Cyber 4.0

Kovelin Naidoo
LAY OF THE LAND

“THOSE WHO DO NOT KNOW THE PLANS OF COMPETITORS CANNOT PREPARE ALLIANCES. THOSE WHO DO NOT KNOW THE LAY OF THE LAND CANNOT MANEUVER THEIR FORCES. THOSE WHO DO NOT USE LOCAL GUIDES CANNOT TAKE ADVANTAGE OF THE GROUND.”

SUN TZU

“I’M HERE TO TELL YOU THAT YOUR CYBER SYSTEMS CONTINUE TO FUNCTION AND SERVE YOU NOT DUE TO THE EXPERTISE OF YOUR SECURITY STAFF BUT SOLELY DUE TO THE SUFFERANCE OF YOUR OPPONENTS.”

Brian Snow, 2012
Head of Information Assurance NSA
STANDARD BANK COMPUTER WAS HACKED IN R300m ATM FRAUD HIT - report

2016-06-30 11:03
Gareth van Zyl, Fin24

According to the police, the syndicate transferred money from its coffers to the personal accounts of some other customers. Afterwards, they connived with the customers to withdraw the money.

2016-10-21
Kwasi Gyamfi Asiedu

TWO GHANAIANS ARRESTED FOR ALLEGEDLY HACKING BANK ACCOUNTS

KENYA REVENUE AUTHORITY ‘LOST $39m TO HACKER’
ORGANISED CRIME
Background + Context

World’s first encrypted wireless Communication network

Real world innovation: Narco submarines 8 tons on board minimum
NEXT GENERATION MALWARE
PAY-PER-INSTALL

Selling mix world downloads.
Loads through the loader.
The price is 70 $ for 1000 installs.
Minimal 500 installations.
To regular customers and for wholesale I make discounts.
The sample is negotiated separately.
For all other questions, write to the jabber.
Sergey.ulanov@exploit.im

Selling android installations:
Price: from 1 dollar to 1.5 - installation.
With you it is necessary: access to statistics and clean apk.
The apk must be crypted. On the test I do not pour, in advance, too.
Downloads: $ 4 - 1000 conversions.
Orders from $ 30
Garant greetings!
Payment Qiwi, Yandex money.
Contact for communication: android2011@xmpp.jp
There is also an android bot with injections on sale. Working on versions from 2.2 to 5.0 and higher.
THREAT ACTORS

NATION STATES

MOTIVATED BY PROFIT

MOTIVATED BY CAUSE
THREE FORCES OF CYBER EFFECT (3FC)

1. Mechanization, water power, steam power
2. Mass production, assembly line, electricity
3. Computer and automation
4. Cyber Physical Systems

4TH INDUSTRIAL REVOLUTION

LAY OF THE LAND

ASSANGE EFFECT

SNOWDEN EFFECT

ATTACK SURFACE COMPLEXITY

http://www.thinkst.com
ASSANGE EFFECT
SNOWDEN EFFECT
ATTACK SURFACE COMPLEXITY
ATTACK SURFACE COMPLEXITY

1991 - 10,239 lines of code
2017 - 33,580,696
LOC % bugs?

20M lines of code

https://www.openhub.net/p/linux
ATTACK SURFACE COMPLEXITY
DDOS & IOT

PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS!!!

WE ARE DDoS HACKERS CARTEL.
All your servers will be DDoS-ed starting Wednesday February 8th 2017 from 8.00am if you don't pay Protection Fee of USD $2,000 by PayPal to: ddoscartel@gmail.com

If you don't pay by Tuesday 7th, attack will start, price to stop will increase to USD $5,000 and will go up USD $500 for every day of attack.

What does this mean?
This means that your website and other connected services will be unavailable for everyone; during the downtime you will not be able to generate any sales. Please also note that this will severely damage your reputation amongst your users / customers as well as strongly hurt your Google rankings (worse case = your website will get DE-indexed).

How do I stop this?
We are willing to refrain from attacking your servers for a small fee. The current fee is USD $2,000. The fee will increase by USD $500 for each day that has passed without payment.
Please send the Protection Fee to the following PayPal address: ddoscartel@gmail.com

This is not a joke.
Our attacks are extremely powerful – sometimes over 1 Tbps per second.
So, no cheap protection will help.

What if I don't pay?
If you decide not to pay, we will start the attack at the indicated date and uphold it until you do, there's no counter measure to this, and you will only end up wasting more money trying to find a solution. We will completely destroy your reputation amongst Google and your customers and make sure your website will remain offline until you pay.
This is not a hoax, do not reply to this email, don't try to reason or negotiate, we will not read any replies. Once you have paid we won't start the attack and you will never hear from us again!
Please note that PayPal is anonymous and no one will find out that you have complied.

Beware
DDoS Hackers Cartel
Twitter: @ddoshackers
Facebook: DDoS Hackers Cartel
Cyber-Security Consultants, Certified Ethical Hacker & Black Hat Hacker
THERE IS HOPE...
FOG OF WAR

SUDDENLY
EXPERTS ON CYBERSECURITY EVERYWHERE
FOCUS AND A CHANGE IN THINKING

- 80 / 20 / Reality
- Bias
- Advocatus Diaboli
- 4ThIR Building blocks
- Security as enabler

<table>
<thead>
<tr>
<th>IDENTIFY</th>
<th>PROTECT</th>
<th>DETECT</th>
<th>RESPOND</th>
<th>RECOVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset management</td>
<td>Access control</td>
<td>Anomalies and events</td>
<td>Response planning</td>
<td>Recovery planning</td>
</tr>
<tr>
<td>Business environment</td>
<td>Awareness and training</td>
<td>Security continuous monitoring</td>
<td>Communications</td>
<td>Improvements</td>
</tr>
<tr>
<td>Governance</td>
<td>Data security</td>
<td>Detection process</td>
<td>Analysis</td>
<td>Communications</td>
</tr>
<tr>
<td>Risk assessment</td>
<td>Information protection and procedures</td>
<td></td>
<td>Migration</td>
<td></td>
</tr>
<tr>
<td>Risk management strategy</td>
<td>Maintenance</td>
<td></td>
<td>Improvements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protective technology</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
THANK YOU

@kvelin

http://blog.cyberelders.org