CAYUSE
COMMERCIAL SERVICES

THREAT PREVENTION AND RESPONSE:

RANSOMWARE DUE DILIGENCE

cayusecommercialservices.com

TABLE OF CONTENTS

THREAT PREVENTION AND RESPONSE:
RANSOMWARE DUE DILIGENCE

Ransomware creates victims out of users. A type of malicious software, or malware, it is used by cybercriminals to hold computer systems and data hostage until a ransom is paid. In recent years, ransomware has become one of the most devastating cyber threats impacting businesses. Through kidnapping data for financial gain or to threaten their victims into providing a payment to 'keep quiet', cybercriminals have gotten savvy enough even to use measures of protection to commit their mischievous acts.

Ransomware is a serious threat to businesses, however by understanding the different types of ransomwares and having a response strategy in place, businesses can develop a comprehensive security plan to combat cybercriminal activity.

THREAT DEFINED

The National Institute of Standards and Technology (NIST) describes a security threat as 'any circumstance or event with the potential to adversely impact organizational operations, organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.'. An IT security threat is an entity or event that gives an Indication of Compromise (IOC).

Ransomware threats can enter a network through several means, including indirect (passive) or direct (active) interactions with users. Indirect methods involve access gained through third party systems or services that have access to the company's network, such as remote services and vulnerable systems on the dark web, or via drive-by downloads on unknown websites. Using legitimate sources to gain entry, this method is oftentimes more difficult to detect.

The indirect approach involves phishing attacks, brute-forcing passwords, or exploiting unpatched

software. Since 2020, there has been a spike in the use of phishing as an initial payload for ransomware attacks. Threat actors resort to phishing activities to acquire the credentials that provide access to remote services such as RDP and VPN servers. They then sell these credential dumps as an initial payload to cyber criminals on dark web forums. This is considered passive reconnaissance since the attacker is not interacting directly with the target.

Direct or active interactions involve access gained through a security flaw or vulnerability. Direct methods such as manipulation of naive users through social engineering are usually done through email exploitations that deliver malicious payloads. When unsuspecting victims open '.xls' and '.doc' files in the emails, macros will execute, run the payload, and load malware directly into the system. Users must be trained to avoid acceptance of these free-ware downloads in tandem with administrators enforcing Data Execution Prevention (DEP). Organizations need to consider advanced threat intelligence capabilities to complement their email security solutions.

One of the most common ways that ransomware accesses a network is through vulnerable systems that have been neglected, however are still connected to the public-facing network and aren't stand-alone systems. Ransomware typically goes after files stored in common locations like the 'desktop' and 'documents' folders. Some of the most frequently exploited, vulnerable internet-facing services include VPNs.

At times, ransomware moves about the network surreptitiously and then infects file system changes to protected folders, which forces a roll-back to the previous backup. This prompts the user to revert to that backup, hindering operations. Conducting backups as a regular routine aids in protection, and organizations that neglect the importance of them create a detriment to business operations and place additional stress on the administrators responsible for completing these reinforcements.

A (BRIEF) RANSOMWARE TIMELINE

The emergence of ransomware and its increasing ability to wreak havoc can be traced back on a timeline starting over 40 years ago.

Late 1980s: Early ransomware, called 'PC Cyborg' locked users out of their computers and demanded payment for a decryption key.

2005: The spread of ransomware through the use of malicious email attachments begins. Individual users became the target of cybercriminals with Gpcode which used Advanced Encryption Standard (AES) to block users from accessing their computers by demanding a ransom payment.

2009: Businesses became the target of ransomware in 2009, when CryptoLocker emerged with increased sophistication and the ability to spread quickly through emails.

2010: Russian cybercrime groups are on the rise. One in particular, the Lurk Group was pivotal in developing the Ransomware-as-a-Service (RaaS) offerings, streamlining ransomware campaigns by eliminating the need for advanced technical expertise.

2019: The development of organized cybercrime groups heightened in 2019 and 2020. Ransomware was used to encrypt the systems and data of their victims, demanding payment in exchange for restoration. In 2019, a ransomware conglomerate the 'Maze Gang' was known for publishing the data of their victims on their own web page, The Maze News. They stole data, making a copy of it prior to encryption, and followed up with delivery of a ransomware note demanding payment. Their malice also included the release of stolen proprietary information to the press if the ransom wasn't paid. They were involved in numerous large scale ransomware operations and attacked prominent, big-name companies by forming a ransomware cartel which shared information and strategic tactics.

2020: The Cybersecurity and Infrastructure Security Agency (CISA) issued an alert notifying healthcare organizations of a ransomware outbreak that was specifically targeting their systems. Ryuk, a ransomware created by WIZARD SPIDER compromised several government agencies and infrastructure organizations associated with energy resources, healthcare, manufacturing, and financial services. One year prior, in 2019, Ryuk had the highest ransom demands, which were upwards of $12.5 million, with a grand total netting more than $150 million by the end of 2020.

January 2023: A significant ransomware takedown occurred on January 26, 2023. It involved a RaaS operation group called HIVE (Highly Intelligent Viruses Everywhere) that was seized as part of a coordinated law enforcement effort involving 13 countries. HIVE actors and followers used single factor logins via Remote Desktop Protocol (RDP) to access private networks and jump servers. They were able to bypass multi-factor authentication systems, gaining access to the networks of their victims. Opening their crime scene enabled even more novice cyber-criminals to launch ransomware attacks on healthcare providers, energy providers, charities, and retailers across the world.

To this day, malice continues to evolve. Ransomware exists that can adapt to things like current events, stimulus checks, and surveys – things that look legitimate until a user opens the attachment and unleashes the nemesis.

TYPICAL TYPES OF RANSOMWARE

Knowledge is power against ransomware. Understanding how the various types of ransomware function and from where they are generated is helpful in formulating a plan of prevention, or attack.

Numerous forms of ransomware exist, each with its own specific motives, characteristics, and methods. There are eight specific types however, that cyber professionals refer to as the 'most common' manifestations.

Encrypting or 'Crypto' Ransomware

This is a malicious type of software that encrypts files and then demands a ransom payment to decrypt them.

Screen Lockers

The victim's computer screen is locked, with prevention in place from accessing it until a ransom is paid. In some cases, a message appears on the screen with instructions on how to do so.

Scareware

This tactic instills fear in the victim through a fake security message or pop-up, warning the user of a virus and frightening them into action.

Leakware

This malware threatens to publicly release information if a ransom isn't paid. The data is usually sensitive in nature and includes personal media such as photos and videos, or personal data such as Social Security numbers.

Doxing Ransomware

A form of victimization, doxing ransomware threatens to release personal information such as email and physical addresses, and phone numbers through venues such as social media while demanding a payment to refrain from doing so.

Fileless Ransomware

Because it is installed directly into the memory of a computer, fileless ransomware is difficult to detect and remove. It gains access typically through social media in the form of spear phishing emails or malicious websites to gain access to a system and encrypt data on the computer.

Double Extortion Ransomware

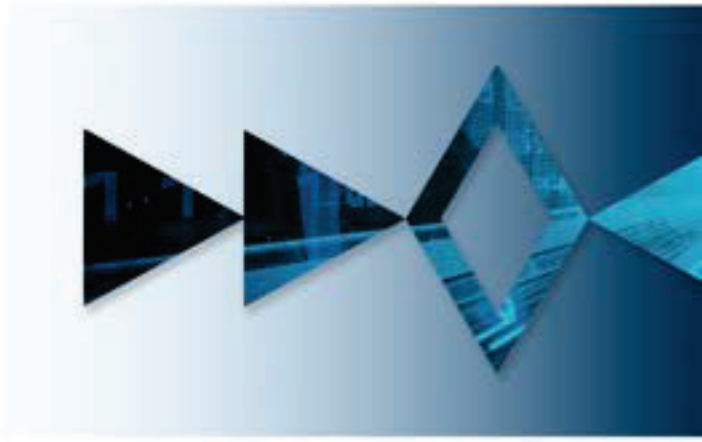
In addition to encrypting the data, with double extortion, companies are threatened to pay an

additional ransom to prevent the disclosure of their stolen information. This form of double exploitation is often the one that worries most companies, because they have to pay both a ransom for the decryption key, as well as hush money to the criminals to avoid disclosing their proprietary and trade secrets to buyers on the dark web.

Ransomware as a Service (RaaS)

Here, the ransomware is provided through a pay-for-use service to those that want to use it for their own personal gain. The RaaS creator provides an online subscription to access illegal ransomware tools and is paid a certain portion of successful ransoms by members that use the subscription service.

Multiple forms and types of malwares are available for criminals to manipulate in order to gain the information they want. It is highly recommended that businesses take a proactive approach to prevent ransomware from entering and spreading.



TECHNIQUES OF CYBERCRIMINALS

Security practitioners must be extra vigilant of the various methods and locations of threats, as they they tend to attack when least expected yet most achievable. In essence, security personnel need to think like cybercriminals in order to design and implement impactful, protective measures. Attacks are unpredictable and thus, security practices need to be in a constant state of readiness. Cybercriminals take full advantage of opportunity by organizing events such as:

Attacks Planned During Annual Security Audits

During technical testing events, cybercriminals can hide under the eyes of authorized penetration testers. Although the testers are supposed to discover and exploit system vulnerabilities, attackers are able to surreptitiously infiltrate the network and remain persistent. They conduct security assessments prior to exploiting weaknesses within the system during an annual audit.

Upper management can also gauge how well their security training program is doing by implementing simulated phishing tests. Phishing simulations appear to be malicious emails launched by attackers, however, are actually fake phishing attacks used against distracted employees by their own team. This can provide critical statistical data collection methods for future use during risk assessments and gap analysis.

Double blind testing is a security measure that allows for implementation of an exercised attack without the cyber defenders knowing. This provides a challenge for them in maintaining control. Unaware of the validity of the attack, they must always react as if it is real. A double blind test can also be helpful in refining the company's user authorization list in order to rule out anyone who is inappropriate to participate in the auditing exercise.

Threat Detection and Mitigation Resources

- *Use of an Endpoint Detection and Response (EDR) system allows for automatic operations on multiple endpoint devices (such as computers, servers, and mobile devices) to assist in tracking attack patterns automatically. Endpoint security solutions constantly monitor end-user devices in real time and use a combination of techniques such as machine learning, behavioral analysis, and threat intelligence to detect and respond to cyber threats.*
- *Implementing User and Entity Behavior Analytics (UEBA), or User Behavior Analytics (UBA) which involve solutions or features that discover threats by identifying activity that deviates from a normal baseline.*
- *Response Teams use the Process for Attack Simulation and Threat Analysis PASTA to help analysts detect blind attacks. PASTA is a risk-centric threat modeling methodology that provides a step-by-step process to inject risk analysis and context into an organization's overall security strategy.*

Attacks Planned on Deleted Files

When a file is deleted from a computer, it isn't immediately erased from the hard drive. The computer regards the space as free, however the file may remain until it is overwritten by another. This 'free' space is often a target. Coded 'logic bombs' are programmed to launch malicious activity once a certain condition is met. For example, a logic bomb can execute malicious activity on a deleted file or can be programmed to delete a file when the user attempts to access it. A logic bomb can also shut down systems or send out spam emails. In business, such malice can wreak havoc on employees, customers, and processes.

For example, the Local Security Authority Subsystem Service (LSASS) is a process in the Microsoft Windows operating system that is responsible for enforcing the security policy. It verifies users who log on to a Windows computer or server, handles password changes, and creates access tokens. Registry keys are important technical components to a computer and its

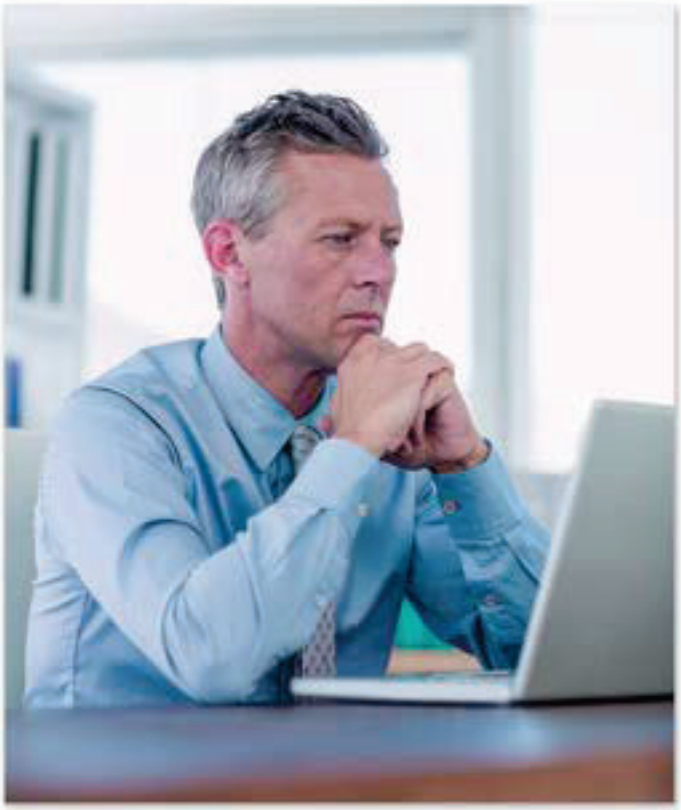
installed programs. If an essential registry entry were to fall victim to a logic bomb attack, it has the potential to damage the computer system and the internal processes that help run those programs.

Threat Detection and Mitigation Resources

Several measures can help in malware and logic bomb situations. Tripwire is a file integrity monitoring tool that watches for changes to critical files on the system and sends out an alert if changes are detected. Keeping anti-malware software updated on a consistent basis is vital. Use of a Host-Based Intrusion Detection System (HIDS) helps to identify internal network threats by giving an analyst deep visibility into the goings on with the company's critical security systems.

Attacks on Privilege Escalation

Attackers don't always abuse user accounts. They also misuse the very tools that protect data, such as encryption and designation. By targeting the resources that have access to restricted information, the attacker has an open path to those same privileges. This can be used to acquire confidential information, modify system settings, or take control of the entire system. Once the system is compromised or data becomes encrypted, it prevents other users from accessing it, thus hindering business processes.



Attacks on Accounts that Linger

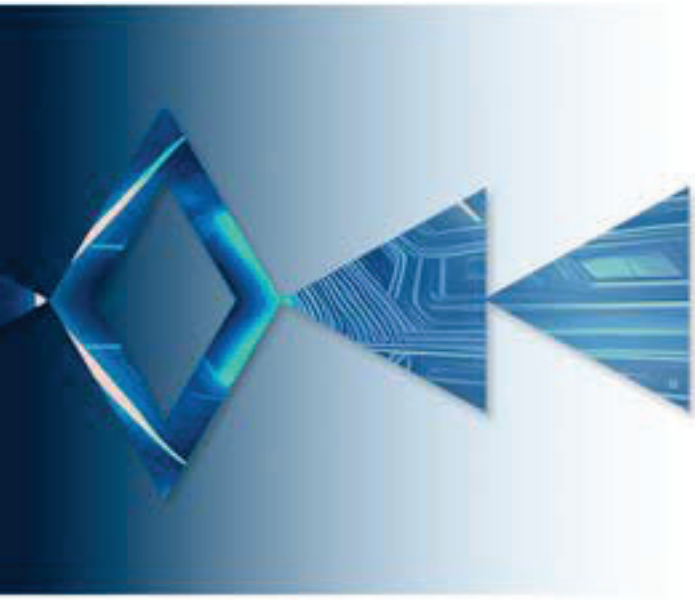
Employee accounts that were supposed to be deleted, however, are still present on the access control list and provide entry points for threat. A non-negligent method, the managers place the account on freeze or hold before deleting in order to audit the previous employee's activity prior to leaving the company. Allowing accounts to linger or letting employees delete their own is dangerous protocol. If the accounts aren't deleted properly, an attacker can use the old, compromised one to laterally traverse the network and cause havoc. The attacker could create an alternate account under a different name for continued access to the system. It is important to note that the company administrator needs to be the only one appointed with the ability and right to delete an employee file at the time of termination from the company.

Threat Detection and Mitigation Resources

Misuse case testing needs to be a part of application/functional testing to both find bugs in the tool and make it 'dummy' proof. Use efficient auditing tools such as iAuditor, Standard Fusion, and Benchmark EHS for compliance standard reviews. For a very economical approach consider using SySmon to forward/mirror Microsoft's application logs.

Ransomware spreads rapidly and can propagate its gain manually or automatically. The attackers have the ability to either manually command the encryptors to run on specific systems, or they deploy the encryptors with existing software development tools, batch files, and group policy objects. Automated propagation exploits the trust relationship between systems by binding PsExec to other systems to execute its payloads.

Software developers are constantly and consistently creating solutions to improve security, protect systems and data, and make daily operational tasks easier for administrators to manage. Unfortunately, the data cannot be recovered if it has already been compromised by ransomware. Companies need to invest in conducting frequent backups and setting the RPO intervals to recover backups on an alternate site for continuous availability.



ALTERNATE FORMS OF RANSOMWARE

Cybercrimes are criminal acts that fall under the Computer Fraud and Abuse Act with convictions that result in criminal charges. The execution of a cyberattack doesn't always require encryption and may stray from the typical definition of ransomware. Something as seemingly benign as a security alarm in a server room has the ability to be compromised.

Having full control of the system, the operational technologies that comprise it, or even the security panel, this type of attack might involve manipulation of functionality during times of an emergency – and the use of fear and chaos to gain advantage.

An attacker might use the company's computer resources to commit a kidnapping. For example, fire suppression systems that use CO2 in lieu of water are designed to suppress or extinguish fires located in sensitive environments such as server rooms, engine rooms, flammable storage areas, and data centers. Using CO2 prevents the risk of water damage. If an attacker is persistent in their

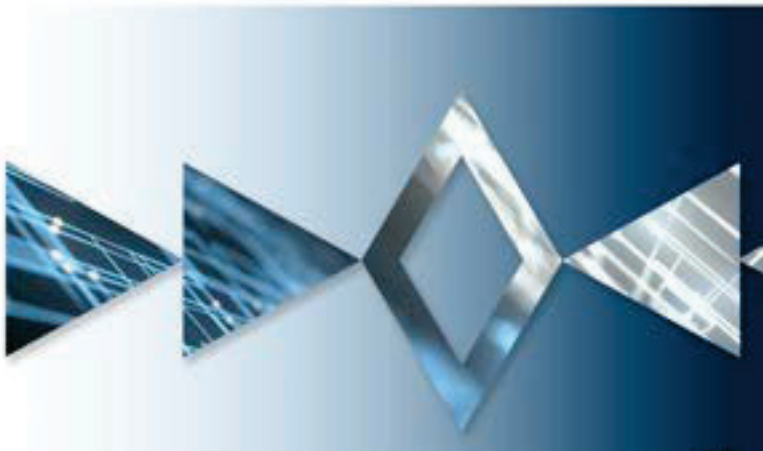
attack campaign, they might opt for taking over the C2 (Command and Control) system, gaining the ability to lock the server room and release CO2 during a non-emergency situation. The danger and control increase exponentially if employees are also in the server room. The attacker may demand a ransom in exchange for their release. Once the attacker gets paid, the air locks to the server room are released while the CO2 is kept in check. The concept of holding humans hostage versus data or files is also a looming threat that must be considered when implementing security measures.

If an internal system is able to detect the temperature in the room that houses critical database servers, it is imperative that proper monitoring is in place to avoid corrosion. Computer systems need to be between 30% and 50% humidity. Too much humidity will damage the system and too little will create electric static. If a cybercriminal is able to change the humidity and disable the sensors, they can use ransomware encryption to prevent the executable system files that interact with the HMI system, thus locking out the administrators who control those systems.

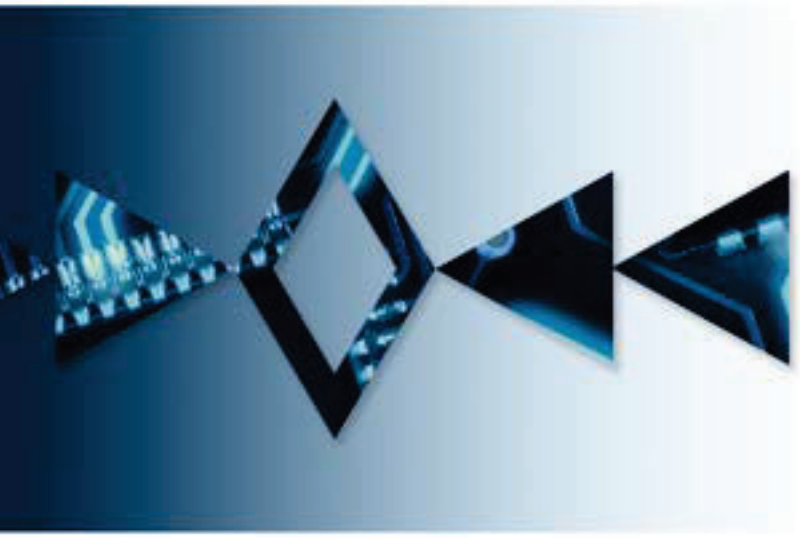
Enterprise organizations should consider adding Occupant Emergency Plans (OEP) and Crime Prevention Through Environmental Design (CPTED) to secure their facility.

- OEPs often focus on personnel, safety, and general property damage prevention rather than addressing specific areas of IT such as business continuity planning. OEPs provide guidance and safety monitoring in order to: sustain personal well-being, minimize threats to life, prevent injury, manage distress, handle travel, and protect property damage from destructive physical events in the wake of a disaster.
- CPTEDs reduce the opportunity for a crime to occur through natural surveillance, access control, territorial reinforcement, and space management such as fences, gates, and guards.

Another type of human-based ransomware is done through the use of pop-ups on a computer screen. The attacker prompts them to appear with verbiage such as 'Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a $100 fine' or 'Your computer has been infected with a virus. Click here to resolve the issue'. From here, they take advantage of the user via backdoor malware variants that can be triggered through clickjacking or drive-by malware downloads.



Most often, attackers, once compensated, will comply and abdicate the decryption key, relinquishing the data back to the company. They do this to gain trust in their reputation. A cyber attacker that doesn't give the encryption key back will likely be denied their ransomware payments at another company, because that company is of the understanding that they will be denied their data, even if they paid for it.



USEFUL SECURITY MEASURES

The requirements of today's technology elicit the need for resilient, reliable systems that resist compromise. Configuring the firewall to block outbound connections, isolating the domain controller during the recovery phase of incident management, and review and monitoring of Group Policy Objects (GPOs) are a few methods of protection.

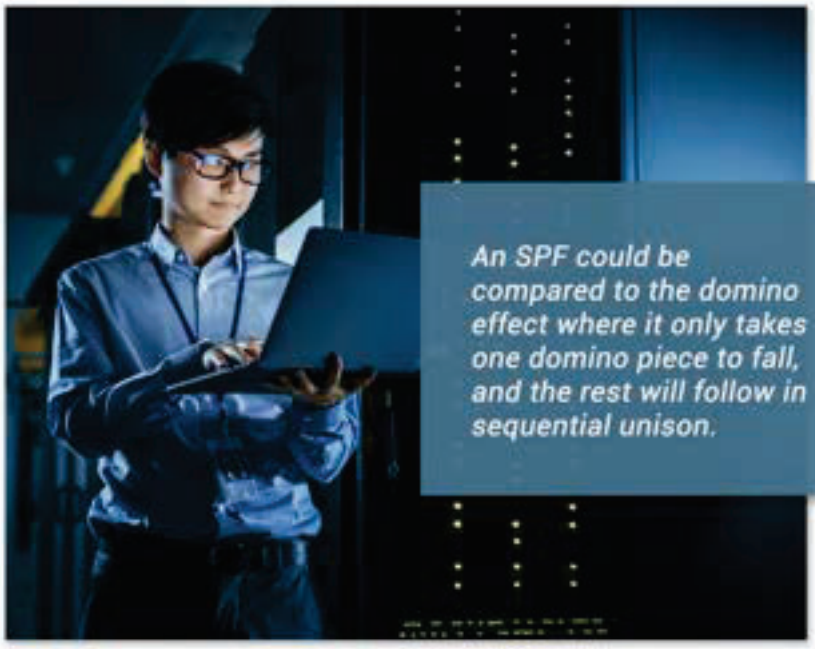
GPOs are made up of a virtual collection of centralized management features and configuration settings that control the user/computer accounts within an OS environment. There are also methods that may be currently in practice and require revisiting in order to be sure the system is resilient and safeguarded.

Forget the SPF

Single Point of Failure (SPF) is a system that entails one single component or process, simplifying the design of the system and reducing cost by eliminating redundancies. It also allows for continuity. Examples of SPFs include a server, a network connection, a power supply, a storage system, or a software application.

Although less complex and often less expensive to monitor and maintain, the downfalls of SPF far outweigh the benefits. Such a configuration poses a risk because if it fails, it will cause the entire system to fail. Because malicious access into an SPF can be detrimental to the entire system, businesses need to enlist a backup plan or redundancy measure in case something goes awry.

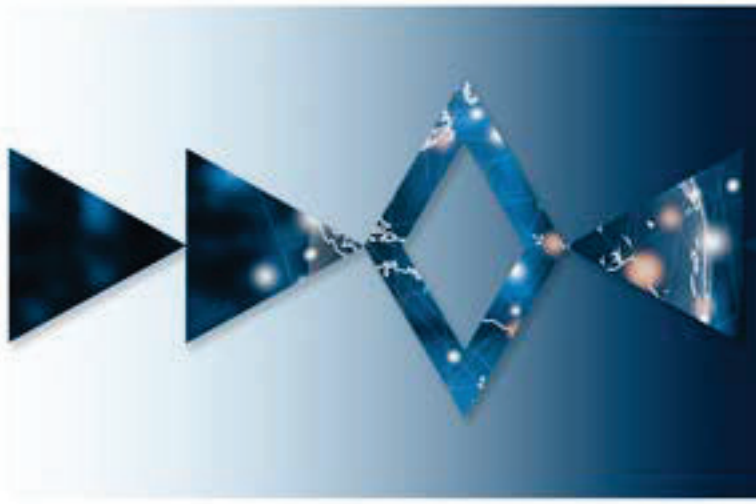
An SPF can also define multiple systems connected to one entity. Normally, attackers try to enter the network through hidden areas such as



An SPF could be compared to the domino effect where it only takes one domino piece to fall, and the rest will follow in sequential unison.

unsecured channels, unused ports, firewall evasion, back doors, Trojans, and tunnels with the use of root kits. Even with a connection of multiple systems, if a primary SPF host goes down, the rest falls behind it. Because of this, attackers are keen to compromise jump servers which funnel information through firewalls, providing different zones of security to the devices on the network.

Situations of multiple network resources relying on one server to operate and stay efficient offer prime target zones for cyberattacks. Criminals target SPFs or C2 centers because their goal is to traverse the network environment to have access to full control of the computer systems, or to eliminate processing functions in their entirety, rather than one by one.



Set up Network Segments

Establishing a system for network segmentation is a necessity. Separating the production, testing, and isolated networks provides a layer of protection between the sensitive, proprietary data on the internal network and everything outside of the network.

Segmentation can be accomplished by establishing Virtual Local Area Networks (VLANs). VLANs are broadcast domains that group together a subset of devices to isolate network traffic over a shared physical LAN, partitioned over a virtual overlay on a logical network. VLANs create a virtual network within a physical one, allowing for multiple users, locations, and departments to access their various resources independently of one another.

Networks that are separated lead to computers that are standalone, which provides good defense in managing technical threats. Because they are segmented and aren't connected to the systems on the production network, they offer a barrier in an unlikely event that a virus or worm were to run rampant. Network segmentation is a powerful risk mitigation tool.

Isolate the Processes

Another measure of security is process isolation, which creates separate environments for running applications. This isolation protects the entirety of the environment from being affected, in the event that the program contains malicious code. Process isolation is used to avoid race conditions which happen when two concurrent threads or processes try to change at the same time. Doing this can cause unpredictable behavior, as the resource may be changed or corrupted by one of the processes. Isolating assures that process activities are protected

while they are in memory by separating them to avoid one process from affecting another on the operating system.

Be Aware of the RDP Network

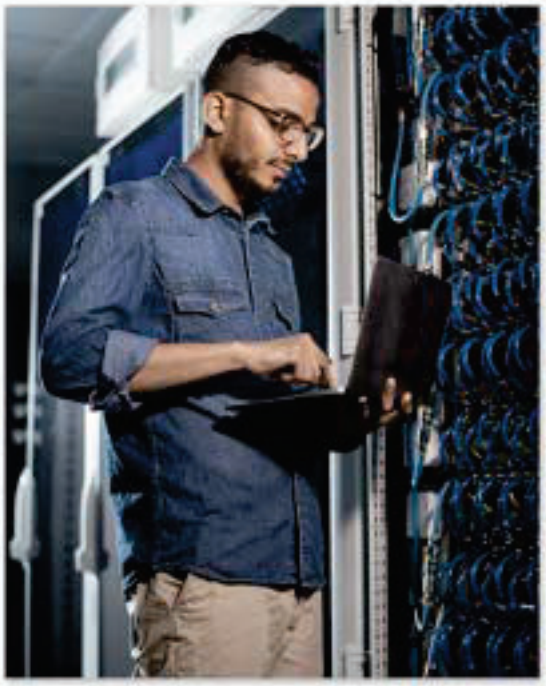
Attackers are also savvy users of Remote Desktop Protocol (RDP) to gain entry to a system through port 3389. This port provides remote network access. Because of this, port masking or administrative privilege restrictions need to be a requirement for users that utilize this port. Through an internet service manager, users are able to change their port default number to an import number of their choice. This helps to avoid a cyber compromise and add protection to the server, making it harder for the attacker to find it.

To engage in RDP, the system administrator:

- Enters the settings and a port registry subkey
- Chooses the decimal base
- Enters the desired port number that they wish to change to

Forwarding and Mirroring

- *Port forwarding* is a technique used to give external devices access to computer services on private networks. This is done by mapping external ports on a router to redirect incoming data traffic to internal IP addresses and ports. Port forwarding provides a layer of security by preventing unwelcome traffic from reaching the internal network.
- *Port mirroring* or port monitoring involves copying incoming and outgoing network traffic from one port to another port. This allows network administrators to monitor and analyze the traffic and detect viruses and malicious activity.



Network monitoring and security audits play a critical role in assuring that the attack surface is reduced to an acceptable level. Confidentiality is key to protecting information against outside threats both in the logical realm, and in the physical world. The art of cryptography and its applications are used as defensive mechanisms by nature, by providing privacy, authentication, and security of information for the average system users.

Behavior-based detection tools specifically aimed at encryption-related ransomware efforts are currently being developed to lure attackers into 'bait' files to trigger a ransomware takedown action. These tools can fight against ransomware by finding and identifying abnormal encrypting activities on the network. They have the capability of fixing corrupted files as well as providing backup copies of those corrupted files.

Threat prevention also extends outward to make sure that threats don't make their way inside the organization, giving the threat the opportunity to manifest in the first place. Securing the perimeter of business IT is much like repairing an open hole in a fence, or redirecting security cameras to make sure they are pointing in the right directions. The structure is in place, however, requires maintenance to enforce and strengthen it as time and threats morph on. The process of preventing threats involves implementation of solutions and policies together, to protect the network perimeter along with the digital infrastructure as a whole.

DECRYPTION RESOURCES

Tools exist that decrypt ransomware files and allow for system restoration. Malwarebytes is one solution of many that provides an effective measure for decrypting files. Formerly known as Advanced Malware Protection (AMP), Cisco Secure Endpoints, a system-friendly and centralized approach that works in conjunction with the Cisco umbrella and Duo (for mobile platforms). They work together to detect, protect, and remove viruses with an added feature for network traffic analysis.

Similar to Norton's anti-virus products, Avast and Bitdefender offer tools that are owned by their brand and available for downloading. BitDefender's anti-ransomware support includes the decryption of files, and their 'Decryption Utility' is used for variants of malware such as DarkSide. Avast's website provides decryption hotfixes using '.exe' for files infected with ransomware. The versatility of both offers tools that are easily scalable.

The best defense is proactivity in guarding your system and data before a ransomware attack occurs. The CVE and NIST have databases that provide continuous updates, keeping cyber experts aware of the latest in security management. If you do become the victim of an attack, it is imperative to act quickly and appropriately, enlisting the right tools to decrypt the ransomware files promptly, getting your business back on track as soon as possible.

ENLISTING A CYBER PARTNER

Cybersecurity in business is a must-have. Without question, making sure that your business has the appropriate measures in place is of the utmost importance. It can, however, seem overwhelming.

Cayuse's Cybersecurity Team combines industry-leading expertise with Department of Defense experience in protecting critical assets, recovering from attacks, and maintaining business operations against today's threat actors. Partnering with our clients and supporting their critical business operations is our mission.

For more than 16 years, Cayuse has served as a technology partner to our clients. Our cybersecurity team holds a combined tenure of over 35 years, along with multiple certifications including: CISSP, CCNA, Certified Ethical Hacker, CSAP, and CBCP.

Learn more about how our team at Cayuse can make sure that your business is ready for the unexpected. Contact us today!

Steve J. Bankhead
Senior Managing Director
Cyber & Operational Resilience
Steve.Bankhead@cayusecs.com

www.cayusecommercialservices.com

Cayuse Commercial Services is part of the Cayuse Holdings family of companies.