Breach simulation scenario #4

Cyber-espionage – The katz-skratch fever

Incident Preparedness and Response Report
Scenario 4/5

verizon✓

Using the breach simulation kits.

This is part four 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

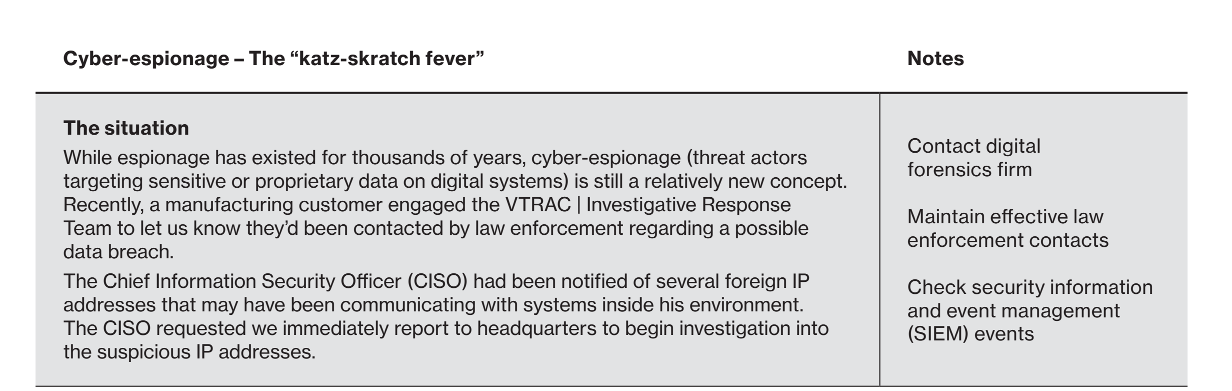
To facilitate a BSK workshop, you’ll need:

- 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.

Cyber-espionage – The katz-skratch fever[1]

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 after it was contacted by law enforcement about a possible data breach.

The Chief Information Security Officer (CISO) had been notified of several foreign IP addresses that might have been communicating with systems inside his environment. The CISO requested we immediately report to headquarters to investigate these suspicious IP addresses.

Investigative response

Our VTRAC I Investigative Response Team understood the potential severity as we deployed to the customer's headquarters the next day. After an initial briefing with the CISO, we started our triage of several in-scope servers and other equipment believed to be involved in this incident. After 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. It scrapes memory of the process responsible for Microsoft Windows Local Security Authority Subsystem Service (LSASS) authentication, revealing clear text passwords and NT LAN Manager (NTLM) hashes.

Notes:

[1] https://enterprise.verizon.com/resources/casestudies/2018/data-breach-digest-2018-the-katz-skratch-fever.pdf

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

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

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

Lessons learned

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

Notes:

Countermeasure solutions

Detection and response

- If not already involved, engage law enforcement when the time is right, as well as 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
- Use internal and external intelligence resources to develop actionable intelligence on threat actor modus operandi and IoCs

Mitigation and prevention

- At least annually, provide users with 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

Countermeasure worksheet

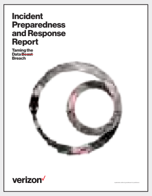
Workshop participants can enter their discussion notes on breach countermeasures here.

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

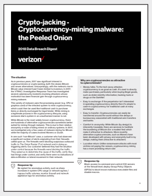
2019 Incident Preparedness and Response Report: Taming the data ~~beast~~ breach.

2019 Data Breach Investigations Report

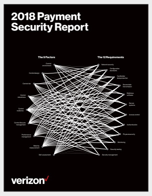
2019 Insider Threat Report: Out of sight should never be out of mind.

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

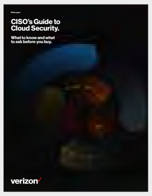
2019 Mobile Security Index: It's time to tackle mobile security.


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/