EXTREME HACKING® NeXTGEN™
The Rules of Engagement Have Changed. Resecure Everything.™
SYSTEM
HACK SYSTEM

ROCHESTON® CERTIFIED CYBERSECURITY ENGINEER

Level 2

RCCE® Certification Program Guide

Introduction (RCCE®) - Advanced Program

A well-known cybersecurity adage goes like this; it's not a matter of if you are attacked, but when. A growing number of businesses are starting to discover how true this is.

Every time technology takes a step towards assisting humans, it poses a new kind of threat to privacy. The latest among them is IoT and Artificial Intelligence (AI). As AI and Machine Learning (ML) are data reliant, it is not tough to imagine the risks that sophisticated AI systems, present for privacy.

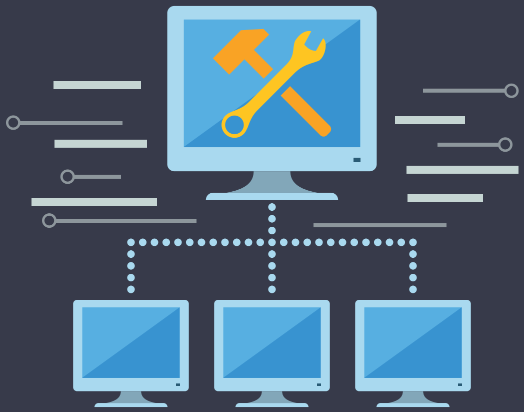
As AI becomes ubiquitous, attacks become more sophisticated. Baseline security is required to reduce the added collateral damages. Threats evolve on an everyday basis, and a lack of evolution in baseline security can be calamitous.

The Rocheston Certified Cybersecurity Engineer (RCCE) – Level 2 program **is targeted towards individuals who already have basic hacking skills.**

RCCE – Level 2 is the most advanced hacking course. Set to disrupt the market, it is cutting edge, and teaches advanced hacking and threat identification/detection concepts.

Benefits

Is our society well-equipped against threats? Can we control the Dark Web? Are we equipped to monitor and reverse engineer cyberattacks on trade secrets and info databases? If not a "Yes", we must prepare! An RCCE – Level 2 is the solution!



Training in neural networks: Neural networks are an inherent part of machine learning. It is important in altering detailed network info for black box attacks.

Nurture a qualified workforce: Job shortages are expected, as firms struggle to find quality employees. Four sectors with 11.7tn in debt are at risk from cyber-attacks. Also, a shortage of 3.5m cybersecurity professionals in the market is expected, by the year 2021.

Battling AI threats: AI speeds up polymorphic malware, with evolving code. Students learn defence/security controls against evolving exploits. AI-based security tech simplifies the protection process.

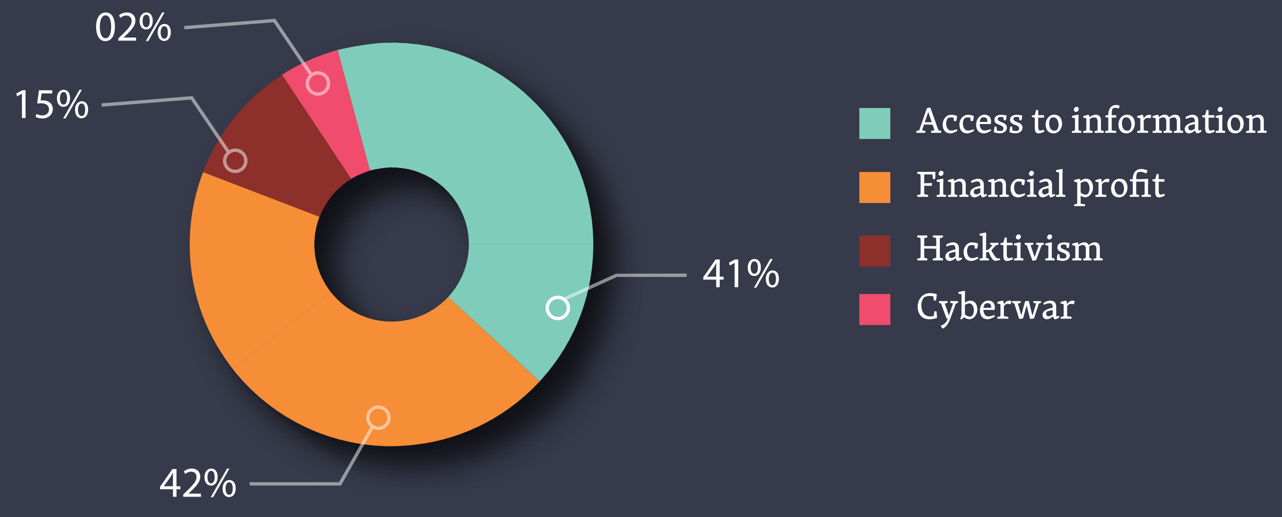
AI-based security tech in cybersecurity: AI-based security tech provides students awareness of deeper levels of security.

AI triumphs over human intelligence: SNAP_R sent 800 spear phishing tweets to more than 800 users, 6.75 tweets/min, it claimed 275 victims. Humans captured 49 individuals, tweeted 129 users at 1.075 tweets/min. In RCCE, students will gain insight into AI-tech.

Extreme Hacking® NeXTGEN™. The most advanced hacking course. Taken to the Extreme.

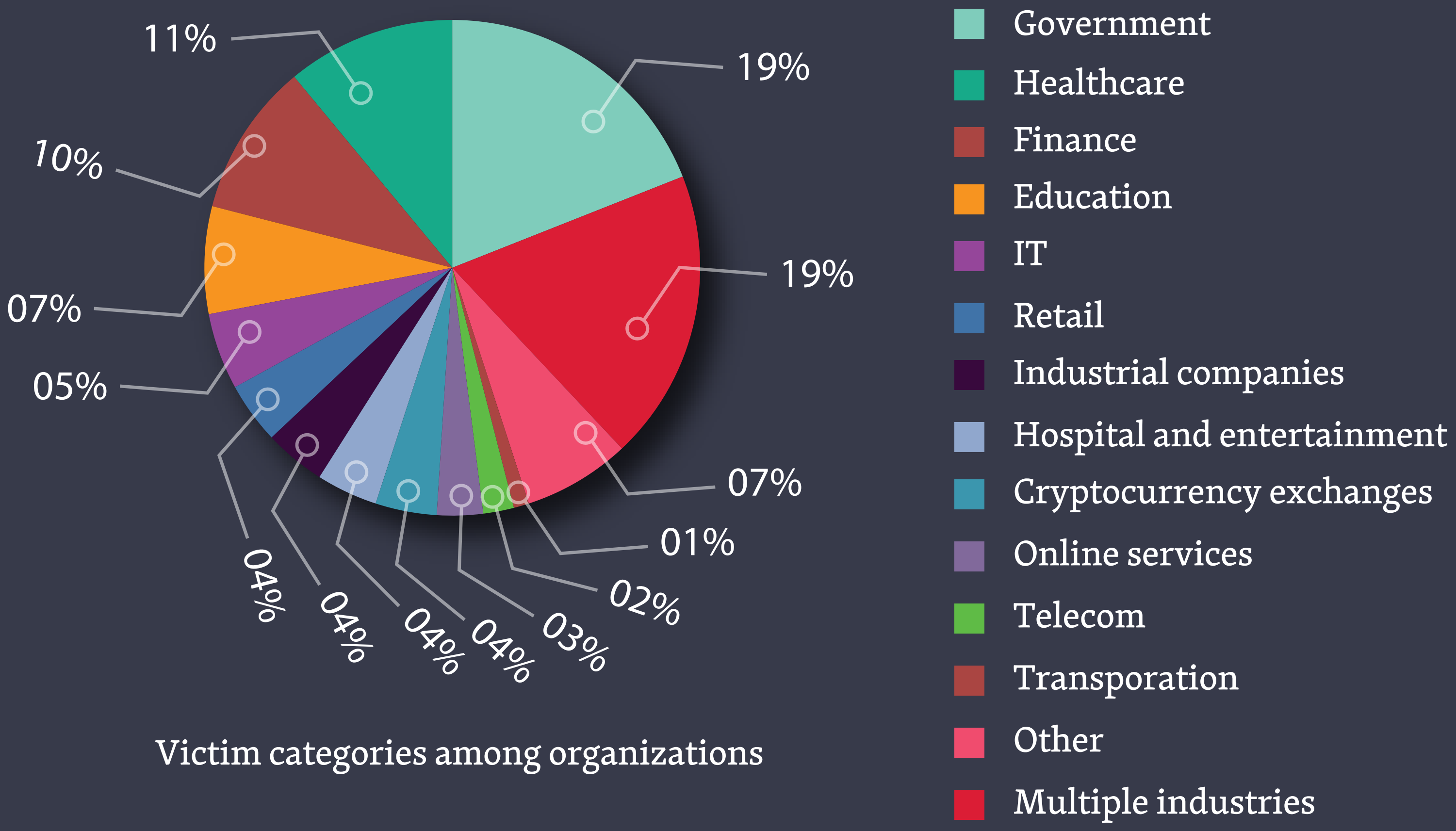
Cybersecurity - Facts and Figures

In 2018, a vast majority of cyberattacks had financial and data related motives. Targeted attacks witnessed an alarming increase, with progressive increases observed during each quarter.



Attacker's motives

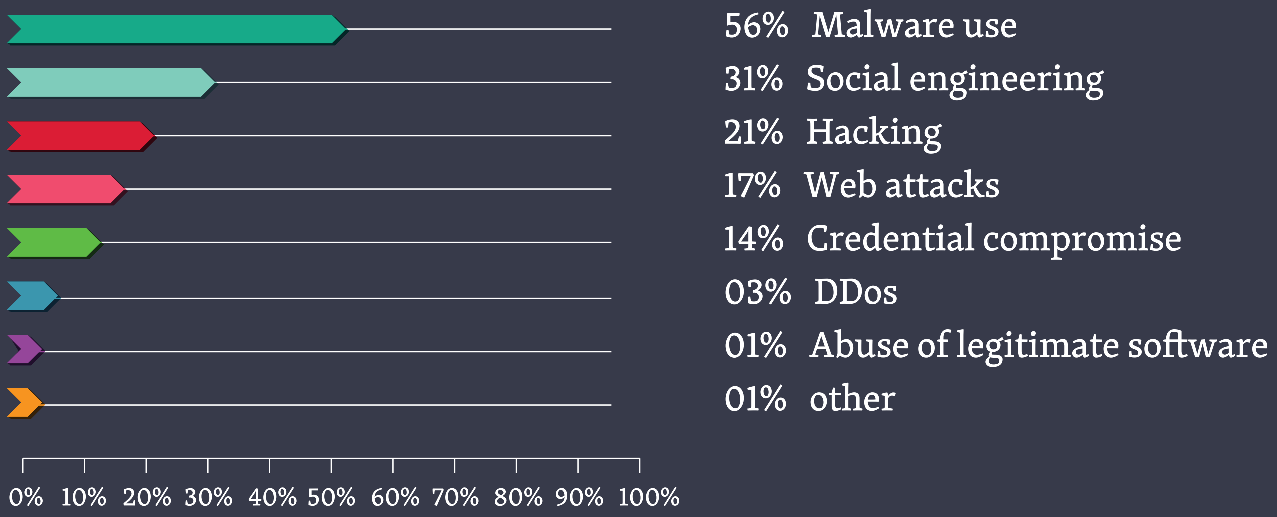
1/4th of attacks were against individuals. State run institutions were **victims in 19% of cases,** health and financial institutions in **11% and 10%**, respectively. Cyber attacks of a grander scale, targeted at more than one industry, have been placed in the 'multiple industries' category.



Victim categories among organizations

Unique incidents **increased by 27%** when contrasted with the previous year. A marked increase was observed during the time of the Winter Olympic Games and FIFA World Cup, when individual and organizational financial activities were frequent.

Attackers often targeted corporate infrastructure and websites. Attacks were observed to be layered, and more intricate than ever before. They often consisted of several phases. Social engineering was also a frequent fixture, with every third attack featuring it.



Attack methods

Victim - Profile

51% of cases had theft of confidential data as a primary objective. State-run websites are targeted to grab public attention. Hacktivist attacks accounted for nearly 1/4th of all events.

The data of **6 million people** was compromised in 2018, consisting of personal data and healthcare related information. Ransomware was a common occurrence in healthcare, as persistent operations are key. Hancock Regional Hospital in the U.S.A. paid **55k US$ in ransom** to obtain control over their own systems.

65% of events against financial institutions were profit-driven. In educational institutions, the damages amounted to around **2 million US$ in 2018. 1/6th of attacks** were ransomware related.

E-commerce stores and portals were targeted, with 70% of attacks aimed at customer data theft, wherein five million cards were compromised.

VPNfilter **malware compromised >500,000 routers**. In another incident, hackers stole private data from 383,000 guests who were at the Marriott Hotel chain. **The entity's stocks fell by 6% in a single day.**

At the individual level, **social engineering accounted for 43% of incidents**. Malware made up 73% of incidents. Spyware infection accounted for 21% of incidents. Mining witnessed a decrease in popularity and it's share among **malware attacks against individuals decreased from 27% to 13%.**

13 15

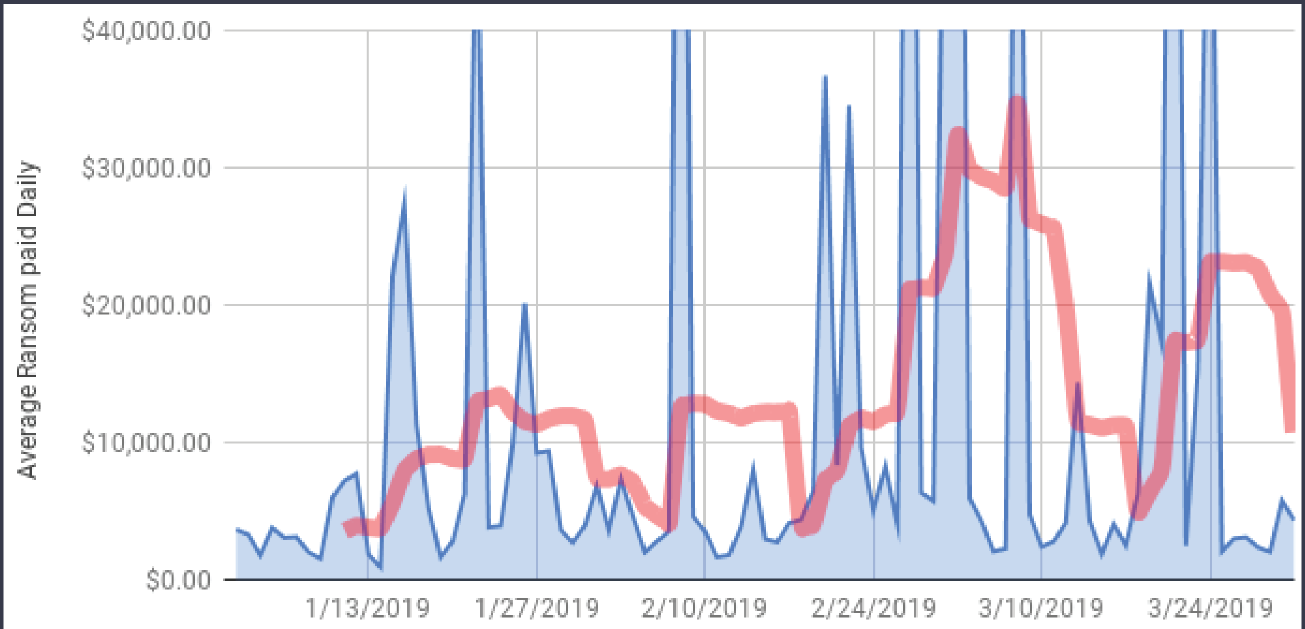
Ransomware amounts up by 90% in Q1 as Ryuk wreaks havoc

Coveware's Q1 Ransomware Marketplace report aggregates anonymized ransomware data from cases handled and resolved by Coveware's Incident Response Team. Unlike surveys, which rely on sentiment, this report is created solely from a standardized set of data collected from every case. By aggregating and sharing this data we believe large and small enterprises can better protect themselves from the persistent and ever-evolving ransomware threat.

How Much Does a Ransomware Attack Cost?

The total cost of a ransomware attack can be divided into two main portions. First, the recovery cost. These expenses cover forensic reviews and assist in rebuilding servers and to workstations If a ransom is paid, then that is also a recovery expense. The second, and often more expensive cost of a ransomware attack is the total cost of downtime. Downtime costs are typically 5-10x the actual ransom amount and are measured in terms of lost productivity (slack labor and lost revenue opportunities).

Ransomware Amount Paid Daily during Q1



In **Q1 of 2019, the average ransom increased by 89% to $12,762,** as compared to **$6,733 in Q4 of 2018.** This increase reflects increased infection by more expensive types of ransomware such as Ryuk, Bitpaymer, and Iencrypt. These are predominantly used in bespoke targeted attacks on larger enterprises.

In **Q1 of 2019, the average ransom increased by 89% to $12,762,** as compared to **$6,733 in Q4 of 2018.** The ransom increase reflects increased infections of more expensive types of ransomware such as Ryuk, Bitpaymer, and Iencrypt. These types of ransomware are predominantly used in bespoke targeted attacks on larger enterprise targets.

7.3 days

Average number of days a ransomware incident lasts

$ 64, 645

Average cost of ransomware incident related downtime

In Q1 of 2019, the average downtime increased to 7.3 days, from 6.2 days in Q4 of 2018. This increase was driven by the higher prevalence of ransomware that is difficult to decrypt, such as Ryuk. Similarly, the majority of the Hermes variants are also time-consuming to decrypt with relatively high data loss rates (10-20%) compared to other types of ransomware. Downtime increased by 47% over Q4. This increase was due to the frequency of attacks where backup systems were wiped or encrypted as part of the attack, an indicator of their increasingly bespoke nature.

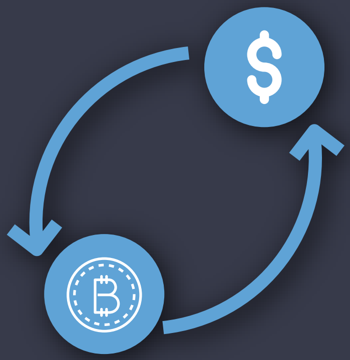
How Much Does Ransomware-related Downtime Cost?

In **Q1, estimated downtime costs per ransomware attack per company averaged $65,645.** The downtime costs become particularly acute for companies that lack cyber insurance and/or business interruption insurance. Downtime costs are estimated based on the geography and industry of the victim (to estimate labor costs), to estimate downtime costs per hour. Actual downtime costs may vary significantly from our estimates.

How Much Data Is Recovered After Paying a Ransom?

When a ransomware victim is forced to pay a ransom there are two success metrics that determine the outcome. First, does the payment result in a working decryption tool being delivered? If the threat actor did not deliver, it is considered a default and will likely lead to a 0% data recovery rate. Second, if a working decryption tool is delivered, how effective is it in decrypting the data? Files and servers can be damaged during or after the encryption process and this can affect data recovery rates even when a decryptor tool is delivered.

How Often Is a Decryption Tool Delivered After Paying a Ransom?



96% Payment Success Rate

In **Q1 of 2019, 96% of companies that paid the ransom received a working decryption tool.** This was a 3% increase from the previous quarter. However, payment success rates varied depending upon the type of ransomware. For instance, the GandCrab TOR site remained very reliable and delivered a decryptor tool shortly after payment was executed. However, some variants of Dharma are much riskier depending on the variant and threat actor.

93% Recovered

7% Lost

In **Q1 2019, victims who paid for a decryptor recovered 93% of the encrypted data.** This statistic varied dramatically depending on the ransomware type. For example, Ryuk ransomware had a relatively low data recovery rate, at ~80%, while GandCrab was close to 100%. Data loss was due to an encryption process that damaged or wiped files, or due to inappropriate data modification to already encrypted files. Of course, sometimes the decryption tools are simply prone to error.

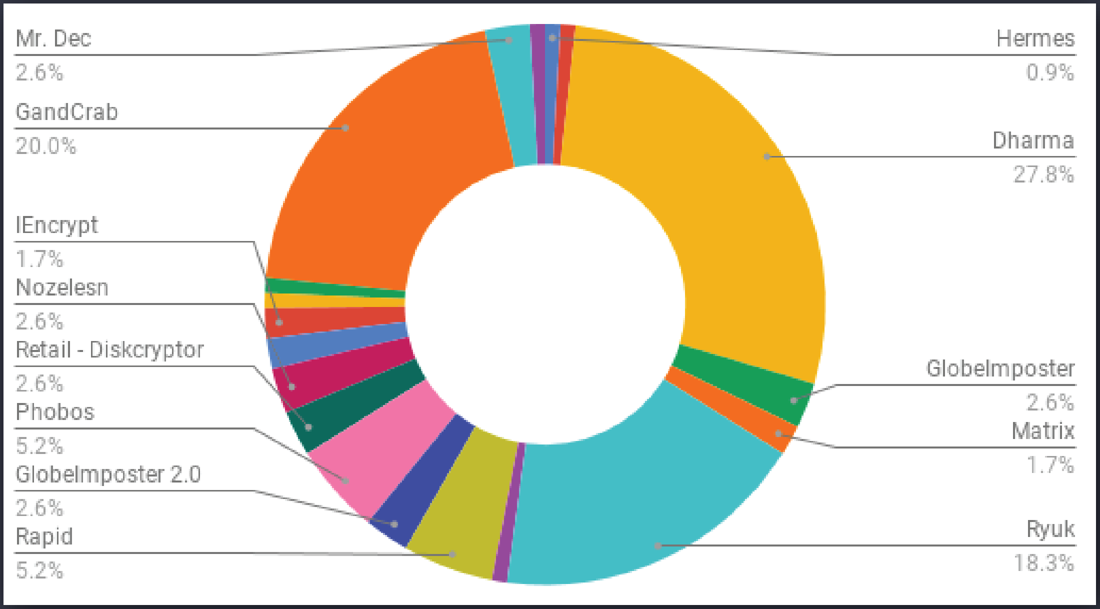
2% Privacy Coins like Dash are used after the fact, but not for the initial payment.

98% Bitcoin is still the most preferred cryptocurrency in ransomware.

Bitcoin continues to be the most common cryptocurrency for ransomware payments. Handling cryptocurrency continued to be a major source of friction for victims, and thus threat actors as well. It is unlikely that ransomware will move towards a different cryptocurrency as they are even more intricate to handle. This is highlighted by the ease with which threat actors are 'mixing' bitcoin or exchanging them for other privacy coins, like Dash or Monero. Gandcrab is the only common type of ransomware that accepts payment in either Dash or Bitcoin. Gandcrab victims who pay with Bitcoin are charged 10% more due to the 'mixing' costs incurred by the threat actors to anonymize the bitcoin after payment.

What Are the Most Common Types of Ransomware?

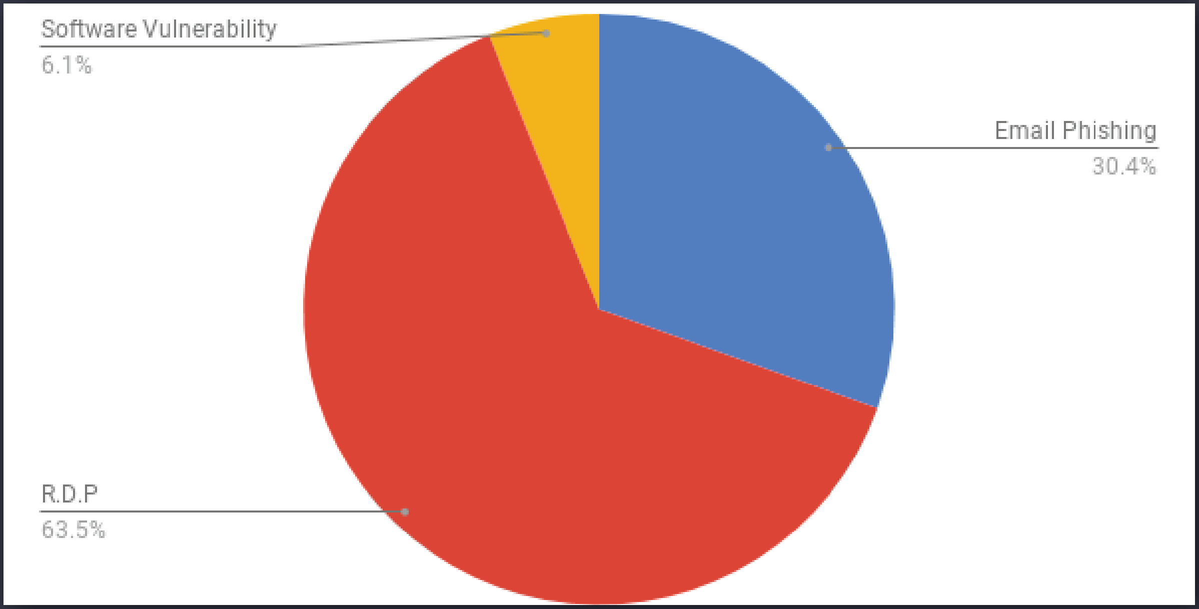
Ransomware Market Share by Type in Q1 2019



Dharma/Crysis continued to be the most prevalent ransomware in **Q1 of 2019, but Ryuk gained significant market share (especially considering it was not in the top 3 in Q4 of 2018).** The 3 most common types (Dharma, Ryuk, and GandCrab) are unique in their distribution methods, targets, and costs. Dharma continued to be operated by an increasing number of technically unsophisticated groups, which depressed data recovery rates despite rising ransom amounts. Ryuk continued to target larger enterprises and shock victims with egregious ransom demands. GandCrab continued to innovate distribution channels, with the developers bundling it with new and popular exploit kits.

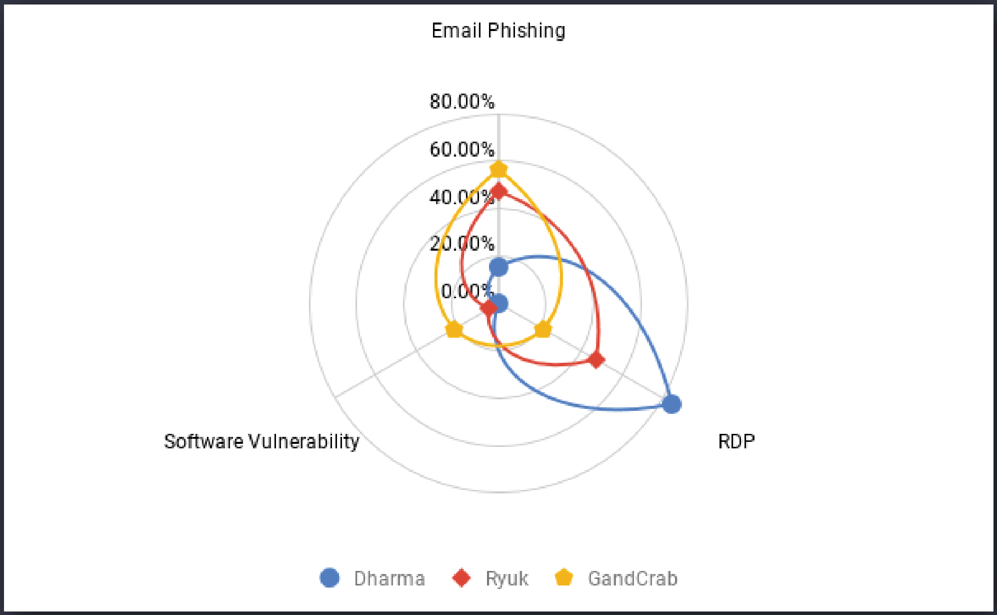
What Were the Most Commonly Identified Attack Vectors for Ransomware?

Common Attack Vectors used by Ransomware in Q1 2019



Prior to a ransomware infection, multiple attack vectors may be used to gain access and/or obtain control of a vulnerable system. Of those attack vectors, the most commonly identified continued to be Remote Desktop Protocol (RDP) based. However, email phishing was resurgent during Q1. We expect phishing-based attacks to increase in market share as social engineering techniques evolve and employee security awareness continues to be a hard problem to solve. Both RDP and phishing-based attacks have the primary goal of gaining elevated credentials. Once credentials are harvested the network can be surveilled, endpoint protection can be sidestepped, backups can be wiped/encrypted, and, finally, the primary servers are encrypted.

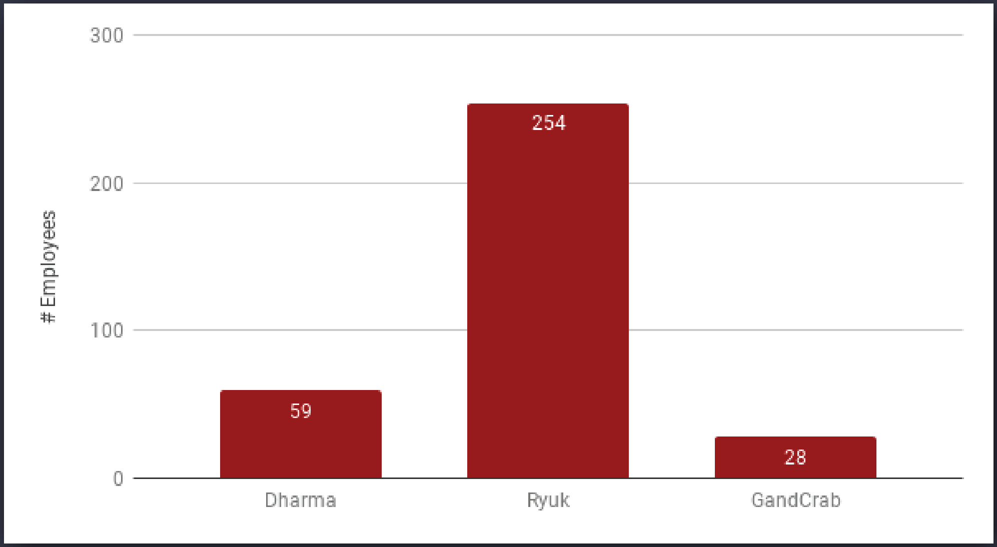
Comparing the Top Three Types of Ransomware by Attack Vectors



The differences in the attack vector are reflected in the sophistication and preferences of the threat actors distributing the ransomware. Dharma continued to exploit exposed RDP ports, which are commonly found in smaller businesses. Ryuk relied much more on targeted email phishing, which reflects the perpetrator's preference to go after larger organizations. These more targeted attacks require more social engineering via spear and whale phishing techniques. GandCrab is one of the only ransomware types to utilize software vulnerabilities, the **apex of which was the Connectwise/Kaseya exploit that impacted numerous managed service providers and their end clients during Q1 of 2019.**

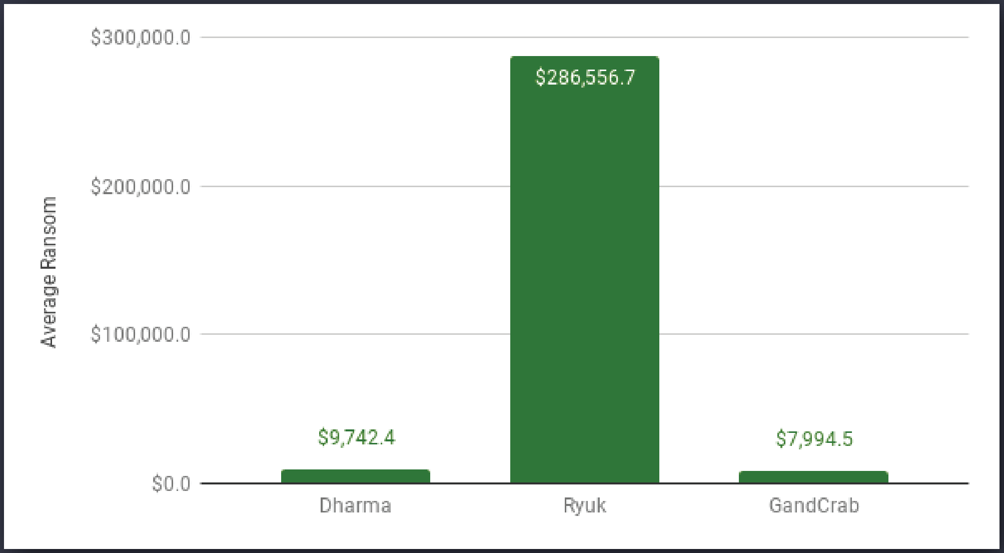
Comparing the Top Three Types of Ransomware by the Size of the Victim Company

Size of Victim Company by Number of Employees



The Q1 data paints a clear picture of Ryuk targeting larger organizations than Dharma and GandCrab. Ryuk was highly virulent in the midmarket and up during Q1, while Dharma variants continued to impact the midmarket and down. GandCrab's impact was more scattered wherein it tended to impact smaller companies and individual consumers.

Average Ransom Amount by Ransomware Type

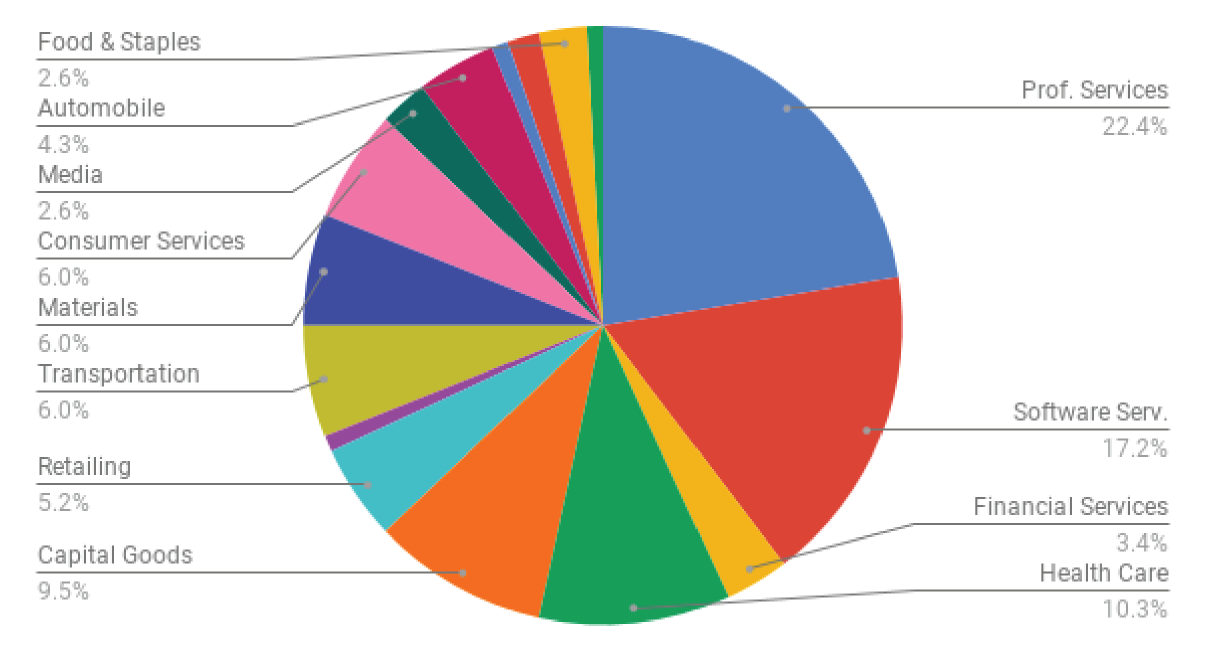


Ryuk continued to set records with ransom demands that are an order of magnitude larger than other types of ransomware. Ryuk targeted larger organizations that have the financial capacity to pay larger demands and a lower tolerance for downtime. However, there is strong resistance forming to the size of these demands and we expect them to level off as Ryuk seeks more targets down market.

What Industries are Commonly Targeted by Ransomware?

Professional services, such as law firms and CPA firms, are very often targeted by ransomware. Small healthcare organizations, such as local specialist offices, are often targeted as well. These firms tend to under-invest in IT security and backup policies, and have a low tolerance for data loss, which makes them vulnerable ransomware targets.

Common Industries Targeted by Ransomware in Q1 2019



What Was the Average Size of Companies Targeted by Ransomware?

In Q1 of 2019, the average company size increased to 114 employees, up from 71 in Q4. This increase reflected an increased prevalence of ransomware types that target midmarket and large enterprises, like Ryuk and LockerGoga. **The result of targeted phishing attacks, these infections were more common in Q1.**

114

Employees

Skills You Will Learn

The following are the skills that the student will pick up upon enrolling for the RCCE program:

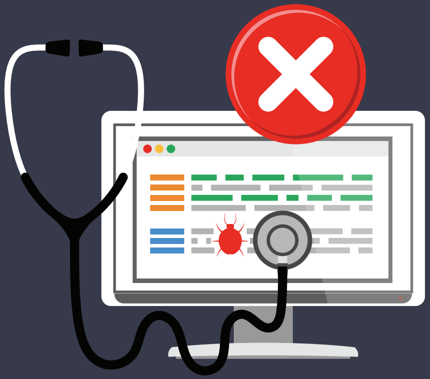
Understanding of advanced cybersecurity solutions: ComplementingRCCE foundation, advanced RCCE imparts specialist knowledge on persistent privacy problems, IoT vulnerabilities, penetration testing, insecure networks and other specialist concepts.

Penetration testing: Penetration tests attempt to utilize vulnerabilities to identify if unauthorized activity is possible. RCCEs will have extensive knowledge carrying out effective penetration tests.

TLS downgrade attacks: Downgrade attacksarea type of cryptographic attack on a device or communication protocol.It chooses an outdated mode of operation over a current one. (Eg., Cleartext, instead of encrypted connection) RCCEs are proficient in initiating and protecting devices/users from these attacks.

Communication encryption: Learn about mail authentication tokens, authorization, and implementation of private servers. Private servers are a sure-fire way of having completely encrypted communication.

Internet disruption testing: Learn about testing business infrastructure, and the state of the server if the web connection is terminated.



Remote access vulnerability testing: Protect yourself from remote exploits by testing for vulnerabilities within your existing devices and infrastructure.

Job Opportunities

- Intrusion Detection Specialist
- Computer Security Incident Responder
- Source Code Auditor
- Virus Technician
- Cyber Security Analyst
- Cyber Security Engineer
- Cyber Security Architect
- Cyber Security Administrator
- Security Software Developer
- Cryptographer
- Crypto Analyst
- Cyber Security Consultant
- Penetration Tester
- Information Security Manager

Who Can Take Up The Progrm

Individuals who wish to build a career across the following industries:

- Healthcare
- Smart Cities
- Industry 4.0
- Transportation
- Electronics
- Governance
- Automation
- Robotics
- Telecom
- Smart Appliances
- Department of Defense
- Finance

Engineers

Cybersecurity Specialists

Data & IT Professionals

Software Professionals

Eligibility

A Bachelor's degree with **one year of professional experience** or credential in computer science, engineering, mathematics, or other information technology related fields.

You will need basic hacking, networking, system administration, and Linux skills.

Note: If you don't have basic hacking skills you can attend Rocheston's Extreme Hacking Foundation Program (which is included in this course).

The Most Advanced Hacking Course In The World

Why RCCE Is DIfferent From Other Cybersecurity Courses ?

A cybersecurity engineer is aknight in shining armour, well-endowed to fight vices inthe ever-expanding cyber world. **An RCCE can fight government espionage, hacktivists, organized crime groups, external/internal data theft and so on.**

Our state-of-the-art RCCE program is one of the industry’s best, with its in-depth, unique, and cutting-edge content.

An **RCC Engineer has market presence and relevance, a key factor for success in today's constantly evolving professional landscape.**

What you will learn in the RCCE Advanced Program:

- Learn Advanced Attack Techniques.
- Become an expert in Advanced Spear Phishing Techniques
- Understand the nuances of Deep Network Insights for Deeper Analytics
- Master Advanced Blockchain Exploits and Cryptocurrency Mining Attacks
- Grasp the concepts of Deepfakes and Generating Automated Fake News
- Follow and assimilate Cognitive-Powered Security Intelligence Platform
- Develop expertise in Hacking Biometric Security, and Facial Recognition Systems
- Obtain knowledge in Attacking Hidden Endpoint Management Firewalls and IDS
- Learn interesting tools in Advanced Mobile Phone Hacking, Spying, GPS and Monitoring
- Comprehend hacking tools for Home Automation and IoT Gadgets

The Most Advanced Hacking Course In The World

Demand for RCCE Level 2 Program

IoT device usage and presence is expanding rapidly. Fifty billion connected devices are expected by 2025. IoT and AI only increase security vulnerabilities. Frameworks are expected to evolve with dependence on IoT tech. This expansion of IoT and machine learning necessitates a cutting edge course. This is where RCCE steps in.

Syllabus

Module 1: Sophisticated and Extremely Advanced Phishing Techniques Harvested by Chinese and Russian Hackers

1.1 Reconnaissance - System profiling and discovering client-side applications to target uses for advanced attacks

1.2 Advanced Attack Techniques - Host a web drive-by attack or transform an innocent file into a trojan horse with server-side dashboards.

1.2.1 Java Applet Attacks

1.2.2 Microsoft Office Documents

1.2.3 Microsoft Windows / Linux Applications

1.2.4 Website Clone Tool

1.2.5 Advanced Spear phishing techniques - Import a message and replace links and text to build a convincing phishing to take over networks.

1.2.6 Send a phishing email and track who clicks and download the payloads

1.2.7 Connect to a central hacking server to share data, communicate in real-time, and control systems compromised during the engagement.

1.2.8 Post Exploitation - execute PowerShell scripts, logs keystrokes, takes screenshots, downloads files, and spawns other payloads.

1.2.9 Covert Communication - Use HTTP, HTTPS, and DNS to egress a network. Use named pipes to control Beacons, peer-to-peer, over the SMB protocol.

Module 2: Network Insights for Deeper Analytics

Module 3: Read Privileged Kernel Memory and Leak Data to Escalate Privileges

Module 4: Advanced Blockchain Exploits and Cryptocurrency Mining Attacks

Module 5: Sophisticated Government use of Cyberweapon Attacks and How they work

Module 6: Principles of Quantum Entanglement to Secure Communication (Unhackable networks)

Module 7: Guidance For Cybersecurity Disclosure and Advanced Techniques for Cyber Bounty hunting

Module 8: Advanced Mobile Banking and ATM Trojans

Module 9: Quantum Computing and Cryptography

Module 10: Dark Web and How to Download Sophisticated Stealth Tools

Module 11: Advanced Cloud Security - Azure, AWS, Digital Ocean, Google VM.

Module 12: H2O Driverless AI, Amazon SageMaker, and Azure Machine Learning AutoML

Syllabus

Module 13: Deepfakes and Generating Automated Fake news

Module 14: Advanced Threat Modelling Attacks

Module 15: Cognitive-Powered Security Intelligence Platform

Module 16: Types of Cyberthreat Intelligence

Module 17: Advanced Ransomware and Cryptojacking Attacks

Module 18: Open Source Intelligence in Cybersecurity

Module 19: Attacking AI Chatbot and Voice Assistants - Siri, Google Home and Alexa

Module 20: DeepLocker: How AI Can Power a Stealthy New Breed of Malware

Module 21: Cybersecurity Insurance

Module 22: Advanced File System Protection With Cyber Deception

Module 23: Legal AI: How Machine Learning Is Aiding, Concerning Law Practitioners

Module 24: Advanced Threat Hunting Techniques

Module 25: Vulnerability Management Process Based on Weaponization and Asset Value

Module 26: Passwordless Authentication With FIDO

Module 27: Advanced PowerShell Attacks

Module 28: Next Generation of the Cyber Range Attacks

Module 29: Advanced Payment Gateway and Financial Cyberattacks

Module 30: Developing Immersive Cybersecurity Simulation

Module 31: Advanced DDOS Attacks Using IoT Botnets

Module 32: Attacking Hidden Endpoint Management Firewalls and IDS

Module 33: Advanced BGP Router Attacks

Module 34: Machine Learning with Automated Software Vulnerabilities

Module 35: Hacking Medical IoT Devices

Module 36: Hacking Biometric Security, and Facial Recognition Systems

Module 37: Threat Intelligence Models for Cyber Warfare

Module 38: Artificial Intelligence and Cyberwarfare

Module 39: Hacking Connected Cars

Module 40: Hacking Power Grids

Module 41: Advanced Mobile Phone Hacking, Spying, GPS and Monitoring

Module 42: Home Automation and IoT Gadgets

- Hacking Amazon Echo to control your house
- Hacking into smart door locks to unlock your doors
- Hacking smart security cameras to monitor you
- Hacking smart switches to control your devices

Syllabus

- Hacking smart bulbs/lights
- Hacking connected garage door opener
- Hacking smart thermostats
- Hacking connected window blinds/curtains
- Hacking connected home appliances
- Hacking smart Tv’s
- Hacking connected fridges
- Hacking smart doors with inbuilt cameras
- Hacking home monitoring systems
- Hacking home surround sound systems
- Hacking video calling bells
- Hacking baby monitors
- Hacking connected children’s toys

Vehicles

- Hacking GPS tracking sensors on vehicles
- Hacking into and controlling Autonomous, smart vehicles
- Hacking into ridesharing applications for call spoofing
- Hacking into drones

Healthcare/Fitness

- Hacking into blood pressure monitoring systems
- Hacking into patient monitoring systems
- Hacking into hospital databases
- Hacking into smart, wireless pill bottles used to track medication
- Hacking into wearable technology
- Hacking GPS chips in smart shoes

Smart Cities

- Hacking election voting machines
- Hacking into government satellite systems
- Hacking the power grids
- Hacking the city’s surveillance systems
- Hacking billboards that are connected to the cloud
- Hacking smart bicycles
- Hacking connected dustbins
- Hacking traffic lights
- Hacking the public transport system(trains/subway)

Cloud and Computing

- Hacking into cloud services to steal data
- Hacking quantum computers to break encryptions. Encryptions that take 38 years or more to crack can be cracked in 10 minutes
- Hacking into and stealing data from facial recognition cameras
- Hacking NFC passports

Manufacturing

- Hacking safety sensors to give false readings
- Hacking into smart machines to disrupt production
- Hacking into systems used to track logistics of companies
- Hacking the robots in factories
- Hacking RFID chips used for tracking of shipments

Module 43: How To Use Tensorflow

Module 44: Advanced EMP Cyberattacks

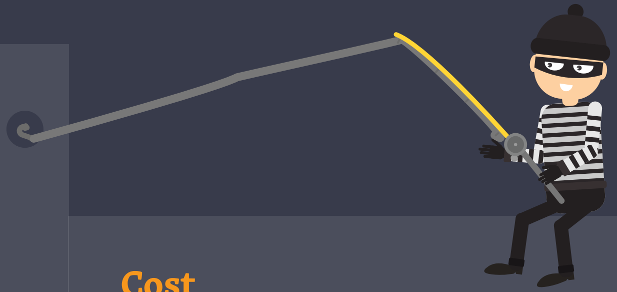
Module 45: Hacking heart devices, pacemakers, insertable cardiac

Module 46: Integrating IoT Security Into Vulnerability Management Program

Module 47: Containers & Cloud Native Security

Course Structure

What the course will consist of:



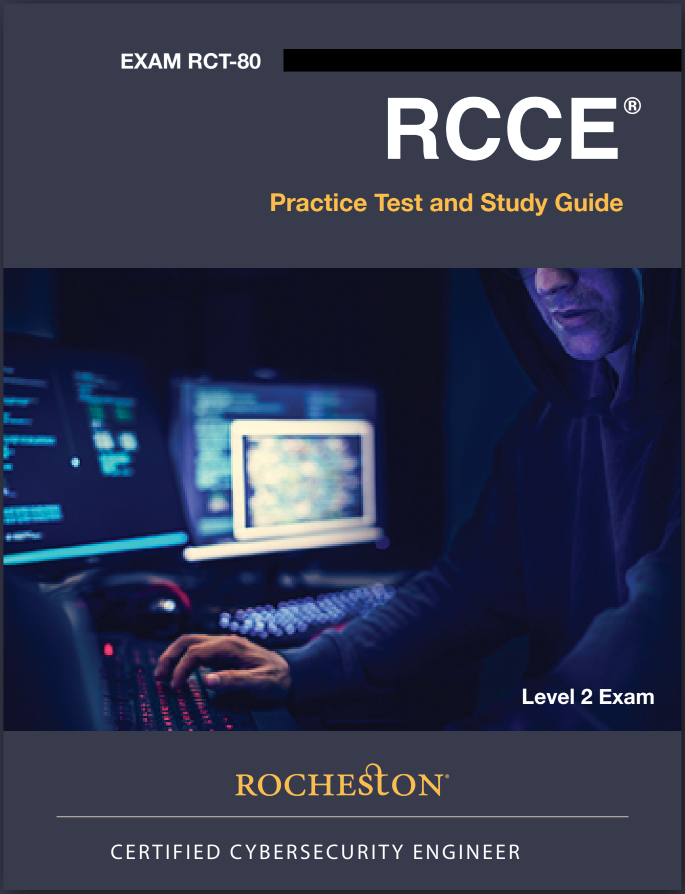
- Exam Code: RCT-80
- No. of Question: 90
- Passing score: 72%
- Exam is available at VUE and Cyberclass®
- The RCCE Level 2 exam will be conducted on the last day of the training
- The students will receive the RCCE Level 2 certification after passing this test
- The certification is valid for 2 years. You can renew at Accord portal

Cost

For pricing in your region, please contact the local distributor.

RCCE® Exam **Preparation Study Guide**

Students will receive **RCCE® Level 2** as part of the training kit. The study guide will prepare the students to pass the test. The guide comes with over **500 sample exam questions.**



EXAM RCT-80

RCCE®

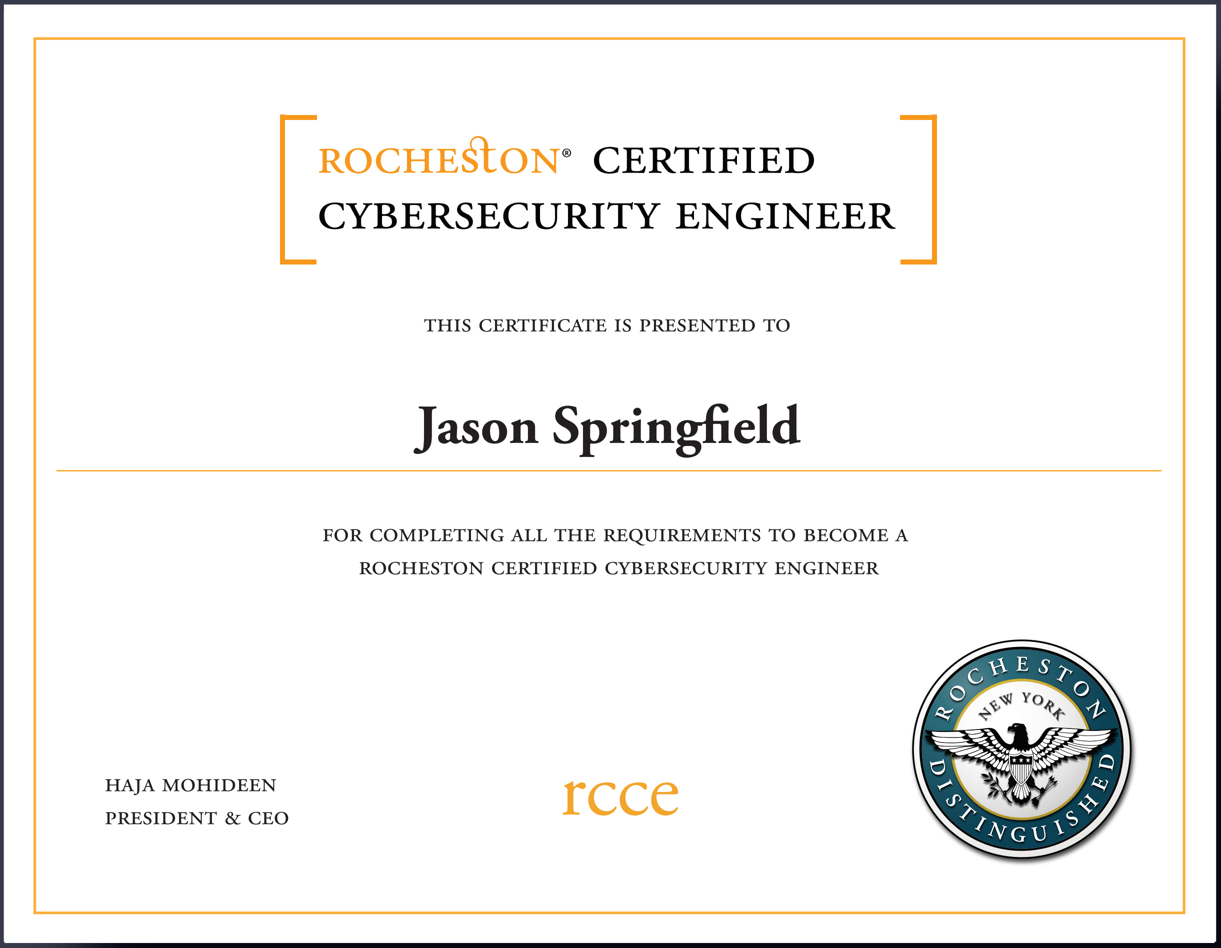
Practice Test and Study Guide

Level 2 Exam

ROCHESTON®

CERTIFIED CYBERSECURITY ENGINEER

RCCE Certificate



ROCHESTON® CERTIFIED CYBERSECURITY ENGINEER

THIS CERTIFICATE IS PRESENTED TO

Jason Springfield

FOR COMPLETING ALL THE REQUIREMENTS TO BECOME A
ROCHESTON CERTIFIED CYBERSECURITY ENGINEER

HAJA MOHIDEEN
PRESIDENT & CEO

rcce

ROCHESTON
NEW YORK
DISTINGUISHED

ROCHESTON® AUTHORIZED
TRAINING PARTNER

ROCHESTON® CERTIFIED CYBERSECURITY ENGINEER

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

ROCHESTON® CERTIFIED CYBERSECURITY ENGINEER

Certified by Rocheston®

The Rules of Engagement Have Changed. Resecure Everything.™

ROCHESTON®

BE EXCEPTIONAL