Identify Targeted Attacks with Symantec Dynamic Adversary Intelligence

Overview

Every day, there are data breaches, virus outbreaks, and many other "disasters" caused by cyber-attacks across the world. Attackers are moving faster, evolving with new attack techniques. Yet most customers are not able to stay up-to-date with today's sophisticated threats. Symantec introduced Dynamic Adversary Intelligence (DAI) to give customers direct benefit from our global threat intelligence and enable them to apply it to their local environment. DAI exposes prioritized threat data to customers, including threat actors, attack techniques, indicators-of-compromise, and more. It also helps distinguish high-impact threats via incidents on the Symantec Advanced Threat Protection console, so that action can be taken on these incidents first.

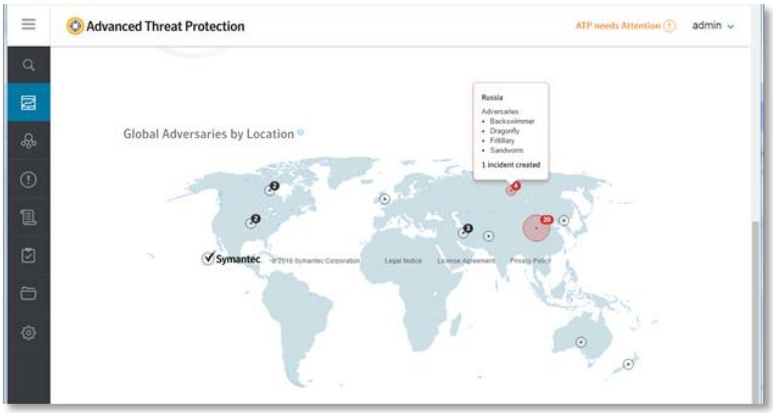
Customer Benefits

- Quickly identify whether customers are currently under a targeted attack
- Prioritize the most critical incidents and shorten the window of exposure
- Highlight local customer impact by monitoring indicators from all known targeted attack adversaries drawing from our global threat intelligence
- Provide granular context to help prioritize and enable faster response to an attack, including:
  - ➢ Information on an adversary, their methods and motives
  - ➢ A list of associated indicators that the customer can use to detect the attack, including additional URLs/IPs to block.
  - ➢ A list of software vulnerabilities used by the adversary to help customer prioritize patching
  - ➢ Links to available literature on the attacks from the security community.

Introducing Dynamic Adversary Intelligence

What's DAI

DAI stands for Dynamic Adversary Intelligence, a high-value feed of actionable intelligence data extracted from comprehensive investigations into targeted attacks. It allows customers to respond to attacks more appropriately, as it highlights the targeted attacks that pose the highest threat level and thus require the most urgent level of response.



Investigations are typically undertaken in response to incidents experienced by our customers, or to third-party reports on targeted attacks that are considered significant. There are various factors Symantec takes into account to determine a significant targeted attack, including:

- Complexity of the attack
- High-value assets that have been targeted
- Prevalence of the attack within Symantec's global telemetry
- Potential for high-data loss or other negative outcomes from the attack
- Past history of the adversary who launched the attack
- Other factors specific to a particular attack

These investigations are carried out by highly skilled Symantec security incident response analysts. They leverage our market leading global telemetry in tandem with detailed analysis and investigation tools to provide exclusive insights on targeted attacks. The DAI feed consists of two types of information: ***Indicators-of-Compromise*** and ***Adversary data***. It is presented as an incident generated in the Symantec Advanced Threat Protection console. Customers can find both types of information and more details of targeted attacks from one place.

Indicators of compromise

An indicator of compromise (IOC) is defined as an observable artifact which indicates a computer intrusion has taken place. IOCs in the DAI feed relate specifically to attacks that Symantec believes to be targeted. IOCs include hash values of files and network patterns (URL pattern/IP pairs) associated with targeted attack actors that have been investigated by Symantec.

Adversary Data

In order to give the customer context around an IOC, Symantec publishes information around known adversaries in the DAI feed. Available information will depend on an adversary in question, as each will vary in tools, techniques and procedures that they use to carry out attacks.

Adversary information includes but not limits to:

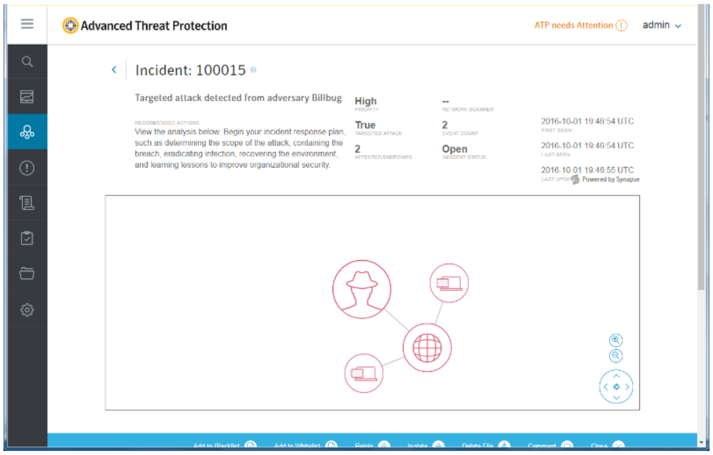
- Known attack vectors (e.g. email, watering-hole, software vulnerabilities)
- Known third party aliases from other security vendors
- References to publicly available literature on the attacks
- Known software vulnerabilities used in the attack
- Known malware families used by the adversary
- The date of the earliest known adversary activity as seen by/corroborated by Symantec
- The countries from where Symantec believes adversaries are coordinating their activities. Note this is based on a number of factors including the victim profile, the time of day when attackers are active, the location of command & control servers that may indicate where the attackers are launching their current attack from[1]

[1] The country listed only reflects where the attackers are operating from. Symantec does NOT imply that a nation-state government is behind the attack.

- The motivation behind the attack. Symantec provides information speculation on the attack motivation, based on available information, such as targeted victims, capabilities of adversary etc.

Prioritize Critical Incidents

Whilst Symantec provides protection against both targeted and indiscriminate cyber-attacks, it recognizes a customer's challenge in prioritizing response to different security alerts in their environment. DAI helps customers distinguish high-impact threats via incidents on the Symantec Advanced Threat Protection console, so that customers can take immediate action on these incidents first.



Advanced Threat Protection

ATP needs Attention

admin

Incident: 100015

Targeted attack detected from adversary Billbug

RECOMMENDED ACTIONS:
View the analysis below. Begin your incident response plan, such as determining the scope of the attack, containing the breach, eradicating infection, recovering the environment, and learning lessons to improve organizational security.

PRIORITY: High
TARGETED ATTACK: True
AFFECTED ENDPOINTS: 2
NETWORK SCANNER: --
EVENT COUNT: 2
INCIDENT STATUS: Open
FIRST SEEN: 2016-10-01 19:46:54 UTC
LAST SEEN: 2016-10-01 19:46:54 UTC
LAST UPDA 2016-10-01 19:46:55 UTC

Symantec's Internet Security Threat Report in 2016 shows a constant increase in the number of targeted attacks identified when compared with previous years. The DAI feed is focused directly on identifying and contextualizing those targeted attacks. Our goal is to identify and prioritize a high-impact incident for customers. By alerting customers to the occurrence of a targeted attack indicator in their environment, as well as supplying actor context, we enable a faster response via a prioritized alert.

Use Cases

Use Case 1: DAI Provides Deep Visibility into Targeted Attacks

Dynamic Adversary Intelligence provides indicators that can identify whether targeted attack is taking place in customer environment. In addition, it exposes threat data and adversary information behind the attack to customers.

Example:

Buckeye is a cyberespionage group that is believed to have been operating for well over half a decade. Traditionally, the group mostly attacked organizations in the US. However, Symantec found that Buckeye's focus appears to have changed as of June 2015, when the group began compromising political entities in Hong Kong via sending malicious emails to targets and attempting to spread within compromised networks in order to steal information.

Leveraging our global threat intelligence, Symantec has built a clear and concise picture of how Buckeye has evolved its tactics in recent years. And powered by Dynamic Adversary Intelligence, Symantec was able to provide indicators-of-compromise and reveal the attack origin, how threats get into a customer environment, what malware tools are used, and who the threat actors are. It also reveals that Buckeye has shifted their attack tactics.

In the past, Buckeye tended to exploit zero-day vulnerabilities. All zero-day exploits known, or suspected, to have been used by this group are for vulnerabilities in Internet Explorer and Flash. Yet more recently, Buckeye used spear-phishing emails with a malicious .zip attachment. The .zip archive attached to the email contains a Windows shortcut (.lnk) file with the Microsoft Internet Explorer logo. Clicking on the shortcut ultimately leads to a Trojan malware. In the Symantec Advanced Threat Protection console, customers can find those granular details of adversary once a targeted attack incident is detected.

Use Case 2: DAI Enables Faster Detection and Remediation

Dynamic Adversary Intelligence (DAI) enables automatic search for indicators-of-compromise, shortening the time for the incident responder to identify and respond to potential targeted attacks.

Example:

A malicious incident was created in Symantec Advanced Threat Protection (ATP) as Dynamic Adversary Intelligence was able to quickly detect a targeted attack from adversary Billbug. DAI alerted the ATP customer to this threat so that they could take action in their ATP console.

With DAI, the customer got a unique visual of every related attack artifact, including the threat actors behind the attack. The customer could then take immediate action to blacklist malicious files and domains, and delete malicious files across all endpoints. They could also isolate infected endpoints from communicating to the rest of the organization and the internet, all through a single console.