

AWAKE In Action

Real world incidents detected and stopped by The Awake Security Platform

Now that security tools that have become proficient at identifying noisy, malware-based attacks, cyber criminals have adapted to using non-malware techniques in a majority of breaches. They rely on tools that already exist within the environment, abusing insider credentials or using SSL tunnels to legitimate sites for command and control. Attackers are also targeting the ever-growing population of non-traditional devices on the network, devices that often lack the same level of security controls. This means that security teams must now detect malicious intent that blends with business-justified activity, a task that is both tedious and challenging for most analysts.

The Awake Security Platform is powered by the real-world expertise of the world's foremost investigators. It applies artificial intelligence to bring these human skills to all customers, instantly analyzing billions of communications to discover every device, user and application on the network. Through autonomous hunting and investigation Awake then detects malicious intent from insiders and external attackers alike. With exhaustive intelligence from the network, Awake uniquely identifies mal-intent to stop lateral movement, credential abuse, data exfiltration, and much more.

Organizations across industries use Awake every day to identify and stop modern threats from both internal and external actors with various malicious objectives. The following pages outline real-world examples where Awake was used to detect and stop interesting and sophisticated threats.

These examples include:

- Employee Selling Corporate Secrets
- Following the Trail of a Spear Phishing Campaign
- Contractor Spying with Security Cameras
- Spear Phishing Detection and Intelligent Response
- Tapping IP Phones in Sensitive Locations

Employee Selling Corporate Secrets

In early 2018, an employee at a large media and entertainment company was caught selling extremely sensitive intellectual property to a third-party. This type of activity would be especially hard to detect using traditional tools such as threshold-based solutions that look for large or anomalous uploads. In this case the files were being sent infrequently, and when they were sent, the amount of data traversing the network was very small.

In addition, this was a case where the perpetrator was authorized to access the information he was sharing. The files in question were sent to this person's corporate email account from others within the organization. And the person did not forward or send all of the attachments contained in any given email. They were selective and only sent very specific files, making their actions unlikely to trigger alarms that typically look for large or continuous uploads.

While the amount of data being uploaded was small and usually only occurred a handful of times per week, Awake identified the activity as "persistent" and "unique," worthy of a closer look.

This is the type of "low and slow" activity that most other solutions miss. However, Awake allowed this organization to identify the activity because of its deep analysis of all traffic crossing the organization's network. Ultimately, the evidence presented by Awake allowed the organization to pursue legal action.

Industry

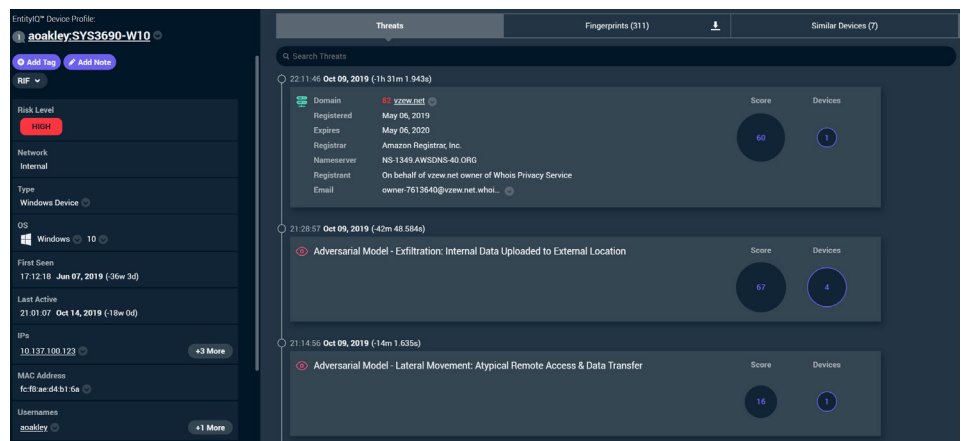
Media and Entertainment

Attacker Objective

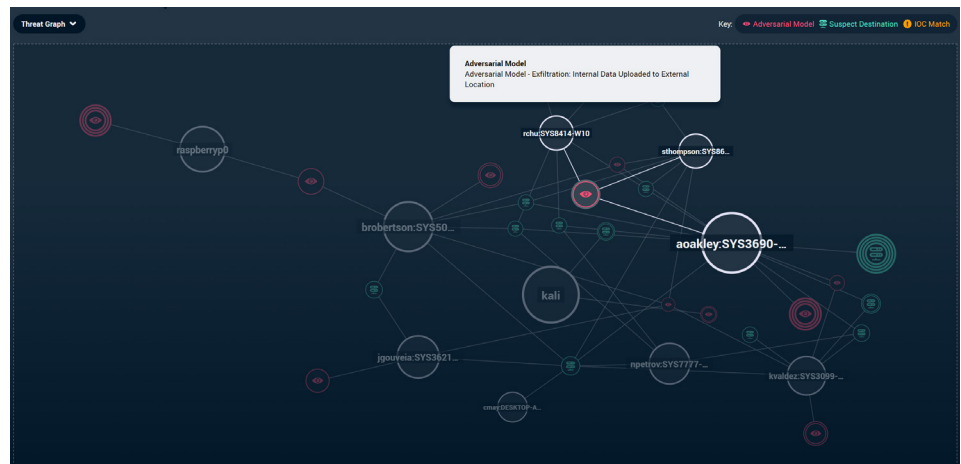
Profit from selling intellectual property

Awake detected this threat as:

- ✓ Rare when compared to any other device in the enterprise that interacts with the same destination domains.
- ✓ Persistent in that it occurred multiple times over a few weeks.
- ✓ Unique to a particular device or person when compared to other similar devices or people, such as those in similar job functions.



The device detail page on Awake's platform shows a timeline with lateral movement, internal data transfer and finally data exfiltration.



The dashboard highlights the risk based on the adversarial models triggered by the perpetrator's device.



Following the Trail of a Spear Phishing Campaign

A multi-billion dollar oil and gas company identified a phishing campaign that targeted 80 people within the organization, and learned that nearly half of them clicked a link in the deceptive email.

The security team was first alerted to this attack by a user who called the help desk to report the suspicious email. After receiving that call, the Awake Security Platform enabled a swift and efficient response that would have taken days to accomplish for analysts using traditional tools.

The Awake Security Platform detected that devices that interacted with the attacker domain subsequently also visited a known good domain. The good domain turned out to be providing JavaScript used to mask the password being typed into the browser to make the site look like a legitimate SharePoint login. However, this exposed the tactics, techniques and procedures (TTPs) being used by the attacker and enabled the security team to identify which users had revealed their usernames and passwords.

Further examination of the attack artifacts revealed an email address where credentials were being sent. This email address was used to identify other domains that share the same attributes such as how and when the domain was registered, where it was hosted, etc.

Most phishing investigations would stop at simply blocking the sender and the bad domain, making it very simple for an attacker to try again. But by enabling the analyst to pivot in one click to other associated domains, Awake helped expose the entire attacker infrastructure.

The company is now using Awake to identify any device using any protocol to visit any domain/IP with TTPs of these attackers. This means that the company does not need to know the list of domains the attacker has registered in the past or will register in the future, nor the IPs they use. They'll simply be alerted if any of those TTPs are seen again.

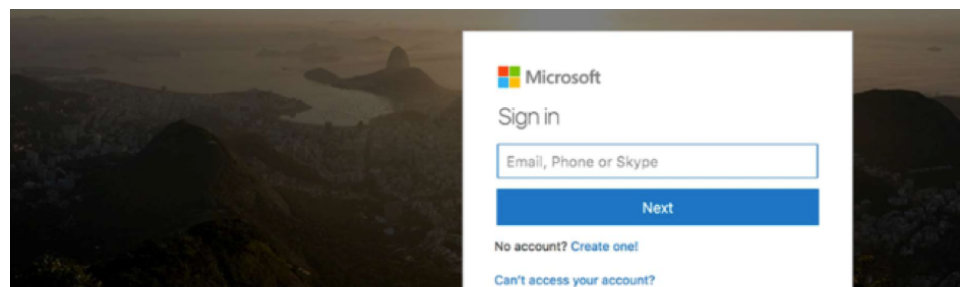
While a detailed investigation like this could typically take days, it was completed in minutes with Awake. And ultimately, Awake turned intelligence generated during the investigation into actionable protection for the organization.

Industry
Oil and Gas

Attacker Objective
Steal credentials

Awake detected this threat by:

- ✓ Surfacing in seconds, the 35 users who clicked on the phishing link as well as the subset that gave up their credentials
- ✓ Highlighting the fake Microsoft SharePoint login site that was used to harvest credentials.
- ✓ Identifying all the devices the victims were using and the different IP addresses those devices had used throughout the time period in question.
- ✓ Exposing the broader attack infrastructure including other domains being used for credential theft.



After clicking on a link, users were directed to this page which looked like a Microsoft SharePoint login but was harvesting credentials and sending them to the attacker.

```
POST["userid"];

TML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">

;#105;#103;#110;#32;#73;#110; to your account</title>
e="text/javascript" src="https://www.sitepoint.com/examples/password/MaskedPassword/MaskedPassword.js"></s
```

The look-alike Microsoft SharePoint login page had an embedded password-stealing script.

Contractor Using Security Cameras to Spy

Surveillance cameras are common devices in any large enterprise, especially those in critical infrastructure industries. One Awake customer in the energy industry had thousands of these cameras on its network and learned that a contractor was using them to spy on employees in sensitive locations.

Identifying what is on the network is a critical first step to securing it, especially as people bring their own devices to work and the number of Internet of Things (IoT) devices steadily increases. The Awake Security Platform automatically identifies and creates profiles of all devices on a network – which in this case, included thousands of IP cameras.

Importantly, these cameras had been compromised before the organization began using the Awake platform. For other security solutions that baseline “normal” activity, this would be a challenge because they wouldn’t see anything anomalous about activity that was present before they got there. However, Awake’s method of profiling each entity and comparing the activity of entities most similar to each other made a significant difference.

Specifically, Awake identified one camera that was communicating with a destination network that none of the other cameras were communicating with. Additionally, Awake identified that this malicious communication was occurring over FTP. The security team was able to retrieve the FTP credentials and then find only one other system on the network that had accessed the same FTP server in question—a device in use by an IT contractor.

Awake Security

Android Device Profile

LogiCam3

Add Tag

Add Note

Risk Level

HIGH

Network

Internal

Type

Linux Device

Threats

Fingerprints (8)

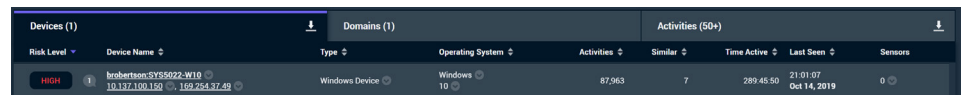
Similar Devices (2)

Search Fingerprints

This	All	Dev	Fingerprints
33.3% of 3.5k	3	TLS Cert Subject Organization Logitech Inc	
100.0% of 30	1	Destination ASN Network Hurricane Electric LLC, US	
33.3% of 36	3	HTTP Response Content Type application/x-kz	

Awake identified an unexpected network connection from an IP camera.

The security team found multiple cameras that were impacted by the malicious activity, including some in data centers and secure facilities for managing critical infrastructure. The team determined nearly all of their cameras were badly configured, giving the attacker easy access to any of them. This customer is an ongoing nation-state target, so identifying this part of their attack surface was critical.



Risk Level	Device Name	Type	Operating System	Activities	Similar	Time Active	Last Seen	Sensors
HIGH	brobertsonSYSS022-W10	Windows Device	Windows	87,963	7	289:45:50	21:01:07 Oct 14, 2019	0

Identifying the malicious contractor by isolating devices that connected to the FTP location.

Industry
Energy

Attacker Objective
Corporate espionage

Awake detected this threat by:

- ✓ Automatically profiling all devices on the network including the thousands of IP cameras.
- ✓ Detecting a single camera that was communicating with a destination network that none of the other cameras were interacting with.
- ✓ Identifying one other device that had accessed the same destination in question—a device in use by an IT contractor.



Spear Phishing Detection and Intelligent Response

A small group of employees at a petroleum refining giant were targeted by a sophisticated spear phishing campaign aimed at stealing credentials to access important information and applications.

The targeted nature of spear phishing makes it especially dangerous because most often, an organization does not become aware of compromised credentials until they're already being used by bad actors. This is because the people being "phished" willfully click on malicious links or provide credentials to attackers who have become extremely adept at spoofing emails to look legitimate. With so much information about a person's professional and personal lives available online publicly, it's increasingly easy for attackers to deceive their targets.

However, while spear phishing attacks vary based on the attacker and the target, there are certain tactics, techniques and procedures (TTPs) common in almost all attacks of this nature. For example, even targeted campaigns are rarely isolated to a single user, so once an email is delivered, a small number of users will typically "take the bait" and click on a link.

At this customer, the Awake Security Platform notified the security team as soon as it discovered the potential breach. The platform recognized that a small number of devices in the organization were visiting a destination domain that had not been previously seen on this network but also had other signs of being a suspect destination..

The security team was then able to take additional steps to further secure the organization. For example, the team was able to detect the use of compromised credentials on systems where they had not been previously used. Similarly, the team created a mechanism to automatically look for attacker attempts to use typosquatting, which typically requires complex manual efforts of forensic detection. With Awake, this complexity is invisible to the analyst who simply invokes a function.

Ultimately, the organization stopped the phishing attack while taking proactive measures to ensure that stolen credentials could not be maliciously used while simultaneously teaching the system to look for similar techniques.

Industry
Petroleum Refining

Attacker Objective
Access critical applications

Awake detected this threat by:

- ✓ Determining which users clicked on the link and submitted credentials, versus those who simply clicked the link and then closed the page.
- ✓ Identifying all the devices that communicated with the destination in question.
- ✓ Generating a list of all the systems where credentials that were now compromised had been used prior to the phishing incident.

Query expression

```
activity.kerberos.client_name.string in incident_20180815.victim.names && !(device.name like incident_20180815.victim.devices)
```

Title

Incident 20180815: Compromised credential used on new system

Severity

10

Expiration date (UTC)

30 days from now 2018-09-15 00:31:00

Awake allowed analysts to quickly and easily create new detections to stop compromised credentials from being used in the future.

Tapping IP Phones In Sensitive Locations

A major consumer finance institution in the U.S. with more than 17,000 IP phones on its network used the Awake Security Platform to determine that four of its phones were being electronically tapped.

The organization's large security team struggled with visibility into the IP phones since existing security controls were blind to these devices. They also exist for the sole purpose of communicating with destinations outside the company, so large volumes of traffic being exchanged with external sources is not unusual. However, it was unusual that only a small number of phones were uploading data to a particular suspect destination every so often.

To find this activity, Awake's analytics did not simply compare the current behavior of these devices to what it observed in the past. In this case, the devices were compromised long before Awake was deployed in the environment so a more basic anomaly analysis would have considered the malicious activity to look "normal" compared to what had been previously observed. Instead, Awake first identified all of the devices with similar behavioral fingerprints and then compared these devices to each other. This allowed it to spot four devices that deviated from the norm.

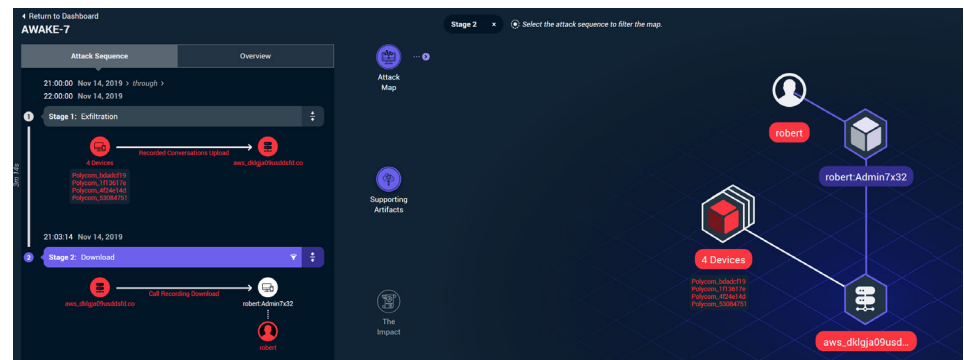
The security team determined that an IT employee was responsible for this attack. He was attempting to obtain information to be used in blackmail and ransom operations. The detailed information gained from Awake's platform enabled the company to immediately stop the activity and gain evidence for legal action. Awake's analysis enabled the security team to quickly find the compromised phones. The phones in question were stationed in executive conference rooms and other sensitive locations that were frequently the site of high-level and sensitive company discussions.

Industry
Financial Services

Attacker Objective
Blackmail and ransom

Awake detected this threat by:

- ✓ Comparing behaviors of IP phones with other IP phones in the environment to spot outliers.
- ✓ Using encrypted traffic analysis to profile the source and destination of the communication.



Awake detected 4 IP phones (out of more than 17,000) that were uploading data to a suspect destination. The attack map correlates and visualizes the threat.



For additional information about Awake please visit awakesecurity.com
©2019 Awake Security, Inc.

About Awake Security

Awake Security is the only advanced network traffic analysis company that delivers a privacy-aware solution capable of detecting and visualizing behavioral, mal-intent and compliance incidents with full forensics context. Powered by Ava, Awake's security expert system, the Awake Security Platform combines federated machine learning, threat intelligence and human expertise. The platform analyzes billions of communications to autonomously discover, profile and classify every device, user and application on any network. Through automated hunting and investigation, Awake uncovers malicious intent from insiders and external attackers alike. The company is ranked #1 for time to value because of its frictionless approach that delivers answers rather than alerts.