DomainTools

FARSIGHT SECURITY
A DOMAINTOOLS COMPANY

CASE STUDY : FARSIGHT CUSTOMER SUCCESS STORY

How ThreatConnect® Leverages DNSDB to Track Down the Grizzly (Steppe)

About Grizzly Steppe

In December of 2016, the FBI and the Department of Homeland Security issued a Joint Analysis Report (JAR) about Russian cyber-attacks titled, "GRIZZLY STEPPE –Russian Malicious Cyber Activity." The report provides technical details about the tools and infrastructure used by the Russian civilian and military intelligence services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election including a range of U.S. Government, political, and private sector entities. The U.S. Government collectively refers to this malicious cyber activity by RIS as"GRIZZLY STEPPE".

The JAR is intended to be a master list of technical indicators and recommended mitigations associated with the Russian hacks. The actors accused of these hacking incidents are known as Fancy Bear and Cozy Bear, or APT28 and APT29. They have been tracked for years by cybersecurity specialists who have long accepted the detailed, public pattern of evidence linking them to Russian intelligence; including technical indicators-of-compromise (IOCs).

ThreatConnect

The Partner

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 leverage the power of ThreatConnect® every day. ThreatConnect® collects and aggregates intelligence from multiple sources including open-source indicator and reputationfeeds, as well as vendor-provided threat intelligence data including the Farsight DNSDB.

The Challenge

The JAR has been controversial within the broader security community and the utility of certain types of data in the report has also been questioned. For example, the IP addresses provided were inconsistent and difficult to utilize for a variety of reasons: (Lee, 2016)

1. First, the provenance of the indicators was not publicly disclosed.
2. Second, over 30% of the IP addresses are mostly useless because they are VPS, TOR exit nodes or proxies and the content from those exit nodes could have come from anywhere and could commingle traffic from multiple sources. (This type of information can be used, but not in the way positioned in the report, and not adequately without additional information such as timestamps.)
3. Third, IP addresses as indicators (especially when associated with malware or adversary campaigns) must contain information around timing, i.e. when were these IP addresses associated with the malware or campaign and when were they in active use? IP addresses can be used by different parties over time, therefore it is critical that nonstatic addresses include accurate timestamps with time zone information.

Due to these shortcomings, ThreatConnect® launched an investigation to validate, contextualize, and enrich the JAR's findings—turning a jumbled list of indicators into actionable intelligence.

The Solution

ThreatConnect used Farsight DNSDB to identify other domains sharing the same infrastructure.

ThreatConnect used the Farsight DNSDB and WHOIS to map registration and hosting consistencies to already known malicious tactics.

Leveraging Farsight DNSDB on their platform allowed ThreatConnect® to extend GRIZZLY STEPPE data. First, researchers utilized the ThreatConnect® platform to find existing information about the IOCs and with whom/what they are associated.

After narrowing down 870 IP addresses, researchers focused on the first 80 addresses listed in the JAR. These addresses were already in the ThreatConnect® platform with possible associations to the Fancy Bear cyberespionage group.

The Results

DNSDB allowed ThreatConnect® to identify realtime and historical contextual data for all of the domains hosted at the identified IP addresses.

Of the 80 addresses examined, 43 were linked to Fancy Bear.

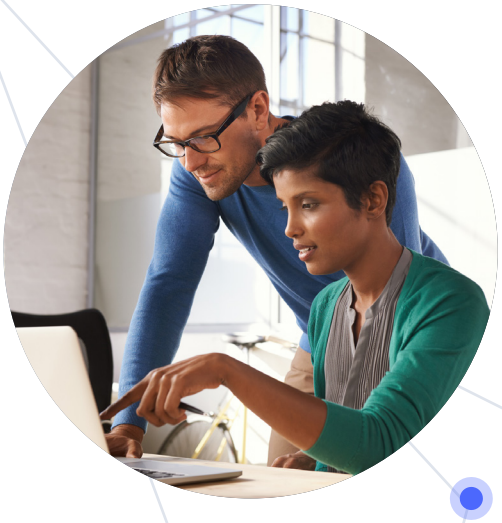
Further analysis of the 80 addresses led to the discovery of 122 additional indicators, 100 of which had not previously been associated with Fancy Bear inThreatConnect®, including 68 domains, 17 IP addresses, and 15 email registrants.

The indicators identified by the team yielded information that can be used to further expose the underlying infrastructure of the cyberespionage group thus benefiting the collective U.S. and international security community.

> With Farsight DNSDB, investigators can easily gain a complete picture of adversary infrastructure and operations, correlate other network and threat data, and save time when it is most critical—during an attack or investigation. For existing threat platforms or SIEMs, Farsight DNSDB allows for increased utility of current investments.

About DNSDB

Farsight 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 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. Farsight DNSDB is engineered and operated by leading Farsight DNS experts.



References

(Lee, 2016)"Critiques of the DHS/FBI's GRIZZLY STEPPE Report." Robert M. Lee, Robert M. Lee, 30 Dec. 2016

http://www.robertmlee.org/critiques-of-the-dhsfbis-grizzly-steppe-report/

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

DomainTools