

Cyber Security Reports

2023.04

NTT Security Japan Inc.

OSINT Monitoring Team, Consulting Services Department

Information Asset Classification: Public
© NTT Security Holdings 29 May 2023



Security Holdings

Content

1.	FBI Announces Takedown of Genesis Market in Joint International Investigation.....	3
1.1.	Overview.....	3
1.2.	Genesis Market and Past Incidents.....	3
1.3.	"Operation Cookie Monster".....	5
1.4.	Summary.....	6
2.	Leaked document 'Vulkan files' and its ripples.....	7
2.1.	Overview.....	7
2.2.	Leaked document 'Vulkan files'.....	7
2.3.	Tools described in Vulkan files.....	9
2.4.	Where Vulkan meets Russia-related APT groups.....	10
2.5.	Summary.....	10
3.	FBI warns of juice-jacking attacks.....	12
3.1.	FBI alert.....	12
3.2.	What a Juice-Jacking Attack Is.....	13
3.3.	Measures against juice-jacking attacks.....	15
3.4.	Summary.....	15

About this report

This report selects and summarizes 3 topics that are considered to be especially important from among various information security incidents and events that occurred during April 2023 and the changes in the surrounding environment. The summary of each topic is as follows.

CHAPTER 1

"FBI Announces Takedown of Genesis Market in Joint International Investigation"

- On April 5, the United States' Justice Department announced that it had taken down the Genesis Market, which had infected users' PCs with malware and sold third parties access to credentials and other information used on infected PCs.
- Cybercriminals, including ransomware groups, were using the Genesis Market as an initial access broker to secure entry points into the targeted networks.
- Since the Genesis Market has continued to exist even after its closure, basic measures, such as installing and updating antivirus software, must be implemented to ensure that business PCs are not infected with malware and become entry points into internal systems.

CHAPTER 2

'Leaked' Vulkan files' and their ripples'

- The Russian IT consultancy NTC Vulkan has provided tools to support cyberattacks and espionage to Russia's state-controlled intelligence agencies, according to leaked documents titled 'Vulkan files'.
- The documents showed that Vulkan had developed tools for Russian intelligence and APT groups to search for vulnerabilities, conduct espionage via social media and other channels, and train agents to carry out cyberattacks.
- The Vulkan files revealed some of the Russian government's preparations for a hybrid war in which it targets cyberattacks and espionage alongside military operations.

CHAPTER 3

'FBI warns about juice-jacking attack'

- On April 6, the Denver bureau of the Federal Bureau of Investigation (FBI) took to Twitter to call attention to a juice-jacking attack that uses USB charging ports in airports and hotels.
- Attackers do tricks such as embedding chips in USB charging ports. If you plug in your phone or tablet for charging, data can be stolen or malware or surveillance software can be installed without your permission.
- Avoid using USB charging ports to avoid juice-jacking attacks. Alternatively, it is recommended to carry and use a dedicated USB cable for charging.

1. FBI Announces Takedown of Genesis Market in Joint Investigation with States

1.1. Overview

On April 5, the US Justice Department announced that it had taken down the Genesis Market, which sold credentials stolen in a cyberattacks. [*]1 The investigation, conducted jointly by the FBI, Europol and others, resulted in the arrest of 119 users of the market. Attempts access the market now indicate that "this site has been seized," along with the logos and other information of the law enforcement agencies in each country that assisted in the investigation.



Figure 1 Genesis Market Screen Shown After Seizure

1.2. Genesis Market and Past Incidents

About Genesis Market

Genesis Market was launched in March 2018 by an administrator believed to be a Russian threat actor. [*]2 Because the market was only accessible by obtaining an invitation code from an existing user, the invitation code was deemed valuable by hackers and was sometimes bought and sold on hacker forums and other sites.

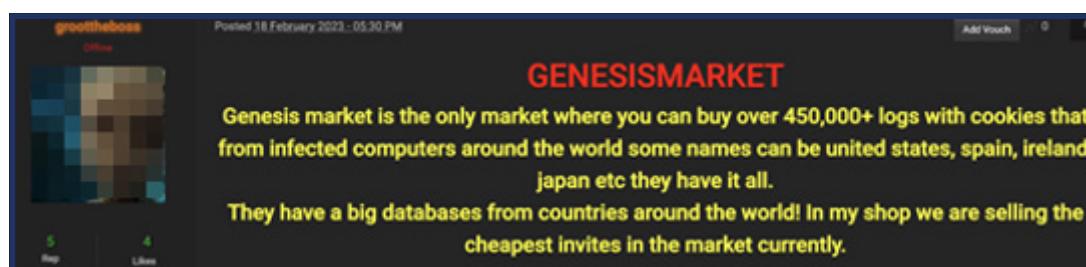


Figure 2 Genesis Market Invitation Code Posts (partially doctored)

The market had developed its own malware and sold access to information collected by bots, referring to PCs infected by malware attachments as "bots." By buying them, users could get real-time information on cookies, login information, auto-fill data in forms, and browser fingerprints, such as browser type and operating system, collected from targeted PCs. [*]3

The difference from selling simple login information is that if a victim of this malware notices a leak and changes their password, the threat actor can get the changed password immediately additionally cookies after authentication, is possible to bypass multi-factor authentication. [*]4 [*]5 [*]6

PC bots used by corporate employees, in particular, have been purchased by cybercriminals, such as ransomware groups, because they are useful for getting inside a corporate network that is being targeted, providing a stepping stone to internal deployment. Services that provide these entry points have played an important role as "initial access brokers" in the recent decentralized cybercrime ecosystem.

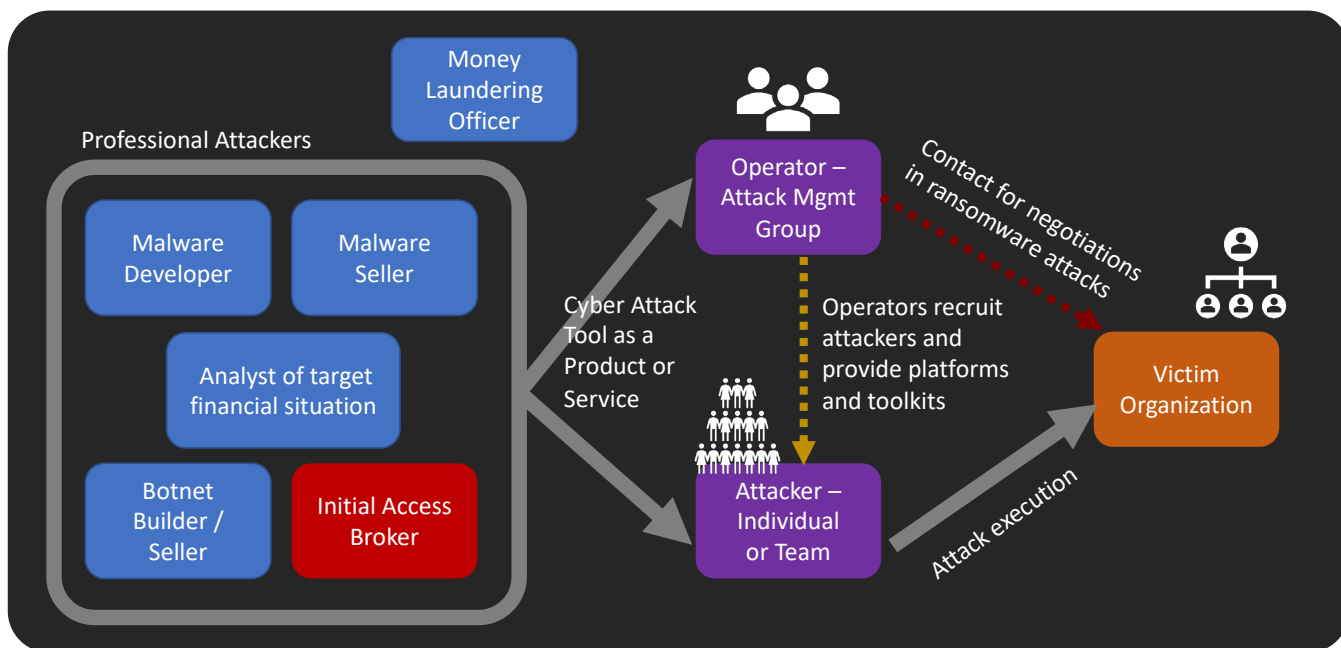



Figure 3: Schematic diagram of the division of labor in cybercrime

Case: Exploitation in attacks on electronic arts

An incident at gaming company Electronic Arts in June 2021 is a known example of a bot sold on Genesis Market being used in an attack. [*]7

It all started when an attacker bought access to an employee's botted PC on Genesis Market for just \$10. [*]8 The attacker was able to log into the company's Slack account using cookies obtained from the bot.

In addition, the attacker used Slack as a springboard to gain access to the company's internal network. He successfully logged into the company's internal network by pretending to be a Slack employee and contacting an IT support representative, who was then tricked into providing him a multi-factor authentication token. The intruders stole a large amount of stored game source code and internal tools and sold them on the market.



July 14, 2021

In June, we reported a recent incident of intrusion into our network (see earlier statement below). This week, we've been made aware of an extortion threat from the alleged hackers, and a portion of some files were released to the public. We have analyzed the files released by the alleged hackers, and at this time, we continue to believe that it does not contain data that poses any concern to player privacy, and we have no reason to believe that there is any material risk to our games, our business or our players. We continue to work with federal law enforcement officials as part of this ongoing criminal investigation.

June 11, 2021

We are investigating a recent incident of intrusion into our network where a limited amount of game source code and related tools were stolen. No player data was accessed, and we have no reason to believe there is any risk to player privacy. Following the incident, we've already made security improvements and do not expect an impact on our games or our business. We are actively working with law enforcement officials and other experts as part of this ongoing criminal investigation.

Figure 4 Statement released by Electronic Arts regarding the incident [*]9

1.3. Operation Cookie Monster

The investigation was led by the FBI and Dutch police, with cooperation from Europol and law enforcement agencies in 45 countries and territories, including Germany, Britain and Australia. The operation was named "Operation Cookie Monster". [*]10 [*]11 [*]12

The investigation resulted in the arrest of 119 users of Genesis Market and the seizure of 11 domain names used by the market. Now, if you visit a URL using these seized domain names, it says "this site has been seized" and the site is no longer available (Figure 1).

However, the manager of the market has not been identified and has not yet been arrested. Sites on the dark web using another domain under ".onion" are still accessible and the market's system appears to be up and running. [*]13 Some have suggested that this is left as a decoy for law enforcement agencies to gather information about hackers as they continue to investigate.

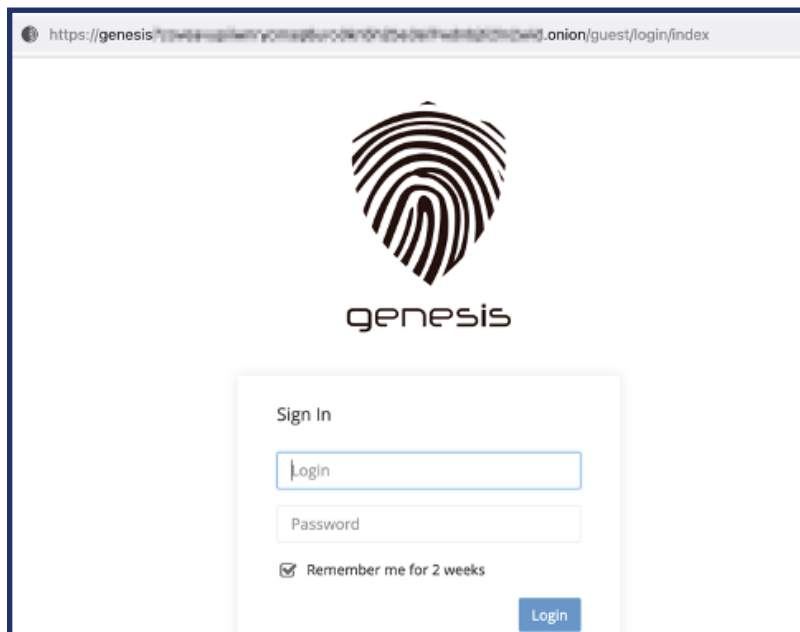


Figure 5 Genesis Market website on the dark web (as of May 15)

1.4. Summary

Genesis Market, which has been involved in cybercrime as an initial access broker since 2018, has been taken down and many of its users arrested. This is a major achievement of international investigative cooperation, but we need to remain vigilant as other markets that offer similar services have been identified. [*]14

An infection with malware from Genesis Market or similar services can trigger an attack that can be very damaging to a business, so basic measures such as not opening suspicious files or URLs and installing or updating antivirus software need to be taken.

2. Leaked Vulkan files and their aftermath

2.1. Overview*15

A leaked document has been reported that reveals some of Russia's efforts in cyberwarfare. It is called the "Vulkan files" because it is an internal document of NTC Vulkan, a Moscow-based IT consultancy. It came to light after a company whistleblower, who opposed Russia's invasion of Ukraine, provided it to Western news outlets.

Analysis of the Vulkan files confirmed the development of large-scale tools to support Russian government cyberattacks and intelligence operations. The documents also showed links between Vulkan, the company behind the tools, and Russian government-affiliated hacking groups that have been implicated in various cyberattacks.

2.2. Leaked documents' Vulkan files' [*]16

Vulkan is an information security specialist IT consulting firm based in Moscow (Figure 6). Its name means volcano in Russian. It was founded in 2010 by Anton Markov, a former Russian army officer. Clients include major Russian companies such as Sberbank, national airline Aeroflot and Russian Railways. Vulkan is positioned as part of the military-industrial complex with close ties to the Russian state because of its founder's connections, person-to-person contacts between the military and intelligence agencies and Vulkan, and because many of its employees are graduates of Bauman University in Moscow, which is under the influence of Russian security agencies.

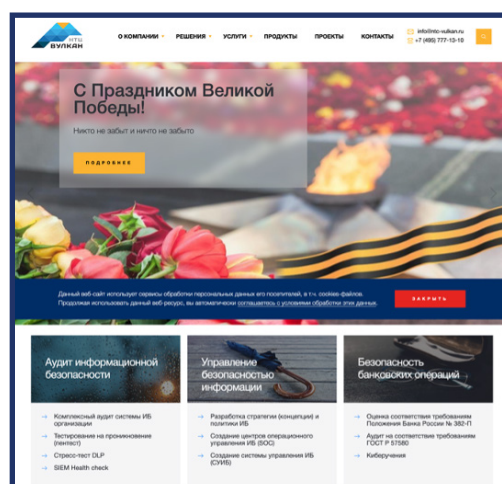


Figure 6 Vulkan Homepage

A whistleblower from Vulkan

In February 2022, Russia began its invasion of Ukraine. Someone inside Vulkan was angry with the Russian actions in Ukraine and with Vulkan for cooperating with the Russian government and secretly contacted German journalists. He then handed over thousands of pages of classified "Vulkan files" to a German press research group about the cyberattack tools Vulkan had provided to Russian government agencies. "We hope to use this information to uncover what is going on behind closed doors," said the whistleblower. [*] 17

The group shared the Vulkan files with the DER SPIEGEL newspaper and several other news outlets with which it has agreements. After scrutiny by experts, including Western intelligence agencies, it was determined to be highly likely to be genuine, and on March 30, 2023, an investigative report on the Vulkan files was published by the DER SPIEGEL newspaper and others.

Contents of Vulkan files

The Vulkan files are over 5,000 pages of data dating from 2016 to 2021, including emails, internal documents, project plans, budgets and contract documents (Figure 7). The analysis reveals a partnership in which Vulkan develops and provides tools for the Russian intelligence community. Among the intelligence agencies with which ties have been found are the GRU, a military intelligence agency, the FSB, an intelligence agency that monitors inside Russia, and the SVR, an external and economic operation. There are also maps of the United States and diagrams of nuclear power plants in Switzerland in the documents, suggesting that the intended targets are Europe and the United States.

It is not clear from the Vulkan files whether the tools developed have actually been used in attacks. On the other hand, due to the practicality and perfection of the tools, it is suspected that it may have been used in cyberattacks that were observed before and during the invasion of Ukraine.

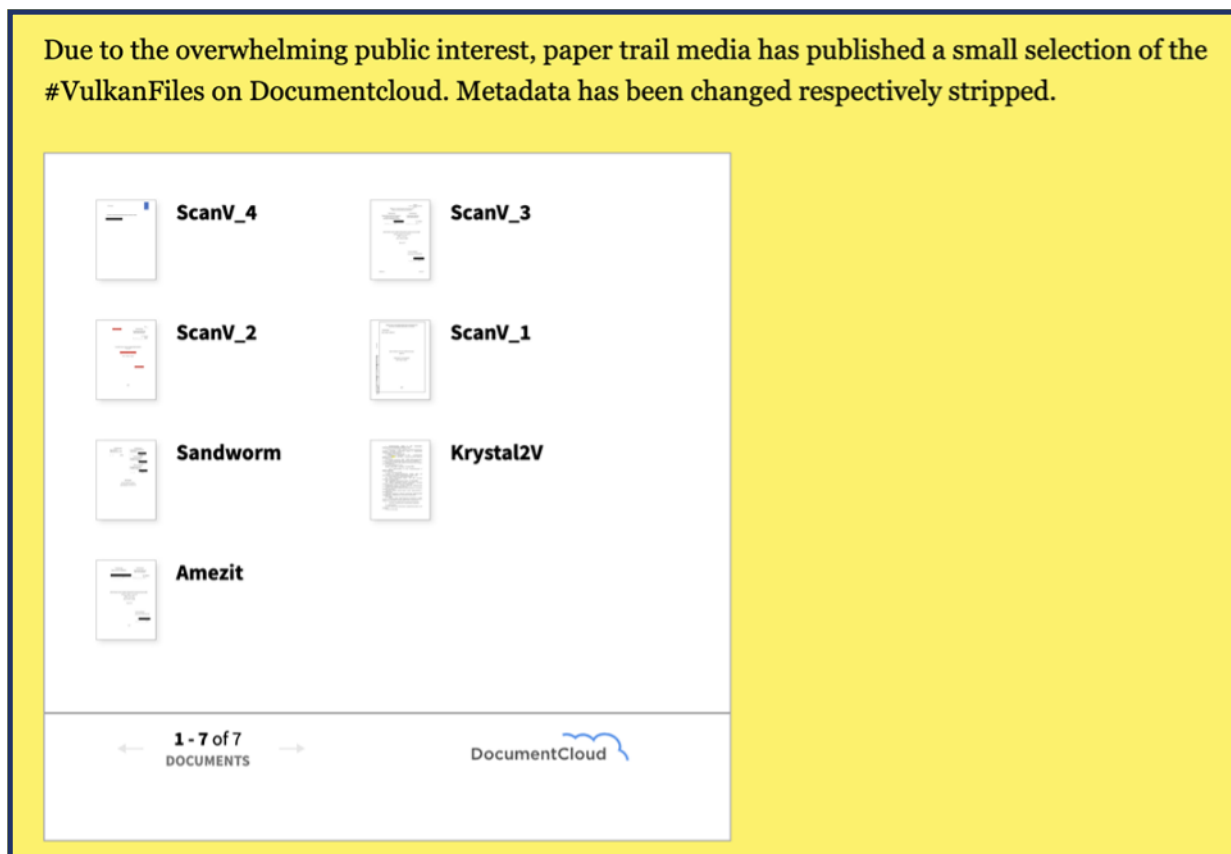


Figure 7 Data from Vulkan files(Some data is available on the site of German media research group paper trail media) [*]18

2.3. Tools described in Vulkan files

The Vulkan files confirmed Vulkan's involvement in three projects to develop cyber-attack and intelligence tools: [*]19 [*]20 [*]21

Scan-V: A tool to search for vulnerable systems

Scan-V is a tool to scan candidate systems around the world and collect vulnerability information. The Vulkan files contain comprehensive documentation on how to build a database to house the collected data.

It is known from the scope of information contained in the Vulkan files that it was developed in conjunction with the GRU intelligence agency, but it is not clear whether the GRU actually purchased or deployed Scan-V. Meanwhile, Google's security team has determined that tools listed in the Vulkan files as a subsystem of Scan-V were being used in the global MiniDuke cyberattack it detected around 2012, and believes its success at that time spurred the project to develop Scan-V itself. [*]22

Amesit: A tool to support information operations

Amesit is a framework-based tool that supports Internet information operations from preparation to implementation. Because it is a large toolset, multiple companies participated in its development, and Vulkan employees serving as the "stewards" frequently visited the FSB headquarters to obtain specifications.

First, intelligence operatives using Amesit monitor, intercept and collect social media and mobile phone calls in order to understand the spread of ideas in Russia and abroad. Next, they determine how they wish to manipulate the situation and create appropriately tailored content for use. Content can be deployed in various formats including text, images, video and audio data. Content can then be spread across multiple channels, including social media, blogs, SMS and email. A document in the Vulkan files explains that Amesit has the ability to manage about 100 fake social media accounts to aid in social media espionage, as well as the ability to avoid investigations that identify where accounts are being impersonated.

It is believed that the Amesit information operations tooling can be used to conduct influence activities either the region around Russia or globally as well. [*]23

Krystal-2B: Cyber espionage training tool

Krystal-2B is a training tool for operatives conducting cyberattacks. Up to 30 people can participate in training at the same time.

It is believed to be designed to support both offensive and defensive exercises, as well as exercises aimed at controlling systems of critical rail, air and sea infrastructure, as well as at vulnerabilities in Russia's military infrastructure.

Krystal-2B used to train Amesit

An exercise plan using the Krystal-2B cyber espionage training tool in the Vulkan files notes the use of Amesit, an intelligence espionage support tool. It also clearly states that the exercise will train the ability to disrupt real-world infrastructure, including systems that control air, sea and rail operations. [*]24 These descriptions suggest that Amesit's plethora of functions extends beyond information operations to the support of public infrastructure attacks.

2.4. Where Vulkan meets Russia-linked APT groups

In the Vulkan files, contacts between Vulkan and Russian APT groups have also been discovered. The Sandworm group, presumed to be the GRU's cyber unit, has been accused by UK and US government agencies of being the main culprit in cyberattacks on Ukraine's power transmission system in 2015, the NotPetya malware outbreak in 2017, and the "Olympic Destroyer attack" on South Korea's 2018 Winter Olympics in Pyeongchang. [*]25 [*]26 The Vulkan files indicate that the Sandworm group retained Vulkan to help build Scan-V.

In other Scan-V developments, Vulkan also appears to have contacts with the Cozybear group, which is part of the SVR, based on analyses which indicate that the related MiniDuke cyberattack was carried out by the group. [*]27 [*]28

2.5. Summary

The Vulkan files have revealed the startling reality of Russian cyberwarfare. Since the 2010s, the Russian government has pursued a strategy of hybrid warfare and has worked to incorporate cyberattacks into this strategy. The combination of the intelligence operations tool Amesit and the training tool Krystal-2B has been speculated as evidence of the high value placed by the Russian government on the deployment of information operations during the execution of cyberattacks on public infrastructure. [*]29

The Vulkan files date back to 2021 and do not directly document the cyberattacks that have taken place in Ukraine since then. However, there have been a great number of hybrid warfare operations against Ukraine, with simultaneous information operations and attacks on critical infrastructure, timed together with missile and military attacks, as described in the documentation of the tools in the Vulkan files. The Vulkan files also appear to reveal some of the activities leading up to the invasion of Ukraine.

3. FBI warns of juice-jacking attacks

3.1. FBI reminder

On April 6, the Denver bureau of the Federal Bureau of Investigation (FBI) posted a call on Twitter to be on the lookout for a "juice-jacking attack" that involves the rigging of USB charging ports installed in airports and other locations. Compromised USB charging ports install malware or conduct other attacks on connected devices (Figure 8). [*]30

According to the Denver bureau, the FBI regularly works with partner organizations to issue alerts and public service notices. [*]31 [*]32



Figure 8 Tweets from the FBI Denver office

3.2. What Is a Juice-Jacking Attack?

Increasing USB Charging Ports [*]33

In the past, it was common to carry your own charger or mobile power bank with you to charge your smartphone or tablet during long business trips/trips. In recent years, however, depending on the grade of the facility and the country/region, there has been an increase in the installation of USB charging ports at airports, hotels and cafes that allow anyone to charge their smartphone or tablet for free, allowing them to easily charge their devices in various places while traveling with just a USB cable.

Although it is not possible to charge a PC with a USB charging port due to output power limitations, it is expected that charging of PCs as well as smartphones and tablets will become more common in the future, as more USB charging ports will be available for PCs. [*]34



Figure 9 USB charging port installed at Haneda Airport [*]35



Figure 10 USB charging port beside a hotel bed [*]36 (red circle added for clarity)

(Method of attack)

Attackers perform tricks such as embedding small chips inside USB charging ports provided in public places. If unsuspecting users connect to the ports, attackers can steal data and install surveillance software and malware. This type of cyberattack that compromises USB charging ports is called a "juice jacking attack."

As a user who is usually aware of security, there is a great deal of resistance to plugging a USB thumb drive into a PC or other device that you do not know about. In comparison, there is little resistance to plugging a smartphone or tablet into a USB charging port as many users do. This is probably because, unlike a USB thumb drive, it is not well-understood that data communication can occur at the same time as charging when a device is connected to a USB charging port.

(Demonstration)

The idea of a juice-jacking attack was first introduced in 2011 at a demonstration during the international security conference called DEFCON. [*]37 DEFCON is held annually in Las Vegas and is attended by many hackers, security experts, researchers, government officials and others. [*]38

Since the initial demonstration, several hackers and cyber researchers have begun to investigate how successful juice-jacking attacks can be executed by circumventing the security measures put in place on devices and by rigging compromised ports to look the same as a regular USB charging port. At DEFCON in 2019, a tool that could be rigged to an iPhone's charging cable to install malware and allow remote control was announced, drawing attention for its use in juice-jacking attacks. [*]39

[O MG adapter]

The tool demonstrated at DEFCON is called the "O MG adapter" and is now marketed to security researchers. The O.MG adapter looks like just a USB conversion plug, but it has a small chip embedded in the connector (Fig. 11[*]40 , Fig. 12[*]41). The small chip turns the connected device into a Wi-Fi access point, allowing an attacker to gain wireless LAN access to the device from the outside without the device's user noticing.

It is easy to embed such hacking cables and parts inside a USB charging port, and some attackers are said to be able to complete the task in minutes ³³.



Figure 11 O.MG Adapter



Figure 12 Connector with embedded chip
(From the video of O.MG adapter maker Twitter)

Fear of its use in attacks

As the Federal Communications Commission's April 2023 announcement ³² noted, there have been no known instances of juice-jacking attacks. However, as demonstrated by the O.MG adapter, the technology required to perform juice-jacking is well-developed, so it's expected that it is already being used in attacks. In addition to fears that it could be used in attacks such as spying on government officials, ³⁹ it's also considered an attractive attack vector for cybercriminals looking for financial gain ³³.

3.3. Measures against juice-jacking attacks

One way to prevent juice-jacking attacks is to avoid using USB charging ports as much as possible. Alternatively, if you carry a commercially available USB "charging-only" cable and use it when connecting a USB charging port. Data communication will not occur and the attack will not be successful.

3.4. Summary

The alert from the FBI has renewed awareness of the potential for unforeseen damage to USB charging ports in public places, as well as free Wi-Fi, which has been flagged as a risk. [*]42 Expect more locations for USB charging ports in the future. When charging devices on the go, it is necessary to be careful.

Disclaimer

While we do our best to be accurate in the content of this article, we do not guarantee its accuracy and will not compensate you for any damages or losses arising from your use of this article. If you have any questions or concerns regarding typographical errors, errors in content, or other matters pointed out in the article, please contact us at the address below.

Contact: NTT Security Japan Inc.

OSINT Monitoring Team, Consulting Services Department

Email address: WA_Advisorysupport@ntt.com

Sources

1. Source: U.S. Department of Justice "Criminal Marketplace Disrupted in International Cyber Operation"
<https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation>
2. Source: KELA, Supply Chain for Cybercrime Market Genesis
<https://ke-la.com/ja/exploring-the-genesis-supply-chain-for-fun-and-profit/>
3. Source: Nikkei XTREND, What is' Browser Fingerprint Technology for Identifying Users?
<https://xtrend.nikkei.com/atcl/contents/technology/00005/00013/>
4. Source: EUROPOL "Takedown of notable hacker marketplace selling your identity to criminal"
<https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals>
5. Source: SOPHOS, Genesis, an invite-only marketplace where credentials are bought and sold
<https://news.sophos.com/ja-jp/2022/08/04/genisis-brings-polish-to-stolen-credential-marketplaces-jp/>
6. Source: SOCRadar (5 Things You Should Know About the Genesis Marketplace)
<https://socradar.io/5-things-you-should-know-about-genesis-marketplace/>
7. Source: Vice "Hackers Steal Wealth of Data from Game Giant EA"
<https://www.vice.com/en/article/wx5xpx/hackers-steal-data-electronic-arts-ea-fifa-source-code>
8. Source: Vice "How Hackers Used Slack to Break into EA Games"
<https://www.vice.com/en/article/7kvkqb/how-ea-games-was-hacked-slack>
9. Source: Electronic Arts Statement on the recent network break-in
<https://www.ea.com/en-au/news/ea-statement-on-june-11-security-incident>
10. Source: Bleeping Computer "FBI seizes stolen credentials market Genesis in Operation Cookie Monster"
<https://www.bleepingcomputer.com/news/security/fbi-seizes-stolen-credentials-market-genesis-in-operation-cookie-monster/>
11. Source: REUTERS "Operation Cookie Monster": International police action seizes dark web market"
<https://www.reuters.com/world/uk/operation-cookie-monster-international-police-action-seizes-dark-web-market-2023-04-05/>
12. Source: U.S. Department of Justice "Genesis Market Disrupted in International Cyber Operation"
<https://www.justice.gov/usao-edwi/pr/genisis-market-disrupted-international-cyber-operation>
13. Source: HACKREAD "Genesis Market's Clearnet domain seized; Dark Web site still online"
<https://www.hackread.com/dark-web-genisis-market-domain-seized/>
14. Source: ReliaQuest "The Technology Adoption Lifecycle of Genesis Market"
<https://www.reliaquest.com/blog/the-technology-adoption-lifecycle-of-genesis-market/>
15. Source: The Guardian "'Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics"
<https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics>
16. Source: The Guardian "'Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics"
<https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics>
17. Source: paper trail media Vulkan Files
<https://www.papertrailmedia.de/investigations/vulkan-files/>
18. Source: paper trail media Vulkan Files
<https://www.papertrailmedia.de/investigations/vulkan-files/>
19. Source: Mandiant "Contracts Identify Cyber Operations Projects from Russian Company NTC Vulkan"
<https://www.mandiant.com/resources/blog/cyber-operations-russian-vulkan>
20. Source: DER SPIEGEL "The 'Vulkan Files': A Look Inside Putin's Secret Plans for Cyber-Warfare"
<https://www.spiegel.de/international/world/the-vulkan-files-a-look-inside-putin-s-secret-plans-for-cyber-warfare-a-4324e76f-cb20-4312-96c8-1101c5655236>
21. Source: The Washington Post "The Vulkan Files: Secret trove offers rare look into Russian cyberwar ambitions"
<https://www.washingtonpost.com/national-security/2023/03/30/russian-cyberwarfare-documents-vulkan-files/>
22. Source: DER SPIEGEL "The 'Vulkan Files': A Look Inside Putin's Secret Plans for Cyber-Warfare"
<https://www.spiegel.de/international/world/the-vulkan-files-a-look-inside-putin-s-secret-plans-for-cyber-warfare-a-4324e76f-cb20-4312-96c8-1101c5655236>

23. Source: The Guardian "Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics"
<https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics>
24. Source: Mandiant "Contracts Identify Cyber Operations Projects from Russian Company NTC Vulkan"
<https://www.mandiant.com/resources/blog/cyber-operations-russian-vulkan>
25. Source: Sandworm Team, MITRE ATT&CK
<https://attack.mitre.org/groups/G0034/>
26. Source: U.S. Department of Justice "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace"
<https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>
27. Source: APT29, MITRE ATT&CK
<https://attack.mitre.org/groups/G0016/>
28. Source: DER SPIEGEL "The 'Vulkan Files': A Look Inside Putin's Secret Plans for Cyber-Warfare"
<https://www.spiegel.de/international/world/the-vulkan-files-a-look-inside-putin-s-secret-plans-for-cyber-warfare-a-4324e76f-cb20-4312-96c8-1101c5655236>
29. Source: Mandiant "Contracts Identify Cyber Operations Projects from Russian Company NTC Vulkan"
<https://www.mandiant.com/resources/blog/cyber-operations-russian-vulkan>
30. Source: Twitter @FBI Denver
<https://twitter.com/FBIDenver/status/1643947117650538498>
31. Source: SLATE "Actually, Charging Your Phone in a Public USB Port Is Fine"
<https://slate.com/technology/2023/04/free-public-phone-chargers-fbi-warning-bad-actors-threat-bogus-debunked.html>
32. Source: Federal Communications Commission "What is' Juice Jacking 'and Tips to Avoid It"
<https://www.fcc.gov/juice-jacking-tips-to-avoid-it>
33. Source: Forbes "How 'Juice Jackers' Plant Malware On Your Phone At Airports And Hotels"
<https://www.forbes.com/sites/suzannerowankelleher/2023/04/20/juice-jacking-malware-phone-airports-hotels/>
34. Source: PC Watch "Panasonic is the industry's first USB outlet to support up to 60 watt PD"
<https://pc.watch.impress.co.jp/docs/news/1500589.html>
35. Source: PR TIMES "Enhanced charging facility at Haneda Airport/Built-in storage battery enables charging during power outages"
<https://prtimes.jp/main/html/rd/p/000000006.000058641.html>
36. Source: Apa Hotel "Official Apa Hotel (Asakusa Shin Okachimachi Ekimae)"
<https://www.apahotel.com/hotel/syutoken/tokyo/shin-okachimachi-ekimae/gallery/>
37. Source: naked security by SOPHOS "Juicejacking - an emergency phone charge can be a security risk"
<https://nakedsecurity.sophos.com/2011/08/19/is-juicejacking-the-new-firesheep/>
38. Source: GMO Cyber Security by Yerae "Festival of Hackers" DEFCON 26 Field Report - Part 1 "
https://gmo-cybersecurity.com/blog/defcon-26_part1/
39. Source: Forbes "Why You Should Never Borrow iPhone Cables"
<https://www.forbes.com/sites/zakdoffman/2021/05/29/apple-iphone-and-ipad-users-warned-not-to-borrow-other-peoples-cables/>
40. Source: Radiolife .com "Conversion Connector Hacking Tools Steal Data"
<https://radiolife.com/internet/virus/61548/>
41. Source: Twitter (@_MG_)
https://twitter.com/_MG_/status/1565003970535247872
42. Source: Spectrum Technology Inc.'s Accident Example (WiFi)
<https://spectrum-tech.co.jp/incident.html>





Security Holdings