金融監督管理委員會保險局　函

地址：220232新北市板橋區縣民大道2段7號17樓
承辦人：李柏寬
電話：02-8968-0899分機0714
傳真：

受文者：中華民國人壽保險商業同業公會（代表人黃調貴先生）

發文日期：中華民國110年3月25日
發文字號：保局(綜)字第1100414363號
速別：最速件
密等及解密條件或保密期限：
附件：如說明(110S402463_1_25085956010.pdf、110S402463_2_25085956010.pdf、110S402463_3_25085956010.pdf)

主旨：有關美國就北韓網路惡意活動發布「北韓網路威脅指引(Guidance on the North Korean Cyber Threat)」及「聯合網路安全報告（Joint Cybersecurity Advisory)」一案，請轉知所屬會員參考，並視業務需求向相關單位分享北韓網路威脅之資訊，及採取相關措施以降低威脅，請查照。

說明：依據本會110年3月3日金管銀法字第1100270624號函（副本）辦理。檢附前函及附件影本1份供參。

正本：中華民國人壽保險商業同業公會（代表人黃調貴先生）、中華民國產物保險商業同業公會（代表人李松季先生）、中華民國保險經紀人商業同業公會（代表人朱水源先生）、中華民國保險代理人商業同業公會（代表人鐘俊豪先生）、中華民國保險經紀人公會（代表人藍維鼎先生）
副本：本局綜合監理組 電2021/02/26交 09:06:29章

檔　　號：
保存年限：

金融監督管理委員會　函

地址：220232新北市板橋區縣民大道2段
7號18樓
承辦人：吳昱賢
電話：(02)89689626
傳真：(02)89691366

裝

受文者：本會保險局

發文日期：中華民國110年3月3日
發文字號：金管銀法字第1100270624號
速別：普通件
密等及解密條件或保密期限：
附件：如說明三附件1 附件2

主旨：有關美國就北韓網路惡意活動發布「北韓網路威脅指引(Guidance on the North Korean Cyber Threat)」及「聯合網路安全報告（Joint Cybersecurity Advisory)」一案，請依說明二辦理，請查照。

訂

說明：

一、近年來北韓利用網路惡意攻擊金融機構或虛擬貨幣交易所等機構所獲得之收益，以資助其發展大規模毀滅性武器及彈道飛彈計畫。

二、鑒於上該惡意網路活動日益盛行，請貴會(社)將旨揭報告轉知各會(社)員機構參考，並視業務需求向相關單位分享北韓網路威脅之資訊，及採取相關措施以降低威脅。

三、檢附旨揭二報告之電子檔各一份。

線

正本：有限責任中華民國信用合作社聯合社（代表人麥勝剛先生）、台北市租賃商業同業公會（代表人李源鐘先生）、中華民國銀行商業同業公會全國聯合會（代表人呂桔誠先生）、中華民國票券金融商業同業公會（代表人廖美祝女士）、中華民國信託業商業同業公會（代表人雷仲達先生）

副本：本會證券期貨局、保險局、檢查局(均含附件)

DPRK Cyber Threat Advisory

Issued: **April 15, 2020**

Title: **Guidance on the North Korean Cyber Threat**

The U.S. Departments of State, the Treasury, and Homeland Security, and the Federal Bureau of Investigation are issuing this advisory as a comprehensive resource on the North Korean cyber threat for the international community, network defenders, and the public. The advisory highlights the cyber threat posed by North Korea – formally known as the Democratic People's Republic of Korea (DPRK) – and provides recommended steps to mitigate the threat. In particular, Annex 1 lists U.S. government resources related to DPRK cyber threats and Annex 2 includes a link to the UN 1718 Sanctions Committee (DPRK) Panel of Experts reports.

The DPRK's malicious cyber activities threaten the United States and the broader international community and, in particular, pose a significant threat to the integrity and stability of the international financial system. Under the pressure of robust U.S. and UN sanctions, the DPRK has increasingly relied on illicit activities – including cybercrime – to generate revenue for its weapons of mass destruction and ballistic missile programs. In particular, the United States is deeply concerned about North Korea's malicious cyber activities, which the U.S. government refers to as HIDDEN COBRA. The DPRK has the capability to conduct disruptive or destructive cyber activities affecting U.S. critical infrastructure. The DPRK also uses cyber capabilities to steal from financial institutions, and has demonstrated a pattern of disruptive and harmful cyber activity that is wholly inconsistent with the growing international consensus on what constitutes responsible State behavior in cyberspace.

The United States works closely with like-minded countries to focus attention on and condemn the DPRK's disruptive, destructive, or otherwise destabilizing behavior in cyberspace. For example, in December 2017, Australia, Canada, New Zealand, the United States, and the United Kingdom publicly attributed the WannaCry 2.0 ransomware attack to the DPRK and denounced the DPRK's harmful and irresponsible cyber activity. Denmark and Japan issued supporting statements for the joint denunciation of the destructive WannaCry 2.0 ransomware attack, which affected hundreds of thousands of computers around the world in May 2017.

It is vital for the international community, network defenders, and the public to stay vigilant and to work together to mitigate the cyber threat posed by North Korea.

DPRK's Malicious Cyber Activities Targeting the Financial Sector

Many DPRK cyber actors are subordinate to UN- and U.S.-designated entities, such as the Reconnaissance General Bureau. DPRK state-sponsored cyber actors primarily consist of hackers, cryptologists, and software developers who conduct espionage, cyber-enabled theft targeting financial institutions and digital currency exchanges, and politically-motivated operations against foreign media companies. They develop and deploy a wide range of malware tools around the world to enable these activities and have grown increasingly sophisticated. Common tactics to raise revenue illicitly by DPRK state-sponsored cyber actors include, but are not limited to:

Cyber-Enabled Financial Theft and Money Laundering. The UN Security Council 1718 Committee Panel of Experts' 2019 mid-term report (2019 POE mid-term report) states that the DPRK is increasingly able to generate revenue notwithstanding UN Security Council sanctions by using malicious cyber activities to steal from financial institutions through increasingly sophisticated tools and tactics. The 2019 POE mid-term report notes that, in some cases, these malicious cyber activities have also extended to laundering funds through multiple jurisdictions. The 2019 POE mid-term report mentions that it was investigating dozens of suspected DPRK cyber-enabled heists and that, as of late 2019, the DPRK has attempted to steal as much as $2 billion through these illicit cyber activities. Allegations in a March 2020 Department of Justice forfeiture complaint are consistent with portions of the POE's findings. Specifically, the forfeiture complaint alleged how North Korean cyber actors used North Korean infrastructure in furtherance of their conspiracy to hack digital currency exchanges, steal hundreds of millions of dollars in digital currency, and launder the funds.

Extortion Campaigns. DPRK cyber actors have also conducted extortion campaigns against third-country entities by compromising an entity's network and threatening to shut it down unless the entity pays a ransom. In some instances, DPRK cyber actors have demanded payment from victims under the guise of long-term paid consulting arrangements in order to ensure that no such future malicious cyber activity takes place. DPRK cyber actors have also been paid to hack websites and extort targets for third-party clients.

Cryptojacking. The 2019 POE mid-term report states that the POE is also investigating the DPRK's use of "cryptojacking," a scheme to compromise a victim machine and steal its computing resources to mine digital currency. The POE has identified several incidents in which computers infected with cryptojacking malware sent the mined assets – much of it anonymity-enhanced digital currency (sometimes also referred to as "privacy coins") – to servers located in the DPRK, including at Kim Il Sung University in Pyongyang.

These activities highlight the DPRK's use of cyber-enabled means to generate revenue while mitigating the impact of sanctions and show that any country can be exposed to and exploited by the DPRK. According to the 2019 POE mid-term report, the POE is also investigating such activities as attempted violations of UN Security Council sanctions on the DPRK.

Cyber Operations Publicly Attributed to DPRK by U.S. Government

The DPRK has repeatedly targeted U.S. and other government and military networks, as well as networks related to private entities and critical infrastructure, to steal data and conduct disruptive and destructive cyber activities. To date, the U.S. government has publicly attributed the following cyber incidents to DPRK state-sponsored cyber actors and co-conspirators:

- ***Sony Pictures***. In November 2014, DPRK state-sponsored cyber actors allegedly launched a cyber attack on Sony Pictures Entertainment (SPE) in retaliation for the 2014 film "The Interview." DPRK cyber actors hacked into SPE's network to steal confidential data, threatened SPE executives and employees, and damaged thousands of computers.

    - FBI's Update on Sony Investigation (Dec. 19, 2014) https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation
    - DOJ's Criminal Complaint of a North Korean Regime-Backed Programmer (Sept. 6, 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- ***Bangladesh Bank Heist***. In February 2016, DPRK state-sponsored cyber actors allegedly attempted to steal at least $1 billion from financial institutions across the world and allegedly stole $81 million from the Bangladesh Bank through unauthorized transactions on the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network. According to the complaint, DPRK cyber actors accessed the Bangladesh Bank's computer terminals that interfaced with the SWIFT network after compromising the bank's computer network via spear phishing emails targeting bank employees. DPRK cyber actors then sent fraudulently authenticated SWIFT messages directing the Federal Reserve Bank of New York to transfer funds out of the Bangladesh Bank's Federal Reserve account to accounts controlled by the conspirators.

    - DOJ's Criminal Complaint of a North Korean Regime-Backed Programmer (Sept. 6, 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- ***WannaCry 2.0***. DPRK state-sponsored cyber actors developed the ransomware known as WannaCry 2.0, as well as two prior versions of the ransomware. In May 2017, WannaCry 2.0 ransomware infected hundreds of thousands of computers in hospitals, schools, businesses, and homes in over 150 countries. WannaCry 2.0 ransomware encrypts an infected computer's data and allows the cyber actors to demand ransom payments in the Bitcoin digital currency. The Department of the Treasury designated one North Korean computer programmer for his part in the WannaCry 2.0 conspiracy, as well as his role in the Sony Pictures cyber attack and Bangladesh Bank heist, and additionally designated the organization he worked for.

- CISA's Technical Alert: Indicators Associated with WannaCry Ransomware (May 12, 2017) https://www.us-cert.gov/ncas/alerts/TA17-132A
- White House Press Briefing on the Attribution of WannaCry Ransomware (Dec. 19, 2017) https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/
- DOJ's Criminal Complaint of a North Korean Regime-Backed Programmer (Sept. 6, 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and
- Treasury Targets North Korea for Multiple Cyber-Attacks (Sept. 6, 2018) https://home.treasury.gov/news/press-releases/sm473

- ***FASTCash Campaign.*** Since late 2016, DPRK state-sponsored cyber actors have employed a fraudulent ATM cash withdrawal scheme known as "FASTCash" to steal tens of millions of dollars from ATMs in Asia and Africa. FASTCash schemes remotely compromise payment switch application servers within banks to facilitate fraudulent transactions. In one incident in 2017, DPRK cyber actors enabled the withdrawal of cash simultaneously from ATMs located in more than 30 different countries. In another incident in 2018, DPRK cyber actors enabled cash to be simultaneously withdrawn from ATMs in 23 different countries.

  - CISA's Alert on FASTCash Campaign (Oct. 2, 2018) https://www.us-cert.gov/ncas/alerts/TA18-275A
  - CISA's Malware Analysis Report: FASTCash-Related Malware (Oct. 2, 2018) https://www.us-cert.gov/ncas/analysis-reports/AR18-275A

- ***Digital Currency Exchange Hack***. As detailed in allegations set forth in a Department of Justice complaint for forfeiture *in rem*, in April 2018, DPRK state-sponsored cyber actors hacked into a digital currency exchange and stole nearly $250 million worth of digital currency. The complaint further described how the stolen assets were laundered through hundreds of automated digital currency transactions, to obfuscate the origins of the funds, in an attempt to prevent law enforcement from tracing the assets. Two Chinese nationals are alleged in the complaint to have subsequently laundered the assets on behalf of the North Korean group, receiving approximately $91 million from DPRK-controlled accounts, as well as an additional $9.5 million from a hack of another exchange. In March 2020, the Department of the Treasury designated the two individuals under cyber and DPRK sanctions authorities, concurrent with a Department of Justice announcement that the individuals had been previously indicted on money laundering and unlicensed money transmitting charges and that 113 digital currency accounts were subject to forfeiture.

  - Treasury's Sanctions against Individuals Laundering Cryptocurrency for Lazarus Group (March 2, 2020) https://home.treasury.gov/news/press-releases/sm924
  - DOJ's Indictment of Two Chinese Nationals Charged with Laundering Cryptocurrency from Exchange Hack and Civil Forfeiture Complaint (March 2, 2020) https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack

Measures to Counter the DPRK Cyber Threat

North Korea targets cyber-enabled infrastructure globally to generate revenue for its regime priorities, including its weapons of mass destruction programs. We strongly urge governments, industry, civil society, and individuals to take all relevant actions below to protect themselves from and counter the DPRK cyber threat:

- **Raise Awareness of the DPRK Cyber Threat**. Highlighting the gravity, scope, and variety of malicious cyber activities carried out by the DPRK will raise general awareness across the public and private sectors of the threat and promote adoption and implementation of appropriate preventive and risk mitigation measures.

- **Share Technical Information of the DPRK Cyber Threat**. Information sharing at both the national and international levels to detect and defend against the DPRK cyber threat will enable enhanced cybersecurity of networks and systems. Best practices should be shared with governments and the private sector. Under the provisions of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. §§ 1501–1510), non-federal entities may share cyber threat indicators and defensive measures related to HIDDEN COBRA with federal and non-federal entities.

- **Implement and Promote Cybersecurity Best Practices**. Adopting measures – both technical and behavioral – to enhance cybersecurity will make U.S. and global cyber infrastructure more secure and resilient. Financial institutions, including money services businesses, should take independent steps to protect against malicious DPRK cyber activities. Such steps may include, but are not limited to, sharing threat information through government and/or industry channels, segmenting networks to minimize risks, maintaining regular backup copies of data, undertaking awareness training on common social engineering tactics, implementing policies governing information sharing and network access, and developing cyber incident response plans. The Department of Energy's Cybersecurity Capability Maturity Model and the National Institute of Standards and Technology's Cybersecurity Framework provide guidance on developing and implementing robust cybersecurity practices. As shown in Annex I, the Cybersecurity and Infrastructure Security Agency (CISA) provides extensive resources, including technical alerts and malware analysis reports, to enable network defenders to identify and reduce exposure to malicious cyber activities.

- **Notify Law Enforcement**. If an organization suspects that it has been the victim of malicious cyber activity, emanating from the DPRK or otherwise, it is critical to notify law enforcement in a timely fashion. This not only can expedite the investigation, but also, in the event of a financial crime, can increase the chances of recovering any stolen assets.

  U.S. law enforcement has seized millions of dollars' worth of digital currency stolen by North Korean cyber actors. All types of financial institutions, including money services businesses, are encouraged to cooperate on the front end by complying with U.S. law enforcement requests for information regarding these cyber threats, and on

the back end by identifying forfeitable assets upon receipt of a request from U.S. law enforcement or U.S. court orders, and by cooperating with U.S. law enforcement to support the seizure of such assets.

- **Strengthen Anti-Money Laundering (AML) / Countering the Financing of Terrorism (CFT) / Counter-Proliferation Financing (CPF) Compliance**. Countries should swiftly and effectively implement the Financial Action Task Force (FATF) standards on AML/CFT/CPF. This includes ensuring financial institutions and other covered entities employ risk mitigation measures in line with the FATF standards and FATF public statements and guidance. Specifically, the FATF has called for all countries to apply countermeasures to protect the international financial system from the ongoing money laundering, terrorist financing, and proliferation financing risks emanating from the DPRK.[1] This includes advising all financial institutions and other covered entities to give special attention to business relationships and transactions with the DPRK, including DPRK companies, financial institutions, and those acting on their behalf. In line with UN Security Council Resolution 2270 Operative Paragraph 33, Member States should close existing branches, subsidiaries, and representative offices of DPRK banks within their territories and terminate correspondent relationships with DPRK banks.

  Further, in June 2019, FATF amended its standards to require all countries regulate and supervise digital asset service providers, including digital currency exchanges, and mitigate against risks when engaging in digital currency transactions. Digital asset service providers should remain alert to changes in customers' activities, as their business may be used to facilitate money laundering, terrorist financing, and proliferation financing. The United States is particularly concerned about platforms that provide anonymous payment and account service functionality without transaction monitoring, suspicious activity reporting, and customer due diligence, among other obligations.

  U.S. financial institutions, including foreign-located digital asset service providers doing business in whole or substantial part in the United States, and other covered businesses and persons should ensure that they comply with their regulatory obligations under the Bank Secrecy Act (as implemented through the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) regulations in 31 CFR Chapter X). For financial institutions, these obligations include developing and maintaining effective anti-money laundering programs that are reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities, as well as identifying and reporting suspicious transactions, including those conducted, affected, or facilitated by cyber events or illicit finance involving digital assets, in suspicious activity reporting to FinCEN.

[1] *The full FATF Call to Action on North Korea can be found here:* https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html.

International Cooperation. To counter the DPRK's malicious cyber activities, the United States regularly engages with countries around the world to raise awareness of the DPRK cyber threat by sharing information and evidence via diplomatic, military, law enforcement and judicial, network defense, and other channels. To hamper the DPRK's efforts to steal funds through cyber means and to defend against the DPRK's malicious cyber activities, the United States strongly urges countries to strengthen network defense, shutter DPRK joint ventures in third countries, and expel foreign-located North Korean information technology (IT) workers in a manner consistent with applicable international law. A 2017 UN Security Council resolution required all Member States to repatriate DPRK nationals earning income abroad, including IT workers, by December 22, 2019. The United States also seeks to enhance the capacity of foreign governments and the private sector to understand, identify, defend against, investigate, prosecute, and respond to DPRK cyber threats and participate in international efforts to help ensure the stability of cyberspace.

Consequences of Engaging in Prohibited or Sanctionable Conduct

Individuals and entities engaged in or supporting DPRK cyber-related activity, including processing related financial transactions, should be aware of the potential consequences of engaging in prohibited or sanctionable conduct.

The Department of the Treasury's Office of Foreign Assets Control (OFAC) has the authority to impose sanctions on any person determined to have, among other things:

- Engaged in significant activities undermining cybersecurity on behalf of the Government of North Korea or the Workers' Party of Korea;
- Operated in the information technology (IT) industry in North Korea;
- Engaged in certain other malicious cyber-enabled activities; or
- Engaged in at least one significant importation from or exportation to North Korea of any goods, services, or technology.

Additionally, if the Secretary of the Treasury, in consultation with the Secretary of State, determines that a foreign financial institution has knowingly conducted or facilitated significant trade with North Korea, or knowingly conducted or facilitated a significant transaction on behalf of a person designated under a North Korea-related Executive Order, or under Executive Order 13382 (Weapons of Mass Destruction Proliferators and Their Supporters) for North Korea-related activity, that institution may, among other potential restrictions, lose the ability to maintain a correspondent or payable-through account in the United States.

OFAC investigates apparent violations of its sanctions regulations and exercises enforcement authority, as outlined in the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, appendix A. Persons who violate the North Korea Sanctions Regulations, 31 C.F.R. part 510, may face civil monetary penalties of up to the greater of the applicable statutory maximum penalty or twice the value of the underlying transaction.

The 2019 POE mid-term report notes the DPRK's use, and attempted use, of cyber-enabled means to steal funds from banks and digital currency exchanges could violate multiple UN

Security Council resolutions (UNSCRs) (*i.e.*, UNSCR 1718 operative paragraph (OP) 8(d); UNSCR 2094, OPs 8 and 11; and UNSCR 2270, OP 32). The DPRK-related UNSCRs also provide various mechanisms for encouraging compliance with DPRK-related sanctions imposed by the UN. For example, the UN Security Council 1718 Committee may impose targeted sanctions (*i.e.*, an asset freeze and, for individuals, a travel ban) on any individual or entity who engages in a business transaction with UN-designated entities or sanctions evasion.

The Department of Justice criminally prosecutes willful violations of applicable sanctions laws, such as the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701 et seq. Persons who willfully violate such laws may face up to 20 years of imprisonment, fines of up to $1 million or totaling twice the gross gain, whichever is greater, and forfeiture of all funds involved in such transactions. The Department of Justice also criminally prosecutes willful violations of the Bank Secrecy Act (BSA), 31 U.S.C. §§ 5318 and 5322, which requires financial institutions to, among other things, maintain effective anti-money laundering programs and file certain reports with FinCEN. Persons violating the BSA may face up to 5 years imprisonment, a fine of up to $250,000, and potential forfeiture of property involved in the violations. Where appropriate, the Department of Justice will also criminally prosecute corporations and other entities that violate these statutes. The Department of Justice also works with foreign partners to share evidence in support of each other's criminal investigations and prosecutions.

Pursuant to 31 U.S. Code § 5318(k), the Secretary of the Treasury or the Attorney General may subpoena a foreign financial institution that maintains a correspondent bank account in the United States for records stored overseas. Where the Secretary of the Treasury or Attorney General provides written notice to a U.S. financial institution that a foreign financial institutions has failed to comply with such a subpoena, the U.S. financial institution must terminate the correspondent banking relationship within ten business days. Failure to do so may subject the U.S. financial institutions to daily civil penalties.

DPRK Rewards for Justice

If you have information about illicit DPRK activities in cyberspace, including past or ongoing operations, providing such information through the Department of State's Rewards for Justice program could make you eligible to receive an award of up to $5 million. For further details, please visit www.rewardsforjustice.net.

ANNEX I: USG Public Information on and Resources to Counter the DPRK Cyber Threat

Office of the Director of National Intelligence Annual Worldwide Threat Assessments of the U.S. Intelligence Community. In 2019, the U.S. Intelligence Community assessed that the DPRK poses a significant cyber threat to financial institutions, remains a cyber espionage threat, and retains the ability to conduct disruptive cyber attacks. The DPRK continues to use cyber capabilities to steal from financial institutions to generate revenue. Pyongyang's cybercrime operations include attempts to steal more than $1.1 billion from financial institutions across the world – including a successful cyber heist of an estimated $81 million from Bangladesh Bank. The report can be found at https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

Cybersecurity and Infrastructure Security Agency (CISA) Technical Reports. The U.S. government refers to the malicious cyber activities by the DPRK as HIDDEN COBRA. HIDDEN COBRA reports provide technical details on the tools and infrastructure used by DPRK cyber actors. These reports enable network defenders to identify and reduce exposure to the DPRK's malicious cyber activities. CISA's website contains the latest updates on these persistent threats: https://www.us-cert.gov/northkorea.

Additionally, CISA provides extensive cybersecurity and infrastructure security knowledge and practices to its stakeholders, shares that knowledge to enable better risk management, and puts it into practice to protect the nation's critical functions. Below are the links to CISA's resources:

- Protecting Critical Infrastructure: https://www.cisa.gov/protecting-critical-infrastructure
- Cyber Safety: https://www.cisa.gov/cyber-safety
- Detection and Prevention: https://www.cisa.gov/detection-and-prevention
- Information Sharing: https://www.cisa.gov/information-sharing-and-awareness
- CISA Insights: https://www.cisa.gov/insights
- Combating Cyber Crime: https://www.cisa.gov/combating-cyber-crime
- Cyber Essentials: https://www.cisa.gov/cyber-essentials
- Tips: https://www.us-cert.gov/ncas/tips
- National Cyber Awareness System: https://www.us-cert.gov/ncas
- Industrial Control Systems Advisories: https://www.us-cert.gov/ics
- Report Incidents, Phishing, Malware, and Vulnerabilities: https://www.us-cert.gov/report

FBI PIN and FLASH Reports. FBI Private Industry Notifications (PIN) provide current information that will enhance the private sector's awareness of a potential cyber threat. FBI Liaison Alert System (FLASH) reports contain critical information collected by the FBI for use by specific private sector partners. They are intended to provide recipients with actionable intelligence that help cybersecurity professionals and system administrators to guard against the persistent malicious actions of cyber criminals. If you identify any suspicious activity within your enterprise or have related information, please contact FBI CYWATCH immediately. For DPRK-related cyber threat PIN or FLASH reports, contact cywatch@fbi.gov.

- FBI Cyber Division: https://www.fbi.gov/investigate/cyber

- FBI Legal Attaché Program: The FBI Legal Attaché's core mission is to establish and maintain liaison with principal law enforcement and security services in designated foreign countries. https://www.fbi.gov/contact-us/legal-attache-offices

U.S. Cyber Command Malware Information Release. The Department of Defense's cyber forces actively seek out DPRK malicious cyber activities, including DPRK malware that exploits financial institutions, conducts espionage, and enables malicious cyber activities against the U.S. and its partners. U.S. Cyber Command periodically releases malware information, identifying vulnerabilities for industry and government to defend their infrastructure and networks against DPRK illicit activities. Malware information to bolster cybersecurity can be found at the following Twitter accounts: @US_CYBERCOM and @CNMF_VirusAlert.

U.S. Department of the Treasury Sanctions Information and Illicit Finance Advisories. ***The Office of Foreign Assets Control's*** (OFAC's) online Resource Center provides a wealth of information regarding DPRK sanctions and sanctions with respect to malicious cyber-enabled activities, including sanctions advisories, relevant statutes, Executive Orders, rules, and regulations relating to DPRK and cyber-related sanctions. OFAC has also published several frequently asked questions (FAQs) relating to DPRK sanctions, cyber-related sanctions, and digital currency. For questions or concerns related to OFAC sanctions regulations and requirements, please contact OFAC's Compliance Hotline at 1-800-540-6322 or OFAC_Feedback@treasury.gov.

- DPRK Sanctions
  - https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx
  - FAQs - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#nk
- Malicious Cyber Activities Sanctions
  - https://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx
  - FAQs - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#cyber
  - FAQs on Virtual Currency - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs

Financial Crimes Enforcement Network (FinCEN) has issued an advisory on North Korea's use of the international financial system (https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a008). FinCEN also issued specific advisories to financial institutions with suspicious activity reporting obligations that provide guidance on when and how to report cybercrime and/or digital currency-related criminal activity:

- Cybercrime
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005
- Illicit digital currency activity
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a003
- Businesses e-mail compromise
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a005
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003

Federal Financial Institutions Examination Council (FFIEC) developed the Cybersecurity Assessment Tool to help financial institutions identify their risks and determine their cybersecurity preparedness. The assessment tool can be found at https://www.ffiec.gov/cyberassessmenttool.htm.

ANNEX II: UN Panel of Experts Reports on the DPRK Cyber Threat

UN 1718 Sanctions Committee (DPRK) Panel of Experts Reports. The UN Security Council 1718 Sanctions Committee on the DPRK is supported by a Panel of Experts, who "gather, examine, and analyze information" from UN Member States, relevant UN bodies, and other parties on the implementation of the measures outlined in the UN Security Council Resolutions against North Korea. The Panel also makes recommendations on how to improve sanctions implementation by providing both a Midterm and a Final Report to the 1718 Committee. These reports can be found at https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports.

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA21-048A

February 17, 2021

AppleJeus: Analysis of North Korea's Cryptocurrency Malware

This Joint Cybersecurity Advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques.

SUMMARY

This joint advisory is the result of analytic efforts among the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Treasury (Treasury) to highlight the cyber threat to cryptocurrency posed by North Korea, formally known as the Democratic People's Republic of Korea (DPRK), and provide mitigation recommendations. Working with U.S. government partners, FBI, CISA, and Treasury assess that Lazarus Group—which these agencies attribute to North Korean state-sponsored advanced persistent threat (APT) actors—is targeting individuals and companies, including cryptocurrency exchanges and financial service companies, through the dissemination of cryptocurrency trading applications that have been modified to include malware that facilitates theft of cryptocurrency.

These cyber actors have targeted organizations for cryptocurrency theft in over 30 countries during the past year alone. It is likely that these actors view modified cryptocurrency trading applications as a means to circumvent international sanctions on North Korea—the applications enable them to gain entry into companies that conduct cryptocurrency transactions and steal cryptocurrency from victim accounts. As highlighted in FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks and the Guidance on the North Korean Cyber Threat, North Korea's state-sponsored cyber actors are targeting cryptocurrency exchanges and accounts to steal and launder hundreds of millions of dollars in cryptocurrency.[1][2][3] The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. For more information on HIDDEN COBRA activity, visit https://www.us-cert.cisa.gov/northkorea.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at https://www.fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.gov.

The U.S. Government has identified malware and indicators of compromise (IOCs) used by the North Korean government to facilitate cryptocurrency thefts; the cybersecurity community refers to this activity as "AppleJeus." This report catalogues AppleJeus malware in detail. North Korea has used AppleJeus malware posing as cryptocurrency trading platforms since at least 2018. In most instances, the malicious application—seen on both Windows and Mac operating systems—appears to be from a legitimate cryptocurrency trading company, thus fooling individuals into downloading it as a third-party application from a website that seems legitimate. In addition to infecting victims through legitimate-looking websites, HIDDEN COBRA actors also use phishing, social networking, and social engineering techniques to lure users into downloading the malware.

Refer to the following Malware Analysis Reports (MARs) for full technical details of AppleJeus malware and associated IOCs.

- MAR-10322463-1.v1: AppleJeus – Celas Trade Pro
- MAR-10322463-2.v1: AppleJeus – JMT Trading
- MAR-10322463-3.v1: AppleJeus – Union Crypto
- MAR-10322463-4.v1: AppleJeus – Kupay Wallet
- MAR-10322463-5.v1: AppleJeus – CoinGoTrade
- MAR-10322463-6.v1: AppleJeus – Dorusio
- MAR-10322463-7.v1: AppleJeus – Ants2Whale

TECHNICAL DETAILS

The North Korean government has used multiple versions of AppleJeus since the malware was initially discovered in 2018. This section outlines seven of the versions below. The MARs listed above provide further technical details of these versions. Initially, HIDDEN COBRA actors used websites that appeared to host legitimate cryptocurrency trading platforms to infect victims with AppleJeus; however, these actors are now also using other initial infection vectors such as phishing, social networking, and social engineering techniques to get users to download the malware.

Targeted Nations

HIDDEN COBRA actors have targeted institutions with AppleJeus malware in several sectors, including energy, finance, government, industrial, technology, and telecommunications. Since January 2020, the threat actors have targeted these sectors in the following countries: Argentina, Australia, Belgium, Brazil, Canada, China, Denmark, Estonia, Germany, Hong Kong, Hungary, India, Ireland, Israel, Italy, Japan, Luxembourg, Malta, the Netherlands, New Zealand, Poland, Russia, Saudi Arabia, Singapore, Slovenia, South Korea, Spain, Sweden, Turkey, the United Kingdom, Ukraine, and the United States (figure 1).

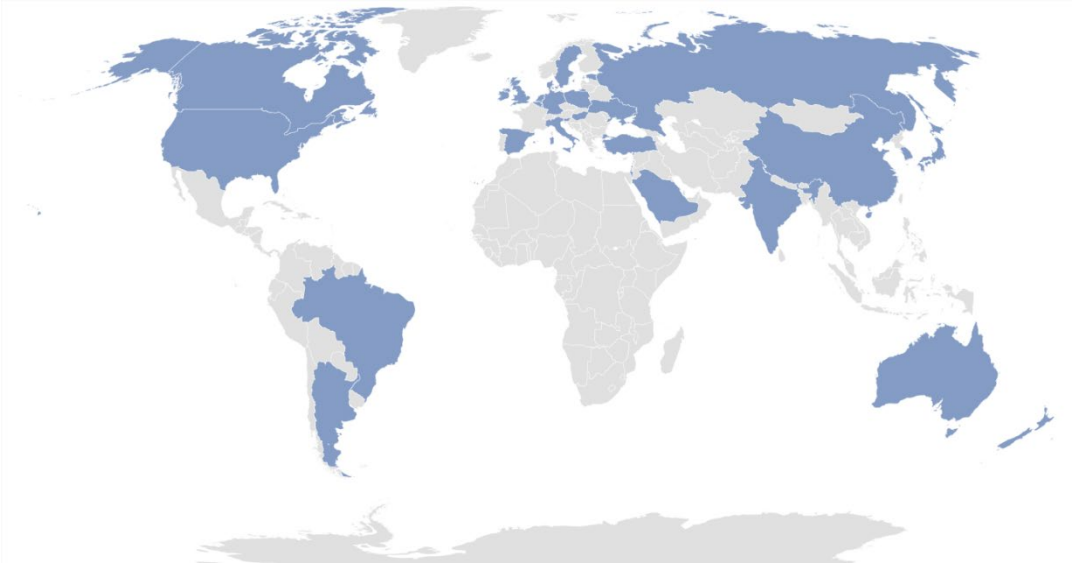

Figure 1: Countries targeted with AppleJeus by HIDDEN COBRA threat actors since 2020

AppleJeus Versions Note

The version numbers used for headings in this document correspond to the order the AppleJeus campaigns were identified in open source or through other investigative means. These versions may or may not be in the correct order to develop or deploy the AppleJeus campaigns.

AppleJeus Version 1: Celas Trade Pro

Introduction and Infrastructure

In August 2018, open-source reporting disclosed information about a trojanized version of a legitimate cryptocurrency trading application on an undisclosed victim's computer. The malicious program, known as Celas Trade Pro, was a modified version of the benign Q.T. Bitcoin Trader application. This incident led to the victim company being infected with a Remote Administration Tool (RAT) known as FALLCHILL, which was attributed to North Korea (HIDDEN COBRA) by the U.S. Government. FALLCHILL is a fully functional RAT with multiple commands that the adversary can issue from a command and control (C2) server to infected systems via various proxies. FALLCHILL typically infects a system as a file dropped by other HIDDEN COBRA malware (*Develop Capabilities: Malware* [T1587.001]). Because of this, additional HIDDEN COBRA malware may be present on systems compromised with FALLCHILL.[4]

Further research revealed that a phishing email from a Celas LLC company (*Phishing: Spearphishing Link* [T1566.002]) recommended the trojanized cryptocurrency trading application to victims. The email provided a link to the Celas' website, `celasllc[.]com` (*Acquire Infrastructure: Domain* [T1583.001]), where the victim could download a Windows or macOS version of the trojanized application.

The `celasllc[.]com` domain resolved to the following Internet Protocol (IP) addresses from May 29, 2018, to January 23, 2021.

- `45.199.63[.]220`
- `107.187.66[.]103`
- `145.249.106[.]19`
- `175.29.32[.]160`
- `185.142.236[.]213`
- `185.181.104[.]82`
- `198.251.83[.]27`
- `208.91.197[.]46`
- `209.99.64[.]18`

The `celasllc[.]com` domain had a valid Sectigo (previously known as Comodo) Secure Sockets Layer (SSL) certificate (*Obtain Capabilities: Digital Certificates* [T1588.004]). The SSL certificate was "Domain Control Validated," a weak security verification level that does not require validation of the owner's identity or the actual business's existence.

Celas Trade Pro Application Analysis

Windows Program

The Windows version of the malicious Celas Trade Pro application is an MSI Installer (`.msi`). The MSI Installer installation package comprises a software component and an application programming interface (API) that Microsoft uses for the installation, maintenance, and removal of software. The installer looks legitimate and is signed by a valid Sectigo certificate that was purchased by the same user as the SSL certificate for celasllc[.]com (*Obtain Capabilities: Code Signing Certificates* [T1588.003]). The MSI Installer asks the victim for administrative privileges to run (*User Execution: Malicious File* [T1204.002]).

Once permission is granted, the threat actor is able to run the program with elevated privileges (*Abuse Elevation Control Mechanism* [T1548]) and MSI executes the following actions.

- Installs `CelasTradePro.exe` in folder `C:\Program Files (x86)\CelasTradePro`
- Installs `Updater.exe` in folder `C:\Program Files (x86)\CelasTradePro`
- Runs `Updater.exe` with the `CheckUpdate` parameters

The `CelasTradePro.exe` program asks for the user's exchange and loads a legitimate-looking cryptocurrency trading platform—very similar to the benign Q.T. Bitcoin Trader—that exhibits no signs of malicious activity.

The `Updater.exe` program has the same program icon as `CelasTradePro.exe`. When run, it checks for the `CheckUpdate` parameter, collects the victim's host information (*System Owner/User Discovery* [T1033]), encrypts the collected information with a hardcoded XOR encryption, and sends information to a C2 website (*Exfiltration Over C2 Channel* [T1041]).

macOS X Program

The macOS version of the malicious application is a DMG Installer that has a disk image format that Apple commonly uses to distribute software over the internet. The installer looks legitimate and has a valid digital signature from Sectigo (*Obtain Capabilities: Digital Certificates* [T1588.004]). It has very similar functionality to the Windows version. The installer executes the following actions.

- Installs `CelasTradePro` in folder `/Applications/CelasTradePro.app/Contents/MacOS/`
- Installs `Updater` in folder `/Applications/CelasTradePro.app/Contents/MacOS/`
- Executes a `postinstall` script
    - Moves `.com.celastradepro.plist` to folder `LaunchDaemons`
    - Runs `Updater` with the `CheckUpdate` parameter

`CelasTradePro` asks for the user's exchange and loads a legitimate-looking cryptocurrency trading platform—very similar to the benign Q.T. Bitcoin Trader—that exhibits no signs of malicious activity.

`Updater` checks for the `CheckUpdate` parameter and, when found, it collects the victim's host information (*System Owner/User Discovery* [T1033]), encrypts the collected information with a hardcoded XOR key before exfiltration, and sends the encrypted information to a C2 website (*Exfiltration Over C2 Channel* [T1041]). This process helps the adversary obtain persistence on a victim's network.

The `postinstall` script is a sequence of instructions that runs after successfully installing an application (*Command and Scripting Interpreter: AppleScript* [T1059.002]). This script moves property list (`plist`) file `.com.celastradepro.plist` from the installer package to the `LaunchDaemons` folder (*Scheduled Task/Job: Launchd* [T1053.004]). The leading "." makes it unlisted in the Finder app or default Terminal directory listing (*Hide Artifacts: Hidden Files and Directories* [T1564.001]). Once in the folder, this property list (`plist`) file will launch the `Updater` program with the `CheckUpdate` parameter on system load as Root for every user. Because the `LaunchDaemon` will not run automatically after the `plist` file is moved, the `postinstall` script launches the `Updater` program with the `CheckUpdate` parameter and runs it in the background (*Create or Modify System Process: Launch Daemon* [T1543.004]).

Payload

After a cybersecurity company published a report detailing the above programs and their malicious extras, the website was no longer accessible. Since this site was the C2 server, the payload cannot be confirmed. The cybersecurity company that published the report states the payload was an encrypted and obfuscated binary (*Obfuscated Files or Information* [T1027]), which eventually drops FALLCHILL onto the machine and installs it as a service (*Create or Modify System Process: Windows Service* [T1543.003]). FALLCHILL malware uses an RC4 encryption algorithm with a 16-byte key to protect its communications (*Encrypted Channel: Symmetric Cryptography* [T1573.001]). The key employed in these versions has also been used in a previous version of FALLCHILL.[5][6]

For more details on AppleJeus Version 1: Celas Trade Pro, see MAR-10322463-1.v1.

AppleJeus Version 2: JMT Trading

Introduction and Infrastructure

In October 2019, a cybersecurity company identified a new version of the AppleJeus malware—JMT Trading—thanks to its many similarities to the original AppleJeus malware. Again, the malware was in the form of a cryptocurrency trading application, which a legitimate-looking company, called JMT Trading, marketed and distributed on their website, `jmttrading[.]org` (*Acquire Infrastructure: Domain* [T1583.001]). This website contained a "*Download from GitHub*" button, which linked to JMT Trading's GitHub page (*Acquire Infrastructure: Web Services* [T1583.006]), where Windows and macOS X versions of the JMT Trader application were available for download (*Develop Capabilities: Malware* [T1587.001]). The GitHub page also included .zip and tar.gz files containing the source code.

The `jmttrading[.]org` domain resolved to the following IP addresses from October 15, 2016, to January 22, 2021.

- `45.33.2[.]79`
- `45.33.23[.]183`
- `45.56.79[.]23`
- `45.79.19[.]196`
- `96.126.123[.]244`
- `146.112.61[.]107`
- `184.168.221[.]40`
- `184.168.221[.]57`
- `198.187.29[.]20`
- `198.54.117[.]197`
- `198.54.117[.]198`
- `198.54.117[.]199`
- `198.54.117[.]200`
- `198.58.118[.]167`

The `jmttrading[.]org` domain had a valid Sectigo SSL certificate (*Obtain Capabilities: Digital Certificates* [T1588.004]). The SSL certificate was "Domain Control Validated," a weak security verification level that does not require validation of the owner's identity or the actual business's existence. The current SSL certificate was issued by Let's Encrypt.

JMT Trading Application Analysis

Windows Program

The Windows version of the malicious cryptocurrency application is an MSI Installer. The installer looks legitimate and has a valid digital signature from Sectigo (*Obtain Capabilities: Digital Certificates* [T1588.004]). The signature was signed with a code signing certificate purchased by the same user

as the SSL certificate for `jmttrading[.]org` (*Obtain Capabilities: Code Signing Certificates* [T1588.003]). The MSI Installer asks the victim for administrative privileges to run (*User Execution: Malicious File* [T1204.002]).

Once permission is granted, the MSI executes the following actions.

- Installs `JMTTrader.exe` in folder `C:\Program Files (x86)\JMTTrader`
- Installs `CrashReporter.exe` in folder `C:\Users\<username>\AppData\Roaming\JMTTrader`
- Runs `CrashReporter.exe` with the `Maintain` parameter

The `JMTTrader.exe` program asks for the user's exchange and loads a legitimate-looking cryptocurrency trading platform—very similar to `CelasTradePro.exe` and the benign Q.T. Bitcoin Trader—that exhibits no signs of malicious activity.

The program `CrashReporter.exe` is heavily obfuscated with the ADVObfuscation library, renamed "snowman" (*Obfuscated Files or Information* [T1027]). When run, it checks for the `Maintain` parameter and collects the victim's host information (*System Owner/User Discovery* [T1033]), encrypts the collected information with a hardcoded XOR key before exfiltration, and sends the encrypted information to a C2 website (*Exfiltration Over C2 Channel* [T1041]). The program also creates a scheduled SYSTEM task, named `JMTCrashReporter`, which runs `CrashReporter.exe` with the `Maintain` parameter at any user's login (*Scheduled Task/Job: Scheduled Task* [T1053.005]).

macOS X Program

The macOS version of the malicious application is a DMG Installer. The installer looks legitimate and has very similar functionality to the Windows version, but it does not have a digital certificate and will warn the user of that before installation. The installer executes the following actions.

- Installs `JMTTrader` in folder `/Applications/JMTTrader.app/Contents/MacOS/`
- Installs `.CrashReporter` in folder `/Applications/JMTTrader.app/Contents/Resources/`
    - **Note:** the leading "." Makes it unlisted in the Finder app or default Terminal directory listing.
- Executes a `postinstall` script
    - Moves `.com.jmttrading.plist` to folder `LaunchDaemons`
    - Changes the file permissions on the plist
    - Runs `CrashReporter` with the Maintain parameter
    - Moves `.CrashReporter` to folder `/Library/JMTTrader/CrashReporter`
    - Makes `.CrashReporter` executable

The `JMTTrader` program asks for the user's exchange and loads a legitimate-looking cryptocurrency trading platform—very similar to `CelasTradePro` and the benign Q.T. Bitcoin Trader—that exhibits no signs of malicious activity.

The `CrashReporter` program checks for the `Maintain` parameter and is not obfuscated. This lack of obfuscation makes it easier to determine the program's functionality in detail. When it finds the

`Maintain` parameter, it collects the victim's host information (*System Owner/User Discovery* [T1033]), encrypts the collected information with a hardcoded XOR key before exfiltration, and sends the encrypted information to a C2 website (*Exfiltration Over C2 Channel* [T1041]).

The `postinstall` script has similar functionality to the one used by `CelasTradePro`, but it has a few additional features (*Command and Scripting Interpreter: AppleScript* [T1059.002]). It moves the property list (`plist`) file `.com.jmttrading.plist` from the Installer package to the `LaunchDaemons` folder (*Scheduled Task/Job: Launchd* [T1053.004]), but also changes the file permissions on the `plist` file. Once in the folder, this property list (`plist`) file will launch the `CrashReporter` program with the `Maintain` parameter on system load as Root for every user. Also, the `postinstall` script moves the `.CrashReporter` program to a new location `/Library/JMTTrader/CrashReporter` and makes it executable. Because the `LaunchDaemon` will not run automatically after the `plist` file is moved, the `postinstall` script launches `CrashReporter` with the `Maintain` parameter and runs it in the background (*Create or Modify System Process: Launch Daemon* [T1543.004]).

Payload

Soon after the cybersecurity company tweeted about JMT Trader on October 11, 2019, the files on GitHub were updated to clean, non-malicious installers. Then on October 13, 2019, a different cybersecurity company published an article detailing the macOS X JMT Trader, and soon after, the C2 `beastgoc[.]com` website went offline. There is not a confirmed sample of the payload to analyze at this point.

For more details on AppleJeus Version 2: JMT Trading, see MAR-10322463-2.v1.

AppleJeus Version 3: Union Crypto

Introduction and Infrastructure

In December 2019, another version of the AppleJeus malware was identified on Twitter by a cybersecurity company based on many similarities to the original AppleJeus malware. Again, the malware was in the form of a cryptocurrency trading application, which was marketed and distributed by a legitimate-looking company, called Union Crypto, on their website, `unioncrypto[.]vip` (*Acquire Infrastructure: Domain* [T1583.001]). Although this website is no longer available, a cybersecurity researcher discovered a download link, `https://www.unioncrypto[.]vip/download/W6c2dq8By7luMhCmya2v97YeN`, recorded on VirusTotal for the macOS X version of `UnionCryptoTrader`. In contrast, open-source reporting stated that the Windows version might have been downloaded via instant messaging service Telegram, as it was found in a "Telegram Downloads" folder on an unnamed victim.[7]

The `unioncrypto[.]vip` domain resolved to the following IP addresses from June 5, 2019, to July 15, 2020.

- `104.168.167[.]16`
- `198.54.117[.]197`
- `198.54.117[.]198`

- `198.54.117[.]199`
- `198.54.117[.]200`

The domain `unioncrypto[.]vip` had a valid Sectigo SSL certificate (*Obtain Capabilities: Digital Certificates* [T1588.004]). The SSL certificate was "Domain Control Validated," a weak security verification level that does not require validation of the owner's identity or the actual business's existence.

Union Crypto Trader Application Analysis

Windows Program

The Windows version of the malicious cryptocurrency application is a Windows executable (`.exe`) (*User Execution: Malicious File* [T1204.002]), which acts as an installer that extracts a temporary MSI Installer.

The Windows program executes the following actions.

- Extracts `UnionCryptoTrader.msi` to folder `C:\Users\<username>\AppData\Local\Temp\{82E4B719-90F74BD1-9CF1-56CD777E0C42}`
- Runs `UnionCryptoUpdater.msi`
  - Installs `UnionCryptoTrader.exe` in folder `C:\Program Files\UnionCryptoTrader`
  - Installs `UnionCryptoUpdater.exe` in folder `C:\Users\<username>\AppData\Local\UnionCryptoTrader`
- Deletes `UnionCryptoUpdater.msi`
- Runs `UnionCryptoUpdater.exe`

The program `UnionCryptoTrader.exe` loads a legitimate-looking cryptocurrency arbitrage application—defined as "the simultaneous buying and selling of securities, currency, or commodities in different markets or in derivative forms to take advantage of differing prices for the same asset"—which exhibits no signs of malicious activity. This application is very similar to another cryptocurrency arbitrage application known as Blackbird Bitcoin Arbitrage.[8]

The program `UnionCryptoUpdater.exe` first installs itself as a service (*Create or Modify System Process: Windows Service* [T1543.003]), which will automatically start when any user logs on (*Boot or Logon Autostart Execution* [T1547]). The service is installed with a description stating it "Automatically installs updates for Union Crypto Trader." When launched, it collects the victim's host information (*System Owner/User Discovery* [T1033]), combines the information in a string that is MD5 hashed and stored in the `auth_signature` variable before exfiltration, and sends it to a C2 website (*Exfiltration Over C2 Channel* [T1041]).

macOS X Program

The macOS version of the malicious application is a DMG Installer. The installer looks legitimate and has very similar functionality to the Windows version, but it does not have a digital certificate and will warn the user of that before installation. The installer executes the following actions.

- Installs `UnionCryptoTrader` in folder `/Applications/UnionCryptoTrader.app/Contents/MacOS/`
- Installs `.unioncryptoupdater` in folder `/Applications/UnionCryptoTrader.app/Contents/Resources/`
    - **Note:** the leading "." makes it unlisted in the Finder app or default Terminal directory listing.
- Executes a `postinstall` script
    - Moves `.vip.unioncrypto.plist` to folder `LaunchDaemons`
    - Changes the file permissions on the plist to Root
    - Runs `unioncryptoupdater`
    - Moves `.unioncryptoupdater` to folder `/Library/UnionCrypto/unioncryptoupdater`
    - Makes `.unioncryptoupdater` executable

The `UnionCryptoTrader` program loads a legitimate-looking cryptocurrency arbitrage application, which exhibits no signs of malicious activity. The application is very similar to another cryptocurrency arbitrage application known as Blackbird Bitcoin Arbitrage.

The `.unioncryptoupdater` program is signed ad-hoc, meaning it is not signed with a valid code-signing identity. When launched, it collects the victim's host information (*System Owner/User Discovery* [T1033]), combines the information in a string that is MD5 hashed and stored in the `auth_signature` variable before exfiltration, and sends it to a C2 website (*Exfiltration Over C2 Channel* [T1041]).

The `postinstall` script has similar functionality to the one used by JMT Trading (*Command and Scripting Interpreter: AppleScript* [T1059.002]). It moves the property list (`plist`) file `.vip.unioncrypto.plist` from the Installer package to the `LaunchDaemons` folder (*Scheduled Task/Job: Launchd* [T1053.004]), but also changes the file permissions on the `plist` file to Root. Once in the folder, this property list (`plist`) file will launch the `.unioncryptoupdater` on system load as Root for every user. The `postinstall` script moves the `.unioncryptoupdater` program to a new location `/Library/UnionCrypto/unioncryptoupdater` and makes it executable. Because the `LaunchDaemon` will not run automatically after the `plist` file is moved, the `postinstall` script launches `.unioncryptoupdater` and runs it in the background (*Create or Modify System Process: Launch Daemon* [T1543.004]).

Payload

The payload for the Windows malware is a Windows Dynamic-Link-Library `UnionCryptoUpdater.exe` does not immediately download the stage 2 malware but instead

downloads it after a time specified by the C2 server. This delay could be implemented to prevent researchers from directly obtaining the stage 2 malware.

The macOS X malware's payload could not be downloaded, as the C2 server is no longer accessible. Additionally, none of the open-source reporting for this sample contained copies of the macOS X payload. The macOS X payload is likely similar in functionality to the Windows stage 2 detailed above.

For more details on AppleJeus Version 3: Union Crypto, see MAR-10322463-3.v1.

Commonalities between Celas Trade Pro, JMT Trading, and Union Crypto

Hardcoded Values

In each AppleJeus version, there are hardcoded values used for encryption or to create a signature when combined with the time (table 1).

Table 1: AppleJeus hardcoded values and uses

AppleJeus Version	Value	Use
1: Celas Trade Pro	Moz&Wie;#t/6T!2y	XOR encryption to send data
1: Celas Trade Pro	W29ab@ad%Df324V$Yd	RC4 decryption
2: JMT Trader Windows	X,%`PMk–Jj8s+6=15:20:11	XOR encryption to send data
2: JMT Trader OSX	X,%`PMk–Jj8s+6=\x02	XOR encryption to send data
3: Union Crypto Trader	12GWAPCT1F0I1S14	Combined with time for signature

The Union Crypto Trader and Celas LLC (XOR) values are 16 bytes in length. For JMT Trader, the first 16 bytes of the Windows and macOS X values are identical, and the additional bytes are in a time format for the Windows sample. The structure of a 16-byte value combined with the time is also used in Union Crypto Trader to create the `auth_signature`.

As mentioned, FALLCHILL was reported as the final payload for Celas Trade Pro. All FALLCHILL samples use 16-byte hardcoded RC4 keys for sending data, similar to the 16-byte keys in the AppleJeus samples.

Open-Source Cryptocurrency Applications

All three AppleJeus samples are bundled with modified copies of legitimate cryptocurrency applications and can be used as originally designed to trade cryptocurrency. Both Celas LLC and JMT Trader modified the same cryptocurrency application, Q.T. Bitcoin Trader; Union Crypto Trader modified the Blackbird Bitcoin Arbitrage application.

PostInstall Scripts, Property List Files, and LaunchDaemons

The macOS X samples of all three AppleJeus versions contain `postinstall` scripts with similar logic. The Celas LLC `postinstall` script only moves the `plist` file to a new location and launches `Updater` with the `CheckUpdate` parameter in the background. The JMT Trader and Union Crypto Trader also perform these actions and have identical functionality. The additional actions performed by both `postinstall` scripts are to change the file permissions on the `plist`, make a new directory in the `/Library` folder, move `CrashReporter or UnionCryptoUpdater` to the newly created folder, and make them executable.

The `plist` files for all three AppleJeus files have identical functionality. They only differ in the files' names and one default comment that was not removed from the Celas LLC `plist`. As the logic and functionality of the `postinstall` scripts and `plist` files are almost identical, the `LaunchDaemons` created also function the same. They will all launch the secondary executable as Root on system load for every user.

AppleJeus Version 4: Kupay Wallet

Introduction and Infrastructure

On March 13, 2020, a new version of the AppleJeus malware was identified. The malware was marketed and distributed by a legitimate-looking company, called Kupay Wallet, on their website `kupaywallet[.]com` (*Acquire Infrastructure: Domain* [T1583.001]).

The domain `www.kupaywallet[.]com` resolved to IP address `104.200.67[.]96` from March 20, 2020, to January 16, 2021. CrownCloud US LLC controlled the IP address (autonomous system number [ASN] 8100), and is located in New York, NY.

The domain `www.kupaywallet[.]com` had a valid Sectigo SSL certificate (*Obtain Capabilities: Digital Certificates* [T1588.004]). The SSL certificate was "Domain Control Validated," a weak security verification level that does not require validation of the owner's identity or the actual business's existence.

Kupay Wallet Application Analysis

Windows Program

The Windows version of the malicious cryptocurrency application is an MSI Installer. The MSI executes the following actions.

- Installs `Kupay.exe` in folder `C:\Program Files (x86)\Kupay`
- Installs `KupayUpgrade.exe` in folder `C:\Users\<username>\AppData\Roaming\KupaySupport`
- Runs `KupayUpgrade.exe`

The program `Kupay.exe` loads a legitimate-looking cryptocurrency wallet platform, which exhibits no signs of malicious activity and is very similar to an open-source platform known as Copay, distributed by Atlanta-based company BitPay.

The program `KupayUpgrade.exe` first installs itself as a service (*Create or Modify System Process: Windows Service* [T1543.003]), which will automatically start when any user logs on (*Boot or Logon Autostart Execution* [T1547]). The service is installed with a description stating it is an "Automatic Kupay Upgrade." When launched, it collects the victim's host information (*System Owner/User Discovery* [T1033]), combines the information in strings before exfiltration, and sends it to a C2 website (*Exfiltration Over C2 Channel* [T1041]).

macOS X Program

The macOS version of the malicious application is a DMG Installer. The installer looks legitimate and has very similar functionality to the Windows version, but it does not have a digital certificate and will warn the user of that before installation. The installer executes the following actions.

- Installs `Kupay` in folder `/Applications/Kupay.app/Contents/MacOS/`
- Installs `kupay_upgrade` in folder `/Applications/Kupay.app/Contents/MacOS/`
- Executes a `postinstall` script
    - Creates `KupayDaemon` folder in `/Library/Application Support` folder
    - Moves `kupay_upgrade` to the new folder
    - Moves `com.kupay.pkg.wallet.plist` to folder `/Library/LaunchDaemons/`
    - Runs the command `launchctl load` to load the plist without a restart
    - Runs `kupay_upgrade` in the background

`Kupay` is likely a copy of an open-source cryptocurrency wallet application, loads a legitimate-looking wallet program (fully functional), and its functionality is identical to the Windows `Kupay.exe` program.

The `kupay_upgrade` program calls its function CheckUpdate (which contains most of the logic functionality of the malware) and sends a POST to the C2 server with a connection named "*Kupay Wallet 9.0.1 (Check Update Osx)*" (*Application Layer Protocol: Web Protocols* [T1071.001]). If the C2 server returns a file, it is decoded and written to the victim's folder `/private/tmp/kupay_update` with permissions set by the command `chmod 700` (only the user can read, write, and execute) (*Command and Scripting Interpreter* [T1059]). Stage 2 is then launched, and the malware, `kupay_upgrade`, returns to sleeping and checking in with the C2 server at predetermined intervals (*Application Layer Protocol: Web Protocols* [T1071.001]).

The `postinstall` script has similar functionality to other AppleJeus scripts (*Command and Scripting Interpreter: AppleScript* [T1059.002]). It creates the `KupayDaemon` folder in `/Library/Application Support` folder and then moves `kupay_upgrade` to the new folder. It moves the property list (`plist`) file `com.kupay.pkg.wallet.plist` from the Installer package to the `/Library/LaunchDaemons/` folder (*Scheduled Task/Job: Launchd* [T1053.004]). The script runs the command `launchctl load` to load the plist without a restart (*Command and Scripting Interpreter* [T1059]). But, since the `LaunchDaemon` will not run automatically after the `plist` file is moved, the `postinstall` script launches `kupay_upgrade` and runs it in the background (*Create or Modify System Process: Launch Daemon* [T1543.004]).

Payload

The Windows malware's payload could not be downloaded since the C2 server is no longer accessible. Additionally, none of the open-source reporting for this sample contained copies of the payload. The Windows payload is likely similar in functionality to the macOS X stage 2 detailed below.

The stage 2 payload for the macOS X malware was decoded and analyzed. The stage 2 malware has a variety of functionalities. Most importantly, it checks in with a C2 and, after connecting to the C2, can send or receive a payload, read and write files, execute commands via the terminal, etc.

For more details on AppleJeus Version 4: Kupay Wallet, see MAR-10322463-4.v1.

AppleJeus Version 5: CoinGoTrade

Introduction and Infrastructure

In early 2020, another version of the AppleJeus malware was identified. This time the malware was marketed and distributed by a legitimate-looking company called CoinGoTrade on their website `coingotrade[.]com` (*Acquire Infrastructure: Domain* [T1583.001]).

The domain `CoinGoTrade[.]com` resolved to IP address `198.54.114[.]175` from February 28, 2020, to January 23, 2021. The IP address is controlled by NameCheap Inc. (ASN 22612) and is located in Atlanta, GA. This IP address is in the same ASN for `Dorusio[.]com` and `Ants2Whale[.]com`.

The domain `CoinGoTrade[.]com` had a valid Sectigo SSL certificate (*Obtain Capabilities: Digital Certificates* [T1588.004]). The SSL certificate was "Domain Control Validated," a weak security verification level that does not require validation of the owner's identity or the actual business's existence.

CoinGoTrade Application Analysis

Windows Program

The Windows version of the malicious application is an MSI Installer. The installer appears to be legitimate and will execute the following actions.

- Installs `CoinGoTrade.exe` in folder `C:\Program Files (x86)\CoinGoTrade`
- Installs `CoinGoTradeUpdate.exe` in folder `C:\Users\<username>\AppData\Roaming\CoinGoTradeSupport`
- Runs `CoinGoTradeUpdate.exe`

`CoinGoTrade.exe` loads a legitimate-looking cryptocurrency wallet platform with no signs of malicious activity and is a copy of an open-source cryptocurrency application.

`CoinGoTradeUpdate.exe` first installs itself as a service (*Create or Modify System Process: Windows Service* [T1543.003]), which will automatically start when any user logs on (*Boot or Logon Autostart*

Execution [T1547]). The service is installed with a description stating it is an "Automatic CoinGoTrade Upgrade." When launched, it collects the victim's host information (*System Owner/User Discovery* [T1033]), combines the information in strings before exfiltration, and sends it to a C2 website (*Exfiltration Over C2 Channel* [T1041]).

macOS X Program

The macOS version of the malicious application is a DMG Installer. The installer looks legitimate and has very similar functionality to the Windows version, but it does not have a digital certificate and will warn the user of that before installation. The installer executes the following actions.

- Installs `CoinGoTrade` in folder `/Applications/CoinGoTrade.app/Contents/MacOS/`
- Installs `CoinGoTradeUpgradeDaemon` in folder `/Applications/CoinGoTrade.app/Contents/MacOS/`
- Executes a `postinstall` script
    - Creates `CoinGoTradeService` folder in `/Library/Application Support` folder
    - Moves `CoinGoTradeUpgradeDaemon` to the new folder
    - Moves `com.coingotrade.pkg.product.plist` to folder `/Library/LaunchDaemons/`
    - Runs `CoinGoTradeUpgradeDaemon` in the background

The `CoinGoTrade` program is likely a copy of an open-source cryptocurrency wallet application and loads a legitimate-looking, fully functional wallet program).

The `CoinGoTradeUpgradeDaemon` program calls its function CheckUpdate (which contains most of the logic functionality of the malware) and sends a `POST` to the C2 server with a connection named "*CoinGoTrade 1.0 (Check Update Osx)*" (*Application Layer Protocol: Web Protocols* [T1071.001]). If the C2 server returns a file, it is decoded and written to the victim's folder `/private/tmp/updatecoingotrade` with permissions set by the command `chmod 700` (only the user can read, write, and execute) (*Command and Scripting Interpreter* [T1059]). Stage 2 is then launched, and the malware, `CoinGoTradeUpgradeDaemon`, returns to sleeping and checking in with the C2 server at predetermined intervals (*Application Layer Protocol: Web Protocols* [T1071.001]).

The `postinstall` script has similar functionality to the other scripts (*Command and Scripting Interpreter: AppleScript* [T1059.002]) and installs `CoinGoTrade` and `CoinGoTradeUpgradeDaemon` in folder `/Applications/CoinGoTrade.app/Contents/MacOS/`. It moves the property list (`plist`) file `com.coingotrade.pkg.product.plist` to the `/Library/LaunchDaemons/` folder (*Scheduled Task/Job: Launchd* [T1053.004]). Because the `LaunchDaemon` will not run automatically after the `plist` file is moved, the `postinstall` script launches `CoinGoTradeUpgradeDaemon` and runs it in the background (*Create or Modify System Process: Launch Daemon* [T1543.004]).

Payload

The Windows malware's payload could not be downloaded because the C2 server is no longer accessible. Additionally, none of the open-source reporting for this sample contained copies of the payload. The Windows payload is likely similar in functionality to the macOS X stage 2 detailed below.

The stage 2 payload for the macOS X malware was no longer available from the specified download URL. Still, a file was submitted to VirusTotal by the same user on the same date as the macOS X `CoinGoTradeUpgradeDaemon`. These clues suggest that the submitted file may be related to the macOS X version of the malware and the downloaded payload.

The file `prtspool` is a 64-bit Mach-O executable with a large variety of features that have all been confirmed as functionality. The file has three C2 URLs hardcoded into the file and communicates to these with HTTP POST multipart-form data boundary string. Like other HIDDEN COBRA malware, `prtspool` uses format strings to store data collected about the system and sends it to the C2s.

For more details on AppleJeus Version 5: CoinGoTrade, see MAR-10322463-5.v1.

AppleJeus Version 6: Dorusio

Introduction and Infrastructure

In March 2020, an additional version of the AppleJeus malware was identified. This time the malware was marketed and distributed by a legitimate-looking company called Dorusio on their website, `dorusio[.]com` (*Acquire Infrastructure: Domain* [T1583.001]). Researchers collected samples for Windows and macOS X versions of the Dorusio Wallet (*Develop Capabilities: Malware* [T1587.001]). As of at least early 2020, the actual download links result in `404` errors. The download page has release notes with version revisions claiming to start with version 1.0.0, released on April 15, 2019.

The domain `dorusio[.]com` resolved to IP address `198.54.115[.]51` from March 30, 2020 to January 23, 2021. The IP address is controlled by NameCheap Inc. (ASN 22612) and is located in Atlanta, GA. This IP address is in the same ASN for `CoinGoTrade[.]com` and `Ants2Whale[.]com`.

The domain `dorusio[.]com` had a valid Sectigo SSL certificate (*Obtain Capabilities: Digital Certificates* [T1588.004]). The SSL certificate was “Domain Control Validated,” a weak security verification level that does not require validation of the owner’s identity or the actual business’s existence.

Dorusio Application Analysis

Windows Program

The Windows version of the malicious application is an MSI Installer. The installer appears to be legitimate and will install the following two programs.

- Installs `Dorusio.exe` in folder `C:\Program Files (x86)\Dorusio`
- Installs `DorusioUpgrade.exe` in folder `C:\Users\<username>\AppData\Roaming\DorusioSupport`
- Runs `DorusioUpgrade.exe`

The program, `Dorusio.exe`, loads a legitimate-looking cryptocurrency wallet platform with no signs of malicious activity and is a copy of an open-source cryptocurrency application.

The program `DorusioUpgrade.exe` first installs itself as a service (*Create or Modify System Process: Windows Service* [T1543.003]), which will automatically start when any user logs on (*Boot or Logon Autostart Execution* [T1547]). The service is installed with a description stating it "Automatic Dorusio Upgrade." When launched, it collects the victim's host information (*System Owner/User Discovery* [T1033]), combines the information in strings before exfiltration, and sends it to a C2 website (*Exfiltration Over C2 Channel* [T1041]).

macOS X Program

The macOS version of the malicious application is a DMG Installer. The installer looks legitimate and has very similar functionality to the Windows version, but it does not have a digital certificate and will warn the user of that before installation. The installer executes the following actions.

- Installs `Dorusio` in folder `/Applications/Dorusio.app/Contents/MacOS/`
- Installs `Dorusio_upgrade` in folder `/Applications/Dorusio.app/Contents/MacOS/`
- Executes a `postinstall` script
    - Creates `DorusioDaemon` folder in `/Library/Application Support` folder
    - Moves `Dorusio_upgrade` to the new folder
    - Moves `com.dorusio.pkg.wallet.plist` to folder `/Library/LaunchDaemons/`
    - Runs `Dorusio_upgrade` in the background

The `Dorusio` program is likely a copy of an open-source cryptocurrency wallet application and loads a legitimate-looking wallet program (fully functional). Aside from the Dorusio logo and two new services, the wallet appears to be the same as the Kupay Wallet. This application seems to be a modification of the open-source cryptocurrency wallet Copay distributed by Atlanta-based company BitPay.

The `Dorusio_upgrade` program calls its function CheckUpdate (which contains most of the logic functionality of the malware) and sends a POST to the C2 server with a connection named "*Dorusio Wallet 2.1.0 (Check Update Osx)*" (*Application Layer Protocol: Web Protocols* [T1071.001]). If the C2 server returns a file, it is decoded and written to the victim's folder `/private/tmp/Dorusio_update` with permissions set by the command `chmod 700` (only the user can read, write, and execute) (*Command and Scripting Interpreter* [T1059]). Stage 2 is then launched, and the malware, `Dorusio_upgrade`, returns to sleeping and checking in with the C2 server at predetermined intervals (*Application Layer Protocol: Web Protocols* [T1071.001]).

The `postinstall` script has similar functionality to other AppleJeus scripts (*Command and Scripting Interpreter: AppleScript* [T1059.002]). It creates the `DorusioDaemon` folder in `/Library/Application Support` folder and then moves `Dorusio_upgrade` to the new folder. It moves the property list (`plist`) file `com.dorusio.pkg.wallet.plist` from the Installer package to the `/Library/LaunchDaemons/` folder (*Scheduled Task/Job: Launchd* [T1053.004]). Because the `LaunchDaemon` will not run automatically after the `plist` file is moved, the `postinstall` script launches `Dorusio_upgrade` and runs it in the background (*Create or Modify System Process: Launch Daemon* [T1543.004]).

Payload

Neither the payload for the Windows nor macOS X malware could be downloaded; the C2 server is no longer accessible. The payloads are likely similar in functionality to the macOS X stage 2 from CoinGoTrade and Kupay Wallet, or the Windows stage 2 from Union Crypto.

For more details on AppleJeus Version 6: Dorusio, see MAR-10322463-6.v1.

AppleJeus 4, 5, and 6 Installation Conflictions

If a user attempts to install the Kupay Wallet, CoinGoTrade, and Dorusio applications on the same system, they will encounter installation conflicts.

If Kupay Wallet is already installed on a system and the user tries to install CoinGoTrade or Dorusio:

- Pop-up windows appear, stating a more recent version of the program is already installed.

If CoinGoTrade is already installed on a system and the user attempts to install Kupay Wallet:

- `Kupay.exe` will be installed in the `C:\Program Files (x86)\CoinGoTrade\` folder.
- All `CoinGoTrade` files will be deleted.
- The folders and files contained in the `C:\Users\<username>\AppData\Roaming\CoinGoTradeSupport` will remain installed.
- `KupayUpgrade.exe` is installed in the new folder `C:\Users\<username>\AppData\Roaming\KupaySupport`.

If Dorusio is already installed on a system and the user attempts to install Kupay Wallet:

- `Kupay.exe` will be installed in the `C:\Program Files (x86)\Dorusio\` folder.
- All `Dorusio.exe` files will be deleted.
- The folders and files contained in `C:\Users\<username>\AppData\Roaming\DorusioSupport` will remain installed.
- `KupayUpgrade.exe` is installed in the new folder `C:\Users\<username>\AppData\Roaming\KupaySupport`.

AppleJeus Version 7: Ants2Whale

Introduction and Infrastructure

In late 2020, a new version of AppleJeus was identified called “Ants2Whale.” The site for this version of AppleJeus is `ants2whale[.]com` (*Acquire Infrastructure: Domain* [T1583.001]). The website shows a legitimate-looking cryptocurrency company and application. The website contains multiple spelling and grammar mistakes indicating the creator may not have English as a first language. The website states that to download Ants2Whale, a user must contact the administrator, as their product is a “premium package” (*Develop Capabilities: Malware* [T1587.001]).

The domain `ants2whale[.]com` resolved to IP address `198.54.114[.]237` from September 23, 2020, to January 22, 2021. The IP address is controlled by NameCheap Inc. (ASN 22612) and is

located in Atlanta, GA. This IP address is in the same ASN for `CoinGoTrade[.]com` and `Dorusio[.]com`.

The domain `ants2whale[.]com` had a valid Sectigo SSL certificate (*Obtain Capabilities: Digital Certificates* [T1588.004]). The SSL certificate was "Domain Control Validated," a weak security verification level that does not require validation of the owner's identity or the actual business's existence.

Ants2Whale Application Analysis

Windows Program

As of late 2020, the Windows program was not available on VirusTotal. It is likely very similar to the macOS X version detailed below.

macOS X Program

The macOS version of the malicious application is a DMG Installer. The installer looks legitimate and has very similar functionality to the Windows version, but it does not have a digital certificate and will warn the user of that before installation. The installer executes the following actions.

- Installs `Ants2Whale` in folder `/Applications/Ants2whale.app/Contents/MacOS/Ants2whale`
- Installs `Ants2WhaleHelper` in folder `/Library/Application Support/Ants2WhaleSupport/`
- Executes a `postinstall` script
    - Moves `com.Ants2whale.pkg.wallet.plist` to folder `/Library/LaunchDaemons/`
    - Runs Ants2WhaleHelper in the background

The `Ants2Whale` and `Ants2WhaleHelper` programs and the `postinstall` script function almost identically to previous versions of AppleJeus and will not be discussed in depth in this advisory .

For more details on AppleJeus Version 7: Ants2Whale, see MAR-10322463-7.v1.

ATT&CK PROFILE

Figure 2 and table 2 provide summaries of the MITRE ATT&CK techniques observed.

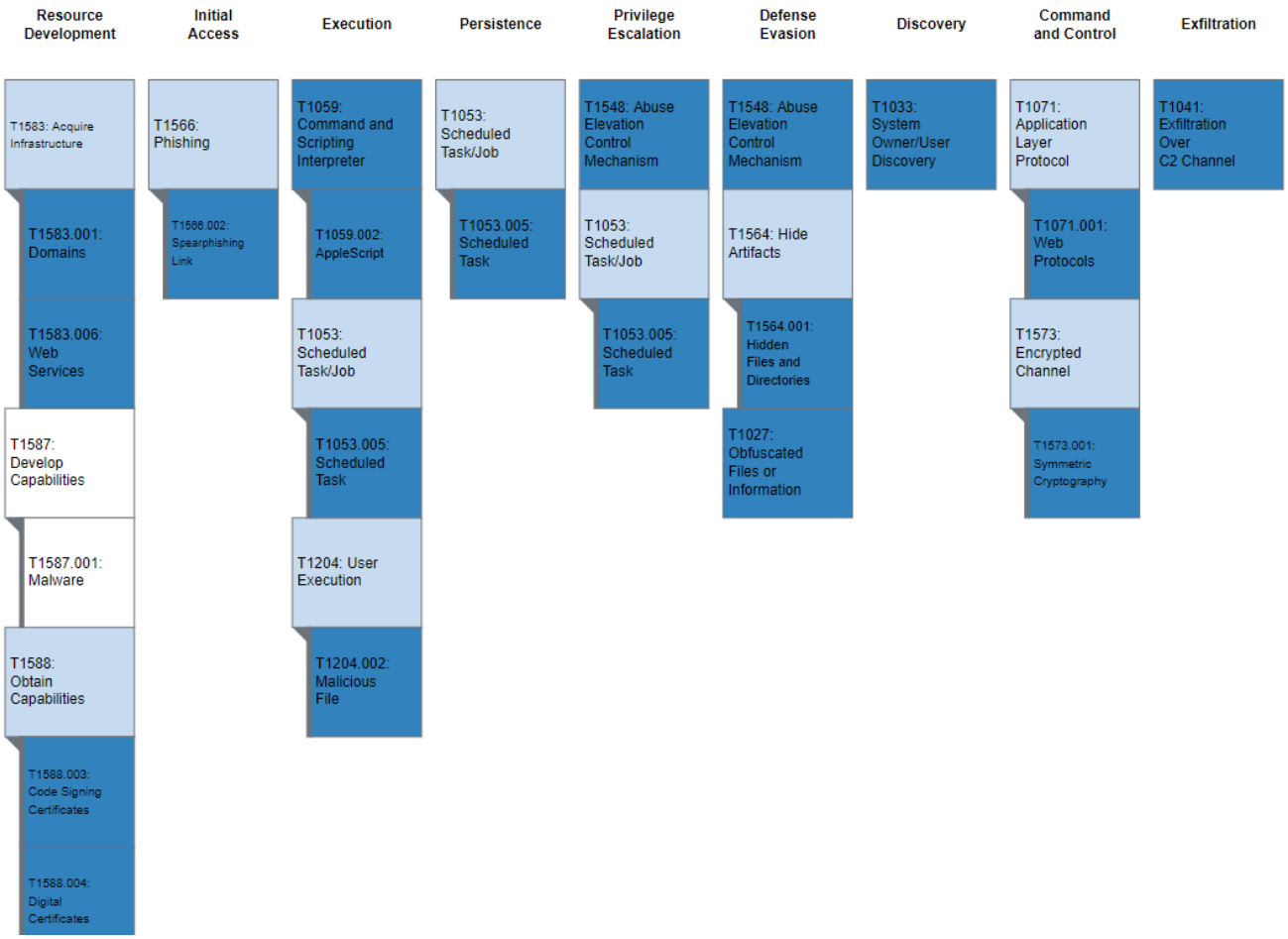

Figure 2: MITRE ATT&CK enterprise techniques used by AppleJeus

Table 2: MITRE ATT&CK techniques observed

Tactic Title	Technique ID	Technique Title
Resource Development [TA0042]	T1583.001	Acquire Infrastructure: Domain
	T1583.006	Acquire Infrastructure: Web Services
	T1587.001	Develop Capabilities: Malware
	T1588.003	Obtain Capabilities: Code Signing Certificates
	T1588004	Obtain Capabilities: Digital Certificates
Initial Access [TA0001]	T1566.002	Phishing: Spearphishing Link
Execution [TA0002]	T1059	Command and Scripting Interpreter
	T1059.002	Command and Scripting Interpreter: AppleScript
	T1204.002	User Execution: Malicious File
Persistence [TA0003]	T1053.004	Scheduled Task/Job: Launchd
	T1543.004	Create or Modify System Process: Launch Daemon
	T1547	Boot or Logon Autostart Execution
Privilege Escalation [TA0004]	T1053.005	Scheduled Task/Job: Scheduled Task
Defense Evasion [TA0005]	T1027	Obfuscated Files or Information
	T1548	Abuse Elevation Control Mechanism
	T1564.001	Hide Artifacts: Hidden Files and Directories
Discovery [TA0007]	T1033	System Owner/User Discovery
Exfiltration [TA0010]	T1041	Exfiltration Over C2 Channel
Command and Control [TA0011]	T1071.001	Application Layer Protocol: Web Protocols
	T1573	Encrypted Channel
	T1573.001	Encrypted Channel: Symmetric Cryptography

MITIGATIONS

Compromise Mitigations

Organizations that identify AppleJeus malware within their networks should take immediate action. Initial actions should include the following steps.

- Contact the FBI, CISA, or Treasury immediately regarding any identified activity related to AppleJeus. (Refer to the Contact Information section below.)
- Initiate your organization's incident response plan.
- Generate new keys for wallets, and/or move to new wallets.
- Introduce two-factor authentication solution as an extra layer of verification.
- Use hardware wallets, which keep the private keys in a separate, secured storage area.
- To move funds out off a compromised wallet:
    - Do not use the malware listed in this advisory to transfer funds; and
    - Form all transactions offline and then broadcast them to the network all at once in a short online session, ideally prior to the attacker accessing them.
- Remove impacted hosts from network.
- Assume the threat actors have moved laterally within the network and downloaded additional malware.
- Change all passwords to any accounts associated with impacted hosts.
- Reimage impacted host(s).
- Install anti-virus software to run daily deep scans of the host.
- Ensure your anti-virus software is setup to download the latest signatures daily.
- Install a Host Based Intrusion Detection (HIDS)-based software and keep it up to date.
- Ensure all software and hardware is up to date, and all patches have been installed.
- Ensure network-based firewall is installed and/or up to date.
- Ensure the firewall's firmware is up to date.

Pro-Active Mitigations

Consider the following recommendations for defense against AppleJeus malware and related activity.

Cryptocurrency Users

- Verify source of cryptocurrency-related applications.
- Use multiple wallets for key storage, striking the appropriate risk balance between hot and cold storage.
- Use custodial accounts with multi-factor authentication mechanisms for both user and device verification.
- Patronize cryptocurrency service businesses that offer indemnity protections for lost or stolen cryptocurrency.
- Consider having a dedicated device for cryptocurrency management.

Financial Service Companies

- Verify compliance with Federal Financial Institutions Examination Council (FFIEC) handbooks at https://ithandbook.ffiec.gov, especially those related to information security.
- Report suspicious cyber and financial activities. For more information on mandatory and voluntary reporting of cyber events via suspicious activity reports, see the Financial Crimes Enforcement Network (FinCEN) Advisory FIN-2016-A005: Advisory to Financial Institutions on Cyber- Events and Cyber-Enabled Crime at https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf and FinCEN's Section 314(b) Fact Sheet at https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

Cryptocurrency Businesses

- Verify compliance with the Cryptocurrency Security Standard at http://cryptoconsortium.github.io/CCSS/.

All Organizations

- Incorporate IOCs identified in CISA's Malware Analysis Reports on https://us-cert.cisa.gov/northkorea into intrusion detection systems and security alert systems to enable active blocking or reporting of suspected malicious activity.
- See table 3 below, which provides a summary of preventative ATT&CK mitigations based on observed techniques.

Table 3: MITRE ATT&CK mitigations based on observed techniques

Mitigation	Description
User Training [M1017]	Train users to identify social engineering techniques and spearphishing emails.
	Provide users with the awareness of common phishing and spearphishing techniques and raise suspicion for potentially malicious events.
User Account Management [M1018]	Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create new Launch Daemons.
	Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create scheduled tasks on remote systems.
SSL/TLS Inspection [M1020]	Use SSL/TLS inspection to see encrypted sessions' contents to look for network-based indicators of malware communication protocols.

Restrict Web-Based Content [M1021]	Determine if certain websites that can be used for spearphishing are necessary for business operations and consider blocking access if the activity cannot be monitored well or poses a significant risk.
	Block Script extensions to prevent the execution of scripts and HTA files that may commonly be used during the exploitation process.
	Employ an adblocker to prevent malicious code served up through ads from executing.
Restrict File and Directory Permissions [M1022]	Prevent all users from writing to the `/Library/StartupItems` directory to prevent any startup items from getting registered since `StartupItems` are deprecated.
Privileged Account Management [M1026]	When PowerShell is necessary, restrict PowerShell execution policy to administrators. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration.
	Configure the Increase Scheduling Priority option only to allow the Administrators group the rights to schedule a priority process.
Operating System Configuration [M1028]	Configure settings for scheduled tasks to force tasks to run under the authenticated account's context instead of allowing them to run as SYSTEM.
Network Intrusion Prevention [M1031]	Use network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware and mitigate activity at the network level.
Execution Prevention [M1038]	Use application control tools where appropriate.
	Use application control tools to prevent the running of executables masquerading as other files.
Behavior Prevention on Endpoint [M1040]	Configure endpoint (if possible) to block some process injection types based on common sequences of behavior during the injection process.
Disable or Remove Feature or Program [M1042]	Disable or remove any unnecessary or unused shells or interpreters.
Code Signing [M1045]	Where possible, only permit the execution of signed scripts.
	Require that a trusted developer I.D. sign all AppleScript before being executed to subject AppleScript code to the same scrutiny as other .app files passing through Gatekeeper.
Audit [M1047]	Audit logging for `launchd` events in macOS can be reviewed or centrally collected using multiple options, such as Syslog, OpenBSM, or OSquery.

	Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges.
Antivirus/Antimalware [M1049]	Use an antivirus program to quarantine suspicious files automatically.

CONTACT INFORMATION

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat.

For any questions related to this report or to report an intrusion and request resources for incident response or technical assistance, please contact:

- The FBI through the FBI Cyber Division (855-292-3937 or CyWatch@fbi.gov) or a local field office,
- CISA (888-282-0870 or Central@cisa.dhs.gov), or
- Treasury Office of Cybersecurity and Critical Infrastructure Protection (Treasury OCCIP) (202-622-3000 or OCCIP-Coord@treasury.gov).

REFERENCES

[1] CISA Alert AA20-239A: FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks

[2] Department of the Treasury Press Release: Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group

[3] Department of Justice Press Release: Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack

[4] CISA Alert TA17-318A: HIDDEN COBRA – North Korean Remote Administration Tool: FALLCHILL

[5] CISA Alert TA17-318A: HIDDEN COBRA – North Korean Remote Administration Tool: FALLCHILL

[6] MITRE ATT&CK Software: FALLCHILL

[7] SecureList: Operation AppleJeus Sequel

[8] GitHub: Blackbird Bitcoin Arbitrage