WATCHTOWER
FLASH REPORT

SentinelOne

CYBER RISK RATING SYSTEM

LOW

- Minimal threat activity, low prevalence of vulnerability, low impact of threat
- **Overall risk assessment: LOW**

GUARDED

- Moderate threat activity, moderate prevalence of vulnerability, low impact of threat
- **Overall risk assessment: GUARDED**

ELEVATED

- Moderate threat activity, moderate prevalence of vulnerability, moderate impact of threat
- **Overall risk assessment: ELEVATED**

HIGH

- Significant threat activity, significant prevalence of vulnerability, Significant impact of threat
- **Overall risk assessment: HIGH**

SEVERE

- Significant/high threat activity, high prevalence of vulnerability, high impact of threat
- **Overall risk assessment: SEVERE**

Chinese APT Targets Global Government Officials

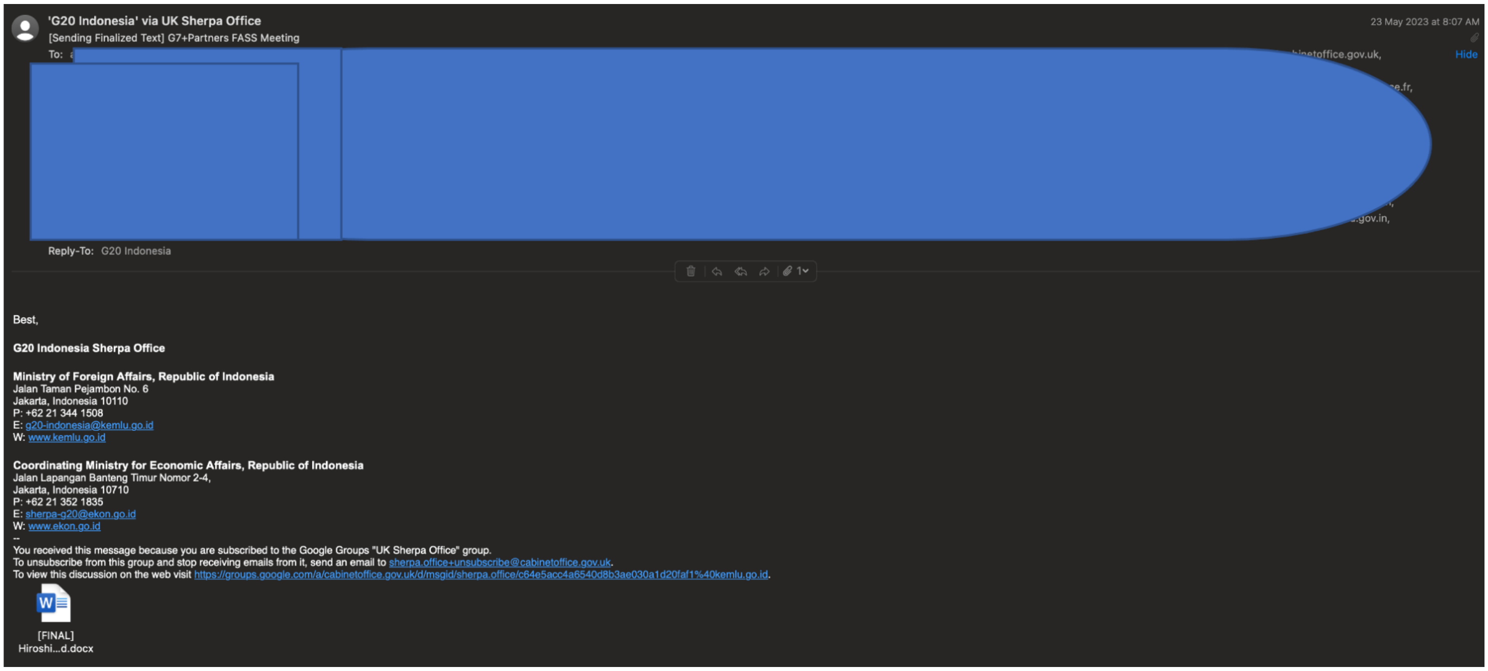
Document Type: WatchTower Flash Report	**TLP:** Green
Date of Publication: 29 May 2023	**Cyber Risk Rating:** Elevated
Date of Research: 23 May 2023	**Threat Actors / Malware Families Referenced:** RoyalRoad, 8.t, CVE-2017-11882

Key Takeaways:

- WatchTower hunters have identified a malicious Rich Text Format (RTF) file exploiting CVE-2017-11882. This document references a recent G7 meeting between the leaders of Ukraine, Australia, Brazil, the Cook Islands, Comoros, India, Indonesia, Republic of Korea, and Vietnam to discuss international peace and security to lure its targets into downloading and opening the document.
- WatchTower was able to match this file, named “[FINAL] Hiroshima Action Statement for Resilient Global Food Security_trackchanged.docx” to another document found here.
- CVE-2017-11882 is a 17-year-old memory corruption issue in Microsoft Office (including Office 360). When exploited successfully, it can let attackers execute remote code on a vulnerable machine. This attacker uses a builder tool named RoyalRoad, which several Chinese APT groups previously used to poison Microsoft Office files to target government officials in 2017.

Technical Details:

Threat actors sent out an email targeting government officials affiliated with France, the United Kingdom, India, Singapore, and Australia. The email’s author claimed to be part of Indonesia’s Ministries of Foreign and Economic Affairs.



'G20 Indonesia' via UK Sherpa Office

[Sending Finalized Text] G7+Partners FASS Meeting

23 May 2023 at 8:07 AM

To: [redacted]

Reply-To: G20 Indonesia

Best,

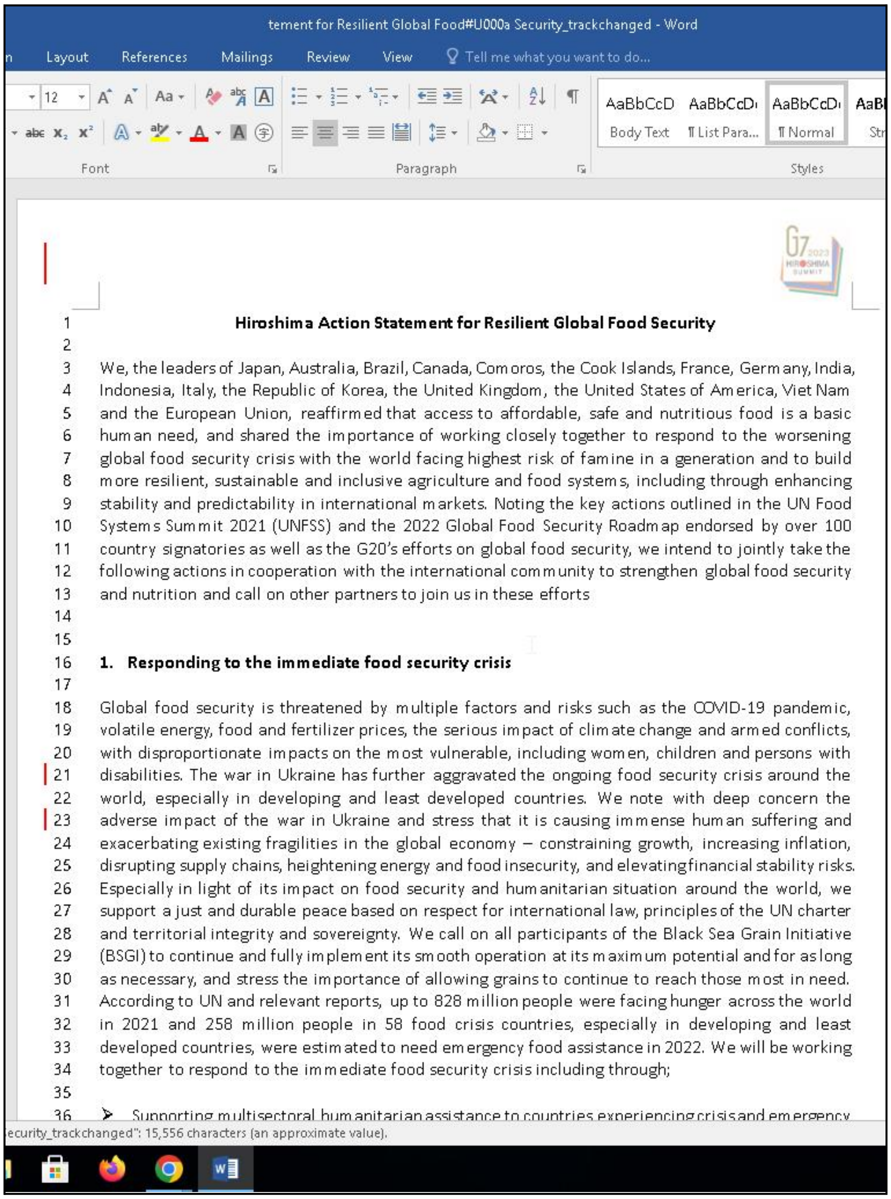
G20 Indonesia Sherpa Office

Ministry of Foreign Affairs, Republic of Indonesia
Jalan Taman Pejambon No. 6
Jakarta, Indonesia 10110
P: +62 21 344 1508
E: g20-indonesia@kemlu.go.id
W: www.kemlu.go.id

Coordinating Ministry for Economic Affairs, Republic of Indonesia
Jalan Lapangan Banteng Timur Nomor 2-4,
Jakarta, Indonesia 10710
P: +62 21 352 1835
E: sherpa-g20@ekon.go.id
W: www.ekon.go.id
--
You received this message because you are subscribed to the Google Groups "UK Sherpa Office" group.
To unsubscribe from this group and stop receiving emails from it, send an email to sherpa.office+unsubscribe@cabinetoffice.gov.uk.
To view this discussion on the web visit https://groups.google.com/a/cabinetoffice.gov.uk/d/msgid/sherpa.office/c64e5acc4a6540d8b3ae030a1d20faf1%40kemlu.go.id.

[FINAL]
Hiroshi...d.docx

The document attached to this email claims to be a series of action statements from the recent G7 meeting in Hiroshima, Japan regarding “global food security.” The document also specifically refers to security issues surrounding the South China Sea. Chinese APT groups have previously used this sensitive political issue against targets within South Asian governments and government-affiliated entities, as shown in the following screenshots:


tement for Resilient Global Food#U000a Security_trackchanged - Word
Layout
References
Mailings
Review
View
Tell me what you want to do...
12
Font
Paragraph
AaBbCcD
Body Text
AaBbCcD
¶ List Para...
AaBbCcD
¶ Normal
Styles
G7 2023 HIROSHIMA SUMMIT
ecurity_trackchanged": 15,556 characters (an approximate value).

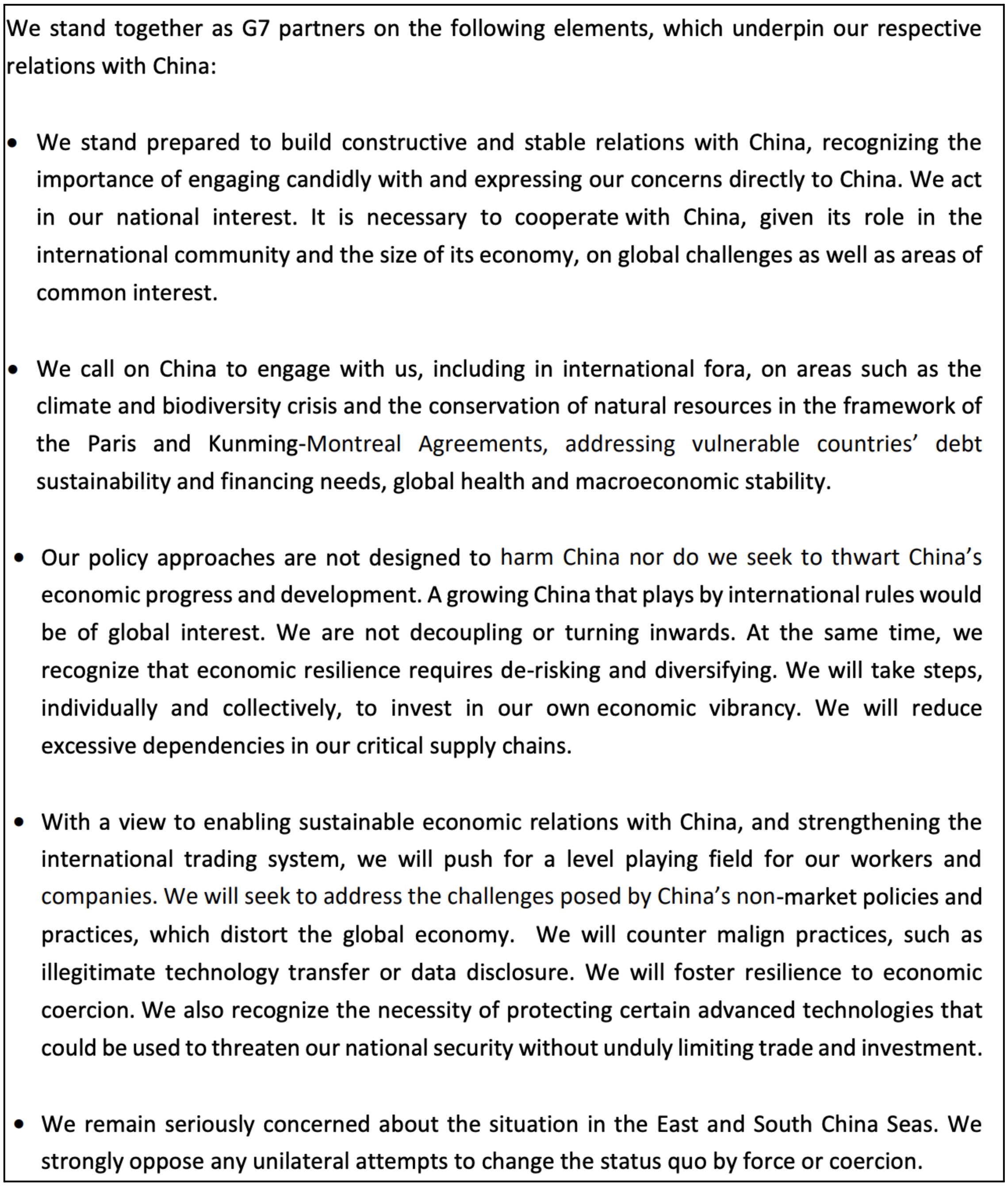
Hiroshima Action Statement for Resilient Global Food Security

We, the leaders of Japan, Australia, Brazil, Canada, Comoros, the Cook Islands, France, Germany, India, Indonesia, Italy, the Republic of Korea, the United Kingdom, the United States of America, Viet Nam and the European Union, reaffirmed that access to affordable, safe and nutritious food is a basic human need, and shared the importance of working closely together to respond to the worsening global food security crisis with the world facing highest risk of famine in a generation and to build more resilient, sustainable and inclusive agriculture and food systems, including through enhancing stability and predictability in international markets. Noting the key actions outlined in the UN Food Systems Summit 2021 (UNFSS) and the 2022 Global Food Security Roadmap endorsed by over 100 country signatories as well as the G20's efforts on global food security, we intend to jointly take the following actions in cooperation with the international community to strengthen global food security and nutrition and call on other partners to join us in these efforts

1. Responding to the immediate food security crisis

Global food security is threatened by multiple factors and risks such as the COVID-19 pandemic, volatile energy, food and fertilizer prices, the serious impact of climate change and armed conflicts, with disproportionate impacts on the most vulnerable, including women, children and persons with disabilities. The war in Ukraine has further aggravated the ongoing food security crisis around the world, especially in developing and least developed countries. We note with deep concern the adverse impact of the war in Ukraine and stress that it is causing immense human suffering and exacerbating existing fragilities in the global economy – constraining growth, increasing inflation, disrupting supply chains, heightening energy and food insecurity, and elevating financial stability risks. Especially in light of its impact on food security and humanitarian situation around the world, we support a just and durable peace based on respect for international law, principles of the UN charter and territorial integrity and sovereignty. We call on all participants of the Black Sea Grain Initiative (BSGI) to continue and fully implement its smooth operation at its maximum potential and for as long as necessary, and stress the importance of allowing grains to continue to reach those most in need. According to UN and relevant reports, up to 828 million people were facing hunger across the world in 2021 and 258 million people in 58 food crisis countries, especially in developing and least developed countries, were estimated to need emergency food assistance in 2022. We will be working together to respond to the immediate food security crisis including through;

➢ Supporting multisectoral humanitarian assistance to countries experiencing crisis and emergency



We stand together as G7 partners on the following elements, which underpin our respective relations with China:

- We stand prepared to build constructive and stable relations with China, recognizing the importance of engaging candidly with and expressing our concerns directly to China. We act in our national interest. It is necessary to cooperate with China, given its role in the international community and the size of its economy, on global challenges as well as areas of common interest.

- We call on China to engage with us, including in international fora, on areas such as the climate and biodiversity crisis and the conservation of natural resources in the framework of the Paris and Kunming-Montreal Agreements, addressing vulnerable countries' debt sustainability and financing needs, global health and macroeconomic stability.

- Our policy approaches are not designed to harm China nor do we seek to thwart China's economic progress and development. A growing China that plays by international rules would be of global interest. We are not decoupling or turning inwards. At the same time, we recognize that economic resilience requires de-risking and diversifying. We will take steps, individually and collectively, to invest in our own economic vibrancy. We will reduce excessive dependencies in our critical supply chains.

- With a view to enabling sustainable economic relations with China, and strengthening the international trading system, we will push for a level playing field for our workers and companies. We will seek to address the challenges posed by China's non-market policies and practices, which distort the global economy. We will counter malign practices, such as illegitimate technology transfer or data disclosure. We will foster resilience to economic coercion. We also recognize the necessity of protecting certain advanced technologies that could be used to threaten our national security without unduly limiting trade and investment.

- We remain seriously concerned about the situation in the East and South China Seas. We strongly oppose any unilateral attempts to change the status quo by force or coercion.

WatchTower reviewed this malicious document and confirmed that it drops an infostealer with the hash value `SHA1: a4e89d1f060e4dfd5f0fd4e7ba8be96967b39ac7` that connects to the following C2: `13.236.189.80`

For more information, guidance, or general help, contact us at watchtower@sentinelone.com. All queries in the report will be available in the WatchTower Hunting Library in our upcoming GSS community.

Tactical Tools for HuntOps:

Hunting Queries:

```
DstIP = "13.236.189.80"
Sha1 = "a4e89d1f060e4dfd5f0fd4e7ba8be96967b39ac7"
```