2018 Data Breach Digest

verizon

Credential theft – the Monster Cache

2018 Data Breach Digest

verizon✓

The situation

Cybersecurity trends continue to show that organizations most often learn of data breaches through external, third-party notifications. In recent years, the information security industry has integrated cyber threat intelligence into cybersecurity and breach response strategies.

The VTRAC | Cyber Intelligence Team monitors the cyber threat pulse 24x7 for our global customers, leveraging cyber threat intelligence capabilities such as: consistent monitoring of the DarkNet (that "not-easily-accessible" part of the internet used for anonymized content sharing), subscribing to threat intelligence feeds, and incorporating databased indicators of compromise from historical incidents.

With this continued growth and reliance on cyber threat insights, the VTRAC cyber intelligence analysts provide customers with proactive mitigation measures and reactive response actions for data breaches. A normal day in the life of a VTRAC cyber intelligence analyst includes frequent requests from our customers asking to "tell me what I don't know."

Mitigation tips

- Keep current on the cyber threat landscape and the threat actions targeting your industry
- Integrate threat intelligence into operations and facilitate threat data dissemination

All successful breaches can be presented as threat actor goals, capabilities and methods. This perspective enables the creation of attack models. When combined with organization profiling, unique risk reporting is possible and can be a valuable input for both strategic and tactical decision-making. It's with this perspective in mind that our cyber intelligence analysts approached the onboarding of a new Rapid Response Retainer Service (RRR) customer one particular afternoon.

Investigative response

Here, the organization operated in an industry frequently targeted by espionage-oriented threat actors who rely heavily on phishing emails as an initial vector. The emails usually seek to entice recipients into providing user name / password combinations for external access points, using methods such as carefully crafted phishing content and links to enticing, yet compromised, watering-hole websites.

Detection tip

Review logs to learn how threat actors are targeting your organization; consider creating honeypots to detect, counteract, and gain insight into targeted attacks.

When we look at the data sold and traded by cyber criminals, stolen credentials are at the top of this list. For opportunistic attackers, this data is sometimes all they need to further an attack on an organization.

During initial DarkNet monitoring efforts, we typically expect to see all sorts of compromised information available on the criminal underground. However, we were surprised to discover a dump of over 500 corporate user account identifiers and password combinations available in a DarkNet forum. No sooner had we reported our findings than we learned other persons in that same organization had engaged our VTRAC | Investigative Response Team to investigate the unauthorized use of an employee's email account.

Investigators performed a forensic examination to analyze threat actor activity associated with the compromised accounts, and report back with significant information relevant to the case. Mail transfer logs associated with the email accounts were examined, along with the phishing email itself, and our threat research was utilized to uncover its origin and provide important context around the threat actor group.

Response tip

Upon being notified of user credential compromise, change them immediately!

Implement $+r0^g passwords

After compromise, reset passwords for all user accounts. Implement a strong password policy that includes:

- Assign all users separate, unique accounts – don't use generic or shared accounts or passwords
- Set first-time passwords to a unique value for new users; require password lengths of at least eight (8), preferably more, alpha-numeric-special characters
- Change user passwords immediately after the first use and then at least every 90 days
- Block historical passwords from being used for at least the previous four (4) utilized passwords and set the lock-out threshold to six (6) times
- Remove / disable inactive user accounts at least every 90 days; immediately revoke access for terminated users

The findings indicated the activity stemmed from a compromised user account from which additional phishing emails were sent internally to much of the end user population. The malicious message included an embedded link to a credential-harvesting site, prompting users to authenticate via username and password.

Lessons learned

Threat intelligence alone may not always be a perfect predictor of data breaches, but the insight provided from modeling attacks and attackers should be considered when making security decisions. The process enables stakeholders to see how threat actors view their organization and provides responders with possible focus areas when scoping cybersecurity incidents. Aside from sensitizing end users to recognize and report email phishing attempts, three recommendations for mitigation, detection, and response are:

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

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!

Look what I can do: the myriad “values” of stolen credentials

Every day, newly harvested login credentials are bought and sold on underground DarkNet forums and marketplaces. While most of these fall into the category of services like streaming media and personal email, the impact of a stolen username / password combination goes far beyond someone watching the latest must-see series on your favorite streaming app.

Here are a few of the damaging after effects seen in our 2017 casework, which is limited only by the creativity of the perpetrators:

- Compromised remote admin app credentials led to RAM scraper malware installation on point-of-sale (PoS) systems. Dozens of retail locations were affected, resulting in numerous payment card data breaches
- Admin accounts credentials harvested from an exploited, externally accessible database allowed attackers to install multi-featured web shells. Within a matter of minutes, sensitive data was being shipped out to systems operating on The Onion Router (Tor) network
- Compromise of an admin account led to numerous follow-on account thefts via credential stealing malware. The highly privileged access rights of the initial account facilitated lateral movement within the network and ultimately resulted in sensitive personnel files being exfiltrated
- The unauthorized use of accounts in a company’s finance department gave threat actors unfettered access to vendor payment information. Multiple fraudulent payments were issued prior to detection, resulting in a lucrative transfer for the criminals
- Ever popular webmail phishing campaigns prompted dozens of unsuspecting employees in one company to divulge their login information. Then the self-service payroll accounts of these individuals were accessed and direct deposit information changed, netting the attacker sizable paychecks for a hard day’s work

Insider threat – the Card Shark

2018 Data Breach Digest

verizon✓

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.

Detection tips

- 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

All we had to go on was a rogue system connected to the network and indications that 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.

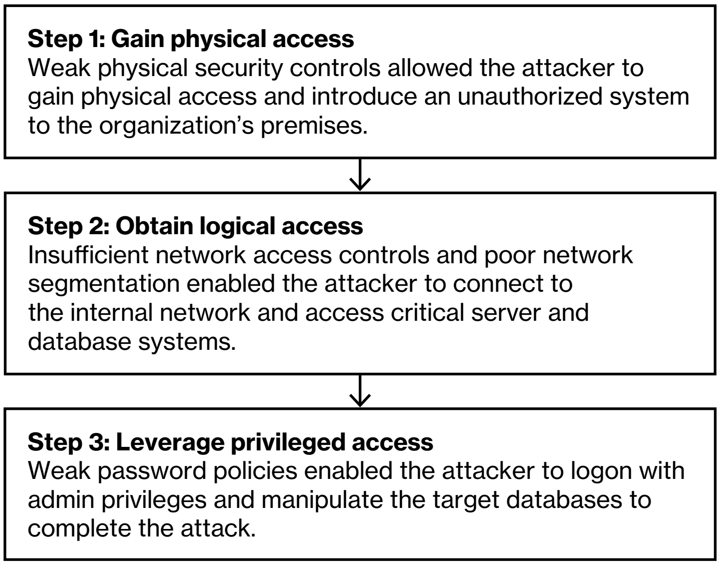
Forensic analysis revealed an attacker with physical access used the suspect system to gain access to one of the application servers via an admin account. The attacker generated scripts to manipulate the database and executed these on the night of the incident. Unfortunately, the suspect system was never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

Mitigation tips

- Restrict physical access: employ physical security measures, such as identity cards, card swipes, and turn-stiles; further restrict access to sensitive areas
- Restrict logical access: segment the network; prevent rogue system connection to the network; implement multi-factor authentication; use complex passwords for all user accounts

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.

Figure 1. The anatomy of the attack

Finally, the lack of proper utilization of network monitoring prevented the organization from detecting this attacker at an early stage.

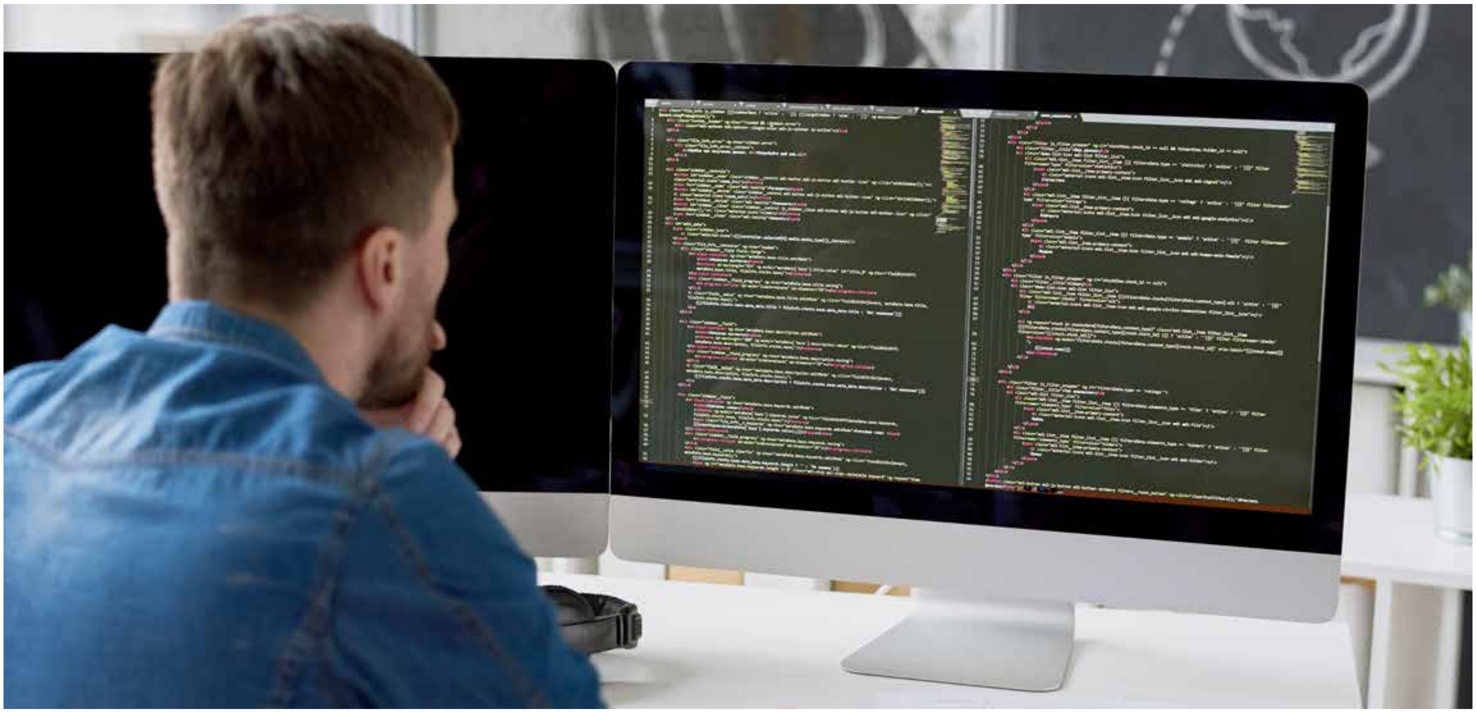
Not known at the end of this investigation was to what level the attacker had "insider" support. Potential answers for many of our questions vanished with the undiscovered suspected system.

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

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
- Restrict logical access: Segment the network; prevent rogue system connection to the network; implement multi-factor authentication; use complex passwords for all user accounts



verizonenterprise.com

Crypto-jacking - Cryptocurrency-mining malware: the Peeled Onion

2018 Data Breach Digest

verizon✓

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.

Response tip

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.

Why are cryptocurrencies so attractive to cybercriminals?

- Money talks: To the tech savvy attacker, cryptocurrency is as good as cash. It's used to directly make purchases, particularly when buying illegal goods, such as stolen identity information, hacking tools or drugs on the DarkNet
- Easy to exchange: If the perpetrator isn't interested in spending cryptocurrency directly then it's simple to cash-in cryptocurrency for traditional cash at many exchanges
- Easy to transfer: Cryptocurrencies can easily be transferred around the world without the delays or bureaucracy associated with traditional wire transfers and banks
- Comfort in anonymity: While Bitcoin (by design) is inherently traceable, there are services to facilitate the laundering of Bitcoin (for a modest fee) which make it attractive to attackers. More recently alternative cryptocurrencies, such as Monero have been developed with privacy and anonymity built in by design, making them attractive to attackers
- Lucrative return: Unlike ransomware attacks with most victims not paying the ransom, cryptocurrency mining has a more promising return rate

Response tip

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.

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.

Response tip

Perform malware analysis to understand malware functionality for detection and response, and mitigation and prevention.

What types of cryptocurrency-related attacks are there?

- Cryptocurrency mining: As detailed in this article, the objective of many attackers is to directly mine cryptocurrencies for illicit profit
- Crypto-malware/ransomware attacks: Prevalent for the past few years, this attack commonly leads to files being rendered useless to its legitimate owner through encryption; the decryption key is provided by the attacker only when a ransom is paid in cryptocurrency
- Cryptocurrency wallet theft: Cryptocurrencies are commonly stored in wallet files, either on an individual system or online wallet service. These wallets contain private keys controlling the cryptocurrency and are attractive targets for cybercriminals. Malware targeting wallet files for theft and phishing attacks to gain online wallet service credentials is on the rise
- Cryptocurrency wallet service/broker distributed denial of service (DoS) attacks: These DDoS attacks prevent users from using their cryptocurrency wallet (e.g., as Bitcoin prices fall, it was time to sell as fast as possible)

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 Management (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.

What can malware analysis tell me about cryptocurrency-mining malware?

In performing malware analysis to understand its functionality, consider conducting these activities:

- Identify any kill-switches and/or configuration files; determine their impact on malware functionalities
- Evaluate blocking malicious remote servers (not just C2) used at firewall and proxy servers
- Evaluate blacklisting malicious domain names at Domain Name System (DNS) level
- Create additional detection rules; perform threat hunting using network Intrusion Detection System (nIDS) / host Intrusion Detection System (hIDS) signature, including YARA rules, file hashes, etc.
- Identify any self-propagation mechanisms; take corrective measures (e.g., reporting to vendor, patching vulnerabilities)
- Eradicate any persistence mechanisms
- Determine encryption mechanism used and possible way to recover encrypted files

Cyberespionage – the Katz-Skratch Fever

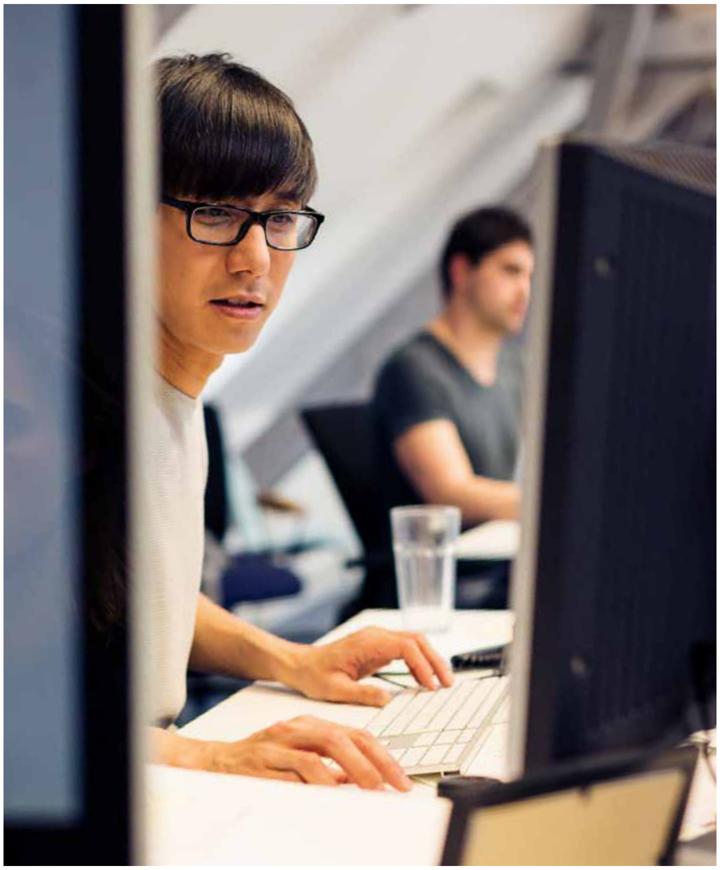
2018 Data Breach Digest

verizon✓

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 (LE) 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.



Response tips

- If not already involved, engage LE, 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 Indicators of Compromise (IoCs)

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 that 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, who had 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 sysadmin 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.

From there, the threat actor obtained the sysadmin's credentials and moved laterally across several domain controllers and engineering file servers. In doing so, they were able to methodically reconnoiter multiple engineering department servers and file shares.

After further examination of the digital evidence, it was determined that approximately 3,000 sensitive, proprietary computer-aided drafting (CAD) drawings, circuit board schematics, and engineering design documents had been uploaded to a FTP site. This site was in the nation-state believed to have committed the break-in.

Since the customer utilized FTP extensively in moving large engineering CAD drawings, it was relatively easy for the threat actor to blend in and exfiltrate the documents.

The threat actor evaded data loss prevention (DLP) detection by sending out the data in small chunks using the WinRAR archiving tool, a favorite software utility used by threat actors to package up their stolen data into an archive file for exfiltration. The archives were password-protected which also prevented any DLP systems from reviewing the data inside.

Mitigation tips

- Provide, at least annually, user cybersecurity awareness training; emphasize awareness and reporting suspicious emails
- Make external emails stand out; prependmarkers 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

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 LE, 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

Supply-chain reaction – the Whole Enchilada

2018 Data Breach Digest

verizon✓

The situation

While many of our investigations here at the VTRAC | Labs are straightforward, involving commodity servers and operating systems, others require us to work directly with embedded systems or hardware components. These engagements are conducted in the Labs where we have more specialized tools at our disposal, beyond what fits in an investigator's "Go Kit".

In one investigation of suspected cyber-espionage, a customer asked us to determine why certain devices were behaving unusually. While reviewing network traffic, the customer realized a particular server model they used extensively had been sending Simple Network Management Protocol (SNMP) traffic to a Southeast Asia IP address.

Since this IP address wasn't associated with any of their vendors or customers, they were concerned about data exfiltration. This increased when the server vendor couldn't explain the remote IP address connections.

Detection tip

Monitor for and alert on suspicious network traffic, such as unusual off-hours activity, volumes of outbound activity, and remote connections.

Investigative response

The customer provided us with one physical server, a verified forensic image of a second, and the suspicious remote IP address. We then went to work setting up an air-gapped environment to physically inspect and test the server in hand.

Nothing out of the ordinary was discovered during the physical inspection; however, a remote management module (the system component responsible for communications management) was identified.

Our next steps were to recreate the suspect communication. The server was connected to a full packet capture (FPC) device. Upon booting, it attempted to find the network node associated with an internal (RFC 1918) IP address, IP 172.16.x.x.

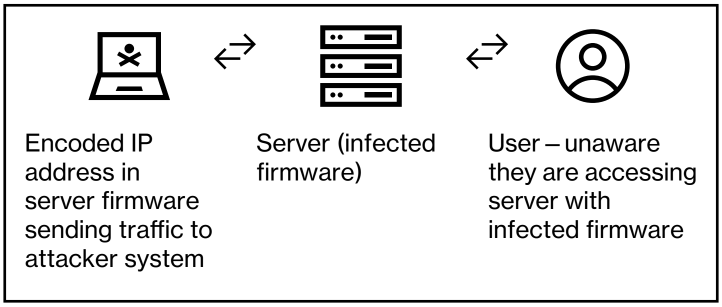

Encoded IP address in server firmware sending traffic to attacker system
Server (infected firmware)
User – unaware they are accessing server with infected firmware

Figure 1. Firmware generated traffic

Response tips

- Keep baseline system images and trusted process lists; use these known standards to compare with compromised systems
- Contain by temporarily blocking outbound internet traffic, changing user account passwords, and searching for indicators of compromise
- Eradicate by disabling compromised user accounts, removing malicious files, rebuilding affected systems

Assuming this was its default gateway, the server was powered down. Traffic for IP 172.16.x.x was routed to the FPC device, and the server was rebooted. Once the server received IP 172.16.x.x in response, it attempted to communicate with the suspicious IP address.

These communications were controlled by the server's firmware, so our next step was to review that. We downloaded several versions of the firmware from the vendor's website, and a review identified the boot loader and file system in use. We found no indication of the suspicious remote IP address hardcoded in the firmware.

With the software ruled out as a suspect, we used an oscilloscope to determine the location and specifications of an active serial port for debugging. This debugging port offered a way of connecting to the main processor associated with remote management. This permitted monitoring of the management card boot process and access to its command shell.

We extracted the firmware source code from the server for analysis, including a search for the suspicious IP address. It took effort but we eventually found it in hexadecimal format in a configuration file. This configuration file was identical to the ones downloaded from the vendor but contained the suspicious IP address in encoded format.

Ultimately, it was determined that all system components and code matched those shipped from the vendor. Due to the complexity of modern computing environments and corporate networks, it's a challenge to keep track of every server and connection required for operation. Here, even the vendor was unaware of owning and using this suspicious IP address which itself led to a very lengthy investigation.

Adding rogue mechanisms, such as remote management modules or similar embedded devices to systems, can provide ingress and egress vectors for threat actors to leverage. Therefore, they must be part of overall device security.

Mitigation tips

- Vet hardware supply chains, to include original equipment manufacturers and value-added resellers, for reputation and reliability
- Adopt an IT management process, that covers design, testing, management and review which aims to maintain confidentiality, integrity, and availability
- Maintain an asset inventory; track and account for all assets, to include critical servers and systems

Lessons learned

The customer had several good security practices in place. For instance, their detection of the unexpected traffic resulted from routine network monitoring. However, had they tested the systems prior to deployment, they might have noticed the suspicious traffic and evaluated the risk it presented. This would have also provided them with an opportunity to work with the vendor at a more relaxed pace.

Regardless, it's good practice to upgrade to the latest version of firmware for testing prior to deployment. With the new firmware in place, a baseline of the system behavior should establish what "normal" looks like. Familiarity with normal setup and behavior can be the difference between detecting anomalies signaling an attack, and becoming aware at a less convenient time.

Mitigation and prevention

- Vet hardware supply chains, to include original equipment manufacturers and value-added resellers, for reputation and reliability
- Adopt an IT management process, that covers design, testing, management and review which aims to maintain confidentiality, integrity, and availability
- Maintain an asset inventory; track and account for all assets, to include critical servers and systems

Detection and response

- Monitor for and alert on suspicious network traffic, such as unusual off-hours activity, volumes of outbound activity, and remote connections
- Keep baseline system images and trusted process lists; use these known standards to compare with compromised systems
- Contain by temporarily blocking outbound internet traffic, changing user account passwords, and searching for indicators of compromise
- Eradicate by disabling compromised user accounts, removing malicious files, rebuilding affected systems

Using cyber threat intelligence

More organizations are incorporating Cyber Threat Intelligence (CTI) into their cybersecurity workflows. Increased insight into supply chain issues is just one of the many upsides. While CTI is the collection, classification, and exploitation of knowledge about adversaries, the CTI process can produce value even when an "adversary" hasn't been identified.

Defined, threat Intel could identify the suspicious traffic:

- Intel feeds / black lists – If the IP address in question was tagged as malicious, combining threat intelligence feeds with SIEM alerting could have warned the SOC of this activity when it started. Ideally, this knowledge would kick off specific escalation procedures
- Threat Intelligence Platform (TIP) – Using a TIP can further enrich what's known about an IP address with further background:
    - Whois information (organization, NetRange, registration date, contact information)
    - Passive DNS (historical IP address to domain mapping)
    - Analyst insights and confidence
    - Associated indicators of compromise
    - Associated threat actors, campaigns, and Tools, Tactics, Procedures (TTPs)
- Geo blocking – If the IP address is in another country, geo blocking can block it (unless it's a country or region for business)
- Threat intelligence sharing – The ability to contact trusted partners when suspicious observables are identified can be invaluable. When carrying out supply chain attacks, threat actors will often target multiple organizations using the same methods. Multiple sightings of suspicious observables in a particular business vertical can be an indication of just such an attack

Third-party palooza – the Minus Touch

2018 Data Breach Digest

verizon✓

The situation

We handle a lot of forensic evidence at the VTRAC | Labs and process it quickly because the VTRAC | Investigative Response Team investigators eagerly awaits it, ready to pore over the system images and associated volatile data.

One Tuesday morning, the investigators were especially anxious. The start of a new investigation had been delayed because the customer's data was hosted at a co-location data center. They had to wait for the data center's "hands team" to connect hard drives to the in-scope servers for data collection.

Several days passed before the VTRAC investigators received a call that the imaging had completed. An additional day passed before they received a tracking number for the evidence shipment via courier.

Finally, we were notified that the evidence shipment had arrived. We retrieved the package from the courier, completed the chain-of-custody and inventory record, and connected the drive for staging. After connecting the drive, we found it contained no data!

So what happened?

Mitigation tips

- Keep an inventory of all assets; document and label systems in remote locations
- Maintain an updated contact list for any co-location services providers
- Test and validate Incident Response (IR) procedures; include co-location services providers

Investigative response

A few days prior, during the engagement scoping process, the VTRAC investigators learned the in-scope servers were housed in a co-location data center. We offered to send investigators onsite for collection. However, the co-location services provider, as a matter of policy, prohibited our access. We were forced to rely on their local team for collection.

Though generally simple, some co-location data centers are well-equipped to handle these requests while others struggle to coordinate with the folks on the ground. There's often no documented process to convey which servers need to have hard drives connected to them, or which physical appliance is hosting a virtual machine.

For this situation, the customer was sharing a physical system with other customers which could prevent the ability to image the drive at all due to commingled customer data.

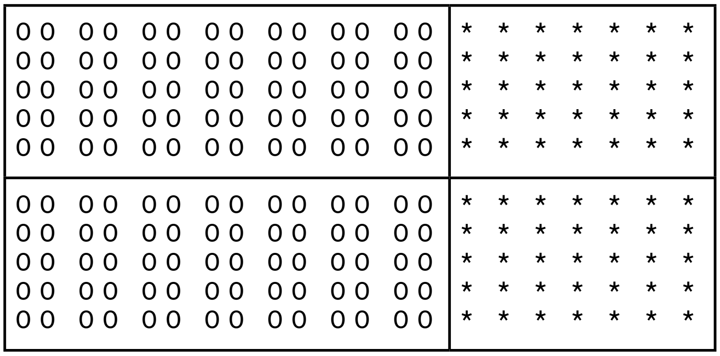
Co-location data center considerations

Accessing data in co-location data centers should be planned well ahead of time. Some of these investigative planning are:

- Know which co-location data center has the in-scope evidence. When using multiple co-location data centers, knowing exactly where your systems, memory, logs, and data is can reduce evidence collection and preservation time
- Know who does what. Not knowing who does what in a data breach causes confusion and wastes valuable resources. Consider using a RACI matrix for stakeholder tasks
- Know who can physically access the systems in the co-location data center. Working through authorization to gain access to your data storage during a cybersecurity incident introduces unnecessary delay
- Know how to and collect the data at the co-location data center. Understanding and testing the evidence collection process ahead of time reduces evidence collection acquisition delays

Response tips

- Integrate third-party contact procedures into the IR Plan; periodically test contact and escalation procedures prior to cybersecurity incidents occurring
- Use co-location services providers with first responders experienced in collecting digital evidence
- Require and validate co-location services providers allow access to digital evidence, to include systems and network logs, quickly



```
00 00 00 00 00 00 00 | * * * * * * *
00 00 00 00 00 00 00 | * * * * * * *
00 00 00 00 00 00 00 | * * * * * * *
00 00 00 00 00 00 00 | * * * * * * *
00 00 00 00 00 00 00 | * * * * * * *
--------------------------------------
00 00 00 00 00 00 00 | * * * * * * *
00 00 00 00 00 00 00 | * * * * * * *
00 00 00 00 00 00 00 | * * * * * * *
00 00 00 00 00 00 00 | * * * * * * *
00 00 00 00 00 00 00 | * * * * * * *
```

Figure 1. “Zeroed-out” hard drive sectors

An additional day’s delay occurred when the co-location services provider requested that our customer provide the collection drives. This required our point of contact to scramble to arrange one-day shipping.

The customer reported no issues with the collection process or with the instructions for encrypting the collection drives prior to shipping to our labs. Still, when we mounted the evidence drives and discovered they were empty, we were shocked.

Typically, an encrypted drive presents itself in one of two ways. If an encrypted container has been used, the file is within the image. If the entire drive is encrypted, the Microsoft Windows operating system will indicate it must be initialized.

Another, less common situation involves one of multiple encrypted partitions, in which case the disk appears initialized but the data is not accessible. Neither thing occurred here.

Suspecting there might be a separate disk partition or some other encryption method involved, we examined the disk with one of our forensic tools. Unfortunately, the hard drive sectors only contained the hexadecimal character “00” which meant it housed no data. We immediately contacted our customer’s point-of-contact to figure out what happened.

Our contact explained that the person responsible for making the shipment initially claimed they’d followed our collection and shipping instructions. However, after some additional probing they admitted consolidating all the data on to a single drive. We never learned exactly why they did this but in doing so, they must have somehow not actually copied the data to the drive. The next day, we received the correct drives in evidence bags and with the chain-of-custody completed. This was a costly lesson as it took several days for the collection effort to begin. The hosting provider’s missteps in collecting the evidentiary data further delayed the commencement of our investigation and disrupted our customer’s business.

Lessons learned

During the engagement, the customer questioned their decision to move their data to a co-location data center. They moved this data without a firm understanding of how relevant data would be collected and without having a solid procedure in place for obtaining the data.

Mitigation and prevention

- Keep an inventory of all assets; document and label systems in remote locations
- Maintain an updated contact list for any co-location services providers
- Test and validate Incident Response (IR) procedures; include co-location services providers

Detection and response

- Use co-location services providers with first responders experienced in collecting digital evidence
- Integrate third-party contact procedures into the IR Plan; periodically test contact and escalation procedures prior to cybersecurity incidents occurring
- Require and validate co-location services providers allow access to digital evidence, to include systems and network logs, quickly

PoS intrusion – the Faux PoS

2018 Data Breach Digest

verizon✓

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.

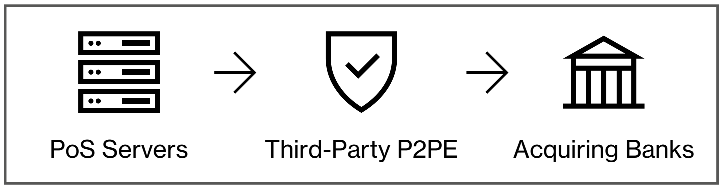


Figure 1. Payment card transaction flow

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.

Detection tip

Conduct proactive network and endpoint based threat-hunting exercises to detect and respond to unknown threats.

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?"

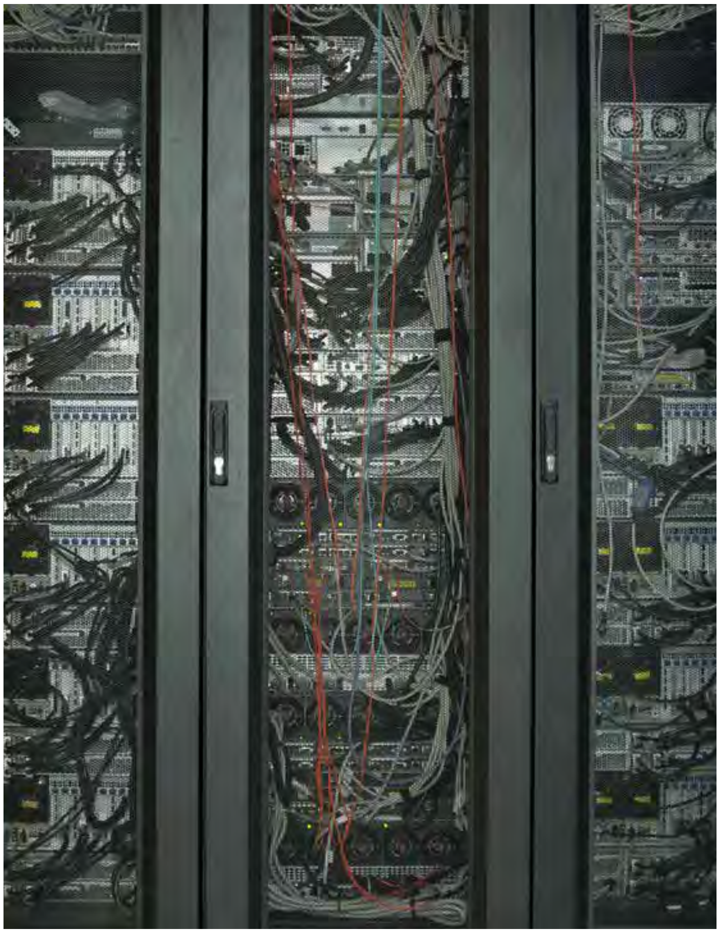
Investigative response

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 necessary 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.



Top five victim-controllable investigative challenges II: Return of the top five victim-controllable investigative challenges!

Two years ago in the 2016 Data Breach Digest – Scenarios from the Field, we presented a sidebar on the “top five victim-controllable investigative challenges.”

These are still as they were in 2016, so here they are again:

- Logs, logs, logs – specifically, the non-existence of, not enough of (rolling over too quickly) or difficulty in locating/retrieving promptly
- Network topologies – the lack of or the severely out of date
- Baseline images and trusted task lists – the lack of, the inaccuracy or the out of date
- “Dual-use” tools (for example, PsExec) – left on the system prior to its breach (and no, storing them in the Windows Recycler is not a security option), or no detection of their use
- Self-inflicted anti-forensics – rebuilding systems and then calling us, containing and eradicating but not properly documenting, pulling the power cable and not the network cable, the infamous ‘quick look’ by an unqualified IT Team member, etc.

Response tips

- Create Incident Response (IR) playbooks to supplement the IR Plan; educate first responders on the importance of effective and timely incident response
- Review network and application logs; review logs related to compromised systems or user accounts to determine other affected assets

Mitigation tip

Establish and implement system-hardening baselines; conduct thorough vulnerability assessments at least quarterly and penetration testing exercises at least annually.

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.

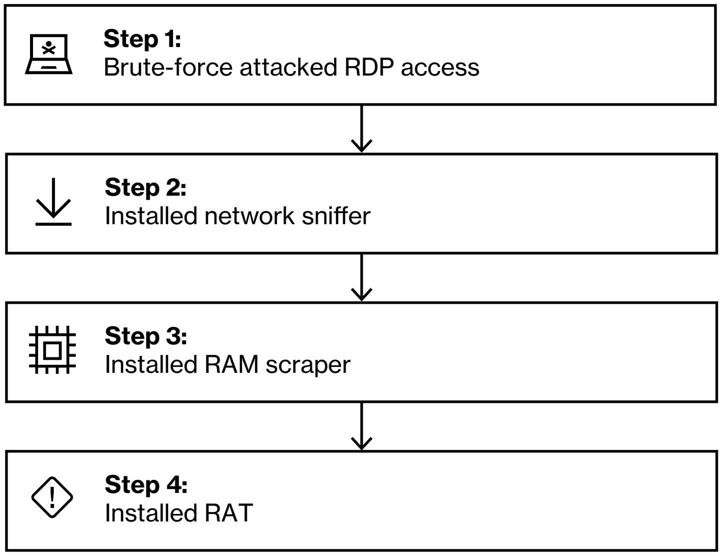
Based on the forensic analysis of the available evidence sources, coupled with an understanding of the payment card data transaction flow and the CPP analysis, it was confirmed that a data breach had occurred.

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.

PCI PAN and track data defined

The PCI Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA-DSS) Glossary of Terms, Abbreviations, and Acronyms, version 3.2, includes these definitions:

- PAN (Primary Account Number) – Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account
- Track Data – Also called "full track data" or "magnetic-stripe data." Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. Can be the magnetic-stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe



Step 1: Brute-force attacked RDP access

Step 2: Installed network sniffer

Step 3: Installed RAM scraper

Step 4: Installed RAT

Figure 2. Third-party server attack stream

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 multi-factor 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.

Mitigation tips

- Implement MFA for all non-console access to systems
- Monitor and assess third-party's PCI DSS compliance status risk ongoing

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

eCommerce breach – the Flutterby Effect

2018 Data Breach Digest

verizon✓

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 non-production 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.

Detection tip

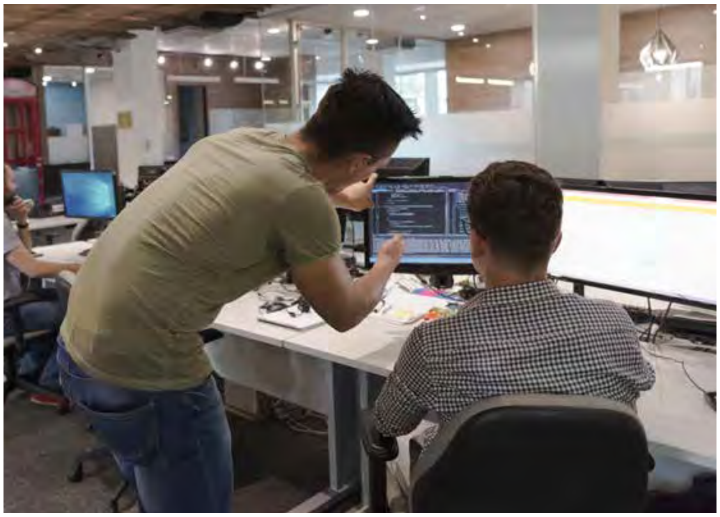
To proactively discover undetected code modifications, regularly perform integrity checks on sensitive code; implement tools to track and monitor website changes.

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.

Mitigation tip

Assess the complete payment process (and not just the P2PE solution); implement further controls with a defense-in-depth approach.



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.

Mitigation tip

Implement system-based controls to help prevent unauthorized access; make it a policy and practice to use admin accounts only when needed.

Detection tip

To help detect unusual privileged account activity, periodically review logs of accounts accessing critical and sensitive systems.

eCommerce cybersecurity trends

Today ecommerce sees a variety of cyber-attacks from a variety of sources. This is a challenge for cybersecurity professionals tasked with protecting their customer data and their company reputation. Some of the cybersecurity threats facing ecommerce include:

- DDoS attacks – Distributed Denial of Service (DDoS) attacks can be targeted or indiscriminant. Attacks against services used by ecommerce companies can disrupt services. This was the case in 2017 when DynDNS was “DDoS’d” disrupting service for Etsy, Shopify, Twitter, PayPal, and Pinterest
- Digital malware over HTTPS – Although protecting customer and payment card data on e-commerce platforms using Secure Sockets Layer / Transport Layer Security (SSL / TLS) encryption is nothing new, cybercriminals have taken advantage of these encrypted channels to move their malware. Faced with this challenge, ecommerce entities have implemented deep-packet inspection firewalls to thwart cybercriminals from using these channels
- APT targeted phishing – Advanced Persistent Threat (APT) phishing emails to trick employees into downloading malware are a common APT tactic. Once an attacker gains access, data theft, fraud, and other activities can last for an extended period. Much worse than a single fraudulent payment, unauthorized access to admin account credentials used for e-commerce platform management can lead to massive data theft and monetary loss

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 that 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). Some of the top takeaways from our AAR are:

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; implementing tools to track and monitor website changes
- Help detect unusual elevated account activity by periodically reviewing logs of accounts accessing critical and sensitive systems

False alarm – the Exposed Flank

2018 Data Breach Digest

verizon✓

The situation

I've been an Information Technology (IT) Security manager at my company for several years now. A few weeks ago, we experienced a Denial of Service (DoS) attack. Thousands of domain user accounts had been locked out due to password related logon failures.

The IT Help Desk had been receiving a high call volume from employees to unlock their domain user accounts. Sometimes, the accounts had been getting locked again within a day or two of being unlocked.

This issue couldn't have come at a worse time. The majority of my IT Security team was on vacation due to the upcoming holiday weekend.

Upon initial review, our Incident Response (IR) Team determined the logon failures generating the lockouts across our domain controllers were originating from a yet to be identified system. My team informed me that their review of the Microsoft Windows Security Event logs on the domain controllers revealed the logon failures were associated with Windows PowerShell commands containing Base64 encoded arguments.

With limited staffing, we couldn't immediately pinpoint the root cause. I was forced to call back my network admins from vacation to investigate. We also triggered our retainer service with the VTRAC | Investigative Response Team to assist with any "deep-dive" aspects of the investigation.

Mitigation tips

- Modify account password lockout policy to be more realistic – trigger an account lockout after five failed password attempts within 30 minutes
- Create an Intrusion Prevention Solution (IPS) rule to identity multiple failed privileged account requests within short timeframes
- Notify certain key IT Security Team members before any penetration testing or security assessment activities occur
- Update user account policy to explicitly require network admins only use admin accounts with Two-Factor Authentication (2FA) for performing specific tasks requiring elevated privileges, and non-elevated privileges for normal workday activity

Investigative response

After arriving at our data centers, the network admins and VTRAC investigators correlated the Windows Security Event logs with other network logs to identify the root cause associated with the anomalous PowerShell activity.

The VTRAC investigators quickly triangulated the source to a strangely named system that didn't follow our standard naming convention. We couldn't immediately identify the system location as our network diagrams hadn't been updated in years. Further inquiries led the investigators to find this system was assigned to a third-party penetration testing vendor.

From conversations with the pen testers, we learned that they had made several attempts at one-off password guessing against approximately 10,000 user accounts from Tuesday to Thursday of that week. On a call with the Microsoft Active Directory Team, we also learned the account lockout policy was set to three failed attempts during a 48-hour period.

During their test, the pen testers assumed a few guesses over the 48-hour timeframe would be acceptable for most account lockout policies. Unfortunately for us, they assumed poorly.

Based on the account lockout policy and the log data we reviewed, we concluded the password guessing by the penetration testing system resulted in the account lockouts. In reversing the Base64 encoded commands, the VTRAC investigators identified the specific accounts being locked out.

During the analysis, we also discovered a user account with elevated privileges had accessed the production environment for standard tasks not requiring elevated privileges. This was something we addressed by making it policy for network admins to use admin accounts only when specifically needed to perform tasks requiring elevated privileges.

Measuring incidents and response

Metrics can track and convey incident occurrences and response activities for senior management. These metrics can then highlight cyber-attack trends, the need for additional resources, training gaps, etc.

Some metrics also serve for establishing Key Performance Indicators (KPIs) for measuring incident response performance against key business objectives as part of the overall cybersecurity strategy for an organization.

Examples of cybersecurity incident and response metrics are:

- # Incidents / Year – the total incidents per year
- # Incidents by Type / Year – the total incidents by category (priority, impact, urgency) per year
- # Hours / Incident – the total resolving incident and incidents handled within the Service Level Agreement for that incident
- # Days / Incident – the total spent resolving incident
- Monetary Cost / Incident – the total estimated monetary cost per incident, to include containment, eradication, remediation, and recovery, and collection and analysis activities
- # Systems Affected / Incident – the total affected per incident

Response tips

- Update contact roster for all critical IT / IT Security Team members; require first line supervisors provide a weekly status update of employee availability to the IT Security Manager on duty
- Implement a Security Information and Event Management (SIEM) solution to manage real-time analysis of software and hardware generated security alerts
- Update network diagrams and asset inventories periodically or whenever network infrastructure or components change

Lessons learned

Immediately following the incident, my IR Team and I compiled a list of observations and associated action items as part of the lessons learned.

Mitigation and prevention

Observation If we had a better password lockout policy, the penetration test wouldn't have triggered this false alarm.

Action item We modified our account password lockout policy to lockout after five failed password attempts within 30 minutes. We also created an Intrusion Prevention Solution (IPS) rule to identity multiple failed privileged account requests within short timeframes.

Observation We realized that if our IT Help Desk receives user account lockout notifications, not all IT Security Team members know of penetration testing activities.

Action item We implemented a requirement to notify certain key IT Security Team members (i.e., those who aren't being "tested") before any penetration testing or security assessment activities occur.

Observation During the analysis, although not directly related to the incident, we discovered a user account with elevated privileges had accessed the production environment for tasks not requiring these privileges.

Action item We updated our user account policy. We now explicitly require network admins only use admin accounts with Two-Factor Authentication (2FA) for performing specific tasks, and non-elevated privileges for normal workday activity.

Detection and response

Observation At a key point in time, we needed to call back several network admins from vacation. Not having an updated contact roster contributed to delays in recalling employees

Action item We updated our contact roster for all critical IT / IT Security Team members. We also made it a requirement for first line supervisors to provide a weekly status update of their employee availability to the IT Security Manager on duty.

Observation We rely on Windows Security Event logs to create an audit trail; however, we didn't configure our systems consistently across the board to capture the data fields for logons.

Action item We evaluated a Security Information and Event Management (SIEM) solution to aggregate system logging and other security sources of information. This will allow us to better manage analysis of software and hardware generated security alerts.

Observation Because our network diagrams and asset inventory hadn't been updated in years. Given the DHCP IP address leasing, it took hours to locate this system.

Action item We made it a requirement to update our network diagrams and asset inventory through periodic reviews or whenever the network infrastructure or its components change. This will give us the ability to quickly identify asset custodians and owners.

ICS attack – the Eclectic Slide

2018 Data Breach Digest

verizon✓

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 (LE) 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 LE 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.

Response tips

- Increase logging and alerting for configuration changes, to include user account creation and modification; enable enhanced logging for PowerShell script triggered actions
- Establish a method for reliable, secure, alternative communications before a cybersecurity incident occurs; incorporate this into the Incident Response (IR) Plan

Traffic Light Protocol (TLP) categories

- TLP Red is the highest and most restricted; its disclosure is highly restricted on a need-to-know individual basis
- TLP Amber is the second highest; its disclosure is restricted individuals and/or organizations
- TLP Green is the third highest; its disclosure is restricted to the community on a need-to-know basis
- TLP White is the least restrictive; it has no disclosure restrictions and can be released to the public community

More information regarding the TLP definitions and usage can be located on the US-CERT web site by using this URL https://www.us-cert.gov/tlp

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 that 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.

Mitigation tips

- 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

Response tip

Comply with industry training and certification requirements; familiarize SOC analysts and incident responders with the ICS environment; train them to respond to ICS related cybersecurity incidents.

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 the following 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

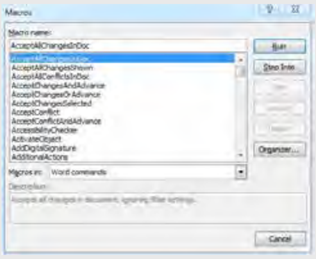
A deeper look into macros, hyperlinks, and processes

Microsoft Word macros

Macros are features grouped together to automate common tasks.

Threat actors use the macros functionality to run malware on systems.

From a cybersecurity standpoint, consider disabling or limiting the use of macros.



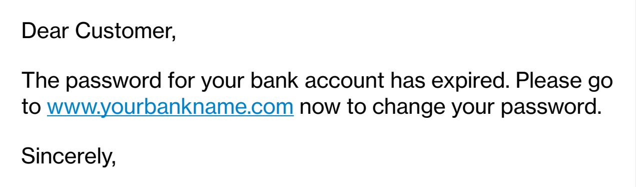
Macro name: AcceptAllChangesInDoc

Macros in: Word commands

Description: Accepts all changes in document, ignoring filter settings.

Website hyperlinks

Hyperlinks, or links, allow documents, web pages, emails to connect with a simple mouse click.

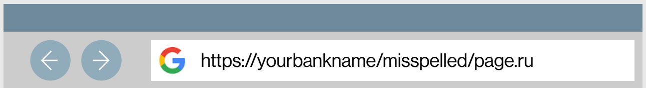


Dear Customer,

The password for your bank account has expired. Please go to www.yourbankname.com now to change your password.

Sincerely,

Threat actors use hyperlinks to track users into "clicking" and inadvertently installing malware.



https://yourbankname/misspelled/page.ru

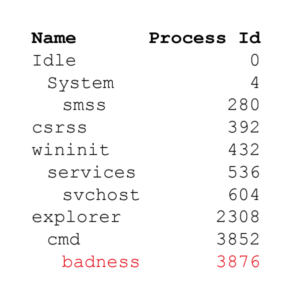
Hover your mouse pointer over an email link to see the actual website. Check to see if the domain name matches.

Running processes

A process is an instance of an application executing. A "spawned child process" is created by another process (a "parent process").

When malware runs on systems, a process is created.

Examine suspicious processes by looking at the surrounding context: time, parent or child processes, the application itself.



```
Name          Process Id
Idle                   0
  System               4
    smss             280
csrss                392
wininit              432
  services           536
    svchost          604
explorer            2308
  cmd               3852
    badness         3876
```

verizonenterprise.com

Digital hijacking – the Crossed Wires

2018 Data Breach Digest

verizon✓

The situation

These are the times that try men's souls, and those of their Human Resources (HR) Department. Shadowy figures consort to defraud the everyman. Are they outside or inside the tent? Who can help keep your ducks in a row and safe from a wolf in sheep's clothing? In a world where everyone could be on the take, something's gotta give...

Monday...
Alice could smell trouble when the lift doors opened, and it was heading her way. Bob, the Chief Financial Officer (CFO), was walking with purpose yet she could see a bitter resignation in his posture.

"Alice, we've got a problem." As the HR Department Head for Wallaby Suds for Duds (WSD) Pty Ltd, Australia's leading laundry soap company, this conversation opener was depressingly common. "Two hundred large just walked out the door. Records show it was paid out in a wire transfer along with a photocopier repair contract."

"I know those photocopiers take a beating at the best of times, and the end of year party is coming up, but $200,000?! That's just unreasonable."

"This is serious, Alice. It's obvious someone's had their hand in the cookie jar and we don't know who. All the instructions were electronic and our bank paid it straight out. It was withdrawn the same day in cash and is gone for good. Untraceable, they say. I've emailed you the details."

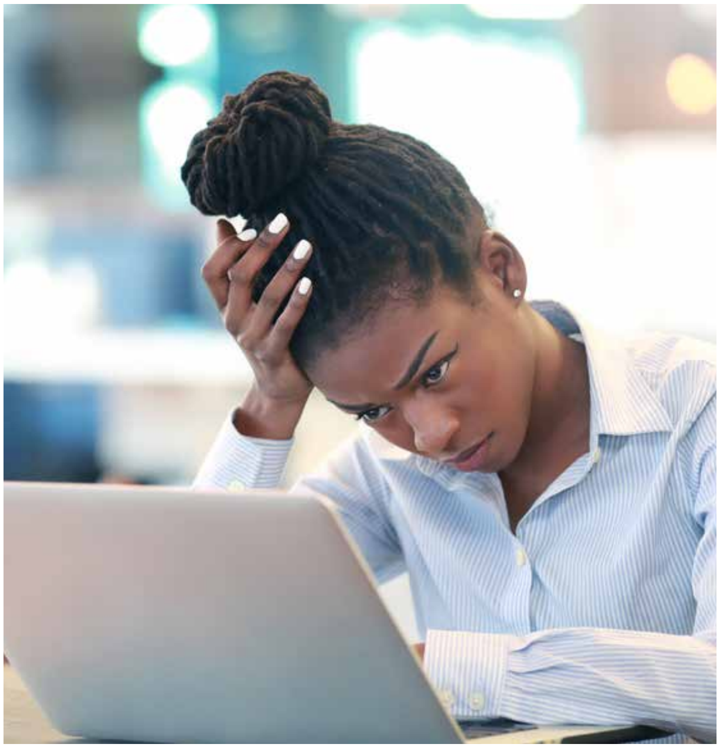
"Accounts Payable still party like it's 1999, do they even have computers down there?" Alice said, noticing a slight glare in Bob's eye. "Oh, don't look at me like that. You can count on me, Bobby. I'll figure this one out, just like I always do."

"Listen Alice, if there's a bad apple in Accounts Payable turning the milk sour I don't want the boys upstairs to be left with another bad taste in their mouths. You know what I'm saying?" An unseasonably cold rain lashed the windows of Alice's office as she saw Bob out. Returning to her office, she sank back into her office chair. It was going to be a long week.

Detection tip

If this was your organization you could contact your IT team and access your up to date, all-encompassing asset register to work out what was is use by Accounts Payable staff. You have one of those, right?

Don't be seduced by the latest Artificial Intelligence-backed software fad or security hardware innovation until you've got the basics right. These include network segregation, user privilege limitations, asset registers, and software patching.



Investigative response

Alice knew she needed to act fast. WSD took security seriously. She recalled from a data breach simulation exercise that the first step was to secure the evidence. Luckily, for Alice, WSD had an established Incident Response (IR) Plan; she was able to quickly run through a checklist of what to get and who to contact.

With the threat actor a potential insider, the first priority was to collect any evidence still in the finance employee's possession. This had to be done quietly, so as not to tip off the employees to the investigation.

One phone call to the IT Department later and the finance laptops were retrieved for "software updates." The laptops were lined up for forensic imaging. For those still powered on, the IT Security Team dumped memory for evidence of on-going activity that hadn't been written to disk. In following their incident checklist, the IT Team was able to quickly collect the data and have the laptops back in place before the first employees arrived the next morning.

Besides the laptops, the IT Team collected network log data. Log data associated with the suspected user systems was exported and marked for analysis. Leaving no stone unturned, Alice even requested the Microsoft Exchange mailboxes be duplicated and reviewed (in the event the insider had an outside contact).

Alice ran a tight ship, but this was an unforeseen iceberg. With losing this kind, she knew it was time to call in the experts. Her staff was well trained as first responders; however, they'd need impartial analysis for any prospective court case. Two hours and a scoping call later, the IT Team encrypted and copied the items requested by the VTRAC | Investigative Response Team for their analysis.

Response tip

Situations like this are stressful for everyone involved. Put in place plans and procedures to collect electronic evidence, and test these periodically as part of a data breach simulation or disaster recovery exercise.

Planning and rehearsal is key to handling incidents correctly. It allows an organization to:

- Maximize electronic evidence availability
- Minimize evidence preservation time
- Improve efficiency by assigning stakeholder roles and responsibilities
- Identify and resolve security posture weaknesses

Wednesday…

While the forensic analysis was underway, Alice concentrated on her favorite part of an investigation: shaking the tree branches to see what fell out. Her fun was short-lived however. She made little progress in identifying anything out of place and none of her employee interviews turned up insight into suspicious activity.

"Either this person is very clever, or it isn't an inside threat," Alice thought to herself on her way to Bob's office. Debriefing him on the day's interviews brought no smile to his face.

"I thought you said you would handle this Alice," Bob remarked sternly.

"I've been working on it, but I am beginning to think we might not be looking at an insider here. I think we need to consider other possibilities."

Bob's face sunk into a frustrated scowl, "Listen. There is no way that money left without someone being directly involved. I'd bet my job on it! Now go find me that person."

As Alice slipped away, she knew she must find a different approach. Either the interviews weren't working or Bob was missing something and she had to discover which. She pulled out her phone and typed a quick email to the security expert reviewing the evidence. "Got time for a call tomorrow? We need a status update."

Minutes later, she received a response with a time and conference bridge number. "Now maybe I'll get some answers," Alice muttered, as she headed home to drink her favorite Scotch and gaze out through her venetian blinds into the seemingly endless rain.

Thursday…
Alice's phone rang; it was the forensics expert. As luck would have it, Bob was passing by and had just popped in. Listening in he gathered everything he needed from what he could hear:

"Yeah fine thanks"…"Unlikely it was an inside job at all?"…"No, what's whaling?"…"Don't be cute kid, I know whales are like big fish"…"What was he in the middle of?"…"oh, right"…"and Bob emailed the accounting package update? Brilliant! I look forward to reading the report."…"Thank you, good bye."

"You can't think I had anything to do with this?!," Bob spluttered.

"Relax Bobby, you're off the hook. So is the team. It was someone else, a man-in-the-middle."

Alice continued on, explaining that two weeks prior an attacker had forged an email to look like it came from Bob. That email instructed the Finance Team to install a patch for the accounting software they used. This update claimed to "add in support for the Euro symbol so we could buy cheaper highlighters from Poland."

"That's crazy!" exclaimed Bob.

"I know, you'd think a group of professional accountants would know they stuck with the Zloty. Anyway, don't interrupt…" Alice decided to stop teasing Bob and proceeded to explain how the attackers did it.

"It was malware. What they thought was a patch actually routed their internet traffic through a server controlled by the attackers allowing them to continue using whatever website your team was using without anyone noticing. If one bank account and sort code gets changed after you think you've logged out, who's going to notice? Anything they typed into the computer was saved for good measure, too."

Once Bob had grasped what had happened they formulated a response. The money was gone – that would not change – but something needed to.

Mitigation tip

Attackers find weakness in organizations' processes and their computers. For example, does your finance team check account details before payment approval, or do they just the payment amount?

Work with your security team to mitigate specific risks to your business. These may include data breaches, employee misconduct, business interruptions, and fraudulent activity.

Two weeks later
Application whitelisting had been deployed to prevent unapproved software from being executed. Internet access was now routed through a proxy server that blocked unknown websites for privileged users, such as administrators and the Finance Team.

The email clients had been patched to mitigate recently discovered vulnerabilities allowing easily spoof emails. The servers reconfigured to enable Domain-based Message Authentication, Reporting and Conformance (DMARC) to add authentication of email senders.

The text '[EXTERNAL]' was also added to any email subject line sent from outside the company to make it even easier to spot spoofed emails, and Alice had finally received funding to roll out mandatory phishing awareness training to all employees.

A "red team" exercise had also been booked to test the new and improved WSD security regime for weaknesses to other types of attack. They'd find a way in, they always did, but between Alice, the IT Team, and the security contractors, together they'd work to mitigate the risk.

Lessons learned

Procedural controls should complement technical controls when securing your business.

Mitigation and prevention

- Work with your security team to mitigate specific risks to your business. These may include data breaches, employee misconduct, business interruptions, and fraudulent activity

Detection and response

- Don't be seduced by the latest Artificial Intelligence-backed software fad or security hardware innovation until you've got the basics right. These include network segregation, user privilege limitations, asset registers, and software patching
- Planning and rehearsing is key to handling incidents. It allows an organization to:
  - Maximize electronic evidence availability
  - Minimize evidence preservation time
  - Improve efficiency by assigning stakeholder roles and responsibilities
  - Identify and resolve security posture weaknesses

Social engineering – the Spiked Punch

2018 Data Breach Digest

verizon✓

The situation

It began on a Monday morning in February. It was like any other day in the Finance department: a team meeting, weekly task list, and a mountain of emails within my inbox. In that pile, I came across what appeared to be a standard email from a long-time vendor.

This email was like many I'd received and actioned every day. It requested a payment and contained a company invoice with bank information for a wire transfer.

I looked at the banking information and noticed that the account was not in our system. With all due diligence, I replied to the requester requesting information. They explained that the account belonged to a subsidiary of the vendor and they supplied me with a stamped letter of authorization. The sender also requested an email confirmation when the transfer occurred.

This wasn't unusual as vendors often requested modifications to invoices. With a volume of similar transactions to plow through, I barely gave it a second thought.

On the day of the transfer, I sent a confirmation email to the requester. A short while later they replied indicating that the bank had received the transfer, but due to "in-country terrorism concerns" the money would be returned.

The requester then asked if I could resubmit the payment but split it into four equal payments. Not wanting to be late, I wasted no time in resubmitting the transfers. They thanked me for my customer service and professionalism.

Mitigation tips

- Review sender email addresses and domains; look for misspellings; confirm emails originate from official corporate customer addresses
- When in doubt, pick up the phone and verify customer requests; confirm requesters are approved vendor contacts through a supplier master repository database; confirm money requests through independent channels other than email

Investigative response

The next day the VPs of Finance, IT Security and Legal called me into an urgent meeting. Before I could even take a seat, they asked "why did you transfer money to a non-approved account? What possessed you to resubmit the transfer into four separate transactions?"

I sat up straight and explained the events leading to the transfers. Less than a minute into my explanation, I was cut-off. It was explained that I was involved in a confidence trick and that I had fallen prey to a fraud, potentially costing the company hundreds of thousands of dollars.

The barrage of questions came thick and fast. They wanted to know why I hadn't validated the email address, how I'd missed the email domain being misspelled by one character, why I hadn't validated the request with a co-worker or matched the invoice to the packing slip and purchase order.

The sender had obtained valid account information along with an "official" looking letter from a parent company we do business with. I later discovered that one of our third-party vendors used a personal web email account to conduct business with the Accounts Payable team. That personal account had been hacked.

The fraudster obtained information from previous email correspondence regarding our internal processes and contact information for payment requests. With this information they created an email address mimicking the legitimate third-party vendor's email. It was misspelled by one character.

Mitigation tips

- Segregate duties: a junior employee sets up the wire transfer and a senior employee reviews and approves the transfer
- Implement internal controls for matching packing slips and purchase orders to payment invoices
- Implement a vendor management policy requiring vendors use a secure corporate email system; prohibit using personal web mail accounts for business

Phishing email indicators

- Examine the sender email address; look for typos or mismatched email domain names
- Examine the email message; look for misspellings; be cautious of requests for "urgent" or "immediate" action
- Be cautious of embedded hyperlinks; hover your mouse over link to reveal domain name

BALANCE OVERDUE!

Kimberly Jones <kjones@spoofedemailaddress.com>

Sent: Mon 10/17/2018 5:09 PM

To: Smith, John

Cc:

Dear Mr Smith,

Payment for invoice #4327394 is over 90 days late. Please click here to pay now and avoid being sent to collections.

Regards, Kim Jones

Account Representative

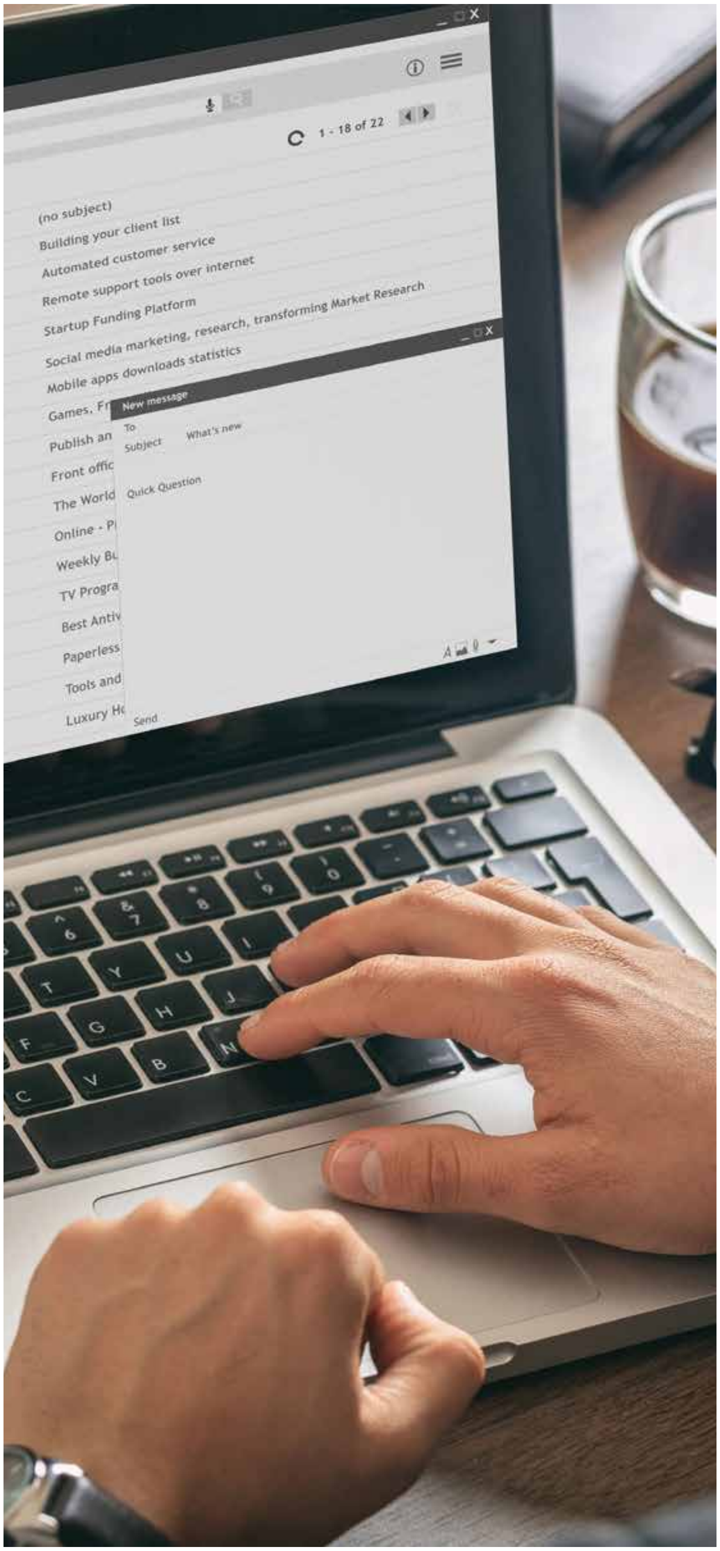
Lessons learned

When the dust settled, we had an email invoice payment request gone bad, large sums of money transferred to a bank account, and an Accounts Payable employee left wondering what went wrong.

Just like the money, I wished I could just vanish. This incident taught us several valuable lessons which we took action on right away:

Mitigation and prevention

- Review sender email addresses and domains; look for misspellings; confirm emails originate from official corporate customer addresses
- When in doubt, pick up the phone and verify customer requests; confirm requesters are approved vendor contacts through a supplier master repository database; confirm money requests through independent channels other than email
- Segregate duties: a junior employee sets up the wire transfer and a senior employee reviews and approves the transfer
- Implement internal controls for matching packing slips and purchase orders to payment invoices
- Implement a vendor management policy requiring vendors use a secure corporate email system; prohibit using personal web mail accounts for business


1 - 18 of 22
(no subject)
Building your client list
Automated customer service
Remote support tools over internet
Startup Funding Platform
Social media marketing, research, transforming Market Research
Mobile apps downloads statistics
New message
To
Subject
What's new
Quick Question
Send

Telephonic pretexting – the Double Fake

2018 Data Breach Digest

verizon✓

The situation

It was like any other day at the IT Help Desk. We were dealing with cases of "slow computers," [re]installing applications and assisting with email connection troubles. It was a fairly normal day until our IT Security Director and the VTRAC | Investigative Response Team gave me a call.

They were investigating a cybersecurity incident involving a senior executive. The executive's account had been disabled and flagged for suspicious activity due to numerous account lockouts and password resets. The Microsoft Active Directory logs indicated the password resets were initiated by folks on my team.

As the IT Help Desk Manager, they needed my assistance with tracking down tickets associated with the password resets.

Detection tip

Create and monitor alerts related to abnormal authentication events, such numerous password resets in a short while and access from foreign sources.

Mitigation tip

Use multi-factor authentication for accessing sensitive resources, such as VPN or email from external sources.

Investigative response

The search associated with the executive's user account over the last week revealed three tickets related to password resets and help accessing our VPN client. Two were calls into our hotline and one was from a walk-up to our in-office window. Luckily, we record all calls into our IT Help Desk hotline.

In listening to the recordings, it became obvious that the person calling the IT Help Desk hotline was not this senior executive. I knew this because I'd worked with them for years, but our analysts wouldn't have recognized their voice.

The caller even had information that helped them bypass some of our cybersecurity measures! I'll summarize each call:

Pretexting call #1

The first pretexting call into our hotline was fairly straightforward.

1. A frantic voice indicated that they were having trouble with email on their phone and had forgotten what username to use. They provided the senior executive's name and title
2. The IT Help Desk analyst then asked the security question on file: "Where did you go to college?"
3. The unknown individual paused for a second (as if they were looking up the information), and provided the answer hesitantly
4. "Correct!" exclaimed the IT Help Desk analyst, and they provided the senior executive's username
5. The caller thanked the IT Help Desk analyst for the information and ended the call

Pretexting call #2

Two days after the first call, the second pretexting call came from an individual called in claiming they needed help with installing the virtual private network (VPN) client and accessing their email.

1. Again, they claimed to be the senior executive and provided their name, title, and username. Having this extra piece of information they skipped the security question
2. Our IT Help Desk analyst then remotely accessed the unknown individual's "home" computer system, installed the VPN client, "reminded" the individual of how to log into the email portal
3. However, that logon failed and since the unknown individual "forgot" their password, the IT Help Desk analyst was happy to reset it for him, giving the unknown individual access

Remember that walk-up to our internal in-office window? That was the actual senior executive walking over because they could not log onto their system after an unknown individual reset their password. Unfortunately, that raised no red flags.

Ultimately, the investigation revealed an unknown individual gained access to the senior executive's email account and stole confidential corporate financial data and business strategy documents via the executive's compromised user account.

Response tip

Consider non-standard evidence sources, such as IT Help Desk tickets, call recordings, and employee interviews.

Mitigation tip

Provide end user and IT Help Desk personnel with awareness training that focuses on technical, and non-technical cybersecurity threats, such as social engineering tactics.

Lessons learned

Using social engineering tactics, an unknown individual gathered enough information to gain access to the sensitive information of one our senior executives.

Mitigation tip

Implement strong verification controls unassociated with easily determined information; limit personal information posted in public forums.

Our authentication security questions shouldn't be connected to information easily obtained in the public forum such as on a popular professional networking website.

We also needed a process for flagging and investigating numerous password resets over a short period. This may have helped us identify the cybersecurity incident earlier.

Response tip

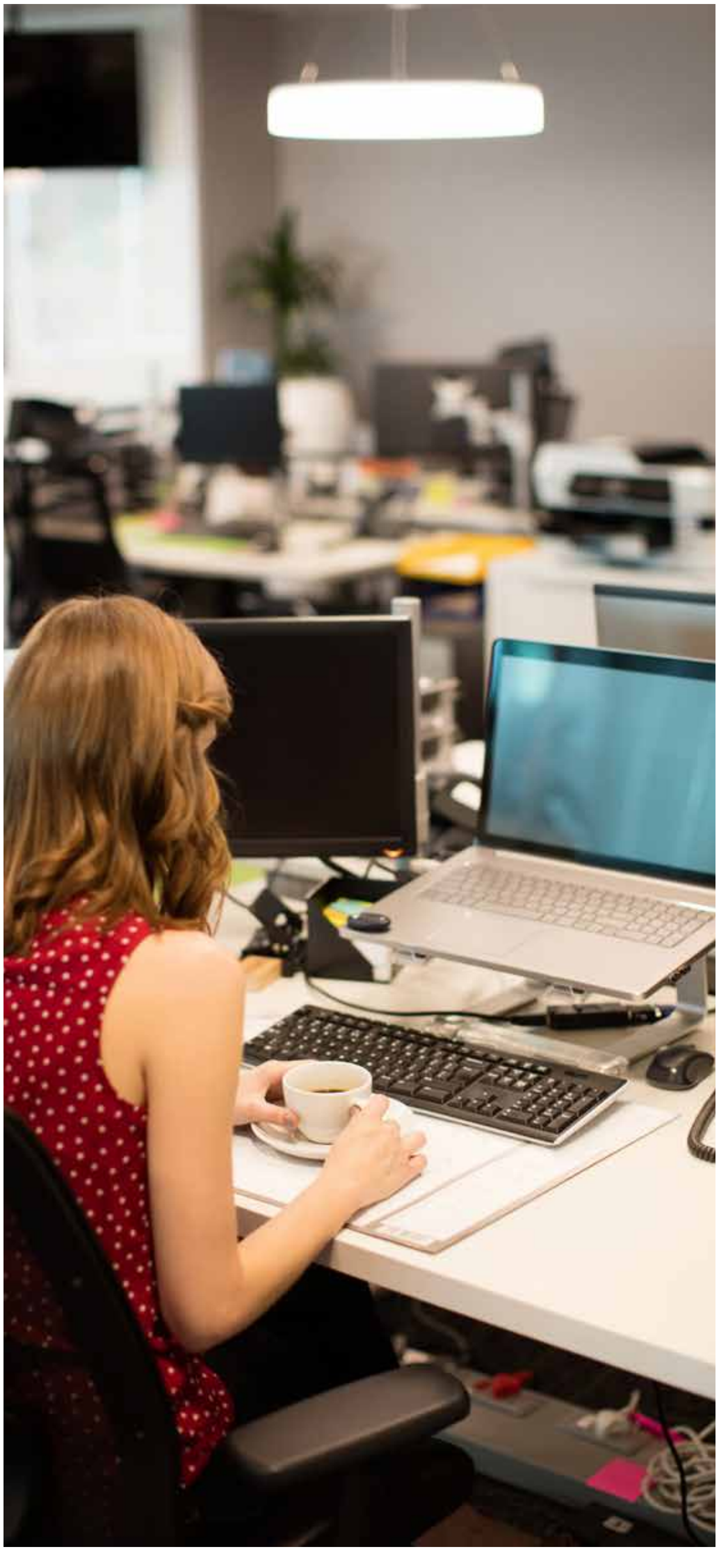
Track cybersecurity events and incidents for resource allocation; use key performance indicators (KPIs) to measure IR effectiveness.

Mitigation and prevention

- Use multi-factor authentication for accessing sensitive resources, such as VPN or email from external sources
- Provide end user and IT Help Desk personnel with awareness training that focuses on technical, and non-technical cybersecurity threats, such as social engineering tactics
- Implement strong verification controls unassociated with easily determined information; limit personal information posted in public forums

Detection and response

- Create and monitor alerts related to abnormal authentication events, such numerous password resets in a short while and access from foreign sources
- Consider non-standard evidence sources, such as IT Help Desk tickets, call recordings, and employee interviews
- Track cybersecurity events and incidents for resource allocation; use key performance indicators (KPIs) to measure effectiveness



Identity theft – the Achilles Steal

2018 Data Breach Digest

verizon✓

The situation

I'm the Chief Operating Officer (COO) of a large corporation. After returning from an overseas trip, I checked my Mourning Dove Investments (MDI) brokerage account. Immediately I was struck by my reduced account balance due to two (2) wire transfers; the first for $150,000 and the second for $160,000 a few days later.

Detection tip

Set-up account change alerts (e.g., port forwarding, account ownership).

Concerned, I called MDI and they verified that two wire transfers went to a bank in Hong Kong. MDI advised that, following protocol, they called my home telephone number and spoke with my wife to verify the transaction. As part of the verification process, MDI confirmed my wife's driver's license number and a security challenge question where the response was related to recent travel.

Response tip

Report fraudulent activity to the appropriate entities, including Law Enforcement.

My wife indicated she had received no contact from MDI. I was immediately concerned that my home telephone number may have been spoofed, so we engaged the VTRAC | Investigative Response Team.

Investigative response

The VTRAC investigators asked about what options and features (call forwarding, etc.) were enabled on my home phone number. I was unsure and needed to check with the telephone company.

Meanwhile, my wife mentioned that over the previous couple months she had noticed a high-pitched buzz for 3-4 seconds when picking up the home phone (a land line) before hearing a dial-tone. She had thought nothing of it until now. I allowed the VTRAC investigators to obtain a copy of my most recent phone bill.

I was also concerned my tablet may have been compromised as it contained potentially sensitive information, such as emails sent by my assistant, travel itineraries, calendar entries, and credit card transactions. While traveling, I'd used my tablet to access the Department of Motor Vehicles (DMV) website and apply for a new driver's license for my wife. I did this over the hotel internet access. This was the last time I could recall my wife's driver's license information being legitimately transferred electronically.

Mobile device security – IT best practices

With our increased mobility and constantly improving technology, more and more critical data is processed, stored, and communicated via smartphones. While focusing their cybersecurity efforts on their networks and systems, companies often overlook mobile device security. Having some simple rules and policies in place can help prevent a data compromise:

- Utilize a Mobile Device Management (MDM) console to establish centralized rule and policy enforcement on corporate issued and BYOD devices
- Require users to enable screen locking with eight or more uppercase-lowercase-alpha-numeric-special characters passcodes on devices accessing company information
- When storing, transmitting, processing sensitive information, enable encryption features for both data-at-rest and data in-motion
- Perform security audits on all authorized mobile device apps
- Establish dialog with your users. Users have a way of findings workarounds to security methods, and if you're unaware of these methods you can't protect against them
- Maintain technology awareness on mobile security. Monitor for cybersecurity threats and know of new risks to educate users and stay in front of new adversaries

Mitigation tips

- Don't access financial institution websites and other sensitive information from unsecure networks
- Use complex passwords; more preferably, use two-factor authentication on all email accounts
- Don't open attachments from unknown senders; never open executable attachments

While investigating the fraudulent wire transfers, I checked my credit card account and determined I'd incurred unknown charges from my cable company. Additional digging revealed an unauthorized email account was created and associated with my cable company account.

I couldn't specifically recall the full cable company email account, however, it was "first_name" followed by additional information "@cablecompany.com." Normally, I use my "MrSmith@Corporation.com" email account and was surprised to learn of this new account.

The VTRAC investigators acquired forensic images of my wife's and my tablets, laptop and corporate Microsoft Windows system. Both tablets were set to create password-protected encrypted backups, which encrypts most user data. We didn't have the password for either tablet; so recovering information from backups wasn't possible.

Without user data such as internet history and messaging, the VTRAC investigators could not search for signs of phishing or suspicious activity on the tablets. However, the VTRAC investigators discovered several dozen suspicious and malicious files on my wife's laptop. These malicious files were primarily within the '/Users/MrsSmith/Downloads/' and the 'MrsSmith@InternetCompany.com \INBOX \ Attachments' folders.

The file extensions for these files were ".zip" and ".exe," which indicated files capable of running on Windows systems. While it's unlikely these files executed on the laptop, if forwarded to a Windows system their malicious nature could then be leveraged.

The VTRAC investigators reviewed the mailboxes on the laptop and discovered three (3) malicious files sent as attachments from my wife's email account to her same email address. None of the emails being sent with malicious attachments were directed to my "MrSmith@Corporation.com" email account.

Detection tip

Keep anti-virus software up-to-date on personal devices used to access corporate email.

Lessons learned

We learned a lot from a mitigation and response standpoint. Some takeaways from our post-incident lessons learned session were:

Mitigation and prevention

- Don't access financial institution websites from unsecure networks
- Use complex passwords; more preferably, use two-factor authentication on all email accounts
- Don't open attachments from unknown senders; never open executable attachments

Detection and response

- Set-up account change alerts (e.g., port forwarding, account ownership)
- Report fraudulent activity to appropriate entities, to include law enforcement
- Keep anti-virus software up-to-date on personal devices used to access corporate email

Mobile device security – user best practices

With mobile devices having become a daily necessity in our lives, they are an increased threat target. While this target has been smaller compared to computers, it's increasing in size. These suggestions will help to reduce the risk of mobile device data being compromised:

- Always utilize a password. Passcodes with eight or more uppercase-lowercase-alpha-numeric-special characters are more secure than the standard 4 or 6-digit pin codes
- Never leave your device unattended. Physical access to a mobile device remains the most reliable way to gain unauthorized access
- Keeping your device up to date will alleviate the most common methods of mobile breaches
- Only use trusted sources for apps. This includes the iTunes store for Apple devices, and Google Play for Androids. Downloading and installing third party apps from other sources increases the chance of installing malicious software
- Enable screen locking. The shorter the timeframe between use and auto lock will reduce the chance that an unauthorized user could easily gain access
- Avoid the use of jail-broken devices. The act of jail breaking inherently decreases the security of a mobile device

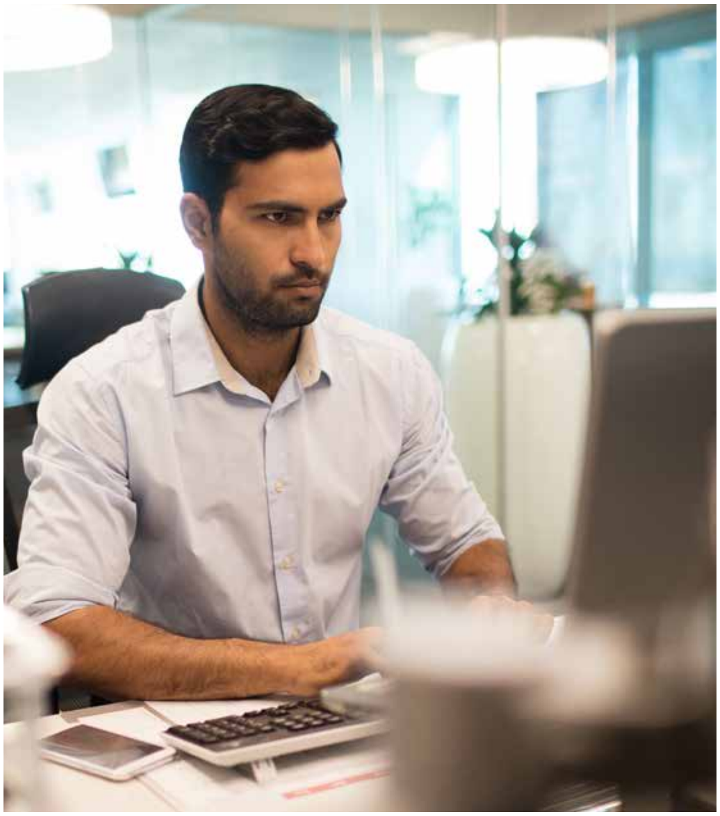
Wi-Fi compromise – the Evil Twin

2018 Data Breach Digest

verizon✓

The situation

Our Chief Executive Officer (CEO) recently read a report indicating many networks could be compromised using common misconfigurations of enterprise wireless networks as the initial attack vector. As the Cybersecurity Director, I had this report to thank for finally securing approval to engage Verizon Professional Services to perform a much-needed penetration test on our wireless network.



Penetration testing

After the assessment was complete, the Verizon penetration testers explained that they had identified specific, high-risk wireless vulnerabilities on our network. These vulnerabilities could lead to an attacker compromising our Active Directory, accessing our enterprise wireless and launching further attacks against our network.

The penetration testers began by configuring an Access Point (AP) with a strong signal to imitate our wireless network name or Service Set Identifier (SSID). Devices, by default, automatically identify known APs based on their SSID and then attempt to connect to the AP with the strongest signal.

This Wi-Fi attack essentially established an "evil twin" AP and intercepted the wireless communications. For clients already connected to the wireless network, de-authentication ("deauth") packets were sent. These deauth packets forced these clients to drop established connections and re-authenticate to the "evil twin" AP.

Mitigation tip

Perform regular vulnerability assessments; regularly patch all wireless clients, Access Points (APs), and Authentication, Authorization, and Accounting (AAA) servers.

Detection tip

Deploy wireless network Intrusion Detection System / Intrusion Prevention System (IDS / IPS) solutions to detect and prevent rogue wireless network clients and APs.

Wireless network group policy

Consider implementing a global policy within the Microsoft Windows Active Directory "Wireless Network Policies Group Policy" extension to deploy specific configurations, to include:

- Disable Internet Connection Sharing (ICS); enable Microsoft Windows firewall
- Allow only trusted and valid server certificates
- Create a trusted Root Certificate Authority (CA)
- Restrict the ability to accept new servers or trusted CAs
- Specify the common name (CN) for only your RADIUS server
- Enable identity privacy to prevent clients from sending their usernames in the outer, unencrypted tunnel

Mitigation tips

- Restrict client connections to APs with trusted Root Certification Authority (CA) certficates
- Require Two-Factor Authentication (2FA) and / or mutual authentication

Our corporate laptops weren't configured properly to validate only our trusted server side certificates. Instead, we allowed our employees to accept new certificates and, as such, the penetration testers were able to present a forged certificate.

Once the forged certificate was accepted, an encrypted tunnel would be established. This then allowed the capture of any credentials sent from the client, including Windows domain user credentials.

The testers now had access to the wireless network and could then determine their level of access into the internal network. As we hadn't segmented our wireless network, it was quickly apparent to them that they had access to our entire network!

Detection tip

Monitor wireless traffic for unusual activity including unexpected after-hours traffic; regularly scan for unknown devices.

Response tip

Leverage an endpoint security solution for attack monitoring / detection; auditing / logging; evidence collection / incident response.

The testers informed us that with that level of access, an attacker could scan for vulnerabilities or even query the domain controller for Service Principal Names (SPNs). This could then lead to the attacker taking over any domain admin accounts and compromising the Windows domain environment.

Once a domain admin account has been compromised, the attackers have virtually unlimited options to further breach the network. Some options include creating new accounts, compromising Authentication, Authorization, and Accounting (AAA) servers (e.g., TACACS+ and RADIUS), installing backdoors, or accessing sensitive financial or intellectual property documents.

Mitigation tips

- Inventory and classify information assets including wireless network clients and APs
- Segment the wireless network from the wired network

Lessons learned

We considered ourselves very lucky to have discovered how easily our network could be compromised through a penetration testing exercise and not as the result of an actual data breach.

We immediately set to work implementing the recommendations the Verizon penetration testers had provided. We also reviewed our Incident Response (IR) Plan and added these recommendations:

Detection and response

- Deploy wireless network Intrusion Detection System / Intrusion Prevention System (IDS / IPS) solutions to detect and prevent rogue wireless network clients and APs
- Monitor wireless traffic for unusual activity including unexpected after-hours traffic; regularly scan for unknown devices
- Leverage an endpoint security solution for attack monitoring / detection; auditing / logging; evidence collection / incident response

Mitigation and prevention

- Perform regular vulnerability assessments; regularly patch all wireless clients, APs, and AAA servers
- Restrict client connections to APs with trusted Root Certification Authority (CA) certificates
- Require Two-Factor Authentication (2FA) and / or mutual authentication
- Inventory and classify information assets including wireless network clients and APs
- Segment the wireless network from the wired network

Other Wi-Fi security considerations

Additional Wi-Fi security considerations include:

- Implement a global policy within the Microsoft Windows Active Directory “Wireless Network Policies Group Policy” extension (see sidebar on previous page)
- Treat these connections as untrusted remote access from the internet and implement VPN
- Time define legitimate time usage
- Utilize Network Access Control (NAC) technology before allowing access to the internal network
- Deploy Extensible Authentication Protocol (EAP) with the Tunneled Transport Layer Security method (EAP-TTLS) using client and server certificates with a Public Key Infrastructure (PKI)
- Quarantine by using dynamic, individualized segmentation for wireless clients with AP isolation
- Quarantine remote connecting devices. For instance, check compliance status in patching, configuration and anti-virus status before allowing further connection to internal network resources
- Configure a “preferred network” list with only corporate-approved wireless networks; restrict user ability to add their own networks to the “preferred network” list. Note: This creates a “convenience drawback” as this prevents users from using their laptop to connect to public Wi-Fi when traveling. Using a VPN when traveling helps mitigate this risk

Twended attack – the Bedeviled Egg

2018 Data Breach Digest

verizon✓

The situation

Network security is our number one priority and our budget reflects that commitment. We rigorously vet cybersecurity products and only purchase those that meet our standards. In addition, we devote considerable investment to developing and deploying in-house solutions designed to harden our network infrastructure. The information we protect is invaluable so we spare no expense.

So, how did we get compromised?

At the end of a workday one of our cybersecurity analysts came across an alert identifying a malware-related intrusion and possible data exfiltration. With all hands on deck, we followed our Incident Response (IR) Plan and immediately collected logs while triggering the Verizon Rapid Response and Retainer Service (RRR) to expedite evidence collection and analysis.

Response tip

Conduct regular data breach and IR simulation exercises; in doing so, leverage realistic scenarios to effectively respond to likely cybersecurity incidents.

Investigative response

Forensic analysis revealed the malicious software introduced into the network originated from an external USB storage device as opposed to the common vectors we encounter, such as a phishing campaign or an exploited vulnerability.

Mitigation tips

- Disable unauthorized system access to external USB storage devices
- Disable physical and logical access for users immediately upon termination

With the analysis conclusively determining a user's system was the initial point of compromise and network entry vector, the bigger question became: "How did the threat actor gain access to the workstation?" It was time to blend the skills of a digital detective and an old-fashioned gumshoe to answer this question.

Through onsite interviews with employees and corporate security reviews of closed-circuit television (CCTV) recordings, we determined that a recently terminated employee leveraged their still-yet-to-be-disabled building access credentials.

The terminated employee gained entry into the building and ultimately to the room where the unlocked system was housed. The security guards stationed at the perimeter of our building are diligent; however, they could only check the access cards of authorized employees and ensure their privileges were current.

Although the terminated employee's network credentials were revoked, the lack of a timely update to the security database made it appear that they were still employed. This allowed the terminated employee to blend in as one of our employees.

The terminated employee understood the sensitive nature of our information and the embarrassment it would cause if it were lost or leaked to the public. To exact revenge for what they considered a groundless termination, the former employee attempted to use their understanding of our network to circumvent our existing security measures.

The former employee's objectives were to collect and disseminate sensitive information, introducing a malware infection (possibly to cover their tracks) that would collect the data and direct it to an anonymized website. The plan almost worked.

Response tips

- Coordinate cybersecurity response activities with stakeholders, including business unit leaders, legal, human resources, and corporate security
- Apply extra diligence in network monitoring; increase employee awareness to report suspicious situations involving disgruntled employees

Lessons learned

Fortunately, our network security solutions detected the malicious activity. However, we realized our policies were not being enforced. An unlocked and unattended networked system and an untimely deactivation of a building access card helped facilitate this data breach.

When we concentrate on only one area of security, attention to detail in other areas (such as physical access) can sometimes be overlooked. In this instance, by focusing solely on cybersecurity we were left open and vulnerable to a physical security threat, and a blended attack with a twist.

Mitigation and prevention

- Disable unauthorized system access to external USB storage devices
- Disable physical and logical access for users immediately upon termination

Detection and response

- Conduct regular data breach and IR simulation exercises; in doing so, leverage realistic scenarios to effectively respond to likely cybersecurity incidents
- Coordinate cybersecurity response activities with stakeholders, including business unit leaders, legal, human resources, and corporate security
- Apply extra diligence in network monitoring; increase employee awareness to report suspicious situations involving disgruntled employees

Cloud storming – the Slivered Lining

2018 Data Breach Digest

verizon✓

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 (LE).

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.

Response tip

Proactively review logs of all internet-facing systems and applications.

Investigative response

The IT Security team further determined that 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.

Mitigation tip

Systematically monitor and test security posture from all angles; provide additional security and monitoring on critical systems.

Out of arm's reach isn't out of harm's way

If a tree falls in your Microsoft Active Directory forest, how much sound do you have to make for your cloud service provider to take an interest?

Many organizations benefit from outsourcing or moving local IT functions to the cloud. However, in doing so, they've lost the ability to physically walk up to a rack of servers and the employees responsible for them and encourage either to work.

Cloud storage can solve issues for organizations but it can also introduce new challenges. For example, the VTRAC | Investigative Response Team encountered a victim organization that eschewed traditional backups to local tape or spinning for cloud storage over a consumer-grade internet connection. Day-to-day business functions weren't affected as a few megabytes of documents per day trickled up to the cloud.

While we were able to investigate the circumstances surrounding the incident, unfortunately, the ransomware encrypted an entire department's work product. In looking at their options, the organization realized that it'd take weeks to download the files required for business continuity. As their cloud storage provider offered no other transfer method, they had no other option than to pay the ransom and hope the files were decrypted successfully.

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.

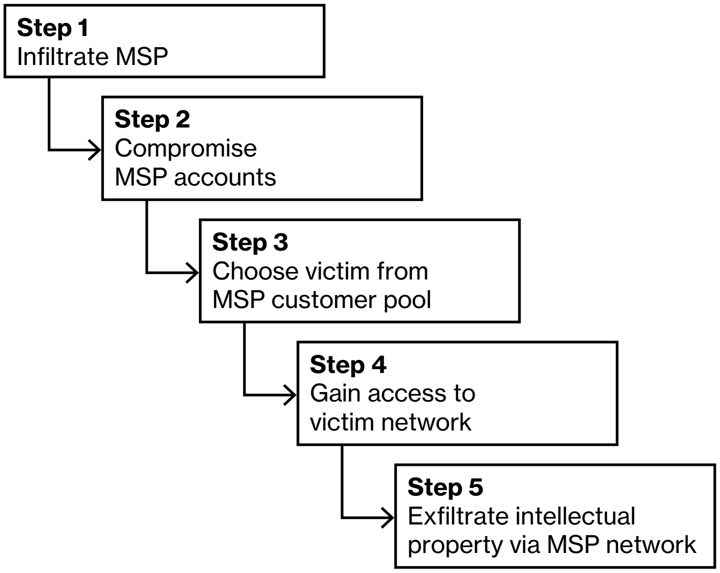

Step 1
Infiltrate MSP
Step 2
Compromise MSP accounts
Step 3
Choose victim from MSP customer pool
Step 4
Gain access to victim network
Step 5
Exfiltrate intellectual property via MSP network

Figure 1. MSP cyber attack stream

Mitigation tips

- Review, reconcile, manage, and monitor all third-party account access
- Enhance user account security by requiring regular password changes, including local admin accounts

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 of the infections dated back 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 (along with various credentials) were at risk. Most importantly, it was possible that our intellectual property was already being exfiltrated.

Detection tip

Employ a file integrity monitoring (FIM) solution to assist with detection efforts.

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.

Response tip

Rebuild all affected systems; expand network logging and monitoring capabilities for areas lacking in network visibility.

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 didn't uncover evidence of data exfiltration, given the length of 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.

What goes up must come down

Have a documented process to extract data wholesale from your cloud environment, whether it be unstructured data (such as file level backups), structured data (such as databases) or entire virtual machines, often simply downloading this data may not be practical, and a hard drive must be shipped or a data center visited.

People say that a backup can't be thought of as a successful backup until it has been restored once. Assume your cloud services will not release your data until you have retrieved it at least once as part your next disaster recovery exercise or Information Security incident simulation.

Lessons learned

A call from LE 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
- Review, reconcile, manage, and monitor all third-party account access
- Enhance user account security by requiring regular password changes, including local admin accounts

Detection and response

- Proactively review logs of all internet-facing systems and applications
- Employ a file integrity monitoring (FIM) solution to assist with detection efforts
- Rebuild all affected systems; expand network logging and monitoring capabilities for areas lacking in network visibility

Web app attack – the Tuple-Row Honey

2018 Data Breach Digest

verizon✓

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 many times 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.

Mitigation tips

- 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

Investigative response

The IT Security team detected significant in-bound traffic accessing the web application server along with several anti-virus 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?"

It was at this point that 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.

Response tips

- Assemble the IR Team; include stakeholders relevant to the specific cybersecurity incident; engage Law Enforcement (LE) 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

A number of 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 thereby reducing the potential for additional data exfiltration.

Mitigation tips

- 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

Response tip

Prepare public relations responses for various data breach scenarios ahead of time; adjust the actual response to the specific data breach circumstance.

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 (LE) 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

Remote code execution

Remote code execution (RCE) flaws give threat actors the ability to execute a malicious code remotely. This could lead to complete control of the web application server with the privileges of the app user account.

Successful exploitation of the RCE vulnerability provides access for the threat actor to further inject and execute shell codes (within the context of the shell). This essentially acts as an easy channel to manually run arbitrary commands.

The most common reasons for the successful exploitation of this vulnerability are lack of proper input and output data validation, and improper handling of untrusted data. Because of this, it's advisable to sanitize user input at the client-level and (even more important) at the server level.

verizonenterprise.com