Network Security Strategies

Protect your network and enterprise against advanced cybersecurity attacks and threats

Aditya Mukherjee

Network Security Strategies

Protect your network and enterprise against advanced cybersecurity attacks and threats

Aditya Mukherjee

BIRMINGHAM - MUMBAI

Network Security Strategies

Commissioning Editor: Vijin Boricha
Acquisition Editor: Meeta Rajani
Content Development Editor: Carlton Borges/Alokita Amanna
Senior Editor: Rahul Dsouza
Technical Editor: Sarvesh Jaywant
Copy Editor: Safis Editing
Project Coordinator: Neil Dmello
Proofreader: Safis Editing
Indexer: Rekha Nair
Production Designer: Jyoti Chauhan

First published: October 2020

Production reference: 1061020

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham
B3 2PB, UK.

ISBN 978-1-78980-629-8

www.packt.com

Packt.com

Subscribe to our online digital library for full access to over 7,000 books and videos, as well as industry leading tools to help you plan your personal development and advance your career. For more information, please visit our website.

Why subscribe?

- Spend less time learning and more time coding with practical eBooks and Videos from over 4,000 industry professionals
- Improve your learning with Skill Plans built especially for you
- Get a free eBook or video every month
- Fully searchable for easy access to vital information
- Copy and paste, print, and bookmark content

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.packt.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at customercare@packtpub.com for more details.

At www.packt.com, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on Packt books and eBooks.

Contributors

About the author

Dr. Aditya Mukherjee is a cybersecurity veteran and an information security leader with over 14 years' experience in leadership roles across information security domains, including defense and law enforcement, financial services, health and public services, products, resources, communications, and media and technology. His core expertise includes cybersecurity strategy, strategic risk and cyber resilience assessment, tactical leadership and development, GRC and security auditing, security operations, architecture and engineering, threat management, security investigations, and forensics.

I would like to sincerely thank my mother and Shri. KumKum Roy Choudhury for all their support and encouragement in my life. I would also like to express my gratitude to those fine individuals and colleagues who have helped me tremendously in the formulation of this piece of literature by sharing their knowledge and constructive criticism – Sameer Bengeri, Pradipta Mukherjee, Abhinav Singh, and Deep Shankar Yadav. Dhanyavaadaha.

3
Mitigating the Top Network Threats of 2020

Today, due to the multi-dimensional and complex setup of networks, security threats are creeping up that result in cyber disruptions and cyber attacks. These threats are commonly seen in networks that don't keep up with the evolving threat landscape due to foundational security and newly identified vulnerabilities that are not managed appropriately. Threats come in multiple types and variations that can employ components such as links, malicious attachments, and application or network misconfigurations to penetrate the infrastructure. This can comprise anything from trojans, viruses, backdoors to insider threats, botnets to DDOS attacks, and many more. Hence, it is important to understand the prevalent network threats that organizations face and how to counter them.

Accordingly, in this chapter, we will take a look at the most commonly faced network threats and how to mitigate them effectively. You will learn some of the most important methods and tools that can be used to secure your network from these threats.

The following topics will be covered in this chapter:

- The top 10 network attacks and how to fix them
- Keeping up with network vulnerabilities
- Vulnerability management life cycle
- Network vulnerability assessment
- Exercising continuous monitoring

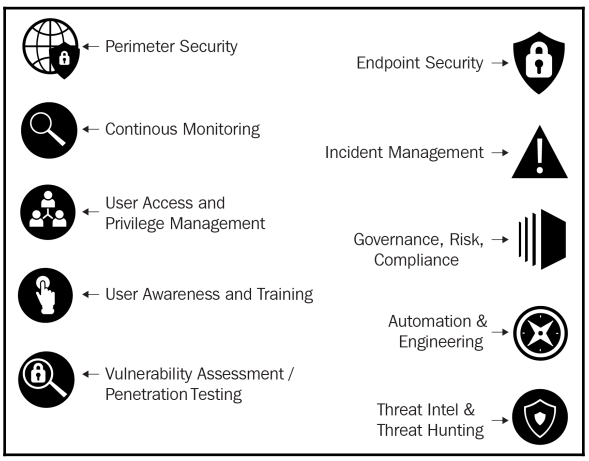
Technical requirements

Before we begin, familiarize yourself with the following services to get the most out of this chapter:

- Logz.io, Google's Project Shield
- Akamai, Radware, Cloudflare, and Oracle WAF Solutions
- SIEM Platforms such as Splunk, ELK, and AlienVault OSSIM
- Vulnerability scanning platforms such as OpenVAS, Nexpose, and Nessus
- Working knowledge of EDR, Firewall, and other security perimeter platforms

The top 10 network attacks and how to fix them

Threat actors aim at intruding on a system/network/infrastructure and gaining access to critical information and data that can be used for a variety of scenarios from ransomware to cyber espionage. It is, therefore, an issue of paramount importance to categorically identify, understand, and defend against such attacks proactively. The following screenshot shows some of the steps that can be taken to beef up your security:



But what are these attacks in the first place? In this first section of this chapter, we will look at the top 10 network attack vectors and how to mitigate them. We will deep dive into each of the attack vectors and understand the threat that they pose and their respective mitigations.

Phishing – the familiar foe

One of the most commonly encountered threat vectors to any organization is phishing. Phishing is a social engineered method that is used by malicious actors to gain access to sensitive data such as **Personally Identifiable Information** (**PII**), for example, credit card details, credentials such as usernames and passwords, and more. It is a dangerous threat that gives hackers access to information that they can leverage for malicious intent. Phishing is most commonly propagated via an email that showcases an appealing scheme or an urgent matter demanding privileged information, made to look legitimate and therefore raising no concerns or doubt in the recipient(s).

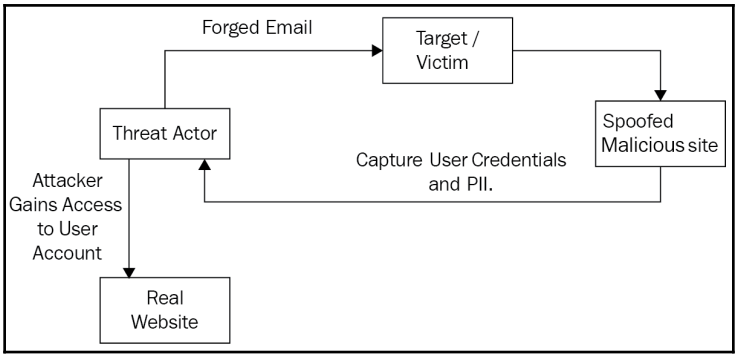
A well-crafted phishing email spoofs its point of origination to an authorized domain or a relatable identity to establish trust with the recipient. Going a step further, it may also mimic the format of the email. It may then ask the user to open a malicious attachment in an attempt to compromise the system by downloading a malicious payload or clicking on a link to capture PII, credentials, and so on.

Such threats may go unnoticed or take time before detection until the attacker moves to the later stages of the cyber kill chain such as **exploitation**, **installation**, **command and control**, and **actions on objectives**, which may raise flags in the environment's security mitigation. This is because if a user is unable to identify a phishing email or the malicious link or the downloaded payload is not detected in the early stages, then the attacker can lay dormant in the environment and wait for a favorable opportunity to execute the attack without being detected. To make things worse, attackers are now actively using a technique known as **Living off the Land** (**LotL**).

This is a technique where attackers make use of trusted off-the-shelf and/or pre-installed system tools and applications to carry out malicious operations without raising any red flags. Authorized tools in the environment are often used for malicious activity and exploitation by threat actors. These include the following:

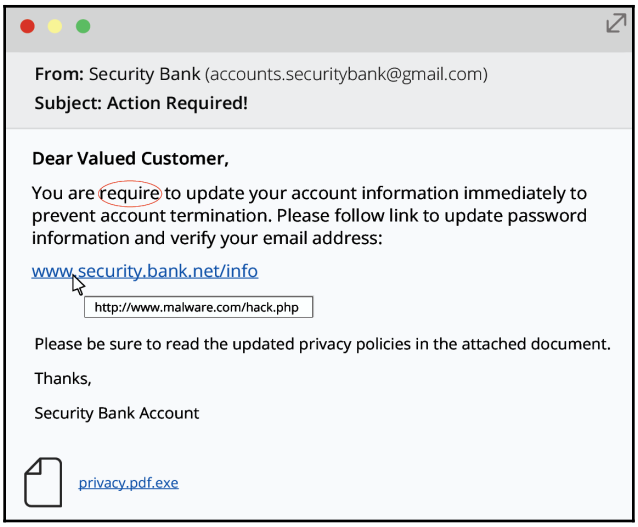
- PowerShell scripts
- VB scripts
- WMI
- Mimikatz
- PsExec

The following diagram shows a phishing campaign from the starting phase to the final stage, where the phishing email (spoofed) is made to look like it comes from a financial organisation. Once received, it requests the user credentials, which are then used by the attacker to cash out the account:



In real-world scenarios and threat campaigns, phishing comes in different types and forms as deployment by the cybercriminal depends on the target profile. Some of the prominent ones are discussed next:

- **Email phishing**: These are generally scam emails with malicious links and attachments forged by cybercriminals and made to appear as if they come from a reputable source. They are also made to impersonate trusted contacts, where once the links are engaged, malicious malware is downloaded automatically or the user is redirected to a phishing website to harvest credentials. The following screenshot shows an example of what a phishing email looks like:



- **Domain spoofing:** Hackers leverage their capacity to purchase identical domains (also known as *typosquatting*) to those of reputable websites. If a domain sounds/looks familiar to a well-known website, the attacker can use this to impersonate a legitimate domain and start sending phishing/scam messages through it. It leads to loss of confidential information and financial loss if a customer is directed to such a site where their information is captured. Major organizations such as LinkedIn and Google are often targeted, for example, with *linkdin.com* rather than *linkedin.com.*
- **Smishing:** This type of phishing is commonly known as SMS phishing and is a serious medium of sophisticated cyberattacks. Targeted victims are lured through SMS alerts, where the threat actor sends SMSes or IM messages that can redirect the user to a malicious site similar to what happens in a phishing email. Victims who are redirected to the fake site can end up providing the attacker with personal information/credentials.
- **Vishing:** Vishing is the equivalent of phishing when conducted over the phone. Threat actors often utilize this technique as a centerpiece to their social engineering campaign, where they may impersonate someone to extract personal or financial information from the target. In September 2019, a German organization reported a security incident where an AI-based voice-generating software was used to fake the voice of the organization's CEO, which resulted in a loss of $243,000.

- **Whaling:** This phishing attack targets a specific group of people in an organization, especially high-profile employees such as senior executive/leadership and hence the name "whales." The attack is launched at such targeted individuals as they hold critical/classified information. C-suite positions such as CEO, COO, and CFO are often targeted using this technique since they are easier targets due to lack of security training and so they are generally unfamiliar with covert intrusion techniques and therefore more prone to such attacks.

Using all of these techniques, attackers can harvest credentials of employees in the organization, harvest credentials of vendor accounts, initiate a foothold and perform lateral movement using malware that is dropped, initiate data exfiltration via mailbox rules (auto-forwarding), and other techniques.

Today, threat actors are utilizing innovative techniques to tempt recipients into getting trapped into interacting with phishing emails. One such example is the research by COFENSE on the recent Adwind Malware Campaign that is targeting the utility industry by attaching an image that looks like an attachment icon for a PFD but, in reality, is a front for an embedded URL that downloads a payload (a malicious `.jar` file) on the host system when the user clicks on it.

How to fix phishing threats

Both companies and individual users are equally important to counter the threat of phishing. We need to take serious measures to curb this widely prevalent threat with appropriate and cyclic security awareness training and mock phishing exercises. Apart from this, we should also focus on the implementation of a strong threat intelligence program to proactively block malicious content, links, email senders, and domains in the organization. We also need to deploy security applications such as EDR and web filters to detect and block any malicious events. As always, keeping all systems and applications updated with the most recent updates and security patches is a good practice against phishing payloads looking to exploit any known flaw or vulnerability.

Look out for these signs to detect a potential phishing attempt:

- The display name and the email address don't match.
- There is a sense of urgency.
- The email signature is not appropriate.

- It may have spelling errors, a generic salutation, or a sender asking for private information.
- It may have attachments or links that don't look right.

We can also deploy mechanisms such as spam filters, and monitor and block illicit downloads and program executions at endpoints. Employees and individuals are also supposed to be educated extensively on how to detect phishing activity through live exercises; they should also be made aware of security best practices such as not using corporate accounts and passwords in third-party websites and services. Data should be classified in the organization, and highly sensitive information should be encrypted and not shared with any non-corporate entity unless specific approvals are in place. Today, Microsoft Outlook comes with plugins and advanced options to make email communication secure. Features such as advanced attachment scanning and link checking ensure blocking of spam and content with lineage to malware such as external links with advanced detection techniques. Apart from this, it employs techniques such as email encryption, prevents forwarding, and has password-protected sharing links to ensure the secure exchange of information.

Organizations also deploy SIEM use cases for effective mitigation against phishing attacks, leveraging message trace/tracking logs, email gateway logs, and exchange audit logs. They can also utilize Azure AD or VPN logs and proxy or next-generation firewall logs. Proactively, every organization should employ strict security policies so that they can deal with violations appropriately. Every employee should be made to understand these policies, adhere to them, and commit to the organizational security program.

Password change policy should be enforced with periodic access reconciliation to prevent authorization creep, thereby maintaining concepts such as least privilege and separation of duties.

Rogue applications and fake security alerts – intimidation and imitation

This is one of the most common network threats encountered by any organization or individual user. Rogue applications, browser plugins, and advertisements on the internet take advantage of the fact that general users panic when they encounter a system virus notification. By exploiting this fear, scammers leverage on it to commit fraud on the internet. It is a trick that makes a user believe that there are viruses, malware, or trojans in their system. They may further display notifications to imitate that the system is not up to date with the latest security measure.

With the fear that a virus has been installed on the computer, scammers easily convince the user to take their offer of updating and installing security settings on the computer. This offer, which is mostly free, convinces the user easily and they are compelled to download the programs offered for the sake of security. They can also send programs to remove the alleged viruses. Nowadays, using this trick, they can easily ask a user to pay for a tool as well that will curb the viruses and fix the security update. This scam is a dangerous network threat that leads to fraud. When the user pays for the alleged tools, they are getting robbed without their knowledge.

In any case, the user accepts to download the programs provided, which inherently has malware, trojans, and backdoors embedded in the application, which is installed in the system automatically and opens the door to system compromise ranging from loss of confidentiality to integrity to availability. The installed malware gives hackers full access to confidential information and sensitive data. In this way, passwords, personal credentials, and other confidential information are hacked without the knowledge of the user. Important information could also be deleted from the computer system or the whole program could be broken down. Rogue applications, browser plugins, and advertisements are therefore a dangerous network threat that should be curbed with absoluteness.

How to fix rogue applications and software threats

Understand that not every warning sent to your computer or encountered online is genuine. Some are rogue and their aim to kickstart or undertake fraudulent schemes. You should not believe information from third-party sites and applications that claim some viruses or programs are harmful to your computer. This information should generally only be taken into consideration when received from your EDR or antivirus application. Such rogue information only pretends to detect non-genuine software and offer to remove them at a fee. This is a scam and the following screenshot shows how such a scam can appear on your system or mobile device:

To avoid such potential of fake updates, it is advised to configure the firewall and proxy to block traffic from low or bad reputation sites. A proficient EDR solution or antivirus application should also be in place at every endpoint with rules configured to block the installation of any unauthorized application on the system. Additionally, keep these mitigations fine-tuned and updated with the latest patches to provide better coverage against new threat vectors. Education is also critical in this aspect and you can be coached not to click on suspicious links.

Insider threats – the enemy inside the gates

This is one of the most obnoxious network threats faced by organizations and companies. It happens when an individual or group of individuals who are either inside the organization or close to the organization (such as contract employees or third-party vendors) having partial or full access to authorized information about the company use their privileges and authorization for malicious intent or to cause harm to the organization. This may vary from attempts to conduct financial fraud to the exfiltration of critical and confidential information.

According to a survey conducted by Accenture and HfS Research, 69% of respondents say their organizations have experienced an attempted or successful threat or corruption of data by insiders in the last 12 months. Read more at `https://newsroom.accenture.com/news/new-report-finds-insider-corporate-data-theft-and-malware-infections-among-biggest-threat-to-digital-business-in-2016.htm`.

These individuals can use this sensitive information deliberately or non-deliberately, negatively affecting the critical systems and data of the organization. It mostly happens when the employees of a certain organization are careless and refuse to comply with the rules, regulations, and policies of the company. They, therefore, use this information to cause insider threats to the company. This type of threat can go to the extent of insiders contacting customers through phishing emails and robbing them. Third-party vendors are also as a result of insider threats. Some of the insiders gain access to information that is very sensitive to the organization and they abuse it by committing threats.

> *"Since detecting insider threats by employees and trusted third parties is the ultimate game of cat and mouse, many leading-edge security organizations are using machine learning to compare the behavior of all users against established baselines of "normal" activity. This allows them to identify anomalous events and spot outliers so they can remediate threats early on."*
>
> *- Gurucul Chief Operating Officer Craig Cooper*

According to IBM's research in the 2016 Cyber Security Intelligence Index, there are two major types of insider threats—malicious and inadvertent. The following table summarizes the two insider threats (malicious and inadvertent) and compares them with external threat actors:

Malicious	Inadvertent	External threat actors
Common goals:	**Common situations:**	**Common scenarios:**
• Sabotage • **Intellectual property** (**IP**) theft • Espionage • Fraud (financial gain)	• Human error • Bad judgment • Phishing • Malware • Unintentional aiding and abetting • Stolen credentials • Convenience	• An external threat actor in the environment goes undetected and stays dormant or uses the LotL technique passively.

In most cases, after gaining access to sensitive data or resources, malicious activity protocols follow, intending to harm the organization. The insiders could be a disgruntled employee performing such actions out of vengeance or in an attempt to exploit their position for personal gains or they could also have been hired by a competitor of the organization to initiate cyber espionage. They abuse the trust and access bestowed upon them by the organization to execute acts such as stealing or selling confidential data or exploiting by tampering or deleting classified data that is crucial to the organization.

In severe cases, there have been reports of business operation disruptions due to such insider threat activity. It is, therefore, a very significant threat to the organization that can be monitored, detected, prevented, and mitigated at the network level by leveraging security principals and best practices.

Former employees, business associates, and contractors of an organization who have access to classified information about the organization are potential threats, especially if they left the organization on hostile terms. One such example is that of Brittany Kaiser from Cambridge Analytica, who had access to the company calendar, contacts, and documents even after parting ways with the organization, which led to the devastating disclosures on the inner workings of the organization (as seen in the Netflix documentary, *The Great Hack*).

How to fix insider threats

As discussed earlier, insider threats make up one of the critical network threats that an organization can experience. Following are some solutions that present mitigations in the prevention of possibilities of experiencing insider threats in an organization.

In a company, access to information by employees should be limited only to the specific areas that they require to get their jobs done, that is, there should be an implementation of security policies, such as information should be available and accessible only based on a *need to know* basis. Data classification, separation of duties, and least privileges are a must. The risk to the company with regards to insider threats depends on how many employees have access to critical resources and sensitive information.

Data classification is a very important aspect that is often overlooked by organizations. Here are a few steps you can take to effectively classify data:

- Ensure that you discover and understand sensitive data.
- Define data classification levels.
- Reduce the sensitive data footprint.
- Enforce and monitor data security policies.
- Have a data security and insider threat program.
- Cultivate a culture of data awareness (shared responsibility).
- Conduct a classification of all systems and processes in the organization.

Former employees should not hold such information and should be made to sign policy agreements when leaving to prevent them from leaking confidentiality and damaging the integrity of the business operations. Company resources such as laptops and handheld devices should be taken into custody. Access to company resources and accounts should be frozen. All credentials and access should be changed or terminated when leaving the organization. In general, the number of employees holding company information is proportional to the amount of risk and threat they get exposed to.

Different types of insider controls from a technology perspective include the following:

- Monitor system and network activity.
- Monitor data exfiltration attempts.
- Establish normal user behavior patterns and set alerts for anomalies.
- Monitor physical access to restricted areas and the printing of documents.

Employee monitoring software should be installed to minimize the risk of malicious activity that may lead to a breach of data. This also helps to secure intellectual property from theft through the detection of insiders who are malicious, careless, and disgruntled. With this kind of monitoring, it becomes easy to view the kind of information that is relayed from one employee to the other and its authenticity. This, therefore, reduces the risk of insider threats because the employees are made aware of the existence of such software programs.

Apart from this, a few other methods that can be employed include the following:

- Utilization of network monitoring
- Access control management
- **User and Entity Behavior Analytics** (**UEBA**)
- **Data-Centric Audit and Protection** (**DCAP**)
- Integration of SIEM to for greater visibility, and identifying anomalous behavior
- Putting prioritized monitoring around crown jewels and high-value targets
- Development of an insider threat program and employee security training

That's all about insider threats. Now, let's move on to our next attack vector—viruses and worms.

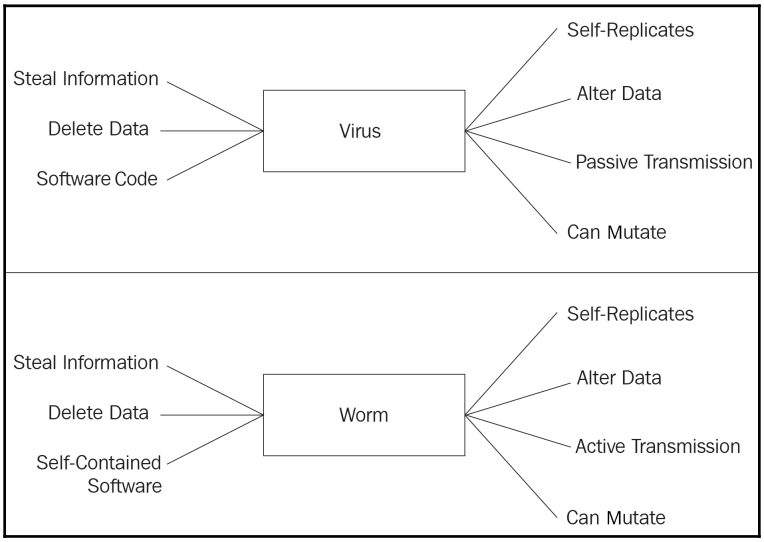
Viruses and worms – a prevailing peril

As far as network threats are concerned, viruses and worms have always been a major concern. These viruses and worms are dangerous because they replicate themselves easily into a computer system and corrupt files and folders and adversely manipulate the performance of the system. Worms tend to replicate themselves through the network by way of attacking other host systems in the network and self-replicating. They may cause a variety of symptoms on the affected system such as a system crash, abnormal application or program behavior, abnormal web browser activity, missing or modified files, and the creation of unknown application icons and processes, among others.

The infamous WannaCry ransomware attack of 2017 utilized a network worm for transportation mechanism, which proved effective for automatically spreading through the environment and executing a copy of itself.

Hence, as evident, if the network is not adequately protected, a virus or a worm can exploit vulnerabilities in the environment and spread quickly from system to system. When networks and systems of an organization are infected with such worms, the danger of collapse is almost certain. They may corrupt the business operation or lead to loss of integrity for the organization.

The following diagram shows how both worms and viruses work differently when they attack a network:



There are a variety of different types of computer viruses and worms that are widely used by threat actors to target organizations, some of which are discussed here:

- **Resident virus**: Resident viruses, for example, Meve, Randex, and CMJ, are found in RAM. They mainly corrupt programs and files and interfere with the normal system operations of a computer.
- **Stealth**: Viruses may appear like real programs by accepting operating system requests but they are not genuine. It is not easily detected by an antivirus. A sparse infector virus is another one that strategically avoids detection. They infect occasionally and may only affect a program on its ninth or tenth execution stage, hence minimizing the rate at which it can be detected.
- **Internet worms**: This malicious software simply appears like an autonomous program. A device that is infected is used to surf the internet looking for other vulnerable devices. The process of exploitation begins as soon as a vulnerable machine on the internet is detected. The most vulnerable and highly exploited systems are those without recent updates for security patches.
- **Spacefiller virus**: The spacefiller virus is also referred to as the "cavity" virus and it mainly affects the space between code blocks to execute malicious commands without theoretically changing the behavior of the affected program. These viruses attach themselves using a stealth technique and can easily affect the start of a program, and users cannot easily detect an increase in the file codes.
- **Macro virus:** The macro virus is another variant that targets software and applications that have macros. They affect the performance of the software and the program through a series of operations. These operations range from tampering with data, redirection, and deleting data.

Apart from these, there are a variety of different classifications of viruses and worms based on the action on an objective such as the Multipartite virus, Browser Hijacker, and the Overwrite virus, to name a few. Similarly, worms can be categorized into different types based on their activities such as email worms, instant message worms, and file-sharing worms, among others.

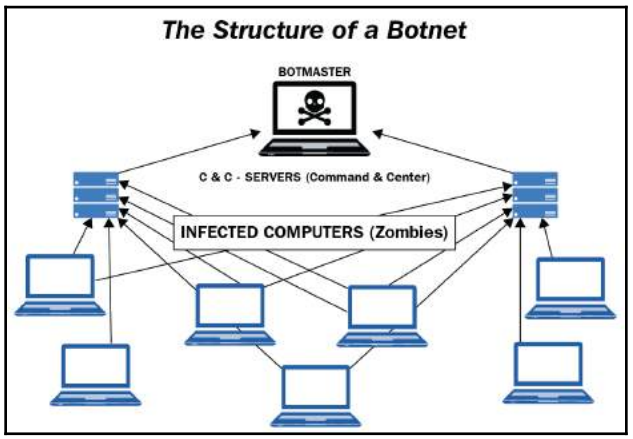
How to fix viruses and worms threats

Organizations should focus on enabling its employees to be vigilant by providing cyclic security awareness training for employees and oversee adherence to security hygiene to avoid downloading third-party applications, clicking and opening random links from the internet, and downloading attachments from unknown email senders. Such attachments are sent by threat actors with malicious intent to automatically download malware and subsequently compromise the system. This is important because, when the links are avoided, the malware cannot be downloaded and therefore hackers cannot have access to the network or systems of the organization. They should also be educated to avoid downloading software that appears free from websites they do not trust. They should also take extra care when dealing with P2P files and their sharing services. Unfamiliar vendors and untrusted websites and particularly clicking their ads is something they should be warned against.

Companies should be swift in the installation of antivirus throughout the organization endpoints and ensure that they are running the most recent version to reduce the risk of being impacted by a new strain of virus or worm. Additionally, ensure that all operating systems and installed applications are updated to the latest security fix or patch to ensure the best security posture against evolving threats that look to exploit known vulnerabilities and application flaws.

Botnets – an adversarial army at disposal

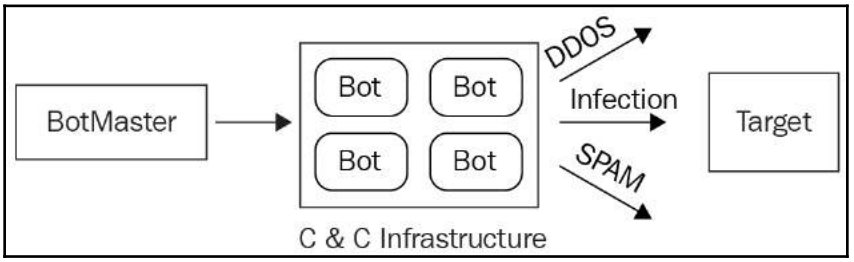
Botnets are a group of interconnected internet devices controlled by malicious attackers for a multitude of threat vectors that can be executed at the will of the attacker. This structure of a botnet can be seen in the following diagram:



Traditionally, botnets were used for DDoS attacks but with time, they have been used for crypto-mining, data extraction, email spam, click frauds, supporting C2C infrastructure, and so on.

Botnets pose a very serious network security threat as they are engineered by cybercriminals to infect as many devices as possible across the internet to attain their goal. Such botnets are inclusive of PCs, servers, smartphones, IP cameras, and other IoT devices that are connected over the internet and are controlled by the botmaster using a command and control application. This enables them to execute and perform automated tasks without the knowledge of the admin/user and remain undetected in the environment.

The following diagram shows how a botnet is launched to an operation:



There are several different types of botnets and each of them is designed by a botmaster to exploit system resources to commit cybercrime-related activities. Some notable types of botnets and the threats to which they expose network systems are outlined here:

- **DroidDream**: This is a variant of a botnet that silently installs malicious applications and malware on Android mobiles. Its widespread was attributed to the fact that it was available on the official Android Market in early March of 2011 before it was removed. Mobiles and other portable handheld Android devices were identified as the key targets for this botnet. The botnet is known to initiate a silent installation post through which it attempts to gain root privileges and steal data such as IMEI, IMSI, country, device model, and SDK version, and forward it to its command and control server. It is also known to have broken out of typical sandboxes that most apps reside in, to potentially gain control over the entire device and its data. Once the device is compromised, it can also download additional malicious apps on the device without any interaction from the user.
- **Tigerbot**: The main objective of this botnet is to collect hidden information like SMSes. Unlike other botnets that are internet-connected, this one is fully controlled by SMS and not web technologies. It is sophisticated to a point that all voice communications can be recorded and sent to the botmaster. The second stage attack is usually blackmail.

- **Zeus**: This is one of the most malicious botnets ever designed. It has the capacity of affecting a wide range of operating systems such as Android, Windows mobile, and Blackberry through processes that are socially engineered. Victims receive fake URLs that automatically download security certificates to the bots. This leads them to access bank details such as mobile transaction authentication numbers and messages sent by banks to their customers and authenticate illegal transactions.
- **Android.Bmaster**: It is commonly referred to as a Million Dollar Mobile Botnet. Trojan applications are activated by this botnet and millions of mobile devices are affected. A lot of money, in terms of millions of dollars, is lost by clients all over the world through premium messages forged by this botnet. It controls SMS applications for vulnerable users and makes them work to the botmaster's advantage.
- **Mirai botnet**: The Mirai botnet took advantage of insecure IoT devices by scanning for open Telnet ports over the entire internet in an attempt to log in with the default device credentials, amassing a huge botnet army at the disposal of the perpetrators. This was later used to launch huge DDoS attacks since September 2016 against various organizations.
- **Smominru botnet**: This botnet was attributed to hijacking more than half a million systems over the globe, intended to mine cryptocurrency and exfiltrate confidential data for selling on dark web forums. Most cryptojackers (unauthorized use of a system for mining cryptocurrency) follow a rather simple path of infiltrating a system by exploiting a known vulnerability or via brute-forcing default credentials. It has been known to utilize an array of techniques from using Mimikatz to EternalBlue exploits to propagate.

Recently, in 2019, another well-known application known as CamScanner was found to be suffering from malicious code due to the use of an advertising library that contained a malicious dropper component. Hence, you can understand that this is always a recurring threat that needs attention.

How to fix botnet threats

Any internet user is a potential botnet victim whether working with an organization or as an individual. The aforementioned threats that they cause can be prevented if serious measures are taken. One of the preventive measures is to keep the computer's operating system and applications up to date via means of installing security patches. Users should also be educated so as not to engage in reckless activities that can put their system at the risk that comes with bot infections. They are supposed to avoid opening messages from unfamiliar emails or clicking on links or downloading applications from websites they are not familiar with. This can be in conjunction with the implementation of anti-bot tools that are swift in detecting bots and blocking them. Firewalls are also important because they can detect botnets and prevent them from spreading in the environment.

Apart from that, we should also focus on limiting the capabilities of internet-connected devices that have internet connectivity as an essential requirement. Here are a few other steps that can be taken in this regard:

- Blocking unwanted inbound and outbound requests
- Implementation of additional authorization and authentication checks
- Network compartmentalization
- Getting rid of default and weak usernames and passwords
- Enforcing authorized software and firmware updates in a timely fashion
- Implementation of least privileges
- Upscaling monitoring capability
- Analyzing network anomalies.

Sinkholes (internal and external) are another enterprise-level tactical approach that can be used to mitigate multiple adversarial techniques and threats.

Trojan horse – covert entry

After a fruitless 10-year siege, the Greeks made their way into Troy using not their sheer strength alone but a tactical approach. Since the dawn of the internet, threat actors have been using the same technique to penetrate infrastructures and environments using malicious applications known as trojans.

Trojans are a type of malicious software that is programmed to take over the target device to impact the confidentiality, integrity, and availability of the targeted system. To gain a foothold in the environment, they imitate legitimate applications or software intending to be initiated by a user post, which they start executing the embedded malicious code to activate. They are often introduced in the environment via malicious emails as attachments and download links or via the installation of untrusted third-party applications that have already been bonded with the trojan.

There are different categories of trojans, depending on the specific mandates they are meant to execute. Following is a comprehensive list of Trojans and the risks to which they expose victims:

- **Trojan-Banker**: The main objective of this trojan is to steal banking account information of users of the affected system. When the trojan is installed in a computer network, it records and relays details about debit cards, credit cards, and e-payment systems via recording keystrokes and screenshots, for example, the Emotet banking trojan.
- **Trojan-Downloader and Trojan-DDoS**: This trojan aims to download malicious programs on a computer, such as additional trojans and adware. Trojan-DDoS is used to initiate DDoS attacks against a specific target using the system resources.
- **Trojan-Spy**: The trojan spy detects and examines how a computer system is used without the knowledge of the user. It can track all applications that consistently run in a computer system. This trojan also employs keystroke monitoring and screenshots to keep track of user activity.
- **Trojan-Mailfinder**: Just like the name suggests, the email finder is a trojan that tracks email addresses from the endpoint user. These email addresses are then used for targeting users in a secondary attack stage. Scams are forged with links and attachments and sent to the recorded email addresses and the spread of malicious malware continues.
- **Backdoors**: This category of trojan provides the threat actor elevated access to the targeted system. The attacker can now execute and terminate applications remotely and receive, send, and modify or delete files. These are often used to unite a collection of impacted devices to form a botnet.

Just like the previous attack vectors, trojans can be mitigated too. Let's understand how.

How to fix trojan threats

Almost all network threats require the same course of prevention strategy. Since the main aim of the threat is to infect a system, it is important to secure the system perimeter and make all of the necessary updates to be protected. Hence, we should ensure that users are following the basic security hygiene practices discussed and applications and systems are hardened using the best security practices such as EDR and firewall.

Rootkit – clandestine malicious applications

Rootkits are malicious applications that focus on providing privileged (administrative level) persistence in the target environment. They allow the threat actor to maintain control of the target system and allow remote execution of commands by the attacker. They can also be manually executed for installation or can be automated. They are often seen to be exploiting known vulnerabilities by employing their exploits for privilege escalation and actions as deemed by the threat actor.

Detection of a rootkit is often difficult because they subvert security software and use tactics to hide using clandestine methods. It often comes with capabilities such as password stealers, keyloggers, and the ability to disable antivirus and other detection mechanisms employed by traditional security software.

Some of the prominent rootkit types are discussed next:

- **Memory rootkits**: These rootkits are found in the system's RAM. A memory rootkit comes accompanied by host software and hides its existence in a computer and eliminates itself from the operating system. The rootkits can hide in the computer memory for as long as years even without the knowledge of the user.
- **User-mode rootkits**: The existence of these rootkits in a computer is either through injection by a dropper or it began during the system startup just like any other program. They mainly infect the operating system of a computer and inject malicious code into the system process. For Windows, the basic focus is the manipulation of the basic functioning of Windows without the user's knowledge.
- **Kernel rootkits**: These are rootkits designed to alter the functioning of a computer's operating system. They corrupt data by adding their own data structures and code that change the system files completely. This greatly and negatively impacts an operating system and slows down the computer's performance. Their impact might not be instant but the system finally gets destroyed.

- **Bootloader rootkits:** They infect the record of the master boot by building blocks or bootkit targets on a computer. They impact the system by furnishing basic commands and loading in the operating system as well as replacing the original bootloader with the malicious one. A user finds it difficult to control this type of rootkit because detecting and exterminating it is tricky. The injected code in the MBR can only damage a computer if a user tries to remove it.
- **Hardware or firmware rootkits:** Such rootkits are found installed on the hardware or the firmware of the targeted system. They can impact the hard drive and the system BIOS of the impacted device. Threat actors have been known to use such rootkits for tampering with and the interception of data being written on the disk.

Let's see how we can mitigate these rootkit threats.

How to fix rootkit threats

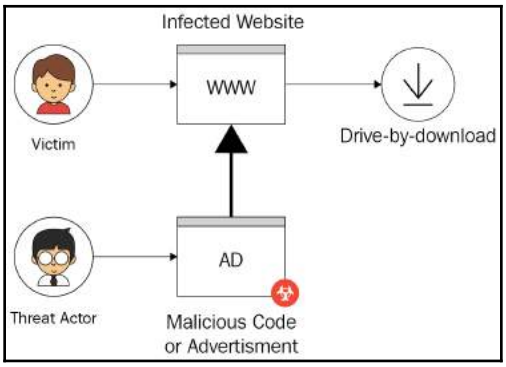
To thwart the threat posed by rootkits, the focus should be on regularly updating the 0perating system and applications and firmware with the latest security patch, alongside looking out for phishing emails and drive-by downloads from unauthorized sources. Organizations should also deploy static analysis, integrity checks, forensic analysis of memory dumps, and signature-based, behavioral-based, and difference-based analysis.

Signature scanning is highly recommended as it can easily identify unfamiliar activities in a computer system from a third party or commands that are not direct from the user. Behavioral-based methods and memory dumps are still viable methods of overcoming the leakage of rootkit viruses in a computer system. They help in carrying out different scanning and this ensures that intruders can be detected in the system. It sends alerts to the user when an unfamiliar activity is detected in the computer network.

Malvertising – ads of chaos

This is one of the common threat vectors used by threat actors to target individuals and businesses alike. The scheme is designed to send code that is illegitimate by maliciously injecting it on genuine online advertisements. This mostly happens in web pages and advertising networks. The injected code hijacks users and redirects them to the dangerous websites that have been linked. It is done without the knowledge of the user as they might perceive that they are clicking on the actual advertisements.

This threat ensures that, when links are sent, malware is installed on the computer system without the knowledge of the user. The malware gets installed silently once the malicious ad is clicked either on mobile devices or computers. This shows how user devices can be targeted, which can lead to a loss of confidentiality and integrity and financial loss:



The main reason behind the deployment of malvertising is to give threat actors access to vulnerable users and devices to introduce crypto-mining scripts, banking trojans and ransomware, and compromises the target to extract financial gains. As a leading threat, it becomes difficult to cope with because some malicious advertisements come from reputable sources and familiar websites.

There have been reports in the recent past that point to malvertising exposing reputable companies with attacks originating from the likes of Yahoo, The New York Times, BBC, AOL, NFL, Spotify, and the London Stock Exchange, where they have been accused of putting users at risk by displaying malicious advertisements.

How to fix malvertising threats

Companies are supposed to be vigilant in their fight against malvertisements to protect their visitors from malicious websites. All running programs on a website are supposed to be examined to detect whether or not they are fraudulent. The domain research tools available should be used to detect whether the sent URLs are genuine even before entering them. All of the code that appears suspicious should also be examined so that users are not redirected to malicious websites. Any advertisement that inherently has encryptions should be decrypted before processing. All of the recurrent ones that are not genuine should be removed from the website and reported as scams to the ad networks. If they persist, the organization should just shift to a different ad network and disassociate with the former.

Ad verification services are very important because they act as watchdogs for the website. They scan advertisement code to verify whether it comes from trusted sources or it is just suspicious code. They are therefore recommended when dealing with malvertising.

Users can protect themselves with the utilization of browser-security plugins, disabling the running of automatic Flash player scripts and scripts from websites, using a reputed ad-blocker, and avoiding clicking on ads from suspicious websites.

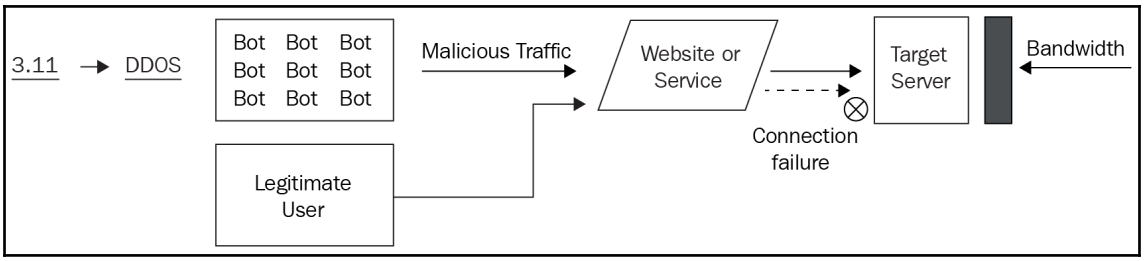
DDoS – defending against one too many

This is one of the most widely encountered cyber disruption/attacks targeting businesses today. These attacks aim to compromise the target by sending an overwhelming amount of requests. They overwhelm these servers with requests for data and services, hence rendering them inoperable.

Their victims are mostly companies that sell products and services online or social media sites and services. Due to the ease and lack of sophistication needed to launch an effective DDoS attack, this has become a favorite attack vector for threat actors resulting in the loss of millions of dollars.

This attack, unlike other network threats, does not target stealing data or accessing sensitive user information; the main objective is to crush the whole system down under the weight of illegitimate requests.

The following diagram shows how this kind of attack is carried out:



DDoS impacts organizations by denying service to legitimate users and disrupting system operations by a flood of connection requests that carry malformed packets. These packets result in denial of services to legitimate users, slowing down of services, and the whole system/service completely shutting down and crashing.

DDoS attacks can be categorized based on the attack mechanism, and two of the most prominent ones are discussed here:

- **Volume-based attacks**: These are attacks where threat actors utilize the large volume of requests to jam services using malformed packets and resulting in flooding the network capability.
- **Application-based attacks**: These are attacks where threat actors utilize known application vulnerabilities to crash the system or service. These are typically vulnerabilities that have high exposure to the availability factor in the CIA triad, and require no user-interaction and/or have remote exploit readily available. Such an application is internet facing and is the ripest target as it is easily accessible over the internet.

Let's understand how such attacks can be mitigated.

How to fix DDoS threats

Since the threat appears as a result of heavy traffic, application servers and services are supposed to have the capacity to handle heavy traffic spikes. Mitigation tools should also be used to address abnormal network spikes and deploy mitigations proactively.

Apart from the basic security hygiene practices of keeping OSes and applications updated to prevent infection, organizations should also focus on the following:

- Having a transparent well-exercised mitigation plan that is practically tested against mock DDoS attacks
- Use of DNS and BGP traffic routing
- Increasing bandwidth and network capacity
- Use of **Content Delivery Network** (**CDN**) for content delivery
- Implementing traffic filtering
- Leveraging connection tracking, IP reputation, deep packet inspection, blacklisting/whitelisting, and rate-limiting

According to F5 Networks, which is a leading player in the application services and application delivery domain, here are some actionable steps to mitigate DDoS as it happens:

- Verify the attack.
- Confirm the DDoS attack.
- Triage applications.
- Protect partners with whitelists.

- Identify the attack.
- Evaluate source address mitigation options.
- Mitigate specific application-layer attacks.
- Increase the application-level security posture.
- Constrain resources.
- Manage public relations.

For strengthening the firewall, platforms such as FireMon, AlgoSec, and Tufin can be utilized.

The complete DDoS playbook link is available in the *Further reading* section.

Ransomware – cyber extortions

This is the most prevalent and dreaded cyber-attack in recent times that has most organizations alarmed. In this attack, a target system or device is locked by an encryption mechanism and is restricted from access to any data from that system. The target can be systems that carry highly classified information or are part of the operational team of the organization.

The stored information is encrypted/locked and kept out of access by the user; some ransomware is also known to block usage of the system itself in an attempt to render the device unusable. In such a case, the user is directed to contact the threat actor for the decryption key to unlock the system and gain access to the data after paying a ransom amount to the threat actor. In most cases, the money is paid through a virtual currency such as Bitcoin to prevent revealing the identity of the threat actor.

Ransomware is mostly spread through infected software applications, scam and phishing emails, malicious attachments, compromised websites with automated downloads or malvertising, and external storage devices that are already infected.

It is recorded that up to 69% of companies that have been attacked by ransomware have lost more than half or even all of their data. (reference: `https://www.metacompliance.com/blog/the-dangers-of-ransomware/`).

Since this attack can result in a significant loss of data, victims often resort to paying the ransom to the cybercriminals to unlock their systems. Threat actors often intimidate victims by threatening deletion to convince the victim to pay up quickly.

Since the dawn of WannaCry, which is well-known ransomware from 2017, organizations of all sizes and segments have been hit by ransomware attacks in one way or another. It is estimated that ransomware incidents cost an average of $2,500 to close to a million dollars. With small and medium-sized organizations being at the biggest risk, the highest ransom paid in 2018 was close to $900,000+. In 2019, the Baltimore city government was facing a ransomware attack with an estimated cost of recovery stretching over $18 million, impacting vaccine production, ATMs, airports, and hospitals among others.

One of the reasons for the wide prevalence of the ransomware attacks is the rise of the ransomware-as-a-service model, which enables the threat actor to leverage pre-built off-the-shelf ransomware tweaked to fit the scope of the attack with custom changes.

Ransomware can be categorized into the following broad types:

- **Encrypting ransomware**: These are ransomware that encrypts files on the target system and asks for crypto-currency for decrypting or releasing the files.
- **Non-encrypting ransomware**: This ransomware does not encrypt files but instead restricts access to the system by displaying pornographic images or directs the user to send premium-rate SMSes or call premium-rate numbers to receive codes to unlock the system.
- **Doxware**: These are attacks where the attacker threatens to publish private information about the victim over the internet. In such attacks, malware is employed to exfiltrate screenshots, webcam recordings, and other private information to humiliate the victim into paying the said ransom.
- **Mobile ransomware**: These are ransomware targeting mobile platforms using a payload to block access to the device using administrative privileges gained during the installation of rogue apps. Such ransomware is also known to lock access to devices and exploit access to cloud backup accounts.

Over the years, attackers have been constantly innovating tactics and techniques to make ransomware infections more potent. Some of them include the following:

- Utilizing fake Adobe Flash updates from the compromised website (Bad Rabbit and TeslaCrypt)
- Phishing campaigns imitating cloud-based Office 365 updates (Cerber)
- Malware-laced macro in Office files (GoldenEye)
- Generic phishing campaigns (LockerGoga and Locky)
- Utilizing wipers to destroy data instead of obtaining a ransom (NotPetya)
- Overwriting the MBR—Master Boot Record (Petya and GoldenEye)
- Utilizing worm-like behavior (WannaCry and ZCryptor).

In 2019, researchers also disclosed ransomware attacks that can infect DSLR cameras exploiting vulnerabilities in the **Picture Transfer Protocol** (**PTP**).

How to fix ransomware threats

Here are a few measures that you can initiate to stay away from ransomware threats:

- **Regularly back up your files**: Ransomware functions by restricting access to data and system operations and, in turn, locking out the user and disrupting business operations. One of the best ways to counter this is by regularly backing up your files. One of the recommended rules to be followed is 3-2-1 in which 3 backups are created, 2 in different formats, and 1 that is stored offsite. When backing up your data periodically, test the backups to ensure that they're readable. Streamline the backup process and coach the respective teams via dry runs.
- **Keep applications and OSes updated**: Often, ransomware that focuses on encrypting files leverage application and/or OS vulnerabilities to infiltrate into the system. WannaCry was one such ransomware that displayed a worm-like propagation capability by leveraging the EternalBlue exploit. The cyclic practice of patching OS and software components in the environment effectively prevents ransomware and other malware attacks that focus on the exploitation of existing security flaws in the target environment.
- **Securely use system components and administration tools**: Today**, c**ybercriminals are misusing legitimate utilities and system administration tools to install and execute malware and conduct malicious activities. Petya utilized PsExec, while various other file-less malware has been known to use PowerShell. To mitigate such malicious use of legitimate applications, enforcement of the least privileges is a viable option. It is also recommended to limit and restrict user access to services, ports, system/software options, and features that do not have a valid business use to limit the attack landscape for the attacker. It is also important to implement application controls, whitelisting, and behavior monitoring capabilities to provide a holistic security landscape.

- **Protecting servers and network**: Security mitigation solutions such as firewalls and IDS/IPS assist in filtering and blocking network traffic and activity that is malicious. By providing forensic information, they assist in detecting incursion attempts and actual attacks. From an attacker's standpoint, all they need is to identify and infect a single vulnerable machine to infiltrate the entire network. Hence, it is important to keep all network components patched and updated, implement multi-factor authentication, account lockout policies, restrict RDP access, and ensure communication channels are encrypted to prevent eavesdropping. Apart from this implementation of network segmentation, data categorization, periodic data backup on separate storage that is not connected to a live environment and is write-protected, and classification are also effective countermeasures.
- **Securing email gateways:** Email gateways continue to be one of the widely exploited attack vectors for malware and ransomware ingestion into the target environment. In accordance with the MITRE ATT&Ck Matrix, this is the phase of initial access. Organizations should implement AI- and ML-based protection mechanisms that can proactively detect and block such malicious attempts. As a best practice, organizations should also deploy URL filtering and categorization, where anything that is not justified with a business need should be blocked. Similarly, disabling browser plugins and third-party components and deploying a sandbox for email attachments and downloaded files and applications should be enforced.
- **Cultivate a security-aware culture:** The human factor of security is often considered the weakest link in the defense mechanism. Social engineering plays a big role in the threat actor's plan of action, be it via a phishing email, vishing, or drive-by download ploy. The need of the hour is to move compliance and regulatory needs and focus on the fine-tuning of IR reaction plans, testing them for efficiency and effectiveness in a quarterly review. In the workplace, a culture of cybersecurity is as equally important as the technologies that stop them.
- **Implement server hardening practices**: Some of the steps you can take under this bracket include restricting admin and elevated privileges, implementing write-access restrictions on remote files, locking down RDP, using a **File Server Resource Manager** (**FSRM**) to block ransomware's changes to your file servers, and so on.

So far in this section, we've seen 10 of the most feared attack vectors that you need to protect your network from. However, besides these, there are a few others that are important to be aware of. Let's take a look at them.

Notable mentions

The overall idea needs to be to have a security-by-design framework and implement it across the environment, which takes care of all the prevalent threats as well as the threats that your industry and organization specifically face.

Besides the aforementioned attacks, there are a few others that need your attention.

Drive-by download

These are downloads that are initiated automatically in the background without the knowledge of the user. Often, malware, viruses, and spyware employ such tactics to download the malicious application on the target system when the user is visiting a website, opening an email attachment, or closing pop-up ads.

A user might visit a malicious website while running a vulnerable version of Flash that might get exploited (or exploit a browser or plugin, hidden IFrames and JavaScript, malvertisements, and cross-site scripting, among other techniques) to initiate the silent download of ransomware or a trojan.

Exploit kits and AI-ML-driven attacks

Today, attackers are heavily leveraging various means to quickly craft exploits and deploy them to attack their intended targets. **Exploit Kits** (**EKs**) are exploit suites that work as a repository for the attackers to utilize and start their attack campaigns in a more streamlined manner. Threat actors host these kits on a website that has been compromised earlier and once a user visits the website, the kit scans for vulnerabilities on the device that it can exploit. Once found, it launches the exploit to compromise the device. Some of the well-known exploit kits are Angler, Magnitude, RIG, Nuclear and Neutrino, Spelevo, and Fallout.

In recent times, AI-powered malware such as DeepLocker has come to light, where researchers found hidden malicious code that can be executed once pre-defined conditions are met. IBM researchers demonstrated this at BH 2018 where a legitimate webcam application with the malicious code was used to deploy ransomware once the user looked at the laptop webcam.

Smart phishing is another example where attackers use AI and ML to form phishing emails using PII information already collected by scrapping through various sources to make it look more legitimate and relevant. Overall, we have seen advancements in the AI-driven use cases by threat actors to do the following:

- Drive autonomous malware.
- Deploy intelligent evasion techniques.
- Implement low-and-slow data exfiltration.

Third-party and supply chain attacks

These attacks are rooted via third-party access to organizations, systems, through an outside partner and vendors, commonly referred to as a third party. These threats exist due to the absence of continuous monitoring, operational visibility, and reporting. Intruders infiltrate these systems via trusted third-party access and gain control of data and systems, and post which confidential data can be exfiltrated or malicious payloads can be dropped.

In 2019, companies such as Cable One, Westpac Bank, the Bank of Queensland, U.S. Customs and Border Protection, Instagram, Truecaller, major Indian banks (Axis, ICICI, IndusInd, RBL), Forbes, Freedom Mobile, Facebook, and several educational institutions were impacted by data breaches due to third-party and supply chain attacks.

Organizations can take the following steps to ensure the protection of their network from supply chain attacks:

- Assess and understand the supplier network.
- Identify and prioritize the risk associated with third-party suppliers and vendor partners.
- Create a comprehensive response plan for supply chain attacks and monitor on a cyclic basis.

The Third-Party Cyber Risk for Financial Services report states that nearly 97% of respondents said that cyber risk affecting third parties is a major issue. - Help Net Security (reference:

`https://www.helpnetsecurity.com/2019/04/03/third-party-cyber-risk-management-approaches/`)

Besides being alert to these threat actors that we just discussed and taking appropriate steps to mitigate them, organizations must also focus on creating an integrated defense architecture. Let's discuss this more next.

Creating an integrated threat defense architecture

Organizations moving forward with detection capability for the aforementioned threat vectors should also focus on the creation of an integrated threat defense architecture for a streamlined and comprehensive approach. Objectives for such should include the following:

- **A central monitoring and response capability**: Such a capability will take care of centralized policy management, provisioning, configuration management, change management, and event management, resulting in smooth security operations and extensive visibility. This can be achieved by deploying a SIEM platform such as Splunk, ArcSight, QRadar, ELK, and AlienVault OSSIM.
- **Security engineering**: This is responsible for extension, streamlining, process enhancement, and fine-tuning security operations and ensuring accurate and adequate enforcement of those controls along with measuring their effectiveness and efficiency.
- **Threat intelligence and threat hunting**: These are responsible for being the eyes and ears of security operations, maintaining situational awareness level for emerging and prevalent threats. Threat hunting teams can leverage these inputs and do proactive threat hunts in the network environment to detect, identify, and mitigate covert threats that have successfully bypassed security mitigations and controls. More on this is discussed in `Chapter 9`, *Proactive Security Strategy*.

Now that we have understood the typical threats that are faced by organizations and their relevant mitigation strategies, it's time to focus on strategies that can assist us in keeping track of new vulnerabilities and assessing the network for threats with the help of continuous monitoring.

Keeping up with vulnerabilities and threats

Attacks on networks often result from the exploitation of existing vulnerabilities, therefore, is it important to fix and keep up with all existing vulnerabilities in the network to prevent threat exposure to the aforementioned threat vectors. This is exactly what we will be learning to do in this section.

Researchers explain that there are a lot of inherent loopholes that lead to network vulnerabilities. These gaps expose the infrastructure to a hacker to readily commit cybercrime. For example, missing data encryption is an opening that makes a network vulnerable and needs to be fixed. Some organizations have inadequate password policies; these passwords are simple and easy to guess and an intruder will not struggle to break into the database by cracking them if a change is not enforced after a while. Critical assets may have missing authentications or authorization checks, which might be a welcome sight for an attacker to easily infiltrate those assets that may process or be very critical to organizational operations.

Understanding various defense mechanisms

There are different types of network vulnerability and, depending on the threat actor's goal and objective, an attack is launched. Vulnerable network systems are weak spots in the defense perimeter and through it, the threat actor can gain full/partial access to data and sensitive information on the impacted system. It is therefore important that companies and individuals take decisive action to curb network vulnerabilities and keep up with them.

Some prominent defense mechanisms against such vulnerabilities are discussed next.

Safeguarding confidential information from third parties

Most people presume that network threats are only due to remote attackers. However, as discussed, various threats can result from aspects relating to how trusted contractors, vendors, and third parties are connected to the environment and how they are managed. It's important to have clear visibility into what level of access is provided to these entities and how they are accessing, processing, and storing information of said organization. Here's how this can be done:

- Organizations should focus on documenting security requirements for each third party in the contracts and put a penalty in case of deviation.
- Conduct periodic security assessments and audits to ensure strict adherence to the security policy and requirements.
- Ensure third parties remediate any security incidents or threats in their environment, showcasing due care and due diligence, and notify the organization in a reasonable time.
- Have clear visibility into what data the third-party accesses, processes, and stores and how.

It's also important to have cyclic security audits in place to maintain assurance into the engagement and identification of any loopholes or blindspots that might result in a potential cyber disruption or cyber threats for said organization.

Implementing strong password policies

In any organization, a strong password policy should prevail and check for **Authentication, Authorization, and Accounting** (**AAA**). Some actionable best practices that can be implemented are discussed here:

- Passwords should be changed within 45-90 days.
- Existing or old passwords should not be used again.
- Passwords should be alphanumeric with a special character and mandated use of 1 or 2 uppercase letters.
- Enforce a minimum password length of 12 or more characters (suggest the use of a passphrase rather than a password).
- Enforce a password audit policy and notify responsible stakeholders of any changes.
- Breaking passwords remains a major focus point for attackers, no matter what their intentions are. Hence, it demands attention and policy enforcement. Organizations are also recommended to monitor dark web and other data leak repositories to ensure situational awareness for possible password breaches.

Enhancing email security

Emails are known for being a potential model for the introduction of scam and other network threats in an environment. The frequent use of email to receive and send data also exposes the platform to misuse. They may carry a nasty virus or malware that installs automatically on a user device. Messages containing highly confidential data may be sent to an outsider or unauthorized user as a medium for data exfiltration. To keep this in check, the organization should focus on the following:

- Enabling security best practices such as SPF, DKIM, and DMARC and the use of 2FA
- Implementing spam filters, email sandboxing for attachments, hyperlink sanitization, and email encryption
- Training employees, including executive leadership, on safe security practices and conducting phishing simulations

Pretty much every organization depends on emails for their business operations and exchange of information. Hence, it is obviously one of the most widely used attack vector by threat actors to infiltrate an organization and make headway into a target environment via means of phishing and malware-laced emails.

Vulnerability management policies

A diligent, streamlined VM policy should be put in place and communicated to all stakeholders and process owners. They should be made to understand it well and perform a compliance acceptance that outlines the consequences of non-compliance. The level of security that an organization is willing to maintain should be well communicated to the team. The team should be made to comply to remove any form of a vulnerability existing in the environment beyond the tolerable timelines. The guidelines of vulnerability management and practices followed should be part of their training. The threats and risks about vulnerabilities and their impact should be classified and the management should be made aware of this for a priority. In this way, an organization can maintain clear visibility into the vulnerabilities that may lead to network threats.

Let's conclude this section by understanding how vulnerabilities can be kept at bay by adopting a few steps as part of the vulnerability management life cycle.

Vulnerability management life cycle

The life cycle of vulnerability management comprises six major steps. These steps are to be followed sequentially without breaking protocol. When the life cycle is completely followed, a security management hedge is built and established to curb all probable vulnerabilities. The steps are as follows:

1. **Discover**: This step focuses on the discovery of all assets within a network and host details such as open services, ports, and operating systems that should be thoroughly examined to detect exiting vulnerabilities, along with a network baseline. An automated schedule should be in place to identify and detect security vulnerabilities regularly.
2. **Prioritize assets**: All assets within the business should be categorized according to their order of value and function (crown jewels and high-value targets should be prioritized). Business criticality, units, and groups should be the basis of classification so that business value can be asserted to every asset group according to their complexity within the business operation.

3. **Assess:** A baseline profile of risks should be determined in an attempt to minimize any possibility of exposing the network to risks. This should be done regarding asset classification, asset criticality, vulnerability, and threat impact.
4. **Report**: The level of risk and threat associated should be measured together with assets in the business unit in regards to policies of security within the unit. All known vulnerabilities should be described, security plans documented, and suspicious activities monitored.
5. **Remediate**: Fixing vulnerabilities is supposed to be made a priority according to the risks that the business is exposed to. A demonstration of progress should be consistently showing the establishment of controls.
6. **Verify**: Follow-ups and activity audits are the best way of showcasing progress. Through them, all threats should be eliminated from the network system. It's always important to verify that the threats are eliminated.

Platforms such as RedSeal and Skybox are exceptional platforms for network modeling and vulnerability management, which grant greater visibility into the network and environment of an organization. Qualys is another market-leading vulnerability management and network security platform.

Next, we will take a look at important attributes around network vulnerability assessments and how we can utilize a scanning tool to analyze a network.

Network vulnerability assessments

Vulnerability assessment refers to the process of identifying, defining, prioritizing, and grouping vulnerabilities within a system, network infrastructures, and applications. The assessment for the organization should be provided with adequate insight and risk background and awareness to understand and overcome possible threats.

Analysis and reviews within the network are done vigorously to detect loopholes and possible security vulnerabilities. The security architecture and the defense mechanism of a network are hence improved by network administrators and security professionals to curb possible threats and vulnerabilities. It is mostly done through special inspections that can detect potential weak points and security holes capable of exploiting a computer network, which can be based on the NIST Cyber Security Framework or other security best practices and industry guidelines for a comprehensive assessment. These inspections can identify and classify vulnerabilities in the environment following which we can go to confirm the appropriateness of countermeasures, effectiveness.

Some of the broad topics that should be focused on during network assessment apart from vulnerabilities are the following:

- Inventory management
- Device and server management (including mobile devices)
- The appropriate configuration of networking devices
- Identifying and accessing management
- User behavior analysis

There are various steps followed in the assessment of vulnerabilities. The initial one identifies the assets within a network and defines the threats and value of each critical assets and devices. This is concerning the input of the client, for instance, vulnerability scanners and security assessment. The definition of a system baseline is also key. It identifies the extent of an exposed threat and the limit of detection for such risks. Vulnerability scans are also performed to determine the level of a vulnerability risk within a network. Finally, a report is created once the vulnerability assessment is done.

Besides these methods, there are also automated platforms that assist us in the process and speed up of assessments. Let's look at a few of these platforms.

Utilizing scanning tools in vulnerability assessment

Vulnerability scanning tools play an important role in network security assessment by automating security testing and audits. They scan websites, applications, and networks to detect various security risks and threats. They generate a list of prioritized vulnerabilities that should be patched and provide steps describing how to remediate them.

Typically, a good vulnerability assessment platform should check for all major threat vectors inclusive of the prevalent and recent ones that are being used by attackers to target organizations. Some of these may include directory listing, PII disclosure, code injection, XXE, SSRF, CSRF, XSS, SQL injection, captcha detection, RFI and LFI, path traversal, source code disclosure, command injection, session fixation, response splitting, insecure cookies, session hijacking, and other OWASP-defined attack vectors.

Some of the well-known vulnerability assessment platforms utilized by security professionals are discussed here:

- **Nexpose**: This tool provides better insights into reported vulnerabilities with an advanced prioritization score and provides continuous monitoring of new assets and devices added to the network. Besides this, it helps in policy assessment with regards to industry standards such as NIST and CIS and provides prioritized remediation reports with ready to use Metasploit integration.
- **Nessus professional**: Nessus provides real-time vulnerability updates; compliance checks against major standards such as NIST, PCI, CIS, and FDCC; and operational capabilities such as coverage across CVEs and scanning time, and accuracy and the UI are major differentiators.
- **OpenVAS**: This is a free and open source feature-rich software vulnerability scanner that provides you with all of the major features of a commercial scanning platform. It includes authenticated and unauthenticated scans and scanning of high and low-level industrial protocols, among other features.

The organization should not completely depend on automated vulnerability scanning tools alone but should also focus on building the capability and training the analyst to conduct manual testing and tweak the logic of the scans to make a more insightful and contextualized scan based on the environment and network landscape as well as the business logic of the processes.

Exercising continuous monitoring

In network security, continuous monitoring is the procedural ritual used to identify cyber threats, security misconfigurations, vulnerabilities, and compliance issues in regards to the operational environment of an organization. It aims at reducing business losses by minimizing the potential of loss or cyber disruption through continuous visibility and provide insights into the day-to-day operational aspects.

Transactional applications and other financial controls are specifically audited continuously to prevent any malicious activity that may severely impact the business of an organization by causing financial and reputational damage along with regulatory fines, if not detected and acted upon in appropriate timelines.

With respect to securing networks, continuous monitoring plays a very vital role by identifying all potential threats in the environment on a real-time basis. In terms of operation, they yield effective and relevant results as it helps to deal with probable potential threats and works strategically while updating real-time threat information, creating awareness of existing vulnerabilities and maintaining visibility through the network. In the case of existing monitoring data that is available, it becomes important to collect additional data points that can either provide context or clarity around the potential threats.

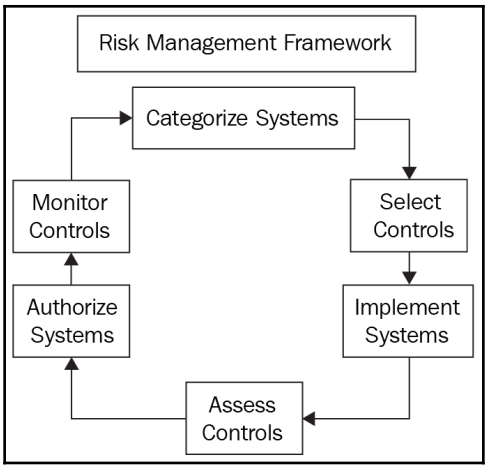
A lot of consulting organizations service solutions and promote the idea of the cyber defense platform, which is a good example of how to operationalize different vendor products and solutions to work synchronously as an integrated solution forming a formidable security posture for the organization. An example of this is the Accenture Cyber Defense Platform, published in 2016, which compromises solutions from vendors such as Splunk (SIEM with security analytics and ML for environment monitoring), Palo Alto, and Tanium (perimeter and endpoints security mitigations). Similarly, organizations such as Wipro and Symantec also have integrated threat management offerings, which are a good industrialized model to implement.

In an organization, risks and threats are addressed by placing mitigating controls in place. These controls and operations should continuously be monitored for their effectiveness in mitigating threats and abnormal activity or unauthorized changes in the environment that need to be reviewed and validated.

This way, the company's operational risk profile is enhanced. There are potential benefits associated with continuous monitoring as the mitigation techniques applied are unique. They focus on identifying loopholes and problems as soon as they occur. Corrective actions are carried out immediately after the detection and this helps to safeguard networks from potential threats.

The NIST Risk Management Framework

The NIST Risk Management Framework is another good example of an information security program that focuses on the management of organizational risks associated with system operations. It provides an effective framework for the selection of appropriate security controls for a system. It also provides a process of integration of security and risk management procedures into the system development life cycle:



It is composed of the following principals:

- **Prepare**: This focuses on the mission of the organization along with the business processes to effectively manage the security and privacy risk level.
- **Categorize**: This classifies information based on impact analysis.
- **Select**: This sets the baseline security controls based on the security categorization as deemed necessary due to the risk levels.
- **Implement**: This deals with the implementation of the security controls and documents how they are operationalized.
- **Assess**: This talks about the effectiveness and efficiency of the applied security controls.
- **Authorized**: This provides the required authorization of the system processes based on the determination of organizational risk to assets, employees, and processes resulting from the system operations.
- **Monitor**: This focuses on monitoring the security controls on an ongoing basis to assess the security control performance, conduct an impact analysis of changes, and report on the same to the management.

Organizations should ensure the inclusion of system and network configuration management tools that can be integrated with GRC and SIEM platforms for centralized data collection and visibility. Additionally, the program should encompass the **Security Content Automation Protocol** (**SCAP**) framework from MITRE and NIST as a best practice, which is a good template that enables seamless risk analysis. Organizations should also take a look at NIST **Information Security Continuous Monitoring** (**ISCM**) from NIST SP 800-137, which talks about the process and procedures for maintaining continuous awareness of information security to support organizational risk management decisions.

Some of the top platforms used for continuous monitoring are as follows:

- **Spiceworks**: Asset management/device status monitoring
- **Snort**: Network intrusion detection system
- **SolarWinds**: Network management/systems management
- **Nagios/Paessler PRTG/Awake Security**: Network and system monitoring
- **Tenable/Rapid7 Insight**: Vulnerability scanning/log analysis
- **Cisco Identity Services Engine**: Network gatekeeping/user and device profiling
- **AppDynamics APM/CA UIM/Amazon CloudWatch**: Cloud service/security monitoring
- **Barracuda Sentinel/Proofpoint Essentials/Mimecast**: Email protection platform

Next, we will take a look at NIST 800-37 and understand the key aspects and attributes of it the same that can be implemented by organizations.

The NIST Release Special Publication 800-37

According to the NIST release, the focus was mainly on information systems and organization framework management. For privacy and security, it approaches the idea as a system life cycle. It's a comprehensive manner of operation holistically addressing supply chain risks, privacy, and security.

The process consists of six actionable steps:

- Categorization and authorization of systems
- Selection
- Implementation
- Assessment
- Monitoring of security controls

In 2018, NIST published an update on SP800-37 (Rev 2) titled *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, which consisted of seven major objectives:

- Provide a correlation between risk management processes and activities at the operational level of the organization.
- Standardize critical risk management preparatory activities.
- Demonstrate how NIST CSF can be associated with RMF and executed using the NIST risk management process.

- Integrate privacy risk management processes with RMF.
- Encourage the development of secure software and systems by following life cycle-based systems engineering processes as prescribed by NIST.
- Integrate **Supply Chain Risk Management** (**SCRM**) with RMF.
- Employ an organization-generated control approach.

You can access the entire copy by visiting `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf`.

In the framework, the integration of risk management in the aforementioned disciplines are at the core mission of the levels of the organizational processes. Practitioners of cybersecurity, IT auditors, the general IT field, and governance professionals become very important as they can understand and contemplate how the recent release of NIST can be impactful to their organizations and companies. The publication of NIST and its release has greatly helped in risk management. Some of the major fundamental focus points include the organization-wide risk management process, utilization of a system development life cycle, enforcement of logical and technical system boundaries, and security control implementation.

Summary

In this chapter, we looked at the various prevalent network threats and their concurrent impact on organizations from a day-to-day operational standpoint. We also discussed how security professionals can work toward mitigating each of them and subsequently forming an integrated fortified cyber defense posture for the environment.

Equipped with the information from this chapter, you should now be able to create a comprehensive plan of which threats you need to check for and how to mitigate each of them, as well as how to create a vulnerability management plan and assess the network's secure state and compliance level.

Following this train of thought, in the next chapter, we will take a look at how to conduct network penetration testing and the various industry best practices. We will take a step-by-step approach for practical penetration testing and enable you to perform network penetration testing and document the findings on your own. We will look at the different tools and platforms that will help us to perform these activities efficiently.

6. Trojans are not capable of which of the following?
    - Stealing data
    - Self-replicating
    - Stealing financial information
    - Stealing login credentials
7. What is the name of the attack where emails are exclusively designed to target any exact user?
    - Algo-based phishing
    - Vishing
    - Domain phishing
    - Spear phishing

Further reading

- Breaking Down the Anatomy of a Phishing Attack: `https://logrhythm.com/blog/breaking-down-the-anatomy-of-a-phishing-attack/`
- Detecting a Phishing Attack with **Phishing Intelligence Engine** (**PIE**): `https://gallery.logrhythm.com/use-cases/detecting-a-phishing-attack-use-case.pdf`
- Emerging Insider Threat Detection Solutions: `https://blogs.gartner.com/avivah-litan/2018/04/05/insider-threat-detection-replaces-dying-dlp/`
- 20 Common Types of Viruses Affecting Your Computer: `https://www.voipshield.com/20-common-types-of-viruses-affecting-your-computer/`
- New Adwind Malware Campaign Targets Utilities Industry Via Phishing Techniques: `https://latesthackingnews.com/2019/08/25/new-adwind-malware-campaign-targets-utilities-industry-via-phishing-tehcniques/`
- The Mirai botnet explained: `https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html`
- Smominru Monero mining botnet making millions for operators: `https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators`
- Major sites including the New York Times and BBC hit by "ransomware" malvertising: `https://www.theguardian.com/technology/2016/mar/16/major-sites-new-york-times-bbc-ransomware-malvertising`
- Cloudflare DDoS Mitigation: `https://www.cloudflare.com/learning/ddos/ddos-mitigation/`

- *DDoS attacks in Q1 2019*: `https://securelist.com/ddos-report-q1-2019/90792/`
- The F5 DDoS Playbook: Ten Steps for Combating DDoS in Real Time: `https://f5.com/Portals/1/Premium/Architectures/RA-DDoS-Playbook-Recommended-Practices.pdf`
- The Next Paradigm Shift AI-Driven Cyber Attacks: `https://www.darktrace.com/en/resources/wp-ai-driven-cyber-attacks.pdf`
- Data Breaches Caused By Third Parties: `https://www.normshield.com/data-breaches-caused-by-third-parties/`
- **Information Security Continuous Monitoring** (**ISCM**) for Federal Information Systems and Organization: `https://csrc.nist.gov/publications/detail/sp/800-137/final`
- Accenture Cyber Defense Platform: `https://www.accenture.com/_acnmedia/accenture/conversion-assets/dotcom/documents/global/pdf/dualpub_26/accenture-splunk-cyber-defense-solution.pdf`
- Wipro's Integrated Threat Management: `https://www.wipro.com/content/dam/nexus/en/service-lines/applications/solutions/integrated-threat-management.pdf`
- Symantec Integrated Cyber Defense: `https://www.symantec.com/theme/integrated-cyber-defense`