Modeling Exercise

Practice time!

- Break up into small groups
  - 4-5 people each
- Read the report provided
- Pull out objects to model in STIX
  - Don’t forget relationships!

Have Fun!

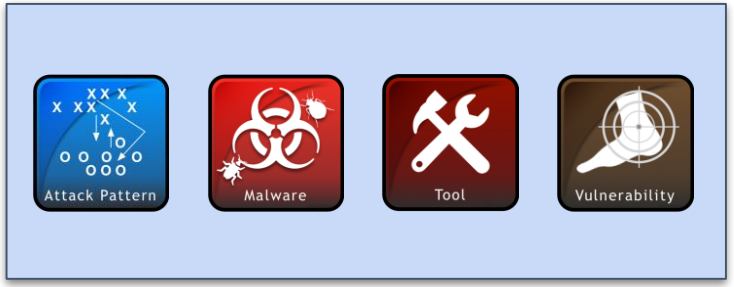
References

Patterning reference card:

https://www.newcontext.com/wp-content/uploads/2018/02/STIX-Patterning-Quick-Reference-Card.pdf

STIX 2.0 Domain Objects (SDOs)

Adversary Objects



TTP Objects

Supporting Objects

Remediation Objects

Detection Objects

What objects did you find?

OASIS

Modeling Exercise – Answers

Basic Modeling

From the report:

Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign

Campaign

In June, FireEye's FireEye as a Service team in Singapore uncovered a phishing campaign exploiting an Adobe Flash Player zero-day vulnerability (CVE-2015-3113). The attackers' emails included links to compromised web servers that served either benign content or a malicious Adobe Flash Player file that exploits CVE-2015-3113.

Vulnerability

Course of Action

Adobe has already released a patch for CVE-2015-3113 with an out-of-band security bulletin (https://helpx.adobe.com/security/products/flash-player/apsb15-14.html). FireEye recommends that Adobe Flash Player users update to the latest version as soon as possible.

The China-based threat group FireEye tracks as APT3, aka UPS, is responsible for this exploit and the activity identified in our previous blog post, Operation Clandestine Fox. This group is one of the more sophisticated threat groups that FireEye Threat Intelligence tracks, and they have a history of introducing new browser-based zero-day exploits (e.g., Internet Explorer, Firefox, and Adobe Flash Player). After successfully exploiting a target host, this group will quickly dump credentials, move laterally to additional hosts, and install custom backdoors. APT3's command and control (CnC) infrastructure is difficult to track, as there is little overlap across campaigns.

Location (2.1 object)

Intrusion Set / Threat Actor

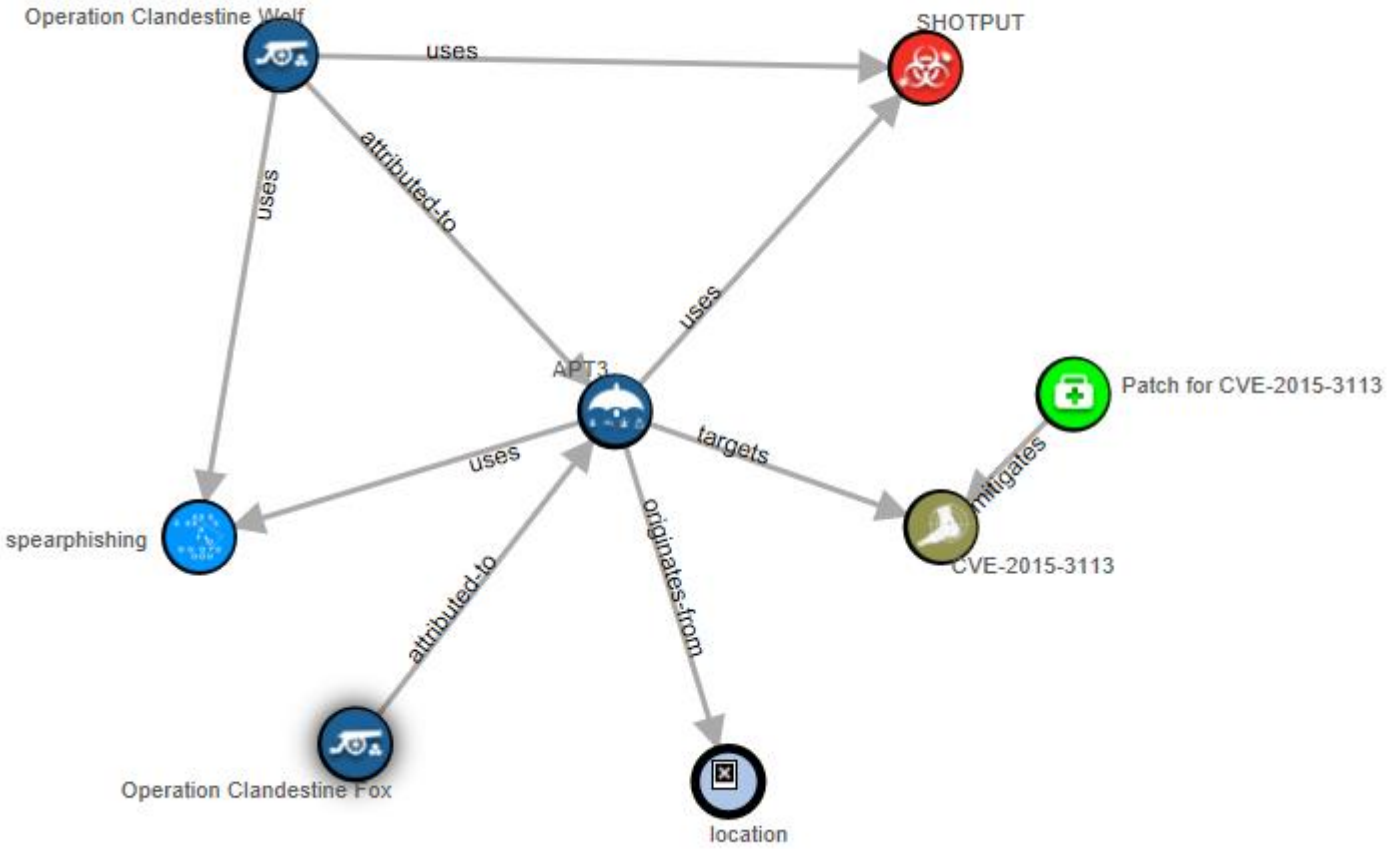
Campaign

Upon clicking the URLs provided in the phishing emails, targets were redirected to a compromised server hosting JavaScript profiling scripts. Once a target host was profiled, victims downloaded a malicious Adobe Flash Player SWF file and an FLV file, detailed below. This ultimately resulted in a custom backdoor known as SHOTPUT, detected by FireEye as Backdoor.APT.CookieCutter, being delivered to the victim's system.

The payload is obscured using xor encoding and appended to a valid GIF file.

Attack pattern

Malware



Moderate Modeling

From the report:

Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign

Campaign

Report

In June, FireEye's FireEye as a Service team in Singapore uncovered a phishing campaign exploiting an Adobe Flash Player zero-day vulnerability (CVE-2015-3113). The attackers' emails included links to compromised web servers that served either benign content or a malicious Adobe Flash Player file that exploits CVE-2015-3113.

Vulnerability

Course of Action

Adobe has already released a patch for CVE-2015-3113 with an out-of-band security bulletin (https://helpx.adobe.com/security/products/flash-player/apsb15-14.html). FireEye recommends that Adobe Flash Player users update to the latest version as soon as possible.

The China-based threat group FireEye tracks as APT3, aka UPS, is responsible for this exploit and the activity identified in our previous blog post, Operation Clandestine Fox. This group is one of the more sophisticated threat groups that FireEye Threat Intelligence tracks, and they have a history of introducing new browser-based zero-day exploits (e.g., Internet Explorer, Firefox, and Adobe Flash Player). After successfully exploiting a target host, this group will quickly dump credentials, move laterally to additional hosts, and install custom backdoors. APT3's command and control (CnC) infrastructure is difficult to track, as there is little overlap across campaigns.

Location (2.1 object)

Intrusion Set / Threat Actor

Campaign

In the last several weeks, APT3 actors launched a large-scale phishing campaign against organizations in the following industries:

- Aerospace and Defense
- Construction and Engineering
- High Tech
- Telecommunications
- Transportation

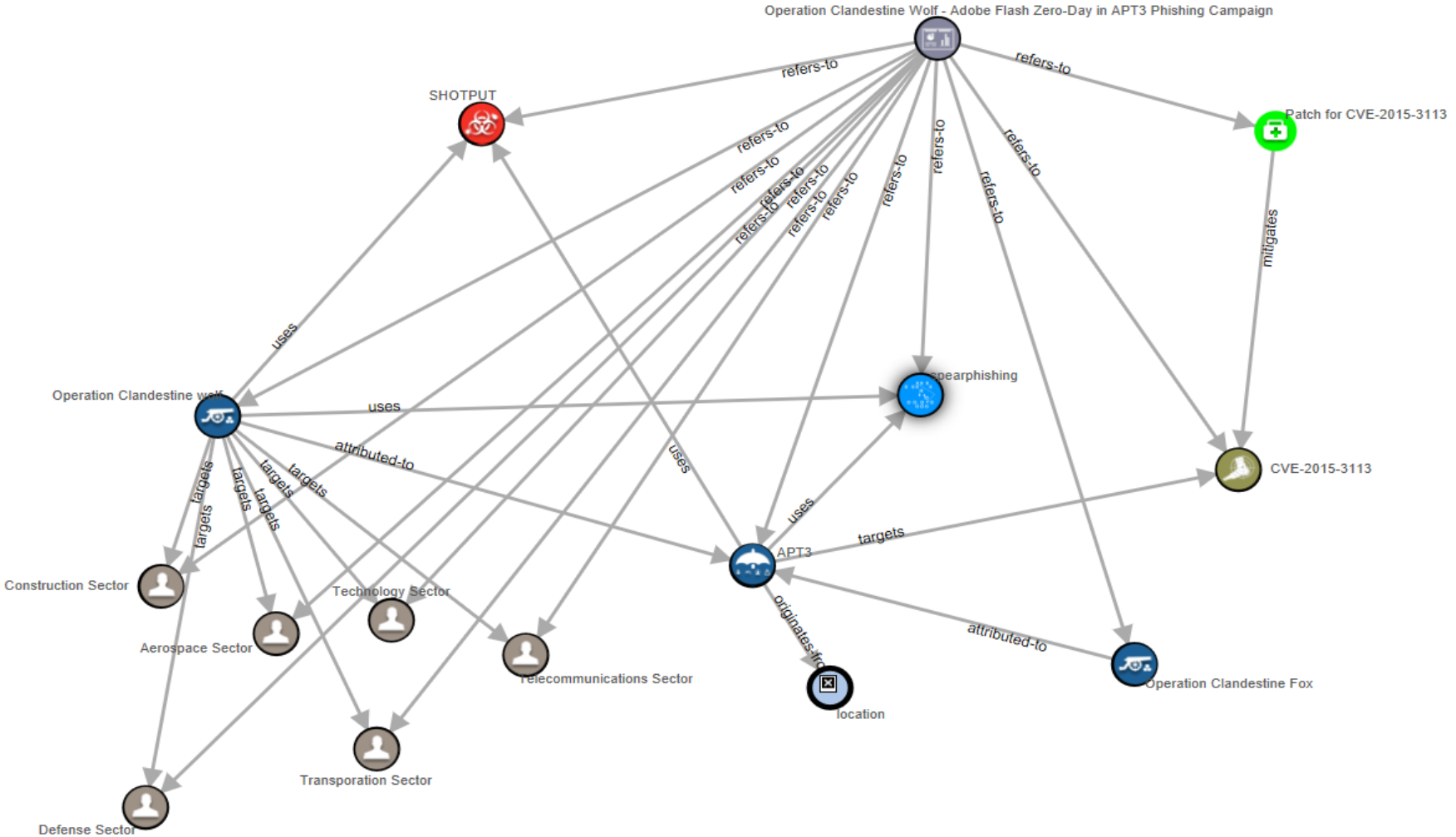
Identity Objects

Upon clicking the URLs provided in the phishing emails, targets were redirected to a compromised server hosting JavaScript profiling scripts. Once a target host was profiled, victims downloaded a malicious Adobe Flash Player SWF file and an FLV file, detailed below. This ultimately resulted in a custom backdoor known as SHOTPUT, detected by FireEye as Backdoor.APT.CookieCutter, being delivered to the victim's system.

The payload is obscured using xor encoding and appended to a valid GIF file.

Attack pattern

Malware


Operation Clandestine Wolf - Adobe Flash Zero-Day in APT3 Phishing Campaign
SHOTPUT
Patch for CVE-2015-3113
Operation Clandestine wolf
spearphishing
CVE-2015-3113
APT3
Construction Sector
Technology Sector
Aerospace Sector
Telecommunications Sector
location
Operation Clandestine Fox
Transporation Sector
Defense Sector
refers-to
uses
attributed-to
targets
originates-from
mitigates

Advanced Modeling

From the report:

Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign

Campaign

Report

In June, FireEye's FireEye as a Service team in Singapore uncovered a phishing campaign exploiting an Adobe Flash Player zero-day vulnerability (CVE-2015-3113). The attackers' emails included links to compromised web servers that served either benign content or a malicious Adobe Flash Player file that exploits CVE-2015-3113.

Vulnerability

Course of Action

Adobe has already released a patch for CVE-2015-3113 with an out-of-band security bulletin (https://helpx.adobe.com/security/products/flash-player/apsb15-14.html). FireEye recommends that Adobe Flash Player users update to the latest version as soon as possible.

The China-based threat group FireEye tracks as APT3, aka UPS, is responsible for this exploit and the activity identified in our previous blog post, Operation Clandestine Fox. This group is one of the more sophisticated threat groups that FireEye Threat Intelligence tracks, and they have a history of introducing new browser-based zero-day exploits (e.g., Internet Explorer, Firefox, and Adobe Flash Player). After successfully exploiting a target host, this group will quickly dump credentials, move laterally to additional hosts and install custom backdoors. APT3's command and control (CnC) infrastructure is difficult to track, as there is little overlap across campaigns.

Location (2.1 object)

Intrusion Set / Threat Actor

Campaign

Two Attack Patterns

In the last several weeks, APT3 actors launched a large-scale phishing campaign against organizations in the following industries:

- Aerospace and Defense
- Construction and Engineering
- High Tech
- Telecommunications
- Transportation

Identity Objects

Upon clicking the URLs provided in the phishing emails, targets were redirected to a compromised server hosting JavaScript profiling scripts. Once a target host was profiled, victims downloaded a malicious Adobe Flash Player SWF file and an FLV file, detailed below. This ultimately resulted in a custom backdoor known as SHOTPUT, detected by FireEye as Backdoor.APT.CookieCutter, being delivered to the victim's system.

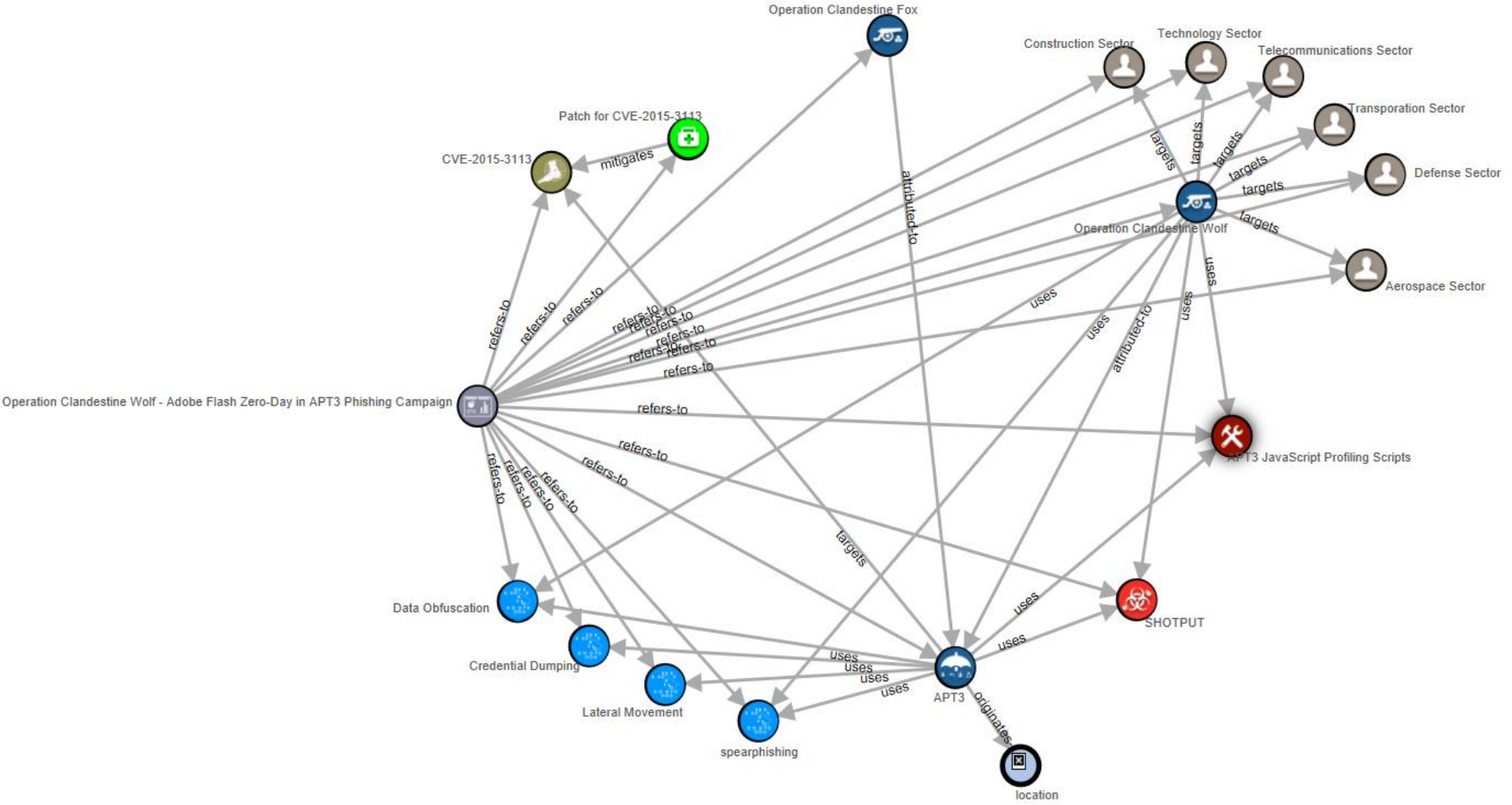
The payload is obscured using xor encoding and appended to a valid GIF file.

Attack pattern - phishing

Tool

Malware

Attack pattern – data obfuscation


Operation Clandestine Fox
Construction Sector
Technology Sector
Telecommunications Sector
Transporation Sector
Defense Sector
Aerospace Sector
Patch for CVE-2015-3113
CVE-2015-3113
mitigates
Operation Clandestine Wolf
Operation Clandestine Wolf - Adobe Flash Zero-Day in APT3 Phishing Campaign
APT3 JavaScript Profiling Scripts
Data Obfuscation
Credential Dumping
Lateral Movement
spearphishing
APT3
SHOTPUT
location
attributed-to
targets
uses
refers-to
originates

What do the objects look like?

(abbreviated)

Intrusion Set, Campaign, and Attack Pattern

Name: "APT3"
Labels: "nation-state"
Aliases: "UPS"

Name: "Operation Clandestine Wolf"
Description: "Operation Clandestine Wolf is the name of a phishing campaign by APT3. It exploited CVE-2015-3113, and ultimately delivered the SHOTPUT malware."

Name: "Phishing"
External References:
Source: capec
external_id: CAPEC-98

Vulnerability, Tool and Location

Name: "CVE-2015-3113"
External References: "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3113"

Name: "APT3 JavaScript profiling script"
Tool types: "information-gathering"

Region: "China"

COA, Identity and Malware

Name: "CVE-2015-3113 remediation"
Description: "Patch Adobe flash"
External Ref: "https://helpx.adobe.com/security/products/flash-player/apsb15-14.html"

Name: "Technology Sector"
Identity Class: "Class"
Sector: "technology"

Name: "SHOTPUT"
Labels: "backdoor"
Description: "Here's everything I know about SHOTPUT"

Questions?

Sarah Kelley

skelley@mitre.org