KING & UNION CASE STUDY

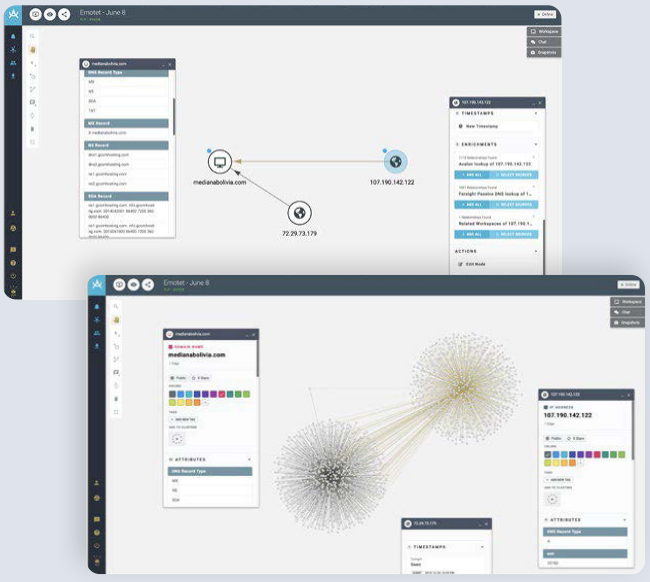
Avalon and DNSDB® Expose Emotet Malware

The Challenge

First encountered in 2014, Emotet is a modular banking Trojan that primarily functions as a dropper for other types of malware. Over the years, the authors of the malware have learned to improve its ability to avoid detection through methods like constantly changing C2 and downloader URLs. In 2018, the United States Computer Emergency Readiness Team (US-CERT) issued an alert highlighting the serious threat posed by the malware. Today, Emotet still ranks among the most costly and destructive malware affecting consumers and organizations. While many researchers remain vigilant, tirelessly tracking and reporting active versions of the malware, their work remains siloed or limited only to those within their network.

The Solution

Using Avalon, their cyber analysis delivery platform, King & Union was able to pull multiple reports into a single environment for real-time visualization and collaboration. Within the platform, Avalon first looked for any related workspaces to see if anyone had worked on the same indicators before. Avalon then automatically performed lookups three rounds out from the original data, providing collaborators with information such as related domain names and email addresses. They then further enriched the data maps with reverse DNS lookups using Farsight's DNSDB to identify possible connections. Within seconds, the Farsight DNSDB revealed two IP addresses were connected by a common C-panel default certificate.



The Results

King & Union's Avalon platform enabled collaborators to work together with data enriched by Farsight DNSDB to quickly visualize, identify and connect domains hosted at different IP addresses. With this information and a better understanding of how the data points were connected, the security team could then work together using Avalon to further uncover the trail of a cybercriminal group.

Why DomainTools

"DNSDB is a hugely powerful tool in identifying relationships between infrastructure on the Internet."

DNSDB®

Farsight DNSDB is a real-time DNS historical database that provides a unique, fact-based, multifaceted view of certain key configurations of the global Internet infrastructure. Farsight collects Passive DNS data from its global sensor array and then filters and verifies the DNS transactions before inserting them into the Farsight DNSDB™ along with ICANN sponsored zone file access download data. The result is the highest-quality and most comprehensive Passive DNS data service of its kind. DNSDB is engineered and operated by leading Farsight DNS experts

About King and Union

King and Union enables security teams to easily create and deliver the right intelligence to the right person across all levels of their organization by unifying data from multiple tools and results from investigations into a single cyber analysis delivery platform. With our platform, Avalon, security teams can quickly visualize threat data and investigate together in real time, and once complete, efficiently create and deliver the finished intelligence required to key stakeholders. Avalon reduces the time on manual, administrative tasks, leaving analysts more time to focus on security, and empowers organizations to take full advantage of the security investments they've made — in people, information and technology.

DomainTools

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.

View our Farsight DNSDB page