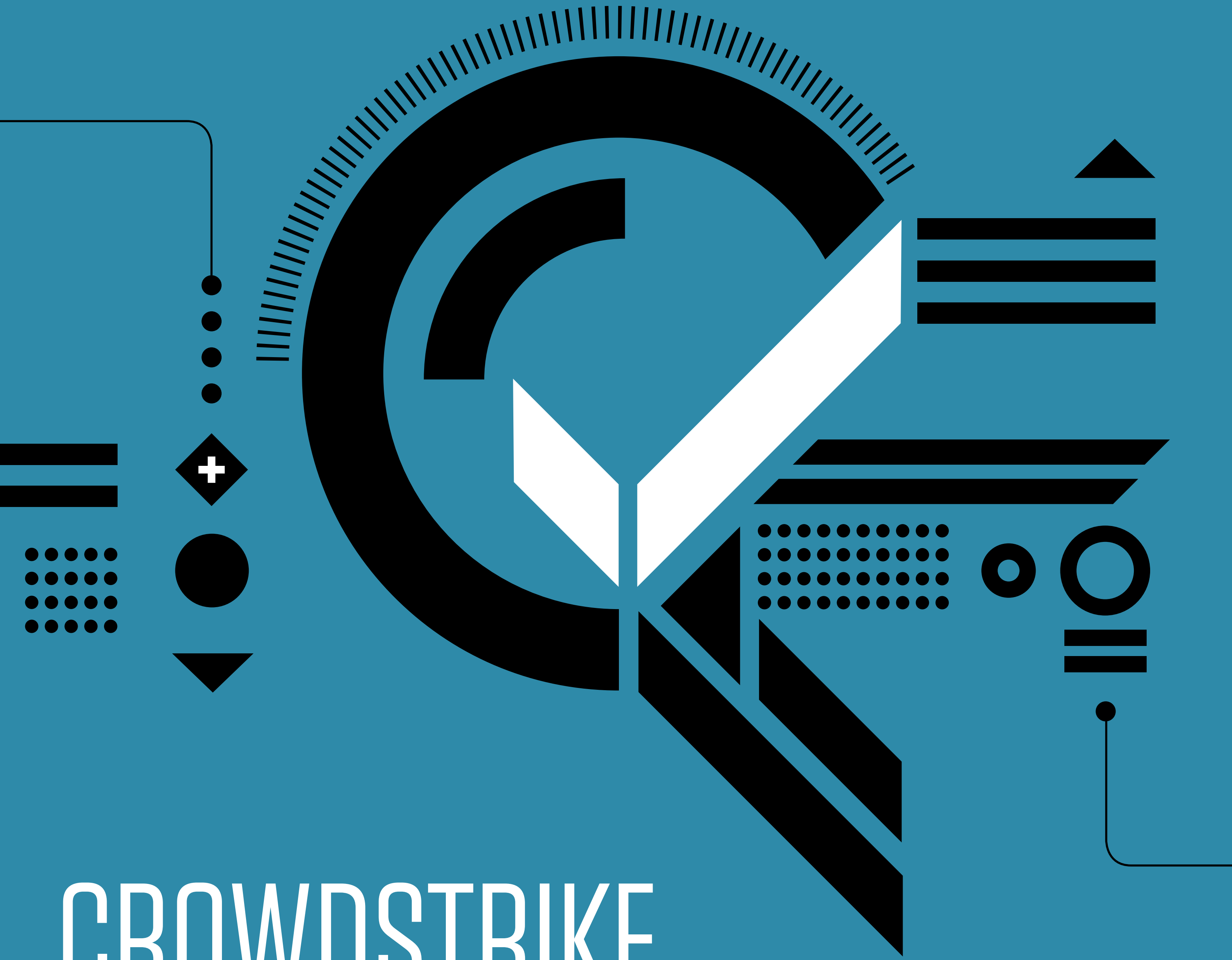
CROWDSTRIKE



CROWDSTRIKE SERVICES CYBER FRONT LINES REPORT

OBSERVATIONS FROM THE FRONT LINES OF INCIDENT RESPONSE AND PROACTIVE SERVICES IN 2019 AND INSIGHTS THAT MATTER FOR 2020

TABLE OF CONTENTS

FOREWORD

The year 2019 ushered in a host of new adversaries, new attack methods and new challenges for those of us in the cybersecurity industry. The CrowdStrike® Services team faced these trials head-on, across geographical regions and within public companies, private industries and governmental entities spanning a variety of digital mediums. The work we're doing — our forte — is incident response and stopping sophisticated breaches, each unique in size, scope and motivation. We conduct hundreds of investigations each year across the globe and have the expertise to respond quickly and begin mitigation immediately — what we refer to as "speed-to-remediation."

There were also a number of significant changes at CrowdStrike in 2019. We became a publicly traded company, significantly expanded our global footprint and increased our corporate hiring count, with Services consultants now located in seven countries and delivering support in over 40 more. Yet, we haven't lost focus on the most important things. The adversaries are as committed as ever, with new attack vectors on the rise, so we must be agile and proactive. They still seek the path of least resistance — as we harden one area, they focus on accessing and exploiting another. Finally, we still maintain that the most critical aspect of a strong cybersecurity posture is early detection, combined with swift response and mitigation.

With that in mind, this year we've decided to provide a new perspective in our Services Report. You'll find that in this report we're focusing on the trends and themes observed in the global incidents we responded to and remediated throughout 2019, rather than the anonymized case-specific victim examples of years past. I'm confident this approach will provide you with greater insight into the front-line view of the digital battle we're fighting, as well as offer pragmatic steps to ensure your organization doesn't become the next statistic in our 2020 report. Our analysis and lessons learned will add value to your proactive security measures and situational awareness for the new year. I encourage you to review the contents and implement procedures as appropriate to help make your environment more resilient and to better protect your organization.

One team, one fight.

Shawn Henry
CrowdStrike, CSO and President of Services

EXECUTIVE SUMMARY

This year’s report takes a different approach from previous years, shifting the emphasis from analyzing specific cases to a broader analysis encompassing trends and themes the CrowdStrike Services team encountered while conducting incident response (IR) investigations for a wide range of organizations throughout 2019. The real-world observations and analysis presented in this report should prove both compelling and practical, including recommendations that you can implement in your organization to improve your cybersecurity readiness. The incidents investigated during 2019 span many countries, regions and industry sectors. However, one thing has remained constant: Cyber adversaries continue to be both relentless and innovative in their efforts to find gaps in your organization's IT infrastructure and exploit them for their own gain.

The findings in this report are derived from data points and insights resulting from IR and proactive services activities over the past 12 months. The following are some of the key findings organizations should heed:

- **Business disruption was the main attack objective.** This was true for 36% of the incidents CrowdStrike Services investigated. Most often this was caused by ransomware, destructive malware or denial of service attacks.

- **The most common MITRE ATT&CK™ techniques focused on account compromise, often via “living off the land” (LOTL).** Credential dumping was the most frequent technique observed, with account discovery in third place. PowerShell, scripting and command line interface rounded out the top five.

- **There was continued improvement in attack self-identification.** The report shows that 79% of organizations the IR team engaged with were able to detect and respond to a breach without external notification — up from 75% in 2018.

- **Dwell time increased slightly.** The average dwell time increased from 85 to 95 days due in part to advanced adversaries employing stronger countermeasures, allowing them to remain hidden longer — in some cases, for years — prior to discovery.

- **Malware and malware-free intrusions were observed in almost equal numbers.** In 51% of the intrusions investigated by CrowdStrike Services, malware-free techniques were used, while 49% were malware-based. In 22% of the cases investigated, malware-based and malware-free techniques were used in concert.

In addition to these key findings, the Services team identified a number of key themes from 2019. Organizations should be mindful of the following:

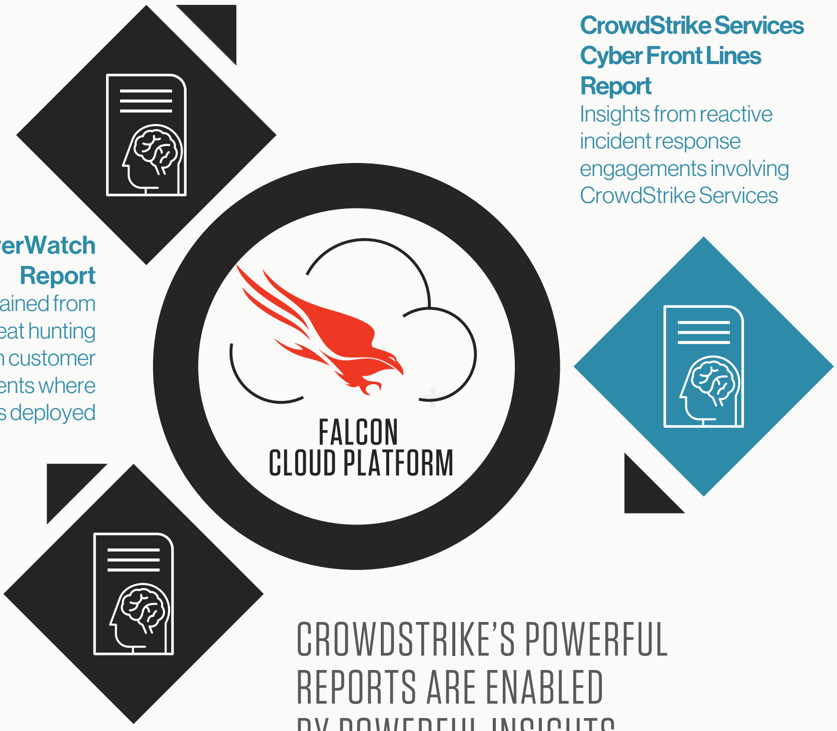
- **Attackers are more deliberate and targeted in their efforts to automate Active Directory reconnaissance.** The use of modern tools such as BloodHound has simplified and automated this process, making attacks easier for bad actors but also providing defenders with a tool they can leverage to identify and remediate weaknesses.
- **Third-party compromises serve as a force multiplier for attacks.** Threat actors are increasingly targeting third-party service providers to compromise their customers and scale attacks.
- **Attackers are targeting cloud infrastructure as a service (IaaS).** Threat activity around API keys for public, cloud-based infrastructure has become more targeted as attackers increase their ability to rapidly and systematically harvest information assets.
- **Macs are now clearly in the crosshairs of the cyber fight.** Threat actors are increasingly targeting macOS environments, using LOTL with native applications and capitalizing on security tools that are less widely used than those available for Windows systems in the same organization.
- **Patching remains a problem.** Basic hygiene still matters, and even though organizations have gotten better at patching, the factors that make patching a challenge have become more complex.
- **How prevention is configured impacts its effectiveness.** The report finds that many organizations fail to leverage the capabilities of the tools they already have. This failure to enable critical settings not only leaves organizations vulnerable, it also gives them a false sense of security.

Threat actors are increasingly targeting third-party service providers to compromise their customers and scale attacks.

As noted in the key findings, there have been improvements in the ability of organizations to self-detect attacks, but the protracted time-to-detect is still troubling. CrowdStrike advocates that organizations follow the “1-10-60 rule” as a best practice: one minute to detect an intrusion, 10 minutes to investigate and one hour to remediate. The recently released **2019 CrowdStrike Global Security Attitude Survey** found that the vast majority of organizations see adherence to the 1-10-60 rule as a “game changer” in ensuring protection. Yet, most survey respondents acknowledged they are falling short in achieving this metric. This is also evidenced in the experience of the CrowdStrike Services team when conducting IR for organizations: Those that meet the 1-10-60 rule can dramatically improve their chances of staying ahead of the adversary and stopping a potential breach from occurring. However, adhering to the rule is a challenging benchmark that requires speed and experience.

In addition, following the recommendations made in this report, while a highly desirable goal, can lead to questions about how to best implement and operationalize the advice provided. CrowdStrike Services is here to help, providing highly skilled cybersecurity professionals who work alongside clients, ensuring that the adversaries are defeated and any damage is quickly remediated.

A UNIQUE PERSPECTIVE



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

Falcon OverWatch Report
Insights gained from proactive threat hunting conducted in customer environments where Falcon is deployed

CrowdStrike Global Threat Report
Global cyber threat intelligence and insights from the Falcon platform and OverWatch

CROWDSTRIKE'S POWERFUL REPORTS ARE ENABLED BY POWERFUL INSIGHTS

Figure 1. CrowdStrike technical reports published annually

CrowdStrike provides a unique perspective when assessing the state of cyber threats. These distinct vantage points are represented in three annual publications, each highlighting the contributions and assessments of individual CrowdStrike teams:

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

The 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 midyear Falcon OverWatch™ Report presents observations from the Falcon OverWatch team as they hunt adversaries. Finally, the real-world experience gained from the Services team as they respond to incidents and breaches is documented in this CrowdStrike Services Cyber Front Lines Report. This comprehensive and holistic view of the threat landscape allows CrowdStrike to provide specific guidance on the actions organizations can take to improve their security postures.

KEY FINDINGS

The data points provided in this section are derived from information CrowdStrike Services has collected in its IR and proactive services work over the past 12 months. The anecdotal nature of this report offers a different perspective from the findings outlined in CrowdStrike reports produced by the Falcon OverWatch and CrowdStrike Intelligence teams. This may include data and insights derived from numerous sources, including the more than 2.5 trillion security events the CrowdStrike Falcon® platform collects each week.

ATTACK IDENTIFICATION

CrowdStrike Services continues to see improvements in organizations' abilities to detect and respond to breaches without external notifications. Comparing this year's findings to those of previous years reveals an improvement in organizations' abilities to self-detect breaches.

Percentage of Organizations That Self-Detected an Intrusion

2017	2018	2019
68%	75%	79%

In 2019, 79% of organizations that engaged CrowdStrike for IR were able to internally detect an intrusion — representing an increase of 4 percentage points over last year. More organizations are detecting breaches, in part as a result of improvements in C-level executives' understanding of cyber risk. One of the key components of a successful change is sponsorship from executive leaders. Over the past year, the Services team engaged with more CEOs and boards of directors than ever before. The visibility into cyber intrusions provided to C-levels and boards and the subsequent investment in security should continue to help protect organizations and their customers.

As a direct result of executive support, organizations are making a greater effort to mature their security operations and postures, particularly with respect to detection. However, organizations need to invest across the entire security stack — including endpoint detection and response tools (EDR), threat intelligence, proactive managed hunting and managed remediation services — if they are to continue improving their ability to self-detect.

DWELL TIME

Dwell time represents the period from when a compromise first occurs to when it is detected. Comparing this year's findings to 2018 indicates that dwell time increased an average of 10 days.

Comparison of Dwell Times

2017	2018	2019
86 days	85 days	95 days

Dwell Time	Percentage of Cases
<= 1 day	16%
2 days to 1 week	13%
1 week to 1 month	23%
1 to 3 months	26%
3 to 6 months	13%
6 months to 1 year	3%
> 1 year	6%

Table 1. Breakdown of dwell times by duration

While the Services team observed a slight decrease in dwell time from 2017 to 2018, 2019 data showed an increase to an average of 95 days that adversaries were able to hide their activities from defenders. The team also observed a significant number of breaches by targeted adversaries that gained initial access more than a year before discovery, and in a number of cases, more than three years. This demonstrates the need for better visibility and for implementing proactive threat hunting to uncover attacks early. It also reveals that state-sponsored threat actors are applying countermeasures that allow them to remain undetected for a protracted length of time — particularly in environments protected by legacy security technologies.

While average dwell time increased overall in 2019, if you exclude the breaches with greater than one year dwell times, the average came in at approximately 60 days. This 60-day period is how long eCrime actors — many leveraging ransomware — typically spend within an environment before executing their attacks. During dwell time, eCrime actors conduct reconnaissance to understand how the target environment works, so they can increase their attack effectiveness. For example, adversaries may probe into how backups work prior to executing ransomware. This allows them to encrypt both the target system and the backups of that system, increasing their leverage over the victim and the likelihood of getting paid, because the company will not be able to simply restore via a backup.

The ability to quickly detect an intrusion is the foundation of rapid response and remediation, which lessens the potential impact of a breach on an organization, its customers and partners. CrowdStrike has been at the forefront of bringing attention to the fact that the security industry needs to dramatically accelerate detection, investigation and remediation. To defeat the adversary, organizations need to be detecting within one minute — in accordance with the 1-10-60 rule. CrowdStrike developed the Falcon platform to reduce the time to detect, investigate and remediate, and thereby reduce dwell time. Please note that the vast majority of engagements covered in this report, which contributed to the dwell time findings, involved organizations that did not have the CrowdStrike Falcon platform installed. There was a small percentage in the process of implementing Falcon and had not fully deployed or configured it, and others that experienced an event outside the boundaries of the Falcon platform.

ATTACK IMPACTS

BUSINESS DISRUPTION

Business disruption dominated the headlines this year. Of the breaches CrowdStrike Services investigated, 36% also experienced a disruption in their organization's business. These disruptions are most often caused by ransomware, destructive malware and denial of service attacks. While the adversary's main goal in a ransomware attack is financial gain, the impact of disruption to a business can often outweigh the loss incurred by paying the ransom. However, this disparity may be shrinking because CrowdStrike has observed eCrime actors substantially increasing their ransom demands over the past year.

DATA THEFT

Data theft was not far behind business disruption and was observed in 25% of the breaches CrowdStrike investigated. This includes the theft of intellectual property (IP), personally identifiable information (PII) and personal health information (PHI). IP theft has been linked to numerous nation-state adversaries that specialize in targeted intrusion attacks, particularly China-based actor groups but also Democratic People's Republic of Korea (DPRK)-affiliated adversaries and a Vietnam-based adversary tracked by CrowdStrike Intelligence as OCEAN BUFFALO. PII and PHI data theft can enable both espionage and criminally motivated operations. Typically, this type of data may be used by a cyber espionage actor to build a dossier on a high-profile target, or a cybercriminal may sell or ransom the information.

MONETARY LOSS

This year we looked at the monetary loss category a bit differently. While ransomware is often motivated by financial gain, as previously discussed, the business disruption effects typically have an even greater negative impact on an organization. As a result, this year we elected to reclassify ransomware under the business disruption category. While the impact of monetary loss was higher in last year's Services report, it accounted for just 10% of the cases in 2019 with ransomware reclassified under business disruption. Attacks included in this year's monetary loss category include crimeware, formjacking, cryptojacking and more.

INITIAL ATTACK VECTORS

In order to more clearly define the vectors by which attackers get into a network, CrowdStrike aligned its initial access attack vectors to the MITRE ATT&CK framework. This is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations of cyberattack and is used as a foundation for the development of specific threat models and methodologies in the private sector, in government and in the cybersecurity product and service community.

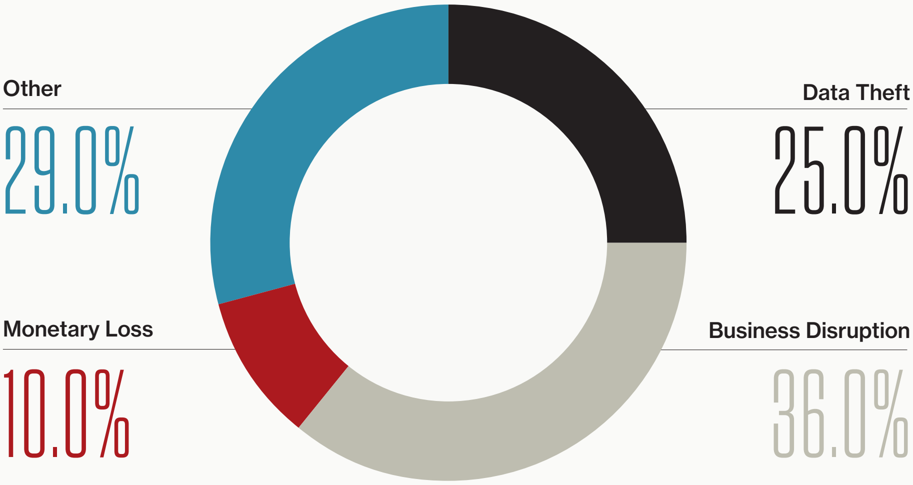


Figure 2. Attack impact by type of damage incurred

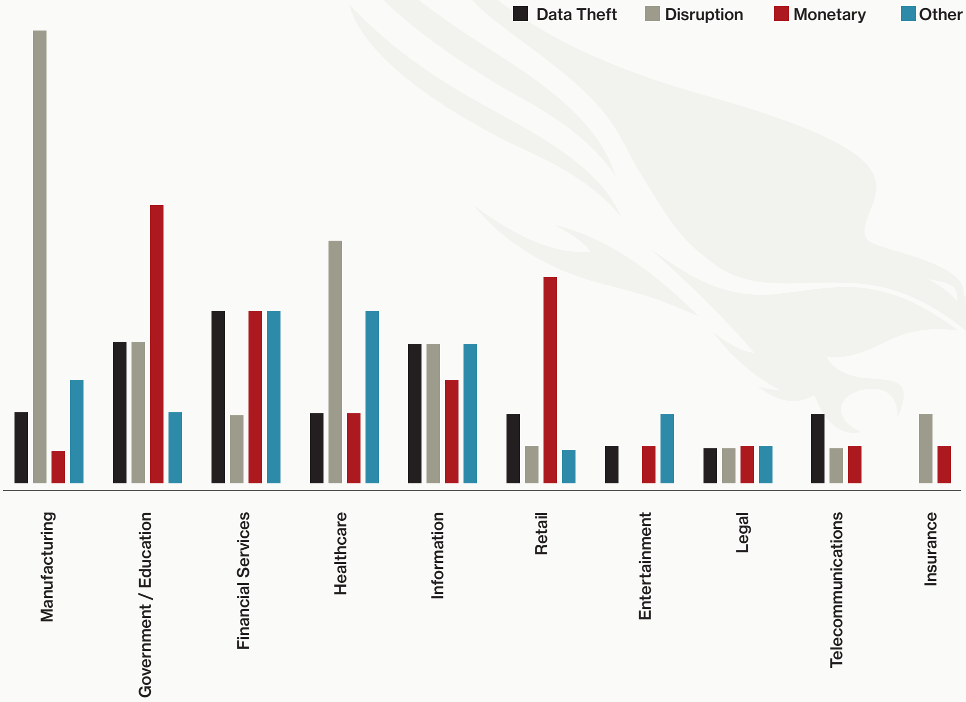


Figure 3. Attack impact by type of damage for top 10 industries

SPEAR-PHISHING

Spear-phishing was the dominant vector used to gain initial access to a network in 35% of the cases CrowdStrike investigated in 2019 — an increase of 2 percentage points over last year. Within the three spear-phishing categories in the MITRE ATT&CK framework, this breaks down as follows: 19% of cases used attachments in a spear-phishing email, 15% used spear-phishing with a malicious link and 1% employed spear-phishing via a service.

WEB ATTACKS

Web attacks were slightly less prominent this year, dropping from 20% of cases in 2018 to 16% in 2019. This includes 12% of the breaches involved in an exploit of a public-facing application and 4% as a result of a drive-by compromise. Websites have long been the front door into an organization, and a lack of web-based security controls and insufficient vulnerability management continue to make this a common initial attack vector. CrowdStrike most commonly observed MITRE Common Weakness Enumerations such as cross-site scripting, SQL injection attacks and OS command injection, often resulting in malware downloads or webshells to establish a foothold.

COMPROMISED CREDENTIALS

Initial attacks involving compromised credentials declined from 20% in 2018 to 16% in 2019. While compromised credentials decreased as the initial attack vector, it was the most common attack technique observed in the entire lifecycle of an attack, often leveraged as a method to move laterally within a network after initial access was gained. A number of factors could influence its decline as an initial attack vector, but the adoption of multifactor authentication (MFA) could be a key contributor. Implementing MFA has been a long, hard-fought battle for many organizations. However, the Services team is seeing more companies realize the value it provides, even in light of the inconvenience it can cause users.

A very popular credential compromise technique observed this year involved threat actors using Remote Desktop Protocol (RDP) to target RDP-enabled computers exposed to the internet. Threat actors performed “credential stuffing,” leveraging publicly exposed servers and using purchased or common username and password combinations. This was a particularly common technique among eCrime actors focused on ransomware distribution.

SUPPLY CHAIN

The software supply chain category is a new addition to CrowdStrike Services reporting for 2019. It encompasses both the supply chain compromise and trusted relationship MITRE ATT&CK initial compromise techniques. In 2019, 6% of the incidents CrowdStrike investigated came as the result of a supply chain compromise. While this is a relatively small number, it is important to recognize that third-party compromises have the potential to be more impactful or far-reaching than attacks originating from other vectors. Nearly every mature organization that CrowdStrike provided proactive services for in 2019 had supply chain risks among their top cybersecurity concerns, due to both the challenges in preventing them and the damage they can inflict. The compromise of remote administrative software, shared connectivity with a managed service provider and third-party script attacks on websites, such as formjacking, were common supply chain attacks observed by CrowdStrike in 2019. Additional analysis and discussion of supply chain attacks appear in the Key Themes section of this report.

OTHER AND UNKNOWN

The “Other” category includes intrusions that result from misconfiguration or commodity malware, or incidents that end up being identified as false positives. The “Unknown” category exists because as organizations self-identify attackers earlier in the attack lifecycle, it often becomes more challenging to understand and classify the true motives of an attacker. In 2019, the unknown category increased from 9% to 14% of the cases encountered. Table 2 shows the percentages of various attack vectors and the techniques used for each.

Category	2018	2019	MITRE ATT&CK Technique
Spear-phishing	33%	35%	■ Attachment: 19% ■ Link: 15% ■ Service: 1%
Web Server Attack	20%	16%	■ Exploit public-facing application: 12% ■ Drive-by compromise: 4%
Compromised Credentials	20%	16%	RDP-exposed, credential stuffing, publicly posted passwords
Supply Chain	Did not collect	6%	■ Trusted relationship: 5% ■ Supply chain: 1%
Other	12%	14%	Misconfiguration, commodity malware, false positive
Unknown	9%	14%	

Table 2. Percentage of initial attack vectors observed

MALWARE AND MALWARE-FREE INTRUSIONS

For years, CrowdStrike has talked about the importance of stopping malware-free attacks. The 2019 report examines the percentage of adversaries that employed malware versus malware-free intrusions or used a combination of these techniques.

MALWARE-FREE INTRUSIONS

In 51% of the incidents CrowdStrike responded to in 2019, adversaries employed malware-free techniques at some point during the intrusion. Malware-free techniques include, but are not limited to, PowerShell, scripting, Mshta and WMI.

The report finds that adversaries continue to rely on malware-free techniques during intrusions. In fact, in 29% of cases in 2019, the adversary used only malware-free techniques. Adversaries that rely solely on malware-free techniques do so to limit their footprint and make it more difficult for organizations to detect and respond. For this reason, organizations need comprehensive visibility into their networks combined with proactive threat hunting to uncover threats not identified by legacy security technologies.

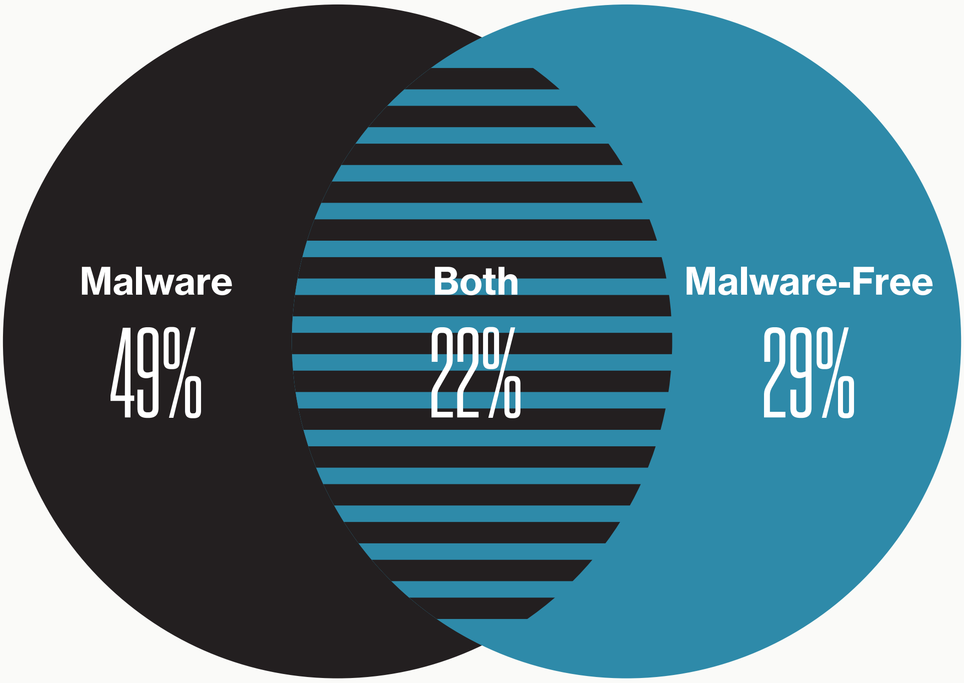


Figure 4. Percentage of attacks by technique

MALWARE INTRUSIONS

Big Game Hunting

From mid-2018 and throughout 2019, the most notable trend among eCrime adversaries has been the use of "big game hunting" (BGH) techniques. BGH attacks focus on high-value data or assets within larger organizations that are especially sensitive to downtime — so the motivation to pay the ransom is consequently very high. Using sophisticated ransomware campaigns to target large organizations, BGH operations have proven to be incredibly lucrative for eCrime adversary groups. These attacks often exhibit a combination of malware-based and malware-free tactics, with the attackers relying on malware for the initial compromise and the encryption of data but using malware-free techniques to move laterally and identify targets. Adversaries that have engaged in BGH operations in 2019 include WIZARD SPIDER, INDRIK SPIDER and DOPPEL SPIDER, as well as affiliates of the ransomware-as-a-service actor PINCHY SPIDER.

Criminal Group Collaboration

Within the incidents the Services team responded to involving malware, the top five malware families were linked to non-state-affiliated criminal groups. What is most interesting is that CrowdStrike has observed collaboration among a number of these threat actor groups. Often, MUMMY SPIDER provides initial access to an environment via Emotet. From there, access is transferred to WIZARD SPIDER or INDRIK SPIDER. WIZARD SPIDER leverages TrickBot to move laterally and deploy Ryuk ransomware. INDRIK SPIDER operates in the same fashion, using Dridex and BitPaymer. CrowdStrike assesses that this collaboration, enabled by MUMMY SPIDER's specialized role within the attack, permits these actors to be more effective and makes the attacks more lucrative. For more publicly available reporting on this topic, please read a blog post on PINCHY SPIDER, two posts on WIZARD and LUNAR SPIDER collaboration (here and here) and follow the links to posts included in the table below.

Rank	Type	Threat Actor Group
1	TrickBot	WIZARD SPIDER
2	Emotet	MUMMY SPIDER
3	Ryuk	WIZARD SPIDER
4	Dridex	INDRIK SPIDER
5	BitPaymer	INDRIK SPIDER

Table 3. Top 5 malware types and related adversaries observed in 2019

TOP ATTACK TECHNIQUES EMPLOYED

Understanding the most common and effective techniques adversaries employ can help an organization deploy security controls commensurate with the proliferation of, and ultimately the risk posed by, each attack technique. The most common technique observed by CrowdStrike Services involved credential dumping, while the third most popular technique included the related practice of account discovery. Often, the goal of an attacker is to gain access to a network via legitimate credentials and escalate privileges to move laterally while masquerading as an actual user or administrator on the network. The illegitimate use of legitimate credentials can be more difficult to identify than malware and other forms of attack.

Many of the techniques observed can be leveraged in LOTL attacks. It's often difficult to distinguish LOTL adversary activity from the legitimate use of these same tools by network administrators. This is precisely why gaining real-time visibility and recording metadata via EDR technologies can add context to analysis that will help distinguish legitimate from illegitimate LOTL activities.

Rank	Type
1	Credential Dumping
2	PowerShell
3	Account Discovery
4	Command Line Interface
5	Scripting

Table 4. Top five MITRE ATT&CK techniques observed in 2019

To help organizations prioritize visibility into and prevention of these most common techniques, the Services team ranked the data by most effective mitigation technique in Table 5. Each technique has been prioritized based on its prevalence in the CrowdStrike Services cases observed in 2019.

EFFECTIVE MITIGATIONS

Understanding the threats and most common techniques leveraged by attackers as described in the previous sections is only useful when accompanied by knowledge of how to detect and prevent them. In addition to a next-gen AV (NGAV) solution such as the Falcon platform, there are a number of effective mitigation techniques the team observed in clients' environments. The following is a list of techniques the Services team found most effective. It should be evaluated in light of your organization's risk profile.

Mitigation	Credential Dumping	PowerShell	Account Discovery	Scripting	Command Line
Active Directory Configuration	🟦				
Credential Access Protection	🟦				
Operating System Configuration	🟦		🟦		
Password Policies	🟦				
Privileged Account Management	🟦				
Privileged Process Integrity	🟦	🟦			
User Training	🟦				
Code Signing		🟦			
Disable or Remove Feature or Program		🟦		🟦	
Application Isolation and Sandboxing				🟦	
Execution Prevention					🟦

Table 5. List of the most effective mitigation techniques

MITRE already maps mitigating measures to adversary tactics in the ATT&CK framework. While this is helpful, it can be difficult to turn mappings like the ones in Table 5 into actionable measures that your security team can pursue. In the following section, the report identifies four fundamental security measures that the Services team has observed frequently making a difference in preventing or detecting the top five attack techniques in a client's environment. While these measures — MFA, network segmentation, AV/anti-malware and log analysis — are fairly fundamental practices, executing them well is not always easy.

MULTIFACTOR AUTHENTICATION

CrowdStrike recommends that organizations enable MFA mechanisms on all public-facing employee services and portals. This will inhibit unauthorized access to employee data and the organization's environment, especially threat actor activity in scenarios where employee enterprise credentials may have been compromised.

NETWORK SEGMENTATION

Security teams could implement segments in their Active Directory forests that do not inherently trust domains or organizational units (OUs) within its forest. The network segments would be separated by subsidiaries or domains and then by organizational units within each domain. These domains and OUs should have controlled and limited account access, specifically by not implementing an inherent two-way trust between parent and child domains. In addition, these network segments should contain a hardened system with endpoint and network-based monitoring that serves as an intermediary or “jump server” between each segment. The jump server functions as a controlled access point between domains. A controlled and segmented network greatly reduces the attack surface and increases the difficulty for threat actors and self-propagating malware to move within an environment.

AV / ANTI-MALWARE

Organizations should implement an advanced endpoint protection agent across their environments. To maximize efficacy, the endpoint protection should contain machine learning to identify anomalies and perform heuristics, in addition to real-time AV and anti-malware capabilities. The endpoint protection should contain both detection and prevention capabilities, so security teams are aware of suspicious events or actions taking place in their environments. Finally, organizations should have a dedicated team that can monitor and coordinate any events identified by the endpoint protection platform. Security teams could also test and implement application whitelisting for critical systems, such as file servers or domain controllers. Application whitelisting can be implemented through Windows AppLocker to help prevent the execution of unknown and untrusted applications or script code. By whitelisting applications, unauthorized and potentially malicious applications and software will be unable to execute, thereby limiting potential attack vectors from both threat actors and insider threats.

LOG ANALYSIS

When it comes to “visibility” within an environment, there is still no substitute for effective log analysis. Aggregating and analyzing security-relevant logs in a security incident and event management (SIEM) tool allows security teams to develop a more complete picture of what is occurring in their environments. While advanced AV and network security tools have the potential to detect or prevent the top five attack techniques listed above, a SIEM with robust detection rules has the ability to catch anything that might slip through the cracks that sometimes exist at the margins of those advanced capabilities. Not only does a SIEM help with log analysis to detect an incident, it also facilitates investigation into any incidents that occur.

Getting the most out of a SIEM tool requires two things: ensuring that it is ingesting and storing the right data; and developing detection rules that effectively alert on suspicious activity without generating too many false positives. Modern SIEM tools include relatively good out-of-the-box detection rules that can then be refined as a security team identifies new use cases. As for which logs to ingest, that will be specific to each organization and the systems that are critical to its operations. At a minimum, CrowdStrike recommends retaining the following logs for the following periods of time:

LOG SOURCE	RETENTION PERIOD
DNS Requests	3 months
Operating System Event Logs	6 months
Web Proxy Logs	6 months
Active Directory Authentication Logs	6 months
Remote Access Authentication Logs	6 months
Router Logs	3 months
Security Tool Alert Logs	12 months
VPN Logs	12 months
Two-Factor Authentication Logs	12 months
Firewall Logs	3 months

Table 6. Types of logs and retention periods CrowdStrike recommends

KEY THEMES

The work CrowdStrike Services undertook in 2019 across all engagements provides evidence of six key themes:

01 **Attackers are leveraging BloodHound to expedite network reconnaissance**

02 **Third-party compromises are serving as a force multiplier for attacks**

03 **Attackers are targeting cloud IaaS**

04 **Macs are now clearly in the crosshairs of the cyber fight**

05 **Patch management and accountability are an old problem deserving of a holistic approach**

06 **Prevention: If you're not flipping all the switches, you are doing it wrong**

These themes are described in the following section of the report.

THEME 1: ATTACKERS ARE LEVERAGING BLOODHOUND TO EXPEDITE NETWORK RECONNAISSANCE

As early as 2017, CrowdStrike observed the use of BloodHound by attackers in real-world intrusions. However, the use of this popular internal Active Directory reconnaissance tool by threat actors increased dramatically in 2019. Since 2018, CrowdStrike observed BloodHound being used particularly in the form of PowerShell-based ingestors like those incorporated by the CobaltStrike and PowerShell Empire penetration testing frameworks. In several large ransomware attacks, eCrime actors have adopted this methodology to accomplish lateral movement and gain privileged access to key assets more quickly.

CrowdStrike has frequently highlighted the BGH phenomenon in ransomware attacks, where attackers are more focused on targeting organizations and data that will maximize the impact of their attack. Increasingly, they are using BloodHound and similar techniques to sniff out a clear path through the victim's network to their objective.

WHY BLOODHOUND?

In many ways, Active Directory is the heart of a network (for those networks that use it, which is the majority). It handles identity, authentication, authorization and enumeration, as well as certificates and other security services. It is designed to help find things, which generally enables and accelerates business operations. But the same characteristics that make it a cornerstone of business operations can make it the perfect guide for an attacker. Since its inception, smart attackers have leveraged Active Directory to map out a target network and find the primary point of leverage needed to gain access to key resources. Modern tools like BloodHound have greatly simplified and automated this process. Smart companies can use these same techniques to find and remediate potentially vulnerable accounts and administrative practices before an attacker finds them, frustrating the attacker's quest for privileged access.

ACTIVE DIRECTORY ANALYSIS AND BLOODHOUND BASICS

In even a modest-sized organization, Active Directory creates an intricate web of relationships among users, hosts, groups, organizational units, sites and a variety of other objects. All those connections in their raw form can be overwhelming but it is important to remember that an adversary is focused on a particular objective. Their goal is to move from whatever they currently have access to, perhaps a single compromised user account on a single laptop, to the prize they are seeking. They need to determine which user account on which host will enable them to access the data they are after. BloodHound is a tool created to facilitate finding that information.

BloodHound is an open-source tool developed by penetration testers. It was first released in August 2016 and has been updated several times since then. Its purpose is to enable testers to quickly and easily gain a comprehensive and easy-to-use picture of an environment — the "lay of the land" in terms of Active Directory on a given network — and in particular, to map out relationships that would facilitate obtaining higher-privileged access to key resources. Table 7 provides examples of data that can be obtained using BloodHound.

User	Computer	Group
Password Change Date Password Not Required	Service Principal Names Local Admins Operating System	Members

Schema	ACL	Host-specific
MemberOf Owns	GenericAll AllExtendedRights	CanRDP HasSession AdminTo

Table 7. Examples of data obtained by BloodHound

BloodHound is designed to feed its data into the open-source Neo4j graphical database. This allows BloodHound to natively generate diagrams, like the one in Figure 5, that display the relationships among assets and user accounts, including privilege levels. By selecting a specific network asset, the user can generate a map that shows paths to achieve privileged access to that host, as well as the accounts and machines from which that access could be gained.

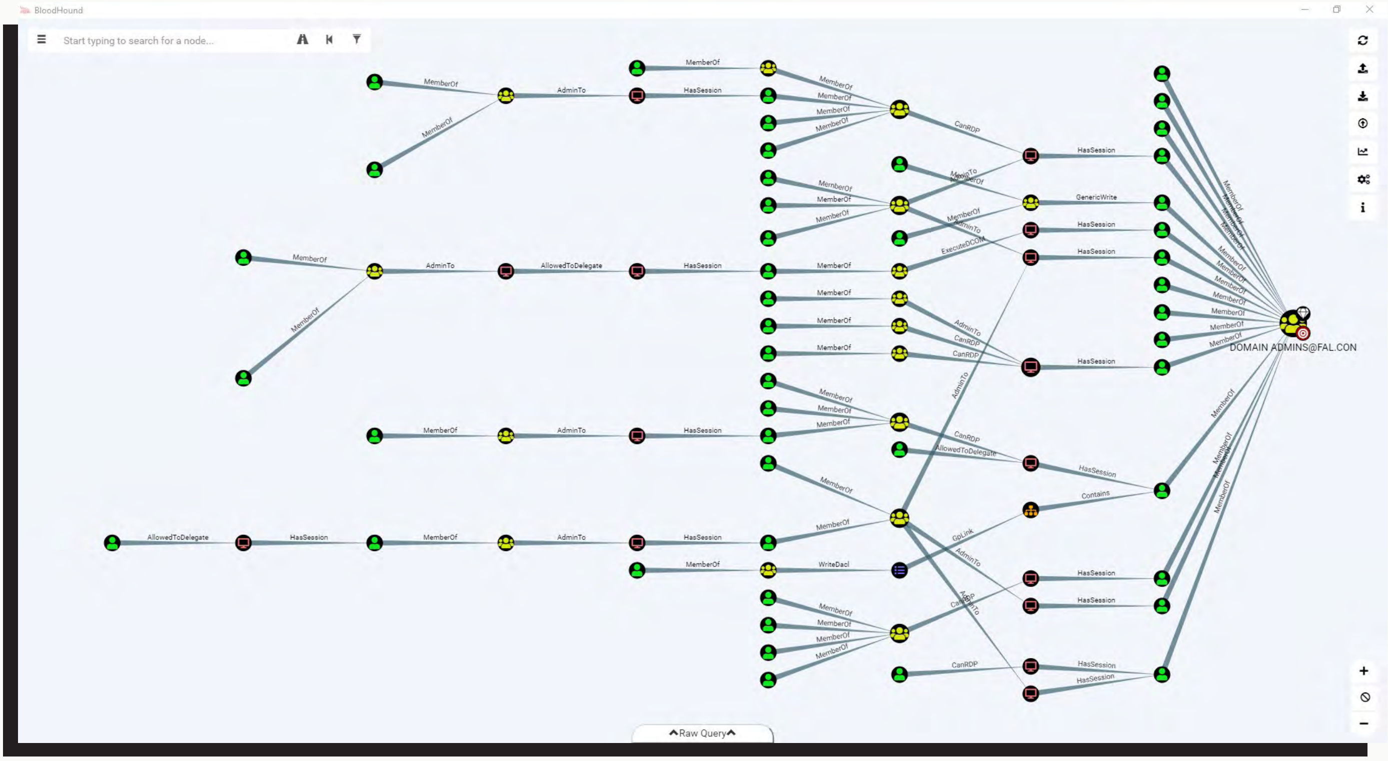


Figure 5. BloodHound diagram showing relationships among assets, user accounts and privilege levels

WHAT CAN BE DONE?

CrowdStrike recommends the following practices:

- **Leverage tools that will detect the use of BloodHound or another ingestor.** For instance, the CrowdStrike Falcon platform can detect and block the PowerShell version of the BloodHound ingestor if “Suspicious PowerShell Scripts and Commands” blocking is enabled in the prevention policy.

- **Use BloodHound for your own purposes.** It is valuable to think about how you can use a tool such as BloodHound to enhance your network defense. BloodHound provides deep insight into how a network is organized and how permissions to access assets on that network are structured. This is information that can enhance your network defense strategy.

- **Map out your network permissions.** Harvest the insights from BloodHound, then study those permissions the way an attacker might. This will allow you to find and eliminate the paths that an attacker might take to elevate their privileges and gain access to your key network and information assets.

- **Change account permissions and privileged account management practices.** This can help you make your network a much harder target for an attacker. In addition, this information can be used to discover security weaknesses, such as accounts that are vulnerable to attacks like Kerberoasting.

THEME 2: THIRD-PARTY COMPROMISES ARE SERVING AS A FORCE MULTIPLIER FOR ATTACKS

Threat actors are constantly seeking delivery methods that are efficient and impactful and provide a low barrier of entry. One such method is through a third-party provider with existing access to other more attractive targets. Past examples of this involved law firms that hold sensitive information belonging to multiple clients, or service providers that require network access from their clients. This type of targeting behavior has persisted, but in 2019, CrowdStrike also observed an uptick in threat actors targeting popular remote administration software platforms — such as those leveraged by third-party providers to manage their customer needs — as an initial entry point into victim environments. Additionally, CrowdStrike saw a rise in attacks against third-party providers that support particular vertical market segments. Similar to more traditional watering hole attacks, compromising a vendor's legitimate access to the victims' networks allows one attack to spawn access to multiple victims in the attackers' target vertical. It's a huge win for the bad guys.

Attacks that originate within third parties can be either targeted or opportunistic. The effects on the victim networks are often a reflection of the attacker's motives.

TARGETED ATTACKS

Targeted intrusion attacks that originate with third-party providers typically follow one of two patterns: Either the threat actor is targeting multiple organizations in a single sector or common interest, or the actor is targeting a specific organization. The former case has become increasingly common in the Services team's experience, with attackers recognizing that a successful compromise of the right third party can yield a treasure trove of information on a particular topic.

Because data theft is often the objective of these types of targeted intrusions, the effects on the victim organizations can vary. While data theft via a third-party compromise can have severe business or operational consequences, it does not usually result in a deliberate disruption or destruction on the part of the attacker, as is the case with opportunistic attacks. Because this type of attack yields continuing returns the longer the attacker persists, attackers are finding more creative and surreptitious ways to gain access and remain undetected in victim environments.

OPPORTUNISTIC ATTACKS

Opportunistic attacks via third-party access can cause significant damage to the victim's organization. This is because most opportunistic attacks focus on ransomware delivery, looking to extract a hefty ransom by encrypting critical business resources, often on systems the victims are not aware have been exposed publicly. In 2019, CrowdStrike worked with victim organizations that had internal systems publicly exposed by their third-party provider unbeknownst to them, and as a result, these internal systems were subjected to massive bruteforce campaigns until the credentials were cracked. In some cases, the attacker moved into the network and identified business-critical systems to receive targeted ransomware. The victim was not monitoring the authentication logs, so unfortunately, the first time they became aware of the issue was when the targeted systems were ransomed.

In these cases, the threat actor will compromise third-party provider credentials, then use access from those credentials to infiltrate and further compromise clients or customers of that third-party provider. Maintaining persistence in the customer's environment is typically accomplished through normal business-to-business applications, such as a GoToAssist (now called RescueAssist), TeamViewer, or by simply leveraging VPN credentials and moving laterally using RDP or Apple Remote Desktop (ARD) rather than using a custom backdoor or proxy utility.

Once inside the victim's environment, the threat actors may proceed with the attack themselves or hand off access to another group — for example, to deploy ransomware. With regard to ransomware, this is another way threat actors are performing BGH or enterprise ransomware attacks. They are simply using third-party access as a force multiplier.

WHAT CAN BE DONE?

Organizations can take action to prevent or minimize the ability of attackers to maliciously leverage third-party provider access. Before engaging in a contract with the third-party provider, organizations should understand what security controls are in place in the provider's environment and how those controls may factor into the organization's overall security posture. If a third-party provider's security posture is not strong and its ability to detect malicious or suspicious activity is slow, it can ultimately have a negative impact on the client organization.

- **Do the basics.** Many breaches — some would argue most breaches — include a large number of events that were not reviewed by the victim, such as failed authentication attempts. While it is important to "keep the lights on" in any business, it is just as important to do preventative maintenance on the business's critical technology systems to ensure they are not vulnerable to attacks. As an incident responder, it is uncomfortable to have to tell the victim of an attack that all that was needed to prevent their massive business interruption was to monitor logs and take appropriate action. Patching systems in 30 days and monitoring critical event logs are practices that all organizations should be performing, regardless of whether or not the system is outsourced to a third-party provider. If the system is critical to the business, it needs to be on a preventative maintenance program.

- **Develop a vendor risk management program.** Vendor risk management programs are designed to limit the risk of an organization suffering a breach as a result of a third-party compromise. These programs work by reducing the likelihood that such a breach can occur, and also by helping to minimize the impact if one does occur. Reducing your risk requires collecting information about your third-party partners. This can come in the form of answers to questionnaires, security risk rating services or requiring that a vendor comply with certain standards or conduct more thorough assessments. Reducing the impact of a third-party breach may mean restricting what third parties can access in your environment and how that access occurs. Strong identity and access management protocols should limit what third parties can access. Mature organizations often place third parties in a separate user group, subject them to additional scrutiny and apply the principle of least privilege. Another way to reduce the impact of a breach via a third party is to increase your access to information if a breach does occur. Contracts that require swift notification of any security incident are becoming increasingly common. Contracts that require the third party to provide information or access in support of a security investigation are less common because they are harder to negotiate, but they are worthwhile for third-party relationships where there is a high level of access to critical resources.

- **MFA is a must-have for any business-to-business network access.** In 2019, CrowdStrike observed an increase in attackers that leverage credentials harvested from a third-party provider environment and then use those credentials to access a client network of that third party. If MFA with a rotating token code as the second access factor had been in place, simply reusing stolen credentials from a third-party provider would not have been effective, and circumventing MFA would have been much more difficult for the attacker.

- **Understand the endpoint detection and prevention capabilities of the third-party provider and client environment.** If third-party providers were breached, how would they know? If a third-party provider's clients were breached, how would they know? Organizations should take steps to understand what endpoint protection or system security detection and prevention mechanisms are in place — not only in their own environment, but also for their third-party providers. In many cases, if the third-party provider could detect an initial breach sooner — by following the 1-10-60 rule, for example — the scope and impact of the attack on the provider and the client would be significantly reduced. In all cases, if both parties had advanced endpoint detection and prevention mechanisms with coverage across all endpoints, the attacker activity would have been prevented or at least detected and quickly mitigated.

- **Find out if the third-party provider has performed a compromise assessment or a cybersecurity maturity assessment of their environments.** During mergers and acquisitions, most companies elect to perform a compromise assessment to understand if the network they plan to purchase and merge with is or has been compromised. Prospective clients of third-party providers can make a similar request of the third-party provider and learn if there has been a proactive service performed recently, such as a compromise assessment or cybersecurity maturity assessment. Both of these assessments can help security teams understand whether their environment was previously compromised and provide information on their overall security posture. Security teams can then use this data to make informed decisions on whether to engage with the third-party provider.

- **Ask the third-party provider to perform a red team assessment.** For an interactive understanding of how effective a third-party provider's security controls are and how they could affect their clients' environments, a red team or adversary emulation exercise can be invaluable. It provides real-world examples and insights into the effectiveness of the client's current security controls and areas for improvement. For example, a red team exercise can reveal just how easy or difficult it would be for an attacker to achieve certain objectives, such as accessing a client organization via a third party or accessing specific controlled data within an environment. The findings from a red team exercise can help an organization, whether it is a third-party provider or the client, make informed security and business decisions going forward.

THEME 3: ATTACKERS ARE TARGETING CLOUD IAAS

In 2018, CrowdStrike Services responded to a number of incidents in which clients' public cloud-based infrastructure was compromised at various levels. In 2019, the Services team observed increasingly sophisticated operations in which financially motivated adversaries sought and used cloud API keys to rapidly and systematically harvest information assets for ransom or sale. They also sought other keys and passwords to facilitate further access, enabling them to repeat the cycle.

Limited or no controls around critical assets is nothing new in information security. However, the phenomenon of IaaS API key theft in particular has opened a vast new attack surface into this age-old struggle. API key theft gives adversaries easy access to critical controls and data assets when not matched with appropriate controls. Many recent cases involved static credentials that were not protected by MFA, IP address-based restrictions or automatic rotation. When threat actors harvested API keys from public source code repositories in prior years, it was typically a crime of opportunity. In 2019, it became targeted, and CrowdStrike responded to multiple cases in which attackers actively sought cloud IaaS API keys in client and third-party infrastructure. In virtually all cases, these long-lived API keys posed an unnecessary liability as they could have been replaced with ephemeral credentials issued through the underlying cloud infrastructure.

In addition, observed detection times ranged from hours to months, and in many cases, data exfiltration occurred before detection. Host-level compromise in the cloud continues, and many cases involved "shadow IT" cloud deployments — deployments that received limited security oversight and investment. The Services team observed gaps in endpoint (instance/VM) detection capabilities, misconfigured logging, lack of system and application vulnerability management, and misconfigured firewall rules. The team also noted that organizations with active security programs had staff who were already stretched thin in their efforts to secure on-premises resources and who also lacked familiarity and experience with cloud environments. Some cases involved serious incidents affecting infrastructure that was already slated to be decommissioned prior to compromise. The Services team consider these trends a contributing factor in compromises resulting from both nation-state and financially motivated operations.

WHAT CAN BE DONE?

CrowdStrike continues to recommend the following practices to help organizations prevent breaches of their cloud infrastructure:

- **Avoid using static API keys anywhere.** Static keys pose a significant risk because they allow enduring access to large amounts of often sensitive data. Instead, use ephemeral credentials for automated cloud activity and enforce the usage of these credentials only from authorized IP address space. Also, require MFA for all user-originated cloud activity.

- **Proactively manage cloud accounts and permissions.** Begin this process by conducting an account inventory to ensure every resource has an identified owner/responsible party. Next, use a cloud account factory model to ensure new cloud accounts comply with security expectations from the start. You should also review permissions in legacy or to-be-decommissioned cloud accounts for excessive public access to hosts and storage services. Finally, find cloud accounts/subscriptions that are not being monitored by looking for references to unrecognized cloud accounts. This can be achieved by collaborating with the finance department to find unrecognized cloud subscriptions.

- **Enable logging and alerting.** Enable detailed logging, including API and data object access logging, to the maximum extent affordable. Also, invest in and tune automated alerting to rapidly identify incidents and revert improper configuration changes.

- **Regularly review firewall rules on the cloud.** Use automated and manual firewall ruleset reviews to avoid global-permit rules in both inbound and outbound contexts.

THEME 4: MACS ARE NOW CLEARLY IN THE CROSSHAIRS

In 2019, CrowdStrike Services observed threat actors increasingly targeting macOS environments and using relatively unsophisticated methods to gain access. The increasing popularity of macOS systems in organizations, combined with insufficient macOS endpoint management and monitoring, has made Macs lucrative targets for threat actors. Once inside a victim environment, the Services team observed threat actors leveraging legitimate user credentials and native macOS utilities to move laterally and persist there while evading detection. The relative lack of monitoring and management of macOS systems, compared to Windows systems in the same organization, has enabled many threat actors to stay active and undetected in macOS environments for months. The following explores some of the techniques threat actors are using to breach macOS environments.

Threat actors frequently gain access to macOS environments using phishing attacks or by targeting vulnerable public-facing infrastructure. Despite the use of spam-filtering solutions by victim organizations, wide-ranging phishing campaigns have been effective in capturing legitimate credentials. Threat actors often use phishing emails to direct the victim to a webpage that mimics a legitimate company login page, where they then capture the user's enterprise credentials. The Services team frequently observed threat actors using these credentials to gain access to networks via a corporate VPN that does not enforce the MFA.

Inside the victim environment, threat actors have largely taken a LOTL approach, using native and first-party utilities to laterally move to other systems and achieve their objectives. This same approach has been observed by different threat actors in Windows environments, using legitimate Microsoft utilities to conduct malware-free attacks. Using LOTL means threat actors don't have to bring their own toolsets to the victim's systems, where endpoint security technologies may detect and block them. However, by using utilities that are either natively present on the macOS system or developed by Apple and available on the App Store, threat actors are more likely to evade detection by legacy signature-based AV.

The team has also observed threat actors living off the land by using legitimate credentials captured from phishing attacks to authenticate to other macOS systems, leveraging tools such as native macOS screen sharing, Apple Remote Desktop and SSH. Native macOS screen sharing and Apple Remote Desktop simplify lateral movement for less-capable threat actors by providing a visual interface to access compromised machines. While the screen sharing method increases the risk of detection by an end user, it can be useful for threat actors that may not be skilled in using SSH or malware for their operations. Insufficient security controls and legitimate usage of these tools by IT teams have provided threat actors with an easy path to lateral movement across victim macOS environments.

While threat actors prefer using legitimate credentials and corporate VPNs to maintain access to a victim environment, the CrowdStrike Services team also observed threat actors occasionally using modified open-source malware to conduct operations and maintain persistence. In the event that a victim organization resets affected credentials or locks down screen sharing and SSH, malware can provide continued access to the environment. While this malware is far more likely to be detected by security tooling than native macOS utilities, it provides greater flexibility for command execution and persistence.

The lack of macOS endpoint management and security tooling can make it difficult for victim organizations to even be aware that an intrusion has occurred, let alone eject the threat actor from the network. MacOS IR investigations are also often hampered by a lack of tooling. In addition, the analyst skill set may not easily transfer from Windows to a macOS environment. Threat actors that are aware of IR investigations were observed leveraging anti-forensic techniques to limit the ability of incident responders to reconstruct malicious activity on macOS systems.

WHAT CAN BE DONE?

CrowdStrike recommends the following practices for macOS environments:

- **Implement stricter controls.** Organizations can increase detection and prevention of threats against their macOS environments by using a combination of security controls and endpoint protection technology. Endpoint management tools allow organizations to enforce policies such as patch installation and restrictions on remote access tools that threat actors leverage during intrusions. Disabling screen sharing and remote access via SSH are key controls that can severely restrict how a threat actor operates in a macOS environment. Restricting the pathways by which threat actors gain access and move laterally through macOS environments is critical to limiting the extent of compromises — even if phishing attacks are successful.

- **Ensure real-time event recording.** Real-time EDR tools, which are part of the CrowdStrike Falcon platform, are essential for early detection of a threat actor's operations. In addition, having real-time data from endpoints is critical when threat actors engage in anti-forensic activity such as clearing logs or command-line history. Real-time data is recorded in the cloud at the time of process and command execution and prevents records from being affected by log clearing attempts by the threat actor.

- **Better triage tools.** When conducting IR investigations, having the right toolset to investigate macOS intrusions is key to success. Triage tools such as CrowdStrike's open-source AutoMacTC are critical to scoping out an affected environment and quickly identifying compromised systems that require further analysis. Leveraging key artifact sources is crucial to understanding a threat actor's actions, even if they engaged in anti-forensic measures. These artifacts include Terminal saved state files, which provide scrollback history for interactive Terminal sessions even if bash history is wiped by the threat actor.

THEME 5: PATCH MANAGEMENT AND ACCOUNTABILITY ARE AN OLD PROBLEM DESERVING OF A HOLISTIC APPROACH

Vulnerability and patch management is a decades-old cybersecurity problem. In 2019, organizations still struggled to identify vulnerabilities, prioritize critical systems and deploy patches. As a result, companies have continued to suffer from ransomware attacks and malware that leverage exploit kits designed to identify and exploit vulnerabilities on unpatched systems. Newly released vulnerabilities such as BlueKeep and DejaBlue will continue to haunt organizations in 2020 and are already being used by attackers to install cryptomining software. The Services team found that clients can often experience vulnerability and patching issues because of departmental conflicts, missing patch management policies and limited accountability. Realistically, patching everything is easier said than done, though organizations have generally gotten better at it over time. Yet, even as they have improved, the factors that make it challenging have become more complex. Fortunately, companies are developing new, risk-based solutions to these problems that can be highly effective in addressing the persistent challenges patching presents.

PROBLEM 1: VULNERABILITIES EVERYWHERE, PATCHES NOWHERE

Information security teams have more data than ever on the vulnerabilities in their environments, while endpoint protection platforms and dedicated vulnerability management tools have become commonplace. But what do information security teams do with all this data? Usually, they rely on information technology (IT) teams to test and deploy patches, since IT teams are responsible for administering systems management and deployment tools. This is where organizations frequently fail. IT teams faced with a myriad of competing demands can often take months to be in a position to apply patches or may decide to defer them altogether because patches can introduce changes that can negatively impact systems.

This shouldn't come as a surprise, since patching naturally pits these teams against one another. Information security wants to keep an organization's critical systems safe, while IT wants to keep them working. If either team fails, it will cost the team its reputation and the business its money.

PROBLEM 2: JUST PATCH EVERYTHING

Information security teams approach IT departments with lists of systems to patch. This is often overwhelming. Even though vulnerabilities are labeled critical, high, medium, low and informational, some IT teams may look at these lengthy lists and not know where to start. The team may decide to patch an internet-facing email server first, since it contains information about the organization's trade secrets and has a high risk of attack. Meanwhile, critical patches to VPN software may be put on hold because of difficult deployment procedures and potential business interruptions. Unbeknownst to the IT team, the information security team may have threat intelligence reports showing that adversaries are actively exploiting the VPN's vulnerabilities.

PROBLEM 3: NO ONE WILL NOTICE

A lack of accountability for failing to implement patches is commonly seen at organizations CrowdStrike Services worked with in 2019. Most organizations do not have formal patching policies or any type of enforcement mechanisms to ensure their systems stay patched, and the incentives for information security and IT teams are often lacking. Pushing out patches isn't exciting work, and these tasks frequently get moved to the bottom of the project list. While automation can help solve this problem for some systems, critical patches on networking equipment or systems that require around-the-clock uptime require maintenance windows and significant resources. Technology teams can too easily forego these tasks in the name of business continuity without experiencing any immediate ramifications.

WHAT CAN BE DONE?

CrowdStrike recommends the following practices for patch management and accountability:

- **Leverage a risk-assessment framework.** Most organizations do not treat vulnerability risk with the same seriousness as other financial, operational or strategic enterprise risks. When vendors enter the market with new products and services that compete with a company's core business, they build new business plans or develop strategies to compete and reduce financial risk. Vulnerability management should use the same methods:

  - Organizations need to create — and obtain executive management sign-off on — vulnerability management and patching policies that define service-level agreements for both information security and IT teams.

  - Both teams need to work together to define the systems they consider most critical. While an IT team may define the phone system as critical to the business, the information security team may consider an internet-facing customer database to be a greater security risk. These perspectives are not contradictory, but together help form a fuller picture of the critical systems on which the enterprise depends. Using these definitions, teams can create a priority list that shows what should be patched first and what operational risks are taken for each system.

- **Employ documentation to drive accountability.** To keep teams accountable, information security and IT managers need to document why they are choosing to address specific vulnerabilities or patches but not others. Assigned members of the executive team should be responsible for signing off on the exceptions, essentially validating that the organization is choosing to accept the vulnerability risk. This hierarchy of vulnerability management can keep teams accountable and ensure that systems are patched in a timely manner. In 2019, CrowdStrike Services saw this framework adopted at more organizations than in years past. A recent healthcare customer implemented this risk-acceptance model to better track which vulnerabilities were not being patched by their IT team. The metrics produced from this framework were reported to key executives who decided to increase investment in vulnerability management. This investment not only led to a significant reduction in the number of vulnerabilities in their environment, it also reduced the average time to remediate vulnerabilities.

- **Hire a dedicated vulnerability management team.** In organizations with sufficient resources, CrowdStrike recommends dedicating information security and IT personnel to vulnerability and patch management. This team is then accountable for identifying vulnerabilities and deploying patches quickly, guided by the risk-assessment framework described above. The key advantage of this solution is that information security leaders can produce metrics that allow them to measure the effectiveness of the program. These metrics can be used to identify program gaps and operational efficiencies and, if needed, to dedicate additional resources to vulnerability and patch management.

- **Deploy patch prioritization and automation tools.** There are tools available that can assist and enhance how organizations operationalize patching efforts. Patch prioritization helps organizations make better decisions to reduce IT security risk, while patch automation solutions can dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation. CrowdStrike Falcon platform customers can benefit in this regard from the patch prioritization and automation applications available in the CrowdStrike Store.

THEME 6: PREVENTION: IF YOU AREN'T FLIPPING ALL THE SWITCHES, YOU ARE DOING IT WRONG

PREVENTION IS MORE IMPORTANT THAN EVER

The year 2019 saw a record number of ransomware infections, data leaks and targeted attacks, and organizations are turning to security tools to solve their problems. The market is full of them, and new tool types are being developed every day to protect against the expanding threat landscape. Companies' cybersecurity budgets are also increasing, giving them the buying power to invest in new technologies. While this is a positive industry trend, CrowdStrike experts saw a troubling parallel trend of tool misconfigurations.

Organizations are buying and deploying security tools at an increasing rate but failing to enable key preventative features that are designed to stop malicious activity. Failure to configure these tools properly is often worse than not having them in the first place. It can provide organizations with a false sense of security and waste tight security budgets. While this is not a new phenomenon, the growing frequency of ransomware and other disruptive attacks has increased the impact on organizations that fail to effectively block malicious activity.

THE WAND IS ONLY AS GOOD AS THE MAGICIAN

The CrowdStrike Services team frequently identified misconfigured tools during IR and proactive services engagements in 2019. Whether conducting a cybersecurity maturity assessment, performing a red team exercise or testing the veracity of a tabletop scenario, it was not uncommon for the team to encounter cutting-edge security toolsets that were not properly arrayed. This included unpatched exploits, severe misconfigurations and botched deployments. During one tabletop exercise, CrowdStrike consultants identified broad whitelisting rules in the customer's AV product that were originally created as part of an IT team developer test. The consultants used this misconfiguration to walk the customer through a simulated incident where attackers leveraged the whitelists to infect endpoints and move laterally throughout the environment. For a small organization, this type of attack could have easily put them out of business.

That isn't to say that large companies are immune to this pitfall. In fact, CrowdStrike Services found that they are often more likely to not configure or misconfigure their security tools, even though they have significantly more resources than smaller organizations. Large enterprises often have sprawling footprints, complex networks and multiple improvement projects running at any given time. It's no surprise that they sometimes fail to dot all the i's and cross all the t's.

This issue isn't just limited to endpoint detection platforms. CrowdStrike consultants also found crucial misconfigurations in intrusion prevention systems, data loss prevention tools, MFA platforms and cloud access security brokers. For example, the CrowdStrike Services team responded to incidents where malware moved laterally into a production environment. While security controls — such as next-generation firewalls that segment corporate and production networks — were in place, the victims had failed to configure any firewall rules. This allowed the malware to quickly spread to business-critical production equipment.

WHAT CAN BE DONE?

Why was this situation so prevalent in 2019? In truth, it's probably not significantly more common now than in years past. However, current threat trends place greater dependence on prevention, which makes misconfigured or under-optimized tools more problematic.

Unfortunately, there is no single cause for this, because like most human factors in security, it manifests in different ways. In some instances, security tools are deployed in "monitor" or "detect" mode during proof-of-concept testing to prevent disruptions in an environment, and more stringent prevention features may never be enabled. In other cases, information security teams are requesting that these features be enabled, but IT teams are not responding to their requests, either because they do not trust the tool or it is not a priority. It's more troubling, however, when companies purchase security tools just to meet compliance requirements, then never fully implement them. This is a dangerous tendency that the CrowdStrike Services team encounters from time to time. Purchasing these tools solely to meet compliance requirements can lead companies to believe they are secure when they are still vulnerable.

Because there is no single cause, there is no single fix. But there are things organizations can do to maximize the efficacy of their tools:

- **Never purchase a tool just for compliance reasons.** It is fine for compliance to be a driver in a technology purchase, but there must be people assigned to use and optimize the tools and processes.

- **Develop implementation plans for any new tools.** These plans should involve both IT and information security teams to ensure that stakeholders are aware of the tool's purpose and intended use. This planning process should also identify the tool's operational impact on the business and the degree to which that can be tolerated.

- **Establish change management guidelines.** A tool's agreed-upon configuration should be documented and then audited multiple times a year. Information security teams should frequently discuss configurations and new features with vendors and support teams to maximize the tool's value and validate its use in the organization's environment.

- **Develop a detection and prevention framework.** Not every tool needs to be deployed with the strictest preventative configurations enabled, especially if compensating controls exist. Implementing a detection and prevention framework should identify the threats and use cases that an organization wants to address and identify which tools map to which use cases. This provides an excellent foundation for determining which use cases to prevent and which ones to detect, and with what tools. It also provides a great source of security metrics.

- **Test yourself.** Regular audits and adversary emulation exercises should ensure that the tools are working as intended.

- **Take a risk-based approach.** Ideally, organizations would tune their toolsets endlessly in pursuit of optimal security. This is great if you have the time and resources, but it's not feasible for most organizations. If you can't lock everything down, choose your battles. Identify the attacks you most want to prevent and focus on them first.

ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services equips organizations with the protection and expertise they need to defend against and respond to security incidents. Leveraging CrowdStrike's world-class threat intelligence and next-generation endpoint protection platform, the CrowdStrike Services incident response (IR) team helps customers around the world identify, track and block attackers in near real time. This unique approach allows CrowdStrike to stop unauthorized access faster, so customers can resume normal operations sooner. CrowdStrike also offers proactive services so organizations can improve their ability to anticipate threats, prepare their networks and ultimately, prevent damage from cyberattacks.

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 2.5 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.

EXPERIENCED A BREACH?

Call +1 855.276.9347

www.crowdstrike.com/services