DomainTools

Deloitte.

Deloitte & Touche LLP
Case Study

Cerber Ransomware Investigation using Farsight's DNSDB

The Customer

Deloitte Touche Tohmatsu Limited (commonly referred to as Deloitte & Touche) is a UKincorporated multinational professional services network. Deloitte is one of the "Big Four" accounting organizations and the largest professional services network in the world by revenue and number of professionals. Deloitte provides audit, tax, consulting, enterprise risk and financial advisory services and employs more than 263,900 professionals globally.

The Challenge

In 2016, the Deloitte Vigilant Services team, headed by CTO Scott Keoseyan, identified a connection between a number of domains registered in their [.]top and .bid top-level domains. The team suspected that these domains were not legitimate web hosts. Instead, they appeared to be a potential criminal infrastructure hosting Cerber ransomware, a file-encrypting malware. They also suspected that the infrastructure was rapidly spreading via spam emails and moving laterally across infrastructure.

The Solution

Using the Farsight DNSDB integrated with the ThreatConnect platform, the Vigilant Services team quickly contained the Cerber threat by quickly distinguishing between a web-hosting IP address and a potential criminal infrastructure.

The Research

1. Inbound spam led the team to a downloadable binary that they submitted to a sandbox for analysis.
2. A recovered sample of DNS queries and a URL request for a domain, revealed that domain kingzoneg[.]top was supporting Cerber ransomware. The team also learned that domain kingzoneg[.]top was resolving to IP address 47.91.76[.]69.
3. Using DNSDB, the team examined IP address 47.91.76[.]69 and discovered that it was hosting other domains like kingzoneg[.]top.
4. Pivoting further in DNSDB, the team learned that IP address 31.41.44[.]59 was also hosting kingzoneg[.]top.
5. Comparing domains hosted on both IP addresses, the team discovered that kingzoneg[.]top was not the only domain hosted. On April 30, 2017, kingzoneg[.]top and five other domains shifted from 47.91.76[.]69 to 31.41.44[.]59.
6. Further research using DNSDB, the team discovered that the six domains shared the same DNS infrastructure.

The Results

Containing Cerber and Preventing Future Attacks

The Deloitte Vigilant Services Team took the following containment steps:

- Using historical DNS record analysis, the team examined DNS records for 31.41.44[.]59 for the week of 4/30/2017 and blocked access to the six domains hosted there. By blocking the infrastructure, they stopped these domains from being used for ransomware campaigns.
- The team sent alerts to the security community on their research around the IP addresses and their findings.
- They then evaluated newly discovered domains hosted on 47.91.76[.]69 for additional threats, and located another domain to investigate and eventually block.

About DNSDB

Farsight Security's DNSDB is a Passive DNS historical database that provides a unique, fact-based, multifaceted view of the configuration of the global Internet infrastructure. DNSDB leverages the richness of Farsight's Security Information Exchange (SIE) data-sharing platform and is engineered and operated by leading DNS experts. Farsight collects Passive DNS data from its global sensor array. It then filters and verifies the DNS transactions before inserting them into the 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. ThreatConnect enhances their own threat intelligence data by leveraging the DNSDB dataset to confirm – or reaffirm — information found in their other threat feed sources.

> Passive DNS allows us to rapidly distinguish between a web hosting IP and a dedicated, subverted infrastructure. Using passive DNS at first, to pivot off and identify infrastructure being leveraged, we were able to identify both infection and payment domains that had been, were being, and going to be used in these [ransomware] campaigns.
>
> **SCOTT KEOSEYAN**
>
> Chief Technology Officer supporting Deloitte & Touche LLP's Vigilant Services

ThreatConnect.

ThreatConnect, Inc. is a leading provider of advanced threat intelligence products and services including ThreatConnect®, a comprehensive threat intelligence platform. Government agencies and Fortune 500 organizations worldwide leverage the power of ThreatConnect every day. ThreatConnect collects and aggregates intelligence from multiple sources including open-source indicator and reputation feeds, as well as vendor-provided threat intelligence data including Farsight Security's DNSDB.

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 DNSDB

DomainTools