The TRIES Framework: Counter-Reconnaissance against EaaS Threat Actors

TAIA GLOBAL, INC. | https://taia.global | January 2015 |

[This Page Left Intentionally Blank]

Executive Summary

Intellectual property theft in the United States is estimated to cost US companies $300 billion per year[1]. For most of this century, it has been believed that nation states are behind this type of cyber espionage, however, there is an under-reported threat actor (hacker groups for hire) who is willing to attack a company's network and cause damage or steal its crown jewels in exchange for very high fees paid by wealthy businessmen or corporate competitors. This has become known in the security world as Espionage-as-a-Service or "EaaS".

These mercenary hacker groups range from small groups with little funding to specialty shops run by ex-government spooks to highly financed criminal groups who use similar if not identical tactics to nation state actors. That they are rarely discovered is due in part to their skill level and in part to being mis-identified as a state actor instead of a non-state actor if they are discovered. The low risk of discovery, frequent misattribution to a nation state, and growing demand of their services ensures that the EaaS threat actor will flourish in the coming 12 to 24 months.

This white paper provides an in-depth, non-technical review of some known EaaS operations against aerospace and defense targets as well as a strategy that can be easily and affordably implemented to augment a company's defenses against the EaaS threat actor.

Figure 1: The TRIES Framework of the EaaS Threat Actor

[1] The IP Commission Report http://www.ipcommission.org/

General Discussion

The aerospace and defense industry is a lucrative target for mercenary hackers because market competition is fierce and the export regulations which control defense articles (ITAR[2]) as well as dual-use products like lasers (EAR[3]) from leaving the US allow hackers to charge more for their services. Other high value technologies beyond aerospace and defense are being targeted by these actors as well.

This white paper is for policy makers, corporate executives, board members, insurance brokers, and investment bankers who desire a better understanding of the overall threat landscape in order to evaluate operational and investment risks as well as learn how to better defend against these attackers.

The EaaS Threat Actors

Su Bin and UC1-2

Su Bin is a Chinese businessman with residency in Canada. The FBI named him in a criminal complaint and he was later indicted by a Grand Jury on five felony charges including conspiracy to steal trade secrets and to illegally export defense articles related to the C-17, F-22, and F-35 aircraft.

Bin is currently in custody in British Columbia while the Canadian government seeks to strip him of his permanent residency status. He worked with two unindicted co-conspirators (UC1-2) located in China. The criminal complaint[4] and the grand jury indictment[5] represent the most detailed look at Espionage-as-a-Service that has ever been made available.

This operation had been running since 2010 or earlier and while Su Bin has been arrested, UC1-2 as well as their colleagues are presumed to still be active.

---

[2] ITAR: InternationalTraffic in Arms Regulations (22 C.F.R. 120-130), under the Arms Export Control Act (Pub. L. 90–629, Oct. 22, 1968, 82 Stat. 1321; 22 U.S.C. 2751).

[3] EAR: Export Administration Regulations (export control on commercial items with potential military application).

[4] Su Bin Criminal Complaint: http://online.wsj.com/public/resources/documents/chinahackcomplaint0711.pdf

[5] Case 8:14-cr-00131-UA https://www.documentcloud.org/documents/1276138-su-bin-indictment.html

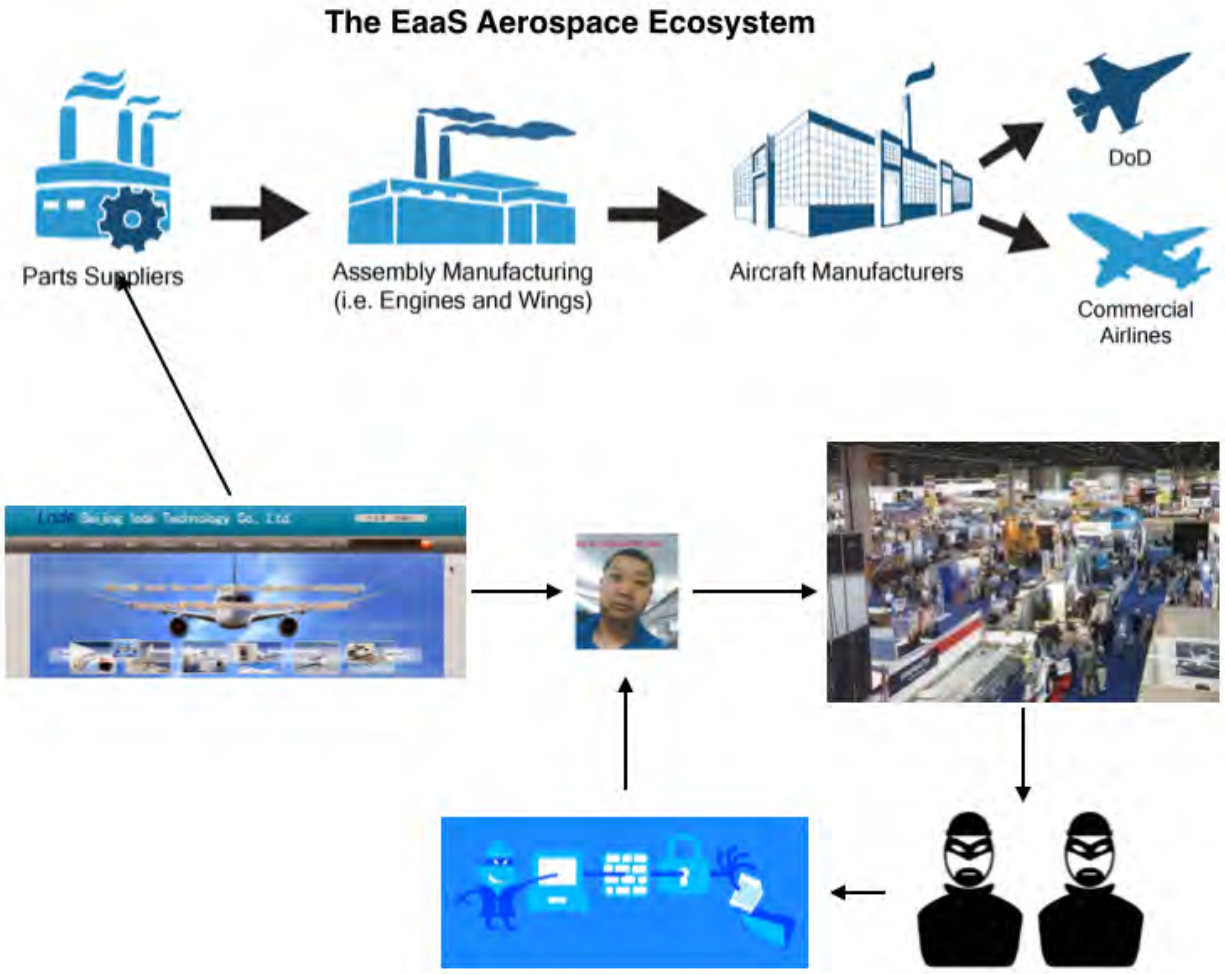

Figure 2: The EaaS Aerospace Ecosystem

The FBI criminal complaint only identified Su Bin, who acted as the subject matter expert (SME) as well as the broker. Bin's company - Beijing Lode Technology Company Ltd. - had been in business since 2003 serving the aviation and space market with cable harness equipment. Lode Tech also had numerous distribution agreements and vendor relationships with other US and foreign companies. He even shared a booth with Boeing (one of his targeted companies) at the Beijing Aviation Expo.

These relationships allowed him to do exactly what his company logo proclaimed "track the world's aviation technology," which in turn made him an excellent SME/broker/ dealer for UC1-2's cyber espionage campaigns.

Figure 3: UC1-2 Funding, Infrastructure, and Targets

Once a company and its specific technology was targeted by Su Bin, the actual network breach was conducted by at least two unnamed co-conspirators (UC1, UC2). They spent several million Yuan for one operation which paid for the establishing of licensed "machine rooms" in Macao and Hong Kong and hop points in the US, South Korea, and Singapore. They claimed to have compromised and maintained control over the networks of US and Taiwanese aerospace companies who are part of the world's top 50 defense contractors.

UC1 and UC2 never communicated electronically between their Mainland China (PRC) offices and their Macao and Hong Kong offices. Information was hand-carried between the two countries so as to avoid detection.

After UC1-2 completed their attack, they notified Bin who would look for buyers if one hadn't already been acquired. These buyers weren't necessarily Chinese companies. One

email from Bin to UC1 indicated that he was unhappy with how cheap one Chinese company's offer was and that he would look for other buyers.

The most recent email exchange dated May 21, 2014 was between UC1 and a third co-conspirator wherein UC1 attached a report which described a partially successful phase 1. According to the report, the company had been successfully targeted and infiltrated, the data had been discovered, downloaded, transmitted via several hop servers until arriving at Macao where it was hand-delivered into China. However, the report also discussed some security measures which "prevented acquisition of the information they sought". The indictment didn't provide any details on what that was but it may have been encryption. Finally the report discussed improvements being made by UC1 so as to overcome whatever roadblock was thrown at them by the target company.

The UC1-2 mercenary group is highly organized, well-funded and actively engaged in successfully attacking some of the best protected networks in the world. Aerospace and defense companies would be well-advised to continue to harden their networks and identify their products and technologies that may be of interest to UC1-2's potential clients.

Pitty Tiger

In 2014, the Airbus Defense and Space CyberSecurity unit published a report called "Eye of the Tiger"[6] about a group of APT[7]-style actors that they named Pitty Tiger. According to the report's authors, the group has been active since 2011 and targets several sectors including Defense and Telecommunications. What makes them unique is that the Airbus team suspects them of being a for-hire hacker group - small, stealthy, with a limited budget and resources who favor a small number of high value targets. Readers who want the technical details of Pitty Tiger's malware family and attack indicators are

[6] http://blog.cassidiancybersecurity.com/post/2014/07/The-Eye-of-the-Tiger2

[7] "APT" stands for Advanced Persistent Threat.

encouraged to download the Airbus team's report. Those details won't be covered in this white paper.

One of Pitty Tiger's victims was a European defense company. The IP addresses used to host the Command and Control domains were mainly located in Taiwan and Hong Kong. The Remote Desktop Connections (RDP) used to control the Command and Control (C2) servers came primarily from Fuqing in the Fujian province of China on the east coast near Taiwan, while other RDP connections came from the United States and Hong Kong.

The Airbus researchers found a reference file containing five Word documents and a small code sample on the attackers' server, which they probably used to show potential clients what could be obtained from their defense company target. It was a "living" document meaning that it contained comments from various users and not just an old archive.

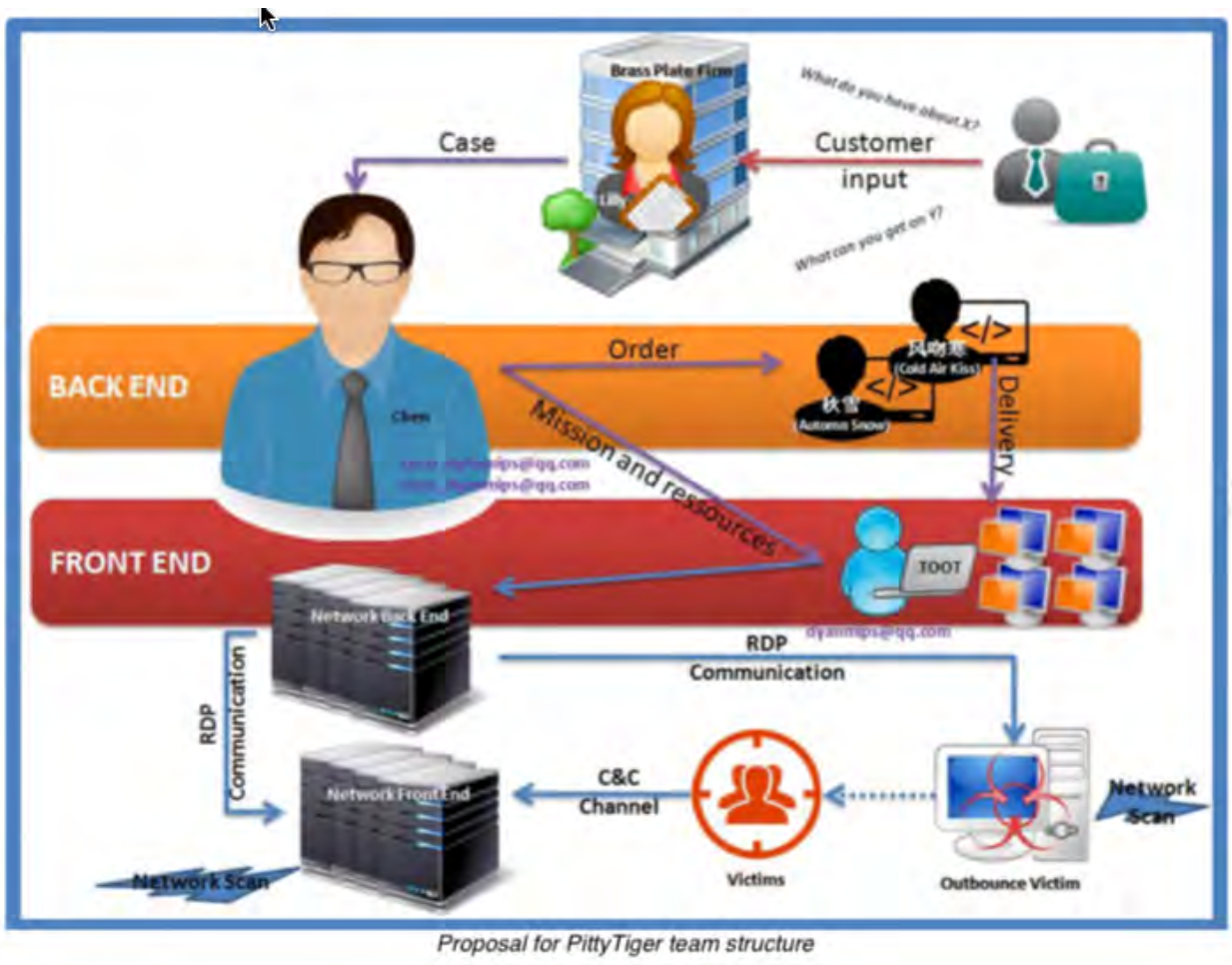

Figure 4: Pitty Tiger team structure

The Airbus researchers created the above graphic as a proposed organizational structure for the Pitty Tiger group with the following description[8]:

"We have strong evidence of a bot operator position [nicknamed TOOT]. We also identified a malware development position. We identified two nicknames for this position on the current campaign, Autumn Snow and Cold Air Kiss. Yet we are unsure that they belong to the group. They might just be a third party providing or selling their malware."

"We have a strong suspicion of a coordinator position, which coordinates the bot operator, provides him with some logistics support (weaponized document, tools …) and reviews the programmers work. We named this position "Chen" in relation with several references of this common Chinese name in the C2 WHOIS and other investigative materials."

"We have some suspicion of a customer relationship manager position that may act as an interface between a customer and Chen. We named this position "Lilly"."

The Airbus team reported that this group has been operating since 2011, possibly 2010, and that it was still active as of July 2014. Unlike UC1-2, this group didn't care about creating an electronic footprint inside Mainland China. "Toot" used both "Chinese Traditional" and "Chinese Simplified" language settings at different times so it's hard to say if he's from Mainland China (where Chinese Simplified is more often used) or from Taiwan, Hong Kong or Macau (where Chinese Traditional is more often used). The Command and Control IP addresses were mostly in Taiwan and Hong Kong.

[8] Ibid., pp. 48-9

The TRIES Framework

Stage 1: TARGET

EaaS threat actors start by targeting. In some cases, the broker may already have a buyer for the information. In other cases, the hackers may already have the data but need the broker to find a buyer. If your company is in the Aerospace and Defense industry, and your products fall under ITAR or EAR export control regulations, then you're most likely a target for a government or a corporate rival who needs what you've developed or are developing.

Stage 2: RECONNOITER

The EaaS actor employs diverse reconnaissance techniques to identify vectors. The Broker is either looking for a specific technology or product that his customer wants to acquire and will pay a premium for, or a hot technology like Wide Area Persistent Surveillance or directed energy weapons that he knows he can find a buyer for.

Stage 3: INFILTRATE

There are many ways to infiltrate a high value network, even if it is very well defended; from a spear phishing attack against a soft target like Human Resources (i.e., Sony and RSA) to compromising a vendor and attacking the target with trusted credentials to, if need be, becoming an employee and gaining access as an insider with malicious intent.

Stage 4: EXFILTRATE

Once the data has been acquired, it's critical to exfiltrate it from the network without being detected. Professional hackers want continued access to their victims over many years and so will patiently take their time to find and test the best methods for exploitation.

Stage 5: SELL

Customers of stolen technologies generally seek to manage their own R&D costs through this type of "technology transfer". As long as the acquisition cost is less than their development cost and as long as the price is right, a deal can usually be struck. Other stolen data is sometimes used as a bargaining chip by the seller to foster buyer confidence.

The unique aspect of the TRIES framework when compared to the Cyber Kill Chain[9] or Indicators of Attack[10] is the process of reconnaissance or "Reconnoitering".

In an EaaS operation, a specific knowledge of the targeted product or technology is a requirement, which is why brokers are also SMEs. However, this offensive tactic can also be used defensively against the threat actor and/or the threat actor's client as a form of Counter-EaaS™[11].

Figure 5: TRIES Framework

[9] Cyber Kill Chain™ is a registered trademark of Lockheed Martin http://www.lockheedmartin.com/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html

[10] Indicators of Attack has been compiled in an easy-to-understand format by CrowdStrike http://blog.crowdstrike.com/indicators-attack-vs-indicators-compromise/

[11] TM Pending

Counter Reconnaissance As A Defense Against EaaS Threat Actors

If your company develops novel technologies or products that are highly competitive or regulated, chances are excellent that you're on an EaaS team's radar (assuming that you haven't already been breached). However, the EaaS team is just the middleman in this operation. You want to know who they might be selling your data to. Before 2015, that information was extremely difficult to obtain. Today, it's not only obtainable but it can inform and integrate with your company's existing network security tools. Taia Global's REDACT is the only product of its kind available outside of a classified environment.

REDACT IP Intelligence

Security Information and Event Management products (SIEM) provide you with almost everything there is to know about who's visiting your company's website except for the most important thing — the name of the organization or agency that's actually doing the visiting. REDACT's IP Intelligence product, built using the Common Event Format (.CEF) standard works seamlessly with your existing SIEM product and will alert you when one of our several hundred Russian, Chinese, French, North and South Korean government-funded State Key Labs, research universities, government investment funds, or state-owned enterprises visits your website. Since researchers, not attackers, are doing the visiting, there's little to no use of proxy servers or other attempts to cloak their IP address. REDACT is dynamic and instantly scalable to meet requirements for both routine and trending alerts and analysis.

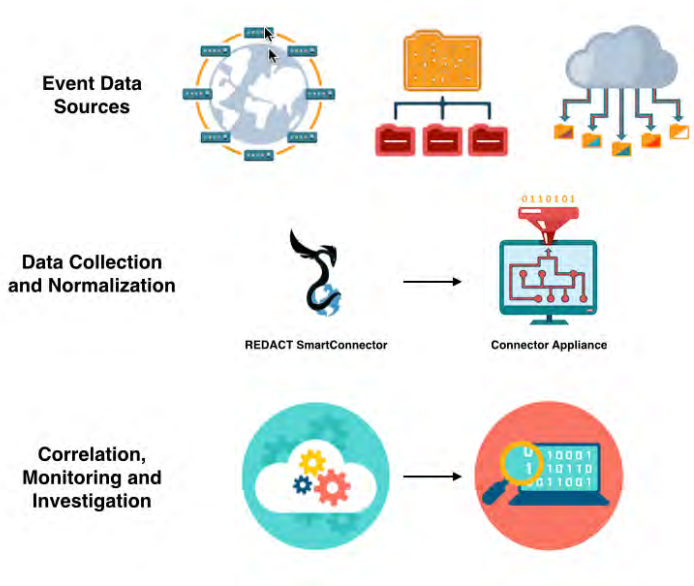

Figure 6: Proposed ArcSight integration using the REDACT SmartConnector (Spring 2015)

REDACT on Tableau

Once REDACT's IP intelligence feed identifies which research institute or entity is searching for information about your company's products or technology, the analyst can "right-click" on the alert and launch Tableau Online which is connected to our REDACT database. The analyst can then mine REDACT for additional information on the institute down to the subject classification or perform a variety of visualizations to better understand the value of your company's technology in comparison to nation state funding contracts.

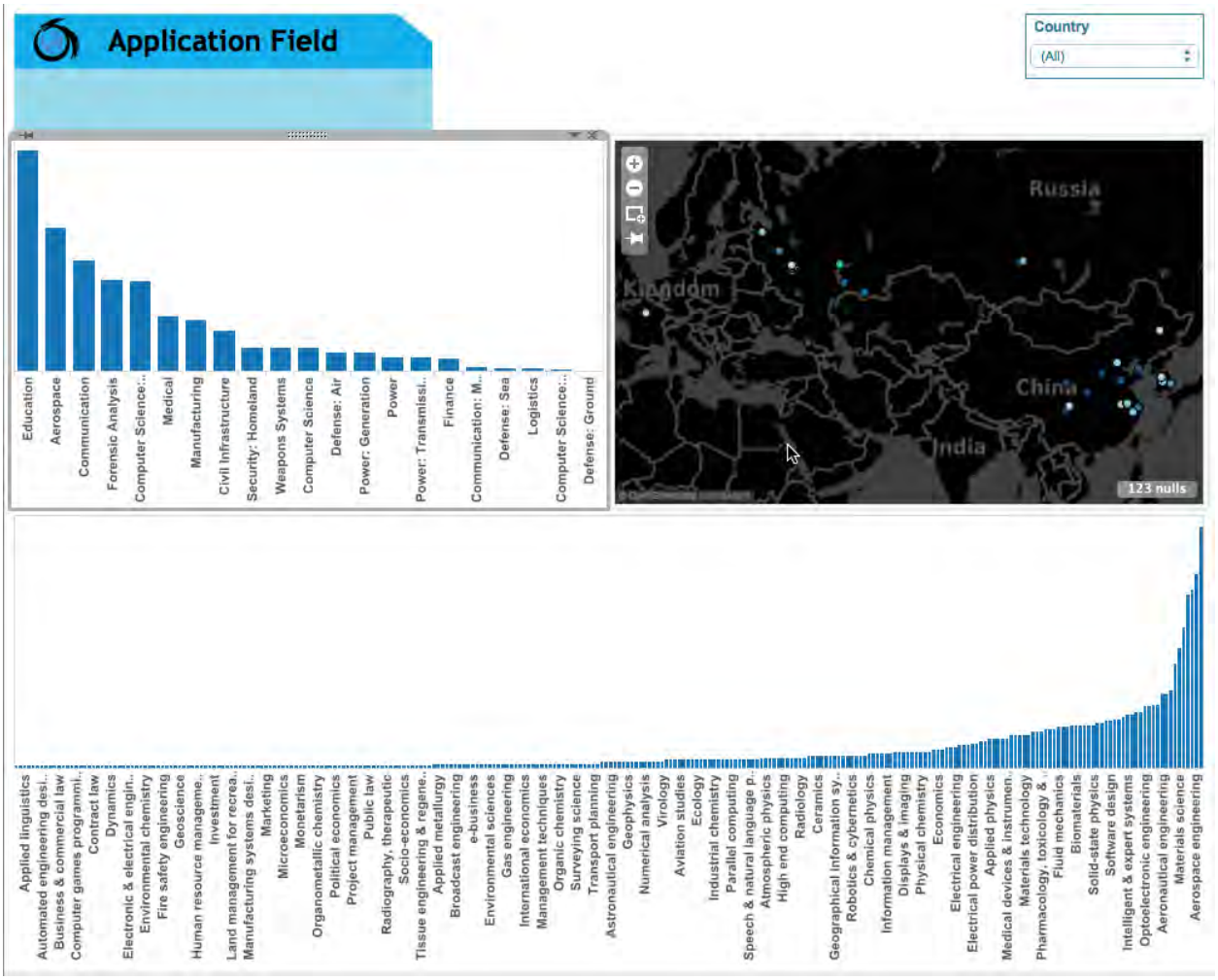

Figure 7: Tableau visualization of REDACT institutes' application sectors and subject areas

REDACT Search

Our secure online search portal hosted on AWS provides the analyst with a way to dig into individual projects (over 4,000 as of January 2015) as well as download custom reports on each research institute as available. REDACT beta clients can request up to six customized reports per year as part of their subscription if they don't already exist in our system.

In addition to obtaining information at the project level, the analyst can see how the research institute is connected to its government funding agency, which government agencies the institute provides its research to and who its government customers are.

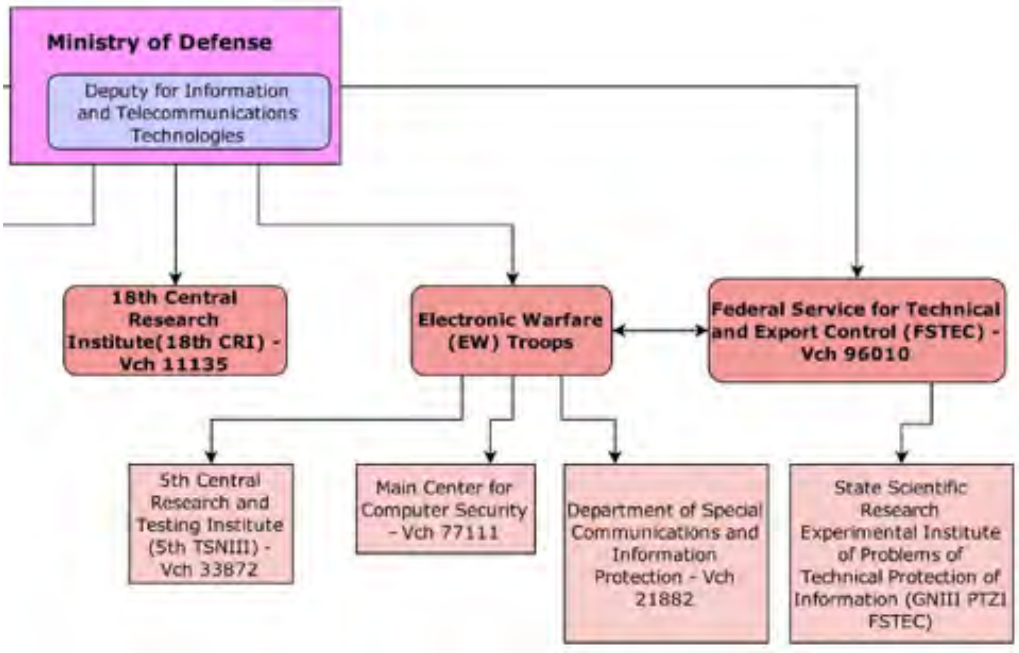

Figure 8: REDACT hierarchy of Russian government affiliations for research entities

Integration with SIEM and DLP Products

If your IT security department uses Security Intelligence and Event Management products which can read Common Event Format (.CEF) files, then our REDACT IP Intelligence FlexConnector will be able to provide real-time alerts when any of our Russian, Chinese, Korean or French institutes visit your websites. Those alerts are entirely customizable in your SIEM dashboard. If you're a HP ArcSight customer, then you'll be able to use our SmartConnector by Spring 2015.

Now that you know which government research entity is interested in your technology, you can use REDACT search to discover which specific projects they've been funded to

develop and match those keywords and phrases to your own products or R&D. Those matches can be used to write policies for your Data Loss Prevention software (DLP) because those are high-risk properties that your company should provide an extra layer of security for.

Identification of Insider Risk

The planting of an insider for espionage purposes has had considerable success over the years, long before cyber espionage was possible. It is still done today, especially for very high value targets with security hardened networks, and continue to operate undetected despite availability of leading and current indicators of nefarious activity. REDACT Search can be used by a company's Human Resources department as part of the vetting process for prospective employees who have graduated from one of the government funded research institutes in our database to complement existing personnel and physical security programs. For example, HR may want to extend the candidate's trial employment period so as to determine the depth of their affiliation.

An Approachable and Affordable Security Tool

REDACT is *approachable*; meaning that your company's CISO won't need to translate technical terms for your CEO and your Board of Directors. By connecting a state-funded research institute to an IP address that has been searching your website for ITAR controlled products, and then showing related projects in their research portfolio, you'll be connecting a lot of dots without having to translate any "geek-speak". In fact, one of the world's largest defense contractors is using REDACT for that very purpose today.

REDACT is *affordable* because our monthly subscriptions start at $1,250 per month and are cancelable at any time. There are discounts for annual subscriptions and Tableau® Reader is free.

CONTACT US FOR A FREE CONSULTATION BY CALLING (855) 777-8242 OR SENDING AN EMAIL TO SERVICES@TAIAGLOBAL.COM.