WEBINAR SUMMARY

July 7, 2020

# How Attackers Confuse Investigators with Cyber False Flag Attacks

**Vince Stross,** Principal Security SE, ExtraHop
**Jake Williams,** Co-founder, Rendition Infosec

## KEY TAKEAWAYS

- Simple yet effective false flag attacks sow doubt and distract investigators.
- False flag attacks can occur in any phase of the Cyber Kill Chain.
- ExtraHop's network detection and response solution helps identify false flags.

in partnership with

ExtraHop

## OVERVIEW

Cybersecurity investigators are interested in not just what happened during an attack, but who attacked the organization and why. False flag cyberattacks intentionally misdirect investigators, leading them to doubt their understanding of which entity attacked and why they attacked.

Understanding the techniques used in false flag attacks can help investigators be more critical of the information they discover, and perhaps dig deeper. ExtraHop's network detection and response (NDR) solution provides incident responders with the detailed data necessary to look critically at attacks and identify false flags.

## CONTEXT

Jake Williams discussed the techniques attackers use to plant false flags. Vince Stross discussed how ExtraHop helps incident responders gather more information about attacks, which can help identify false flag operations.

## KEY TAKEAWAYS

### Simple yet effective false flag attacks sow doubt and distract investigators.

Hackers use false flag cyberattacks to fool victims into misidentifying the perpetrators or the purposes of an attack. An attacker's potential goal for a false flag operation may be:

- **Distract investigators** to increase the cost of forensics.
- **Sow seeds of doubt** about attribution.
- **Delay the investigation** long enough to prevent action.
- **Cause another entity to act** based on preliminary forensics, such as launch a retaliation against the incorrectly identified perpetrator.
- **Cause experienced investigators to believe false attributions**, even at the conclusion of the investigation.

Successful false flag operations are tailored to the sophistication level of the target, as measured by the intersection of instrumentation and investigator expertise/resourcing. It the target is incapable of seeing or understanding the artifact that the attack leaves behind, then the operation cannot achieve its goal.

### False flag attacks can occur in any phase of the Cyber Kill Chain.

Lockheed Martin's Cyber Kill Chain provides a useful model for understanding the deterministic phases of an adversary operation. False flag attacks can occur throughout any of the seven phases of the Cyber Kill Chain.

**Seven Phases of Lockheed Martin's Cyber Kill Chain**

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and control (C2)
7. Actions on objectives (AoO)

Many of the techniques used to attack targets, such as leasing infrastructure in the country the attacker intends will take the blame, are legal and can be used in red team security engagements. Questions about the legality and ethics of using various techniques for testing should be discussed with the company's lawyer before they are used.

### 1. Reconnaissance

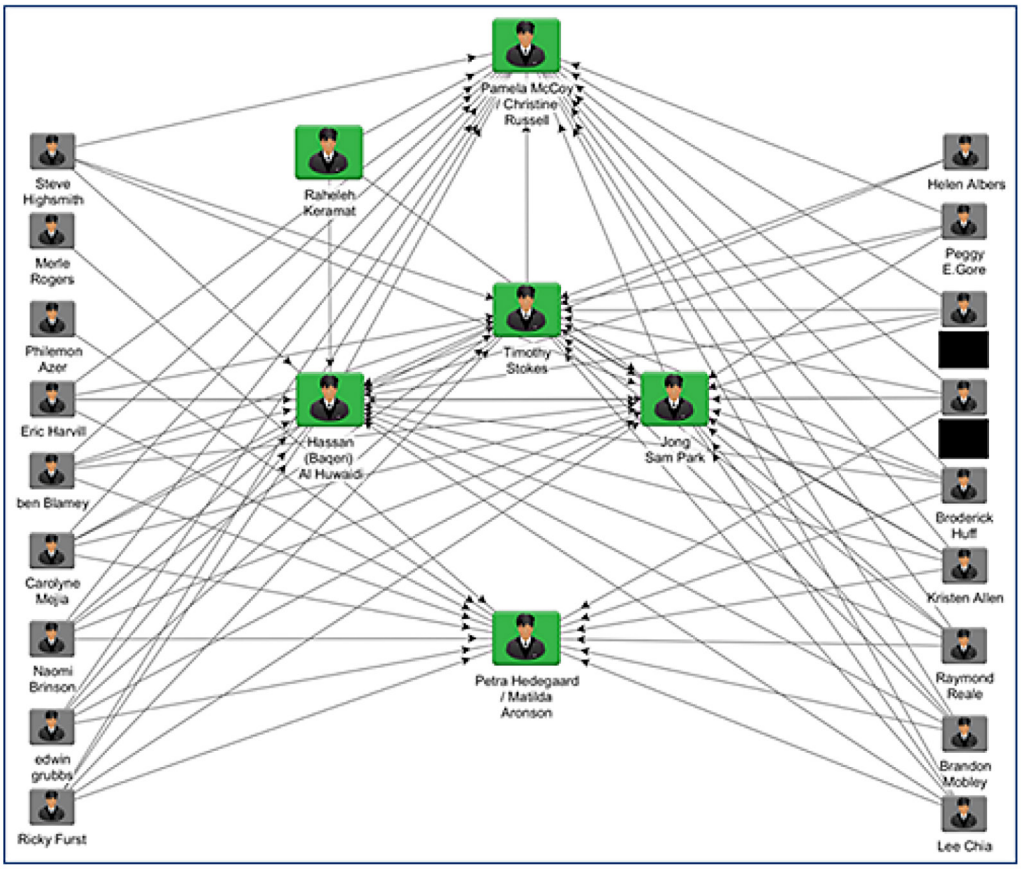
Common reconnaissance phase techniques for false flag operations include:

- Buying, leasing, or compromising infrastructure in the country being blamed, such as using internet otocol (IP) addresses that come from a specific country.
- Changing user agents (Yandex, Baidu, Qihoo).
- Changing HTTP(S) referrers.
- Changing browser accept-language settings.
- Creating social media links to known or suspected attacker personas.
- Using revealed email addresses to register in public forums.

#### Reconnaissance Example: Faking Personas

Attackers often use social media and supporter networks when creating fake personas. Following known threat actors on social media sites links the false persona to the group, even if they are not followed back. This is used to confuse investigators, tricking them into thinking the persona is part of the threat group.

**Example: Faked persona network for a suspected Iranian threat group**



> "If you as an attacker want to appear to be part of a group, it's as simple as creating a convincing persona and then following other people you know are linked to that threat actor."
>
> *Jake Williams, Rendition Infosec*

**2. Weaponization**

False flag operation techniques in the weaponization phase include:

- Forging document metadata, such as including a Windows Cyrillic code page in the metadata of documents purportedly stolen from the Democratic National Committee in the 2016 election.
- Modifying Rich Headers in the portable executable (PE) header; these carry information about the toolchain used to build the executable and can be used to identify malware.
- Using known PowerShell code snippets.
- Embedding content known to match patsy Yara signatures in executables.
- Using patsy language snippets, such as from the CIA's UMBRAGE team.

**3. Delivery**

Delivery techniques for false flag operations include:

- Using virtual private network (VPN) infrastructure providers known to be used by the patsy.
- Using port forwarding to camouflage email servers so they look as though they are pointing to the patsy government infrastructure.
- Creating operations security (OPSEC) "mistakes" during delivery. For example resend a phishing document from a country-specific free email domain to confuse investigators.

**4. Exploitation**

Exploitation-phase false flag attacks are difficult. They typically require nation-state level resources and don't provide a real return on investment. When carried out, they typically use the same general attack techniques used by the patsy country or group. In some cases, exploits can be stolen from the patsy and reused.

**5. Installation**

False flag techniques during installation include:

- Using some of the same host-based artifacts that known patsy malware uses.
- Employing the same patterns for registry keys and file/director names as used by the country or group being mimicked.
- Using mutual exclusion objects, or mutexes, but only if the target is likely to discover them.

### 6. Command and Control (C2)

C2 techniques are hard to catch but can be used for false flag operations. Common techniques include using:

- Specific protocol variations commonly used by the patsy.
- HTTP server software and configured modules, especially if unique software or configurations are used.
- Remote language used for C2 web pages (PHP, Java, etc.).
- C2 webpage and HTTPS variable naming conventions.
- Unique cipher suites used for encryption.

### 7. Actions on Objectives (AoO)

In the AoO phase, investigators of advanced persistent threats (APT) intrusion focus on artifacts of execution to determine what actions were performed, such as what the attacker was looking at or stole. False flag techniques during the AoO phase tries to confuse intent by impacting the tools used to investigate artifacts, such as:

- Copying prefetch entries from remote machines or editing prefetch entries.
- Modifying AppCompactCache to insert fake executables run.
- Poisoning the well with AmCache; as the tool stores the full path of the executable and the secure hash algorithm 1 (SHA1), it is extremely useful for leaving false flags.
- Confusing intent by feeding false data to WordWheel, which stores all Window search bar searches.
- Changing TypedURLs registry keys in NTUSER.DAT/.
- Providing fake information for visited sites and saved forms (e.g., fake logins).
- Impacting remote desktop protocol (RDP) usage, including keymapping.
- Poisoning command histories on the target, which is useful for Linux.
- Modifying PowerShell transcripts.

## ExtraHop's network detection and response solution helps identify false flags.

A leader in cloud-native NDR, ExtraHop takes advantage of the thousands upon thousands of artifacts and data points it extracts off networks in real time to help identify both actual attacks and false flags.

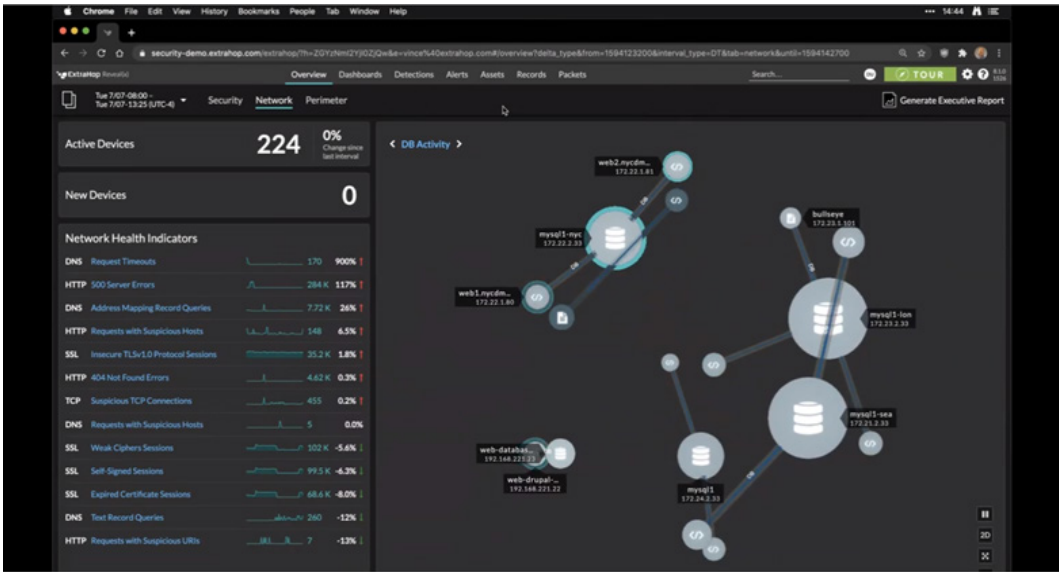
> "ExtraHop provides full 360-degree coverage [of all the network communications for] on-premises and in the cloud."
>
> *Vince Stross, ExtraHop*

**ExtraHop provides insight into potential security breaches**


Most NDR tools on the market focus on signatures and rules. ExtraHop Reveal(x) focuses on behavior, applying machine learning (ML) algorithms to identify anomalous behavior and enabling rapid drill-down.

For example, while other solutions only record metadata about alerts, ExtraHop records all of the metadata and then hooks detections to it. This supports an investigative workflow, which can be used to identify false flags.

**ExtraHop records all metadata, enabling deep research into potential attacks**




## ADDITIONAL INFORMATION

For a demo of ExtraHop Reveal(x), visit http://extrahop.com/demo/

# BIOGRAPHIES

## Vince Stross

Principal Security SE, ExtraHop

Vince is a Principal Security SE at ExtraHop with over 20 years of experience in security, IT operations, cloud/hybrid full-stack development, management, and gardening. Vince considers himself a Comprehensivist. He believes that helping his customers shine a light on their unique threat landscape requires comprehensive understanding and visibility into the complex relationships of interconnected systems in the East-West traffic corridor.

## Jake Williams

Jake Williams

Jake Williams is the co-founder of Rendition Infosec and a principal consultant performing incident response, computer forensics, penetration testing, malware reverse engineering, and exploit development. Jake is a certified SANS Instructor and course author and trains thousands annually in information security topics.

Prior to founding Rendition Infosec, Jake worked in various roles with the US DoD performing offensive and defensive cyber operations in classified environments. Jake regularly briefs Fortune 500 executives on information security topics and has a knack for translating complex technical topics into verbiage that anyone can understand.