Global Threat Intelligence Center

Monthly Threat Report

January 2022

Contents

Looming challenges of 2022

Lead Analyst: J. Michael Daniel, President and CEO, Cyber Threat Alliance

Herb Lin, a well-respected cybersecurity expert, once joked that "It's easy to be a cybersecurity expert. Just declare that tomorrow will be worse than today, and you'll probably be right." Unfortunately, 2022 is unlikely to prove that statement wrong. Therefore, the question for cybersecurity leaders is not whether cyber threats will evolve or grow worse, but how they will change and what steps organizations can take to prepare.

Based on reports by Cyber Threat Alliance members and partners, at least five trends will drive the cyber threat landscape in 2022:

- **Ransomware as a lucrative business model –** not surprisingly, ransomware will continue as a top threat. Although the US and other governments have stepped up their efforts to combat ransomware, those actions will take time to bear fruit. In the meantime, malicious actors will continue to ride the current wave of ransomware attacks. They will seek new methods to take advantage of old vulnerabilities, find new vulnerabilities to exploit, and develop different ways to pressure organizations to pay. For most organizations, a ransomware attack is the serious cyber incident they are most likely to face; as a result, building resilience to such an event should be the highest priority for most cybersecurity leaders.

As the promise of practical quantum computing grows closer, the possibility that advances will render current encryption algorithms ineffective increases.

- **Hardening insurance market –** as insurance companies continue to lose money on cyber-insurance policies due to ransomware attacks, they will tighten requirements on policyholders. While insurance companies previously competed to see who could impose the least burden on their policyholders, mounting losses are changing the nature of competition. The insurance industry calls this change "hardening." Insurers will increase premiums and deductions, but they will also require policyholders to thoroughly demonstrate cybersecurity capabilities to qualify for policies. For example, companies might have to demonstrate that they use multi-factor authentication or limit the functionality of administrative accounts. Cybersecurity leaders should prepare themselves for more scrutiny, higher premiums, and more exclusions from their insurers.
- **Incident reporting requirements –** breach reporting, or a legal requirement to notify customers or users that attackers have compromised their personally identifiable information due to a cyber incident, is now quite common worldwide. However, requirements to report cyber incidents to governments, whether they involve PII breaches or not, are much less common. The US Congress considered legislation to make cyber incident reporting mandatory for many organizations. That mandate did not pass this year, but the likelihood that Congress will eventually enact some reporting requirement is very high. Other countries are considering similar legislation. Cybersecurity leaders should begin preparing to incorporate a reporting requirement into their incident response plans.

- **The need for "Crypto Agility" –** as the promise of practical quantum computing grows closer, the possibility that advances will render current encryption algorithms ineffective increases. For some organizations, the need to protect certain information for more than three to five years means that the window for addressing the threat posed by quantum computing is now. However, most organizations do not understand what crypto they use, what systems and processes it covers, or how they could replace it. Cybersecurity leaders should begin to develop their "crypto agility" or the ability to shift encryption algorithms rapidly to be ready to deal with breakthroughs in cracking encryption algorithms that render particular encryption methods vulnerable.
- **Increases in systemic risk –** the recent increases in working from home, internet-connected devices, and reliance on cloud services are not going to reverse any time soon. As a result, the risk of a cyber incident having an unforeseen, economy-wide impact continues to increase. These risks are inherently difficult to manage because no one organization controls them. This trend puts pressure on cybersecurity leaders to focus on the response and recovery steps in the Cybersecurity Framework.

Although these trends are not likely to make the lives of cybersecurity professionals easier, they also provide an opportunity for companies to make effective cybersecurity a competitive advantage. If a company can stay online when others cannot, that organization can continue to earn revenue when others might not. A company with better cybersecurity practices will be able to obtain a cyber insurance policy at a lower price. Preparing for incident reporting requirements, even seeking to take advantage of such requirements to obtain assistance in the event of a major cyber incident, will make a company more resilient to cyber threats. So will investing in crypto-agility. Handled in the right manner, these trends mean that good cybersecurity is becoming an advantage that can pay for itself. So, while tomorrow will still be worse than today in terms of the general threat, it does not have to be worse for any individual company.

The Cyber Threat Alliance (CTA) is a 501(c)(6) non-profit organization that is working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field.

Highlight Article

Partnership and collaboration via the National Cyber-Forensics and Training Alliance

Lead Analyst: Jeremy Scott, Director,
Global Threat Research, GTIC, US

The National Cyber-Forensics and Training Alliance (NCFTA) is a non-profit corporation founded in 2002, focused on identifying, mitigating and disrupting cyber-crime threats globally. Industry, academia and law enforcement created the NCFTA for the sole purpose of establishing a neutral, trusted environment enabling two-way information sharing. Through the NCFTA, the NTT Global Threat Intelligence Center (GTIC), private industry partners and government work together in this neutral, trusted environment.

Information sharing

Establishing trusted relationships is critical to information sharing and sharing near real-time information is important to NCFTA analysts and partners. NTT established a trusted relationship with the NCFTA through years of partnership. The GTIC provides an on-site resource that gives us the unique opportunity to embed that resource at one of the three NCFTA offices. The resource continues to report to the GTIC but works alongside the NCFTA's team of intelligence analysts, other industry subject matter experts and law enforcement agents to collaborate and share intelligence.

The GTIC is also considered a remote partner in that the NCFTA intelligence analysts virtually support the GTIC through various communication channels, working groups, webinars and training events.

GTIC researchers leverage information from the NCFTA to identify missing artifacts from research initiatives regarding various threats through the NCFTA sharing channels and data feeds. Information from the NCFTA also helps validate information GTIC has collected from our own research. The vast amount of unique data from all collaborators has allowed GTIC to evolve processes and more efficiently track elusive campaigns.

Trusted sharing allows the GTIC to improve our intelligence, providing more accurate and timely intelligence to our clients.

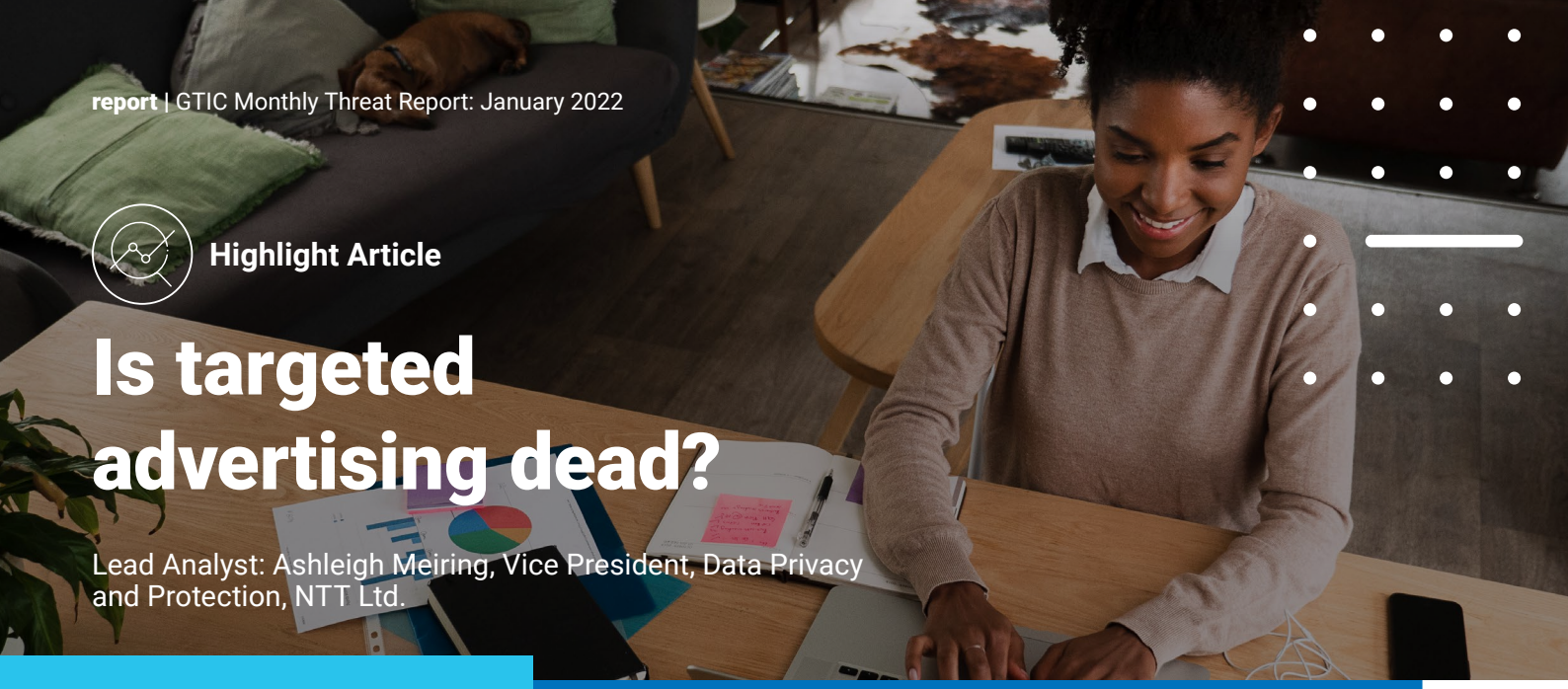
Trusted environment

When law enforcement needs help understanding an event, it relies on the NCFTA community of industry partners to provide insight into the scope and impact of the threat. Similarly, when NTT needs the support of government or law enforcement, the GTIC can make the necessary connection facilitated by the NCFTA. These trusted relationships enable NTT and law enforcement to align priorities and resources without compromising privacy, ethics, or the integrity of the research or the investigation.

NTT recently discovered COVID-related fraud activity targeting a healthcare manufacturing company. The NCFTA introduced the GTIC to the appropriate law enforcement agency and began working with law enforcement to take action against these actors. We shared intelligence with the alliance to aid in tracking the campaigns carried out by the criminal organization.

Continued collaboration

GTIC and NTT have continued to foster a greater relationship with the NCFTA through our involvement and support. NTT has a membership seat on the NCFTA Partner Advisory Committee which provides a formal mechanism for private sector partners to provide input to and receive feedback from the NCFTA. This membership helps ensure that the interests and initiatives of NTT and our industry partners are incorporated into mutually beneficial projects or initiatives. The NTT Global Threat Intelligence Center looks forward to the continued evolution of sharing and partnership to protect customers and improve internet security.



Highlight Article

Is targeted advertising dead?

Lead Analyst: Ashleigh Meiring, Vice President, Data Privacy and Protection, NTT Ltd.

When Google announced its plan to phase out third-party cookies, it helped force the targeted marketing industry and businesses to reconsider how we approach data collection and market profiling.

The June 2020 announcement was an interesting move from Google and will have a widespread impact. Chrome is the most-used desktop browser, and Google dominates search, browsers and ads. Google, and the data it collects, plays a critical role within the targeted advertising industry. But the move toward restricting third-party tracking is in line with more privacy-forward browsers and practices and perhaps indicates Google's desire to become a more privacy-conscious company.

But let's take a step back – what are these cookies, why is Google's move so significant, and who does it impact?

What is a cookie?

A cookie is a small text file used on websites. Organizations use several types of cookies to support how individuals interact with their websites and applications, track individuals across devices and sites, manage their preferences, and receive content.

A cookie can maintain the user's details and ensure they are authenticated to use the site. An organization can also use the contents of cookies to monitor how an individual uses certain pages such as where they click, what they click on, and what they interact with on a webpage. Beyond that, insights organizations obtain from cookies can optimize webpage performance or make a browsing experience more beneficial to visitors. In light of the many different contexts in which organizations can use them, not all cookies are bad. Even targeting cookies presents benefits to individuals when managed according to individual preferences.

'Targeting' cookies understand user behavior by looking at website interactions and searches, then using this data to create a profile of individual users. The organization then uses this profile to direct more meaningful, timely and relevant content to enable more effective advertising. If you were searching 'best-selling books of 2021' you might start to see targeted advertising for books across different webpages and platforms that you use.

The cookie privacy debate

From a privacy perspective, the use of cookies, and specifically targeting cookies, have certainly raised some concerns. From a vendor or seller point of view, cookies have value since they allow the organization to customize the browsing experience to each individual. But, should organizations be able to track user behavior and create user profiles? Should they be able to use this data to develop insights into individuals, their preferences, and possibly direct their actions? Should they then be able to use that data commercially and essentially profit off the use of this information?

Initially, concerns around the use of cookies arose because individuals were mostly not even aware organizations were tracking them. To solve this problem, organizations began implementing pop-up statements. When visiting new web pages, the site tells users that it is using cookies, so they were at least conscious that the organization was observing their activity.

We've recently seen organizations introduce elements of increased user control as pop-ups on a new webpage. You can now accept or decline cookies and specify what type of cookies a website can or cannot use (i.e., performance, authentication, social networking or targeted marketing). But, users tend to view these pop-ups as more of an annoyance than something that results in meaningful interaction or rebalances control on data ownership and privacy protection.

The cookie ban: monopoly or new business models emerging?

Initially, Google planned to outright ban all third-party cookies by mid-2022 but has since delayed this until 2023. But with the removal of third-party cookies, the targeted advertising industry faces some real risks. This industry is based on collecting, generating, and selling profile data. Therefore, they are wondering how they can survive and what it means for their business when third-party cookies are no longer available via Chrome.

While the effect of such a ban might most directly affect the business-to-consumer (B2C) industry, the business-to-business (B2B) industry will also undoubtedly be affected too. Even companies like NTT use cookies to generate insights into our marketing campaigns and ensure our clients are being served the content that is of greatest value to them. When done correctly, this can enable users to find the most desirable information with less effort on their part.

While cookies are often given a bad name, in both the B2C and B2B scenarios, they can be beneficial to inform a user of something they need when the user needs it or find new and interesting things about brands the user cares about. But, that customization comes at a price – in this case, the profiling of user's behavior online.

At present, there is no single solution or alternative to removing third-party cookies. There is a strong proposal from Google to use federated learning. Federated learning relates the data of individuals into groups of individuals who have similar interests and qualities. This enables Google to support anonymity since the supporting organization is not tracking individuals on an individual level but rather a group level. While this may be a great leap forward compared to existing models, it certainly is not a simple solution. At this time, this technology would be one that Google entirely controls, it could take an entire business model away from a huge industry, raising competition concerns.

> Individuals are not only the product but also participate in the **digital economy built around the buying and selling of user data.**

On the other hand, there have been some innovative new business models emerging. For instance, you can sign up to some applications, check your preferences for what type of personal information you prefer to be shared or not, brands you like to see advertisements from, companies you don't want your data shared with and so on. For consenting to the use of your data you can earn rewards like discounts, vouchers or even credits towards future purchases. In this model, you can benefit from the fact that others are also profiting off the use of your data. And, you increase the likelihood that the ads you're being served are of value to you. Here, individuals are not only the product but also participate in the digital economy built around the buying and selling of user data.

Innovation on the horizon

The 2023 extension is ultimately good news. With no clarity on the best technology or solution going forward and how to support the industry that relies on third-party cookies, organizations have more time and opportunity to create innovative ideas.

Ultimately, targeted advertising is not dead. It's likely about to be reborn with some incredibly powerful innovations that will enable mutually beneficial arrangements between users and businesses, a rebalancing of control between the two and ultimately stronger relationships between consumers and the brands they love. And, you might just come out of it with a little more control over your data.

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.

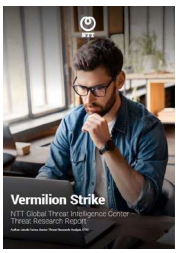
Our **Global Threat Intelligence Center** goes beyond a traditional research-only approach by combining focused research with detective technologies. This results in **true applied threat intelligence** to protect our clients with effective tools and services which reduce security risks and threats.

Recent assets

2021 Global Threat Intelligence Report

Our 2021 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



Vermilion Strike Report

During our threat research the GTIC used information from a public blog to initiate a deeper dive into Vermilion Strike. Vermilion Strike is a Linux reimplementation of the Cobalt Strike Beacon, built from the ground up by threat actors.

Download report

If you haven't already, **register to receive the Monthly Threat Reports** directly to your inbox each month. Sign up for our **Emerging Threat Advisory** and security bulletins for visibility of emerging threats and vulnerabilities that are being actively exploited across the world, sourced from our global threat intelligence platforms.


NTT