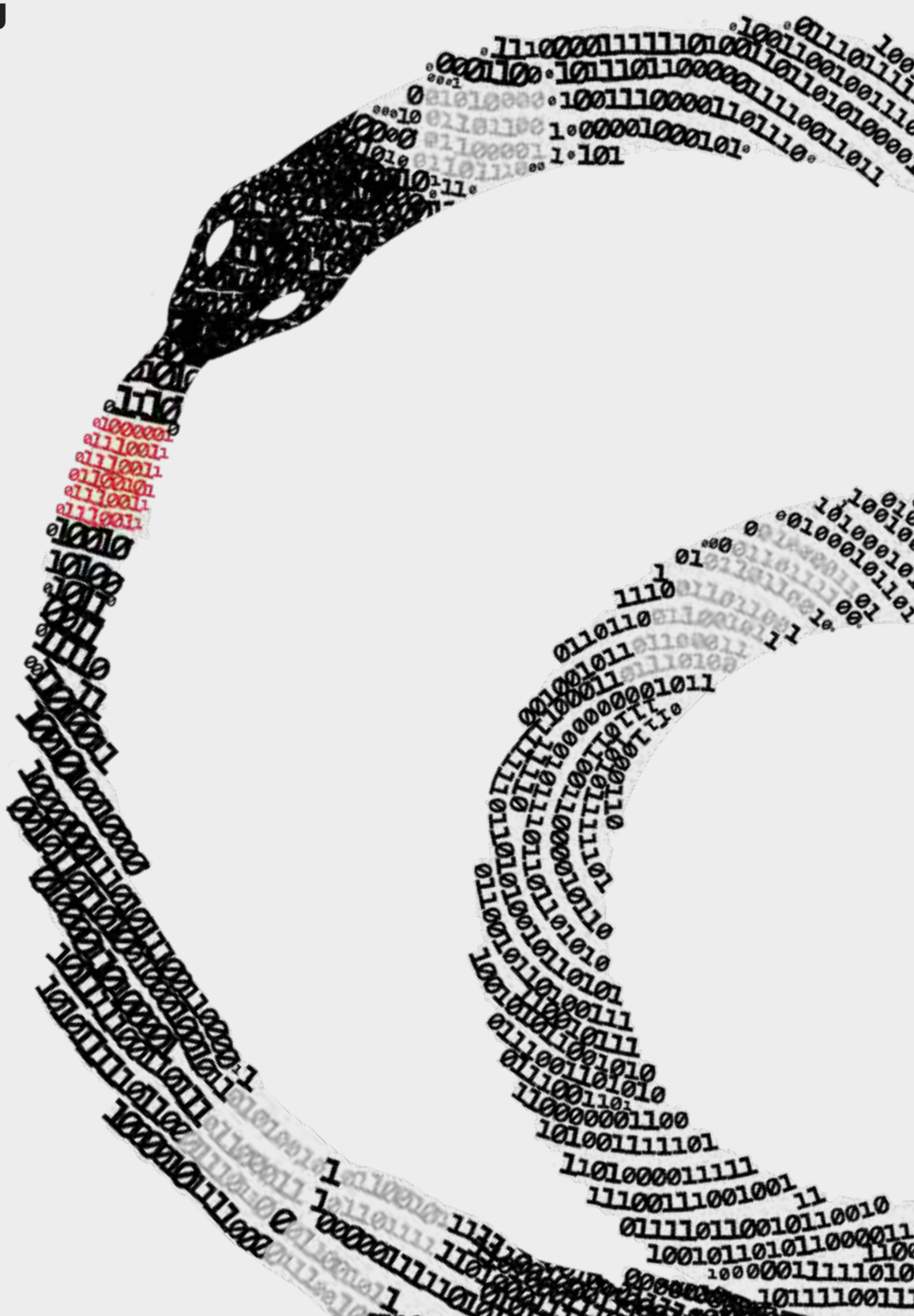
Breach simulation scenario #5

Cloud storming – The slivered lining



verizon

Using the breach simulation kits.

This is part five in a series of five data breach scenarios we're using to illustrate the need for an IR Plan, playbooks and their underlying components. These scenarios, together with the countermeasure worksheet and solutions, form Breach Simulation Kits (BSKs). BSKs can facilitate data breach simulation workshops involving internal IR stakeholders and tactical responders, as well as external entities. Conducting a BSK workshop session is a five-step process.

Step 1 – Getting started

To facilitate a BSK workshop, you'll need:

- A suitable facility – a "war room" or conference room free of noise and other distractions
- A whiteboard or butcher-block paper and markers
- Printouts of scenarios and countermeasures worksheets (and highlighters) for each participant

A typical BSK workshop session consists of 1-2 scenarios and can last for 1-2 hours, depending on participant knowledge levels and experience.

Step 2 – The scenario

Begin the workshop by distributing printouts of the scenario (including situation, response and lessons learned) to participants (optional: distribute the countermeasure worksheet).

Cyber-espionage – The "katz-skratch fever"	Notes
The situation While espionage has existed for thousands of years, cyber-espionage (threat actors targeting sensitive or proprietary data on digital systems) is still a relatively new concept. Recently, a manufacturing customer engaged the VTRAC | Investigative Response Team to let us know they'd been contacted by law enforcement regarding a possible data breach. The Chief Information Security Officer (CISO) had been notified of several foreign IP addresses that may have been communicating with systems inside his environment. The CISO requested we immediately report to headquarters to begin investigation into the suspicious IP addresses.	Contact digital forensics firm Maintain effective law enforcement contacts Check security information and event management (SIEM) events

Figure A: The scenario – The situation, response and lessons learned

Give participants 10-15 minutes to read the scenario, highlight and take notes. Allow participants to talk and discuss among themselves.

Step 3 – Countermeasure worksheet

After participants have read the scenarios, facilitate a discussion by selecting a participant to walk through the situation, response and lessons learned. Discuss key observations on countermeasures. Take notes on the whiteboard or butcher-block paper (or use the countermeasures worksheet) by progressing through the six phases of incident response (include prevention and mitigation countermeasures).

Phase	Countermeasure
1 – Planning and Preparation	• Create an IR playbook for cryptocurrency-related scenarios; train incident responders on efficient and effective response activities
2 – Detection and Validation	• Conduct periodic threat hunting activities across the network to locate and identify any undetected cyber threat activity evading traditional cybersecurity tools • 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

Figure B: Countermeasure worksheet – the six phases of incident response plus mitigation and prevention

Give the participants 15-20 minutes to discuss, and be sure everyone has an opportunity to speak.

Step 4 – Countermeasure solutions

Distribute countermeasure solutions (answers). Continue facilitating the discussion by comparing participant solutions to countermeasure solutions. Do they differ? Did the participants come up with more actionable items than those provided in the countermeasure solutions?

Detection and response

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

Mitigation and prevention

- Provide, at least annually, user cybersecurity awareness training, emphasizing 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 multifactor authentication; require virtual private network (VPN) access for remote connections to the corporate environment

Figure C: Countermeasure solutions

Give the participants 10-15 minutes to discuss.

Step 5 – Lessons learned

Complete the session by conducting a lessons-learned discussion, noting participant feedback (e.g., what went well, what went less smoothly and what can be improved on in the next session). Assemble feedback and countermeasure solutions in an action plan to update the IR Plan, determine additional IR resource requirements, and identify internal IR stakeholder and tactical responder training needs.

Give participants 10-15 minutes to discuss.

Cloud storming – The slivered lining[1]

The situation

It was a normal workday when I inspected the alarmed access and egress points at our corporate office. As I was walking through the hallways, I received a phone call from law enforcement. The officer informed me that certain systems on our network were likely compromised, because they were contacting an IP address identified as malicious.

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

Investigative response

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

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

Leveraging the VTRAC | Cyber Intelligence Team, they found the RAT was associated with an advanced persistent threat (APT) group. The APT was commonly associated with attacks aimed at stealing intellectual property and leveraging managed service providers (MSPs) as attack vectors. The MSP cyberattack stream was essentially:

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

With a list of APT-associated indicators of compromise (IoCs), our IT Security team quickly scanned our network for other potentially compromised systems. The scans identified multiple infected systems. Even worse, many infections dated back a few years.

Notes:

[1]https://enterprise.verizon.com/resources/casestudies/2018/data-breach-digest-2018-cloud-storming.pdf

The most common malware found by the scans were backdoor tools used by the APT to maintain persistence on the network. Further analysis 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.

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

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

We set about identifying and then rebuilding all affected systems. For those areas of the network we found "lacking in adequate visibility," we expanded our logging and monitoring capabilities.

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

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

Lessons learned

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

Notes:

Countermeasure solutions

Detection and response

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

Mitigation and prevention

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

Countermeasure worksheet

Workshop participants can enter their discussion notes on breach countermeasures here.

Phase	Countermeasure
1. Planning and preparation	
2. Detection and validation	
3. Containment and eradication	
4. Collection and analysis	
5. Remediation and recovery	
6. Assessment and adjustment	
0. Mitigation and prevention	

Table 4 - Breach simulation countermeasure worksheet

Data breach and cybersecurity resources

https://enterprise.verizon.com/resources/

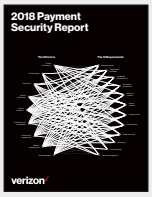
2019 Incident Preparedness and Response Report: Taming the data ~~beast~~ breach.

2019 Data Breach Investigations Report

2019 Insider Threat Report: Out of sight should never be out of mind.

2019 Mobile Security Index: It's time to tackle mobile security.

2018 Data Breach Digest (18 scenarios)



2018 Payment Security Report

2019 CISO's Guide to Cloud Security: What to know and what to ask before you buy.

5 Considerations for Evaluating a Modern Enterprise Security Platform.

For the Verizon Incident Preparedness and Response report, executive summary and additional scenarios, visit
enterprise.verizon.com/resources/reports/vipr/

verizon