Rewterz Threat Alert – SharpPanda Chinese APT Group Targets Southeast Asian Government - Active IOCs - Rewterz

Published: 2022-01-25 · Archived: 2026-04-05 12:57:30 UTC

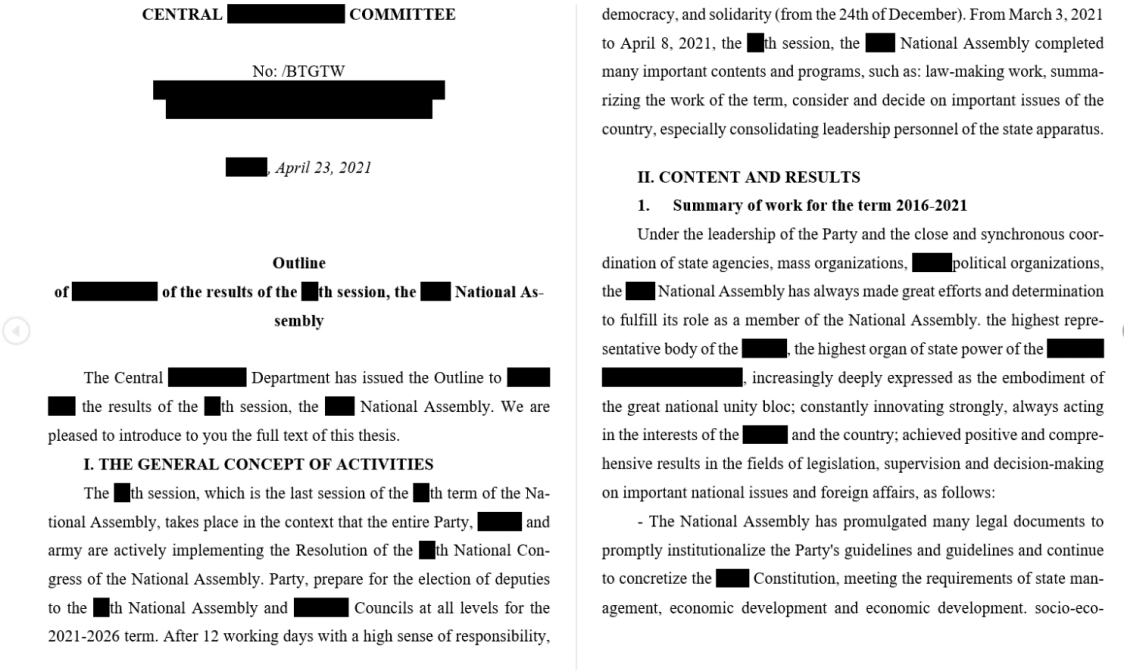
Severity

High

Analysis Summary

SharpPanda, the Chinese advanced persistent (APT) threat actor that has been active since at least 2018, has reinforced its cyber warfare activities. SharpPanda APT attacks and targets Southeast Asian government users with template injection of malicious documents. The attackers use spear-phishing to gain initial access and leverage old Microsoft Office vulnerabilities together with the chain of in-memory loaders to attempt and install a previously unknown backdoor on the victim's machines. Upon opening the document, it connects back to the hacker's server to download the payload file.

The investigation starts from the campaign of malicious DOCX documents that are sent to different employees of a government entity in Southeast Asia. In some cases, the emails are spoofed to look like they were from other government-related entities. The attachments to these emails are weaponized copies of legitimate-looking official documents and use the remote template technique to pull the next stage from the attacker's server.



CENTRAL [redacted] COMMITTEE

No: /BTGTW

[redacted]

[redacted], *April 23, 2021*

Outline

of [redacted] of the results of the [redacted]th session, the [redacted] National Assembly

The Central [redacted] Department has issued the Outline to [redacted] the results of the [redacted]th session, the [redacted] National Assembly. We are pleased to introduce to you the full text of this thesis.

I. THE GENERAL CONCEPT OF ACTIVITIES

The [redacted]th session, which is the last session of the [redacted]th term of the National Assembly, takes place in the context that the entire Party, [redacted] and army are actively implementing the Resolution of the [redacted]th National Congress of the National Assembly. Party, prepare for the election of deputies to the [redacted]th National Assembly and [redacted] Councils at all levels for the 2021-2026 term. After 12 working days with a high sense of responsibility, democracy, and solidarity (from the 24th of December). From March 3, 2021 to April 8, 2021, the [redacted]th session, the [redacted] National Assembly completed many important contents and programs, such as: law-making work, summarizing the work of the term, consider and decide on important issues of the country, especially consolidating leadership personnel of the state apparatus.

II. CONTENT AND RESULTS

1. Summary of work for the term 2016-2021

Under the leadership of the Party and the close and synchronous coordination of state agencies, mass organizations, [redacted] political organizations, the [redacted] National Assembly has always made great efforts and determination to fulfill its role as a member of the National Assembly. the highest representative body of the [redacted], the highest organ of state power of the [redacted], increasingly deeply expressed as the embodiment of the great national unity bloc; constantly innovating strongly, always acting in the interests of the [redacted] and the country; achieved positive and comprehensive results in the fields of legislation, supervision and decision-making on important national issues and foreign affairs, as follows:

- The National Assembly has promulgated many legal documents to promptly institutionalize the Party's guidelines and guidelines and continue to concretize the [redacted] Constitution, meeting the requirements of state management, economic development and economic development. socio-eco-

Impact

- Template Injection
- Exposure of Sensitive Data

Indicators of Compromise

IP

- 45[.]91[.]225[.]139
- 107[.]148[.]165[.]151
- 45[.]121[.]146[.]88

MD5

- 1e9f1746c2dbea0df5017afdf8b94189
- d598749a8c86b1cdd313ff6c86626c86
- d843b58f31c687d22de09a6765b3ba3b
- 51205f6ca73745b97b77095a2bfd7091
- 8bcea4940166222eff5c4ed897e5cccf
- 31565db2614bb5de2baf1a5c07771860
- 24448ffdb1a8ba9a9202a9c7178301c4
- fc51ba4706ac462d2fec8ba2be04dc1d
- 494a01d421997040de3583b3e08212a7
- f706f042c1953a9cea932d3cd770b2ad
- eff68f1096ae56ae94f439a8e5effe3d

SHA-256

- 6f66faf278b5e78992362060d6375dcc2006bcee29ccc19347db27a250f81bcd
- 0c346972a2ccebb2642ced34213f43595896da233f06f6251967517ae342908f
- d198c4d82eba42cc3ae512e4a1d4ce85ed92f3e5fdff5c248acd7b32bd46dc75
- 0752c24ded7cc434a56fdd10c4f2c45144ca53252192e21cfa4cee3a5ad68796
- 928f540c9658a458edc649371e178a7c83e2a9291f5b23ae326c3d64bfa902c6
- 4cc521b470d08c9684cd15ffac032accd50439b81873ee2d87897ab8c495744b
- 0e8fb748cd58ab2fa754e2fa16e4390327a10593ca72bb6a3b90a1885cbe5387

SHA-1

- f9d958c537b097d45b4fca83048567a52bb597bf
- 417e4274771a9614d49493157761c12e54060588
- 176a0468dd70abe199483f1af287e5c5e2179b8c
- 8bad3d47b2fc53dc6f9e48debac9533937c32609
- aa5458bdfefe2a97611bb0fd9cf155a06f88ef5d
- 0726e56885478357de3dce13efff40bfba53ddc2

Remediation

- Block the threat indicators at their respective controls.
- Search for IOCs in your environment.
