CrowdStrike Products

CROWDSTRIKE



# THE EVOLUTION OF RANSOMWARE: HOW TO PROTECT AGAINST NEW ADVERSARY TRENDS AND METHODS

There's no question that ransomware continues to be a growing threat. In fact, the ransomware adversaries that proliferated in 2020 are as motivated as ever, evidenced by the introduction of increasingly damaging tactics, techniques and procedures (TTPs) outlined extensively in the **CrowdStrike 2021 Global Threat Report**. High-profile global attacks across the public and private sectors offer just a glimpse of the much larger cybercriminal industry, especially since not all ransomware attacks make the news. In fact, in a CrowdStrike-sponsored **2020 CrowdStrike Global Security Attitude Survey**, 56% of respondents admitted their organization had suffered from a ransomware attack in the previous 12 months.

This paper explains the evolution of ransomware by breaking down trends in online extortion threats, and provides prescriptive advice on how to protect and secure your organization against such an attack.

# EVOLUTION OF RANSOMWARE AND CURRENT TRENDS

## AN OLD SCHEME

Even though ransomware has been in the headlines consistently over the past six years or so, the idea of taking users' files or computers hostage by encrypting files, hindering system access or other methods — and then demanding a ransom to return them — is quite old. In the late 1980s, criminals were already holding computers or files hostage in exchange for cash sent via the postal service. One of the first ransomware viruses ever documented was the AIDS trojan (PC Cyborg Virus) that was released via floppy disk in 1989. Victims needed to send $189 USD to a P.O. box in Panama to restore access to their systems, even though it was a simple virus that utilized symmetric cryptography.

## MONETIZATION

Despite its long history, ransomware attacks were still not that widespread well into the 2000s — probably due to difficulties with payment collection. However, the emergence of cryptocurrencies, such as Bitcoin in 2010, changed all that. By providing an easy and untraceable method for receiving payment from victims, virtual currencies created the opportunity for ransomware to become a lucrative business.

## EASIER BUT STILL CUMBERSOME

eCrime — a broad category of malicious activity that includes all types of cybercrime attacks, including malware, banking trojans, ransomware, mineware (cryptojacking) and crimeware — seized the monetization opportunity that Bitcoin created. This resulted in a substantial proliferation of ransomware beginning in 2012. However, this ransomware business model is still imperfect, because while Bitcoin payments are easy transactions for criminals to use, they are not always so easy for their non-tech-savvy targets to navigate. To ensure payment, some criminals have gone so far as to open call centers to provide technical support and help victims sign up for Bitcoin — but this takes time and costs money.

## CASE STUDY: DARKSIDE RANSOMWARE DISRUPTS COLONIAL PIPELINE

A ransomware attack disrupted Colonial Pipeline in May 2021 — the pipeline transports almost half of all fuel consumed on the East Coast of the United States — underscoring the fragility of critical infrastructure, and the magnitude of the problems faced by the public and private sector leaders who are charged with protecting it.

On May 10, the FBI publicly indicated the Colonial Pipeline incident involved DarkSide ransomware. It was later reported that Colonial Pipeline had approximately 100GB of data stolen from its network, and the organization allegedly paid almost $5 million USD to a DarkSide affiliate. According to **Reuters**, "The Justice Department on Monday recovered some $2.3 million in cryptocurrency ransom paid by Colonial Pipeline Co, cracking down on hackers who launched the most disruptive U.S. cyberattack on record" (June 7, 2021).

DarkSide is associated with a criminal group tracked by CrowdStrike Intelligence as **CARBON SPIDER**. Security researchers, customers and anyone interested in learning more about the technical tradecraft, targeted verticals and origin of CARBON SPIDER can explore the **CrowdStrike Adversary Universe** for intelligence on this tracked adversary and many others.

## BIG GAME HUNTING

To optimize their efforts, eCrime operators decided to pivot from the "spray and pray" style of attacks that were dominating the ransomware space and focus on "big game hunting" (BGH). BGH combines ransomware with the TTPs common in targeted attacks aimed at larger organizations. Rather than launching large numbers of ransomware attacks against small targets, the goal of BGH is to focus efforts on fewer victims that can yield a greater financial payoff — one that is worth the criminals' time and effort.

This transition has been so pronounced that BGH was recognized as one of the most prominent trends affecting the eCrime ecosystem in CrowdStrike's 2020 and 2021 Global Threat Reports. This tectonic shift toward BGH has been felt across the entire eCrime ecosystem, with ransom payments and data extortion becoming the most popular tactics for monetization in 2020. Throughout 2020, BGH continued to be a pervasive threat to companies worldwide across all verticals, with CrowdStrike Intelligence identifying at least 1,377 unique BGH infections.

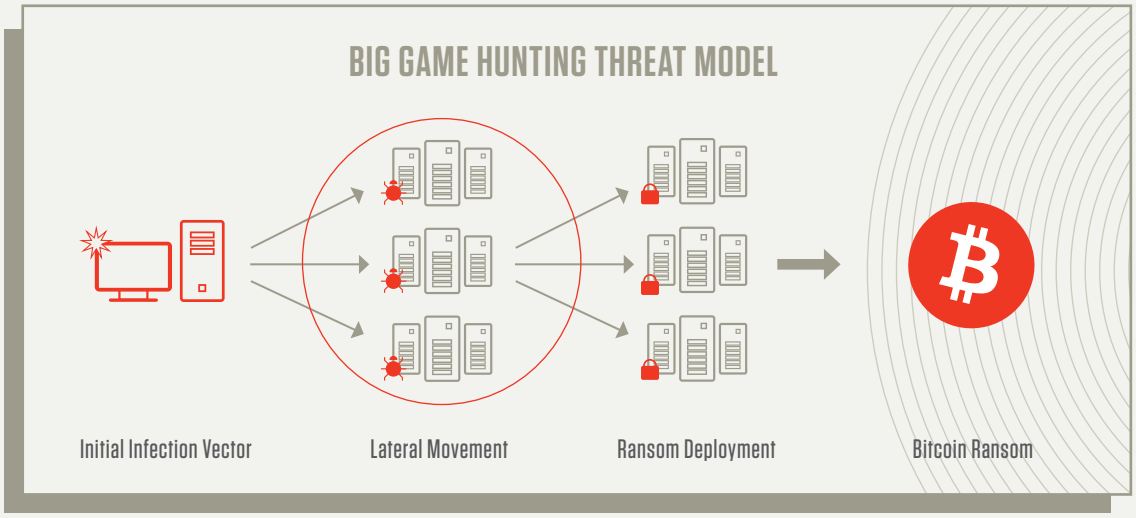



**Figure 1. Adversary groups are targeting enterprise organizations in BGH attacks that garner huge payoffs.**

# THE ACTORS BEHIND RANSOMWARE ATTACKS

CrowdStrike Intelligence monitors the eCrime ecosystem by tracking eCrime organizations, independent threat actors and their relationships. For example, the creator of Samas (aka Sam Sam) was identified as a threat actor named BOSS SPIDER; INDRIK SPIDER was credited with the creation of Dridex; and WIZARD SPIDER, also known as the Russia-based operator of the TrickBot banking malware — which in the past had focused primarily on wire fraud — was identified as the group that created Ryuk. These groups have been observed propagating ransomware attacks that are part of the BGH trend and raking in huge profits through targeted attacks that reap big rewards.

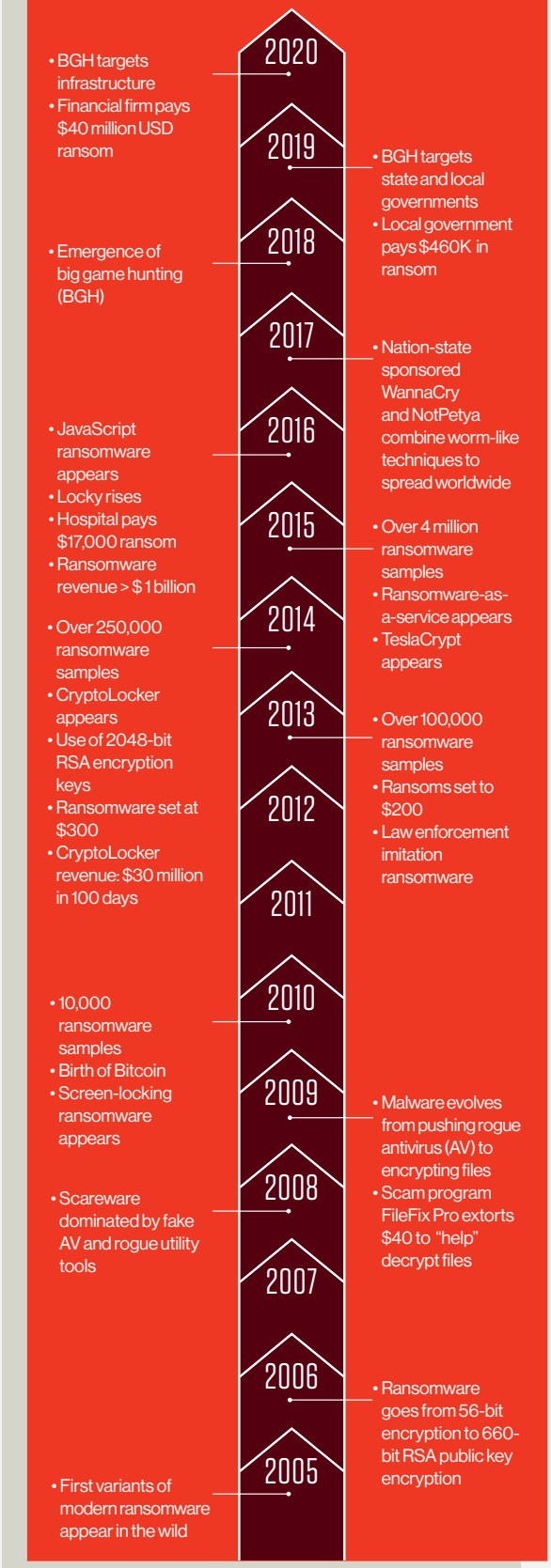
CrowdStrike has also observed that threat actors have started working together to facilitate targeted attacks and increase capabilities as "megacorps." The CrowdStrike 2021 Global Threat Report notes that WIZARD SPIDER — a BGH actor and established eCrime "megacorp" — has sustained its high-tempo operations to become the most reported eCrime adversary for the second year in a row.

# MORE SOPHISTICATION AND BLURRED LINES

Just like any software developer, eCrime groups constantly strive to improve and upgrade their ransomware with new functionality. WIZARD SPIDER, for example, has added many new capabilities to Ryuk and removed useless and obsolete functionality from the code. This group also added new enumeration modules that are downloaded onto victim systems to locate credentials and perform lateral movement within the victim's environment — with the objective of gaining access to the domain controller. Successfully gaining such access allows WIZARD SPIDER to deploy Ryuk ransomware throughout the victim's environment.

To complicate things, a trend observed in 2018 that continues today is the blurring of lines between nation-state and eCrime ransomware campaigns. Whether the ransomware code is stolen or willingly shared between nation-state actors and cybercriminals remains unclear, but CrowdStrike has observed both types of adversaries using similar malware, such as Ryuk, either for immediate financial gain or to create a distraction designed to obscure the origin of a nation-state attack.

## THE EVOLUTION OF MODERN RANSOMWARE



# HOW RANSOMWARE WORKS

There are many points of entry for ransomware, with phishing emails and website pop-ups among the most common vectors. Another entry route involves using exploit kits that take advantage of specific vulnerabilities.

## DARK PSYCHOLOGY: COMBINING BUSINESS SAVVY WITH RUTHLESS SOCIAL ENGINEERING

Technology and human nature are two sides of the same coin when it comes to ransomware attacks. In one case observed by CrowdStrike, a CEO's email was spoofed and the attacker used social engineering to trick employees into clicking a link in a fake email from the executive. To succeed, this attack required methodical research into the company's management, its employees and the industry. As BGH attacks increase, social engineering is becoming a more intensive presence in phishing attacks. Social media also plays a huge role, not only enabling attackers to discover information on potential victims but also as a conduit for deploying malware.

## WEBSITE POP-UPS AND EXPLOIT KITS: A DAMAGING COMBINATION

Website pop-ups and exploit kits can be used together to propagate ransomware that allows attackers to create "Trojan pop-ups" or advertisements containing hidden malicious code. If users click on one of them, they are surreptitiously redirected to the exploit kit's landing page. There, a component of the exploit kit will discreetly scan the machine for vulnerabilities that the attacker can then exploit. If the exploit kit is successful, it sends a ransomware payload to infect the host. Exploit kits are popular with eCrime organizations due to their automated nature. In addition, exploits are an efficient fileless technique, as they can be injected directly into memory without writing anything to disk, making them undetectable by traditional antivirus software. Exploits kits are also proliferating among less sophisticated attackers, because they do not require a great deal of technical know-how to deploy. With a modest investment on the darknet, virtually anyone can get into the online ransom business.

## FILELESS ATTACKS: RANSOMWARE WITHOUT RANSOMWARE

Fileless ransomware techniques are increasing. These are attacks in which the initial tactic does not result in an executable file written to the disk. Fileless ransomware uses pre-installed operating system tools, such as PowerShell or WMI, to allow the attacker to perform tasks without requiring a malicious executable file to be run on the compromised system. This technique is popular because fileless attacks are able to bypass most legacy AV solutions.

For a detailed explanation of how fileless ransomware works, download the **CrowdStrike fileless ransomware infographic.**

## NOTEWORTHY STRAINS OF RANSOMWARE

**BitPaymer:** Targets enterprise organizations using the Dridex loader module to gain an initial foothold in the victim's network

**DarkSide:** RaaS traditionally focused on Windows machines and recently expanded to Linux, targeting enterprise environments running unpatched VMware ESXi hypervisors or stealing vCenter credentials

**Dridex:** A strain of banking malware that leverages macros in Microsoft Office to infect systems

**Hermes:** RaaS first distributed in 2017 — in mid-August 2018, a modified version of Hermes, dubbed Ryuk, started appearing in a public malware repository

**KeRanger:** First ransomware targeting Mac OS X, was also able to encrypt Time Machine backup files

**PowerWare:** Encrypts hostage files through "fileless" infection

**Ransom32:** Written in Javascript, making it suitable for cross-platform infection on Mac and Linux systems

**Ryuk:** Similar to Samas and BitPaymer because it targets enterprise organizations and uses PowerShell — PsExec is used to push out its binary

**Samas:** Leverages vulnerable JBOSS systems to spread across a network and even attack backup files on the network — targets large organizations per BGH

**WannaCry:** Ransomware worm that takes advantage of the Microsoft Windows exploit EternalBlue — encrypts using the AES cipher

## RANSOMWARE AS A SERVICE (RAAS) AND ACCESS BROKERS

Because cybercriminals are always looking for ways to optimize their operations and generate more profits, they have been inspired by the SaaS (software as a service) model to create a RaaS (ransomware as a service) model. RaaS providers offer all of the attack components needed to run ransomware campaigns, from malicious code to results dashboards. Some even include a customer service department, putting ransomware within the reach of non-technically savvy criminals. In addition, the subscription cost is usually covered as a portion of the proceeds from the campaign, making this a cost-efficient model for cybercriminals to adopt.

RaaS providers offer all of the attack components needed to run ransomware campaigns, from malicious code to results dashboards.

An example of this type is the notorious RaaS CARBON SPIDER. CARBON SPIDER deepened its commitment to BGH in August 2020 by utilizing its own ransomware, DarkSide, and in November 2020, extended its footprint in BGH by establishing a RaaS affiliate program for DarkSide. This program allows other threat actors to use DarkSide ransomware while paying CARBON SPIDER a cut.

Access brokers are threat actors that gain backend access to various organizations (both corporations and government entities) and sell this access either on criminal forums or through private channels. Buyers save time with pre-identified targets and established access, allowing for more targets and faster deployments that result in a higher potential for monetization. Access broker utilization has become increasingly common among BGH actors and aspiring ransomware operators. CrowdStrike Intelligence has observed some access brokers associated with affiliates of RaaS groups.

## MALWARE OBFUSCATION IMPLEMENTED INTO BUILD PROCESSES

In 2020, CrowdStrike Intelligence observed WIZARD SPIDER and MUMMY SPIDER implement open-source software protection tools into their malware build processes.

The use of obfuscation techniques in malware is not new, but the inclusion of open source tools into build processes is novel, supporting advanced adversaries seeking agile development processes. Due to open source complexity, this tactic may have limited adoption by less sophisticated threat groups.

## TARGETING VIRTUALIZATION INFRASTRUCTURE

In 2020, CrowdStrike Intelligence observed both SPRITE SPIDER (the operators of Defray777) and CARBON SPIDER (the operators of DarkSide) deploy Linux versions of their respective ransomware families on ESXi hosts during BGH operations. While ransomware for Linux is not new, it is new for BGH actors to target Linux, ESXi specifically. This is a natural target for ransomware operators, as more organizations are migrating to virtualization solutions to consolidate legacy IT systems.

# HOW TO PROTECT AGAINST RANSOMWARE

## PRACTICAL STEPS

Backups are a good defense but must also be protected as they often are the first thing attackers prohibit or try to destroy in an environment. Making sure backups are secure and separately accessible even in a compromised environment, is a standard precautionary measure.

In September 2020, the U.S. Department of Homeland Security's Cyber and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC) published a joint **Ransomware Guide** outlining additional measures organizations should take to understand and handle the ransomware threat. The guide advises on how to protect against ransomware, prepare for a potential incident, recover from an attack and where to find help. It includes practical recommendations such as keeping systems patched and up to date, training end users, and creating and executing an incident response plan.

## USING THE MITRE ATT&CK® FRAMEWORK TO ASSESS READINESS

The MITRE ATT&CK framework is a comprehensive matrix that inventories and classifies techniques and tactics used by adversaries. It includes ransomware-specific techniques under a category called "Impact." The information it provides allows security teams to see how they might be attacked, reflect on their abilities to detect and stop such techniques, and plan for optimal protection.

## THE CROWDSTRIKE APPROACH

Because ransomware creators constantly shift their techniques, the CrowdStrike Falcon® next-generation endpoint protection platform empowers security teams to leverage an array of complementary prevention and detection methods, including the following:

- **IT hygiene** for quick identification and elimination of malicious or noncompliant activity by providing unmatched real-time visibility into devices, users and applications within your network
- **Machine learning** for the prevention of both known and previously unknown or "zero-day" ransomware without requiring updates
- **Exploit blocking** to stop the execution and spread of ransomware via unpatched vulnerabilities
- **Indicators of attack (IOAs)** to identify and block additional ransomware behaviors and protect against fileless and new categories of ransomware
- **Automated threat analysis** to immediately obtain all of the details about the ransomware found, including origin, attribution, similar families and indicators of compromise (IOCs )
- **Zero Trust** to understand behavioral data, limit the attack surface with segmentation, automate security tied to context and continuously verify access with the least friction

For organizations that want expert management, threat hunting, monitoring and remediation done for them, CrowdStrike Falcon Complete™ managed detection and response (MDR) **delivers a 403% ROI with 100% confidence**, with a best-in-class breach prevention warranty of up to $1 million USD.

The Falcon endpoint protection platform also maps to the MITRE ATT&CK framework with alerts in the Falcon platform. This allows security teams to quickly and clearly understand what is happening on their endpoints if an attack occurs — including the stage of the attack and any known adversary group that is linked to it.

## INDICATORS OF ATTACK: A UNIQUE AND EFFICIENT WAY TO THWART FILELESS MALWARE

Fileless ransomware is extremely difficult to detect using signature based methods, sandboxing or even machine learning-based analysis. CrowdStrike has developed a more effective approach using **indicators of attack (IOAs)** to identify and block additional unknown ransomware and other types of attacks. IOAs look for early warning signs that an attack may be underway — signs can include code execution, attempts at being stealthy and lateral movement, to name a few. By identifying the execution of these activities in real time, including their sequence and dependencies, IOA technology can recognize them as early indicators that reveal the true intentions and goals of an attacker.

IOAs also provide a reliable way to prevent ransomware from deleting backups. This gives users the ability to restore encrypted files, even if the file encryption began before the ransomware was stopped. This ability for IOAs to monitor, detect and stop the effects of what ransomware is attempting to achieve allows attacks to be stopped before any damage is done. In fact, the IOA approach is so effective and resilient against ransomware iterations that a single IOA can cover numerous variants and versions of multiple ransomware families, including new ones as they are released in the wild.

# CASE STUDY:
## HOW FALCON PROTECTS AGAINST DARKSIDE RANSOMWARE

The CrowdStrike Falcon platform incorporates intelligence derived from continuous monitoring of the TTPs of over 160 identified threat actors and numerous unnamed groups, enabling protection from sophisticated attacks, including DarkSide ransomware.

CrowdStrike employs a layered approach when it comes to detecting malware, including machine learning and IOAs. As Figure 2 shows, the Falcon sensor is able to kill the ransomware process as soon as the file encryption behavior is seen.

**This video** demonstrates how the DarkSide ransomware sample is immediately blocked and quarantined by the Falcon platform upon execution. CrowdStrike's machine learning engine is part of the Falcon agent and can protect the system online or offline. In addition to machine learning, the Falcon platform's built-in behavioral detection also identifies the rapid encryption of files and blocks the ransomware execution to protect the system.

CrowdStrike takes layered security to the next level by integrating machine learning and behavioral detection within a single lightweight agent to protect those systems critical to customers.

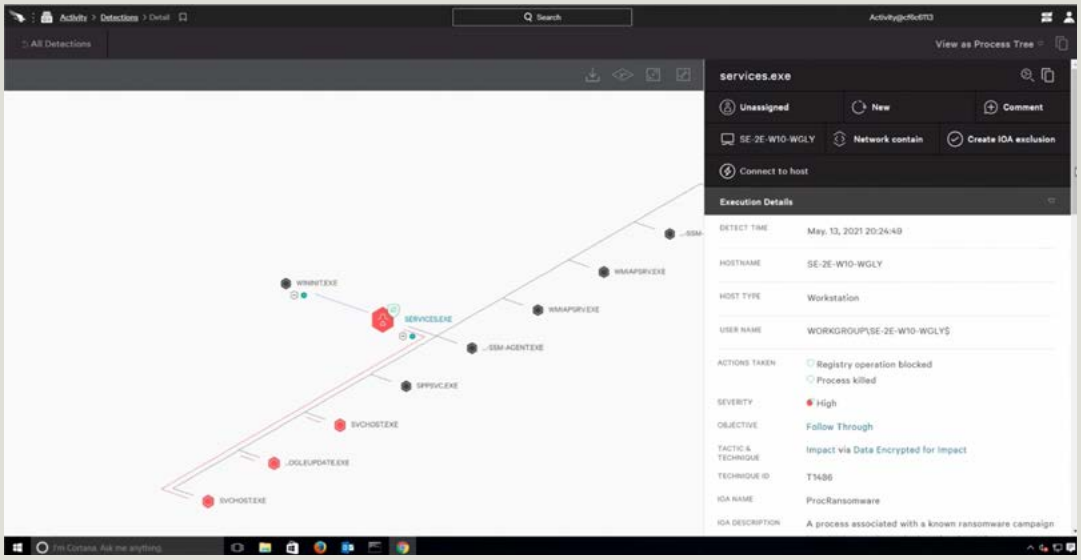



**Figure 2. CrowdStrike protects against DarkSide ransomware with layered technologies**

# CONCLUSION

As headlines continue to remind us, ransomware remains a significant threat from cybercriminals and nation-state actors that are constantly working to increase their malicious capabilities. CrowdStrike is committed to defending against ransomware by evolving and innovating its security technology to stay a step ahead of even the most determined adversaries.

As this paper makes clear, it requires a combination of elements to adequately protect your organization. This includes taking practical steps to align your organization with sound security practices, and also deploying the innovative, cloud-native, next-generation prevention and detection technology provided by the CrowdStrike Falcon platform.

# ABOUT CROWDSTRIKE

CrowdStrike, 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 upward of 1 trillion endpoint-related events per day 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.**

Speak to a representative to learn more about how CrowdStrike can help you protect your environment:

**Phone: 1.888.512.8906**

**Email: sales@crowdstrike.com**

**Web: www.crowdstrike.com**