This resource was adapted from the http://kinomakino.blogspot.com/2015/10/ Web site on July 12, 2018.

Zeltser, L. (n.d.). Cyber threat intelligence and incident response report. Retrieved from http://kinomakino.blogspot.com/2015/10/

# Incident Response Report

|  |  |
| --- | --- |
| Incident Name |  |
| Report Author |  |
| Report Date |  |
| Revision Dates and Notes |  |

## Executive Summary

Describe in up to 3 paragraphs your key observations and takeaways related to the intrusion. Explain the adversary’s tactics, techniques, and procedures. Outline the most significant courses of action taken to defend against the adversary when responding to the intrusion. The remainder of the report should substantiate this summary.

## The Adversary’s Actions and Tactics

Summarize in 1 paragraph the adversary’s actions and tactics, as well as the effects that the intrusion had on the victims. This section of the report overlays the intrusion kill chain’s phases over the diamond model vertices to capture the core characteristics of the malicious activities.

### Description of the Adversary

Describe observations and indicators that may be related to the perpetrators of the intrusion. If possible, highlight the attributes of the adversary operator and the adversary’s potential customer. Outline potential motivations and identifying elements. Categorize your insights according to the corresponding phase of the intrusion kill chain, as structured in the following table:

|  |  |
| --- | --- |
| Reconnaissance |  |
| Weaponization |  |
| Delivery |  |
| Exploitation |  |
| Installation |  |
| Command and Control |  |
| Actions on Objectives |  |

### The Adversary’s Capabilities

Describe the adversary’s capabilities in terms of tactics, techniques, and procedures (TTPs). Address the tools and tradecraft employed by the intrusion perpetrators, such as exploit backdoors, staging methods, and situational awareness. Categorize your insights according to the corresponding phase of the intrusion kill chain, as structured in the following table:

|  |  |
| --- | --- |
| Reconnaissance |  |
| Weaponization |  |
| Delivery |  |
| Exploitation |  |
| Installation |  |
| Command and Control |  |
| Actions on Objectives |  |

### The Adversary’s Infrastructure

Describe the infrastructure, such as IP addresses, domain names, program names, and son on, used by the adversary. Categorize your insights according to the corresponding phase of the intrusion kill chain, as structured in the following table:

|  |  |
| --- | --- |
| Reconnaissance |  |
| Weaponization |  |
| Delivery |  |
| Exploitation |  |
| Installation |  |
| Command and Control |  |
| Actions on Objectives |  |

### The Victims and Affected Assets

Describe the victims affected by the adversary’s actions. Address applicable victim identifiers such as people and organization names. Also outline the affected victim assets, such as networks, systems, and applications. Categorize your insights according to the corresponding phase of the intrusion kill chain, as structured in the following table:

|  |  |
| --- | --- |
| Reconnaissance |  |
| Weaponization |  |
| Delivery |  |
| Exploitation |  |
| Installation |  |
| Command and Control |  |
| Actions on Objectives |  |

## Course of Action During Incident Response

Summarize in 1 paragraph the steps you’ve taken when responding to the various phases of the intrusion chain. The section below should describe your actions in greater detail.

### Discover

Describe in the following table the steps you have taken to determine what the adversary has done so far as part of the intrusion, as determined based on the analysis of logs, network packer captures, forensic data, and other sources:

|  |  |
| --- | --- |
| Reconnaissance |  |
| Weaponization |  |
| Delivery |  |
| Exploitation |  |
| Installation |  |
| Command and Control |  |
| Actions on Objectives |  |

### Detect

Describe in the following table the measures you have put in place to identify the adversary’s future activities related to the applicable intrusion phase. Explain how you defined and deployed indicators and signatures, additional sensors or instrumentation, security event data monitors, and so on:

|  |  |
| --- | --- |
| Reconnaissance |  |
| Weaponization |  |
| Delivery |  |
| Exploitation |  |
| Installation |  |
| Command and Control |  |
| Actions on Objectives |  |

### Deny

Describe in the following table the measures you have implemented to block the adversary from taking the malicious actions, staying within the context of the intrusion phase described in this report. For instance, did you block specific IPs at the perimeter firewall, patch targeted vulnerabilities, block e-mails that matched specific patterns, and so on?

|  |  |
| --- | --- |
| Reconnaissance |  |
| Weaponization |  |
| Delivery |  |
| Exploitation |  |
| Installation |  |
| Command and Control |  |
| Actions on Objectives |  |

### Disrupt

Describe in the following table the measures you have established to interfere with the adversary’s attack in progress to cause it to fail. For instance, did you use an intrusion prevention system or firewall to terminate the adversary’s active network connections, quarantine suspicious files, distribute updated antivirus signatures, and so on?

|  |  |
| --- | --- |
| Reconnaissance |  |
| Weaponization |  |
| Delivery |  |
| Exploitation |  |
| Installation |  |
| Command and Control |  |
| Actions on Objectives |  |

### Degrade

Describe in the following table the actions you have taken to slow down or otherwise degrade the attack in progress. One example of such measures might be to configure the network equipment to rate-limit the connections attributed to the adversary.

|  |  |
| --- | --- |
| Reconnaissance |  |
| Weaponization |  |
| Delivery |  |
| Exploitation |  |
| Installation |  |
| Command and Control |  |
| Actions on Objectives |  |

### Deceive

Describe in the following table the steps you have taken to misinform the adversary in the context of the applicable intrusion phase. Deception might involve planting fake assets that might interest the intruder, redirecting the adversary’s network connections, fooling malware into believing the targeted system is already infected, employing honey tokens, and so on.

|  |  |
| --- | --- |
| Reconnaissance |  |
| Weaponization |  |
| Delivery |  |
| Exploitation |  |
| Installation |  |
| Command and Control |  |
| Actions on Objectives |  |

### Destroy

Describe in the following table the offensive actions you have taken against the adversary to reduce their ability to carry out the intrusion. Such steps are generally unavailable to private individuals or firms outside of specific law enforcement or military organizations, although coordination and intelligence sharing with these organizations is within scope of this section.

|  |  |
| --- | --- |
| Reconnaissance |  |
| Weaponization |  |
| Delivery |  |
| Exploitation |  |
| Installation |  |
| Command and Control |  |
| Actions on Objectives |  |

## Intrusion Campaign Analysis

If applicable, summarize in 1 paragraph the relationship between the intrusion discussed earlier in the report and other related intrusions that, when taken together, form a campaign. Mention the indicators and behaviors shared across the intrusions within the campaign. Outline the commercial, geopolitical, or other factors that might have motivated the adversary’s activities.

### Other Intrusions in the Campaign

Describe other incidents or intrusions that share commonalities with the intrusion discussed earlier in the report. Explain whether the shared attributes indicate a low, medium, or high likelihood that the intrusions form a larger campaign. Provide internal and external intrusion names or other relevant identifiers. Include references to related internal and external documents. Clarify when the intrusions occurred.

### Shared Intrusion Attributes

Specify the key indicators and behavioral characteristics that are consistent across intrusions within the campaign. Categorize the attributes according to the kill chain phase when they were exhibited and their relevance to the adversary description, attack infrastructure, capabilities (tactics, techniques, and procedures), and the affected victims. Wherever possible, account for Adversary, Infrastructure, Capabilities, and Victim in each applicable phase of the kill chain.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Adversary | Infrastructure | Capabilities | Victim |
| Reconnaissance |  |  |  |  |
| Weaponization |  |  |  |  |
| Delivery |  |  |  |  |
| Exploitation |  |  |  |  |
| Installation |  |  |  |  |
| Command and Control |  |  |  |  |
| Actions on Objectives |  |  |  |  |

### Campaign Motivations

Outline the likely motivation for the adversary’s activities across the intrusion campaign, including the relevant commercial, geopolitical, or other factors. If practical, offer substantiated theories regarding the attribution of the campaign to specific individuals, groups, or nation states.

### Third-Party References

Provide references to third-party data about the intrusion discussed in this report, the campaign that it is a part of, or the associated adversaries.