Incident Preparedness and Response Report
Scenario 1/5

Breach simulation scenario #1

Crypto-jacking – The peeled onion

verizon

Using the breach simulation kits.

This is part one 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

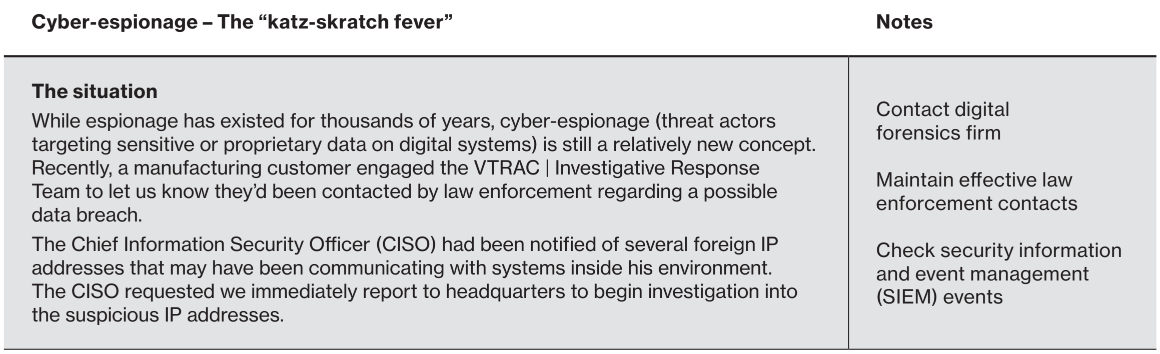
To facilitate a BSK workshop, you'll need:

- 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.

Crypto-jacking – The peeled onion[1]

The situation

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

There are hundreds of alternative cryptocurrencies, which may be suited for mining through malware, because of either increased anonymity or the relative ease in mining on ordinary systems.

In one such non-bitcoin case, a customer who had observed many alerts originating from its firewalls called on us. The firewalls were blocking suspicious outbound traffic to The Onion Router (TOR) network and triggering alerts. The customer believed it had the situation under control because the firewalls were blocking the traffic.

The company asked us to determine the cause of the traffic, confirm that the situation was under control, and verify there were no indications of data exfiltration or lateral movement in the network.

Investigative response

Before engaging us, the customer obtained full packet captures (FPCs) of network traffic and dumped the physical memory from a system generating the suspicious outbound traffic. We dove into the network FPCs and memory, and soon provided actionable intelligence on other potentially compromised systems on the network. These IoCs included system names, IP addresses, malware file hashes/file names and malicious process names.

While a review of active network connections revealed a majority of traffic was blocked by the firewall, successful connections were occurring to resources in the TOR network. This was due to the firewall's filtering being based on IP address blacklisting, which didn't encompass all TOR addresses used by the malware.

Notes:

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

Our client also observed that additional 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 running on the sample system, as well as other infected systems.

Meanwhile, our VTRAC | Network Forensics Team reviewed the FPCs and confirmed that the malware used a propagation method similar to well-known ransomware instances, leveraging digital tools leaked by "The Shadow Brokers" hacking group.

Examining an image of the sample system confirmed it wasn't patched against a known vulnerability, making the propagation possible. This was contrary to our customer's belief they were properly secured.

We then further assisted our customer by analyzing firewall logs to identify other systems beaconing to the TOR network and requiring remediation. Notably, this analysis identified over 300 infected devices.

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, which were based on legacy operating systems.

Lessons learned

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

On this occasion, the malware targeted cryptocurrency mining; more nefarious malware could have leveraged the same vulnerabilities and made a more significant impact on the business.

Notes:

Countermeasure solutions

Detection and response

- Create an IR playbook for cryptocurrency-related scenarios; train incident responders on efficient and effective activities
- 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
- 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
- Employ enterprise and host-based antivirus solutions with up-to-date signatures to detect and eradicate threats as they arise
- Analyze malware functionality for detection and response, as well as mitigation and prevention

Mitigation and prevention

- Block and alert internet connections to cryptocurrency mining pools; include TOR networks, unless there's a valid business reason not to do so
- 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
- Establish a patch management program; apply security patches as soon as possible; confirm patching succeeded
- 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
- Conduct regular security assessments; evaluate defensive architecture design based on sandboxing, web browser separation and virtualization for select activities

Countermeasure worksheet

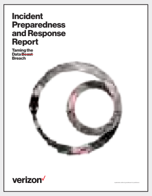
Workshop participants can enter their discussion notes on breach countermeasures here.

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/

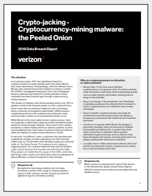

Incident Preparedness and Response Report
Taming the Data Beast Breach
verizon

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

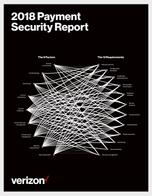
2019 Data Breach Investigations Report

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

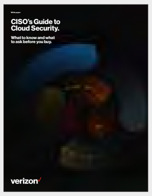
2019 Mobile Security Index: It's time to tackle mobile security.


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/