ACAMS

Cybersecurity Risk We All Face

Jerry Craft | August 2017
About Your Speaker
About Nth Generation Computing
Ransomware Attacks & Extortion
Hacking 101
Website Hacking 101
Phishing, Smishing and Lying
Nation State Attacks
Jerry Craft – Nth Generation Computing

- Senior Security Consultant, CISO and Ethical Hacker
- Formerly Chief Information Security Officer for 6 billion dollar financial institution.
- 25+ years of IT and Security experience.
- Security author, instructor, and speaker

- Certified Information Systems Security Professional (CISSP)
- SANS Institute GIAC Security Professional (GSEC)
- SANS Institute GIAC Penetration Tester and Ethical Hacker (GPEN)
- SANS Institute GIAC Forensic Examiner (GCFE)
- SANS Institute Instructor for SANS 560: Ethical Hacking and Penetration Testing
Jerry Craft – Nth Generation Computing

• Reviewed and secured the following business verticals
  • Finance, Healthcare, Government, Utility, Educational and Retail environments.

• Work with businesses and perform forensic understanding to hacking attacks.

• Perform incident response on hacking incidents to help customers understand a breach, and get law enforcement involved when necessary.

Nth Generation is a 26 year old solution provider that has access to the latest technology, and performs security engagements using highly skilled ethical hackers, and former CISO’s.

- Founded in 1991
- Southern-California focused
- Offices in San Diego (HQ) and Irvine
- HP Security Partner of the Year 2015
- Cylance Security Partner of the Year 2017
Consulting Engagements

- Ethical Hacking
- Red Team (Physical Security)
- Risk Assessments
- Social Engineering
- Security Roadmaps
- Cloud Computing Assessments
- Virtual CISO
- Security Consulting
Ransomware Attacks and Extortion
Ransomware 1989-2017  AIDS Trojan to Cryptolocker
Nth Generation

Ransomware 1989-2017  AIDS Trojan to Cryptolocker

INTRODUCTION

Welcome to the interactive computer program called AIDS Information. This program is designed to provide up-to-date information about you and the fatal disease AIDS (Acquired Immune Deficiency Syndrome). The health information provided to you by this program could save your life.

Here is how the program works: First, the computer will ask you a series of questions about your personal background, behaviour and medical history. Then the program will calculate your chances of being infected with the AIDS virus and inform you about your present degree of risk. Then it will provide you with advice on what you can do to reduce your risk of future infection, based on the details of your own lifestyle and history. Finally, it will give you the chance to ask questions or to make comments.

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don’t use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers:

The price of 365 user applications is US$189. The price of a lease for the lifetime of your hard disk is US$378. You must enclose a bankers draft, cashier’s check or international money order payable to PC CYBORG CORPORATION for the full amount of $189 or $378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-12-44, Panama 7, Panama.

Press ENTER to continue
Ransomware 1989-2017  AIDS Trojan to Cryptolocker

• Ransomware is a type of malware which is classified as a Trojan.

• It restricts access to, or, damages the computer for the purpose of extorting money from the victim.

• It also has the capability to encrypt a users files, display different threat messages, and force the user to pay ransom via an online payment system.

• There have been more than 700,000 ransomware attempts between 2015-2016.

• Most companies simply restore the data, or pay the ransom.
Ransomware 1989-2017  AIDS Trojan to Cryptolocker

1. Ransomware will become just another tool in the hacker utility belt.
2. We’ll see more attacks designed to publicly shame the victims.
3. More examples of ransomware using no executable as a means of evading detection.
4. If there is a decline in ransomware it will be because of law enforcement action.

https://en.wikipedia.org/wiki/Ransomware
Ransomware 2017

Ransomware 2017

Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

Cryptolocker – Hollywood Presbyterian Medical Center
Computer access was blocked and not restored until payment was made.
HBO offered hackers $250,000 'bug bounty', leaked email claims

 Apparently ‘surprised’ by release of documents, TV network attempts to push back ransom deadline with promise of payment
Hacking 101
Virus/Worm 2008 -- Conficker

1. Hacker developed vulnerability (**MS08-067** Microsoft Windows)
2. Fast spreading worm that targets vulnerability
3. Blended threat that infects, disables security, backups, deletes data and opens a connection to a remote computer
4. Spreads by copying itself to folders, drives, etc.

https://en.wikipedia.org/wiki/Conficker
1. NSA developed vulnerability (**MS17-010** Microsoft Windows / AKA EternalBlue)
2. Used by hackers worldwide for a WannaCry ransomware attack 5/12/2017.

What do hackers look for to find vulnerabilities?

What if I type HELO 1000 times?
Blue screen of death!

A problem has been detected and Windows has been shut down to prevent damage to your computer.

**DRIVER_IRQL_NOT_LESS_OR_EQUAL**

If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:

```plaintext
*** STOP: 0x00000001 (0x0000002, 0x00000000, 0xF86B5A89)

```

```plaintext
***
gv3.sys - Address F86B5A89 base at F86B5000, DateStamp 3dd991eb
```

Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further assistance.
Computer memory for the win!
Blue screen of death!

Hacked for the win!
The proliferation of cyber-events and cyber-enabled crime represents a significant threat to consumers and the U.S. financial system. The Financial Crimes Enforcement Network (FinCEN) issues this advisory to assist financial institutions in understanding their Bank Secrecy Act (BSA) obligations regarding cyber-events and cyber-enabled crime. This advisory also highlights how BSA reporting helps U.S. authorities combat cyber-events and cyber-enabled crime.

Through this advisory FinCEN advises financial institutions on:

I. Reporting cyber-enabled crime and cyber-events through Suspicous Activity Reports (SARs);

II. Including relevant and available cyber-related information (e.g., Internet Protocol (IP) addresses with timestamps, virtual-wallet information, device identifiers) in SARs;

III. Collaborating between BSA/Anti-Money Laundering (AML) units and in-house cybersecurity units to identify suspicious activity; and

IV. Sharing information, including cyber-related information, among financial institutions to guard against and report money laundering, terrorism financing, and cyber-enabled crime.
Website Hacking
Website Compromises...

The image shows a login screen with a SQL injection vulnerability. The username field contains the string `' or 1=1--`, which is a common indicator of SQL injection attacks.
Phishing / Smishing and Lying.
Dear valued customer of TrustedBank,

We have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.
Phishing
Whale Phishing

- Whale phishing is a term used to describe a phishing attack that is specifically aimed at *wealthier individuals*. Because of their relative wealth, if such a user becomes the victim of a phishing attack he can be considered a “**big phish**,” or, alternately, a whale.

- Whaling attack emails comprise of a legal summon, consumer complaint, or managerial issues that require an **urgent reply** from the receiver.
Nth Generation

Whaling...

Urgent Request

Stu Sjouwerman <stus@knowbe4.

to me

Alanna

I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap.

Request from CEO

Subject: Immediate Wire Transfer

To: Chief Financial Officer

High Importance

Please process a wire transfer payment in the amount of $250,000 and code to “admin expenses” by COB today. Wiring instructions below...
Catfishing

Hackers catfish tech execs on LinkedIn

- “Mia Ash” – April 2016 – persona befriended male employees of oil and technology firms in Israel, Saudi Arabia, India, US and Iraq.
- Hacking group in Iran is believed to be behind the accounts. – Secureworks.
- Group named Cobalt Gypsy
- Purpose: steal credentials from employees who would have access to their companies computer networks.
- LinkedIn is a great-successful way for hackers to target people because users are inclined to trust others on the site.

Whaling...

Oops! You clicked on a phishing email.
Remember these three ‘Rules To Stay Safe Online’

✓ RULE NUMBER ONE:
  • Stop, Look, Think!
  • Use that delete key.

✓ RULE NUMBER TWO:
  • Do I spot a Red Flag?
  • Verify suspicious email with the sender via a different medium.

✓ RULE NUMBER THREE:
  • “When in doubt, throw it out”. There are a thousand ways that internet criminals will try to scam you, and only one way to stay safe: Stay alert as YOU are the last line of defense!

PLEASE NOTE:
This message came from KnowBe4, LLC and not from the company whose name is mentioned in the body of the email message, as that company has no association with KnowBe4, LLC and does not endorse the services of KnowBe4, LLC. The purpose of this message is to demonstrate how phishing attacks can come in emails that deceptively appear to be from reputable companies.
State & Nation State Attacks
Who are the attackers?

- United Kingdom
- Russia
- Iran
- Israel
- United States
- China
- North Korea
Exposed 22 million current and former employees records compromised and stolen.

1. Identify undercover officers
2. Neutralize U.S. government officials
3. Threaten overseas family members
4. Harass clearance holders or their families in the United States
5. Wire you for sound
6. Figure out exactly what it takes to get a security clearance
7. Publish the data
8. Guess passwords
Who are the attackers?

- Who is number 1: China, then North Korea, Russia
- I have investigated these types of attacks.
  - Purpose was to take intellectual property
  - To destroy the business competition.
  - Improve the intellectual property for China to resell and win deals.
Key Takeaways
What can be done?
What can be done?

Suggested Roadmap

1. Security Roadmap and Continues Improvement Plan Development
2. Security Program and Policy Review and Amendment
3. Crisis Management, Business Continuity and Disaster Recovery Readiness Assessment
4. Security Controls Effectiveness Assessment
5. ICS/SCADA Risk Assessment

7) From where should we start?

Consultation
What can be done?

VIRTUAL CISO PROGRAM

As Cybersecurity continues to be top of mind for all organizations, many do not have the resources to hire a full-time CISO and others would rather leverage external resources to complete the task allowing the business to stay focused on other matters at hand.

Understanding your need for solid security solutions at a reduced cost, Nth Generation is now offering Virtual CISO services. With this Virtual CISO program, Nth Generation provides seasoned security consultants delivering on the CISO role for significantly less than a full-time resource.

5 REASONS YOU NEED A VCISO

1. LOWER COST
   Hiring and keeping skilled security experts is pricey. Without resources to hire a full-time CISO, it’s possible to leverage external outlets at a significantly lesser cost, while allowing you to improve your security posture efficiently.

2. RAMP CYBERSECURITY
   The Virtual CISO leads your technical resources and serves as an evangelist for your cybersecurity program. They leverage the NIST Cybersecurity framework to quickly assess current-state security and define future-state vision.

3. NO NEED TO BECOME AN EXPERT
   Keep your current IT team focused on your core business. The Virtual CISO offering from Nth allows you to keep your team focused and moving forward with your business needs, while keeping your environment secure.

4. MARKET DEMAND
   CISOs and Cybersecurity experts are in high demand and finding the right candidate in a timely manner is becoming harder. Nth’s Virtual CISO offering enables organizations to achieve high levels of information security maturity with minimal cost and resource allocations.

5. IMMEDIACY
   Get immediate access, assessments and recommendations from experienced security experts. If you have an immediate need to ensure you are meeting compliance standards, are using best practices and have the best technology solutions to prevent a cyber-attack.

Once your requirements are defined, Nth will work on project-basis, a time-and-materials basis, or a bucket of hours.

www.Nth.com | (800) 548-1883