Ransomware Update

Garrick Ng
Cyber Security Professionals Awards - Gold Winner
Smart City Consortium Security SIG Chairman
Chief Technology Officer
Cisco Hong Kong, Macau, Taiwan
Nov 2017
The Evolution of Ransomware Variants

The confluence of easy and effective encryption, the popularity of exploit kits and phishing, and a willingness for victims to pay have caused an explosion of ransomware variants.
Ransomware in 2016: $1 billion

Locky, Cerber, CryptXXX, Cryptowall, …

Source: Cisco MCR and Goggle research report
Your computer files have been encrypted. Your photos, videos, documents, etc.
But, don’t worry! I have not deleted them yet.
You have 24 hours to pay 150 USD in BitCoin.
Your computer files have been encrypted. Your photos, videos, documents, etc...
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.

If you do not have bitcoins Google the website localbitcoins.
Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept either one.
Send to the Bitcoins address specified.
Within two minutes of receiving your payment your computer will receive the decryption key and return to normal.
Try anything funny and the computer has several safety measures to delete your files.
As soon as the payment is received the encrypted files will be returned to normal.

Thank you

59:59

1 file will be deleted.

Please, send $150 worth of Bitcoin here:
1FbyNgDnqYQR5v5HJ8PTAE&k4qwNBcz.

I made a payment, now give me back my files!
Your files have been encrypted. We will delete files every hour.

Ransom / Reclamation fee: $300 USD

You must pay $150 USD in Bitcoins to the address specified below:

Depending on the amount of files you have, your ransom can double to $300 if not paid within 36 hours.

Take a picture of the BTC address, ransom ID and contact email.

We will delete files every hour until you pay.

Your payment BTC Address is 1aQYwHfGK37YfVxMrG4bcPqX5qW9.

Every time you restart your computer, it re-encrypts everything. It will take a while for you to see this screen again. Take a photo in case you want to contact us.

Email: crypto@hitman.com

Questions: email us: crypto@hitman.com

5 files will be deleted. 1 archives remain.

Send: Envie $150 worth of Bitcoin to your BTC address.

I made a comment. hope you like back up files. Nice of you to check defenses now and then.

Email: crypto@hitman.com

Email: crypto@hitman.com

Email: crypto@hitman.com
RaaS
14-Year-Old Japanese Boy Arrested for Creating Ransomware
Swansea Police, Massachusetts $750
Dickson County Police, Tennessee $572
Tewksbury Police, Massachusetts $500
Midlothian Police, Chicago $500
Melrose Police, Massachusetts $450

Melrose Police Dept, MA. $500
工學院某老師

釣魚信件騙取密碼

寄件者：support@sth.edu.hk
主旨：重要提示：親愛的電子郵件帳戶的用戶
內容：
您的郵箱已超過管理員設置的默認存儲限制。
您目前正在運行的低，你可能無法發送或接收新郵件，
直到您重新驗證您的郵箱。
重新驗證您的郵箱，請點擊下面的連結，
並正確填寫所需的所有信息：
http://redcliffebedandbreakfast.com/wp-infile/reemail.html

謝謝
系統管理員

學校郵件主機
名譽評等降級
寄外信件遭退

利用盜取之帳號密碼
帳號密碼取得
重新驗證畫面
請點擊”鍵接”
We have FW, and we have Anti-Virus
How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTISING

Web redirect

WEB LINK

EXPLOIT KIT DOMAINS

Angler

Nuclear

Neutrino

C2

Malicious Infrastructure

File drop

RANSOMWARE PAYLOAD

Encryption Key Infrastructure

How Ransomware Works

User Clicks a Link or Malvertising Ad

Email w/ Malicious Attachment

Initial Exploit Using Angler or other malware kits

Command & Control callback

Ransomware payload downloaded and installed

Key retrieval and payment information

COMPROMISED SITES AND MALVERTING
Most Ransomware Relies on DNS and C2 Callbacks

- **COMPROMISED SITES AND MALVERTISING**
  - Web redirect
  - Web link

- **PHISHING SPAM**

- **EXPLOIT KIT DOMAINS**
  - Angler
  - Nuclear
  - Neutrino

- **C2**

- **Malicious Infrastructure**

- **Encryption Key Infrastructure**

- **File drop**

- **RANSOMWARE PAYLOAD**

- **Email attachment**
<table>
<thead>
<tr>
<th>NAME</th>
<th>DNS</th>
<th>IP</th>
<th>NO C&amp;C</th>
<th>TOR</th>
<th>PAYMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locky</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>SamSam</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS (TOR)</td>
</tr>
<tr>
<td>TeslaCrypt</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>CryptoWall</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>TorrentLocker</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>PadCrypt</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS (TOR)</td>
</tr>
<tr>
<td>CTB-Locker</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>FAKBEN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS (TOR)</td>
</tr>
<tr>
<td>PayCrypt</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
<tr>
<td>KeyRanger</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DNS</td>
</tr>
</tbody>
</table>
Predictive

100B requests per day
85M daily active users
12K enterprise customers
160+ countries worldwide
CRYPTOLOCKER

The "Ripple Effect" by OpenDNS Research

https://youtu.be/acwD_OA3QZ4
Basic defense: Prevent, Detect and Contain Ransomware with Cisco Email Security, Umbrella, and AMP for Endpoint
14 Day Free Trial of Cisco Umbrella

Get started in 30 seconds
No credit card or phone call required.

WHAT IS INCLUDED?

✓ Threat protection like no other — block malware, C2 callbacks, and phishing.
✓ Predictive intelligence — automates threat protection by uncovering attacks before they launch.
✓ Worldwide coverage in minutes — no hardware to install or software to maintain.
✓ Weekly security report — get a personalized summary of malicious requests & more, directly to your Inbox.

First name

Last name

Company Email

Company Phone

Company Name

Select your country

Are you an MSP, IT services provider or reseller? No

CREATE MY TRIAL
Continuous Analysis and Retrospective Security
Only AMP for Endpoints Continuously Monitors, Records, and Analyzes All File Activity, Regardless of Disposition

- Recording
  - Identify a point of origin
  - Track its rate of progression and how it spread
  - See where it's been
  - See what it is doing
  - Surgically target and remediate
Network File Trajectory for 0517f034...588e1374

File SHA-256: 0517f034...588e1374
File Name: WindowsMediaInstaller.exe
File Type: MSEXE
File Category: Executables
Current Disposition: Malware
Threat Score: High

Trajectory:
Dec 06, 2015
10:57 17:40 18:06 18:10 18:14 18:17

IP Addresses:
10.4.10.183
10.5.11.8
10.3.4.51
10.5.60.66
What customers are saying about AMP for Endpoints

"We displaced Symantec Endpoint Protection and within 10 days, we detected over 500 new vulnerabilities in our environment, increased our threat detection by 200% and reduced our incident response time by 10 days. Overall, AMP for Endpoints has been one product that has increased our security visibility the most in the past 18 months."

— Chief Information Security Officer, Medium Enterprise Computer Software Company

Visit https://www.techvalidate.com/collections/amp-for-endpoints-survey-results for more quotations and metrics
Ransomware 2.0

Targeted Ransomware (APT)

Cryptoworm

Source: Cisco MCR and Google research report
Hollywood Presbyterian Medical Center
Methodist Hospital in Henderson, Kentucky
Chino Valley Medical Center in Chino, Ontario, California
Desert Valley Hospital in Victorville, Ontario, California
Ottawa Hospital, Canada
MedStar managed hospitals in Baltimore, Washington, Maryland
King’s Daughter’s Health, Indiana
Alvardo Hospital Medical Center, San Diego
Chino Valley Medical Center, California
Desert Valley Hospital, California
LA Hollywood Presbyterian Medical Center, $17000
Email, financial aid, voice mail, phone system. $28,000 ransom
San Francisco MUNI Railway, 900 computer encrypted, demand for $73,000
메인 사이트의 트래픽 과부하로 인해 임시 사이트를 운영하고 있습니다.

랜섬웨어 서버복구 과정에 대한 공지,

사이트 복원을 바롯한 문의 사항에 대한 응대를 진행하고 있습니다.

이용에 불편을 드려 죄송합니다.

임시 사이트 바로가기 ➔

기존 사이트 바로가기 ➔
Due to heavy traffic on the main site, we run temporary sites.

Notice of Ransomware server recovery process.

We are responding to inquiries, including site restoration.

We apologize for the inconvenience.

153 Linux servers, 3400 websites encrypted. $1 million US paid
WANNACRY?

12/5/2017
We're currently experiencing significant problems with our IT and telephone network.

Please try to contact us via our social media channels or email for assistance.
300,000 victims in 150 countries
NotPetya / Petrwrap / Nyetya
Reckitt Benckiser - $117 million

Maersk - $200-$300 million

Fedex and TNT: $300 million

Merck: $310 million
Why so powerful?

WannaCry = Ransomware + Exploit + Worm
WannaCry

In Sandbox? (Anti-Sandbox technique)
Check domain (Kill Switch)

Windows SMB Exploit
MS17-010
WannaCry Defense

In Sandbox? (Anti-Sandbox technique)

NSA

SMB 445 TCP

Lateral Movement

SMB

445 TCP

Scans IP subnet

445 TCP

Scans external IPs

ETERNALBLUE

DOUBLEPULSAR

Encrypt

Windows SMB Exploit MS17-010

NGFW/IPS/AMP

Email Security

DNS Security

Endpoint security

Identity, Posture & SD-Segmentation

NGFW/IPS/AMP

Network Visibility, Behavior Analysis
Timeline of ‘WannaCry’ Ransomware Defense

**Microsoft Security Bulletin**
- March 14th, 2017
  - Patch Tuesday, Microsoft released a patch (MS17-010) to fix this new vulnerability.

**Cisco NGFW | Meraki MX**
- March 14th, 2017
  - The same day, Cisco NGFW released SniffTM signatures to detect WannaCry with high sensitivity for MS17-010.

**Shadow Brokers**
- April 14th, 2017
  - A group known as the “Shadow Brokers” released a list of vulnerabilities believed to have originated from the National Security Agency (NSA). They claim to have obtained the vulnerabilities from the former head of the NSA: The Deus Ex Machina.

**Cisco NGFW | Meraki MX**
- April 25th, 2017
  - Cisco published a list of vulnerabilities related to WannaCry, including MS17-010.

**Cisco TALOS**
- With more than 250 threat intelligence responders around the globe and a global network of intelligence and data sources, Cisco TALOS provides Cisco customers with up-to-date threat information.

**Cisco Umbrella**
- May 12th, 2017 | 10:50 UTC
  - Cisco Umbrella identified the attack type as “ransomware” and spread globally to thousands of companies.

**Cisco AMP**
- May 12th, 2017 | 6:33 UTC
  - AMP detected and blocked WannaCry infections, which led to widespread WannaCry activity.

**Cisco Umbrella**
- May 12th, 2017 | 2:43 UTC
  - Cisco Umbrella blocked WannaCry globally, helping to contain the spread and recovery of affected users.

**Cisco Investigate**
- May 12th, 2017 | 2:30 UTC
  - Cybersecurity analysts identified the new attack and coordinated a global response to contain and eradicate WannaCry.
Best Practices – Things I Can Do!

1. Do you have good disaster recovery (People/Process/Tools)? Train to implement it on a regular basis.
2. Do you have good offline back ups? Test them regularly.
3. Patch your systems, update your AV ASAP
4. Additional layer of defense such as DNS (Umbrella) and Anti-malware solution
5. End of life hardware / software?
6. Educate users on emails with links and attachments
Ransomware Defense for Dummies

www.cisco.com/go/ransomware
Ransomware Defense Prevention Validation

Tested against >20 REAL Ransomware Attack families to validate the solution
- Cisco Umbrella
- Cloud Email Security w/AMP
- AMP for Endpoints
- AMP ThreatGrid

Cloud and software solution that enables quick deployment and protection

www.cisco.com/go/safe
$10 Million in Cisco Global Cybersecurity Scholarships!

In our digital era, organizations are relying increasingly on cybersecurity to protect themselves, enable trust, move faster, add value, and grow. As the volume and sophistication of cyberattacks rises, organizations are experiencing a significant shortage of IT professionals with cybersecurity skills.

To help close this security skills gap, Cisco is introducing the Global Cybersecurity Scholarship program. Cisco will invest $10 million in this program to increase the pool of talent with critical cybersecurity proficiency. Cisco also has enhanced its Security certification portfolio with a new CCNA Cyber Ops certification.

Thank you very much for your interest in the Cisco Global Cybersecurity Scholarship program. We will reopen registration for the Cybersecurity Scholarship in the fall of 2017. Please fill out the form below if you are interested in applying for the scholarship program, and we will notify you of next steps when registration opens.
Cisco Networking Academy, a Cisco Corporate Social Responsibility program, is an IT skills and career building program available to learning institutions and individuals worldwide.
# The Networking Academy Learning Portfolio

## Current & Planned

**Exploratory**

- **Networking**
  - Introduction to Cybersecurity
  - Introduction to IoT
- **Security**
  - Introduction to Cybersecurity
- **IoT**
  - Introduction to IoT
- **OS & IT**
  - NDG Linux Unhatched
- **Programming**
  - NDG Linux Unhatched
- **Business**
  - Be Your Own Boss
- **Digital Literacy**
  - Get Connected

**Foundational**

- **Networking**
  - Networking Essentials
  - Mobility Fundamentals
- **Security**
  - Cybersecurity Essentials
  - IoT Security*
- **IoT**
  - IoT Fundamentals:
    - Connecting Things, Big Data & Analytics
    - Hackathon Playbook
- **OS & IT**
  - NDG Linux Essentials
  - IT Essentials
- **Programming**
  - CLA: Programming Essentials in C
  - CPA: Programming Essentials in C++
  - PCA: Programming Essentials in Python*
  - Emerging Tech Workshop: Collaboration / Spark API*
- **Business**
  - Entrepreneurship
- **Digital Literacy**
  - Get Connected

**Career-Ready**

- **Networking**
  - CCNA R&S: Introduction to Networks, R&S Essentials, Scaling Networks, Connecting Networks
  - CCNP R&S: Switch, Route, TShoot
  - Emerging Tech Workshop: Network Programmability*
- **Security**
  - CCNA Security
  - CCNA Cyber Ops*
- **IoT**
  - NDG Linux I
  - NDG Linux II
- **Programming**
  - CLP: Advanced Programming in C*
  - CPP: Advanced Programming in C++*

*S Available within 12 months

---

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential.
Specifically for Self-Paced Courses

Networking
• Packet Tracer 101
• Packet Tracer 101 Mobile
• Introduction to Packet Tracer

IoT
• Introduction to IoT
• Introduction to the Internet of Everything

Security
• Introduction to Cybersecurity
• Cybersecurity Essentials

Business Literacy
• Entrepreneurship

Digital Literacy
• Get Connected
To get this slide and more about NetAcad Program, pls leave your contact by scanning this QR code:
Garrick Ng - CTO: garng@cisco.com
Shania Ting - Security Sales Manager: hoting@cisco.com
Tommy Mak - Security Consultant : tomak@cisco.com
Eric Tsoi - Security Consultant: eritsoi@cisco.com
Garrick Ng - CTO: garng@cisco.com
Shania Ting - Security Sales Manager: hoting@cisco.com
Tommy Mak - Security Consultant: tomak@cisco.com
Eric Tsoi – Security Consultant: eritsoi@cisco.com