applications in 30% of investigated cases in order to gain initial access. The Services team witnessed adversaries firsthand as they capitalized on new vulnerabilities, often within 24 to 48 hours after security researchers publicly released proof-of-concept (POC) exploits.

While attackers have always targeted internet-facing infrastructure, the volume of incidents that began this way in 2020 represents a shift in the threat landscape. Several factors likely fueled this shift, but three deserve particular attention.

- The large number of published vulnerabilities: At the time of this writing, 2020 is on track to see approximately 19,000 newly published vulnerabilities, according to the National Vulnerability Database — representing the most vulnerabilities ever published in a single year, up nearly 9% from 2019.
- The critical nature and severity of the vulnerabilities identified in public-facing applications in 2020 were a factor, such as those outlined in Table 3 below.
- There was an acceleration and shift toward businesses offering more external services as they pivoted to remote work models.

**5 COMMON WEAKNESSES WERE SEEN IN 27% OF CROWDSTRIKE'S 2020 INCIDENT RESPONSE ENGAGEMENTS**

It's important to note that application vulnerabilities are not the only way attackers gain initial access via publicly facing applications. In fact, attackers gained initial access via remote login services exposed to the internet and with single-factor authentication in 14% of the incidents investigated. Adversaries often achieved this access via brute force, password spraying, credential-stuffing attacks or previously compromised credentials likely purchased on dark web forums.

The most common exploits across all of the investigated incidents targeted remote code execution vulnerabilities in Citrix ADC/NetScaler appliances and Microsoft SharePoint, as well as arbitrary read/write vulnerabilities in Pulse Secure VPN and Telerik UI for ASP.NET. Other less common public-facing applications exploited include Microsoft Exchange, Zoho ManageEngine and ConnectWise. The top five most common public-facing application vulnerabilities or remote external services that CrowdStrike observed being exploited for initial access represent 27% of all incident response engagements that CrowdStrike conducted in 2020.

| Rank | Weakness | Targeted Industries |
|---|---|---|
| 1 | Exposed login service (e.g., RDP) with single-factor authentication | Agriculture, Defense, Financial, Government, Healthcare, Information Technology, Manufacturing, Professional Services, Retail |
| 2 | Citrix ADC/Gateway (NetScaler) CVE-2019-19781 | Agriculture, Defense, Energy, Entertainment, Financial, Government, Healthcare, Information Technology, Professional Services, Retail |
| 3 | Pulse Secure VPN CVE-2019-11510 | Defense, Education, Hospitality, Information Technology, Manufacturing, Professional Services, Telecommunications |
| 4 | Telerik UI for ASP.NET CVE-2019-18935 | Education, Healthcare, Information Technology |
| 5 | Microsoft SharePoint CVE-2019-0604 | Education, Government, Retail |

**Table 3. Most common public-facing application vulnerabilities or remote external services exploited in 2020**

CrowdStrike observed that when the adversary gained initial access by exploiting a public-facing application or using valid accounts on remote external services, the attack resulted in ransomware 36% of the time. Moreover, 16% of the time, these same initial access techniques led to a breach of sensitive data such as intellectual property, personally identifiable information (PII), personal health information (PHI) or payment card information (PCI). Perimeter-facing vulnerabilities along with applications that are not protected by multifactor authentication clearly bring significant financial impacts to businesses — system and network downtime were also routinely observed.

## WHAT CAN BE DONE TO DOUBLE DOWN ON DEFENSES FOR PUBLIC-FACING APPLICATIONS?

In order to protect internet-facing applications, CrowdStrike recommends implementing the following best practices to mitigate adversaries obtaining initial access via public-facing applications or external remote services.

- **Inventory your public-facing applications, services and systems.** Organizations should have a complete inventory and understanding of their externally facing applications and remote access services, including the software and versions running on them. They should incorporate this inventory into their asset management and vulnerability management processes. It's impossible to defend systems you don't know are there.

- **Patch vulnerable web applications.** Applications and operating systems should be kept up-to-date by installing all vendor-released patches. In situations where proof-of-concept exploits have been publicly released but vendor patches are not yet available, vendor mitigation steps should be implemented.

- **Perform web application penetration tests.** Organizations should have a third party conduct web application penetration tests to identify and fix vulnerabilities or misconfigurations that an attacker could exploit to gain access.

- **Enforce multifactor authentication (MFA) on public-facing applications and services, such as RDP and VPNs.** Single-factor, password-based authentication is vulnerable to brute-force, password-spraying and credential-stuffing attacks. MFA increases attacker complexity and increases the likelihood of detection before a successful attack.

- **Restrict systems with remote login services such as RDP and Secure Shell (SSH) exposed to the internet.** Allowing remote connections from all external IP addresses greatly increases the chance of system compromise. Systems that require external-facing remote login for business purposes should be restricted based on source IP address. Systems that do not require external-facing remote login for business purposes should have the service disabled.

# THEME 5: STATE-SPONSORED ADVERSARIES LEAVE SMALLER FOOTPRINTS

The CrowdStrike Services team continued to respond to state-sponsored adversary intrusions at organizations throughout 2020. While many organizations think they may not be a target of state-sponsored adversaries, some should think again. In 2020, CrowdStrike saw state-sponsored adversaries target organizations ranging from 500 to 50,000+ endpoints across 10 industries. This section highlights key trends observed to be employed by nation-state adversaries and also provides considerations for preventing and responding to nation-state adversaries.

**CrowdStrike Services saw state-sponsored adversaries target organizations ranging from 500 to 50,000+ endpoints across 10 industries.**

## STATE-SPONSORED ADVERSARIES EMPLOYED A SIGNIFICANT NUMBER OF N-DAY VULNERABILITY EXPLOITS

In 2020, the CrowdStrike Services team observed state-sponsored actors achieving access to target networks through supply chain attacks, physical access, watering hole attacks, spear-phishing and via vulnerable public-facing applications. CrowdStrike Services observed heavy use of known vulnerabilities ("N-days") to compromise externally facing applications. Notably, CrowdStrike Services identified that nation-state actors leveraged the use of Pulse Secure VPN, Citrix ADC and Zoho Desktop Central vulnerabilities in 2020. As mentioned, the exploitation of these vulnerabilities often came 24 to 48 hours after the release of POC code through open-source repositories, demonstrating significant capabilities for rapid development.

## STATE-SPONSORED ADVERSARIES PUT A BULLSEYE ON CLOUD ENVIRONMENTS

In 2020, CrowdStrike Services increasingly responded to incidents in which nation-state adversaries also targeted and compromised cloud infrastructure. In many of these cases, the actors were able to gain access to the environment either through credential theft in traditional on-premises systems or through improperly configured services. In addition, the Services team responded to incidents where top commercial cloud providers were used as initial staging points to further blend in with legitimate traffic.

In the previous edition of this report, the Services team noted that exposed cloud application programming interface (API) keys with minimal restrictions and often a lack of additional auditing represented the bulk of intrusion cases involving cloud infrastructure as a service (IaaS). In 2020, the Services team identified that in a subset of incidents, the adversaries compromised the control plane of the tenant and performed actions-on-objectives tasks directly through the tenant console. The team also observed them taking advantage of single-factor authentication access to IaaS consoles and leveraging Microsoft Azure to push Cobalt Strike beacons via PowerShell. During these incidents, preconfigured logging and enhanced auditing of individual service components played a critical role in providing the Services team with the ability to track and contain adversary actions.

## STATE-SPONSORED ADVERSARIES LEVERAGED INCREASINGLY SOPHISTICATED ATTACK TECHNIQUES WHILE LEAVING EXTREMELY SMALL FOOTPRINTS

State-sponsored adversaries continue to blend in by using "living off the land" (LOTL) techniques both within traditional enterprise environments and in the cloud, as well as using custom implants that leave minimal artifacts for traditional forensic analysis. In 2020, delivery of more sophisticated implants by nation-state actors — often leveraging memory and modular based implants — typically occurred through watering-hole attacks or supply chain compromise. In a subset of these cases, the actors leveraged LOTL techniques and commodity toolsets (e.g., certutil, msbuild, bits, Cobalt Strike, generic webshells, etc.), while others leveraged custom and some previously unknown implants to maintain persistence. Commonly, the identified implants leveraged a multi-stage framework in which a minimal footprint was maintained on the disk through a persistent loader. The implants were activated through preconfigured command-and-control channels, and subsequent payloads were retrieved in a modular fashion that were loaded only in memory for execution to carry out their specific task.

These sophisticated techniques are one of the reasons why state-sponsored adversaries persist in networks much longer than average. Although the overall dwell time for incidents investigated by CrowdStrike Services decreased in 2020 compared to 2019 (from 85 days to 79 days), state-sponsored adversary dwell time significantly exceeded the overall average dwell time by a factor of nearly 10 — just under two years. That means while the average attacker spent two to three months in a network before discovery, the average state-sponsored threat actor/group spent nearly two years in a network prior to discovery.

When state-sponsored threats were identified, the availability of volatile evidence such as memory dumps and full network packet captures played a crucial role in enabling the CrowdStrike team to perform forensic analysis of systems affected by the identified implants. Organizations with the visibility and infrastructure in place to capture necessary telemetry during active operation periods played a critical role in enabling the Services team to successfully carry out the investigation and assist the organization in answering key questions related to the incident.

## PREVENTING AND RESPONDING TO STATE-SPONSORED INTRUSIONS

CrowdStrike recommends the following practices when defending against nation-state threat actors:

- **Establish strong IT hygiene with an asset inventory and consistent vulnerability management.** Inventorying and patching external infrastructure on a regular basis increases the difficulty of initial access for nation-state actors. Creating contingency plans for applications that cannot be immediately patched — such as increased monitoring, access restrictions and backup applications — can help organizations reduce their risk in situations where applications do not have patches available.

- **Protect your cloud infrastructure and workloads.** Critical applications and data are being moved to the cloud, and while organizations are getting better at protecting their cloud environments, they continue to strategically assess their security posture in traditional ways. Traditional tabletop assessments and red team engagements are no longer enough. Organizations must adopt a cloud-focused assessment strategy to keep up with the changing threat landscape. Cloud security assessment and cloud-focused tabletop assessments can identify gaps in cloud protections and logging. Additionally, the CrowdStrike Falcon Horizon CSPM module can help organizations manage the security of their cloud workloads.

- **Establish a plan for a coordinated remediation event (CRE).** With nation-state actors maintaining a longer dwell time than their eCrime counterparts, organizations must learn to manage longer-term incidents. Executing containment actions too quickly can result in the threat actor changing its tactics, techniques and procedures (TTPs). And, containment actions can sometimes be impactful to a network, causing downtime or signaling your intent prior to the action being taken. A CRE is a detailed procedure for removing a threat actor from the network in one fell swoop. Implementing a CRE plan prior to an incident can help organizations reduce the likelihood of re-compromise when defending against nation-state threat actors.

- **Develop an ongoing relationship with law enforcement agencies.** It is good to have a relationship with law enforcement prior to a breach. While some organizations may be wary of involving multiple external parties in an investigation, having a relationship with law enforcement can be a valuable tool during an investigation. A few things that law enforcement relationships may offer:

  - Intelligence on threat actor groups
  - Guidance on ransom payments
  - Tracing of unauthorized payments

# THEME 6: AFTER THE BREACH: MAKING IMPROVEMENTS TO STOP THE NEXT BREACH

Over the years, there have been multiple permutations of the cybersecurity incident response lifecycle, but no matter how that model evolves, two things remain constant: It starts with preparation and ends with applying lessons learned. These parts of the process don't typically garner much attention — after all, the exciting stuff is what happens in between. In 2020, however, CrowdStrike Services saw a growing number of organizations focusing intently on the post-incident period. The Services team also saw them expand the scope of this process, focusing less narrowly on the specifics of the incident and broadening the process to drive more holistic change.

**"Never let a good crisis go to waste."**

## OPPORTUNITY FROM CRISIS

A significant cyber breach can be devastating to an organization, and experiencing a second breach on the heels of the first is far more catastrophic. This is why business leaders always ask, "What are we doing to keep this from happening again?" It's a pivotal question, especially for a security team whose performance is likely under a microscope. Mishandle it and you may never regain your leaders' confidence. Answer it well, and you will not only win back their trust but also lay the foundation for a stronger security program moving forward.

Providing a good answer requires expansive thinking, and perhaps an embrace of the aphorism, "Never let a good crisis go to waste." In the wake of a major incident, cybersecurity awareness is high, risk tolerance is low, and past assumptions about operational and budgetary constraints are subject to change. While it is important to address the root causes of the incident that occurred, it is a mistake to stop there. The next incident is unlikely to exactly mirror the last one, and any improvement plan should not only address the specific causes of the last incident but also weed out the seeds of the next one.

## POST-INCIDENT PLANNING

Any holistic response process is going to be a marathon, not a sprint — and the course of that marathon will be different for each organization. In most cases, the following steps are certainly worth considering:

- **Expedite recovery.** Before any plans for improvement can begin, it is essential to secure and restore the environment quickly. Third-party assistance — such as CrowdStrike's Endpoint Recovery Services — can streamline the containment, remediation and recovery phases of an incident using more streamlined and surgical workflows versus the traditional approach of rebuilding IT environments. This approach allows the business to get back to work more rapidly and less expensively, and allows the security team to train its focus on making improvements.

- **Test new controls.** Many remediation plans involve implementing new controls, such as implementing multifactor authentication, updating firewall rules, changing group policy configurations or patching a key vulnerability. Depending on the nature of the new controls, it may be necessary to perform technical tests to verify they are working as intended.

- **Conduct a lessons-learned process.** This is the traditional post-incident review, which focuses on identifying and understanding the root causes of the incident as well as understanding what went well and what did not during the response. Although it is an indispensable part of the response lifecycle, it is by definition focused on the last battle and may or may not provide useful insights for fighting the next one.

- **Secure executive buy-in.** In the wake of a major incident, the security team is going to be subject to additional scrutiny. Clear, open communication with leadership is critical to restoring their trust in a security program. Beyond explaining "What happened?" to leadership, security leaders will be expected to explain "How will we prevent future incidents?" as well as "How do we know that we're taking the right approach?" Executives should be briefed on the way forward and updated at key points along that journey. By outlining a plan that includes the steps below, the security team can give executives confidence that security will take a broad, open-minded approach to making improvements. It may also help to bring in third-party experts to attest to this approach and assure executives that the path forward you have charted is the right one.

- **Perform a technical assessment.** The goal of a technical assessment should be to identify and understand factors about your organization's network that could make future incidents more or less likely. It is not a penetration test — presumably a threat actor just succeeded at that — but it may take different forms depending on the nature of the incident and investigation that occurred. For instance, if the investigation was confined to a specific network segment or specific business unit, an enterprise-wide compromise assessment can give confidence that the attacker did not move into parts of the environment that were beyond the scope of the initial investigation. If the prior investigation was thorough, consider an IT hygiene assessment to identify weak passwords, active directory configurations or missed patches that could open the door to the next attacker.

- **Perform a programmatic assessment.** The post-incident period is the perfect time to evaluate a security program from top to bottom — and consider the people, processes and technologies. The just-completed incident exposed some weaknesses but probably not all of them — and possibly not the most significant ones. A full assessment will help provide an objective understanding of the security program's current maturity, facilitate conversations about where it ought to be and prioritize which improvements to make first. It provides the prerequisite understanding before you can effectively answer "What are we doing to keep this from happening again?"

- **Develop a roadmap.** The steps above are all likely to identify things your organization can do to be more secure. Your roadmap should reflect which

of those things you are going to prioritize and your timelines for completing them. It's important to take a risk-informed approach, prioritizing quick wins to show progress while also investing in the improvements that are going to most significantly reduce your risk — even if they're longer-term efforts.

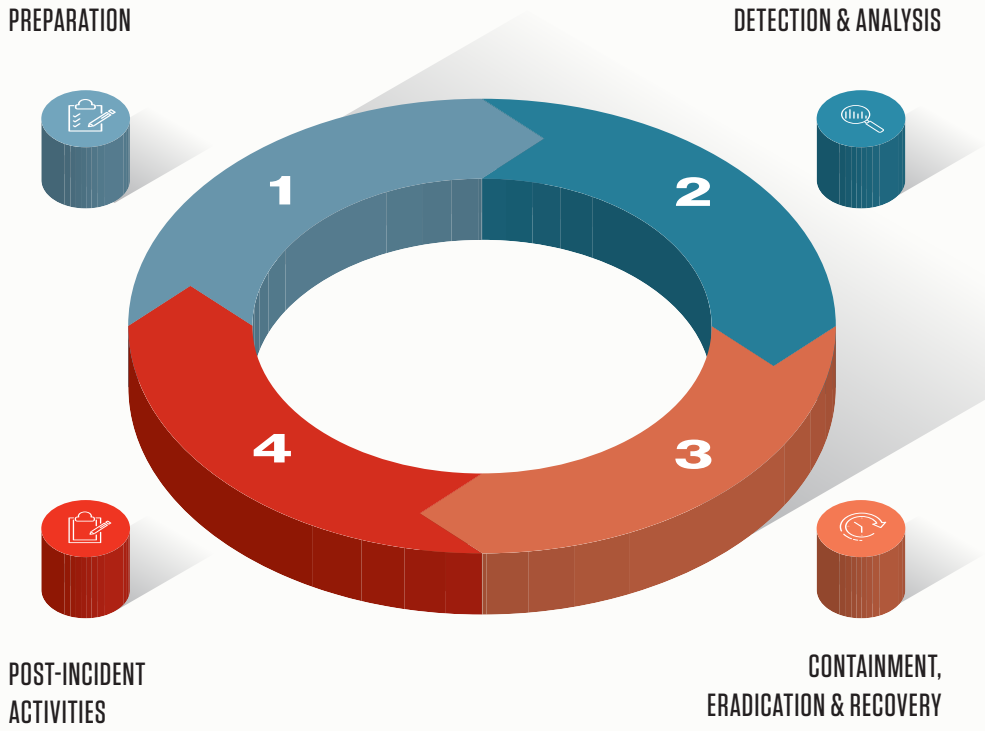
- **Execute with accountability.** Depending on the nature of the changes an organization needs to make, executing on its roadmap may take years. These long, complex improvement plans require careful management and checkpoints along the way to ensure everything remains on course. Strong project management can help track milestones and ensure plans stay on schedule. It may also be necessary to seek outside guidance, both to ensure that the improvements you're making are addressing the risks they're meant to and also to consider whether changes in the threat landscape merit a realignment of priorities.

- **Test your progress.** Once specific projects are completed, run tests to ensure they are working. Use penetration tests to validate technical controls, and run exercises to test new processes.

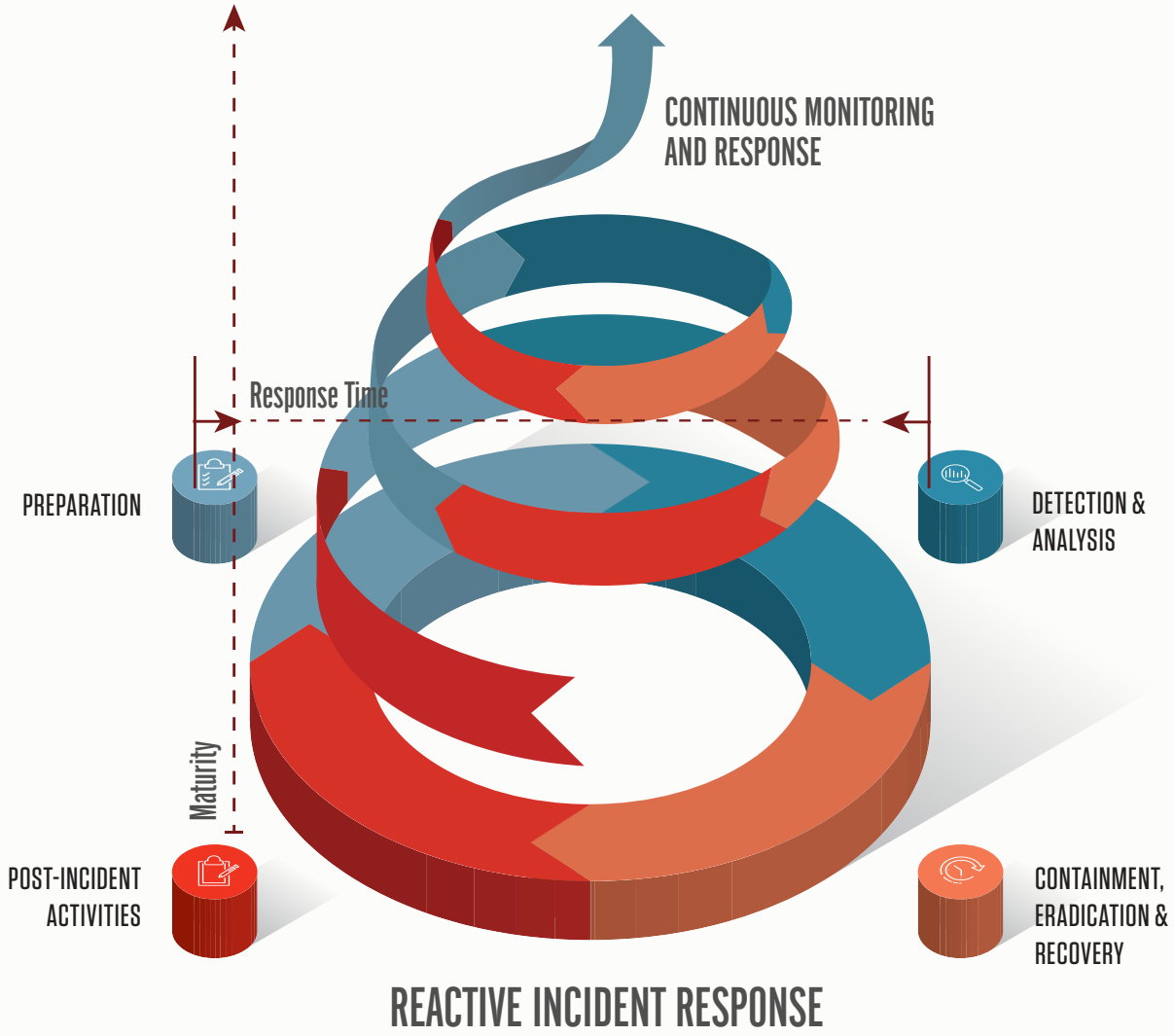
## PREPARING FOR THE NEXT BATTLE

In some respects, the visual of the incident response lifecycle does security teams a disservice. The notion of a "cycle" implies a circular path, where you return to where you were before.

## THE INCIDENT RESPONSE LIFECYCLE



Taking a more expansive approach to the post-incident review process gives security teams another path. Rather than circling back to the beginning, the aim is to arrive back at the pre-incident phase better equipped to stop incidents from occurring and respond effectively to those that do. The goal is not to eliminate security incidents — it would be a grave mistake to promise such a thing to leaders who ask about stopping the next one. The goal is to turn that cycle into an upward spiral, where future incidents are less frequent and less severe. At the apex of that spiral is the **continuous monitoring and response process**, where new threats are identified and remediated in near real time.



# ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services equips organizations with the protection and expertise they need to defend against and respond to security incidents. Leveraging the cloud-delivered CrowdStrike Falcon® platform — including next-generation endpoint protection, cyber threat intelligence gathering and reporting operations, and a 24/7 proactive threat hunting team — the CrowdStrike Services team helps customers identify, track and block attackers in real time.


- **CrowdStrike Incident Response Services** stop active breaches with full threat visibility and containment, digital forensic investigation and root cause analysis, rapid endpoint recovery and remediation so you can get back to business faster.

- **CrowdStrike Endpoint Recovery Services** helps organizations to rapidly contain any malware or ransomware outbreaks even if the attack is impacting hundreds or even thousands of systems, and then to recover the endpoints and systems with speed and precision, avoiding potential business interruption.

- **CrowdStrike Falcon Complete** provides a comprehensive managed endpoint protection solution, to help organizations achieve continuous monitoring and response. It delivers unparalleled security by augmenting the CrowdStrike Falcon® platform with the expertise and 24/7 engagement of the Falcon Complete team. The team manages and actively monitors the Falcon platform, remotely remediating incidents continuously as they occur. Falcon Complete enables organizations with effective and mature endpoint security without the difficulty, burden and costs, and backs it with a Breach Prevention Warranty of up to $1M.

Further, CrowdStrike delivers a comprehensive portfolio of services to help organizations answer three key security questions:

**Am I Breached?**

**Am I Mature?**

**Am I Ready?**

CrowdStrike **Strategic Advisory** and **Technical Services** proactively deliver **assessments** that help enhance your cybersecurity posture and improve your IT hygiene, **exercises** that help improve your team's readiness to defend against today's sophisticated attacks, and **programs** that help you implement best practices in cybersecurity and threat intelligence. See the table below for a full list of CrowdStrike Services.

| AM I BREACHED? | AM I MATURE? | AM I READY? |
|---|---|---|
| Incident Response<br>Compromise Assessment<br>Endpoint Recovery<br>Network Security Monitoring | Cybersecurity Maturity Assessment<br>Cloud Security Assessment<br>Active Directory Security Assessment<br>SOC Assessment<br>IT Hygiene Assessment<br>Security Program in Depth<br>Cybersecurity Enhancement Program<br>Threat Intel Program Development | Tabletop Exercise<br>Live Fire Exercise<br>Adversary Emulation Exercise<br>Red Team / Blue Team Exercise<br>Penetration Testing |

Services Retainer | Falcon Operational Support | Falcon Training (CSU)

CrowdStrike Incident Response and Proactive Cybersecurity services are available under a **Services Retainer**, giving you on-demand access to the full portfolio of CrowdStrike services and expertise as and when you need them. To learn more, visit **www.crowdstrike.com/services/** or contact **services@crowdstrike.com**.

# ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 4 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: **We stop breaches.**