ZDNet | MENU | US

MUST READ: Cybersecurity: Why a culture of silence and driving mistakes underground is bad for everyone

Chinese cybercriminals spent three years creating a new backdoor to spy on governments

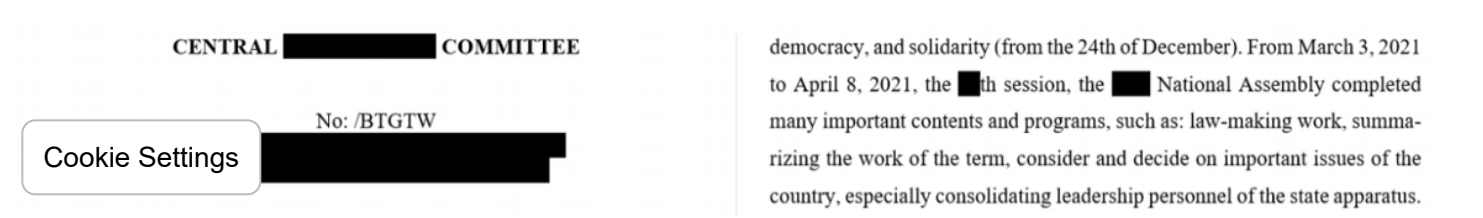
The new tool has been used in ongoing cyberespionage activities.

By Charlie Osborne for Zero Day | June 3, 2021 -- 10:00 GMT (03:00 PDT) | Topic: Security

A new backdoor used in ongoing cyberespionage campaigns has been connected to Chinese threat actors.

On Thursday, Check Point Research (CPR) said that the backdoor (https://research.checkpoint.com/2021/sharppanda-chinese-apt-group-targets-southeast-asian-government-with-previously-unknown-backdoor/) has been designed, developed, tested, and deployed over the past three years in order to compromise the systems of a Southeast Asian government's Ministry of Foreign Affairs.

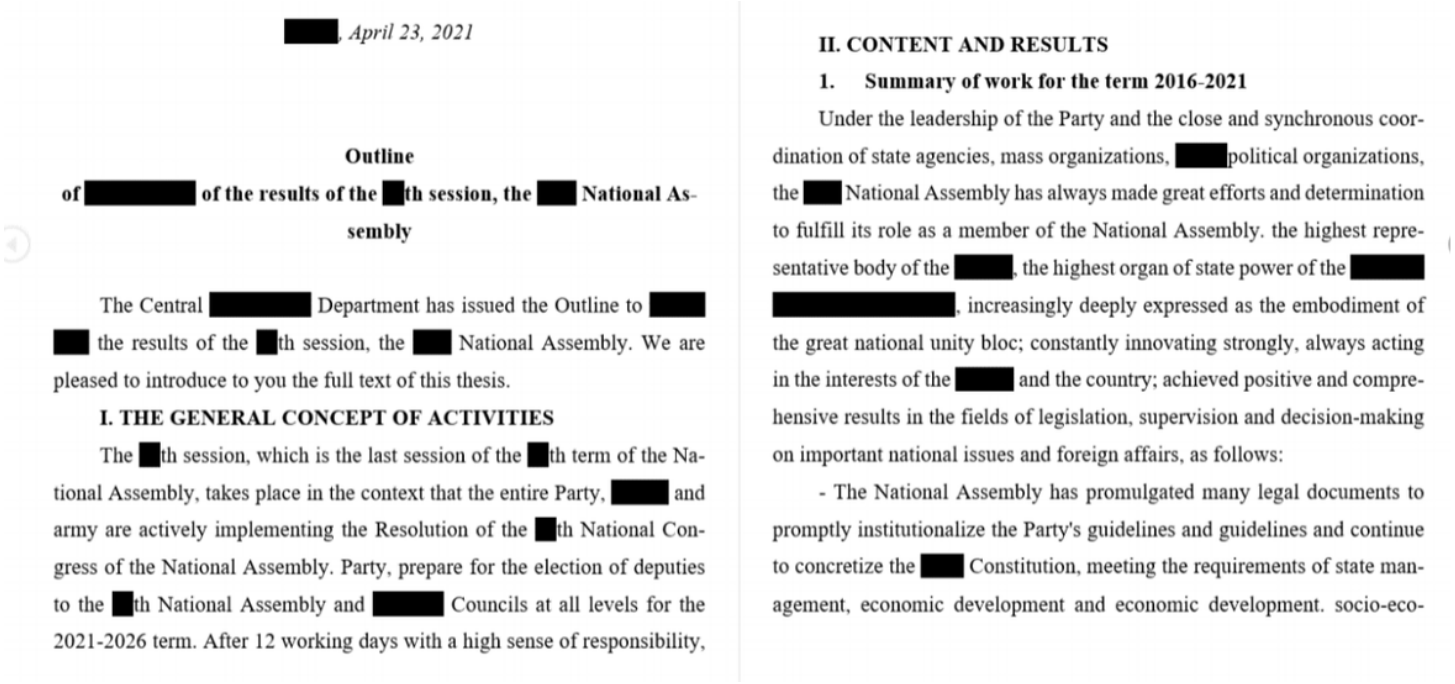
The Windows-based malware's infection chain began with spear phishing (https://www.zdnet.com/article/what-is-phishing-how-to-protect-yourself-from-scam-emails-and-more) messages, impersonating other departments in the same government, in which members of staff were targeted with weaponized, official-looking documents sent via email.


CENTRAL [redacted] COMMITTEE

No: /BTGTW [redacted]

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.

Cookie Settings



[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,

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-

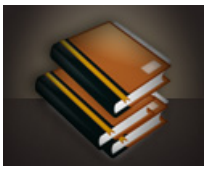
If victims open the files, remote .RTF templates are pulled and a version of Royal Road (https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html), an RTF weaponizer, is deployed.

The tool works by exploiting a set of vulnerabilities in Microsoft Word's Equation Editor (https://www.zdnet.com/article/windows-patches-microsoft-kills-off-words-under-attack-equation-editor-fixes-56-bugs/) (CVE-2017-11882 (https://nvd.nist.gov/vuln/detail/CVE-2017-11882), CVE-2018-0798 (https://nvd.nist.gov/vuln/detail/CVE-2018-0798), and CVE-2018-0802 (https://nvd.nist.gov/vuln/detail/CVE-2018-0802)).

CPR says that Royal Road is "especially popular with Chinese [advanced persistent threat] APT groups."

The RTF document contains shellcode and an encrypted payload designed to create a scheduled task and to launch time-scanning anti-sandboxing techniques, as well as a downloader for the final backdoor (https://www.zdnet.com/article/cyber-espionage-campaign-opens-backdoor-to-steal-documents-from-infected-pcs/).

Cookie Settings



(https://adclick.g.doubleclick.net/pcs/click%253Fxai%253DAKAOjstHwRYf8KDUVqGh-jfi5210j0r1BKPrfI8hTOFvm_UxLD2krx7lXBRictb-QJLsqatH4zETfooUrvTTuWKyBlHJl_7hcdf8_cs2P8s5GQjfwnClYrETfAThH1gVxuaTfso0yR2JlMi37LJDQT48zUEb6OZG-QhJWmoQA45IRQcLSo3fiyCdLxqgmhKL9x82kEMOBTSQqJThGlcf56ToGdNHKkXPe5WsRxSxt_m6AjPZBdgDsyKMM5_TDjsuxVs_Ba6Fd7yZDsd6YvSCc5t9xGc253C45Fuqyg%2526sig%253DCg0ArKJSzNCjGJf6HDwREAE%2526fbs_aeid%253D%255Bgw_fedition=en&ursuid=&devicetype=desktop&pagetype=&assettitle=&assettype=&topicguid=&viewguid=d2a1b71f-1c47-4f92-bb06-d97c6c03b890&docid=33171834&promo=1065&ftag_cd=TRE-00-10aaa4f&spotname=dfp-in-article&destUrl=https%253A%252F%252Fwww.techrepublic.com%252Fresource-library%252Fwhitepapers%252Fparagon-automation-using-closed-loop-automation-in-service-performance-asean%252F%253Fpromo%253D1065%2526ftag%253DTRE-00-10aaa4f%2526cval%253Ddfp-in-article%2526source%253Dzdnet%2526tid%253D406210527504906131&ctag=medc-proxy&siteId=&rsid=cnetzdnetglobalsite&sl=&sc=us&assetguid=&q=&cval=33171834;1065&ttag=&bhid=&poolid=&tid=406210527

Paragon Automation: Using Closed-Loop Automation in Service Performance - ASEAN

(https://adclick.g.doubleclick.net/pcs/click%253Fxai%253DAKAOjstHwRYf8KDUVqGh- ...

Juniper's Paragon Automation is cloud-ready, providing flexible deployment optior ...

Resource Center (https://www.techrepublic.com/resource-library/content-type/resourcecenter/) provided by Juniper Networks (https://www.techrepublic.com/resource-library/company/juniper-networks/)

Dubbed "VictoryDll_x86.dll," the backdoor has been developed to contain a number of functions suitable for spying and the exfiltration of data to a command-and-control server (C2).

SECURITY

(https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/)

Cyber security 101: Protect your privacy from hackers, spies, and the government
(https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/)

Simple steps can make the difference between losing your online accounts or maintaining what is now a precious commodity: Your privacy.

R ww.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-g

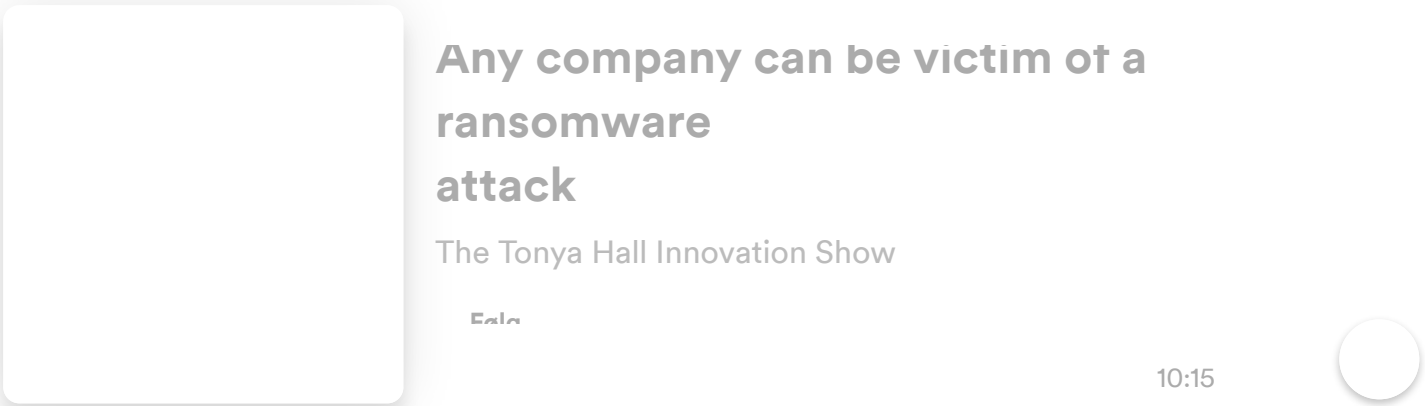
Cookie Settings

These include the read/write and deletion of files; harvesting OS, process, registry key and services information, the ability to run commands through cmd.exe, screen grabbing, creating or terminating processes, obtaining the titles of top-level windows, and the option to close down PCs.

The backdoor connects to a C2 to pass along stolen data and this server may also be used to grab and execute additional malware payloads. First stage C2s are hosted in Hong Kong and Malaysia, while the backdoor C2 server is hosted by a US provider.

CPR believes it is likely that the backdoor is the work of Chinese threat actors due to its limited operational schedule -- 1.00 am -- 8.00 am UTC -- the use of Royal Road, and due to test versions of the backdoor, uploaded to VirusTotal in 2018, which contained connectivity checks with Baidu's web address.

"We learned that the attackers are not only interested in cold data, but also what is happening on a target's personal computer at any moment, resulting in live espionage," commented Lotem Finkelsteen, head of threat intelligence at CPR. "Although we were able to block the surveillance operation for the Southeast Asian government described, it's possible that the threat group is using its new cyberespionage weapon on other targets around the world."



PREVIOUS AND RELATED COVERAGE

- Chinese hackers cloned attack tool belonging to NSA's Equation Group (https://www.zdnet.com/article/chinese-hackers-cloned-attack-tools-belonging-to-nsas-equation-group/)
- President Xi Jinping wants China to accelerate efforts in becoming technologically self-reliant

Cookie Settings

t.com/article/xi-jinping-wants-to-accelerate-efforts-in-making-china-technologically-self-reliant/)