Global Threat Intelligence Center

Monthly Threat Report

March 2021

Contents

In 'zero' we trust

Lead Analyst: Danika Blessman, Senior Threat Intelligence Analyst, Global Threat Intelligence Center, US

According to the National Institute for Standards and Technology (NIST), zero trust (ZT) is 'the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets and resources.' Essentially, a security concept based on the thought that organizations should not automatically trust anything – outside or inside its perimeters – but should instead verify everything. Verification should take place even if a previously trusted resource or device connects to the network.

Trust is an incredibly important aspect to network security, but there is also the need for devices to connect to a network to conduct normal day-to-day operations. There needs to be a system of controlled access management which does not negatively impact operations. Within a ZT framework, users are not necessarily able to access areas of the network, data and applications to which they do not specifically require access.

While the concept is not new, zero trust is back in the headlines of late due to the recent SolarWinds breach, and has received renewed interest and traction during the widespread shift to remote work and the evolution of the cloud during COVID lockdowns.

'Trust, but verify.' A phrase often used during the Cold War, it no longer truly applies where network security is concerned because, in the cyber world, attribution of activity from adversaries is difficult – even verifying those on your network is often difficult as well. The amount of activity we see from trojans and keyloggers, or access obtained via a stolen or guessed password, or via internal propagation from some network vulnerability, have all helped complicate our ability to really 'know' who is in our environment.

Organizations no longer have the benefit of moving at their own pace to ensure the proper security measures are in place to continue verifying a secure network environment. Organizations are forced to not only keep up with rapidly changing demand of the market, along with internal and external users, but to move at the pace of every vulnerability and threat actor targeting the network. This rapid, continuous transformation of the network environment has eroded traditional defenses. A static, trusted state in a network environment can no longer be assumed.

So where is the happy medium?

A ZT environment might be the answer.

Adopting a ZT framework could allow cyber-resiliency and agility in an organization's defenses – a layered approach to make it inherently secure by design. A ZT framework can also offer continued verification of users and devices through various means – such as multifactor authentication, known endpoints and employing the concept of least privilege for users on the network within each application.

The ZT architecture works by focusing on:

1. Enforcing policy-based control.
2. Providing greater visibility across the network environment.
3. Using detailed security logs to assist in detecting anomalies in the network.

Integrating a ZT framework will go a long way in removing some of the guesswork in protecting your organization's network and infrastructure and allow for resiliency in network defense – a better way to address unprecedented and unanticipated threats to your network.

So, zero trust is not necessarily a security solution, per se, but an overall strategy with which, as we mentioned above, organizations can ensure a 'secure by design' type of network security framework. This is done by knowing what users and devices are on the network and giving the least amount of access necessary to each for their roles. Organizations should also be aware of what happens to devices once they leave a trusted network and are brought back onto the network, such as with mobile devices.

As more users and devices connect to a network, the less secure a traditional perimeter-based approach becomes. Each time a user or device – particularly a mobile device – is automatically trusted, it places your organization's sensitive data and infrastructure at risk. Shifting to a ZT model, specifically with rigorous network access controls which span the network, will greatly enhance any layered defenses already in place.

To learn more about the ZT framework and strategies, please check out the discussions in our recent eBook here.

In addition, look to this year's Global Threat Intelligence Report (GTIR), coming out in May, in which our research analysts take a look at the effects of implementing zero trust within your organization's network.

> Each time a user or device – particularly a mobile device – is automatically trusted, **it places your organization's sensitive data and infrastructure at risk.**

References

https://www.nist.gov/publications/zero-trust-architecture

https://www.nist.gov/news-events/news/2020/08/zero-trust-architecture-nist-publishes-sp-800-207

#Spotlight 1

Growing cyberthreats to the **healthcare supply chain**

Lead Analyst: Mihoko Matsubara, Chief Security Strategist at NTT, Cybersecurity Policy

The world is now fighting against two types of viruses – COVID-19 and computer viruses. The healthcare sector provides one of the most crucial and needed services, especially during the COVID-19 pandemic. Yet, it is also one of the most targeted sectors by cyber espionage and ransomware attacks. Healthcare has been one of the seven most highly-targeted industries globally in each of the nine years we've produced the Global Threat Intelligence Report.

The sector did not have the most robust cybersecurity posture even before the pandemic. Our 2020 Global Threat Intelligence Report found that the healthcare industry scored only 1.12 in terms of cybersecurity maturity level while the financial industry showed a maturity of 1.86 points.[1] Furthermore, the pandemic has made it challenging for healthcare institutions to continue to invest in cybersecurity due to the increasing safety budgets for patients and medical staff.

These are some of the reasons why attackers are taking advantage of a wide variety of vulnerabilities and malware to launch cyber espionage and ransomware attacks. The number of detected cyberattacks on the healthcare sector globally jumped by 45% between October 2020 and January 2021.[2]

And, this is not just criminals looking to steal resources or information to help enable identification theft. Cyber espionage efforts are trying to steal information on COVID-19 vaccines not only from pharmaceutical companies and universities but also from regulators. The European Medicines Agency admitted in December 2020 that vaccine-related documents which were submitted for approval had been unlawfully accessed by cyberattackers. Reportedly, the documents were from Pfizer and BioNTech as well as Moderna.[3]

Damages caused by ransomware attacks on healthcare can be devastating, such as worsening illness or death, because ransomware prevents hospitals from accessing their patient database. In the United States, 560 healthcare facilities were hit by ransomware attacks in 2020.[4] Furthermore, criminals have also started to target cold chain logistics infrastructure that is necessary for secure transportation of COVID-19 vaccines. In November 2020, a ransomware attack temporarily suspended business operations at Americold, a major US cold storage company.[5]

The healthcare supply chain needs cybersecurity support such as cyberthreat intelligence and cybersecurity tools and services more than ever. The world fortunately started to see some silver lining: COVID-19 Cyber Threat Coalition[6] and CTI League[7] consist of cybersecurity volunteers who share cybersecurity insights and help with healthcare institutions experiencing cyberattacks. While the offer has now expired, we offered free cybersecurity consulting services to impacted healthcare institutions in 2020. Your help is also indispensable to protect ourselves and healthcare from the two types of viruses.

References

[1] NTT Ltd., '2020 Global Threat Intelligence Report,' July 2020, https://hello.global.ntt/en-us/insights/2020-global-threat-intelligence-report, 18.

[2] Check Point, 'Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again,' January 5, 2021, https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/.

[3] Jack Stubbs, 'Hackers steal Pfizer/BioNTech COVID-19 vaccine data in Europe, companies say,' Reuters, December 10, 2020, https://jp.reuters.com/article/us-ema-cyber/hackers-steal-pfizer-biontech-covid-19-vaccine-data-in-europe-companies-say-idUSKBN28J2Q7, and John Bowden, 'Moderna vaccine data accessed in cyberattack on EU regulator,' The Hill, December 15, 2020, https://thehill.com/policy/cybersecurity/530225-moderna-vaccine-data-accessed-in-cyberattack-on-eu-regulator.

[4] Emsisoft, 'The State of Ransomware in the US: Report and Statistics 2020,' January 18, 2020, https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/.

[5] Phil Muncaster, 'Americold Operations Downed by Cyber-Attack,' Infosecurity Magazine, November 18, 2020, https://www.infosecurity-magazine.com/news/americold-operations-downed-by/.

[6] https://www.cyberthreatcoalition.org/

[7] https://cti-league.com/

#Spotlight 2

A look at critical infrastructure - **are we at risk?**

Lead Analyst: Zhanwei Chan, Principal Business Development Specialist - Business Development, NTT Ltd., Australia

Cyberattacks are a way of life. Systems are hacked, information is stolen, ransom is demanded – unfortunately, these are all part of normal business. But, what happens when an attack is not just about the data?

Threats against our critical infrastructure can have a devastating impact not only on the services being attacked, but on the wellbeing of those affected. How do we treat a cyberattack, when the only real goal of that cyberattack is to injure people?

What happened?

On 5 February 2021, the Oldsmar Water Treatment Plant in Florida US was remotely compromised. According to the official police report, the chronology of the event is as follows:[1] [2]

- **5 February 2021, 8:00 AM:** SCADA system City of Oldsmar's water treatment plant was remotely accessed. The remote access was brief and did not raise any concern.
- **5 February 2021, 1:30 PM (for 3-5 minutes):** The SCADA system was remotely accessed again. This time, various functions relating to the sodium hydroxide mixture were opened. The cybercriminal increased the sodium hydroxide mixture by 111 times the normal amount.

Sodium hydroxide is a chemical used in sanitization as part of normal processing in the water treatment plant. The adjusted levels, after the attack, would have made the water unsafe for human consumption.

Based on the press conference, official communications and local news report, the following technical architecture and design were noted:

- The cybercriminals accessed the SCADA system using TeamViewer.
- The SCADA system was exposed to direct internet access.
- There was no firewall protection between the SCADA system and the internet.

These three issues would allow anyone from the internet to scan and identify systems which can be accessed using the TeamViewer application.

A quick search using Shodan.io indicates that there are about 67,000 TeamViewer systems which can be accessed via the internet, almost 16,000 of them in the US.

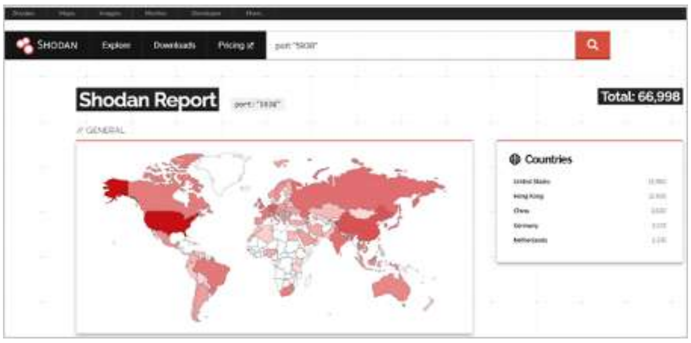

Figure 1: Shodan report showing TeamViewer systems accessible via the internet

Two additional issues aid in explaining why exposure helped make these systems vulnerable.

1. **Shared passwords**
   Shared passwords mean anyone who knows the password can access any applicable system, and there are more people to target to potentially obtain the password.
2. **Unsupported Windows 7**
   Security updates for Windows 7 ended on 14 January 2020 (more than a year ago). However, paid extended security support is still available until 14 January 2023.[3] An unsupported operating system can be more susceptible to exploitation as it may contain vulnerabilities which are never patched.

It is worth noting that patching of industrial systems is often complicated by the applications which operate on them and cannot always be performed in a timely manner.

Lessons learned

The cyberattack on Oldsmar is very unfortunate. To prevent events like this from happening, we need to collectively ask what happened and why. Understanding the details behind this attack can help us identify corrective actions to take in order to mitigate future incidents.

1. **Would regular security monitoring identify threats in time to mitigate the attack?** In this case, the initial remote connection did not raise an alarm, but an observant employee was able to identify unusual activity and take action. Not every victim is going to be in a position to take such action and continuous monitoring of critical assets is a key cornerstone to any security program.
2. **Were the systems running applications and services which were not needed?** The investigation report states in part 'Remote access has been allowed because it allows plant personnel to access the system while out in the field – in making programming adjustments/changes quickly.' In this case, it appears there was good reason to allow remote services, however, could the implementation and security controls around the implementation have been better?
3. **Was access managed appropriately?** It is not uncommon within the industrial systems operations to implement technology and access which could put SCADA systems at risk. The reality is that in industrial system operations, remote access must be simple, easy and fast. However, organizations must take appropriate care to make sure applications and services are implemented in a secure manner, and that they areclosely monitored and managed effectively.

> There are about **67,000 TeamViewer** systems which can be accessed via the internet, almost 16,000 of them in the US.

The list of questions which such environments should consider is much longer than these three – but these provide a starting point to help organizations understand what actions must be taken to effectively protect industrial controls systems and critical infrastructure.

Over the coming weeks, we will be posting additional articles on our blog on how to secure industrial controls systems.

Follow our blog here: https://hello.global.ntt/en-us/insights/blog

References

[1] Pinellas County Sheriff's Office Report and press conference: https://www.pcsoweb.com/21-015-detectives-investigate-computer-software-intrusion-at-oldsmar%E2%80%99s-water-treatment-plant

[2] Advisory from Massachusetts government after the cyberattack: https://www.mass.gov/service-details/cybersecurity-advisory-for-public-water-suppliers

[3] Microsoft support of Windows 7: https://docs.microsoft.com/en-us/troubleshoot/windows-client/windows-7-eos-faq/windows-7-extended-security-updates-faq

NTT's Global Threat Intelligence Center

The NTT Global Threat Intelligence Center (GTIC) protects, informs and educates NTT Group clients through the following activities:

- threat research
- vulnerability research
- intelligence fusion and analytics
- communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking their threat and vulnerability research and combining it with their detective technologies development to produce applied threat intelligence. The GTIC's mission is to protect clients by providing advanced threat research and security intelligence to enable NTT to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT's threat research is focused on gaining understanding and insight into the various threat actors, exploit tools and malware – and the techniques, tactics and procedures (TTP) used by attackers.

Vulnerability research pre-emptively uncovers zero-day vulnerabilities that are likely to become the newest attack vector, while maintaining a deep understanding of published vulnerabilities.

With this knowledge, NTT's security monitoring services can more accurately identify malicious activity that is 'on-target' to NTT Group clients' infrastructure.

Intelligence fusion and analytics is where it all comes together. The GTIC continually monitors the global threat landscape for new and emerging threats using our global internet infrastructure, clouds and data centers along with third-party intelligence feeds; and works to understand, analyse, curate and enrich those threats using advanced analysis techniques and proprietary tools; and publishes and curates them using the Global Threat Intelligence Platform (GTIP) for the benefit of NTT Group clients.

Our **Global Threat Intelligence Center** goes beyond a traditional research-only approach by combining focused research with detective technologies. This results in **true applied threat intelligence** to protect our clients with effective tools and services which reduce security risks and threats.

Recent assets

2020 Global Threat Intelligence Report

Our 2020 Global Threat Intelligence Report (GTIR) is the culmination of the data the Global Threat Intelligence Center gathered and analyzed throughout the year. We produce this report by collecting a broad set of global data (log, event, attack, incident and vulnerability) to identify key cybersecurity trends of which businesses need to be aware.

Download report

If you haven't already, **register to receive the Monthly Threat Reports** directly to your inbox each month.

NTT