


CYBER
THREAT
ANALYSIS

CHINA

Recorded Future®

By Insikt Group®

April 20, 2023



Xiaoqiying/Genesis Day Threat Actor Group Targets South Korea, Taiwan

Executive Summary

The threat actor group Xiaoqiying (aka Genesis Day, Teng Snake) is a primarily Chinese-speaking threat group that conducted website defacement and data exfiltration attacks on more than a dozen South Korean research and academic institutions in late-January 2023. More recently, its affiliated threat actors have signaled a new round of cyberattacks against organizations in Japan and Taiwan. Based on the analysis of the group's Telegram channels, postings on special-access forums, and its presence on a clearnet website, we conclude that this is a hacktivist group primarily motivated by patriotism toward China, and it will likely conduct similar cyberattacks against Western and NATO targets, as well as any country or region deemed hostile to China.

Key Findings

- The threat actor group operated primarily on 2 Telegram channels — an announcement channel and a members channel under the moniker “Genesis Day” — until early February 2023, when news about its cyberattacks in South Korea, which was conducted under the moniker of “Xiaoqiying”, reached the media. The 2 Telegram groups then went offline.
- Based on chat logs from the Telegram announcement channel, the group has been in operation for much of 2022 and made unverified claims of compromising the networks of organizations in the US, Ukraine, Taiwan, South Korea, Japan, and other Western countries. The group also claimed to have working relationships with APTs and threat groups around the world, giving it the capacity to launch cyberattacks against any region deemed hostile to China.
- The group maintains the clearnet website [eisae\[.\]org](http://eisae[.]org) to announce its activities, including “Operation South Korea”, which allegedly compromised a number of South Korean organizations beginning in late-January 2023. The website also provides contact information for membership recruitment.
- Sample data allegedly gathered from the attacks was shared on the now-defunct BreachForums by “abort” and on Ramp Forum by “uetus”. Both actors claimed to operate on behalf of “Genesis Day”; “abort” was banned due to complaints of file download links containing malware. More recently, uetus also claimed to have penetrated an unnamed Japanese financial institution and the National University of Taiwan as part of a new operation by Genesis Day.
- Per its Telegram channel chat logs, the threat group likely exploits vulnerabilities in internet-facing devices and remote access tools to gain initial access. In addition, allegedly “cracked” versions of penetration tools, including Cobalt Strike, Brute Ratel, Burp Suite, as well as proof-of-concept code (POC) for exploits and other malware, were shared across the threat group's Telegram channels.
- The chat logs on the 2 Telegram channels did not reveal clear ties with the Chinese government, but reflected a strong pro-China and anti-West sentiment. In addition, the threat group does not appear to be financially motivated, as it did not seek profit from data and access sales.

Background

Since January 25, 2023, open-source reporting from South Korea has revealed a mass cyberattack against websites belonging to 12 South Korean research and academic institutions during the Lunar New Year holiday. The cyberattack was conducted by a Chinese-speaking threat group identified as 晓骑营 (pronounced “Xiaoqiying” and translates to “Dawn Cavalry”). According to a report from Gnews (gnews.org), the Korea Internet & Security Agency (KISA) identified the affected research and academic institutions, which include the Korean Research Institute for Construction Policy, Korean Archaeological Society, Woorimal Academic Society, Korean Academy of Basic Medicine & Health Science, Association for Studies in Parents and Guardians, Research Institute for Early Childhood Education, Korean Lesson Study Group for Social Studies, Korean East-West Mind Science Association, Korean Cleft Lip and Palate Association, Korean Association for the Education and Rehabilitation of the Blind and Visually Impaired, Jeju Education & Science Research Institute, and the Korean Society for the Study of Educational Principles.

According to KISA reports, all 12 of the abovementioned websites suffered website defacements in which the adversaries replaced each hosted website with their own in a compromised server. The compromised websites either had a generic error page or a claim, including the threat group’s name written in Chinese characters (晓骑营), that the threat group had compromised and invaded the “Korean Internet”. KISA also identified IP addresses linked with the attack to origins within various countries such as China, the US, Singapore, and Taiwan. Based on a [report](#) from The Korea Times (koreatimes.co.kr), the Chinese threat group disclosed on its public Telegram channel that it included KISA as one of its potential targets and is the first government agency targeted by the threat group. Other reports claimed that the threat group threatened to target approximately 2,000 government agencies, including South Korea’s Ministry of Culture, Sports, and Tourism.

Since then, reports disclosed that some websites had recovered from the website defacement attacks. However, Xiaoqiying announced that they had stolen a total of 54 gigabytes of data from various organizations, including the institutes’ staff members and researchers’ personally identifiable information (PII). An investigation is currently underway, and KISA has not officially confirmed whether the hackers are Chinese or have links to the Chinese government.

Our initial tracking of the threat group came from its 2 Telegram channels, in which the group was known as “Genesis Day”. One of the administrators of those Telegram groups had 晓骑营 (Xiaoqiying) as part of their handle as well as an associated GitHub page. Since the Chinese characters 晓骑营 (Xiaoqiying) were used as the group’s moniker in the website defacement attacks in South Korea, the group is now better known by the new name instead.

Threat Analysis

Telegram Groups

Our analysis of Xiaoqiying's activity on Telegram is based on 2 Telegram invitation links¹ obtained in early January 2023. One of these links was for the announcement channel and the other was for the communications channel. By joining the 2 Telegram channels, we downloaded the chat logs and the files shared. From analyzing the downloaded data, we identified the threat group's administrators, tools and data shared among members, tactics, techniques, and procedures (TTPs) used by the threat group, and connections with other special-access cybercriminal forums and threat actors. We also assessed the credibility of the offers and predicted the future course of action of the group.

The Genesis Day threat group was active on Telegram up until February 2023 when the news of its alleged breaches reached the media. Then, both Telegram channels went offline. These 2 Telegram channels included an announcement channel and a member channel. Both channels consisted primarily of Chinese-speaking users.

Genesis Day Group (Announcement Channel)

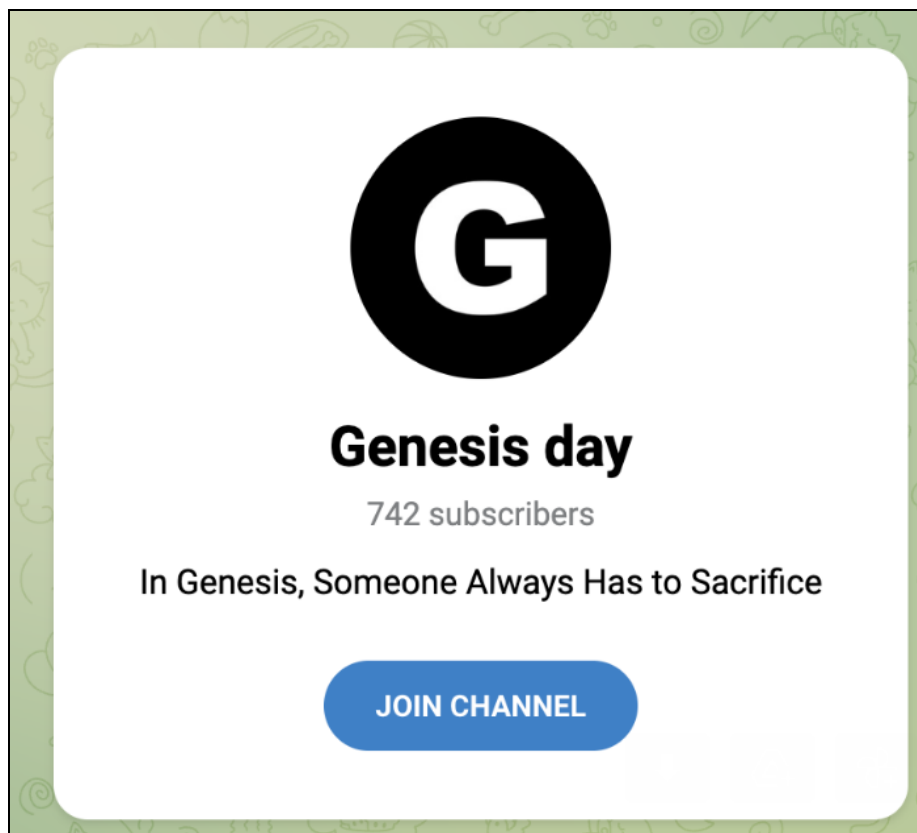


Figure 1: Genesis Day announcement channel (Source: Telegram)

¹ The Telegram invitation links are <https://t.me/+WDdywrfEZ38zNDM1> (announcement channel) and https://t.me/+m_sWpWEQfo4ZGU1 (communications channel).

This channel was created on August 16, 2021, and had more than 700 subscribers as of mid-January 2023. We obtained leaked data, tools, malware source codes and samples, files related to US government entities, credit card data, and more from the group's Telegram channel. Files of interest that were shared in the group include the following:

- Allegedly cracked versions of Cobalt Strike, Brute Ratel, and Burp Suite
- A list of offers from “johnhana”, a highly credible member of the now-defunct BreachForums who frequently posted China-related data leaks
- A speculative report on the members of “AgainstTheWest”, a threat group targeting Russia, China, Iran, and North Korea that was active on both BreachForums and Raid Forums, a now-defunct predecessor to BreachForums
- A list of information about the alleged members of “Killnet”, a pro-Russian hacktivist group that has been active since Russia's invasion of Ukraine in February 2022
- Alleged source code of BPFDoor malware from Red Menshen
- PHP Library Remote Code Access (RCE) proof of concept, which includes a link shared on Packet Storm Security
- A database from WeLeakInfo[.]com containing credit card information and Stripe accounts

In addition, proofs of concept and exploits of the following CVEs were shared in the announcement:

- CVE-2022-34305 (Apache Tomcat vulnerability)
- CVE-2022-20006 (Android vulnerability)
- CVE-2022-34918 (Debian and Linux vulnerabilities)
- CVE-2021-23017 (Fedora operating system vulnerability)

These proofs of concept and exploits may have been used in compromising some of the websites listed in **Appendix B** as some of those websites have PHP or Apache servers that might have been unpatched.

Xiaoqiying's administrators also recruited on the Telegram channels, requesting skilled members interested in joining the collective to send their resumes to ADKF3R@proton[.]me. **Appendix A** includes a complete list of the files shared in the Telegram channel.

The chat log consists entirely of announcements from the administrator “Genesis Day” as other users appeared to be muted. Analysis of these announcements showed a strong pro-China, anti-West sentiment. On December 31, 2022, Genesis Day posted a new year's message, shown in **Figure 2** and translated on the following page.



Genesis day 08:44

2022 Genesis day 年鉴

2022.2 起草美国NSA下属tao行动办公室BE小组马甲对华行动名单，并长期跟踪这一组织

2022.4 组织策划入侵FBI，成功获取其内部解析规则api和令牌生成，未果。

2022.5 参与corecode对韩行动，其入侵韩国卫生部和国防部，该行动被vx收入年鉴，并受到韩国s2情报公司调查。

2022.11 供应链未授权入侵西方数家企业生产内网，成功接管权限289台

2022.11 入侵台湾某知名高校，成功获取内网权限

2022.12 入侵韩国某知名高校，成功获取内网权限

2022.12 入侵台湾某行业前三供应商，成功获取内网权限，可拿域控。

2022 .12 入侵美国某公司，成功获取内网权限。

2022.12 入侵韩国某软件供应商公司，成功获取内网权限

2022.12 入侵台湾某部委后台

2022.12 入侵成功获取乌克兰国防部某系统账号密码，未果

2022.12 入侵三星某内网rdp权限，成功登录三星内部系统，获取其内部资料。

.....

新的一年，本频道将计划针对西方北约成员国及相关仇华行为国家或地区，发起新一轮大规模的op行动瘫痪相关欧美敌对地区的网络基础设施。我们将积极联系世界范围的盟友及apt成员，合作伙伴有但不限于apt35.corecode.匿名者.lapsus.Hive.巴基斯坦apt组织.俄罗斯apt组织.solitbit.ares.Prynt Stealer...没有中国的世界将毫无意义，我们做的只是让这个国家再次回到本属于她的位置上去。组织致力于新世纪起源日破晓前夜的挥刀，欢迎加入我们,期待我们...。

新年快乐各位 08:51

Figure 2: The new year message posted by Genesis Day" on December 31, 2022, served as a summary for the group's activities in 2022 and a call to action for 2023. The English translation is provided below. (Source: Telegram)

Genesis day 2022 Activity Summary

February 2022 — Drafted the plan of compiling the handles of the “BE” group of NSA’s TAO Unit who conducted cyber operations on China, and planned to track this group for the long term.

April 2022 — Planned to penetrate the FBI, successfully obtained internal parsing rule API and generated token, no further success.

May 2022 — Participated in the “corecode” [sic]² operation against South Korea, and infiltrated the Ministry of Health and Defense Ministry . The operation was documented by “VX”³ and investigated by an intelligence company “S2”⁴.

November 2022 — Unauthorized supply chain infiltration into the enterprise production intranet of numerous western companies, successfully taken over the admin privileges of 289 machines.

November 2022 — Penetration into a well-known higher education institute in Taiwan, and successfully obtained intranet access.

December 2022 — Penetration into a well-known higher education institute in Taiwan, and successfully obtained intranet access.

December 2022 — Penetrated into a top-3 supplier of a certain sector in Taiwan, successfully obtained intranet access and access to the domain controller.

December 2022 — Penetrated a certain US company, successfully obtained intranet access.

December 2022 — Penetrated a software supplier in South Korea and successfully obtained intranet access.

December 2022 — Penetrated into the backend of a Taiwanese government agency.

December 2022 — Successfully obtained the account names and passwords of a certain system of Ukraine’s Ministry of Defense, no further success.

December 2022 — Penetrated into Samsung and obtained RDP privilege, successfully logged into Samsung’s intranet and obtained its internal documents.

.....

In the upcoming year, this channel will plan to launch another round of operations against NATO members and related countries/regions that are hostile to China, to paralyze the network and infrastructure of these countries. We are actively cooperating with our global allies and APT members, our partners include but are not limited to APT 35, Corecode [sic], Anonymous, Lapsus, Hive, Pakistani APTs, Russian APTs, Solitbit.ares [sic]⁵, Prynt Stealer, A world without China would be a meaningless world, we are only trying to restore this country to her rightful place. We strive to wield our swords at the dawn of this new era. You are welcomed to join us, expect us ...

Happy New Year everyone

² Possibly referring to “Code Core”, which is another moniker associated with Xiaogqing

³ Possibly referring to VX Underground

⁴ Possibly referring to S2W, a data intelligence company in South Korea

⁵ Possibly referring to Solidbit ransomware and Ares

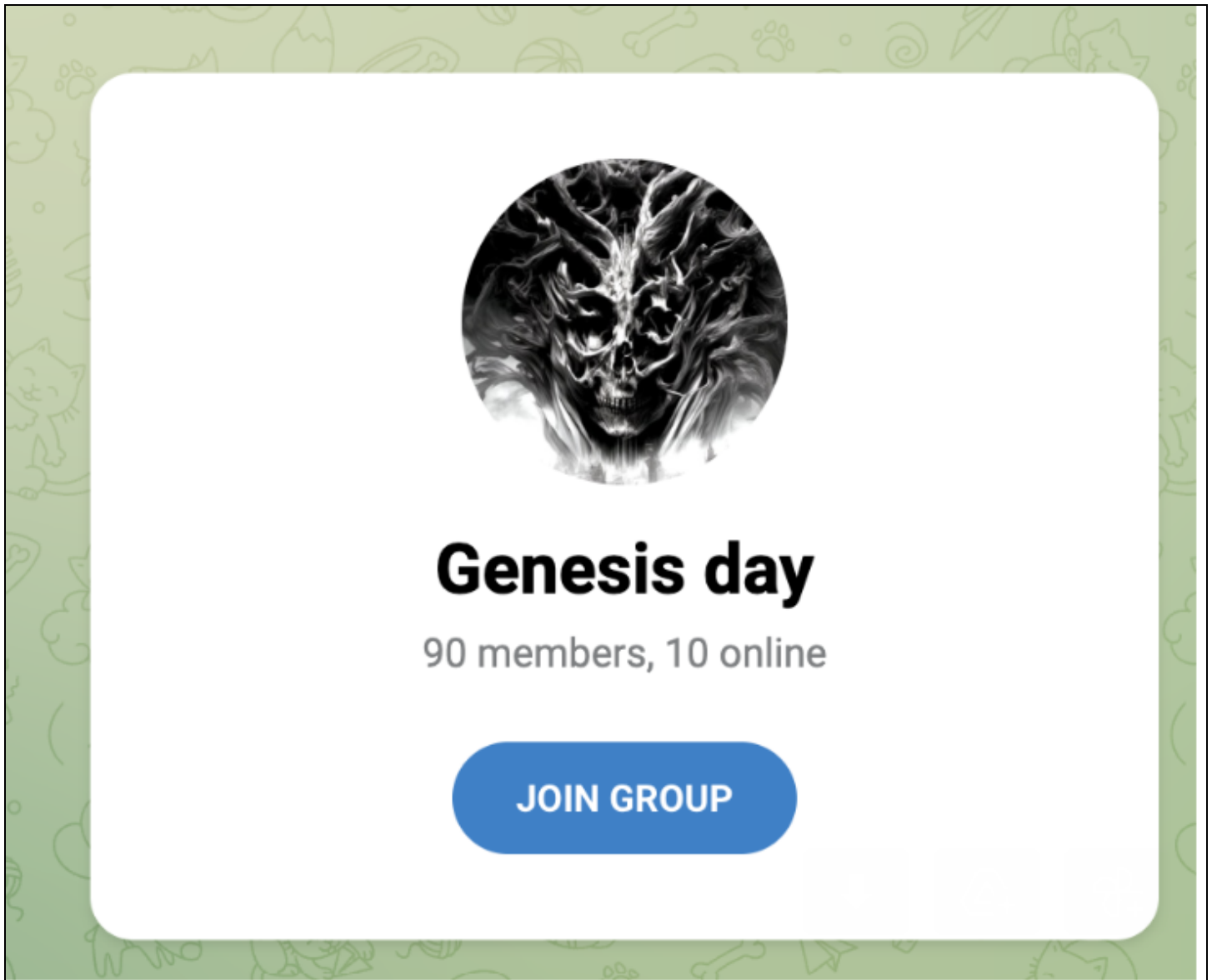
Genesis Day Channel (Members Channel)

Figure 3: Genesis Day member's channel (Source: Telegram)

The channel was created on December 27, 2022 and has 90 members as of mid-January 2023. Most of the conversations in the Telegram channel appear to be discussions on cybersecurity and geopolitical issues. The channel has 2 administrators: “Сергей” (Sergei), with the personal Telegram handle @rebook_cc, and “晓骑营openAI” (Xiaoqiying openAI), with the personal Telegram handle @TeteeserisBot. 晓骑营openAI also maintained a personal GitHub account at tubosheu.github[.]io, which went offline in early February 2023. On January 7, 2023, the threat actor posted the following statement on their GitHub page: “We plan to start a new round of operations against South Korea, and this will result in long-term data leakage. This operation will be long-lasting, and it will be updated on the official blog in lock-step.”

Below the declaration, the threat actor provided a list of email addresses and usernames of what appear to be South Korean nationals, with some of the listed email addresses having South Korean corporate domains for South Korean companies. The GitHub page went offline in early February 2023 along with both Telegram channels.

晓骑营

🏠 首页 📁 归档 🏷️ 标签 📁 分类 🗨️ 留言板 🌐 友链 📅 日志 👤 Myself ☰ 菜单 ▾

2023-1-7-韩国行动

📅 Created 2023-01-07 | 🔄 Updated 2023-01-07

👁️ Post View: 2552

CYBER SECURITY TEAM

我们准备针对韩国进行新一轮的行动，这次会长期造成数据泄露。

本次行动是长期，会同步更新在官方微博

用户名	邮箱	其他信息
ywshin70	214933	Kab00020200113104802

신용 drogon12!! shin1234551@gmail.com

TuBo
晓骑营官方负责人

Articles: 3 | Tags: 3 | Categories: 2

🔄 晓骑官方

📢 Announcement

Figure 4: The declaration of a “New Round of Operation Against South Korea” on the GitHub page of 晓骑营 openAI (Source: GitHub)

Dark Web and Special-Access Forums

On January 17, 2023, abort, a member of the now-defunct BreachForums, claimed that the Genesis Day threat group had hacked into the internal FTP service and the internal employee systems of the Samsung Group intranet due to South Korean cooperation with NATO and targeting Russia, Iran, and China. The threat actor shared alleged intrusion credentials in an Anonfiles link and claimed that the threat group would disclose Samsung Group's business data files in France, internal material flow analysis (MFA) flow chart, internal demonstration video, and the procedures for Samsung's internal system login, intranet system employee access credentials, and all Samsung employee credentials. The threat actor registered for an account on BreachForums on October 16, 2022, and had made 9 posts up to that point. However the account was permanently banned on BreachForums after several replies complained that the anonfiles link shared by the threat actor contained malware.

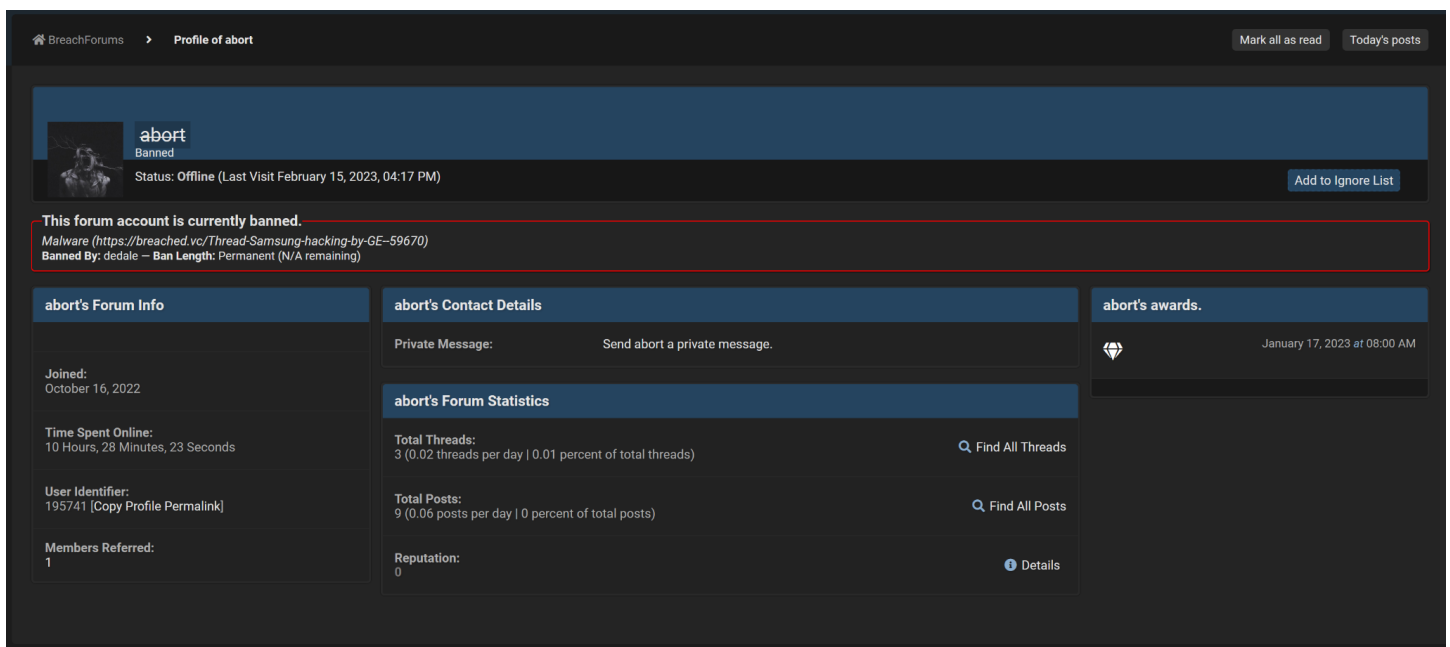


Figure 5: The screenshot shows that the threat actor abort was banned on BreachForums for posting the link to Samsung files that allegedly contained malware (Source: BreachForums)

On the same day, the threat actor uetus, who also claimed to operate under Genesis Day, made a similar post with an identical file download link on Ramp Forum. However, most of the replies complained that the link provided by the threat actor was not working. On February 16, 2023, uetus made a reference about being banned on BreachForums but also noted that new operations on South Korea are being planned.

On March 12, 2023, uetus made a post claiming to have penetrated a Japanese financial group and offering to sell access along with data from the customer and business system, which includes intranet access and customer loan data from 2001 to the present, as well as loan records with dozens of listed

companies. On March 22, 2023, “Liltys”, who had previously posted about selling ESXiArgs ransomware builders, asked uetus if they could work together to deploy EXSiArgs ransomware.

On April 5, 2023, uetus made another post on the Ramp Forum claiming to have compromised “Taiwan University” and leaked 25 GB of its data. Once again uterus claimed to operate on behalf of Genesis Day and stated that the motivation for the attack was due to the strengthening of cooperation between Taiwan and NATO. They claimed to have compromised the university’s internal network twice, gained access to the intranet, and shared a sample of the stolen data on the forum. The threat actor also stated that they would continue targeting Taiwan for the foreseeable future. The claim by uetus is consistent with the “Genesis Day 2022 Activity Summary” stated above in which they claimed to have achieved “penetration into a well-known higher education institute in Taiwan, and successfully obtained intranet access” in December 2022. Further examination of the screenshots shared by uetus shows the domain of vdi.ntu.edu[.]tw, which indicates the university in reference is likely the National Taiwan University, and the threat actors likely gained access to the Virtual Desktop Infrastructure (VDI). Another screenshot shows a TeamViewer remote control terminal, which means the threat actor might have gained access through a TeamViewer vulnerability.

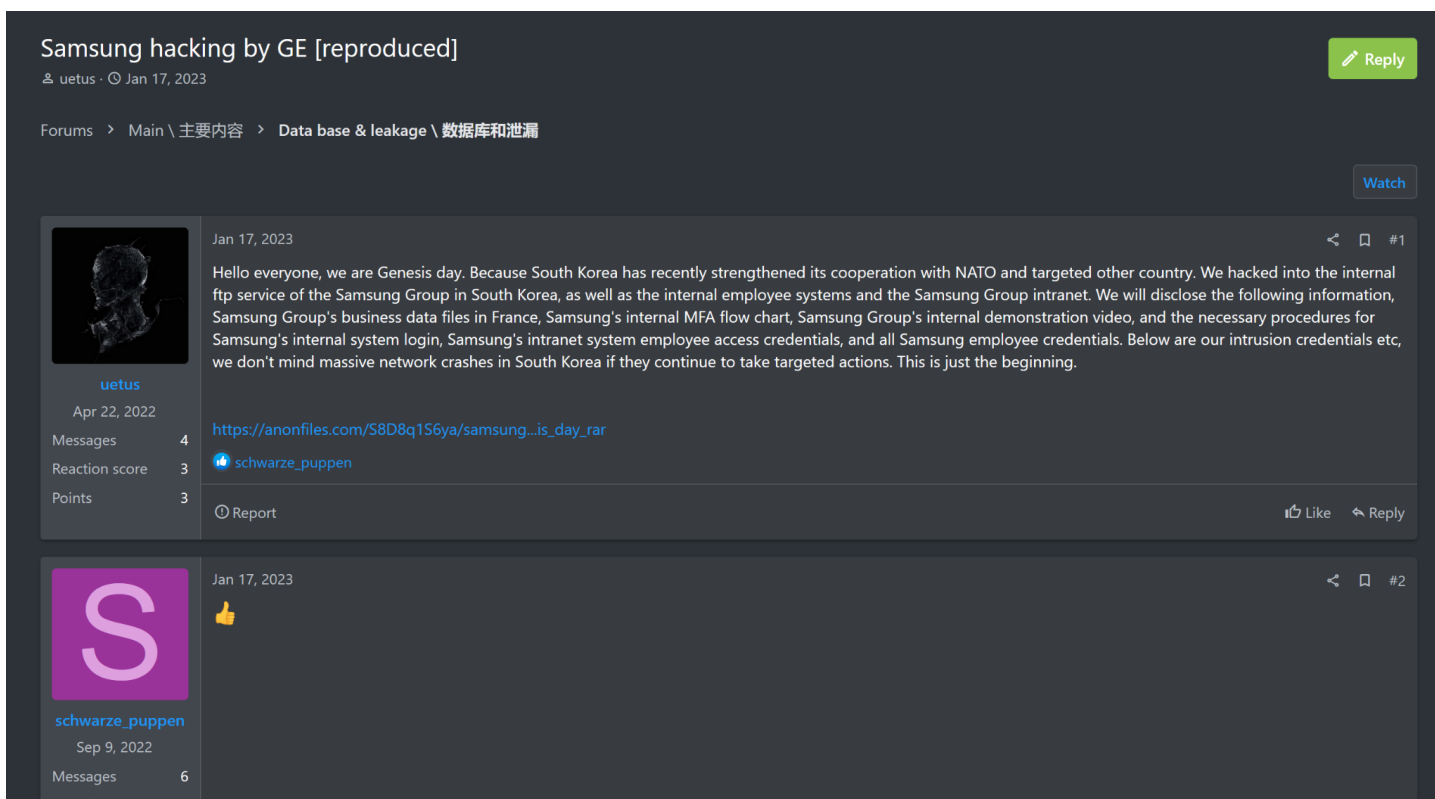


Figure 6: The post on Ramp Forum by uetus on Samsung (Source: Ramp Forum)

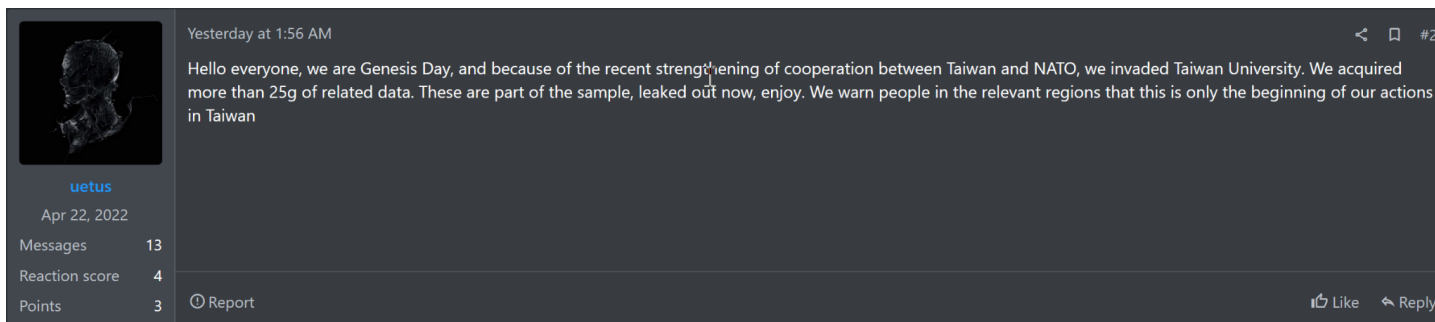


Figure 7: The post on Ramp Forum by uetus on the National University of Taiwan (Source: Ramp Forum)

Cleartnet

The Xiaoqiying group maintains a cleartnet website, [eisae\[.\]org](http://eisae[.]org), which acts as its public-facing announcement channel. The website shares the same logo as the GitHub page of 晓骑营openAI that went offline in early February 2023. Whois data shows that the domain was created on January 5, 2023. Live DNS lookup in Recorded Future shows that the domain resolves to 2 Cloudflare IP addresses: 172.67.139[.]24 and 104.21.87[.]2. DomainTools hosting history shows that on January 6, 2023, the domain changed from 34.102.136[.]180 to the current Cloudflare IP addresses. The IP address 34.102.136[.]180 shows a high malicious risk score of 89 on Recorded Future and was last associated with APT36's data exfiltration campaign targeting military and political users with Android malware.

At the time of this report, there are 7 announcements on the website. The "first published" date appears to pre-date the creation of this website. Recorded Future downloaded the data via the links included in the announcements, but we were unable to verify whether they were from the organizations they allegedly belong to or came from earlier data breaches.



Figure 9: The landing page of the website [eisae\[.\]org](http://eisae[.]org), the announcement page for the Xiaoying group (Source: [eisae\[.\]org](http://eisae[.]org))

Announcement 1

(First published January 3, 2022, updated February 19, 2022)

This is a recruiting message written in Simplified Chinese, Korean, and English. It listed the benefits of being a group member, including permission sharing, zero-day sharing, access to internal intelligence, sharing of malware libraries, proprietary tools, and camaraderie with fellow team members. It asked for those interested to send resumes to [xiaoeisae@proton\[.\]me](mailto:xiaoeisae@proton[.]me) and highlight the applicant's skills, experiences, and achievements. Neither the Korean nor the English announcements seemed to be written by native speakers.

Announcement 2

(First published on January 4, 2022; updated February 19, 2023)

In a message written in Simplified Chinese, the group claimed that an unnamed website has an unconditional remote code execution (RCE) vulnerability, and POC and EXP script tools are already written.

Announcement 3

(First published on January 7, 2022; updated February 19, 2023)

In a message written in Simplified Chinese, the group announced the end of its operation targeting South Korea.

Announcement 4

(First published on January 20, 2022; updated February 19, 2023)

In a message written in Simplified Chinese, the group announced “Operation South Korea 2, No. 2023-2” against the Korean Research Institute for Construction Policy. The message claimed the group had obtained access and data from Korean Research Institute for Construction Policy (ricon.re[.]kr) and offered screenshots as proof. Download links to stolen files were provided (contact Recorded Future for more details). This activity was [confirmed](#) in the news, and the network of the affected organization was recovered on January 30, 2023.

Announcement 5

(First published on January 25, 2022; updated February 19, 2023)

In a message written in Simplified Chinese, the group announced “Operation South Korea 3, No. 2023-3” against various educational institutions in South Korea. The group claimed to have penetrated the websites of dozens of research institutions and obtained over 50 GB of files, and claimed to have deleted the affected databases after file exfiltration. Download links to stolen files were provided (contact Recorded Future for more details). Some of the websites affected are listed in **Appendix B**.

Announcement 6

(First published on February 14, 2022; updated February 19, 2023)

In a message written in Simplified Chinese, the group welcomed new members and encouraged those who are feeling hesitant to join. It also claimed to have penetrated the IP addresses listed in **Appendix C**.

Announcement 7

(First published on February 18, 2022; updated February 19, 2023)

In a message written in Simplified Chinese, the group announced “Operation South Korea - 4, No. 2023 -4” against the Korean Accreditation Support Center (kab.or[.]kr). It claimed to have obtained 40,000 pieces of data including employee names, email addresses, passwords, and other sensitive information. The information obtained encompassed many government, businesses, and academic institutions. Screenshots were offered as proof of successful penetration. Download links to stolen files were provided (contact Recorded Future for more details).

Outlook

Xiaoqiying/Genesis Day threat group appears to be an ideologically driven hacktivist group that is not chiefly concerned with financial gains. The group claimed to be responsible for some unverified cyberattacks before the confirmed intrusions against numerous South Korean organizations in January and February 2023. As a result, we rate its credibility as moderate. It shared available penetration testing tools, malware, proofs of concept and exploits, and leaked data, and it claimed to have working relationships with some well-known cybercriminal and APT groups around the world. The group appears to be ambitious and is actively recruiting individuals with hacking skills.

Although it shows no clear ties to the Chinese government, Xiaoqiying is staunchly pro-China and vows to target NATO countries as well as any country or region that is deemed hostile to China. The most recent postings by its affiliated threat actors on special-access forums shows it has possibly compromised new targets in Japan and Taiwan and signaled a new round of cyberattacks against these countries. We recommend that organizations that are possibly targeted by this group, especially education, research, and government organizations in the Asian Pacific region, maintain a frequent patching cadence for their internet-facing devices and disable any unnecessary remote access tools. We will continue to monitor the activity of this group.

Appendix A

List of files shared on the Genesis Day Announcement Channel

Filename	Description
028cc9bd7fbfe1bfa963c40a63e0a71.png	Screenshot of chat
1659665503104.png	A list of Chinese data leaks
1659665516233.png	A list of Chinese data leaks
1663574132558.png	"Prynt Stealer has been activated" screenshot
2022年苹果越狱.docx	2002 Apple jailbreaking (in Russian)
2ef7eddf1db93a0fd43d377c146f432.png	Screenshot of chat
57f028d9c743ff63e1a141ca86b09d2.png	Screenshot of chat
59d7c5b56cdda281f74edfc2477f81e.png	Screenshot of Raid Forums user johnhana
5cdfbfaad93f79d42feecf08a9c7afa5363c847d3e9cb18c3d6188a757b292c6.7z	Password-protected 7-Zip file
604e88f08910155b245248ef0422070.png	Screenshot of chat
7b9f85b999f114d4209ad6b635929cb.png	Screenshot of chat
A Detailed Analysis of The Last Version of REvil Ransomware.pdf'	REvil ransomware report
AA21-265A-Conti_Ransomware_TLP_WHITE.pdf	Conti ransomware report
ChangeUrlScheme.exe	Korean software
Chrome-Android-and-Windows-0day-RCE-SBX-main.zip	Chrome and Windows exploit
Cobalt_Strike_4.7_original.jar	Cobalt Strike
CompTIA_Advanced_Security_Practitioner_CASP+_CAS_004_Cert_Guide.epub	Ebook on CompTIA certificates
GBL_USER.csv	scu.co[.]id user accounts
I3GSvcManager.exe	I3GSvcManager installer
MST_INVOICE_DETAIL.csv	Customer invoices
Nasa Sats.txt'	NASA satellite locations
Optus-10200-leak.rar	Optus data leak samples
PHP 库远程代码执行poc.txt'	PHP RCE POC

RFatw成员挖掘与关联猜想报告.doc	Analysis and speculations of Possible Members of AgainstTheWest on Raid Forums
Red Menshen BPFDoor Source Code().c'	Source code of Red Menshen BPFDoor
SARP_Samsung_Electronics_Corp_AD_Registration_Portal_User_ManualEN.pdf	Samsung user manual
The_Bvp47_a_top-tier_backdoor_of_us_nsa_equation_group_ii.en.pdf	Report on NSA Equation Group
Win32.Borat.rar	Password-protected .rar file
af470804de1edd93a0a7fec6143139.png	Johnhana Raid Forum screenshot
bruteratel.rar	Brute Ratel
burp crack.rar'	Burp Suite
burpsuite_pro_v2022.5.1.zip	Burp Suite
cobaltstrike.jar	Cobalt Strike
cobaltstrike4.4.rar	Cobalt Strike
d73bade8f7d6c4aa176528872d43260c6063e14ec29e35b3baab8a8263ddd173.7z	Password-protected 7-Zip file
f42bfc1d902f8faf3694b0c7a4d4ce481bbe1dc8851d652db1118ef610ee3c19.7z	Password-protected 7-Zip file
fb0420918514a5836cb1d04813f0935.png	Screenshot of chat
fbileak文件.rar	FBI leak document
ins封号思路.txt	INS
killnet成员信息.txt	Killnet membership information
letters-to-jokowi.zip	Unknown data
rrrrrrrr.wmv	Security footage of unknown entity
sitemap.xml	Cia[.]gov website sitemap
twitter.rar	Twitter leaks
weleakinfo.com.rar	WeLeakInfo[.]com containing credit card information and Stripe accounts
xiaomi_remove_mi_account_and_frp.rar	How to remove Mi accounts

Appendix B

Partial List of Domains Allegedly Compromised by Xiaoqiying

Domains	Organization
woorimal[.]org/pages/index.php	Woorimal Academic Society
aspg.or[.]kr	Association for Studies in Parents and Guardians
kriee.or[.]kr/pages/index[.]php	Research Institute for Early Childhood Education
kmhs.newnonmun[.]com	Korean Academy of Basic Medicine & Health Science
klsgss.or[.]kr	Korean Lesson Study Group for Social Studies
kewms.co[.]kr	Korean East-West Mind Science Association
cleftlp.or[.]kr/pages/index.php	Korean Cleft Lip and Palate Association

Appendix C

List of IP Addresses Allegedly Compromised by Xiaoqiying and Organizations They Correlate To

IP Addresses	Organization
hxxp://211.56.76[.]12:11001/wls-wsat/index.html	Korea Telecom
hxxp://114.108.133[.]70:7001/wls-wsat/index.html	LG DACOM KIDC
hxxp://61.79.234[.]100:7002/wls-wsat/index.html	Korea Telecom
hxxp://222.107.71[.]133:8111/wls-wsat/index.html	Korea Telecom
hxxp://211.220.216[.]122:8015/wls-wsat/index.html	Korea Telecom

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,500 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at [@RecordedFuture](https://twitter.com/RecordedFuture)