



NTT Ltd. Global Threat Intelligence Center

Monthly Threat Report

July 2020

Contents

Feature article: Advanced Persistent Threat focus on COVID-19	03
Spotlight article: Growing and maturing collaboration via the Cyber Threat Alliance	05
Spotlight article: Considerations for secure SD-WAN	06
About NTT Ltd.'s Global Threat Intelligence Center	08



Advanced Persistent Threat focus on COVID-19

Lead Analyst: Danika Blessman — Sr. Threat Intelligence Analyst,
Global Threat Intelligence Center, US

Novel virus; same Advanced Persistent Threat (APT) disease

COVID-19 may be a relatively new disease, but the threat from Advanced Persistent Threat (APT) actors is not. Their activities continue, despite COVID-19; in fact, the virus might add fuel to the fire, or provide a cover for other operations.

Extortion, espionage, financial gain and disinformation are all reasons APTs conduct various operations, especially now, during a global crisis. We've mentioned before, bad guys – including state-sponsored APTs – will take advantage of others' vulnerabilities. 'Normal' APT campaigns during the pandemic may be covered by a smokescreen of operations using COVID-19 as a theme, or operations to glean COVID-19 data or research. As industries grapple with how to deal with our new reality, maybe we should ask: 'What are we not seeing?'

Some believe APTs have changed their tactics in response to COVID-19 – but have they really changed? Have they shifted focus? Or is it business as usual – and then some?

Organizations and industries considered essential have been targeted: power grids, oil and gas, postal and delivery services, first responders and law enforcement – assets which are even more valuable during a global crisis. If the world sees

a resurgence of COVID-19, as many medical authorities are predicting, and as countries are rethinking their supply chain models and dependencies for various goods, these industries will continue to be heavily targeted.

Revelations of nation-state APT campaigns have recently surfaced, particularly targeting essential services like oil producers, healthcare research agencies and government organizations. While the world is 'distracted' by COVID-19, APTs are attempting to garner intelligence. Some of this is intelligence on the virus; and some actors want to exact 'revenge' for the virus.

We've observed APTs, particularly those suspected to be backed by nation-states, focusing their intelligence-gathering efforts on COVID-19 research. Many nations are attempting to get the upper hand on COVID-19 research – both for the health of their citizens, as well as for monetization of a potential (and very valuable) treatment or vaccine. Unsurprisingly, APTs are targeting the healthcare industry heavily while it's at its most vulnerable. From international organizations to research organizations to hospitals and even individual healthcare workers and first responders.

Recent reporting suggests that APT groups with links to Iran have attempted to breach the World Health Organization (WHO) via a phishing campaign, likely seeking information on testing, treatments or vaccines. It's

currently unclear if any accounts were compromised or if the attack was successful.

In addition, DarkHotel (an APT suspected to be affiliated with North Korea) targeted the WHO, also potentially looking for information on testing, treatments or vaccines. Researchers discovered a malicious site in mid-March which mimicked the WHO's internal email system, likely designed to obtain credentials from multiple agency staffers. The attack appeared to attempt to gain and maintain a foothold within the WHO's network, as well as gain access to other healthcare and humanitarian organizations connected to the WHO network. This suggests the threat actor may have been seeking intelligence over financial gain.

The UK and US recently issued a joint alert that these same suspected nation-state-backed APTs were targeting research institutions and pharmaceutical companies at the forefront of the search for treatments or a cure. In fact, at least one company in the forefront of the search for a vaccine and treatments has been targeted, though we should expect to see many more in the same situation.

Maybe we should
ask: **'What are we
not seeing?'**

Suspected Iranian-based threat actors have targeted staff at pharmaceutical company in recent weeks, as one of their drugs reportedly showed promise at treating COVID-19. Threat actors used a spear-phishing email to send a fake login page designed to steal login credentials to a top legal executive in the company. The infrastructure used in this attempt had previously been used by a suspected Iranian-sponsored group known as Charming Kitten. Nations like Iran, who have seen devastating effects from COVID-19, may be more incentivized to gain access to a treatment more quickly, giving further motivations to target healthcare and pharmaceutical organizations.

China has turned to virtual private networks (VPNs) for officials working remotely amid the COVID-19 pandemic; DarkHotel targeted these VPNs in what researchers called a zero-day attack. At least 200 VPN servers connecting to multiple endpoints were compromised as of the first week of April.

In addition, APT32 (attackers linked to the government of Vietnam) have been targeting China, reportedly over its perceived lack of accurate information dissemination during, and overall handling of, the initial outbreak. Attacks appear to have been carried out by targeting staff email accounts of China's Ministry of Emergency Management, the center of the national effort to contain the virus, as well as the government of Wuhan. Spear-phishing emails contained a malicious link harboring a virus called Metaljack allowed access to the targeted machine upon a successful download.

'Normal' APT operations have also continued during this same timeframe; and operations related to – or leveraging – COVID-19 may serve as a smokescreen while countries continue to focus their efforts in response to the pandemic, from both healthcare and cybersecurity perspectives, at minimum.

Recently, the government of Australia warned that a sophisticated state-sponsored threat actor had been attacking both government and corporate institutions. These attacks leveraged unpatched versions of Telerik UI and

Network segmentation between teams and projects, is likely **one of the best ways to protect internal resources.**

two Microsoft vulnerabilities exploiting SharePoint and Internet Information Services (IIS). The Australian Cyber Security Centre (ACSC) stated that they 'identified no intent by the actor to carry out any disruptive or destructive activity within victim environments.' This suggests that the purposes of the attacks are likely to conduct either cyber-espionage or collect intelligence data.

Companies researching the disease should expect to be targeted whether for purposes of medical advantage to better treat or prevent COVID-19, for monetary gain (to extort to avoid damage to research), or purely to inhibit the target from making progress. As result, healthcare organizations should look to enhance their network security measures – particularly in those areas involved in COVID-19 research. It's worth remembering that like many attackers, APTs are adept at moving laterally through an organization's network and may be able to move from a target in the legal department, as mentioned above, to those scientists involved in COVID-19 research. Best practices, at a **minimum**, are essential. Network segmentation between teams and projects, is likely one of the best ways to protect internal resources. Air-gapped computers – that is, those not connected to the internet – are an even better option for COVID-19 research.

Just because your organization may not be considered an essential service doesn't mean you should let your guard down. In fact, just the opposite; if operations leveraging COVID-19 are being used as a smokescreen to conduct

other operations, you may be facing even more risk. There will always be targets of opportunity. Continue best practices and awareness of both your network environment and the global state of things.

Cyber-operations do not exist in a vacuum – they are driven by an incredible number of factors and exist within a giant umbrella of these factors. Cyber-operations may very well be increasing, as people around the world attempt to physically distance themselves ... in fact, cyber-operations – and other asymmetric capabilities – are likely being enhanced by this factor.

Sure, this may be a new virus; but it's the same APT disease.



#Spotlight 1



Growing and maturing collaboration via the **Cyber Threat Alliance**

Lead Analyst: Jeremy Nichols — Director, Intelligence Fusion & Analytics, Global Threat Intelligence Center, US

The Cyber Threat Alliance (CTA) was formed as a not-for-profit organization working to improve cybersecurity by enabling near real-time, high quality threat information sharing amongst member organizations.

CTA membership has allowed the our Global Threat Intelligence Center (GTIC) to continue to mature our research, threat hunting and intelligence dissemination processes through automated and manual intelligence sharing between members. The GTIC has actively migrated to the CTA's new technical intelligence sharing platform and extended our own sharing and collaboration across members.

Transforming sharing

Beginning last fall, the GTIC began to migrate from the legacy submission process to the new CTA platform while we were also merging companies within NTT Ltd. This meant not only a technical change on the intelligence structure and submission process, but new and changing threat data internally, which we wanted to leverage.

As a result of all the moving parts, GTIC designed toward an Extract, Transform, Load (ETL) model which allows us to more easily plug in new data sources without writing new connectors from the ground up. The pipeline brings together telemetry and insights from our threat intelligence platform, Managed Security

Service (MSS) platform, backbone data, honeypots and threat feeds to form contextual sightings of threats from our multiple vantage points.

With the platform migration also came the migration from modeling threats in STIX1.2 packages to structuring intelligence submissions into STIX2.0 bundles. For a bit more background, OASIS has done a great overview on the differences between versions [here](#). STIX 2.x is much cleaner and more contextual than 1.x was, and includes more robust relationships and sightings. This allows researchers to better understand attacks and threats being faced from an actor and campaign perspective, as opposed to simply capturing high level details.

Collaborative opportunities

We continue to participate in working groups and subcommittees. In relation to a malware disruption effort, we have gained tremendous insight into tracking the infrastructure of specific malware families as well as helpful tips for reverse engineering related samples. With such a group of talented personnel, our researchers have also been able to piece together missing artifacts from current research initiatives regarding the malware. In addition to this, with the vast amount of unique data from all collaborators, GTIC has evolved new processes to efficiently track elusive campaigns.

One byproduct of the working groups and early sharing is visibility across threats being tracked by members which

are not always ready for dissemination yet. We discovered COVID-19-related fraud activity being conducted by Nigerian actors targeting a health care manufacturing company. While we began working with law enforcement to take action against these actors, we shared some of our findings across members of the CTA Algorithm & Intelligence committee and another member reached out to share similar findings they were actively tracking. While these turned out to be different actors with similar tactics, techniques and procedures (TTP), this complementary research helped each team, and highlights the power of collaboration and visibility enabled within the Cyber Threat Alliance.

Continued momentum

GTIC has encountered our fair share of difficulties during the migration process, but we are pleased with the results of our work and the work of all contributing members. The volume of contextual cyberthreat intelligence submitted in the last couple months alone is fantastic, and further powered through the formal and informal collaboration between member organizations. The NTT Global Threat Intelligence Center looks forward to the continued evolution of sharing and partnership to protect customers and improve internet security.



#Spotlight 2



Considerations for secure SD-WAN

Lead analyst: Gareth Waters — Principal Go-to-Market Strategist, Australia

As businesses continue to digitally transform and rapidly expand their footprint, they've been looking for a network that balances cost, user experience, agility and efficiency. The answer, and solution rapidly increasing in adoption, is a software-defined wide area network (SD-WAN).

SD-WAN is a virtualized network overlay, meaning it's a lightweight replacement for traditional physical WAN infrastructure. It's transport type agnostic (it can support MPLS, internet, 4G/LTE, etc.) and dramatically simplifies the complexity associated with the management, configuration and orchestrations of networks. Because of all this, it can be delivered cost-effectively, provide business flexibility and be deployed as required from a centralized orchestration point. It can be an ideal solution for already 'thin on the ground' IT teams.

But, in an era of increasing cyberattacks, how does an SD-WAN stack up in terms of security?

Challenging assumptions: SD-WANs are not inherently secure

SD-WANs are built from a combination of commercial off-the-shelf and open source software that once combined, can result in security gaps across the architecture. As shown in Figure 1, there are in fact several layers of potential vulnerability, depending on the equipment and connectivity types you use, and your architecture design logic.

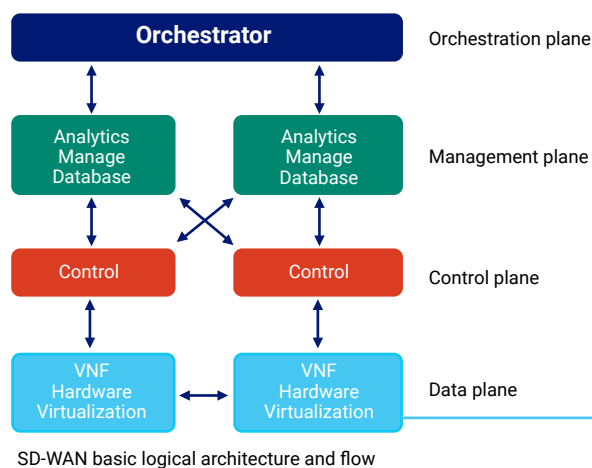
Furthermore, while partner WAN technologies have some native security features, unless reviewed holistically, it's likely not enough to ensure your SD-WAN is inherently secure. It is a fundamental

requirement to do a risk analysis and assessment that considers your organization's risk profile at the outset of designing your SD-WAN and selecting appropriate security controls.

That said, at a minimum, you need to consider the following to secure your SD-WAN:

- network segmentation to secure specific areas of the network reduce or slow the spread of threats
- data encryption and VPN to ensure confidentiality of data traversing your network
- security tools to stop malware and perform content filtering
- ability to prevent malicious access and attacks

Threat modeling



Threats may exploit weaknesses in:

1. **Data plane:**
 - Outdated operating systems (Ubuntu, Debian, CentOS)
 - Out of Band (OOB) baseboard controllers (BMC, IPMI)
2. **Control plane:** Network element packet processors
3. **Management plane:** Management interfaces (Cli, SSH, WebUI)
4. **Orchestration plane:** Orchestration interfaces (REST API, XML)
5. **Cryptographic layer** (PKI, VPN)

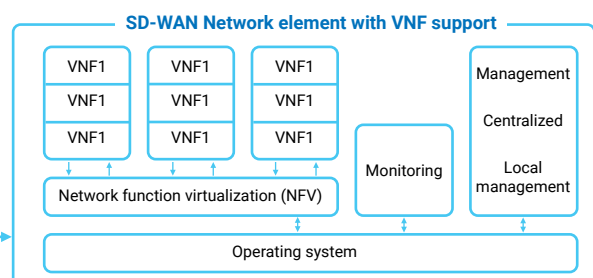


Figure 1: Threat modeling an SD-WAN logical architecture

The controls you ultimately select will also depend on how you decide to deploy security as part of your SD-WAN solution.

There are a few models to consider:

- **Centralized:** Network and security controls are managed in a central hub. While this provides 'absolute security', the tradeoff lies in application performance.
- **Decentralized:** Security control lies at each branch office location for flexibility and autonomy. However, this tends to result in inconsistent security across the organization and is likely also costlier to deploy and manage.
- **Cloud-based (i.e., Secure Access Service Edge or SASE):** This combines WAN capabilities with cloud-native security functions like secure web gateways, cloud access security brokers, firewalls and zero-trust network access. However, to be truly effective, it requires close collaboration between networking, security and DevOps teams.

The importance of threat modeling

Threat modeling is a process that can help you to identify possible threats and vulnerable areas across your architecture as shown in Figure 1. Proper threat modeling can provide insight into how controls should be prioritized so that any potential exposure is mitigated.

Threat modeling should be conducted early in the development of your SD-WAN, so issues can be remediated early and to avoid much costlier fixes later on. It can lead to proactive design decisions, which reduce the threat at the outset, helping your architecture to be secure by design.

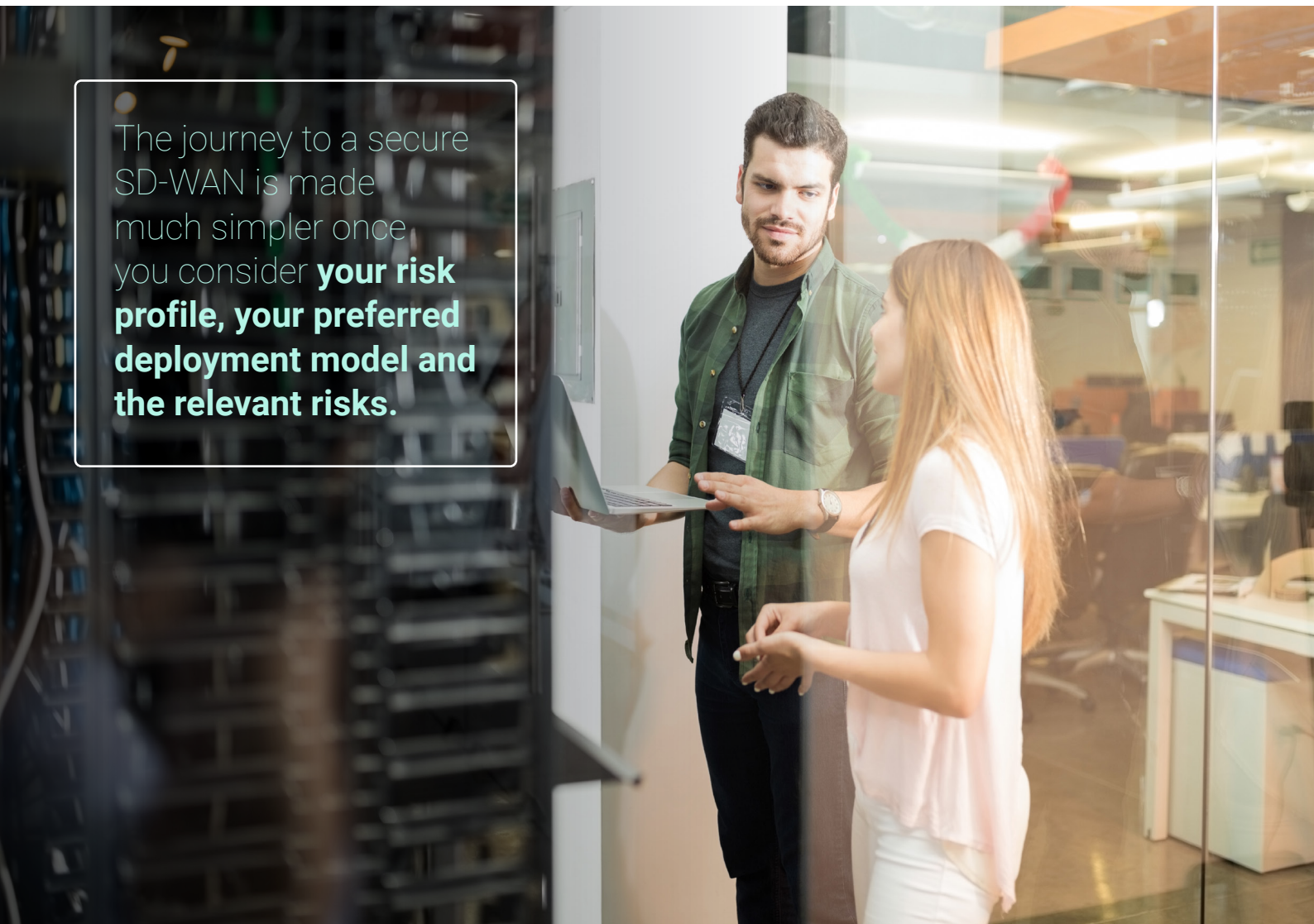
Threat modeling can provide insight to **mitigate potential exposure.**

Conclusion

In summary, security should be a fundamental requirement for your SD-WAN deployments to minimize your overall business risk. Moreover, it is far easier, cost-effective and less risky to deploy security from the beginning (building a solution that is secure by design) rather than implement the SD-WAN solution then attempt to retrofit security into that solution. The journey to a secure SD-WAN is made much simpler once you consider your risk profile, your preferred deployment model for your branches, and the risks which exist across the reference architecture components.

This article provides a summary of the security considerations for your SD-WAN. If you'd like to do a complete technical deep dive into architectures, controls and threat modeling, you can watch our BrightTalk webinar on the topic [here](#) or speak to your NTT Ltd. network or security representative.

The journey to a secure SD-WAN is made much simpler once you consider **your risk profile, your preferred deployment model and the relevant risks.**



NTT Ltd.'s Global Threat Intelligence Center

The NTT Ltd. 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 Ltd. to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT Ltd.'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 Ltd.'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

The 2020 NTT Ltd. 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.

