TETRA
TOP TEN

740 REGENT ST., STE. 203, MADISON, WI 53715
+1 (608) 509-4445
TETRADEFENSE.COM

THE TETRA TOP TEN

In cybersecurity, there's no such thing as an isolated incident. A glaring, obvious security flaw is often the product of several other discreet, under-the-radar ones. When it comes to the ransomware cases we investigate daily, we see connections in tactics, tools, and even the known exploits attackers may leverage.

All attacks, no matter their impact or media coverage, share a recurring theme: there are simple, and oftentimes inexpensive preventative measures that can be taken before disaster strikes — or to avoid one altogether.

OUR APPROACH

Cybersecurity is constantly challenged by opposite (and often stronger) forces meant to break it down. When attack plans are constantly executed against you, *agility* is required to side-step, thwart, and defend. In the spirit of agility and moving as quickly as the opponent, Tetra Defense offers the ten most easily implemented, most effective security "wins" first.

Informed by a team of experienced security professionals, internal threat intelligence, industry reports, and custom tools, Tetra prioritizes what is often an overwhelming list of security to-dos.

Through the Tetra Top Ten, your organization can achieve the most effective security "wins" all while thwarting the most common ransomware attack vectors we see daily.

1

Hardening & Patching of External-Facing Systems

What it is:

One of the most common misconceptions related to cyber attacks is that cyber criminals operate by targeting individual companies. While that may happen to the biggest companies, for small-mid size businesses, the cyber criminals most often are targeting your organizations' vulnerabilities, not your company.

Every service and system an organization leaves exposed to the public internet is at risk of being compromised. For externally facing devices, it is important to eliminate as many security risks as possible — a process known as "hardening" devices. This is extremely important, as having vulnerable externally facing devices are among the most common ways threat actors can gain a foothold in your network

Why it's important:

Cyber criminals often use scanning tools to find any computer in a certain area that has a vulnerability that they know how to exploit. After performing this scan, they may have a list of hundreds, or thousands, of computers that have this vulnerability. Then, one by one, they'll exploit those vulnerabilities. Only after they've exploited that vulnerability and gained access to the network will they find out whose network they've actually compromised.

Ransomware operators are actively exploiting unpatched, external-facing systems like firewalls and email gateways. These servers are often assumed to be highly trusted within (and have wide-ranging access to) a network, making them the perfect entry for a threat actor. Ideally, all systems would be patched and up to date, but external-facing systems are a top priority because of this ongoing, malicious scanning and its constant stream of vulnerabilities.

Here's what we recommend:

In order to protect against this common exploitation vector, Tetra recommends the following tasks:

- Identify external-facing systems by looking up IP addresses and DNS subdomains for your organization.
- Block public access to the services Remote Desktop Protocol (RDP), Secure Shell (SSH), Telnet, and File Transfer Protocol (FTP).
- Ensure external-facing systems (such as firewalls, VPN gateways, and email gateways) are patched.
- Perform vulnerability scans against external-facing systems.
- Choose website and e-commerce hosting providers that are dependable and secure.
- Avoid hosting commonly attacked services like WordPress internally.
- Configure automatic updates on workstations and laptops where feasible.

Tale from the trenches:

Microsoft Exchange is an email gateway used by many organizations to send and receive email. Organizations that host Exchange on-premises (unlike Microsoft Office 365 or Google Apps that are hosted in the cloud) have to handle patching and secure configuration of all infrastructure.

In a recent ransomware case handled by Tetra, a threat actor was able to exploit a vulnerability in Microsoft Exchange that allowed them full privileged access to the Exchange web server. The threat actor was able to install Cobalt Strike, a threat emulation software used by both legitimate security professionals and threat actors. Within a few minutes of exploiting the server, Cobalt Strike was used as a Remote Access Trojan (RAT). Within 90 minutes, the threat actor was able to deploy LockBit ransomware.

This case did not rely upon user interaction to initiate its chain of events. This threat actor

took advantage of excessive permissions granted to several users and the lack of network segmentation to quickly bring the organization down. Luckily in this case, the victim organization was able to recover from backups, yet exploits like this are still a textbook example of why it's critical to ensure that external-facing systems are up to date and have settings configured securely.

Services to consider:

Organizations can keep track of vulnerabilities by subscribing to email updates from vendors, using services like Shodan.io to monitor their external footprint, or purchasing scanner services to check for exploitable vulnerabilities.

Low cost and/or free tools like PDQ Deploy, Chocolatey, and even Windows Update are available to handle these update deployments. Organizations should also consider utilizing cloud services like Microsoft Office 365 or Google App Suite instead of hosting external-facing services on-premises.

2

Protect Remote Access with Multi-Factor Authentication

What it is:

Two-Factor or Multi-Factor Authentication (MFA) is a security setting available on many everyday tools and programs. This security feature works upon login — when a user inputs a legitimate username and password, a second barrier requires a response to access the account.

This barrier typically requires a user to input a code (either from SMS or generated from an app like Google Authenticator), respond to a prompt (like Duo or Microsoft Authenticator), or plug in a security key. Authenticating any or all of these barriers helps ensure that the person trying to access the account is actually the person to which it belongs.

While effective, MFA can be cumbersome. The time it takes to retrieve a new device or remember an oddly specific answer sacrifices convenience, especially when websites and tools can "remember" an account on a user's behalf. Despite the inconvenience, we cannot stress the importance of this security setting enough. MFA effectively blocks access from threat actors that may have acquired account credentials through malware, phishing, or other methods. If the malicious actors attempt to login using these credentials, but they cannot retrieve the code delivered via text message or app, they will not be able to gain access to the system.

Why it's important:

Strong and unique passwords for accounts are no longer enough to protect accounts from unauthorized access. There are many other ways usernames and passwords can be compromised, and it's safe to assume that with enough effort your username and password could be stolen or guessed. This is exactly what MFA protects against.

Threat actors constantly scan the internet in hopes of accessing external systems. They are equipped with stolen username/password credentials — some of which come from other websites or organizations that suffered a breach (typically called a "credential stuffing" or "credential reuse" attack), some of which are purchased from the dark web as a result of these breaches, or other successful incidents that involve the use of credential-harvesting malware.

Here's what we recommend:

Tetra recommends organizations configure MFA for all external-facing and remote-access systems, including cloud services and Virtual Private Networks (VPNs). Tetra especially recommends MFA for initiating banking transactions — these accounts take priority considering they harbor a greater risk of being compromised by threat actors from the public internet. For greater protection, Tetra also recommends MFA for access to internal management tools like firewalls or privileged accounts.

Tale from the trenches:

In a recent case, a company used a VPN equipped with geo-location blocking, a control that blocks access from threat actors trying to log in from improbable locations. For example, if a user typically logs in from Madison, Wisconsin, but then a short time later attempts to log in from Moscow, Russia, the control will block this improbable login. Using this safeguard, the company allowed employees to work remotely using personal devices, with access determined by their VPN.

Unfortunately, one employee's home computer had pre-existing malware — one with the ability to scrape credentials. In having access to this home computer, the threat actor behind the malware was able to access the VPN with scraped credentials, and thus access the corporate network. Once inside, they were able to deploy ransomware.

This is an example where MFA could have prevented the corporate network access when

focusing on the VPN alone. It is important to note that while effective in protecting accounts, MFA could not address the malware that had already compromised this user's home laptop. This is where best practices in taking inventory, hardening, patching, and network scanning would come into play.

Services to consider:

The Tetra Defense cyber risk team has worked with a variety of tools that deploy MFA. Some are often built into popular software/operations systems, but other tools include:

- Google Authenticator
- Duo
- LastPass
- Microsoft Authenticator

Another tool to consider for MFA would be physical tokens such as YubiKeys.

3

Protect Users with Email Security Gateways

What it is:

If a malicious message makes its way to an end-user's inbox, an entire network's security falls into the hands of that user. While education and awareness training are important, a safer bet is to keep bad emails from reaching inboxes to begin with.

An email security gateway acts as a protective barrier between emails from the outside internet and individual inboxes within a network. Gateways should scan incoming attachments and links within messages, only allowing those that are trusted to be presented to an end-user. Rather than relying on an end-user's instinct, an email gateway effectively helps ensure that a malicious email is never even read.

Why it's important:

Many of the ransomware incidents we respond to, even for large organizations, can begin with just one email to a single user. Since this method of entry is still so prevalent, we emphasize strong email filtering, scanning, and preventive controls as a critical safeguard. Well-configured email gateways are recommended as of late since traditional spam filtering no longer thwarts even the average ransomware operators from deploying their tools.

Here's what we recommend:

To protect against the threats that are directly sent to users, Tetra recommends the following priorities:

- Ensure email is filtered using scanning technology that can open attachments and links to find advanced threats.
- Quarantine or block documents that are password protected as threat actors often use these to bypass scanning.
- Ensure that these attachment types are blocked by email gateway, at a minimum.*
- In addition to what Microsoft recommends blocking, file extensions like .iqy, .xlsm, .xltm, .xlam, .xlsb, .dotm, .docm, .pptm, .ppsm, .ppam, and .potm are often used to deliver malware and should be quarantined or blocked.

*Blocking email from suspicious or unwanted senders involves adding individual senders, or entire categories of senders, to a 'block list' that will prevent those suspicious emails from ever reaching your users' inboxes. A malicious email usually requires some action by a user (clicking a link, opening an attachment, etc.) in order for the threat contained in that email to 'activate.' By blocking those emails, you can prevent harmful malware from entering your network.

'Blocking' can be done in a few ways. You can block individual senders ('attacker@suspiciousemail.com'); you can block entire domains (e.g. blocking all emails from '@suspiciousemail.com'); and finally, you can block based on the origination location of the emails (e.g. blocking all emails from an entire group of countries).

Tale from the trenches:

In several recent cases, Tetra has responded to ransomware incidents that struck several days or even months after a user opened an email containing a malicious document. In one incident, a user at a satellite office received an email containing a password-protected zip archive. The email included the password for it, and within that zip archive there was a malicious Word document. Once the user opened the Word document, a command-and-control beacon was installed on the workstation, and over a month later, a threat actor returned to steal data and encrypt the network's main servers with ransomware.

Another major threat that can be thwarted with email gateway protection is Business Email Compromise (BEC). Tetra Defense has investigated many Microsoft Office 365 cases where proper framework policies (email gateway, sandboxing, etc.) were not employed in the

environment. A recent case involved a fraudulent invoice being paid in the amount of $900,000 — the request coming from what looked like an internal account that was actually a spoofed email. In this case, an email gateway protection policy could have noticed this email impersonation and flagged it as “external” or quarantined it.

Services to consider:

For users of Microsoft Office 365, we recommend their instructions for setting up an email gateway, as well as their insight on which file types to be on the lookout for. Some organizations can set up impersonation protection for their employees as well. Organizations should configure mail flow rules to block or quarantine potentially dangerous attachments such as password-protected files.

Google Apps also includes several features for attachment protection and impersonation protection that should be enabled.

QUESTIONS TO CONSIDER

- Do you have a way to detect and respond to successful email phishing attacks?
- Do you automatically lock or quarantine inbound email from suspicious or unwanted senders?
- Do you automatically scan inbound and outbound email attachments and links for malicious content?
- Do you customize the security settings of your organization's email software to better protect users and workstations?
- Do you regularly train users on how to detect phishing emails and report them?

4

Ensure Critical Data is Backed Up and Can Be Restored

What it is:

It's happened countless times: a slip of the finger leads to an important document disappearing. Hours' worth of work was recorded on an external drive, but then dropped, never to be accessed again. Just when all hope seems lost, system and data backups are there. If there is a hardware failure, an accidental deletion, or any other kind of data loss situation, backups are what can recover important function or data.

For these everyday cases, backups are important. In the case of ransomware, backups are vital. When a ransomware incident encrypts critical data, backups are the first possible remedy. This is why they are also a prime target of threat actors.

Why it's important:

In many ransomware incidents, backups are often targeted, encrypted, or completely deleted by threat actors. This goes beyond primary or live data — threat actors spend the extra time it takes to search a network to find all backups and encrypt them as well. Corrupting backups through encryption or deletion gives threat actors significantly more leverage when demanding a ransomware payment. If a victim organization can't retrieve data from their backups, they may consider paying for the data that the threat actor encrypted.

Here's what we recommend:

Follow the 3-2-1 backup strategy:

- 3 – Keep 3 copies of any important file: 1 primary backup of the live data used daily, and 2 backups of it.

- 2 – Keep the files on 2 different media types to protect against different types of hazards. These copies are meant to be on-site, or at least easily accessible, to restore quickly from most incidents. This helps recover quickly from server failure, accidental deletion, etc.

- 1 – Store 1 copy offsite (e.g., outside your home or business facility). This recommendation started in case of physical disasters like fires or floods within the four walls of an organization. In the case of remote working, this strategy is more effective when backups can be stored "off" of the organization's network. Physical space is less of an issue in many cases we respond to, especially when employees can work within one network, no matter where they may be physically located. The same applies here — without proper protections, this copy can appear to be on the same network and can be just as easily reached by a threat actor.

In addition to following good backup practices, organizations must regularly test restoration of backups. If you can't restore from the backups you're saving, then they are rendered useless.

Beyond configuring backups and testing them through restores, we also regularly find that organizations with extra storage capacity to hold copies of live systems can recover more quickly after a ransomware incident. During a ransomware incident, Tetra often recommends organizations take backups of encrypted data prior to recovery in order to keep forensic data for an investigation, but more importantly, to preserve encrypted data in the event that a decryption tool does not work as hoped. A stretch goal for an organization's backup strategy is to ensure that the organization has enough storage capacity to take backups of all live systems for preservation during an incident.

Tale from the trenches:

While many factors influence whether or not a client has the option to forgo paying a ransom, the most common scenario is when they have properly operating backup systems that can be restored easily.

Tetra Defense had a case where a client had a recurring infection of Emotet and Trickbot, bringing in the Ryuk ransomware, and encrypting all production data. Luckily, the client regularly restored data from protected, offsite backups each time, and returned to business within a day. After the Ryuk ransomware hit them for the fourth time, they contacted Tetra Defense and asked for assistance. Had proper procedures been ignored, it's very likely that in one of these incidents, the threat actor would have also encrypted or destroyed all backups, prompting a potential ransom demand as high as $400,000 for their industry.

The most widespread problem we see regarding backup practices in the cases we respond to is the network segmentation of backups. Many organizations are well-prepared and have good systems to protect against physical failure of equipment, but these practices do not protect against a ransomware incident. Even if they are in different physical locations, if the threat actor can encrypt the backup systems, then they won't be helpful for restoring after the ransomware is deployed.

Services to consider:

Our team crosses paths with numerous tools and services through our work. When it comes to backup methodology, here are some of our fan favorites:

- Veeam
  Backup & Intelligent Recovery, DR Orchestration, Cloud mobility, Copy Data Management, Monitoring & Analytics
- Datto
- Acronis
  Safeguards your data from recent ransomware strains.
- Synology
  Protection against encryption-based ransomware.

5

Endpoint Detection and Response Agents

What it is:

Traditionally, organizations deployed antivirus (AV) solutions to thwart threat actors in their environments. Traditional AV relies upon an extensive list of file names, file characteristics, and other static indicators to find the malicious tools used by threat actors. These days, threat actors have changed their techniques and tools so that one list of suspicious file names will no longer cut it.

As a result, Endpoint Detection and Response (EDR) tools have been developed that analyze the behavior of systems to find threat actors from not-so-obvious angles — these tools look beyond a single file based on a single set of known characteristics.

Why it's important:

While many actors use tools that simple AV mechanisms can detect and block, other attacks may rely upon several chained techniques for a threat actor to perform their actions. We also frequently encounter tools like Mimikatz (used for harvesting credentials) that are not blocked by traditional AV. Both AV and EDR tools must be in place, well-configured, and constantly monitored to ensure that systems remain secure.

Here's what we recommend:

Tetra recommends implementing an EDR tool like SentinelOne to an organization's defenses. These tools not only have advanced detections compared to traditional AV, but they also have tamper protection which will prevent a threat actor from removing detection mechanisms.

Tale from the trenches:

A recent case that Tetra responded to involved a client who's IT staff had installed a robust AV solution on all systems but one, which only used an outdated version of Windows Defender. Analysis revealed that the robust solution was able to block the execution of Emotet, which is known to be associated with Trickbot and Ryuk ransomware as a bi-product. Although other systems were protected against Emotet, this one system allowed Trickbot to install on it, which led to the download and execution of Ryuk ransomware which hit the major servers within the environment.

Tetra was also able to assist a Managed Detection & Response (MDR) client with preventing a Ryuk ransomware infection delivered through BazarLoader malware. Tetra was able to alert the client upon behavior known to be associated with BazarLoader malware rather than specific, known characteristics of file-based malware. With this behavioral insight, Tetra was able to alert the organization quickly and prevent further infection.

Services to consider:

EDR tools like SentinelOne are a good example of a more robust protection against the latest malware compared to traditional AV.

To learn more about Tetra Defense Incident Response operations and SentinelOne, visit our website here:

6

Privileged Access Management

What it is:

This concept refers to the “principle of least privilege.” Employees should only have access to the systems and data that are required for their job. For example, human resources staff do not need the personal data of clients, and sales staff do not need records of each employee. Similarly, privileged users like system administrators do not always need to act as privileged users to do everyday tasks like checking email.

Why it's important:

Aside from strategic business reasons, limiting and managing privileged access ensures that threat actors have a harder time of elevating their permissions to infiltrate an organization’s network.

If an attacker is able to access an account, they will attempt to escalate its privileges and access as many parts of your network as possible. Making sure that all accounts in your organization have limited access to only the relevant areas needed to do their job.

Here's what we recommend:

- End users should not be local administrators on their endpoints used to check email or other web-related tasks.
- Employees with administrative privileges should have separate privileged and non-privileged user accounts.
- Administrative credentials should be issued individually. Shared logins are often a target for threat actors and make it difficult to determine the root compromise of a security incident. If an organization uses shared logins, those should be stored securely in a password manager rather than a document on a file share.
- Administrative credentials should not be able to log in remotely using tools like a VPN. Instead, an employee with an administrator account should first log in to a VPN with a non-privileged account and later escalate privileges, preferably on a trusted administrator host.
- Organizations should create multiple tiers of administrators. For example, Help Desk often does not require full domain administrator privileges, and can have an administrator account created with password reset privileges, but without full server administrator rights.
- Organizations should regularly review and audit the membership and usage of administrative credentials. Finding new administrative accounts should be an alert for an organization.

Tale from the trenches:

In a recent ransomware case, a threat actor was able to compromise one workstation and then use those credentials to log into another host in the network. Once the threat actor moved to the second host, they were able to gain administrator credentials and then steal data and encrypt the file server. If the first user account had been prevented from logging into other hosts through privileged access management, it would have been more difficult for the threat actor to achieve their goals.

In a Business Email Compromise (BEC) case, a Microsoft Office 365 user with Exchange Admin privileges received a phishing email designed to steal credentials. The user visited a phishing page and unknowingly gave the threat actor their credentials to log into Microsoft Office 365, granting the threat actor Exchange Admin access to their organization. With this access, the threat actor was able to act as multiple users in the organization and steal more than $200,000 with several different forms of invoice fraud and manipulation.

If the user account had not been granted Exchange Admin privileges, the threat actor would not have been able to perform the invoice fraud on behalf of other users. While this attack is considered to be a simple BEC, the threat actor could have used these credentials to conduct other attacks, such as impersonating the user and then sending ransomware.

Services to consider:

Managing privileged access requires providing users a secure place to store secrets like passwords, along with managing privileged access accounts effectively. Organizations should encourage the use of password managers such as LastPass to ensure shared passwords are not stored in easily found locations on a network. HashiCorp Vault is another tool that can be used to manage passwords and other secrets.

Organizations with on-premises Active Directory should implement Local Administrator Password Solution (LAPS) from Microsoft to manage local administrator accounts on endpoints.

Windows PowerShell includes Just Enough Administration that can be used to constrain administrative privileges.

Tools like CyberArk, Centrify, BeyondTrust, and Okta can all be leveraged to manage privileged access.

KEEPING ACCOUNTS REINED IN ON ONLY THE ACCESS THEY REQUIRE WILL HELP SHRINK YOUR ATTACK SURFACE

7

Network Segmentation

What it is:

Network segmentation, in very general terms, means limiting what portions of the network can talk to each other. For example, typical employee users on a network should not have access to a backup archive for the entire organization — “access” not defined as a password that would allow entry, but “access” defined as “physically incapable of being available” within this segment of the network.

Why it's important:

Ransomware operators scour and search through a network once they have access, strategically exploiting access wherever they can inflict the most damage. During the initial phases of an intrusion, a threat actor will try to map out where they can gain access to administrator credentials and then find storage servers, backups, and other systems of value. When deploying ransomware, the operators will use various network protocols to initiate ransomware and encrypt as many systems as possible. The threat actor’s mission is much more difficult to accomplish when organizations leave as few avenues of attack as possible.

Here's what we recommend:

Access between workstations and servers should be limited based on need or job function. In smaller organizations, this may be hard to separate, but in larger organizations this can be easier to distinguish.

- Internal network access should be limited by the following parameters:
  - Public-facing servers (such as web servers) should be isolated in a perimeter network or "DMZ." This should have limited ability to communicate within your organization.
  - Server Message Block (SMB) traffic should be blocked from reaching workstations or servers that do not need it, such as domain controllers or file servers.
  - Access to Remote Desktop Protocol (RDP) ports (such as TCP 3389) within your network should be limited or blocked except from trusted administrative hosts within the network.
  - Access to infrastructure management (routers, firewalls, virtual machine hosts such as VMware, etc.) within your network should be limited or blocked except from trusted administrative hosts.
- Egress from your network should be limited.
  - Block unnecessary outbound ports. In addition to blocking SMB internally, organizations should block traffic going to the internet on port 445 as well. Organizations should block ports like 4444 (Metasploit) and 50050 (Cobalt Strike).
  - Organizations should use firewall application categorization (such as Palo Alto App-ID) to block malicious applications along with services that threat actors are known to use to exfiltrate data (such as MEGA.nz and Sendspace).
- Domain controllers (and other critical infrastructure that does not require internet access) should be blocked from communicating with the internet.
- Domain controllers should not host multiple functions — their only purpose is to be a domain controller. If you need a file server or accounting server, separate those functions out. Domain controllers and many other servers should not have the ability to initiate connections with workstations and laptops.
- Outbound DNS queries should be filtered through internal servers and logged. Threat actors are often able to leverage tools like DNScat to make covert command and control connections from a victim network. Workstations and servers should not be able to directly communicate with the internet on port 53.

Tale from the trenches:

In every ransomware case we work, once threat actors gain initial access to a host, they start attempting to steal administrator credentials. Once the threat actor has administrator credentials, they can move from their first point of entry to domain controllers and file servers either using SMB tools or Remote Desktop. The threat actors will then use those same protocols to deploy ransomware. Ensuring these protocols are limited makes it much more difficult for a threat actor to take down an organization with malware and gives your organization more time to react.

Services to consider:

To facilitate network segmentation, organizations should use a combination of host-based firewalls like Windows Firewall along with a network firewall.

DNS resolvers such as Quad 9 and Cisco Umbrella can be leveraged to block suspected malware from reaching target servers. Other solutions like Infoblox can be used to further analyze suspicious domains.

Threat intelligence feeds such as RiskIQ and DomainTools can give organizations real-time information on IP addresses and domains to block.

IN CYBERSECURITY, NEW DISCOVERIES ARE MADE POSSIBLE THANKS TO THREAT INTELLIGENCE.

8

Logging, Monitoring, and Alerting on Traffic

What it is:

Computer software and operating systems generate many different types of logs that record activities and who performed them. Nothing gives a clearer view into what actions a threat actor took once they got into your system than detailed logs. If well-configured and reviewed regularly, they can help you detect the presence of a hacker within your network sooner rather than later.

Why it's important:

Audit logs are important not only for investigating how a cybersecurity incident occurred, but also aid in answering questions (should there be any) related to privacy liability. Logs not only answer, “Who did it?” but also answer, “What did they see and do?” Audit logs, network logs, and file system metadata can help answer whether threat actors were able to view or steal data, which can help limit the liability of an organization in the event of an intrusion.

Here's what we recommend:

- Ensure that audit logs are configured according to best practices recommended by Microsoft, CIS Benchmarks, and/or DISA STIGS to ensure appropriate events are stored.
- Ensure that network devices are logging all network flows.
- Configure systems and network devices to ship logs to a centralized log storage platform such as a Security Information Event Monitor (SIEM) or Security Orchestration, Automation, and Response (SOAR) system.
- Organizations with cloud services should ensure they are enabling all alerting and retention options available.
- Configure SIEM and SOAR to alert on malicious or suspicious activity identified using rules frameworks such as SIGMA.

Tale from the trenches:

Ransomware is prolific in that its malware scans a network and targets systems and attached drives to encrypt. In most cases we've observed that are associated with ransomware, we either see evidence that a threat actor has used a tool to clean the logs, selective cleaning over a certain time period of activity, or the logs have exceeded the 20MB default size limit. This prevents the analysis from determining possibly how the attack vector occurred, or how the threat actor or malware moved laterally around the network.

With inaccurate or unorganized logs, threat actors can easily cover their tracks. Catching a threat actor red-handed may be a difficult feat, but logging is what can ultimately prove their actions to thwart any new ones from happening.

Services to consider:

There are several logging platforms currently available, many of which require tuning to ensure proper coverage for alerting on suspicious activity. These include free and/or open-source solutions such as Elastic or OSSIM, along with commercial solutions such as Sumo Logic, Splunk, LogRhythm, or QRadar.

9

Complete Inventory and Patch Management Cycle

What it is:

Once again, knowing the inventory of devices is a highly recommended practice within an organization — you simply can't secure what you can't see, or what you don't know exists. Without this inventory, it is impossible to know which assets are up-to-date and which need to be updated or replaced. Addressing both inventory and patching in a constructive way will ensure that these vulnerabilities do not have a place on your network.

Why it's important:

A complete inventory is going to be important for an organization to accomplish — the Center for Internet Security even recommends this as their number one safeguard. However, in terms of how ransomware most often operates, having all possible applications identified and patched is much less critical than getting the easiest points of access closed.

Ideally, all systems should be patched, but if there are systems not exposed to the internet without external egress to the internet, the risk posed by not patching immediately is decreased.

Here's what we recommend:

Implement a patch management system, ideally on a tool or device-specific basis. Monthly or weekly patches are better than not updating at all, but the best possible schedule is to automatically update all tools and services as soon as updates are available.

Tale from the trenches:

A recent ransomware investigation relied upon an out-of-date operating system and web browser to launch an initial infection.

While conducting research, the end-user of a workstation on the victim's network browsed an article on a newspaper website infected with a known exploit toolkit. The page automatically downloaded a fake Google Chrome update to the workstation, complete with a prompt for the user to launch the update. The unsuspecting user ran the toolkit and downloaded a trojan, all the while believing they were updating their browser. This activity gave the threat actor remote access to the endpoint, which ultimately allowed them to deploy ransomware.

This infection relied upon user interaction to initiate its chain of events, however the exploit in question was targeted to run on a Windows 7 workstation. If the workstation had been running an up-to-date operating system, the exploit would have failed. Exploits like this demonstrate how crucial it is to keep workstations' operating systems up to date, with default settings configured securely.

Services to consider:

Similar to monitoring the external vulnerabilities that offer threat actors an entry into a network, organizations can keep track of all vulnerabilities by subscribing to email updates from vendors, using services like Shodan.io to monitor their external footprint, or purchasing scanning services to check for new exploits.

Low cost and/or free tools like PDQ Deploy/Inventory, Chocolatey, and even Windows Update are available to handle these update deployments. Windows Intune can be utilized by organizations with applicable Microsoft 365 subscriptions to maintain patching. Other tools such as Automox and SCCM are available to maintain patches as well.

10

Security and Awareness Training

What it is:

Security awareness training is arguably the most approachable aspect of cybersecurity considering it is meant to educate all end-users within an organization. Several practices exist such as phishing simulations that yield detailed reports, lesson modules that teach the latest social engineering scams, among many other teaching methods to foster a better understanding of cybersecurity across an organization.

Why it's important:

Ensuring users are aware of what they click on is important, but if you're implementing good systems with Tetra's Top 2 (MFA), 3 (email gateways & scanning), and 5 (EDR blocking), then phishing becomes less of a risk. As an organization begins to mature its network segmentation and other controls, then phishing becomes even less of an option — the threat hopefully never makes it to an end-user's inbox.

Here's what we recommend:

Of all aspects of an information security program, this is the one that most non-technical users might be (or at least should be) aware of. On Tetra's prioritized list, we do not mean to downplay its importance. What we want to foster is a more robust cybersecurity environment that keeps the safety of the entire network less in the hands of individual users, and more in the proven technical practices that thwart ransomware. A phishing simulation or an awareness campaign does not make a secure company, but it does help to equip end-users with the skills they need to keep their endpoints safe (and keep their online behaviors safe while off the clock as well).

Tale from the trenches:

Even with some of the best security practices, employees can play a key role in a cyber incident. Tetra once investigated an incident of a high-value company that enabled MFA, which should have prevented a login from an unknown 3rd party. Upon being blind-sided by an infection of Sodinokibi ransomware, Tetra discovered that the employee behind an administrator account never completed the process of setting up MFA.

Upon investigation, this user's laptop showed other numerous risky behaviors. There was a saved text file containing user credentials and passwords — both to their desktop and to a personal online account. Personal cloud accounts were on their work laptop, and they were actively using torrents to search for, download, and install movies and cracked software. Even worse is that this user had sent email attachments including a username and password list — a spreadsheet containing employee names, phone extensions, and IP addresses, all in plain text.

This case was a unique mix of both an investigation of an active ransomware incident and an internal investigation of missteps taken by an IT employee. While security awareness training usually ranks lower priority-wise, employee behaviors can affect the overall security of a network.

Services to consider:

There are some great vendors out there, like Infosec and KnowBe4 that offer economical and effective role-based training.

Cybersecurity doesn't just happen.

The biggest misconception in cybersecurity is that you can depend solely on robust tools to protect your network, yet no matter how advanced a security solution, it becomes obsolete within weeks. This industry always has opposite and often unequal forces working against each other, making the need for experienced people behind your tools more important than ever before. Tetra's Cyber Defense Operations actively address these opposite & unequal forces.

Rather than "set it and forget it," Tetra provides **agile** security to actively mitigate threats as they happen, all informed by the latest threat intelligence and the cases we respond to daily. This approach protects the four frontiers of your network by leveraging our favorite **tools**, all backed by our experienced security **team**.

To learn more about our Cyber Defense services, visit www.tetradefense.com/cyber-defense-operations/

ABOUT TETRA

Tetra Defense began with one goal in mind: To **go beyond** what's been done before. Backed by the experience of our Cyber Defense Operations team, we provide Managed Detection & Response services for clients to protect both their endpoints and their inbox with a combination of leading security tools, custom-built services, and the diligent monitoring and insight from our team.

TETRA DEFENSE