Ransomware Annex to G7 Statement

October 13, 2020

The G7 expresses its concern over the use of malicious cyber-attacks, especially ransomware. Ransomware attacks against hospitals, financial institutions, schools, and other critical infrastructure in G7 countries have been growing in scale, sophistication, and frequency. Attacks have intensified in the last two years, and illicit actors have exploited the pandemic to conduct ransomware attacks. For many companies, ransomware causes significant economic damage and threatens customer protection and data privacy. Ransomware attackers demand payments primarily in virtual assets to facilitate money laundering. The payment of ransoms demanded by these criminals can incentivize further malicious cyber activity; benefit malign actors and fund illicit activities; and present a risk of money laundering, terrorist financing, and proliferation financing (ML/TF/PF), and other illicit financial activity. In some cases, this activity occurs without victims even achieving a return to normalcy.

We call upon all countries to effectively implement the Financial Action Task Force (FATF) standards to reduce criminals' access to and exploitation of financial services, particularly the updated FATF standards on virtual assets. We welcome the continued work of the FATF to address risks posed by those assets and other emerging technologies, while recognizing opportunities they may offer.

The G7 will enhance its efforts at coordinated responses to ransomware, including where possible information sharing, economic measures, and support for effective implementation of the FATF standards.

I. Threat

The financial services sector has become an attractive target for ransomware attacks, and financial institutions have reported increased sophistication in malicious cyber-enabled attacks in recent months. Some prominent strains of ransomware have been linked to groups that are vulnerable to influence by state actors.

Examples demonstrate that virtual assets play an important role in most ransomware attacks. In instances where the victim does not own enough virtual assets to pay the ransom, the victim will often send funds via wire transfer, automated clearinghouse, or credit card payment to an exchange to purchase the type and amount designated in the ransom demand. From there the victim will send the virtual asset, often from a wallet hosted at the exchange, to the criminal-designated account or address.

The COVID-19 pandemic has expanded opportunities for ransomware attackers. Phishing emails using COVID-19-related subject lines or content are the latest method to get targets to click on ransomware links. Threat actors deploying ransomware also use fraudulent notifications for updates delivered through email or a compromised website to trick users into downloading the malware.

Ransomware attacks can impose devastating consequences on victims and those that depend on them. Not only can the financial costs be high, but the disruption to critical sectors, including financial services and healthcare, as well as the exposure of confidential information, can cause severe damage. The payment of ransom may encourage future ransomware payment demands, especially against the victim or type of victim that has proven profitable in the past.

Ransomware is primarily a profit-seeking endeavor, and its purveyors generally focus on the most lucrative targets, such as those with significant sources of funding or those with limited cyber security protection.

Ransomware attackers are criminals, many of whom are involved in transnational organized crime groups, and a received ransom payment constitutes criminal proceeds. Those criminals that have employed the use of malware may also be linked to states seeking to evade sanctions. Ransomware proceeds could also be used to finance terrorism once they have been converted into anonymously-held funds by a victim payment into an unidentified virtual asset wallet. If employed by a state-sponsored or linked actor, ransomware payments could offer a possible profit source to finance the proliferation of weapons of mass destruction.

II. G7 Efforts to Combat Ransomware

Noting the seriousness of the money laundering and terrorist financing threats of ransomware, in addition to the other dangers it poses, the G7 commits to coordinated action to address and mitigate this threat.

The G7 is committed to working with our financial sectors to combat ransomware. The G7 reminds financial institutions that the payment of ransom entails financial activity and as such is subject to AML/CFT laws and regulations. The G7 notes that even companies whose primary business is not financial services, such as a cyber-incident consulting firm, may fall under the obligations for financial institutions if they provide qualifying services, such as money transfers. The G7 reminds obliged entities, including traditional financial institutions and virtual asset service providers, that their AML/CFT obligations, including those related to customer due diligence, suspicious activity reporting, transaction monitoring and targeted financial sanctions, apply to all financial activity. This includes payments that are indicative of ransomware activity. Financial institutions and the public should be especially alert to prevent sanctions evasion in line with their national legal obligations. Furthermore, it should be noted that a substantial proportion of ransomware attacks are believed to stem from jurisdictions with elevated ML/TF/PF risks and that G7 jurisdictions have imposed targeted financial sanctions on known malicious cyber actors.

The fact that criminals often demand that ransoms be paid in virtual assets is of particular concern to the G7 and magnifies the need for all countries to effectively and expeditiously implement the FATF's standards on virtual assets and virtual asset service providers. The G7 notes the importance of virtual asset service providers having effective programs in line with the FATF standards and national obligations, notably including the need to hold and exchange information about the originators and beneficiaries of virtual asset transfers (i.e., "the travel rule").

G7 jurisdictions will share information related to ransomware threats, including financial intelligence and cyber tactics, techniques, and procedures where possible as appropriate and to the greatest extent possible under applicable law in order to guide coordinated action. This includes, but is not limited to, exploring opportunities for coordinated targeted financial sanctions, consistent with national law and regulation, against ransomware operators and their facilitators and promoting available technical innovations to protect cyber assets. The G7 further commits to lead by example in implementing and encouraging the worldwide implementation of AML/CFT obligations on virtual assets and virtual asset service providers considering that the FATF has updated its standards to clarify their application to virtual assets and virtual asset service providers.

Mitigating the threat before an incident is a key component. Companies need to move beyond traditional perimeter security to defend against ransomware, by employing layered security to prevent, detect, and remediate malicious activity that may be conducted within the network. Companies may also consider altering their own internal response and recovery plans in light of the potential sanctions violations particularly if current plans consider paying a ransom. Additional measures to aid in prevention and mitigation in the event of a ransomware compromise can be found at:

1. Canada:
    a. On the Canadian Centre for Cyber Security webpage: https://cyber.gc.ca/en/guidance/ransomware-how-prevent-and-recover-itsap00099.
2. France:
    a. On the dedicated ransomware page of the French website of the Agence Nationale de Sécurité des Systèmes d'information (ANSSI): https://www.ssi.gouv.fr/actualite/ne-soyez-plus-otage-des-rancongiciels/.
    b. Information on the cooperation with financial supervisors can be found here or here.
3. Germany:
    a. On the German Federal Office for Information Security ransomware webpage: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/Ransomware/Ransomware_node.html
4. Italy:
    a. On the following webpage: https://csirt.gov.it/ https://www.commissariatodips.it/notizie/articolo/campagna-no-more-ransom/index.html
5. Japan:
    a. On the Japan National Police Agency Cybercrime Project webpage: https://www.npa.go.jp/cyber/ransom/index.html.
6. United Kingdom:
    a. https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
    b. https://www.ncsc.gov.uk/blog-post/bring-your-own-device-the-new-normal
7. United States:
    a. On the U.S. Cybersecurity and Infrastructure Security ransomware webpage: https://us-cert.cisa.gov/Ransomware.

b. In FinCEN's ransomware advisory: https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2020-a006
c. In OFAC's ransomware advisory at: https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001.

####