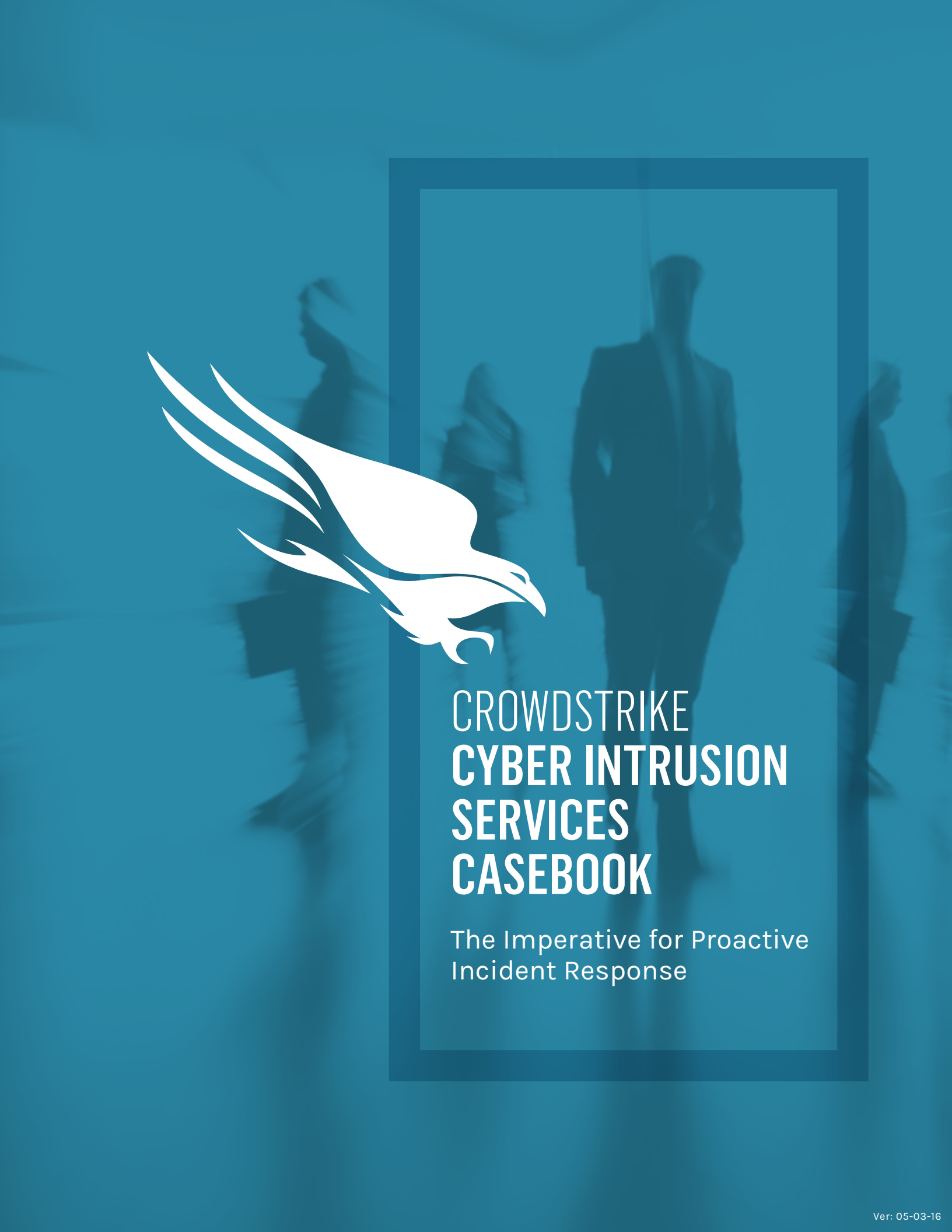


CROWDSTRIKE
CYBER INTRUSION SERVICES CASEBOOK

The Imperative for Proactive Incident Response

Ver: 05-03-16

"At this very moment, hackers throughout the world are scanning networks and looking for victims. Companies that are prepared can handle these as routine incidents, rather than an inevitable series of high-profile crisis events. Preparation is the most significant aspect to lowering business risk."

SHAWN HENRY
PRESIDENT, CROWDSTRIKE SERVICES, INC.

CONTENTS

This following report prepared by CrowdStrike's Services team focuses on actual intrusion cases the team has remediated, drawing conclusions and insights from these recent global attacks targeting large organizations. Based on the team's extensive experience in the field, the report reveals information that may fundamentally change the way both executives and security professionals view and respond to such attacks in the future. It also provides proactive steps organizations can implement to improve their success rate in preventing, detecting and responding to these attacks.

The real-life engagements documented in the CrowdStrike Cyber Intrusion Services Casebook offer important details about attackers' tactics, techniques, and procedures, while describing novel strategies devised by the CrowdStrike Services team for effectively removing these threats from victims' networks. In addition, the report reveals evidence of several emerging trends observed in attack behaviors, such as how quickly adversaries attempt to reinfect an organization after initial remediation, the importance and means of obtaining credentials, and the unsettling frequency in which multiple attackers have been discovered simultaneously targeting the same organizations.

After analyzing key data from hundreds of incident response and proactive services investigations,

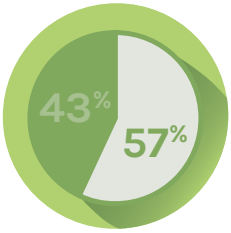
CROWDSTRIKE'S **KEY FINDINGS** INCLUDE:

ORGANIZATIONS MUST DEFEND AGAINST **MULTIPLE CONCURRENT ATTACKERS** IN THE SAME VICTIM ENVIRONMENT.

CrowdStrike identified multiple distinct adversary teams operating in 25 percent of our engagements. Defending against multiple adversaries carrying out concurrent attacks within an enterprise environment requires development of advanced surveillance capabilities and an ongoing, evolving understanding of attacker tradecraft, motivations and tool sets.

REINFECTION ATTEMPTS OCCUR WITHIN **TWO DAYS.**

On average, adversaries engage in reinfection attempts within two days of comprehensive remediation efforts. CrowdStrike assisted multiple clients who encountered reinfection attempts within hours and some outliers that identified attempts after a month of continuous monitoring. The one consistency in our data is nearly every organization remediating targeted attacks will experience attempted reinfection. Immediate reinfection initiatives must now be considered part of adversaries' standard operating procedure. As a result, enterprise security teams must develop appropriate strategies, countermeasures, and detection capabilities to address this inevitability.



SELF-DETECTION IS GAINING WITH 57% OF ORGANIZATIONS **DISCOVERING BREACHES INTERNALLY.**

CrowdStrike has seen a marked increase in the number of organizations self-detecting breaches, far above what has been previously reported. We attribute this to two factors: organizational maturity and improved endpoint and network detection technology. Our client sample used for this casebook skews towards medium to large sized businesses and that segment has invested heavily in improving people, processes, and technology to combat advanced threats. Organizations capable of self-detection are far more likely to identify breaches in their early phases and hence tend to suffer less loss and recover rapidly. Self-detection should be a goal of every security team, and it is encouraging to report that an increasing number of teams are reaching this goal.

CROWDSTRIKE'S **KEY FINDINGS** (CONT'D):

CREDENTIALS ARE A CRITICAL TARGET.

Regardless of adversary or motivation, the most common goal of attackers is to secure domain and enterprise credentials. Once this goal is achieved, the most common assumptions of risk and security management are altered because the adversary becomes — for all intents and purposes — an enterprise administrator on the network. They don't need malware because they…are you.

COMPROMISED ACCOUNTS ARE **HOARDED,** BUT USED SPARINGLY.

Unlike large-scale attacks of the past, adversaries no longer need to compromise hundreds of accounts to accomplish their objectives. As a result, they are cautious about how active they are on the accounts they have taken over, keeping them in reserve to avoid detection. This stealthier, more cautious approach makes detecting and responding to intrusions more difficult.

EXPERIENCED STAFF AND MATURE PROCESSES ARE DEFINING FACTORS OF A RAPID BREACH RECOVERY.

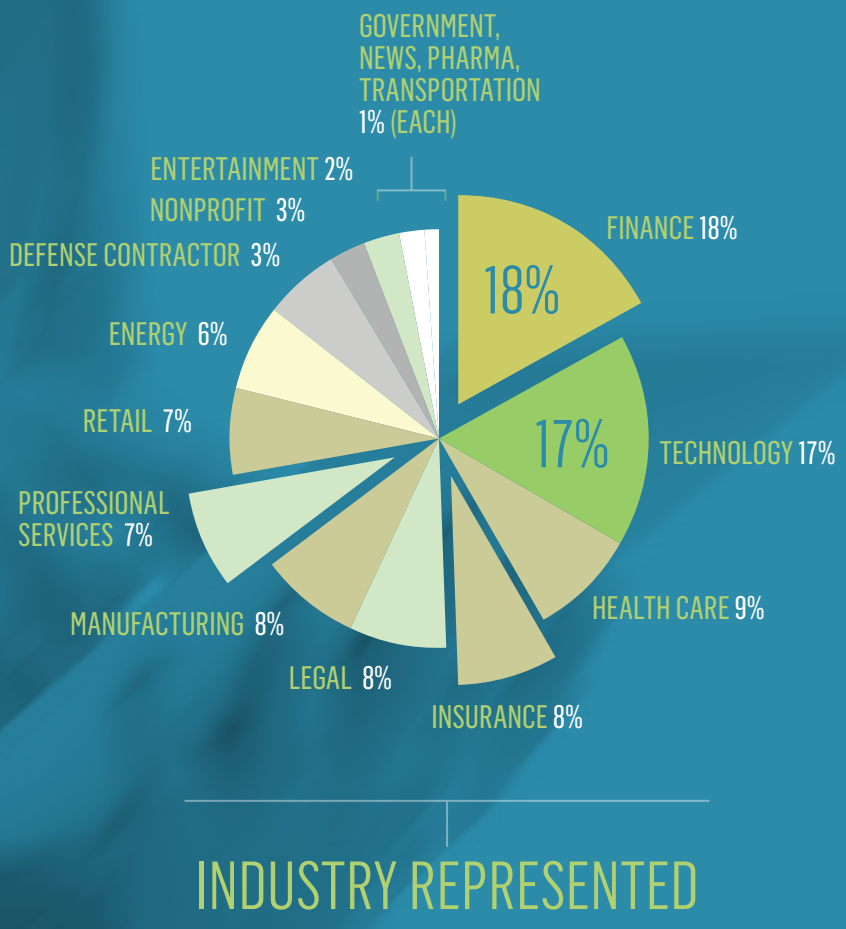
The review of CrowdStrike investigations found wide variation in the duration of investigations. The biggest factors determining the length and breadth of engagements revolved around the maturity of processes and people responsible for security, visibility, and response activities within the enterprise site. Inexperience at institutional and individual levels is a major factor that causes investigations to take longer than necessary. Conversely, organizations that are well resourced and have strong, mature processes with experienced staff experience shorter investigation cycles.

FIELD **DATA:**

The field reports that follow are based on a sampling of incident response investigations CrowdStrike has conducted for a collection of organizations representing a wide spectrum of economic sectors in terms of size and industry segments. Individually, these examples illustrate how organizations are being targeted and attacked, along with the measures that were taken to respond, remediate and recover. Taken together, these cases help provide indications of emerging trends that are driving the time and effort required to detect, prevent, contain, mitigate, and recover from actual or attempted intrusions.

To illustrate how the trends outlined above manifest themselves in real-world environments we cite two investigative and remediation efforts that were resolved quickly and efficiently because of good foundational preparation; this is contrasted with two engagements that took much longer than necessary to complete due to a variety of organizational factors.

A deeper exploration of some of these investigations is discussed in the case study section of this report.



FIELD NOTES: **LESSONS LEARNED**

INVESTIGATION 1:

Subject Matter Experts (SME's) + Good Processes = Nimble and Quick Remediation.

The FBI alerted a relatively small defense industry organization to an ongoing intrusion inside of their network. This led to a fast-paced investigation, largely because the organization was able and willing to act promptly on recommendations.

The organization's leadership team had implemented strong automated processes and reporting capabilities and as a result, the organization quickly and efficiently absorbed the results of CrowdStrike's investigation and rapidly deployed recommended countermeasures. Dozens of malware samples and utilities, together with an equally large number of compromised accounts used by the attackers, were uncovered. The adversary was identified as a nation-state actor interested in both industrial and state secrets.

Working closely with the client's team, the remediation effort began within days after the investigation commenced. The final investigation identified repeated instances where the attackers removed gigabytes of data from the organization's network during a multi-year period. Perhaps even more notable, within days of the initial comprehensive remediation activity, multiple attempts by the attackers to re-compromise the environment were detected and immediately blocked, showing the persistence of Advanced Persistent Actors.

TAKE-HOME **POINT**

A nimble internal team augmented by subject matter experts quickly conducted a thorough investigation, remediated the incident and successfully addressed ongoing attempts by the attacker to re-compromise the organization's networks.

INVESTIGATION 2:

Segmentation and Segregation of Accounts and Roles Minimizes Adversaries Attack Plan.

Internet service providers are an extremely attractive target for hackers. It should come as no surprise that most companies in this vertical take security very seriously, and invest heavily in detection, containment and recovery capabilities. However, even with best-in-class perimeter security, providers recognize the changing nature of today's threat landscape and operate from the assumption that breaches still are likely to have occurred. During a proof-of-concept exercise of CrowdStrike's endpoint monitoring solution, attacker activity was identified and linked to additional alerts from network intrusion devices. An investigation was launched and revealed that multiple accounts had been compromised; the vast majority of which were being actively leveraged by the attackers.

As part of a multi phased remediation approach, the provider implemented strong segregation of duties and segmented credentialing processes, which meant the compromised accounts were of little to no value to the attackers. The provider had assigned different accounts to discrete functions, and "time-limited" privileged accounts by generating new passwords after each use. This made it virtually impossible for attackers to move laterally across the provider's infrastructure without detection.

Attackers appeared to have been targeting credentials across many environments and were testing the validity of the credentials they obtained. Interestingly, once attackers realized the extent of the provider's segmentation, they decided to compromise large numbers of accounts to see if they could find the right combination of credentials to move laterally and achieve their goals. This frantic level of activity by the adversary resulted in their making many observable mistakes. CrowdStrike and the provider successfully identified, observed, and blocked these attacks as they were launched in real-time. This placed the organization in a better position to detect and ultimately prevent the attacker's reactions to their efforts on a continuous basis.

TAKE-HOME **POINT**

Strong internal processes and controls denied the attacker's ability to achieve their objectives and proportionately reduced the time required to detect, contain, and remediate the event.

AN OVERVIEW OF **ENDPOINT, NETWORK MONITORING,** AND **TRIAGE COLLECTION**

TRIAGE DATA COLLECTION

Triage, or live response, data collection is a means to collect critical volatile data from endpoints. Often used in the initial scoping phase of an investigation, triage data collection allows traditional forensic analysis to be accomplished at enterprise scale.

NETWORK MONITORING

Adversaries must communicate with systems to accomplish their objectives, and network monitoring takes advantage of this fact to identify malicious communications and help scope attacker activity. Full packet capture (pcap) or network session (flow) data is collected and analyzed at choke points within an environment. Network monitoring and analysis can be particularly effective at protecting egress points and sensitive parts of the network such as those known to house important data or legacy systems with known vulnerabilities. CrowdStrike's sensor and network analytics solution is called Falcon Network.

ENDPOINT MONITORING

The focus of every attack is an endpoint, and endpoint monitoring technologies take advantage of this fact by installing kernel-level detection mechanisms to record system activity at a granular level. In addition to detection performed at the system level, data can be aggregated and used to detect anomalies and track activity across an entire enterprise.

Falcon Host is CrowdStrike's endpoint protection solution. It consists of two components: a cloud-based application and an host-based sensor. The latter is capable of executing a wide range of necessary functions, including the identification of unknown malware, detection of zero-day threats, and seamless integration into an organization's current environment. Falcon Host uses CrowdStrike's Advanced Threat Intelligence Cloud, which combines advanced machine learning and graph data models to analyze billions of endpoint events, spotting and correlating anomalies that can be used to trigger an alert when an attack is underway.

INVESTIGATION 3:

Siloed Teams + Limited SME's = Longer Remediation.

In the case of a multi-billion dollar multinational organization, the initial investigation used host-based and enterprise forensic tools to identify multiple accounts in active use by attackers. Additional network and log analysis quickly identified login attempts on an even greater number of additional compromised accounts. Attacker account usage was tracked to the VPN. CrowdStrike worked with the client to rapidly implement a two-factor authentication solution to halt the progress of the breach. This interim remediation step proved useful as additional compromised accounts were easily identified through the increased authorization requirements and logging. It continued to prove advantageous throughout the investigation as attackers continued to probe for unprotected accounts in an attempt to regain access to the VPN.

A significant challenge for this multinational organization was the presence of decentralized teams working under different legal frameworks without a central leadership authority.

Internationally distributed teams pursued independent detection and remediation strategies in what eventually proved to be a less than functional effort. The lack of efficient coordination between international IT groups created gaps that ended up being a prime driver for the large number of compromised accounts. The attackers were able to take advantage of the confusion and jurisdictional upheaval to stay in the network much longer than similar organizations that employ a unified and integrated enterprise-wide response plan.

MOST COMMON BREACH TYPES

Intellectual Property (IP) Theft

Monetary Theft

Web Server Compromise

Data Destruction

Credential Theft

TAKE-HOME **POINT:**

International organizations with shared networks but lacking centralized IT security leadership, face additional challenges that can lead to uncoordinated processes, longer timeframes for containment, and increased damages.

MOST COMMON INITIAL ATTACK VECTORS

- Distributed Denial of Service (DDOS)
- Web Server Vulnerabilities
- Web Application Vulnerabilities
- Misconfigured DMZ Servers
- Spear Phishing
- Third Party Trust Relationships
- Strategic Web Compromise
- Weak Authentication Mechanisms
- Malicious Insider Threats
- SQL Injection

INVESTIGATION 4:

Lack of Centralized Logs Results in Adversaries Early Success.

In this engagement, attackers had access to key enterprise resources at a mid-sized defense contractor over a long period of time. The victim organization initially implemented a fragmented remediation strategy that lacked comprehensive scope and, as a result, the adversary was able to remain active even during the organization's initial remediation process. For instance, when the organization blocked a newly identified compromised account from being able to authenticate to the virtual private network (VPN), the attacker rapidly switched accounts to stay a step ahead of the organization's remediation efforts.

CrowdStrike was engaged and identified a critical factor complicating the investigative effort - the organization's lack of a usable centralized logging solution and the absence of key log sources — specifically: VPN logs and two-factor authentication logs.

While logs were being fed into an analytical tool, analysts could not run queries across time frames greater than 24 hours. Had the team been able to search across the months of data contained in a security information and event management (SIEM) system, they would have been able to develop long-term insight into emerging threats, as well as real-time access to security alerts generated by network hardware and applications. However, these systems and configurations were not in place when CrowdStrike initiated the investigation.

CrowdStrike worked with the team to identify how the attackers were abusing the organization's VPN and helped to implement a more manageable log collection and review process. With external access successfully blocked, and greatly improved network visibility, the organization was able to move quickly towards a successful coordinated remediation event.

TAKE-HOME **POINT:**

Having security technology is advantageous, but organizations will not be able to reap the full benefits until they are able to apply effective continuous monitoring capabilities across the enterprise. An overall security monitoring strategy should be driven by use cases that are developed with specific threat vectors in mind.

RECOMMENDATIONS

In an age where information is the ultimate currency, traditional strategies focused on malware, perimeter defense, detection of malicious websites and unpatched vulnerabilities are not nearly enough to get the job done

Instead, executives and officials in public, private and non-profit ORGANIZATIONS MUST CONSIDER THE FOLLOWING:

- Organizations must be able to self-detect system and network intrusions, evaluate weak points and implement tools to defend against emerging and enduring adversaries.
- Centralized processes, visibility, reporting, and leadership result in faster and more effective remediation.
- High-profile data breaches have become an all too common occurrence, and companies are stepping up their game in an effort to thwart those threats. In the past, organizations have relied in large part on defending the perimeter. Unfortunately, if the sole security focus is on defending assets by keeping attackers out, efforts become futile once attackers have breached the perimeter.
- Moreover, significant enterprise intrusions can no longer be seen as stand-alone events from a single adversary that are point-in-time events. Today, intrusions are the result of complex and constantly evolving attacks from a diverse community of adversaries who will return to the scene of the cybercrime repeatedly in concerted attempts to reinfect their targets.
- This emerging perspective on the threat landscape requires enterprise security teams to execute both proactive and reactive incident response strategies that are continuously engaged and more deeply vigilant to detect anomalous behaviors that may not be associated with known malware signatures.
- Organizations that have yet to experience a major incident should consider identifying and recruiting IT and security professionals that have successfully mitigated a major breach. Teams with strong subject matter expertise and experience in incident response can react faster and significantly mitigate damages.
- Comprehensive network and next generation endpoint detection, prevention and response tools provide maximum visibility to an organization. With this level of visibility, incidents can be quickly contained and attackers thwarted before significant losses occur. Enterprises can invert the traditional "watch and learn" incident response model, forcing adversaries to adapt, make mistakes, and ultimately fail in their objectives.

As is the case in most competitive situations, battles are often won and lost before any contact with adversaries. Exceptional performers were successful because of strong processes, well-trained teams already in place, capable host and network visibility, and a comprehensive understanding of risk management imperatives prior to experiencing attacks. By contrast, the investigations that struggled were hampered by poor strategy, communication, and non integrated platforms used to support an uncoordinated response to breaches.

In the pages that follow, we provide more detailed case studies of how organizations have dealt with the risks, threats and actual attacks that are rapidly becoming an ongoing reality of doing business in today's global digital business environment. Our hope is that knowledge of how others have successfully responded to attacks can help you improve your own defenses.

"Bad things can happen to anyone, but the damage can be contained if organizations have protocols in place to restore the confidentiality, availability and integrity of systems and networks."

PENETRATION TESTS AND RECOMMENDATIONS HIGHLIGHT PRESSING PRIORITIES FOR GLOBAL HEALTHCARE INDUSTRY
(CASE STUDY 3)

DETAILED CASE STUDIES

1

TECHNOLOGY ORGANIZATION BATTLES TARGETED ATTACKS

The global technology market is growing rapidly, wit Forrester projecting 6.3 percent growth in 2016, following gains of 4.1 percent in 2015. The U.S. market is expected to set the pace and market opportunities are being pursued aggressively by private and state-owned companies around the world. For certain nations with governments that are looking to advance their manufacturing objectives — while shoring up their military capabilities — technology companies represent an important target for espionage.

THE CLIENT

The organization — a leader within its industry — is grappling with fierce competition from rivals both inside and outside the United States. They posted annual revenues in the billions of dollars in 2014 and had thousands of hosts within the environment. Beginning in 2014, the organization became increasingly aware of — and concerned about — the threats posed by nation-state adversaries interested in stealing intellectual property for industrial espionage purposes.

SITUATION ANALYSIS

In the aftermath of a data breach of another organization in its industry, this organization called CrowdStrike to ensure its systems and networks were protected.

While the organization had a nimble and capable information technology organization, executives decided to augment their team with outside consultants to increase the bandwidth of their security team and help focus their efforts on threats from sophisticated adversaries.

THE CROWDSTRIKE PROCESS

CrowdStrike performed a compromise assessment on the organization's network to determine whether it was currently compromised, or showed evidence of past compromise.

During the assessment, CrowdStrike's endpoint monitoring sensors reported alerts indicating preliminary attacker activity. CrowdStrike initiated an incident response investigation by augmenting the security team, providing subject matter expertise, and guiding the investigation.

The attackers initially targeted email servers, attempting to retrieve messages from a number of key people in the organization, including senior engineers and the organization's chief technology officer. The adversary also targeted the information security staff's email, and attempted to place malware onto their laptops.

It became clear that the attacking team was specifically looking to obtain engineering data. They also sought opportunities to monitor what the security staff knew about the attack, and what action was being taken in response to the intrusion.

With a host-based sensor already in place, the organization was provided with comprehensive and real-time visibility into adversary activity on every endpoint. Falcon sensors were able to immediately and continuously detect and prevent attacker actions rather than relying on periodic 'sweeps and scans' of the environment that focused on detecting compromise after a breach had already occurred.

Simultaneously, CrowdStrike worked with the organization to design and implement a detailed remediation plan,

1 (CONT'D)

which included updates to network architecture. Near real-time visibility afforded by host and network sensors allowed rapid identification of where and how the attackers were accessing the enterprise environment. For example, CrowdStrike identified multiple attempts to install back doors on employee laptops. Excellent visibility afforded the ability to immediately block the installation of the back doors without losing track of additional and subsequent attacker activity.

Analysts determined that the attackers were exploiting the organization's virtual private network (VPN), as well as accessing a Microsoft Outlook Web Access (OWA) portal, both of which were using single-factor authentication. Previously established processes and working relationships between teams forged during the initial compromise assessment allowed the organization to move exceptionally fast. The addition of two-factor authentication on the VPN was implemented in only two days.

Implementing two-factor authentication for the globally distributed OWA required more effort, so the decision was made to disable OWA as a stopgap measure — requiring remote users to access all email via the now-well-protected VPN — until two-factor authentication could be implemented for the OWA environment.

After successfully mitigating attacker access, CrowdStrike technology continued to monitor the organization. Months later, the attackers attempted to return, exploiting a similar vector — a different web application — to access an Internet-facing system not protected by an endpoint sensor. The attacker used credentials obtained from this system to attempt to move laterally and dump credentials on another system. At this point, the CrowdStrike endpoint monitoring solution detected and prevented the attacker's attempts to dump credentials. This detection alerted the security team of the initial compromised system, allowing them to mitigate access to that system and remediate it, thereby preventing a larger compromise.

Because the client now had experience detecting and responding to attacks — and had developed a stronger response playbook that included detection and response as part of their daily procedures — the entire team moved with much greater agility to respond to the new intrusion. The incident was quickly analyzed and mitigating actions were taken to prevent the new tactics, techniques, and procedures (TTPs) from being successful. As a result, the compromise was fully mitigated in less than one hour.

RESULTS AND OUTCOMES

- During the initial attack, adversaries appeared to be primarily interested in emails, as well as data related to the layout of the newtwork. This is an indication that the attackers were preparing for a long stay, and were seeking ways to evade defenders. In this case, however, the adversaries were completely ejected from the network within two weeks. The security team's enhanced visibility into infrastructure behavior prevented the swift reinfection.

- During a follow-up attack, adversaries demonstrated interest in the exact same information, but accelerated detection and response procedures now in place facilitated rapid remediation, preventing them from achieving actions on target. CrowdStrike was able to immediately mitigate the attackers' access and prevent their ability to successfully use new malware within the environment.

2

DEFENSE CONTRACTOR GAINS EDGE OVER NATION-STATE ATTACKS

Defense firms have long been viewed as attractive targets for cyber attacks, with defense contractors facing a growing number of compromise attempts. While large defense contractors often have a designated team to handle security, that is not always true for the smaller, more agile firms in the market who are introducing new, innovative solutions. In these cases, IT generalists often must "wear the security hat," juggling day-to-day enterprise technology management responsibilities while combatting determined adversaries that work around the clock to penetrate networks.

THE CLIENT

This case study features an organization that builds solutions for the defense and homeland security sectors. This organization's systems were targeted by a nation-state adversary attempting to obtain intellectual property.

SITUATION ANALYSIS

In early 2015, the organization was notified by the FBI of an attack in which a large amount of data was removed from the organization's network. The organization contacted CrowdStrike about the intrusion, and triage efforts began the same day.

Among the weapons commonly used by these adversaries were webshells. Webshells are back doors that provide malicious actors with unrestricted remote access to compromised web servers. In this case, both adversary groups identified were known to employ a variant of the webshell — called "China Chopper" — to gain control of the organizations' systems and network.

THE CROWDSTRIKE PROCESS

In order to immediately curtail further attacker access, CrowdStrike worked with the organization to increase host and network visibility in the enterprise, while also moving quickly to re-architect the organization's credential management program.

With upgraded visibility, investigators focused on two time-critical objectives:

- Determine what the attackers are currently doing and how they are doing it in order to mitigate access to the environment
- Determine what has previously happened in the environment and whether any of the activity requires legal or regulatory compliance and/or disclosure

Real-time visibility at the endpoints allowed the defense contractor to detect attacker activity as it occurred — rather than rely on intermittent audits that identify intrusions after systems are already compromised — greatly accelerating the response process.

Analysts quickly identified the presence of heavily used webshells on two systems, which were introduced via the insertion a single line of code within legitimate ASPX pages.

2 (CONT'D)

Investigators were able to determine that attackers had maintained undetected access to the organization's network for years. Eventually, dozens of pieces of malware and utilities used by the attackers were identified. At the culmination of the investigation, hundreds of instances of data theft were identified, much of which occurred during the year prior to notification.

With good visibility and a plan in place, the defense contractor worked with CrowdStrike to implement a comprehensive remediation effort within days of the investigation's launch.

The timing for initiating the remediation activity was strategic: the effort took advantage of a holiday period that traditionally has been a downtime period for that specific group of nation-state adversaries.

Two days later, multiple attempts were made by attackers to regain access to the environment using invalid credentials and now non-existent webshells. Host and network-based detection facilitated the remediation of multiple new webshells and compromised credentials in less than an hour.

WEBSHELLS

Similar to other backdoors, a webshell enables attackers to gain access to a virtual terminal from which they can execute commands or upload and download files. Most often found on Internet-facing web servers, they can be implemented as standalone files or as a single line of code inserted into existing pages on the server. Depending on the adversary, they may be used as a primary means of access to the network, or as a backup to be used in the case of full remediation efforts. Due to their simplicity and diversity, webshells often easily evade anti-virus and application whitelisting solutions.

RESULTS AND OUTCOMES

- CrowdStrike worked with the defense contractor to conduct a thorough investigation, remediate the incident, and fully mitigate any attempts by attackers to re-compromise the networks. The accelerated pace of this approach allowed the entire incident response effort to be completed in four weeks.
- CrowdStrike and the organization developed a strategic remediation plan that was executed in less than two weeks. The organization used the new visibility into the enterprise to validate the successful remediation efforts – and to immediately stop repeated subsequent attempts by attackers to regain a foothold.
- Subsequent to the initial remediation effort, the attackers attempted to deploy two new webshells. Not only did endpoint detection alert and disrupt every new attempt at reinfection, newly installed webshells were mitigated and contained.

3

PENETRATION TESTS AND RECOMMENDATIONS HIGHLIGHT PRESSING PRIORITIES FOR GLOBAL HEALTHCARE INDUSTRY

With a treasure trove of medical records, including personally identifiable information (PII) — such as social security numbers and a fast-track menu of connected health devices — it comes as no surprise that the $2.9 trillion healthcare market increasingly is under siege by cybercriminals. It explains why 87 percent of respondents to a 2015 Health Information Management Society (HIMSS) survey reported that cyber security has become a higher priority issue over the past 12 months.

Given the magnitude of the threat and the the target-rich environment, a growing number of organizations in the healthcare industry are being advised to conduct in-depth penetration tests.

THE CLIENT

In this case study, we see how a large healthcare organization proactively identified and addressed potential threats. Executives at the organization wanted to identify any potential vulnerabilities in their own network, and selected CrowdStrike to conduct a thorough series of internal penetration tests to discover potential problems.

SITUATION ANALYSIS

The primary goals of the penetration tests were to independently verify whether the organization's systems and networks were vulnerable, and assess their ability to identify and respond to a targeted attack. The organization also wanted to know what it needed to do moving forward to optimize its security capabilities.

CrowdStrike's penetration testers employed tactics to emulate the actions of adversaries most likely to target the organization. The team crafted attacks and behaviors likely to be employed by typical attackers in this vertical. A plan was designed to:

- Test the organization's current defenses and their ability to detect attacks
- Improve their capability to detect and defend against potential attacks in the future

CrowdStrike applied insights from its most current threat intelligence reports and implemented techniques that regularly thwart forensic and other detection technologies. A wide variety of tradecraft was identified and incorporated into the test plan.

3 (CONT'D)

THE CROWDSTRIKE PROCESS

CrowdStrike launched the penetration test by establishing an initial foothold via a spear phish attack using a Java exploit for a vulnerability on the healthcare organization's internal systems that had not been patched. This simulated the ability of advanced adversaries to weaponize payloads to evade perimeter defenses providing a high success rate of subsequent exploitation.

Testers executed a custom remote access tool (RAT) on the compromised system and commenced information gathering. Interestingly, the penetration test team was able to exploit a weakness in a running service that had been configured to use Domain Administrator credentials. This particular service was present on a significant percentage of systems in the network, unnecessarily exposing some of the most valuable credentials to broad risk.

With elevated privileges, the team initiated lateral movement, including the installation of several Sticky Keys exploits — often employed by adversaries. A Sticky Keys attack requires only a simple registry or file change and greatly facilitates Windows remote desktop lateral movement by providing system-level privileges while leaving no log records. It also offers adversaries the ability to survive a full organizational password reset.

Next, the penetration test team simulated the dumping of the active directory database from domain controllers, and set up multiple command and control infrastructures designed to test various defenses, including use of a custom covert messaging protocol. In this network, outbound connections were restricted by perimeter devices and web gateways, forcing the pentest team to adapt to a hostile environment.

The team ultimately gained access to a large amount of sensitive data including contracts, employee and customer records, and healthcare data. Throughout the engagement, the healthcare organization was updated on milestones achieved and given the opportunity to help direct activity to better defended critical assets.

At the conclusion of the test, CrowdStrike recommended a number of improvements to the client's systems, networks, and policies. While the organization had a very capable security operations center (SOC) and internal processes, additional recommendations were made to improve monitoring for anomalous network traffic, harden workstations, and better limit access to key infrastructure. Specific recommendations applicable to a wide range of organizations includes the following:

IOAs

The use of Indicators of Compromise (IOCs) has been the traditional focus of endpoint detection, but modern adversaries have adapted to more easily evade IOC sweeps. The differences between IOC and Indicators of Attack (IOA) are important to note. In a forensics investigation, IOCs essentially represent evidence that proves the network's security has been breached. Unfortunately, by the time the IOC has been discovered, the network likely has been compromised. Conversely, IOAs reflect a series of actions the attacker must perform in order to be successful. They are a set of actions that are required for any tool or technique to accomplish common attacker behaviors like code execution, persistence, command and control, and lateral movement.

A proper IOA approach not only can collect and analyze exactly what is happening on the organization's systems and networks, it can do so in real time and even prevent the action from being succesful.

3 (CONT'D)

- **Ongoing and Evolving Penetration Testing.** The penetration test revealed significant vulnerabilities that potentially placed the organization at risk. Further testing was recommended to validate all new and updated applications. This is particularly important in the case of "homegrown" software and apps, which are prime targets for attackers, even when servers have been patched.

- **Monitoring and Consolidating All Internet Connections.** The penetration test exploited the fact that the organization had a fragmented set of ingress and egress points for data. Monitoring egress points helps identify data that is leaving the network — an essential tool in identifying hacking attempts and for intercepting sensitive data that may be on the way out of the organization.

- **Identify, Segregate and Prioritize Logging of Critical Data.** This limits risk to mission-critical data and allows organizations to apply more resources to assets that are most important, from a business and compliance perspective. Organizations must identify their most sensitive data or network segments and increase security monitoring to mitigate rapid changes in the current threat environment.

- **Centralize Logging.** This is a measure that can be leveraged to quickly detect and act on anomalous behavior. A centralized log repository should be indexed and searchable and contain information from various sources that can be used to establish facts about how users have interacted with network hosts and services. A logging strategy should be driven by use cases and could include the following sources, among others: Active Directory/LDAP Authentication, DNS DHCP, NetFlow, Proxy/Firewall, VPN Session Authentication

- **Patch Operating Systems and Third-Party Applications.** Effective — and fast — patch management is one of the easiest and cheapest ways to eliminate vulnerabilities.

- **Use Active Directory to Tightly Control — Or Remove — Administrator Privileges on Local Workstations.** Attackers have a great propensity for launching attacks via local admin accounts, because once they compromise a local workstation, they can move laterally through the system and access (or alter) other credentials. Putting in place a tiered Active Directory architecture can isolate credentials and minimize potential damage if an account has been compromised.

- **Be Proactive by Designing Incident Response Plans Before They Are Needed.** Bad things can happen to anyone, but the damage can be contained if organizations have protocols in place to restore the confidentiality, availability and integrity of systems and networks.

- **Have an External Communications Plan.** Healthcare companies must comply with federal laws about when PHI has been compromised. Planning the process for informing clients, law enforcement, investors and other key constituents about a data breach is a top priority for all entities in the healthcare vertical.

RESULTS AND OUTCOMES

- By applying a structured penetration testing methodology focused on the type of attacks that specific adversaries would execute, CrowdStrike was able to prove that a broad range of data on the healthcare company's system was vulnerable and work with them to mitigate these risks prior to an attack .

- The client was able to use the results of the test to spur enterprise-wide updates to their infrastructure and processes. Recommendations were prioritized and internal teams were formed to address critical threats immediately.

ABOUT **CROWDSTRIKE**

CrowdStrike is the leader in next-generation endpoint protection, threat intelligence and response services. CrowdStrike's core technology, the Falcon platform, stops breaches by preventing and responding to all types of attacks – both malware and malware-free. CrowdStrike has revolutionized endpoint protection by combining three crucial elements: next-generation AV, endpoint detection and response (EDR), and a 24/7 managed hunting service — all powered by intelligence and uniquely delivered via the cloud in a single integrated solution.

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 incident response (IR) team helps customers around the world identify, track and block attackers in near-real time. This unique approach allows CrowdStrike to curtail unauthorized access faster, so customers can resume normal operations sooner. CrowdStrike's IR consultants also offer proactive services to improve organizations' ability to anticipate threats, prepare their networks, and ultimately prevent damage from cyber attacks.

EXPERIENCED A BREACH?
Call 855.276.9347 or
email services@crowdstrike.com

CROWDSTRIKE

WWW.CROWDSTRIKE.COM