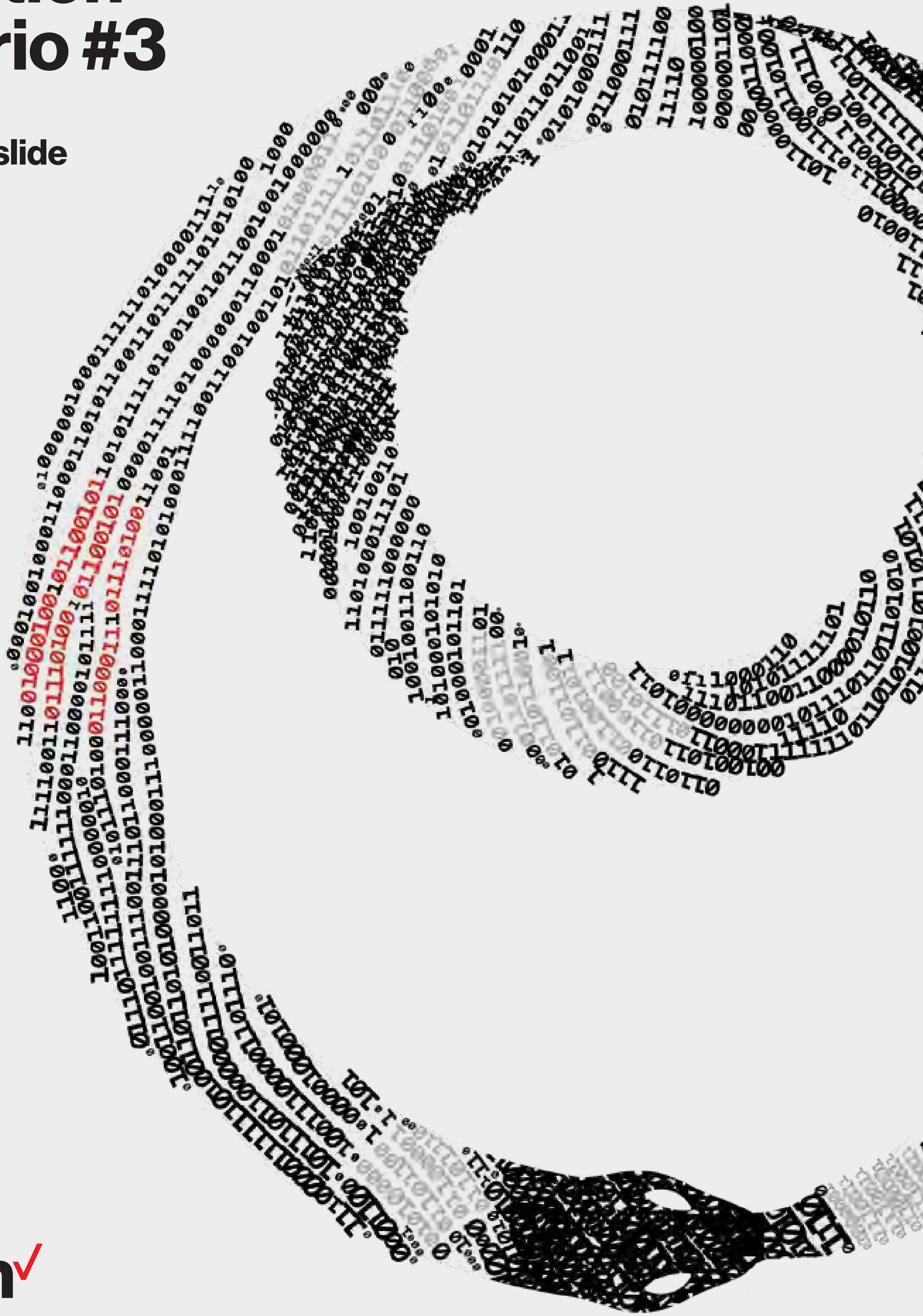
Incident Preparedness and Response Report
Scenario 3/5

Breach simulation scenario #3

ICS attack – The eclectic slide



verizon

Using the breach simulation kits.

This is part three 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

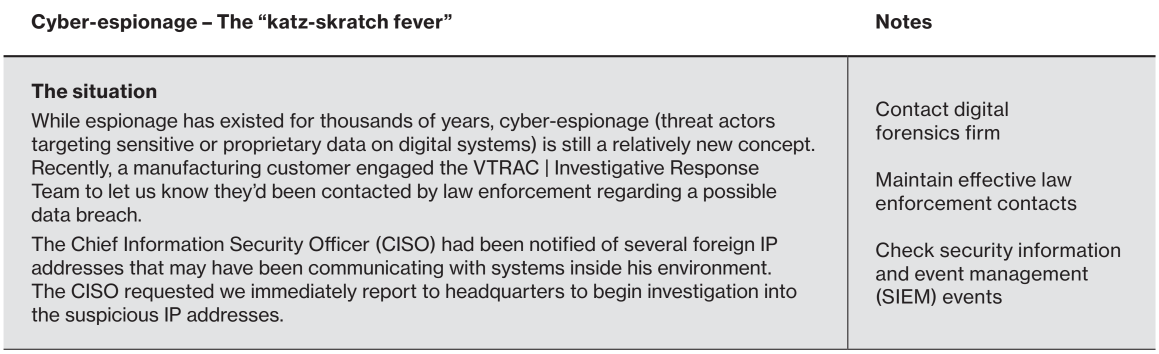
To facilitate a BSK workshop, you'll need:

- 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.

ICS attack – The eclectic slide[1]

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 Security Operations Center (SOC) lead analyst in critical infrastructure protection (CIP), I was used to such after-hours calls. What was unusual was the next statement: “Law enforcement called and they believe we may be compromised.”

When I arrived, the office was in a frenzied state. Because 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 it difficult to share information with colleagues not physically present in the office.

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) was an email address, which law enforcement believed was involved in a spear phishing attack against various organizations in the energy sector.

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

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

Investigative response

VTRAC investigators examined the suspicious attachments and soon presented their findings. They found that 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 the software to download a malicious payload.

When opened, the document “searched” for a specific, malicious template via the server message block (SMB) protocol hosted on the threat actor’s server.

Notes:

[1] https://enterprise.verizon.com/resources/casestudies/2018/data-breach-digest-2018-the-peeled-onion.pdf

Once downloaded, the malicious template used macros to spawn a Microsoft PowerShell (command prompt) instance to steal user account credentials.

It turned out that the targeted users had not corresponded with the threat actor. However, they all had very public profiles on a popular professional social media networking website. The threat actors likely used these profiles to select 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 accessing these systems, we created a PowerShell script to search for IoCs, and then loaded them on to a USB device. We identified a plant engineer with the appropriate level of system access, made a one-time exception and had him plug the USB device into the OT systems to run the script and scan for any IoCs.

Lessons learned

While we found no additional IoCs, we identified several improvements that could be made to our incident response approach. During our after-action review, we set out to accomplish these enhancements as soon as possible.

First, we set up an alternate communication method separate from the corporate network. This provided the SOC analysts with a way to communicate securely should our corporate network be compromised.

Next, we educated end-users to be careful with information they share online, as threat actors can use it 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 a requirement that all SOC analysts and cybersecurity incident responders take required NERC CIP training and undergo additional background screening as an enhanced security measure.

Notes:

Countermeasure solutions

Detection and response

- Establish a method for reliable, secure, alternative communications before a cybersecurity incident occurs; incorporate this into the 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; train SOC analysts and incident responders to respond in the Industrial Control System (ICS) environment

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

Countermeasure worksheet

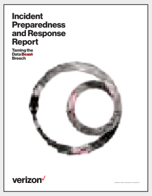
Workshop participants can enter their discussion notes on breach countermeasures here.

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/

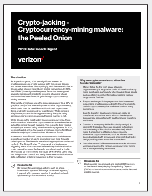

Incident Preparedness and Response Report
Taming the Data Beast Breach
verizon

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

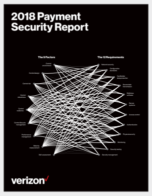
2019 Data Breach Investigations Report

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

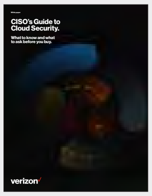
2019 Mobile Security Index: It's time to tackle mobile security.


Crypto-jacking - Cryptocurrency-mining malware: the Peeled Onion
2018 Data Breach Digest
verizon

2018 Data Breach Digest (18 scenarios)



2018 Payment Security Report


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

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.
verizon

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✓