CASE STUDY : RED CANARY, INC.

DomainTools

Crimeware Investigation: Connecting the Dots with Farsight NOD

red canary

INDUSTRY:

Managed Detection and Response

HEADQUARTERS:

Denver, CO

OBJECTIVE:

Investigate Newly Observed Domains

DOMAINTOOLS SOLUTION:

Farsight Newly Observed Domains™, the world's largest, most robust historical Passive DNS database available in the threat intelligence market today.

NOD KEY BENEFITS:

Farsight's Newly Observed Domain (NOD) product allows our platform near real-time access to data that supports not only our detection capabilities but also our investigative process. The combination of the two has provided extraordinary value over time, despite the evolution of malware as well as actor tactics."

Keith McCammon
Co-Founder and CSO, Red Canary

COMPANY:

Red Canary Managed Detection and Response combines industry-defining technology, process, and expertise to accurately detect threats that bypass other security tools. The solution empowers organizations to stop attacks before they result in breaches.

"About 75% of NOD-derived detections are high severity threats. It is a very specific piece of intelligence that helps us find the worst types of threats."

The Red Canary Approach

Red Canary was built to bring threat detection and response to businesses whether they have 50 or 50,000 employees. Red Canary continuously analyzes every piece of activity from every endpoint across an organization, hunting for patterns of system and user activity that are commonly associated with cyber threats and attacks. Anything that looks potentially threatening is investigated by a Red Canary expert analyst who uses the full historical recording of what happened on the system and an arsenal of investigative tools. If the Red Canary analyst's investigation confirms the activity is a threat, the customer is immediately notified with the information they need to understand the threat and the tooling to stop the attack before it results in a breach.

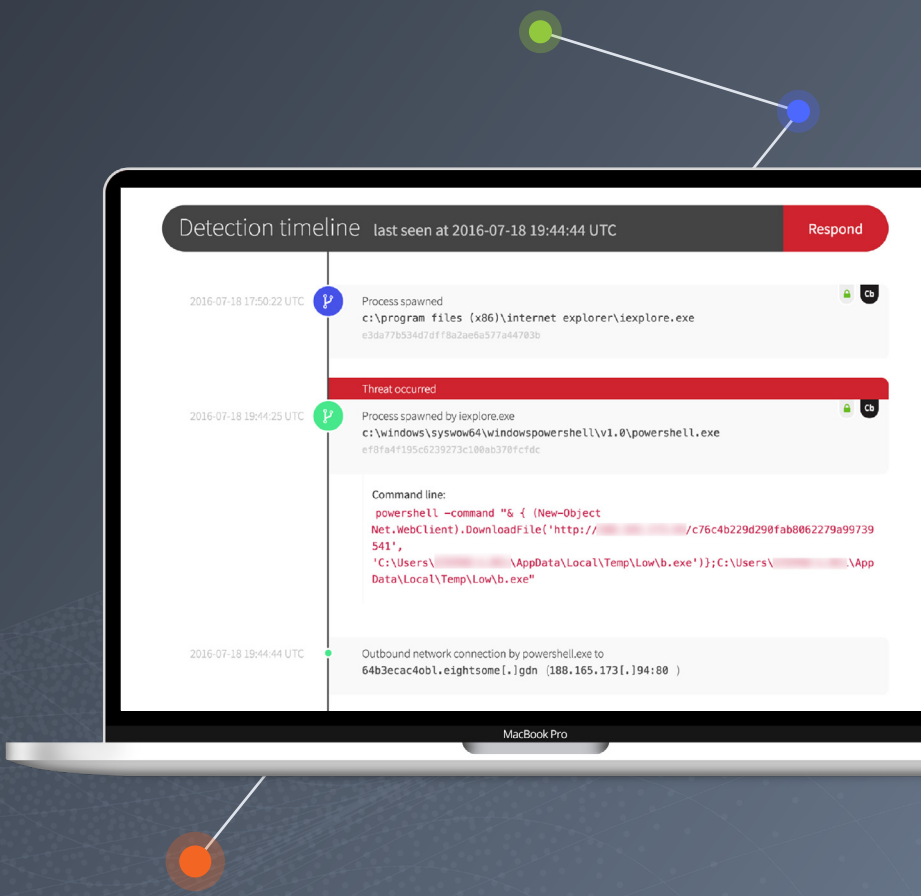
Farsight NOD Selection Process

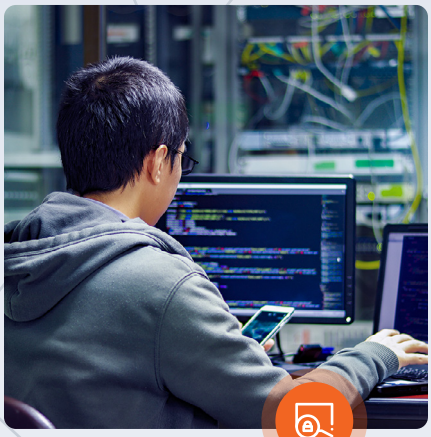
Red Canary collects telemetry data from endpoints including all domain requests. Through market research and evaluation of open source and other commercial threat feed providers, Red Canary determined that Farsight is the industry's leading Passive DNS database with a variety of focused solutions including Newly Observed Domains (NOD). The real-time intelligence enables Red Canary to quickly and accurately determine when an endpoint is connecting to a newly registered domain.

Red Canary uses **Farsight Newly Observed Domain (NOD)** to enrich and confirm their findings during an investigation, providing primary and secondary indication of a potential threat based on endpoint behavior.

How We Use Farsight NOD

For all Red Canary customers, network connections are correlated and alerted on the Farsight NOD solution. NOD is treated as a primary and secondary indicator with high fidelity. Regardless of the process making the network connection, be it a web browser or an algorithmically generated file name, a connection to a new domain is something interesting from the standpoint of understanding the process and user behaviors.





Farsight NOD as a Primary Indicator

When a newly observed domain is accessed, an alert is triggered and investigated by a Red Canary analyst. Depending on the process making the connection, this activity helps to drive the analyst deeper into the behaviors leading up to and after the connection. For example, a new binary or archived file is downloaded from a browser; either just released to the wild or perhaps a polymorphic binary from an exploit kit. But this file has not executed yet and no other behaviors have been raised to indicate a potential compromise. The event raise for the new domain connection can help direct an analyst to that file creation and identify the suspect binary prior to execution and further compromise. Now that the new domain has been identified as malicious, further actions can be taken to surface the bad domain and IP across the entire customer base.

NOD as a Secondary Indicator

Not every newly observed domain is considered bad. Therefore, Red Canary also ties NOD with other detectors. For example, malicious binary execution and a Newly Observed Domain event. While the execution of malicious binary is sufficient for the analyst escalating to the customer, the presence of NOD connection either by the malware directly or a related process provide further details of activities leading to the compromise.

About DomainTools

DomainTools is the global leader for Internet intelligence and the first place security practitioners go when they need to know. The world's most advanced security teams use our solutions to identify external risks, investigate threats, and proactively protect their organizations in a constantly evolving threat landscape.

Farsight NOD

DomainTools