Knownsec Hong Kong

Threat Trend, Intelligence and Response

Anthony LAI
Director, Knownsec Hong Kong

About Knownsec

- We set up Knownsec Hong Kong since 2012. Knownsec HQ in Beijing is set up since 2007
- Invested by Tencent over 300 Million RMB
- We focus on promoting the products in Web security including
  - WebSOC - Web Monitoring and Vulnerability Discovery Solutions
  - Jiasule - Cloud-based Anti-DDoS Solutions, focus on Application Layer
  - ZoomEye - A platform to detect IoT security and vulnerabilities
  - Star Map - Threat Monitoring
  - Firewall (aka Knownsec Shield)
  - Brand Protection - Alert the users and label the sites/links in search engine for any fake web sites which is harmful to the brand of the client
  - Phishing and Fake Websites: Threat Intelligence Data and We carry it out with Tencent.
- We also provide consultancy and penetration test service to client

Knownsec.Asia

Who am I?

- Focus on security research and consulting in security for 13 years.
- Work on malware and target attack analysis
- Publish the talks at Blackhat USA and DEFCON, Syscan Taiwan, HITCON, Codegate, HITB GSEC and HTCIA Asia Pacific Conference
- Currently doing a part-time doctoral research over machine learning and threat clustering and attacker profiling
- SANS course mentor and certified with SANS GREM (Malware Reverse Engineer and Analyst) and GXPN (Advanced Exploit Researcher and Penetration Tester)
- Passionate over Capture The Flag (CTF) game and our group, VXRL & Friends, got Rank 8 in Facebook CTF in Singapore among 21 teams.

Agenda - Part 1 (15 minutes)

Supply Chain Security

Threat and Defense

Best Practices

Supply Chain Security - Threat Ecology

SUPPLY CHAIN SECURITY

A program that focuses on the potential risks associated with an organization's suppliers of goods and services, many of which may have extensive access to resources and assets within the enterprise environment or to an organization's customer environments, some of which may be sensitive in nature.

as an ingress point into their ultimate target.

There are many ways a supply chain breach could occur. For example, a software manufacturer could be breached via malware that modifies source code that is then distributed to enterprises that use the software. Another common compromise vector might be the theft of a vendor's credentials that grant remote access to an enterprise the vendor works with, leading to infiltration of the enterprise network from an already trusted source (the vendor network). Figure 1 illustrates a typical supply chain breach.

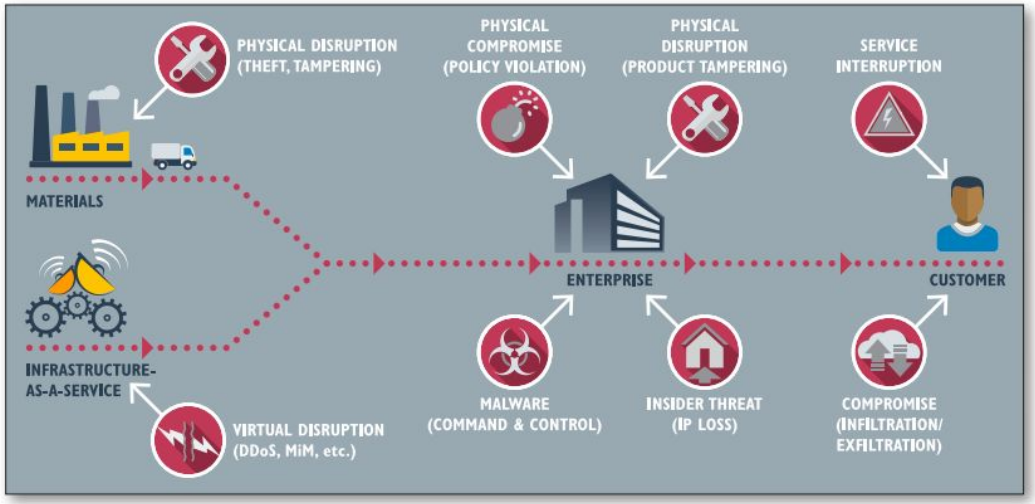


Figure 1. Anatomy of a Supply Chain Breach

Threat Ecology - More

DIGITAL GUARDIAN Solutions Products Services Resources About

DATAINSIDER Data Protection Security News

SUPPLY CHAIN CYBERSECURITY: EXPERTS ON HOW TO MITIGATE THIRD PARTY RISK

Nate Lord
Last Updated: Thursday July 27, 2017

23 information security experts provide tips for securing data across business partners, suppliers, and other third parties.

When companies think about security, they most often think of securing their networks, software, and digital assets against cyber attacks and data breaches. But the supply chain - whether a traditional manufacturer or service provider's supply chain or the "data supply chain" relied on by most large companies - is also vulnerable to security risks, as has been seen in a litany of major data breaches via third parties.

Practically every company has a place in the supply chain, and supply chains are evolving to be as much about the flow of information as they are about the flow of goods and services. Thus, it comes as no surprise that supply chain security is a highly complex, evolving function, and it's one that security pros and business executives are giving more attention as the risks facing information throughout the supply chain become increasingly obvious.

Supply chain security is every company's responsibility. The supply chain as a whole is only truly secure when all entities throughout the supply chain carry out effective, coordinated security measures to ensure the integrity of supply chain data, the safety of goods, and the security of the global economy. To find out what tactics and methods companies can utilize to enhance the security of their supply chains and contribute to global supply chain security, we asked a panel of security experts and supply chain professionals to answer this question:

Process

Vendor Management

Define Important Vendors

Specify Primary Contacts

Establish Guidelines and Controls

Integrate with the Organization’s Practices

Figure 2. Building a Vendor Management Program

The next several sections outline some of the best practices and changes organizations need to make internally to ensure that they are not exposing themselves to risks from vendors and partners that comprise their supply chains. Best practices typically involve the triad of security operations: people, process and technology, as illustrated in Figure 3.

Figure 3. The Triad of Security Operations[11]

Best Practice (1)

Organizations that are adapting their security review processes to better encompass the supply chain should follow these guidelines:

- **Decide on a list of controls with which supply chain organizations need to demonstrate compliance.** This list may vary for each organization, depending on the type of business performed, data and asset sensitivity involved, and other factors. Classifying organizations into categories based on these factors, and then defining specific lists of security requirements per category, is a manageable way to handle reviews.

- **Determine the frequency of security reviews for internal and regulatory compliance needs.** Reviews should be completed at least annually, but twice per year (or even more frequently in some types of organizations) is preferred.

Best Practice (1 - Continue)

Define a remediation and arbitration process for handling supply chain organizations that are not currently meeting security requirements.

This process should include specific timelines for remediation, as well as termination of the relationship if security requirements cannot be met.

Best Practice (2)

Some of the mechanisms to prevent privileged insider abuse highlighted by CERT include the following:

- **Enforce separation of duties and least privilege**.

  Separation of duties implies that no one employee can perform all privileged actions for a system or application. Least privilege implies that employees are granted only the bare minimum privileges needed to perform their jobs. By using these controls, an organization limits the damage a privileged user could inflict.

- **Implement strict password and account management policies and practices.**

  This should be enforced for all users, including administrators an other privileged users. This practice makes it harder for attackers to

Best Practice (2 - Continue)

Log, monitor and audit employee online actions.

Organizations need to be vigilant about what actions privileged users are taking, and should use a variety of logging and monitoring techniques to detect malicious or suspicious actions quickly and initiate response actions if needed.

- **Use extra caution with system administrators and privileged users.**

  Because these users are often granted the “keys to the kingdom” in terms of access and capabilities, additional safeguards often need to be implemented to adequately monitor and manage their behavior.

Best Practice (3)

Network Isolation and Segmentation

Network isolation and segmentation changes can help with improving supply chain security as well. Using both Layer 2 (VLAN) and Layer 3 (IP addresses and subnets) segmentation to isolate traffic into “zones” can be effective for keeping traffic related to supply chain organizations separate from other internal traffic and result in better malware detection and control (in the case that a breach does occur within or transiting the supply chain network). Most sophisticated malware and attacks rely on lateral movement in networks.

Best Practice (4)

Analytics and Threat Intelligence

Many organizations use or plan to use security analytics tools and threat intelligence to help identify and combat advanced attacks. Highly customized analytics platforms, while expensive and complex, can provide enormous value in the form of more predictive trends, granular patterns of internal and external-facing network and application behavior, and even user and group profiling for target analysis. In fact, monitoring specific users that are known to be high-value targets is a viable technique that could help to detect targeted attacks quickly, although privacy concerns are important to take into account.

Best Practice (5)

Exfiltration Monitoring

Monitoring egress points from the internal network is another way to improve security within the supply chain. Sometimes referred to as egress monitoring or exfiltration monitoring, intercepting user traffic bound for the Internet before it hits the perimeter allows security teams to see what data is being sent to the Internet over internal network channels. This is likely where security personnel will detect infected end-user systems transmitting bot command and control information. Some of the most common protocols and standards used for data exfiltration or command and control include **HTTP/HTTPS, FTP/FTPS/SFTP, SSH, IRC, email, P2P, and DNS or ICMP for covert channels.**

Best Practice Summary

Table 1 summarizes basic and more comprehensive supply chain security elements.

Table 1. Elements of Supply Chain Security Programs

	Basic	More Comprehensive
People	Background checks	Security requirements spelled out in in contracts
Process	Contract review Vendor security control and risk review	Implementation of a complete vendor management program
Technology	Network segmentation Privilege management and monitoring	Third-party code review and vulnerability management Exfiltration monitoring Security analytics and threat intelligence

Agenda Part 2 (20 minutes)

Case Study

Threat Intelligence Tricks

Intelligence Data Manipulation and Integration

Our Weapons . Monitor your devices and systems

Prepare your people

Recommendation

Case Study: Public Listed Firm (1)

Story

A ransomware hits a public listed firm three times, encrypt files and data, they have engaged Microsoft Forefront Anti-Virus at low cost.

The infection cause is that their staff opened malicious document at their Yahoo! Mail.

MS Forefront only detect it in 1-2 days later; Checkpoint IPS can’t detect and block and only capture the outbound IP address

Case Study: Public Listed Firm (2)

Solutions

Deploy customised Microsoft Security Policy

Consider threat intelligence platform and feeds so as to gain first hand attack indicators instead of waiting for AV vendor signature, it is

Lesson Learnt

Do you think it is enough with just firewall, IPS and anti-virus software?

Threat Intelligence Tricks

Threat Intelligence is defined as a collaborative platform with various attack and indicators shared by industry.

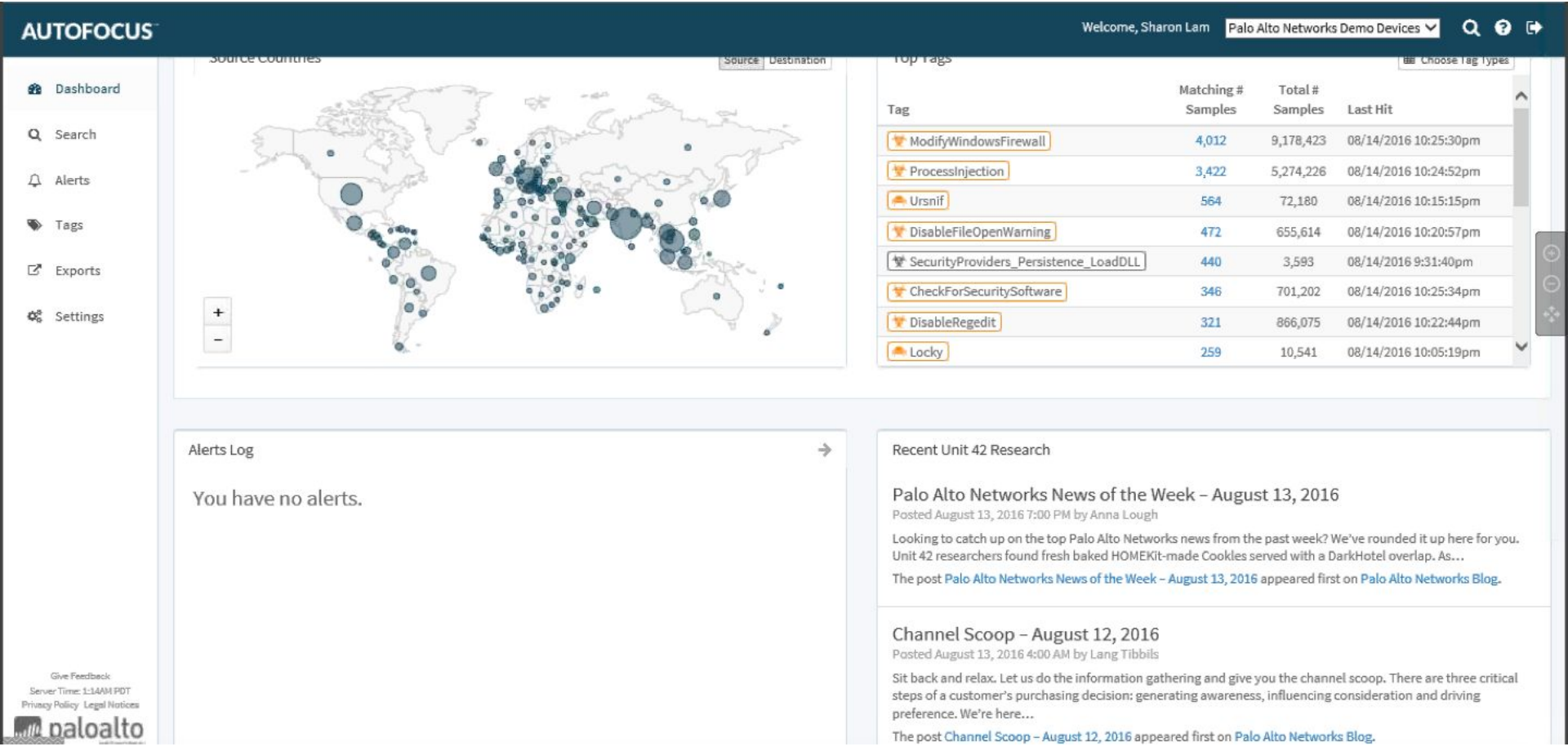
Understand most of the attack vectors in your network and in industry

- Target attack via email attachment
- Network attack
- Software vulnerability and exploitation
- Remote code execution in various systems

Understand and estimate the risk, impact and loss, get to know the overview at a glance

It is taken a preventive + detective control instead of just detective one

AutoFocus Platform - Dashboard



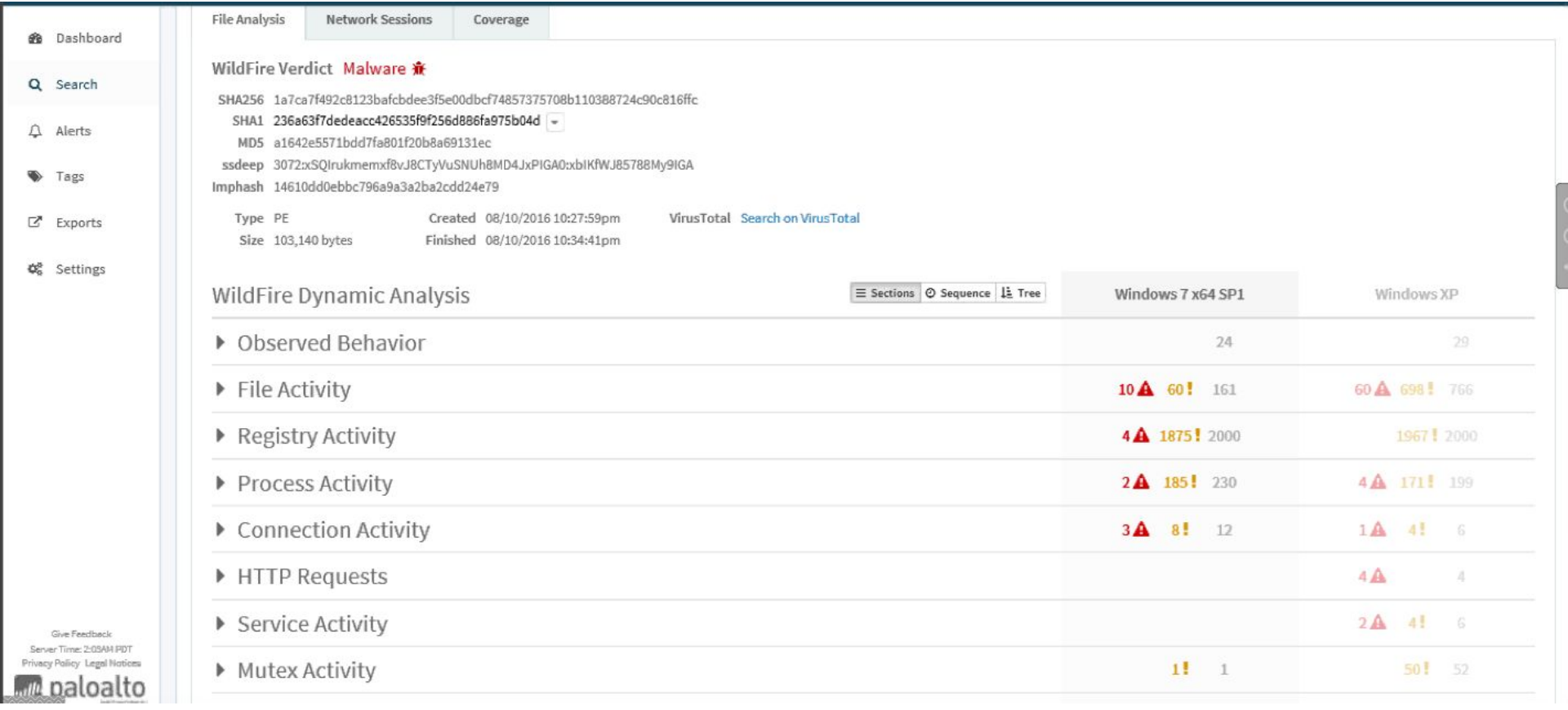
Threat Intelligence Tricks

Understand the features and analysis indicators of those attack vectors in your network and in industry, whether they are comprehensive:

- Malware: C2 server IP address, domain name, passive DNSs, encryption routine, registry, etc indicators.
- Network:
- Exploitation:

Get to know the research team and publication from the threat intelligence platform provider - Simply reading their blogs and publication, decide whether they are on the leading role, it is not just solely determined by the tool.

AutoFocus Platform (2) - Analysis Indicators



Intelligence Data Integration and Manipulation

Intelligence data could be easily integrated and posted to various control gates

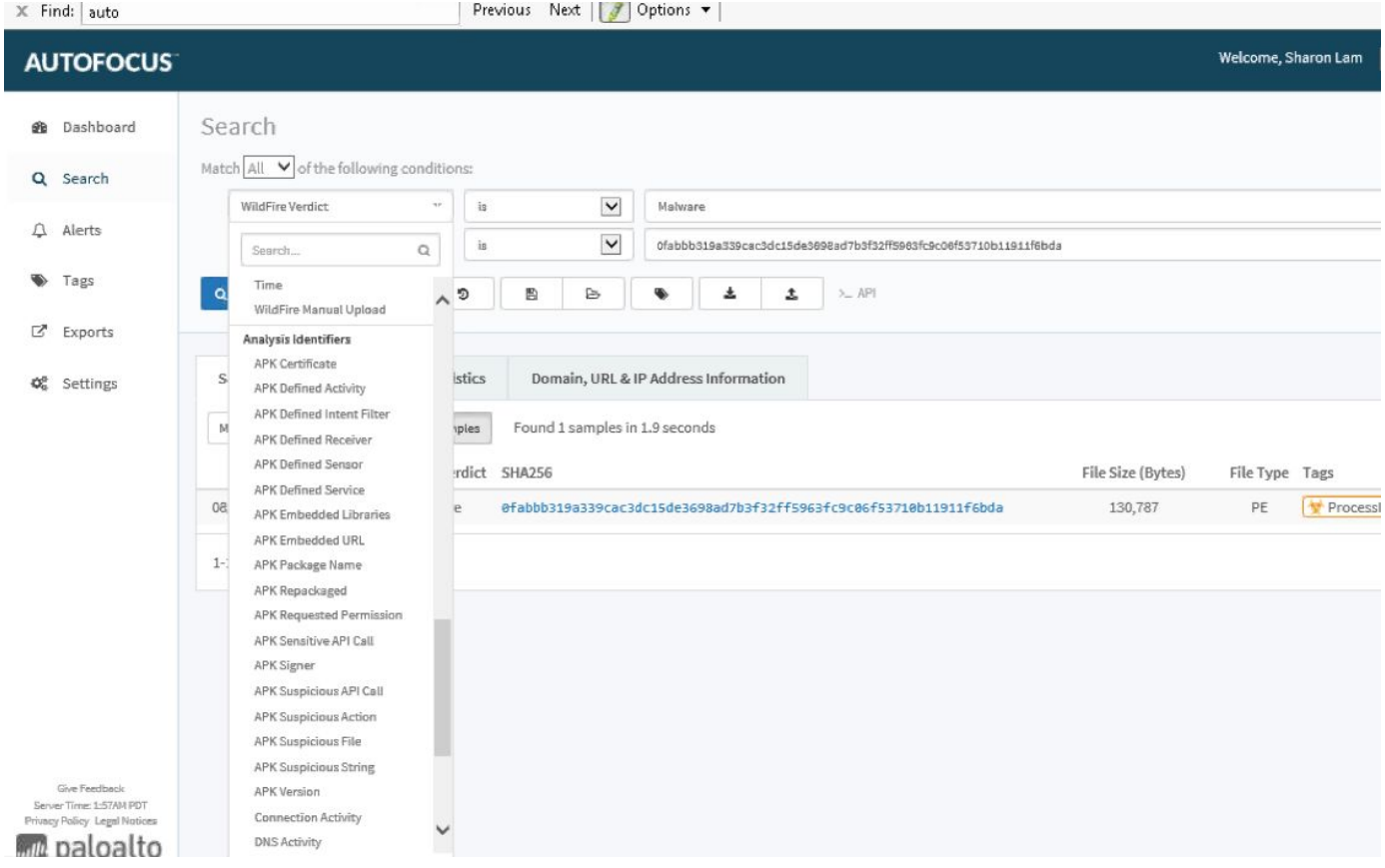
Attack indicators could be shared and provided on timely basis.

How much data could be shared within the industry?

Search query and data could be easily executed, imported and exported.

Alert is automated

AutoFocus Platform (3) - Search Facility



Intelligence Data Integration

End-Point

Microsoft EMET could be good for end point detection but it could be easily disabled and bypassed for advanced exploit:

http://researchcenter.paloaltonetworks.com/2014/12/exploits-built-circumvent-microsoft-emet-means/

Performance

Meanwhile, It’s better to consider an end point with the following features:

Bottleneck is the performance and need to tune about it. We need to balance the user experience.

Monitor your or/and 3rd party vendors, systems and devices with Knownsec products/services

Demonstration

- Knownsec Star Map - Security Operation Center - Threat Monitoring
- ZoomEye - Ongoing monitoring
- WebSOC - Ongoing monitoring
- SeeBug / POC Suite (https://github.com/knownsec/Pocsuite)

Prepare your people

We provide training for SANS 504 Incident Response course so as to strengthen the technical and response skills when incident happens

We train Macroview SOC staff with SANS 504 course so as to provide secondary support.

We would be the on-site investigator and responder and trainer of SANS 504 course. The target audience is:
Incident handlers

- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

SANS 504 Incident Response Syllabus

Prerequisite

- A strong desire to understand hacker tools and techniques
- A foundational understanding of the Windows Command Line
- A foundational understanding of core networking concepts such as TCP/IP
- A strong desire to understand how key defensive tactics can thwart advanced attackers

SANS 504 Incident Response Syllabus

Syllabus details could be found from here:

https://www.sans.org/selfstudy/course/hacker-techniques-exploits-incident-handling

Recommendation

Threat intelligence is not just for detective control but a collaborative source of information so that you could engage and prevent it in advanced.

We need systems to keep monitor the attack and recent threats.

Train your people so as to address and respond to the incident and understand attack analysis indicators.

Carry out regular drill over the network like inviting red team to do penetration test (like delivering malicious payload) and check whether the platform is effective.

Contact

Web site

http://www.knownsec.asia/

Team

- Anthony LAI, General Manager
  - anthonylai@knownsec.com
- Eric FAN, Consultant
  - ericfan@knownsec.com
- Alan Ho, Consultant
  - alanho@knownsec.com

Reference

Knownsec POCSuite:

URL: https://github.com/knownsec/Pocsuite

Mcafee 2017 Threat and Trend Report

URL:
https://www.mcafee.com/hk/resources/reports/rp-threats-predictions-2017.pdf

SANS Reading Room - Supply Chain Security

URL:
https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252