KNIGHTINK

ISOLATED CASTLES:
INCIDENT RESPONSE IN THE NEW WORK FROM HOME ECONOMY

It can no longer be a topic of debate. If you have enterprise assets connected to the Internet, you will get breached. It is only just a matter of when. Every organization, especially in today's work-from-home economy must have a documented incident response plan and sets of playbooks that form the incident response procedure.

Summary

This paper discusses the challenges for incident handlers to respond to breaches in the new work-from-home economy and what tactics, techniques, and tools can be used to respond to incidents, including those affecting workloads in the cloud.

Author Information

Alissa Valentina Knight
Partner
Knight Ink
1980 Festival Plaza Drive
Suite 300
Las Vegas, NV 89135
ak@knightinkmedia.com

Publication Information

This white paper is sponsored by Tanium, Inc.

Initial Date of Publication:
March 2021
Revision: 0.1

TABLE OF CONTENTS

TABLE OF CONTENTS

KEY POINTS

- Today's Chief Information Security Officer (CISO) faces a number of challenges, including the realization that it is no longer a question if they will be breached, but when.

- Prevention is no longer achievable; thus, focus has shifted to lowering the mean-time-to-detection (MTTD) and mean-time-to-response (MTTR).

- CISOs are now ensuring that the environment is collecting as much forensic data as possible that will best inform the incident response and digital forensics effort when the IR process is initiated.

- Nothing inside or outside the perimeter should be trusted; users and devices should be authenticated, authorized, determined based on who, what, when, and even where a user or device is from and what it is trying to access.

- The concept of zero-trust (ZT) security effectively erases the castle approach to security architecture in that the "castle has left the moat" with data now being everywhere.

- Data is no longer behind the defenses of a network perimeter but instead extends to mobile devices, cloud drives, and cloud servers. The threat to those assets are everywhere, everyone, and everything.

- Exacerbating digital forensics in the new work-from-home economy are cloud workloads, cloud drives, and software-as-a-service, with each cloud service provider (CSP) having its own idiosyncratic methods in what IR functions are supported and what cloud technologies can support the creation of forensic data that can help in a breach.

- In a recent study performed by Netwrix, insider threat concerns with CISOs are at the highest they have ever been with 85% of respondents saying they sidestepped existing cybersecurity controls in their security posture in order to support their entire workforces working from home. Of that 85%, 58% believe that user behavior changes in their work-from-home environment will create a risk to corporate data by ignoring previous rules they followed at their desk in the office. [1]

- In 2019 B.P. (Before Pandemic), incident response handlers enjoyed much simpler times. When a machine was potentially compromised or an employee investigation was being performed by Human Resources, they could simply walk up to the machine and grab a full or logical acquisition of the disks and whatever is sitting in volatile memory. Today, if remote acquisition is not possible, systems are being shut down and physically shipped to the forensic examiner, losing whatever forensic data may lie in volatile memory.

- When a user working from home has been breached and their laptop used as a beachhead by the adversary to pivot laterally into the internal network, the system would need to be shipped to the forensic examiner to have either a full or logical acquisition performed of the drive. In most cases, this would require the system to be powered off before shipping. The acquisition could be performed remotely, but a full acquisition of a 1 TB hard drive over a home DSL or cable connection could take an unreasonable amount of time as it is uploaded to the cloud.

- When companies architect their cloud migration and digital transformation strategy, they should always consider the incident response and forensics steps that will need to be taken and what forensic data will be available to them in the event of a breach.

- Hunting for artifacts when you have a specimen, such as a malicious binary and corresponding hashes of malicious files, is a crucial capability for any unified endpoint security solution required by an incident handler.

- Asset cataloging along with patch management ensures that assets are identified and deviations from secure baselines and patched vulnerabilities introducing critical and unacceptable risk to the business is properly managed.

- The most important requirement of any incident handler is access to forensic data for analysis, inclusive of both network and endpoint security events and logs. In today's distributed environment where company assets are sitting in employees' homes, it is important that incident handlers have access to an endpoint security solution capable of pulling needed forensic data off an endpoint.

- When an asset has been determined to be compromised, it must be immediately isolated or micro-segmented from other enterprise assets to prevent further lateral movement by adversaries and malware. Being able to quickly and automatically isolate hosts based on indicators of compromise (IOCs) is a critical feature of any endpoint security solution.

- In today's work-from-home economy, companies should have a documented incident response plan and set of playbooks that form the incident response procedure. Beyond this, every organization should have a unified endpoint security solution capable of blending asset management, patch management, and security and response capabilities.

INTRODUCTION

Over 117 million people worldwide have contracted COVID-19 while the number of exposed records as a result of cyber breaches by the end of September 2020 alone reached a staggering 36 billion -- the worst year on record. While 2020 will undoubtedly be known in the annals of history for the COVID-19 pandemic, it will also be known for the cybersecurity breaches that made front-page news. Not only did 2020 breaches include ransomware payouts that caused Telex to file bankruptcy after it paid out a whopping $2.3 Mn in ransom and the first-ever death of a patient directly attributed to a cybersecurity incident in Germany, but also it included state-sponsored hacks that followed the U.S. presidential election affecting FireEye, Solar Winds, and numerous government agencies including the U.S. Treasury.

Whatever the number of cybersecurity breaches and their severities that affected 2020, the challenges of the incident response effort is rarely, if ever, covered in news stories. This paper attempts to demystify these challenges now exacerbated by a new shelter-in-place economy where an organization's assets are at employees' homes, servers are in the cloud, and very little is left on-prem. Before diving into incident response and forensics in this new scattered enterprise, I will first explain the concept of zero-trust (ZT) security, which replaces the old "castle and moat" security architecture of enterprise networks that this new enterprise home office fits perfectly within.

Today's Chief Information Security Officer (CISO) faces a number of challenges, including the realization that it is no longer a question of if they will be breached, but when. Prevention is no longer achievable; thus, focus has shifted to lowering the mean-time-to-detection (MTTD) and mean-time-to-response (MTTR) instead. CISOs are now more focused on ensuring that the environment is collecting as much forensic data as possible that will best inform the incident response and digital forensics effort when the IR process is initiated.

This paper is written for CISOs and cybersecurity engineers wanting to better understand the challenges introduced by breaches where assets involved in the breach are sitting in employees' homes and how to instrument the new scattered enterprise with the tools that support the incident response effort.


KNIGHTINK

DEMYSTIFYING ZERO TRUST

It was 2010 when John Kindervag, then an analyst with Forrester Research, first wrote about the idea of a zero-trust (ZT) security framework in which the idea of a network edge or perimeter was no longer the front lines of the cyber battlefield for an organization.

Instead of an organization implicitly trusting anything inside its perimeter, ZT described a new concept that nothing inside or outside the perimeter should be trusted. It further required that both users and devices should be authenticated and authorized based on who, what, when, and even where a user or device is from and what it is trying to access. The idea was that anything and everything should be scrutinized.

The concept of zero-trust (ZT) security effectively erases the castle approach to security architecture in that the castle and moat have now turned into a distant memory with data now being everywhere -- no longer behind the defenses of a network perimeter. Instead, enterprise data now extends to mobile devices, cloud drives, cloud workloads and the threat to those assets are everywhere, everyone, and everything.

This approach to cybersecurity implements an inside-out mentality of protecting the organization's most critical assets where security is designed as "micro-perimeters" around the assets being protected. It's now being realized that the "barbarians" are already inside the gate.

ZT could never be a more relevant concept to security architecture than it is now in this new scattered enterprise with user laptops in employees' home networks, servers in the cloud, and third-party suppliers with access into intranet applications and data.

ZERO TRUST: USERS

Security organizations need to decouple the individual whom they trust from the user account they have been assigned.

Essentially, you might be able to trust the individual, but you cannot trust that individual's user account when it is logging into the environment and that it is indeed the person it was assigned to.

The concept of zero-trust for users is that every interactive login and every service account login should be authenticated and authorized. Simply put, just because someone is logging into a device because they have a user account in the active directory domain, it does not necessarily mean it is them and that they should be authorized to even do so. Most importantly, once a user account is authenticated and authorized, they should continue to be authenticated and authorized depending on the resources they are requesting over the duration of their connection to the environment.

In a recent study performed by Netwrix, insider threat concerns with CISOs are at the highest they have ever been with 85% of respondents saying they sidestepped existing cybersecurity controls in their security posture in order to support their entire workforces working from home. Of the 85%, 58% believe that user behavior changes in their work-from-home environment will create a risk to corporate data by ignoring previous rules they followed at their desk in the office. [1]

ZERO TRUST: NETWORKS

ZT security models were being adopted by organizations well before the COVID-19 pandemic. Those who did had a head start over other CISOs with employees' home networks clearly being an untrusted environment.

With many organizations, the enterprise VPN infrastructure was never scoped out to support 100% of the entire workforce from bandwidth utilization and license limitations. Therefore, many organizations quickly deployed RDP servers that faced the internet in order for employees to remote in to access intranet servers and data. However, this created even more concerns over the trustworthiness of employees' home networks and the systems they remoted in since many organizations didn't have a sufficient number of laptops to issue to every single employee.

The threat of the corporate intranet being infected by malware such as ransomware because an employee remoted in from a machine that was infected with ransomware on their home network quickly became an increasing concern. A majority of home users typically don't have the network and endpoint security controls enjoyed from a large cybersecurity budget in an office.


KNIGHTINK

2019 B.P.

INCIDENT RESPONSE

In 2019 B.P. (Before Pandemic), incident handlers enjoyed much simpler times. When a machine was potentially compromised or an employee investigation was being performed by human resources, they could simply walk up to the machine and image it to grab a raw copy of the disks and whatever is sitting in volatile memory. Today, if remote acquisition is not possible, systems are being shut down and physically shipped to the forensic examiner, losing whatever forensic data may lie in volatile memory.

Exacerbating digital forensics in the new work-from-home economy are cloud workloads, cloud drives, and software-as-a-service, with each cloud service provider (CSP) having its own idiosyncratic methods in what IR functions are supported and what cloud technologies can support the creation of forensic data that can help in a breach.

All CSPs operate off a shared responsibility model, meaning the CSP is responsible for security of the cloud while customers are responsible for security inside the cloud. Some CSPs do not provide log data to customers in a breach because of the multitenant nature of cloud services. There have been multiple incident response events I have handled where much of the log data was not accessible because the CSP refused to provide it. These are all pre-sales questions that must be considered and asked of the CSP prior to deciding on a provider. This most often occurs with the smaller versus larger CSPs.

INCIDENT RESPONSE TO REMOTE WORKERS

As a result of companies not having the infrastructure, VPN licenses, and laptops available to issue to an entire workforce moving to remote work, companies had to support the mass exodus to home networks overnight. Due to an infrastructure that could not support the bandwidth and licenses required by all the concurrent VPN sessions from remote users, companies had to quickly implement stop-gaps which came in the form of Remote Desktop Protocol (RDP) servers. These RDP servers face the internet offering unencrypted, remote access into the intranet from anywhere. Unfortunately, while this made it possible for the entire workforce to access intranet resources, it also increased the company's attack surface and operational risk.

Home users certainly do not have the same cybersecurity budget their employers have to secure their home network and endpoints. Many home networks even have default administrator passwords on their home routers and Wi-Fi access points. Due to the lack of security controls, adversaries quickly turned their attention to the home user. The lack of network security controls include interdiction of network traffic that most adversaries would have to contend with when they have established a beachhead on a corporate network.

Additionally, home users also do not typically have the same network and endpoint security controls in place enjoyed on corporate networks. These include network intrusion detection and prevention systems, filtering to check for drive-by-downloads from hijacked web sites, and endpoint detection and response (EDR) agents.

Many companies also have been dealing with a shortage of laptops having to allow employees to use their own home workstations to remote into the network using RDP or VPN. This created an ingress point where an adversary could hop into the corporate network through this remote connection, either because of VPN split tunneling or simply over RDP.

Since the start of the pandemic, the sites, and endpoint detection and response (EDR) agents.

United Nations (UN) reported a 350% increase in the number of phishing sites created [8].

When a home system has been breached and used as a beachhead by the adversary to pivot laterally into the internal network, the system, if a company-issued laptop, would need to be shipped to the forensic examiner. The examiner would the full or logical acquisition of the drive, which would in most cases require the system to be powered off before shipping. The acquisition could be performed remotely, but a full acquisition of a 1 TB hard drive over a home DSL or cable connection could take an unreasonable amount of time for the image to be uploaded to a cloud drive.

Furthermore, if the laptop is shipped to the examiner, this undoubtedly creates a new concern over downtime for the employee, their home system having to be used for company work until a new one is shipped out, and a question as to whether or not any other assets on the user's home network have also been compromised in the breach. If the laptop needs to be shipped to the examiner, the examiner loses the ability to perform an acquisition of forensic data sitting in volatile memory when the system is powered down.

INCIDENT RESPONSE TO CLOUD WORKLOADS

Incident response of workloads or cloud drives sitting in CSPs can also be a challenge for incident handlers. Certainly, the tools needed to perform acquisitions of cloud drives, such as Box, Dropbox, or AWS S3 buckets are needed. The ability to shut a workload down and ship it to an examiner is of course not an option with CSPs.

When an organization chooses a CSP outside of the larger CSPs, they also run the risk of not being allowed access to important forensic data, such as event logs or alerts because of the nature of some CSPs and multi-tenant environments. This multi-tenancy has been an issue in many IR investigations I have handled where some of the smaller CSPs simply would not cooperate with me in providing the needed evidence or logs in order to fully investigate the event. Some CSPs will also prevent the acquisition of a drive depending on the type of server the company is hosting on.

When companies architect their cloud migration and digital transformation strategy, they should always consider the incident response and forensics steps that will need to be taken and what forensic data will be available to them in the event of a breach. Instead of planning for how to prevent it in the first place, CISOs who now realize it is not a question of “if” but “when” a breach occurs, must instead plan for the breach and what will be available to them in the response effort.

Beyond the importance of having predefined IR playbooks and regularly performing incident response tabletop exercises, it is important to know what technologies offered by your CSP can provide needed forensic data in an incident response effort.

Different CSPs offer different cloud technologies to support investigation efforts in a breach. Some of those technologies, whether at the network or endpoint level are described in further detail below for two of the major CSPs, that CISOs need to consider.

INCIDENT RESPONSE IN AWS

AWS has published numerous white papers for customers to consider when architecting their cloud environments in AWS and what to consider in the event of a breach. The most beneficial paper was recently published in 2020, AWS Security Incident Response [4].

AWS describes three separate domains in its shared responsibility model where customers will be responsible for response and containment. These are the service domain, where incidents affect the AWS account itself; IAM permissions; resource metadata; billing; and other areas of the AWS account administration.

"Responses to breaches of the AWS service domain are handled exclusively with AWS APIs, have root causes associated with your configuration or resource permissions, and might have related service-oriented logging" (AWS Incident Response, 2020). Much of the forensic data to consider here depends on the AWS service. For example, if an S3 bucket data disclosure occurs, review of the S3 bucket policy, S3 access logs, and potentially AWS CloudTrail logs would be in order.

Breaches occurring within the infrastructure domain directly affect data or network activity to/from resources within your cloud environment, such as traffic to/from EC2 instances or S3 buckets. Response actions by the incident handler often will include operating system (OS)-level interactions of the EC2 instances or containers and potentially AWS APIs.

Finally, incidents impacting applications installed within AWS cloud resources, affect source code, and will include much of the same techniques and tools used in the infrastructure domain that include tools now supporting cloud forensics and recovery options. Breaches in the infrastructure domain would include the use of familiar incident response and forensic tools that support cloud acquisitions, analysis of network capture files (PCAPs), or disk blocks on Amazon Elastic Block Store (Amazon EBS) volumes.

It is important in AWS to know what security tools are available to you natively within the environment, such as Amazon S3 access logs, Amazon CloudTrail, AWS logs, VPC flow logs, and security monitoring services, such as Amazon GuardDuty, Amazon Detective, AWS Security Hub, and Amazon Macie.

For a more holistic, global view of all of your prioritized security alerts and compliance status across your entire AWS cloud of AWS services, consider using AWS Security Hub.

INCIDENT RESPONSE IN AZURE

Microsoft Azure offers a number of capabilities to generate security events that can then be sent automatically to its security information and event management (SIEM) solution it offers -- Microsoft Sentinel. Sentinel is far more than just a SIEM, and includes security orchestration, automation, and response (SOAR) as well as the ability to bring in threat intelligence feeds and perform threat hunting.

Azure Security Center (ASC) allows for the configuration of logs and other security events to be generated and sent automatically using the ASC connector to Azure Sentinel where they can be automatically turned into tickets for further investigation.

Both network and endpoint logs and telemetry data can be captured within the Azure cloud. To collect network telemetry, network security groups provide the ability to capture flow logs. Azure Network Watcher as well as Azure Monitor can also collect network telemetry data for analysis in a breach.

2020 A.P.

INCIDENT RESPONSE

2020 AFTER PANDEMIC (A.P.) INCIDENT RESPONSE

Incident response playbooks must be adapted to this new work-from-home (WFH) enterprise where many companies are staying in a permanent state of WFH for all employees that will require existing IR playbooks, policies, and procedures to be updated.

While the network infrastructure will change wherever endpoints are moved to, whether in the corporate intranet, to the employee's home, or to CSPs, what will always remain a constant is the endpoint itself. This is why having an endpoint detection and response (EDR) solution capable of disparate hunting of artifacts, asset identification and management, generating and pulling the necessary forensic data off the endpoint, and the capability to isolate the host while forensics is performed is critical to any solution.

Afterall, you cannot protect, and you cannot respond to assets you do not know you have.

Combining endpoint management with endpoint security capabilities provides the CISO eyes and ears across all assets on-prem, in the cloud, and to employee homes that allows her to keep mean-time-to-detection (MTTD) and mean-time-to-response (MTTR) low.

ARTIFACT HUNTING

Hunting for artifacts when you have a specimen, such as a malicious binary and corresponding hashes of malicious files is a crucial capability for any unified endpoint security solution that requires zero infrastructure is important.

In a breach, backdoors, ransomware, and other malicious software (malware) will be discovered by incident handlers. Having an EDR in place capable of searching every asset, whether on-prem, at employee homes, or in the cloud for specific hashes of those discovered artifacts is crucial to the success of the incident response effort in order to find every host involved in the compromise. These artifacts identify the lateral movement of the adversaries after the initial beachhead is established.

In every breach, adversaries will establish a command-and-control (c2) connection allowing the adversaries to regain access to the target network using software that “phones home” to predefined C2 servers on the Internet. This is essential to understand the full breadth of the breach and to determine what, if any, data may have been accessed by the adversaries based on where malware is discovered. When an EDR agent is deployed on every single endpoint, artifacts can be searched for globally and sent back to the incident handler for further analysis.

ASSET MANAGEMENT

No distributed environment can be secured when the attack surface is not fully mapped out and understood. In order to secure assets, you need to know what assets you have. Asset management is critical in an EDR capability, ensuring that the business can continuously maintain and update the asset management system as assets are added or removed from the environment. Combining asset management with detection and response capabilities ensures that all potential ingress points are identified.

Asset cataloging along with patch management ensures that not only assets are identified but deviations from secure baselines and patched vulnerabilities introducing critical and unacceptable risk to the business on endpoints is properly managed.

COLLECTION OF FORENSIC DATA

The most important requirement of any incident handler is access to forensic data for analysis, inclusive of both network and endpoint security events and logs. In today's distributed environment where company assets are sitting in employees' homes, it is important that incident handlers have access to an endpoint security solution capable of pulling needed forensic data from an endpoint.

Forensic data from endpoints should include logs from Syslog on *nix-based systems, logs from Windows Event Log on Microsoft Windows-based systems, and logs from network devices, such as routers and switches.

Of course, events and alarms from security information and event management (SIEM), network detection and response (NDR), and EDR events complete the picture that the forensic analyst must analyze and interpret data from in order to answer the who, what, where, when, why, and how questions expected as an outcome to a breach.

ASSET ISOLATION

When an asset has been determined to be compromised, it must be immediately isolated or micro-segmented from other enterprise assets to prevent further lateral movement by adversaries and malware. Being able to quickly and automatically isolate hosts based on indicators of compromise (IOCs) is a critical feature of any endpoint security solution.

Incident handlers will want to isolate hosts so the tedious task of imaging the drives and volatile memory of the host can be performed without worrying about further compromise.


KNIGHTINK

CONCLUSION

AUTHOR'S FINAL
THOUGHTS

CONCLUSION

If you have enterprise assets connected to the Internet, you will get breached -- it is only just a matter of when. Every organization, especially in today's work-from-home economy, must have a documented incident response plan and sets of playbooks that form the incident response procedure. Beyond this, every organization should have a unified endpoint security solution capable of blending asset management, patch management, and security and response capabilities.

The biggest concern incident handlers have when walking into an incident response scenario is the availability of forensic data for analysis and how access will be facilitated to systems requiring a disk and volatile memory acquisition and where those systems are physically located.

When endpoints are spread across on-premises networks, cloud service providers, and employees' homes, an effective endpoint security solution enables the incident handler to acquire vital forensic data from endpoints remotely as well as empower them to quickly isolate a host that has been compromised. Therefore, it is critical to manage and contain the compromise so the businesses can respond to and recover from threats and breaches with near-instant speed, visibility, control, and at any scale.

SOURCES

[1] Muncaster, P. (2020, December 09). Insider cybersecurity risk soars during lockdownPP. Retrieved March 09, 2021, from https://www.infosecurity-magazine.com/news/insider-cybersecurity-risk-soars/

[2] Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August 06). Computer security incident handling guide. Retrieved March 09, 2021, from https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

[3] Amazon Web Services (n.d.). Incident Domains. Retrieved March 09, 2021, from https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/incident-domains.html

[4] Amazon Web Services (2020, June). AWS Security Incident Response Guide. Retrieved March 08, 2021, from https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf

[5] Amazon Web Services (n.d.). Best Practices for Security, Identity, & Compliance. Retrieved March 09, 2021, from https://aws.amazon.com/architecture/security-identity-compliance/?cards-all.sort-by=item.additionalFields.sortDate&cards-all.sort-order=desc

[6] Amazon Web Services (2016, August). AWS Security Best Practices. Retrieved March 08, 2021, from https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

[7] Amazon Web Services (2016, June). AWS Cloud Adoption Framework Security Perspective. Retrieved March 08, 2021, from https://d1.awsstatic.com/whitepapers/AWS_CAF_Security_Perspective.pdf

[8] Lederer, E. (2020, August 07). UN reports sharp increase in cybercrime during pandemic. Retrieved March 09, 2021, from https://apnews.com/article/virus-outbreak-counterterrorism-health-crime-phishing-824b3e8cd5002fe238fb9cbd99115bca

[9] Msmbaldwin. (n.d.). Azure security benchmark v2 - incident response. Retrieved March 09, 2021, from https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-incident-response


KNIGHTINK

ABOUT THE AUTHOR

Alissa Knight is a partner at Knight Ink and blends influencer marketing, content creation in writing and video production, go-to market strategies, and strategic planning for telling brand stories at scale in cybersecurity.

She achieves this through ideation to execution of content strategy, storytelling, and execution of influencer marketing strategies that take cybersecurity buyers through a brand's custom curated journey to attract and retain them as long-term partners.

Alissa is a published author, having published the first book on hacking connected cars and am working on a new series of books into hacking and securing APIs and microservices.

ABOUT KNIGHT INK

Firm Overview
Knight Ink is a content strategy, creation, and influencer marketing agency founded for category leaders and challenger brands in cybersecurity to fill current gaps in content and community management. We help vendors create and distribute their stories to the market in the form of written and visual storytelling drawn from 20+ years of experience working with global brands in cybersecurity. Knight Ink balances pragmatism with thought leadership and community management that amplifies a brand's reach, breeds customer delight and loyalty, and delivers creative experiences in written and visual content in cybersecurity.

Amid a sea of monotony, we help cybersecurity vendors unfurl, ascertain, and unfetter truly distinct positioning that drives accretive growth through amplified reach and customer loyalty using written and visual experiences.

Knight Ink delivers written and visual content through a blue ocean strategy tailored to specific brands. Whether it's a firewall, network threat analytics solutions, endpoint detection and response, or any other technology, every brand must swim out of a red sea of competition clawing at each other for market share using commoditized features. We help our clients navigate to blue ocean where the lowest price or most features don't matter.

We work with our customers to create a content strategy built around their blue ocean then perform the tactical steps necessary to execute on that strategy through the creation of written and visual content assets unique to the company and its story for the individual customer personas created in the strategy setting.

Contact Us
Web: www.knightinkmedia.com
Phone: (702) 637-8297
Address: 1980 Festival Plaza Drive, Suite 300, Las Vegas, NV 89135

Knight Ink
1980 Festival Plaza Drive
Suite 300
Las Vegas, NV 89135
ak@knightinkmedia.com