Know Your Network, Know Your Enemy

Things You Need To Do When Your Preventive Measure Fails.

Joon Kim(Hyukjoon Kim)
CEO Naru Security Inc.

In his book "The Signal and The Noise" Nate Silver[1] mentioned difference between Precision and Accuracy. The differences, Silver says is, that precise forecasts masquerade as accurate ones and some of us get fooled and double down our bets. Although it is told in the perspectives of economics but it is also true for Information Security which now suffering from highly organized movements of attackers.

As cyber-attacks become sophisticated, the more software and products are deployed in a network hoping the more the products the better the defense capability become. However, this approach tends to worsen the situation adding more noise than the signals of wily intruders who have owned your network. Naru Security Inc. has developed novel approach to intruders who have already bypassed preventive measures such as firewalls, IDS/IPS, and more sandbox based technologies in your network.

Its capabilities of detecting intruders beyond current defense mechanisms are proven by identifying on-going cyber-attacks in global business corporation, government organizations, hospitals and many other organizations known to have one of the most effective cyber security operation units in the world.

Current cyber defense system focuses heavily on precision over accuracy covering some areas of intrusions with the out-of-sample sampling bias problems[2]. In this paper, In this paper, it will be introduced with strong case studies strong case studies of how to gain both precision and accuracy in detecting on-going cyber-attack in your network.

All that matter is to differentiate signal of IoC from noise in your network.

Table of Content

[1] Nate Silver is a statistician, writer, and founder of The New York Times political blog FiveThirtyEight.com. Silver also developed PECOTA, a system for forecasting baseball performance that was bought by Baseball Prospectus. He was named one of the world's 100 Most Influential People by Time magazine. He lives in New York

[2] A systemic error due to a sample of a group in which all factors or participants are not equally balanced or objectively represented.

1. Objective and Scope

It is July 7th 2009, when the new ear of cyber-attacks begins in South Korea. Major government and financial institute in Korean and US were under heavy DDoS attacks. Although it is “just” named as another Distributed Denial of Service Attacks, the Techniques, Tactics and Procedures were completely unknown to at least to Korean cyber security industry. While our defense system were prepared against noisy flooding attacks at the national gateway, the attacker went low with application attacks from more than 50,000 well distributed compromised hosts in Korean networks, crawling small at the edge aggregated to large traffics at the gate of targeted networks.

It is told there has been at least 6 months to build such attacking infrastructure from army of zombified computers to globally distributed command and control channels. However, it is still unclear what the attacker’s goal to achieve through such well-organized movements. It seems the occurrence of DDoS attacks dropped significantly in these days, It reappears in another form of global plague of cyber terrorism and cyber espionage.

While attacker become more and more sophisticated, defense system tend to focus more on instantaneous threats with no context rather than complete the whole picture of attacker’s movements inside the protected networks. ConnecTome is developed to simplify the analysis process of on-going cyber-attacks in your networks covering three major processes of situation awareness, threat recognition and incident recognition.

2. Situation Awareness

Situation Awareness is one of the least practiced process in the field of Information Security. When your anti-virus reports you that you have 100 malwares in your network, how do you know whether it is serious or not without any reference point. Some members of your security team could think that the network is now safe as it recognized and removed the threats. In the mean while other members of your team still feel very uncomfortable over the uncertainty. This kind of discrepancy caused by the lack of seeing the whole picture of your network and it seriously impairs the performance of your security team.

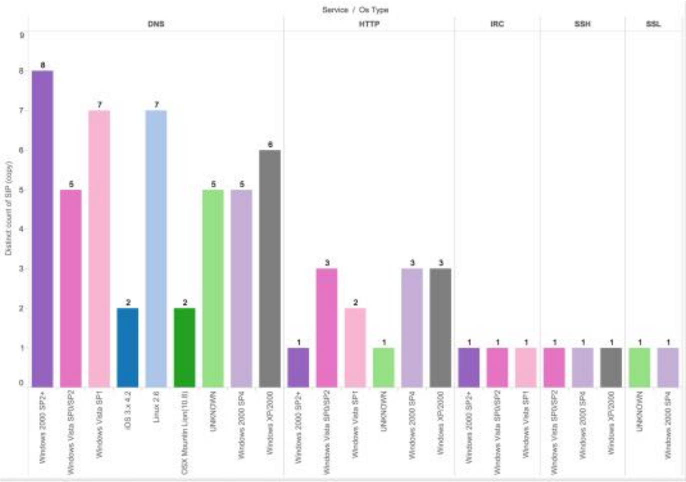


Fig 1. Internal Network Host and Service Distribution

ConnecTome keeps track of number of hosts in your networks along with its subnet distribution, operating system, listening ports, protocols, number of binary files delivered through http/smtp/ftp protocols and the inner and inter-network communications. Moreover, it oversees the whole persistent traffics in your network whether it is in a form of periodic beaconing or a reverse tunneling. Figure 1 is part of graphical report generated by ConnecTome showing number of operating system and binding network services like dns, http, irc, ssh and ssl.

Without situation awareness of your network, your security team would only have some vague awareness of possible intruders lurking out your networks, giving no way to measure the security risk in your organization. Measured risk grease the wheels of your security processes meanwhile the uncertainty grinds them to a halt.

3. Threat Recognition

Threat recognition phase in ConnecTome performed by identifying anomalous behaviors in the networks making use of the knowledge gained through situation awareness phases. It is comprised of four out of five distinct stages from the Cyber-Kill-Chain[3] Process of Initial exploitation, establishing command and control channel, lateral movements and data exfiltration/system destruction.

It is the Initial exploitation stage where it is usually covered by preventive measures such as Intrusion detection system, anti-virus software, sandbox based technologies and more. As it is heavily covered by other devices, ConnecTome only keeps track of incoming binary files in the form of MIME messages in http, smtp and ftp protocols. Once it sees the binary files in the wire, it reconstructs the file and generating hash values of MD5 and/or SHA256 to compare it with an external intelligence. The results are reported in three distinct categories of known good, known bad, and unknown.

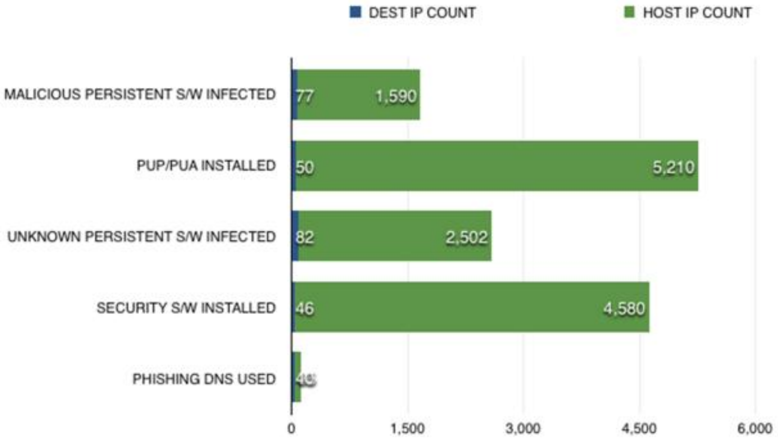


Fig 2. Types of beacon style persistent connections

Second stage of threat recognition is tracking command and control channels and it tracks both beacon and reverse channel form of persistent connections. As most enterprise and government networks are protected by some types of access control device like firewall, it is impossible for intruders to connect directly from outside. Instead, intruders exploit software and/or human vulnerabilities to infiltrate malwares inside the protected networks. Once it is installed successfully, it calls back to its master who is physically outside of the networks. To allow the attacker to control the compromised host from outside, it periodically beacons to fetch a command from its master. But to overcome the inherited shortcoming of beacon style command and control, attacker usually establish reverse tunnel style backdoors by which she can gain high degree of freedom in controlling compromised host. ConnecTome keeps track of complete list of command and control and label it as known good, known bad and unknowns. Figure 2 depicts overall beacon style persistent traffics in an organization. Despite the network is protected by antivirus software and sandbox based malware defense system, large number of hosts are periodically communicating with known bad destination identified by virusTotal API. Followed by the malicious persistent s/w infected, there is PUP/PUA[4] installed metrics. It shows the number of total destination in blue, which is 50 for PUP/PUA, and number of potentially infected internal hosts, which are more than five thousand hosts.

Since PUP/PUA is not usually installed by exploitation of software vulnerability but by human interaction, it successfully bypasses the sandbox based automated malware defense system. Most PUP/PUA has capability of installing arbitrary software, fetching command from external server and updating program, it can be easily abused by determined intruders by hijacking the infrastructures build by them. The real value

[3] Cyber-kill-chain" describes the structure of the intrusion, and the corresponding model guides analysis to inform actionable security intelligence. Through this model, defenders can develop resilient mitigations against intruders and intelligently prioritise investments in new technology or processes

[4] A PUA / PUP (potentially unwanted application / potentially unwanted program) is a software that may be unwanted on the PC and sometimes comes bundled with freeware software

of the ConnecTome is not finding known malwares in user's network but differentiating unknown persistent traffics to unknown one.

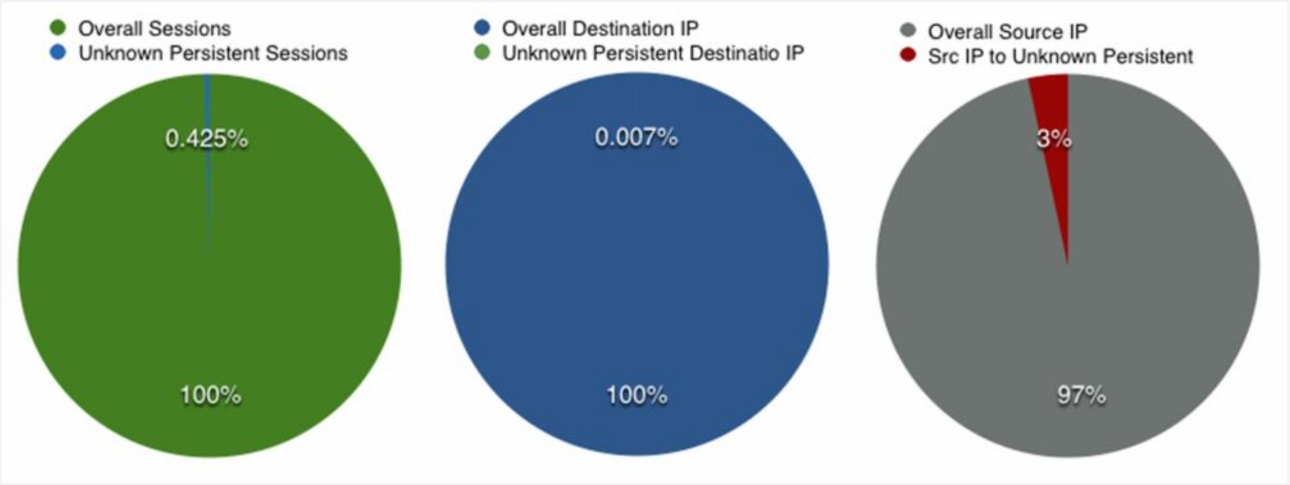


Fig 3. Ratio of unknown persistent traffics in an global corporate network

As it does not rely on any known signatures in detecting persistent traffics but it find them by examining network traffics both in real-time and historical analysis. By using patent pending technology developed by Naru Security, ConnecTome can find any persistent connections in networks. It seems daunting just by looking at the size of traffics on regular organizations. For example, In an large global corporate environment of 2G pipe at the gateway with 10,000 internal hosts, around 100 million network sessions are generated per day. However, there has been only 500 thousands unknown persistent traffics found in the network. It could still be thought as a big number but there has been only 26 unique destination IPs to be examined, which is only 0.007% of overall destination IP addresses of the organization.

ConnecTome does also tracks third stages of the simplified cyber-kill-chain, which is a lateral movement. It oversees the traffics of which both source and destination addresses are either in private or in user defined range and calculate the order of degree of lateral movements. When it calculates the degree, it handles complete connection and connection attempt differently. Users in monitored network can whitelist known good internal traffics so that it only highlights the unknown traffics between internal hosts.

Last stage in threats recognition phase provides exfiltration detection functions. As the other detection mechanisms, it uses protocol detection and anomaly detection in byte distribution. In protocol detection mode, it oversees ftp, http and smtp traffics with large outbound traffic size both in one-time and historical byte accumulation mode. Some intruders do not send big at once. Instead, she splits the big file with many small chunks and 'exfiltrates data', so that it can bypass size based memoryless systems like IDS/IPS or any other policy violation detection. ConnecTome is equipped with big data analysis engine and it examined outbound data using regular batch process adding all outbound and inbound data bytes. Watching the ratio over the time, it generates alert either by absolute accumulated size of the outbound bytes or by the reversed distribution of inbound and outbound data size. In user network, hosts act as sink and the server does as source of the data. When such ratio breaks, it should be a good symptom of possible data exfiltration.

In this phase, we have discussed four major stages of Cyber-Kill-Chain, which ConnecTome is dealing with finding threats in one's networks. Although we have introduced the notion of Cyber-Kill-Chain, we did not make full use of the "Chain" elements but the events in each stages of the Cyber-Kill-Chain. In the next phase we will discuss the way to put things together to achieve the goal of ConnecTome. To identify undetected cyber incident in one's networks.

4. Incident Recognition

Incident Recognition connects the movements of intruders inside the network by connecting dots in each stages of the Cyber-Kill-Chain. Intruders are not moving linearly following the steps of initial exploitation, building command and control, extra tool download, lateral movement, and data exfiltration. Intruder rather moves to fulfil her objectives in targeted network. Figure 4 is showing modified version of Cyber-Kill-Chain for modelling intruders inside protected network. Initial Exploitation proceeds with the command and control stages. Once intruder builds solid command and control infrastructure, she can take any movements of exfiltrate data from the first point of infection, downloading extra tool to create reverse tunnel, looking for ultimate target around the network.

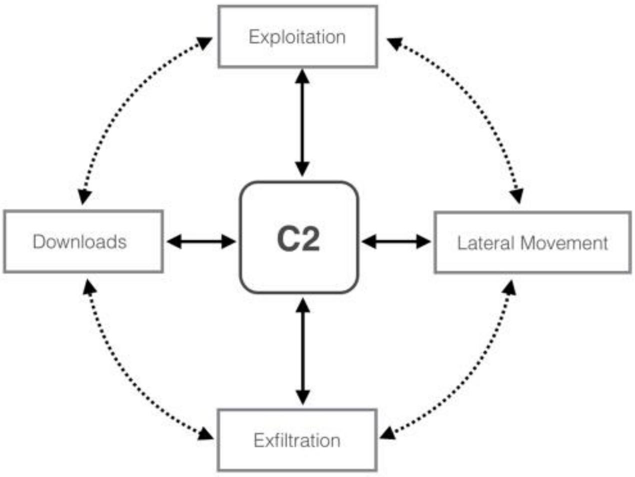


Fig 4. Modelling intruders using Cyber-Kill-Chain

As non-automated movements cannot be made solely by malware, every other movements pivots around command and control stages. Based on the circular Cyber-Kill-Chain model, ConnecTome correlates the each stages of the Kill Chain. Using this approach, ConnecTome won't count any combination of movements without command and control stage. On the other hands when a command and control channel is detected, it starts to correlate movements and calculate values to determine the response priorities. With this approach, incident can successfully prioritized so that the intruders who has higher activities can be handled by the security team.

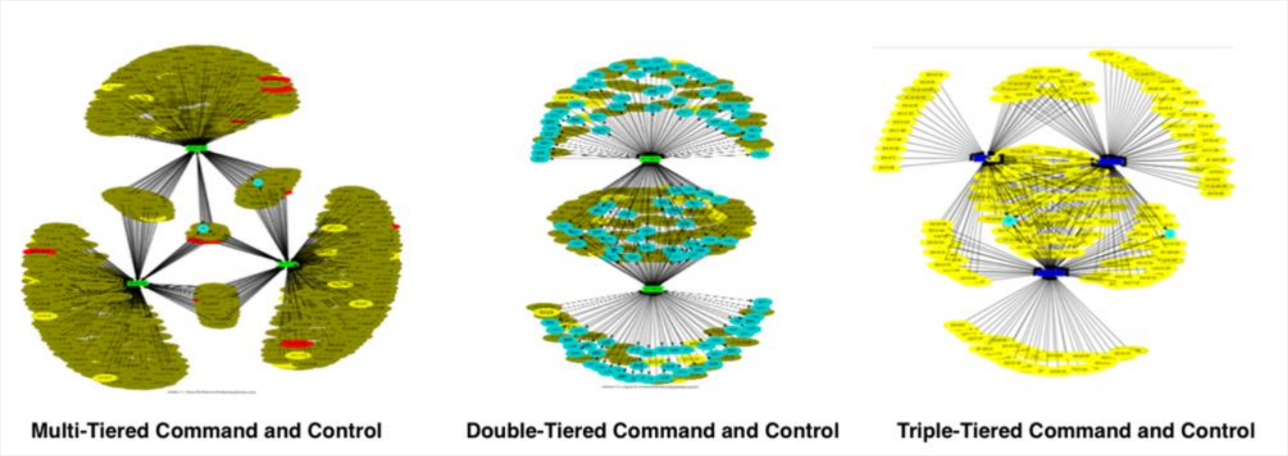
As ConnecTome has capability of clustering network traffic information gathered from multiple locations, it can not only see the traffics from the internet gateway but from any locations within the internal networks. Table 1 is an example of event correlation and corresponding threat level calculated by ConnecTome

Example Detection Scenarios

Kill Chain Stages	Indicator of Compromise	Threat Level
1	Downloading Unknown Binary File to a User PC	0%
2	After Downloading the Binary File, New Persistent Traffic Detected	30%
2	Persistent Reverse Tunnel Traffic Detected	60%
3	Failed Connection Attempts to PCs in the Local Network	70%
3	Successful SSH Connection is made after Several Login Failure	80%
4	Continuous Data Flow from Internal Hosts to External Network	90%

Table 1. ConnecTome event correlation and corresponding threat level

5. Conclusion



Multi-Tiered Command and Control

Double-Tiered Command and Control

Triple-Tiered Command and Control

Fig 5. Types of command and control channel detected by ConnecTome

It is year of 2004, Richard Bejtlich, Chief Security Strategist at FireEye, says “Prevention Eventually Fails” in his book Tao of Network Security. However, majority of industry still believe in the myth of perfection defines at the gateway allocating 90% of defence system for preventive measures. From numerous on-site analysis experience, we have identified there exists many intruders inside the network, bypassing layers of preventive measures, building its own infrastructures for gathering valuable informations through the network. Figure 5 is showing different types of command and control channels detected through ConnecTome form our customer’s network. The structural differences among three comes from the size of compromised hosts it controls and maturity of the c2 infrastructures.

ConnecTome is a network security analysing platform to identify on-going cyber attacks in your network. It has three phase of situation awareness, threat recognition and incident recognition. In situation awareness phase, it draws base line of your network security posture. Along with the base line established, it identifies possible threats in your network using the model of Cyber-Kill-Chain Process in a very granular fashion. The last phase of whole process is incident recognition and it performs consequence analysis using both real-time and historical analysis. In this phase, the system calculate the threat level of possible security breach by connecting the possible intruders movements of downloading malwares, building command and control channel, lateral movement and data exfiltration.

EPS-ConnecTome’s data centric process delivers clear notion of security posture of your organization having your security team to be on the same page. It converts recognition of initial exploitation from disaster to blessing by providing complete picture of intruder’s movements in your network so the you can be total control of her movement before the goal of incident is fulfilled.