I am Yin Minn Pa Pa from Myanmar currently studying as first year Ph.D student at Yokohama National University. The research area I am focusing is network security.

私はミャンマーからのインミンパパと申します。現在横浜国立大学で博士課程後期１年生としてネットワークセキュリティーの研究をしております。

Outline of Research

研究の概要

Network security is becoming of great importance because of intellectual property that can be easily acquired through the Internet. There is a large amount of personal, commercial, military, and government information on Internet. All of the information can be leaked easily from malware-infected computers. (Malware = Malicious Software such as computer virus program).

ネットワークセキュリティーはなぜ非常に重要になっているとインターネットで知的財産は簡単に取得出来ることからです。多くの個人的、商業、政府や軍の情報はインターネットであります。すべての情報は、マルウェアに感染したコンピュータから簡単に漏洩することができます。（マルウェア＝悪意があるプログラム）

In addition to information leakage, groups of thousands of malware-infected computers (botnet) are controlled by hackers and are abused for large-scale cyber crimes such as attacking and breaking down Internet infrastructure of the whole country.

情報漏洩に加えマルウェアに感染した多くのコンピュータグループ（ボットネット）は攻撃者にコントロールされ攻撃や全国インターネット破壊などの大規模なサイバー犯罪ができます。

In order to reduce cyber crimes of today's Internet, there are two approaches. The first one is identifying malware-infected computers. Once malware-infected computers are identified, network administrator can block their connection to hackers. The other is detecting hacker side attack infrastructure. To commit large-scale cyber crimes, hackers need their own infrastructure. Once hackers' infrastructure is detected, network administrator can block the incoming connection from them.

サイバー犯罪を減らすためには二つの方法があります。一つはマルウェアに感染したコンピュータを特定することです。マルウェアに感染したコンピュータが見つけると、ネットワーク管理者は、攻撃者への接続をブロックすることができます。もう一つは、攻撃者側の攻撃インフラを検出することです。大規模なサイバー犯罪をするのには、攻撃者側にも自分の攻撃インフラは必要です。攻撃者側のインフラが検出されると、ネットワーク管理者はそれらからの着信接続をブロックすることができます。

I am currently doing research on identifying hacker side infrastructure. In hacker side infrastructure, there is an important system called DNS (domain name system). As a hacker, in order to build communication channel between hacker and infected computers, DNS is necessary. That is why I am mainly focusing on a method of identifying hacker's DNS infrastructure .

現在、私は攻撃者側のインフラを特定することについている研究をしております。攻撃者側のインフラで　DNS(Domain Name System)と呼ばれる

重要なシステムがあります。攻撃者側と感染したコンピュータ間の通信チャネルを構築するためには、DNS が必要です。だから私は攻撃者側の DNS インフラを識別する方法について研究を中心しております。

Study Plan

1. In Master Thesis research, I focused mainly on identification of malware-infected computers.
2. In First Year Ph.D course, I am now focusing on identifying hackers' side attack infrastructure.
3. In Second Year Ph.D course, I will do visualization system of hackers' side DNS servers in order to understand large scale cyber attacks easily.
4. In Third Year Ph.D course, I will focus on an effective countermeasure of malware infected computers and hacker's side DNS infrastructure. Then, I will document all my researches as Ph.D thesis.

研究計画

1。修士論文の研究ではマルウェアに感染したコンピュータの識別を主に中心しました。

2。現在博士課程１年目には攻撃者側のインフラを特定することについている研究をしております。

3。今後博士課程２年目には攻撃者側の DNS インフラを可視化して大規模サイバー攻撃を簡単に理解出来るシステムを作ります。

4。最後の博士課程３年目にはマルウェアに感染したコンピュータと攻撃者側の DNS インフラの効果的な対策について研究をします。最後に前の研究をまとめで博士課程論本を書きたいと思います。

Future Plan

After graduation, I would like to go back to my country. For the development of Myanmar, I would like to try my best from any corner I could do.

Currently, IT development is gaining momentum in Myanmar. The more IT involves in daily lives of Myanmar people, information security will be in need for them in near future. In that time, I would like to be a skillful security engineer to fulfill the needs people as much as I can.

In a situation of no Internet, insufficient books and computers and no skillful teacher, my university life in Myanmar had to face a lot of difficulties. The worst is lack of skillful teacher in IT security field. I want the younger generation of my country not to suffer like me. That is why I would like to contribute as much as I can for the development of IT education in Myanmar.

将来の計画

卒業した後はミャンマーに帰ります。ミャンマーの発展のために自分が出来ることなら何でも一生懸命頑張りたいと思います。

現在、ミャンマーで　IT は飛躍的に発展しております。ミャンマー人の生活に IT は必要になるほど、近未来にネットワークセキュリティーは非常に重要になるそうです。その時私は人々の必要なものをかなえる巧みな情報セキュリティーエンジニアとして行きたいと思います。

インターネットや不十分な書籍やコンピュータや巧みな先生とかない状況で私のミャンマーでの大学生活は、多くの困難がありました。一番困ったのは情報セキュリティーをよく分かる先生はないことでした。将来のミャンマーの若者に私みたいな困ることがないようにしてくれたいと思います。だからミャンマーの IT 教育のために自分が出来るだけ手伝をして一生懸命頑張りたいと思います。

Research I have conducted in the past

1. In 2005, I did the research on “Network Security in Local Area Network”.
2. In 2012, I did the research on “Search Engine based investigation on misconfiguration of zone transfer”.

   For this work, I could fix big security issue of Myanmar Network and received best paper award at 8th Asia Joint Conference on Information Security held in Korea, July 2013.
3. In 2012, I have initiated Japan-Myanmar network security collaboration research. I work as volunteer Engineer on the research of “Identification of malware-infected computers in Myanmar network using DNS traffic”.
4. In 2013, January, as a co-worker, we did research on “A Method for Detecting Malware-Infected Hosts with Similarity of Name Resolution Behavior”.
5. In 2013, March, I did research on “ Finding Malicious Authoritative Name Server”.

前の研究

１．２００５年に“ローカルエリアネットワークセキュリティー” に関する研究を行いました。

２．2012 年に "検索エンジンに基づいてゾーン転送の設定違いの調査"に関する研究を行いました。

この研究のことでミャンマーのネットワークの大きなセキュリティ問題を解決し、韓国で 2013 年 7 月に開催された 第 8 回情報セキュリティアジア合同会議で最優秀論文賞を受け取りました。

3. 2012 年に日本とミャンマーのネットワークセキュリティの共同研究を開始しました。"DNS トラフィックを使用してミャンマーのネットワーク内のマルウェアに感染したコンピュータを見つける方法"に関する研究にボランティアとして研究を行いました。

４．2013 年 1 月には、同僚として、"名前解決の挙動の類似性を利用してマルウェアに感染したホストを検出する方法"に関する研究を行いました。

5. 2013 年 3 月には、"悪意がある権威 DNS サーバを探する"に関する研究を行いました。