RSA Conference 2019

BETTER.

LEARNING LABS

Verizon Incident Preparedness Workshop

Chris Novak

Director | VTRAC – Global

John Grim

Managing Principal | VTRAC – Americas

Eric Gentry

Managing Principal | VTRAC – RRR

Ashish Thapar

Managing Principal | VTRAC – APJ

Table of Contents

Verizon Incident Preparedness Workshop

Introduction

What if the next data breach beast reared its ugly head and appeared in your camp? And, key stakeholders are still in denial that a data breach *could*, let alone *did*, happen.

Over the years, our caseload continues to support our observation that data breach scenarios are not so much about threat actors, or even about exploited vulnerabilities, but are more about the situations in which incident response (IR) stakeholders find themselves.

The “Verizon Incident Preparedness Report” tackles data breach preparation for that inevitable spar with the demon of death in the age of digital heroes. We looked to put this session's attendees in the shoes of incident responders seeking to improve breach response efforts and mitigate future cybersecurity incidents.

As we moved through each 'phase', we highlighted crucial situational pivot points as experienced in our investigative response casework and seen through trending metrics in our IR Capability Assessment and Data Breach Simulation observations.

Finally, we concluded the session by re-capping, what is in our experience, the 10 incident response elements to tame the data beast.

The VTRAC Team – First Hand Experience

The VTRAC (Verizon Threat Research Advisory Center) team is a leading benchmark in the digital forensics, computer incident response, electronic discovery, and IT investigative arenas, providing both public and private sector organizations with leading services and support. VTRAC team personnel hail from military, law enforcement, and IT technical backgrounds affording customers direct access to a wealth of highly specialized investigative experience and expertise.

Here are key credentials of the VTRAC team:

- Investigations for hundreds of global commercial enterprises and government agencies annually
- Cyber intelligence, endpoint forensics, network forensics, threat hunting, malware reverse engineering subject matter expertise
- Well versed in criminal and civil investigative requirements and extensive experience providing in-court testimony in both expert and fact witness capacities
- Caseload and editorial contribution to annual Verizon Data Breach Investigations Report (DBIR) and its companion—the Data Breach Digest

VTRAC Team Technical Profiles

Learning Lab Approach

The session covered one sample Data Breach Scenario as picked up from the Verizon Data Breach Digest to highlight the situational challenges and the countermeasures recommended.

Scenario 0: Credential Theft – the Monster Cache

To get folks thinking about incident response, this was the sample data breach scenario covered in the session prior to the exercise:

Incident Background

- Industry frequently targeted by espionage-oriented threat actors via phishing emails as entry vector
- +500 corporate user credentials dumped and available in DarkNet forum
- Transfer logs, phishing email, and threat intelligence uncovered source and provided threat actor context
- Activity stemmed from compromised account with phishing emails sent to internal end users
- Email included link to credential-harvesting site, prompting users to authenticate with credentials

Mitigation and Prevention

- Keep current on the cyber threat landscape and threat actions targeting your industry
- Integrate threat intelligence into operations and facilitate threat data dissemination
- Implement Multi-Factor Authentication (MFA)

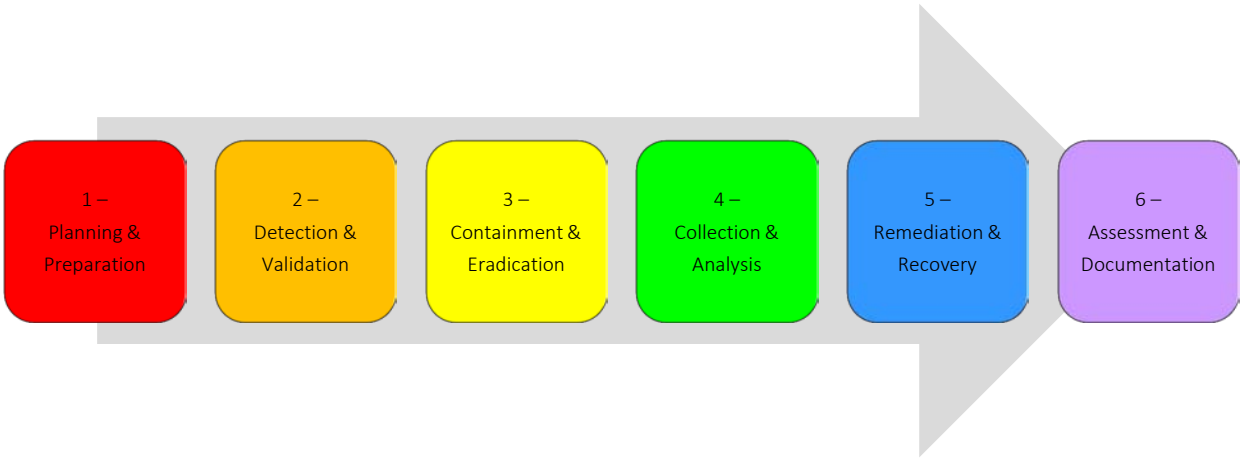
Detection and Response

- Review logs to learn how threat actors are targeting your organization
- Consider creating honeypots to detect, counteract, and gain insight into targeted attacks
- Upon being notified of user credential compromise, change them immediately!

Group Exercise

All the four VTRAC presenters organized all the session attendees into four discussion groups. Each discussion group was assigned two scenarios to be worked upon. These discussion groups' participants sat together in a roundtable format to carry out these tasks under supervision, guidance, and expert advice provided by the VTRAC presenter for each of the assigned scenarios in the exercise:

1. Understand the incident scenario
2. Highlight and capture key observations
3. Discussion amongst the group members regarding the scenario background
4. Deliberate on the Incident Preparedness Strategy across all six (6) phases:
    a. Planning & Preparation
    b. Detection & Validation
    c. Containment & Eradication
    d. Collection & Analysis
    e. Remediation & Recovery
    f. Assessment & Documentation
5. Identify, document and present on:
    a. What preparatory actions could have been taken?
    b. What activities would be important to detect and triage the incident?
    c. How would this incident be contained, the threat eradicated, and the situation be recovered?
    d. What steps could be taken to prevent / mitigate the incident?
6. Obtain best practices and expert advice from VTRAC presenter based on real-world experiences



Scenario 1: Insider Threat – the Card Shark

The Situation

Despite seeing most attacks coming from outside sources (e.g., hacking, spear phishing, etc.), occasionally we see attacks emanating from within a victim organization's own network environment. One such case involved payment card data compromise involving unauthorized automated teller machine (ATM) withdrawals resulting in significant financial loss. For this case, we—the VTRAC | Investigative Response Team—were engaged to conduct a Payment Card Industry (PCI) forensic investigation.

Investigative Response

After arriving onsite, the first thing we noticed was that we were granted immediate access with no security or identification checks. This was unexpected and unusual, considering the circumstances. We were also informed that most of the staff who we wished to interview had been replaced due to the incident and that the new staff were still becoming familiar with the environment.

Our initial security information and event management (SIEM) log analysis identified a malicious system within their environment. This system was neither corporate-owned nor "known" which raised multiple questions, including how the system made its way onto the network, where it was located, how it gained access into the PCI environment and why no one noticed the initial alerts.

All we had to go on was a rogue system connected to the network and indications it accessed critical PCI server databases and conducted unauthorized withdrawals. We still didn't know how the system came to be on the network or exactly how the attack occurred, so we focused in on gathering further information.

We set about conducting interviews and collecting technical information, such as the network topology, to fully scope out the incident and identify possible intrusion vectors. The insight provided by this additional information revealed the entire network structure was flawed from the ground up.

Despite a few internal firewalls, the network was essentially flat. In addition, full network access was available to any connected device due to the lack of even rudimentary access controls. In-place network monitoring was not correctly configured, and while there was a SIEM in place no one was reviewing and investigating alerts.

These fundamental design flaws in the entire network weren't only an open door for attack, but also made it trivial for a threat actor to fly under the proverbial radar.

We reviewed the physical security controls at the location where the attacker's system was determined to have connected during the attack. The location was a main data center, which was a large office building with a publicly accessible area.

To our surprise, the data center's access was secured only with a standard keyed door. Once inside, all offices were easily accessible. This lax security posture included no identification verification, no access control lists, and no one consistently occupying the security desks. We quickly realized that accessing the employee areas from the public areas would've been relatively easy due to the weak physical security.

Besides the poor physical security, we identified major flaws in the organization's digital security posture. These flaws included easily guessable passwords, unchanged admin account passwords, shared user and admin accounts, database access by default user accounts, and admin privileges for every database user account.

Forensic analysis revealed an attacker with physical access used the suspect system to gain access to one of the application servers via an admin account. The attacker generated scripts to manipulate the database and executed these on the night of the incident. Unfortunately, the suspect system was never found and therefore was not available for analysis.

Lessons Learned

In the end, it was obvious what lead to the compromise:

- Step 1: Gain physical access. Weak physical security controls allowed the attacker to gain physical access and introduce an unauthorized system to the organization's premises.
- Step 2: Obtain logical access. Insufficient network access controls and poor network segmentation enabled the attacker to connect to the internal network and access critical server and database systems.
- Step 3: Leverage privileged access. Weak password policies enabled the attacker to logon with admin privileges and manipulate the target databases to complete the attack.

Finally, the lack of proper utilization of network monitoring prevented the organization from detecting this attacker at an early stage. Not known at the end of this investigation was to what level the attacker had "insider" support. Potential answers for many of our questions vanished with the undiscovered suspected system.

Detection and response

- Properly configure network security monitoring software (e.g., SIEM, Intrusion Detection System (IDS)) based on use cases; regularly review outputs and events
- Train employees on cybersecurity policies and procedures, and in doing so, sensitize them to report suspicious cybersecurity and physical security incidents; conduct periodic mock incident table-top exercises to test responders and stakeholders
- Include an Insider Threat Playbook within the Incident Response Plan; hold After Action Reviews (AARs) after incidents and capture lessons learned for future improvements
- Proactively assess for payment card fraud; contact acquirers and card brands; conduct internal checks and audits (cover all 12 PCI DSS requirements); engage law enforcement when the time is right

Mitigation and prevention

- Restrict physical access: Employ physical security measures, such as identity cards, card swipes, and turn-stiles; further restrict access to sensitive areas; monitor via closed-circuit camera system; prohibit personal devices on the network
- Restrict logical access: Segment the network; prevent rogue system connection to the network; implement multi-factor authentication (MFA); use complex passwords for all user accounts; apply the principle of least privilege for access to sensitive data

Scenario 2: eCommerce breach – the Flutterby Effect

The Situation

The call center was receiving a high call volume from online customers having issues paying for products. Specifically, there appeared to be a consistent issue with “frozen pages” when attempting to submit payment on our checkout webpage. As the Incident Commander for an online retailer, I was alerted immediately as this could have a potentially negative impact on our online sales.

This issue couldn’t have come at a worse time. Due to the holiday season, our IT staff wasn’t permitted to change the web application or the production environment.

My initial thoughts were this issue was likely related to some bug within our point-to-point encryption (P2PE) setup as it dealt with payment card data at the point of checkout. Payment card data was encrypted prior to being received by our systems, which relaxed any concerns of potential payment card related fraud.

As a first step, we tested the checkout process within our nonproduction development environment. After repeated attempts, we observed no issues with the checkout process; the data inputs and outputs looked normal.

This was perplexing as our development checkout process should’ve been a perfect replica of our production instance. There were no changes logged in our change management platform and no employees had changed the production platform in several weeks.

We then focused on the production environment, attempted the checkout process “live” and received the frozen page. We hash-checked the development pages associated with checkout process against those pages in production. If something was different between development and production, a hash check would reveal an affected page. Sure enough, the hash differed in the checkout webpage and contained a JavaScript code involved in the processing of payment cards.

A quick comparison revealed five lines of code had been inserted into the production page. A preliminary review of the code suggested that it used a simple regex string to look for payment card data strings and send it to an external domain.

Investigative Response

Prior to this discovery, our Chief Information Security Officer (CISO) had notified the VTRAC | Investigative Response Team. Their investigation revealed an attacker had gained access to our payment processing application.

After gaining access, the attacker modified the payment processing code on the application. During the checkout process, this JavaScript code then redirected the payment card data via the web browser to a remote internet domain. So, although we were using P2PE, the solution was irrelevant for these attacks as the theft occurred before the data ever made it to our systems or the payment processor.

However, the malicious code failed to execute cleanly causing the Internet Explorer browser to hang. We cleaned up the malicious sections of code and implemented stronger access controls for future code updates.

Lessons Learned

One thing we realized from the start of this incident was that policy-based restrictions don't prevent unauthorized users from breaking them. We had written policies restricting personnel from modifying the production environment. However, there was no actual system or logical restrictions preventing access and later changes to critical and sensitive systems.

We were lucky to have caught this early on. Given this attack occurred during our busy season, this could've hurt a large part of our customer base. With this in mind, when the dust settled, we compiled a list of actions to undertake as part of our after action review (AAR).

Mitigation and prevention

- Assess the complete payment process (and not just the P2PE solution); implement further controls with a defense-in-depth approach
- Implement system-based controls to help prevent unauthorized access; make it a policy and practice to use admin accounts (with two-factor authentication) only when needed

Detection and response

- Proactively discover undetected code modifications by regularly performing integrity checks on sensitive code; implement tools to track and monitor website changes; implement a change control process for modifications
- Help detect unusual elevated account activity by periodically reviewing logs of accounts accessing critical and sensitive systems
- Regularly review and update firewall configurations / Access Control Lists (ACLs)
- Implement a File Integrity Monitoring (FIM) solution

Scenario 3: Crypto-jacking – the Peeled Onion

The Situation

As in previous years, 2017 saw significant interest in cryptocurrencies or crypto-jacking, both the classic Bitcoin and newer alternatives. Unsurprisingly, with the meteoric rise in Bitcoin value interest hasn't been limited to investors. In 2017, the VTRAC | Investigative Response Team has investigated several cybersecurity incidents involving attackers whose motivation has been financial gain through cryptocurrency mining malware.

This variety of malware uses the processing power (e.g. CPU or graphics card) of the infected system to mine cryptocurrency, which could then be used like traditional cash to purchase items or directly exchanged for legal tender. While mining is a legitimate process in the cryptocurrency lifecycle, using someone else's system in an unauthorized manner is not.

While Bitcoin is the most widely known cryptocurrency, there are hundreds of alternative cryptocurrencies sometimes better suited for mining through malware. This is due to their relative anonymity or ease of being mined on ordinary systems. In 2017, we investigated only a few cases of malware mining for Bitcoin while the majority of cases involved Monero or Zcash.

In one such "non-Bitcoin" case, a customer who had observed a significant number of alerts originating from their firewalls called upon us. The firewalls were blocking suspicious outbound traffic to The Onion Router (Tor) network and in doing so, triggering alerts. Our customer believed they had the situation under control because the firewalls were blocking the traffic. They asked us to determine the cause of the traffic, verify they had things under control, and verify there were no indications of data exfiltration or lateral movement in their network.

Investigative Response

Prior to engaging us, the customer had obtained full packet captures (FPCs) of network traffic and captured a physical memory dump from a system generating the suspicious outbound traffic. We dove into the network FPCs and the memory dump, and soon provided actionable intelligence to identify other potentially compromised systems on the network. This actionable intelligence—indicators of compromise (IoCs)—included system names, IP addresses, malware file hashes / file names and malicious process names.

A review of the active network connections immediately revealed that while the majority of traffic was blocked by the firewall, there were successful connections to resources in the Tor network. This was due to the firewall filtering being based on IP address blacklisting, which didn't encompass all Tor addresses used by the malware. It was also observed that further network connections were being made to a mining pool associated with the Monero cryptocurrency. All malicious network activity was identified as originating from the Microsoft "powershell.exe" process (a command line shell and scripting tool) running on the sample system and other systems found to be infected.

Meanwhile, in reviewing the FPCs our VTRAC | Applied Intelligence (a.k.a. Network Forensics) team confirmed the malware used a propagation method similar to that of well-known ransomware instances.

The method leveraged leaked hacking tools by the hacking group "The Shadow Brokers." An examination of an image of the sample system confirmed it wasn't patched against a known vulnerability (CVE-2017-0143: Windows SMB Remote Code Execution Vulnerability) that made the propagation possible. This was contrary to our customer's belief they were properly secured.

We then analyzed firewall logs to identify any other systems beaconing out to the Tor network and requiring remediation. We assisted the customer with a remediation plan that involved providing samples of the malware to their anti-virus vendor, patching vulnerable systems, eradicating the malware and rebuilding key systems based upon legacy operating systems.

Lessons Learned

During the investigation, it was discovered that hundreds of systems within the network hadn't been patched with the latest Microsoft Windows patches. Prompt and proper patching could have averted this incident.

On this occasion the malware targeted cryptocurrency mining, but more malicious software could've leveraged the same vulnerabilities and made a more significant impact on business.

Mitigation and prevention

- Conduct regular security assessments; evaluate defensive architecture design based on sandboxing, web browser separation, and virtualization for select activities
- Establish a vulnerability patch management program; apply security patches soon; confirm patching succeeded
- Employ enterprise and host-based anti-virus solutions with up-to-date signatures to detect and eradicate threats as they arise
- For critical systems and servers, deploy File Integrity Monitoring (FIM) and Application White Listing (AWL) solutions; add Intrusion Prevention System (IPS) rules; disallow internet browsing
- Block and/or alert on internet connections to cryptocurrency mining pools; include Tor networks, unless a valid business reason not to do so
- To the extent possible, remove local admin; force standard user use for web browsing activity and force escalation for privileged user use in other context

Detection and response

- Be vigilant for anomalous activity, such as sharp increases in system CPU usage or network egress / ingress traffic volumes; monitor firewall and network appliance logs for anomalous activity
- Block access to command and control (C2) servers at the firewall level; deploy Group Policy Objects (GPOs) to block known malicious executable files and disable macros
- Perform malware analysis to understand malware functionality for detection and response, and mitigation and prevention
- Conduct periodic threat hunting activities across the network to locate and identify any undetected cyber threat activity evading traditional cybersecurity tools
- Create an Incident Response Playbook for cryptocurrency related scenarios; train incident responders on response efficient and effective activities

Scenario 4: Cloud storming – the Slivered Lining

The Situation

It was a normal day at the office as I inspected the alarmed access and egress points at our corporate office. As I was walking through the hallways, I received a phone call from law enforcement.

The officer informed me that certain systems on our network were likely compromised since they were contacting an IP address that they'd identified as malicious.

With a timeframe and the malicious IP address in hand, I engaged our Information Technology (IT) Security team as well as our Chief Information Security Officer (CISO). Our initial network review revealed two systems—one in California and one in Virginia—communicating with the malicious IP address.

Investigative Response

The IT Security team further determined these two systems contained intellectual property that could severely affect our business if exposed to our competitors. Our CISO triggered our retainer service with the VTRAC | Investigative Response Team, bringing them in to assist with the investigation.

Within 24 hours, the VTRAC investigators were onsite at each data center to collect evidence from the two systems. Using the leads provided by our IT Security team, the VTRAC investigators identified an active open source Remote Access Trojan (RAT). Malware analysis of the RAT revealed domain names resolving to the malicious IP address.

Leveraging the VTRAC | Cyber Intelligence Team, the RAT was associated with an Advanced Persistent Threat (APT) group known as APT10. APT10 was commonly associated with attacks aimed at stealing intellectual property and leveraging Managed Service Providers (MSPs) as attack vectors. The MSP cyber-attack stream was essentially:

- Step 1: Infiltrate MSP
- Step 2: Compromise MSP accounts
- Step 3: Choose victim from MSP customer pool
- Step 4: Gain access to victim network
- Step 5: Exfiltrate intellectual property via MSP network

With a list of APT10 associated indicators of compromise (IoCs), our IT Security team quickly scanned our network for other potentially compromised systems. The scans identified multiple infected systems. Even worse, many infections dated to 2015!

The most common malware found by the scans were backdoor tools used by APT10 to maintain persistence on the network. Further analysis also found multiple compromised user accounts, including administrator accounts. In addition, the threat actors were observed accessing our network via an IP address associated with our MSP.

The VTRAC investigators determined the threat actors leveraged our MSP accounts and network to gain access into our environment. This also correlated to attack vectors utilized by APT10.

With evidence pointing to an APT attack, and given the lengthy time of compromise, it was highly possible other systems in our network (with various credentials) were at risk. Most important, it was possible that our intellectual property was already being exfiltrated.

At this point, a War Room with all Incident Response (IR) stakeholders was already established to shape our response. We set about identifying and then rebuilding all affected systems. For those areas of the network we found "lacking in adequate visibility" we expanded our logging and monitoring capabilities.

We decided that an effort to understand the full extent of the threat actors' actions in our network would have been too resource intensive. So we committed our efforts to determining if data exfiltration had occurred, and securing the company's network. Ultimately our containment, eradication, and remediation efforts succeeded, as we observed no additional APT10-related activity in our network after the initial detection.

Although the investigation uncovered no evidence of data exfiltration, given the time we were compromised our executives were concerned the threat actors may have accessed our intellectual property. We continued to work with the VTRAC investigators to monitor relevant online forums and marketplaces in the DarkNet to see if any of our data ends up in the public or available "for sale" by the threat actors.

Lessons Learned

A call from law enforcement turned into a major incident that could've put our company in jeopardy. Even though our stakeholders responded we still had several lessons learned from this incident.

Mitigation and prevention

- Systematically monitor and test security posture from all angles; provide additional security and monitoring on critical systems; conduct periodic threat-vulnerability scanning
- Review, reconcile, manage, and monitor all third-party account access
- Enhance user account security by requiring regular password changes, including local admin accounts; monitor and manage privileged accounts
- Harden systems; disable / remove unnecessary applications; create baseline images; classify critical assets

Detection and response

- Proactively review logs of all internet-facing systems and applications; conduct threat hunting activities; collect and analyze affected systems and associated system logs
- Employ a file integrity monitoring (FIM) solution to assist with detection efforts; employ an Intrusion Detection System (IDS); collect and analyze network logs
- Take affected systems offline; restore systems from baseline images/ rebuild all affected systems; expand network logging and monitoring capabilities for areas lacking in network visibility
- Leverage threat intelligence resources; consult with legal counsel; contact law enforcement when the time is right

Scenario 5: Cyber-espionage – the Katz-Skratch Fever

The Situation

While espionage has existed for thousands of years, cyber-espionage (threat actors targeting sensitive or proprietary data on digital systems) is still a relatively new concept. Recently, a manufacturing customer engaged the VTRAC | Investigative Response Team to let us know they'd been contacted by law enforcement regarding a possible data breach.

The Chief Information Security Officer (CISO) had been notified of several foreign IP addresses that may have been communicating with systems inside his environment. The CISO requested we immediately report to their headquarters to begin investigation into the suspicious IP addresses.

Investigative Response

As VTRAC I Investigative Response Team investigators, we understood the potential severity and deployed to the customer's headquarters the next day. After an initial in-briefing with the CISO, we started our triage of several in-scope servers and other equipment believed involved in this incident. Upon collecting several memory dumps and full disk images, we reviewed the digital evidence.

That evening, we discovered a unique software program on one of the primary systems. Well-known by penetration testers and IT security professionals, 'Mimikatz' is a powerful credential theft tool that scrapes memory of the process responsible for Microsoft Windows authentication (LSASS) and reveals clear text passwords and NT LAN Manager (NTLM) hashes.

With this information, the threat actor could traverse multiple systems in a network. Knowing this was a critical piece of the investigative puzzle, we immediately shared the file's metadata with our VTRAC | Cyber Intelligence Team.

By the next morning, the VTRAC intelligence analysts informed us this file was routinely used by a specific nation-state to attack U.S. companies. Additional queries revealed the threat actor had intentionally targeted one employee, a senior IT system administrator, with access to multiple servers including domain controllers across the customer's engineering division.

The investigation also revealed a key component of the attack. Specifically, the sys admin received a phishing email about his 401K retirement plan which appeared to originate from his plan administrator. The email contained a PDF attachment, which upon opening silently installed Mimikatz.

Lessons Learned

To summarize the lessons learned from this engagement, recommendations were made for both mitigation and prevention, and for detection and response.

Mitigation and prevention

- Provide, at least annually, user cybersecurity awareness training; emphasize awareness and reporting suspicious emails
- Make external emails stand out; prepend markers to the 'Subject:' line indicating externally originated emails
- Move beyond single-factor authentication and implement multi-factor authentication; require virtual private network (VPN) access for remote connections to the corporate environment

Detection and response

- If not already involved, engage law enforcement, when the time is right, and third-party investigators, when applicable
- Collect access logs to key servers and email; prior to system shutdown, collect in-scope volatile data and system images; examine quickly
- Utilize internal and external intelligence resources to develop actionable intelligence on threat actor modus operandi and IoCs

Scenario 6: ICS attack – the Eclectic Slide

The Situation

It was late in the evening when I got the call. “We’re going to need you to come into the office.” As the Security Operations Center (SOC) lead analyst in critical infrastructure protection (CIP), I was used to getting calls after hours. However, what was unusual was the next statement. “law enforcement called and they believe we may be compromised.”

When I arrived, the office was in a frenzied state since it was not clear how (or even if) we’d been compromised. We assumed the worst and avoided communicating through typical corporate channels. This made information sharing with colleagues not physically present in the office difficult.

We were also informed that any new information we found or received from the FBI was “TLP Red” and couldn’t be shared publicly.

The first indicator of compromise (IoC) we were given was an email address which law enforcement believed was involved in a spear phishing attack against various organizations within the energy sector.

Sure enough, after searching through our email appliance we found the specific address had sent several emails. Each targeted an executive or lead engineer at our electrical plant.

The emails came with an attached Word “resume” for recipients to review. I reviewed the attachment in our malware analysis environment and saw nothing out of the ordinary - no web links, no macros, and no child processes being spawned. I called the VTRAC | Investigative Response Team to assist.

Investigative Response

The VTRAC investigators examined the suspicious attachments and presented their findings soon after. They found the threat actor was using a Microsoft Word template hosted on the internet and communicating with a command and control server. This technique, later coined “Template Injection,” was a novel way of leveraging Microsoft Word to download a malicious payload.

When opened, the Word document “searched” for a specific, malicious template via the server message block (SMB) protocol hosted on the threat actor’s server. Once downloaded, the malicious template used macros to spawn a Microsoft PowerShell (command prompt) instance to steal user account credentials.

It turned out the targeted users had not corresponded with the threat actor. However, they all had very public profiles on a popular professional networking social media website. The threat actors likely used these profiles in selecting their targets.

Armed with this additional information, we immediately asked targeted users to change their account passwords. We then forensically collected the systems and volatile data associated with these users.

Some engineers had access to highly privileged operational technology (OT) systems within the plant. This was an issue as none of the SOC analysts had taken the North American Electric Reliability Corporation (NERC) CIP training required to access the plant systems.

With time of the essence, and no SOC analyst being able to access these systems, we created a PowerShell script to search for the IoCs we then loaded on a USB device. We identified a plant engineer with the appropriate level of system access, made a one-time exception and had him plug the USB device into the OT systems to run the script and scan for any IoCs.

Lessons Learned

While we found no additional IoCs, we identified several improvements to make regarding our incident response approach. During our after action review, we set out to accomplish these actions as soon as possible:

First, we set up an alternate communication means separate from the corporate network. This provided the SOC analysts with "secure comms" should our corporate network be compromised.

Next, we educated our end users to be careful with the information they share online as threat actors can use this information to identify "high-priority" attack targets. Then, we implemented firewall rules to block external SMB connections to unknown public addresses.

Last, but not least, we made it a requirement that all SOC analysts and cybersecurity incident responders take the required NERC CIP training and undergo additional background screening as an added security measure.

Mitigation and prevention

- Isolate OT networks; use dedicated OT systems; disable email and internet access, and access to networks at security-levels lower than the OT environment
- Implement firewall rules blocking SMB connections to unknown public internet spaces; add detections for Microsoft Office and other user applications spawning PowerShell child processes
- Sensitize employees to the security implications of posting sensitive information on social networking sites

Detection and response

- Establish a method for reliable, secure, alternative communications before a cybersecurity incident occurs; incorporate this into the Incident Response (IR) Plan
- Increase logging and alerting for configuration changes, to include user account creation and modification; enable enhanced logging for PowerShell script triggered actions
- Comply with industry training and certification requirements; familiarize SOC analysts and incident responders with the industrial control system (ICS) environment; train them to respond to ICS related cybersecurity incidents

Scenario 7: PoS intrusion – the Faux PoS

The Situation

Reliance on third-parties has increased significantly. The practice not only benefits the business financially but also provides an opportunity for any organization to focus on their core business strengths while letting expert third parties handle selective domains.

As the Business Unit Leader for a large "brick and mortar" merchant in the Asia-Pacific region, that was my expectation. I had worked with a third-party vendor, utilizing their point-to-point encryption (P2PE) solution to establish a more secure transaction flow between our Point-of-Sale (PoS) systems and our acquiring banks.

All was fine until our acquiring banks informed us of a suspected payment card industry (PCI) data breach. Fraudulent transactions worth millions of dollars had occurred in various parts of the world.

The common point of purchase (CPP) analysis from the payment card brands had identified us as the likely source of the stolen payment card data. This reported data breach wasn't limited to a store, or even a region, but was spread throughout our global store network.

I kept asking myself, "What could have gone wrong?" "Where had we been breached?" "Was it in our corporate network?" "Was it at our stores?" "Or perhaps it was one of our service providers?"

Investigative Response

We quickly established a War Room and core team coordinating internal meetings and sessions with the acquiring banks and payment card providers. In parallel, we engaged the VTRAC | Investigative Response Team as the PCI Forensic Investigator (PFI) for the PCI investigation.

The VTRAC PFIs meticulously combed through the incident background information, payment transaction flow, CPP analysis data from payment card brands, our IT environment details, and our third-party access.

This was followed up with a game plan to collect and analyze the PoS servers and terminals at the CPP-identified stores, along with the in-scope business units and approximately a dozen third-party servers.

Unfortunately, valuable forensic artifacts were lost due to the actions of the vendor. They had restarted systems, executed anti-virus scans, deleted existing local system accounts, changed passwords, deleted various logs, and changed the systems. This had all been conducted without our approval and just prior to the evidence collection.

The VTRAC PFIs soon identified a litany of issues. These included unrestricted ingress from the internet to the PoS servers, single-factor authenticated logons from unknown external IP addresses using a Remote Desktop Protocol (RDP), a backdoor Trojan virus, RAM scraper and network sniffer software on the systems. They also found over 100,000 transaction log entries with primary account numbers (PANs) and full Track 1 and/or Track 2 information in clear text on the third-party server.

Based on the forensic analysis of the available evidence sources, coupled with an understanding of the payment card data transaction flow and the CPP analysis, it was confirmed that a data breach had occurred.

This breach occurred first through a brute-force attack on RDP access, followed by installing a network sniffer, a RAM scraper, and finally a Remote Access Trojan (RAT) on the third-party payment card data processing server.

Now that the investigation was complete, I prioritized the remediation, recovery, prevention, and mitigation actions.

The affected systems were cleaned and/or rebuilt, RDP access was restricted using source address-based filtering, and multifactor authentication (MFA) was required for all remote login connections.

A thorough review of the security controls of the third-party service provider brought up gaping holes, not only from the PCI DSS perspective but also from basic hygiene security controls that ideally should be implemented for any secure enterprise.

We immediately initiated a process for regular, independent PCI DSS compliance assessments of our third-party service providers. We can't blindly rely on our service providers to always be doing the right thing.

Lessons Learned

For us, the investigation highlighted several procedural and technical issues that had led to this incident. Further, the investigation was very complex and arduous due to the unavailability of some crucial digital evidence. Among their findings, the VTRAC PFIs made these recommendations.

Mitigation and prevention

- Establish and implement system-hardening baselines; conduct thorough vulnerability assessments at least quarterly and penetration testing exercises at least annually
- Implement MFA for all non-console access to systems
- Monitor and assess third-party's PCI DSS compliance status risk ongoing

Detection and response

- Create Incident Response (IR) playbooks to supplement the IR Plan; educate first responders on the importance of effective and timely incident response
- Conduct proactive network and endpoint based threat hunting exercises to detect and respond to unknown threats
- Review network and application logs; review logs related to compromised systems or user accounts to determine other affected assets

Scenario 8: Web app attack – the Tuple-Row Honey

The Situation

We're a growing technology consulting business. Recently, we won a huge contract requiring us to hire a significant number of technical staff in a short period of time. The award generated a lot of good press for us and we received several inquiries from people interested in joining our company.

As the Human Resources (HR) Manager, I had seen often where rapid hiring led to candidates who looked great on paper but fell short of the mark in skills. I had also seen highly qualified candidates overlooked because they were intimidated by the traditional job interview. So, I suggested we host an online "hackathon" event to assess technical skills in near real-time and identify quality candidates.

We have many virtual teams collaborating on projects while spread across the country. So I decided the hackathon would require candidates to work together in teams to solve a business problem. With this, we could assess their technical and teamwork skills. From the hackathon, we were looking to hire project managers, business analysts, network architects and information security analysts.

After explaining the benefits and reassuring management that a hackathon isn't actual "hacking," the idea was embraced and I was asked to lead the initiative. My HR colleagues engaged our Information Technology (IT) team to help us set up the event. The IT team proposed using a web application but it would take at least three months to design, test, and implement. We let them know we had only two weeks. After initial push back, the IT team agreed and quickly set to work.

Over the next two weeks, I worked with our external recruiting agency to develop a list of candidates to invite for the hackathon event. The theme would be "Technology to Improve Business and Personal Productivity" and the results were targeted to help our consulting business and employees with their own work-life balance.

During that time, the IT team designed and tested the web application. The app included the hackathon project questions and an online registration form which saved the candidate details to a database. HR and management approved the web application and the next day we went live with registration.

The hackathon was an enormous success resulting in multiple hires. However, a few days after it finished I received an alert on my mobile phone: "Confidential – Web Application Data Breach Incident." Our Chief Information Security Officer (CISO) was calling an Incident Response (IR) stakeholder meeting.

Investigative Response

The IT Security team detected significant in-bound traffic accessing the web application server along with several antivirus detection alerts. We engaged the VTRAC | Investigative Response Team and they were on their way to investigate.

The IR stakeholder meeting attendees included our General Manager, a General Counsel Representative, the CISO, the IT Security Team, the IT Team who'd worked on the hackathon web application, two VTRAC investigators and me.

The CISO started by informing us that our "Hackathon Talent Search Event" was the apparent source of a cybersecurity incident and later Personal Identifiable Information (PII) data breach.

I couldn't believe what I was hearing as we'd taken precautions to vet the candidates. I blurted out, "Why'd they go and cause this trouble on our systems when they were looking for an employment opportunity with us?"

At this point the General Counsel Representative leaned forward and asked "So, let me get this straight. You're saying we've got a breach of PII on our hands here?!"

The VTRAC investigators went to work with our IT Security team and determined that the incident wasn't caused by one of the job candidates, but by a malicious attacker who'd discovered the web app server and exploited a vulnerability. The vulnerability was described as a Remote Code Execution (RCE) attack. The investigators also determined that a legacy version of the web application framework was used and a web application firewall (WAF) was not in place.

Several web shells allowing remote access were discovered on the server. The attacker accessed these web shells prior to their detection and quarantine by the installed anti-virus software.

The investigation also discovered indications of remote logins and successful database queries on the job candidate database. Finally, the logs also indicated the attacker had plundered the data, including the candidates' personal information.

Since the attacker accessed PII data, we had a legal obligation to notify several States' Attorneys General and the affected individuals. I immediately worked with our Legal Team and the Executive Management Team to craft data breach notification letters, create holding statements, and tailor our corporate messaging around this unfortunate event.

The IT team knew that the web application was running a legacy framework and had been planning to upgrade it after the first hackathon. Given that the invite was sent to a handful of vetted individuals, they assumed it would be okay to briefly run the legacy application without a WAF.

Fortunately, they had segmented the web application from the corporate network reducing the potential for additional data exfiltration.

Lessons Learned

The big lesson learned was that once you place a server on the internet without security configuration it's there for all to see and access, not just the select individuals who you invite.

The IT Security team must be an active player in all projects, not just as an afterthought. It's important to not rush development without considering the wider organizational security implications.

Mitigation and prevention

- Develop web apps based on industry best practices; follow the secure software development lifecycle; incorporate information security throughout the lifecycle
- Scan web apps for vulnerabilities; perform periodic penetration tests; develop a patch management program to swiftly patch and update identified vulnerabilities
- Set host-based and enterprise anti-virus solutions to be continuously updated with the latest engine and virus definitions
- Install WAFs, a File Integrity Monitoring (FIM) solution, and host / network Intrusion Detection Systems (IDS); maintain enough logging
- Implement proper data segregation and network segmentation, especially with critical data and systems

Detection and response

- Assemble the IR Team; include stakeholders relevant to the specific cybersecurity incident; engage law enforcement at the right time and with advice from legal counsel
- Engage a qualified and experienced digital forensics firm for investigative response activities to include malware analysis, endpoint forensics, network forensics, threat intelligence, and containment and eradication support
- Collect and preserve evidence; use vetted tools and procedures for evidence collection and preservation; potential evidence includes volatile data, hard disk drive images, network packet captures, and log data
- Leverage established and documented evidence handling procedures; use evidence tags, chain of custody forms, and an evidence tracking log to secure, preserve, collect, and store evidence
- Prepare public relations responses for various data breach scenarios ahead of time; adjust the actual response to the specific data breach circumstance

Appendix: Countermeasures Worksheet

Phase	Mitigation and Prevention	Detection and Response
1 – Planning & Preparation		
2 – Detection & Validation		
3 – Containment & Eradication		
4 – Collection & Analysis		
5 – Remediation & Recovery		
6 – Assessment & Documentation		