CYBER THREAT ANALYSIS

CHINA

Recorded Future®

By Insikt Group®

September 24, 2025

RedNovember Targets Government, Defense, and Technology Organizations

RedNovember has significantly broadened its targeting to include the US defense industrial base, aerospace, and high-technology manufacturing verticals, including semiconductors.

RedNovember continues to conduct spearphishing campaigns, but is increasingly pursuing vulnerability exploitation against edge devices, including firewalls and VPNs, and access to OWA instances.

RedNovember continues to target government and military organizations, including in relation to high-profile geopolitical events, economic opportunities, or military exercises.

Note: The analysis cut-off date for this report was July 25, 2025

Executive Summary

In July 2024, Insikt Group publicly reported on TAG-100, a threat activity group conducting suspected cyber-espionage activity targeting high-profile government, intergovernmental, and private sector organizations globally using the open-source, multi-platform Go backdoor Pantegana. At the time, we did not attribute this activity to a particular country; however, after reviewing all available evidence, we assess that TAG-100 is highly likely a Chinese state-sponsored threat activity group. Accordingly, Insikt Group now tracks this group under the designation RedNovember.

Between June 2024 and July 2025, RedNovember (which overlaps with Storm-2077) targeted perimeter appliances of high-profile organizations globally and used the Go-based backdoor Pantegana and Cobalt Strike as part of its intrusions. The group has expanded its targeting remit across government and private sector organizations, including defense and aerospace organizations, space organizations, and law firms.

Using Recorded Future Network Intelligence, Insikt Group identified new likely victims, which include a ministry of foreign affairs in central Asia, a state security organization in Africa, a European government directorate, and a Southeast Asian government. RedNovember also targeted at least two United States (US) defense contractors, a European engine manufacturer, and a trade-focused intergovernmental cooperation body in Southeast Asia.

We observed RedNovember reconnoitering and likely compromising edge devices for initial access, including SonicWall, Cisco Adaptive Security Appliance (ASA), F5 BIG-IP, Palo Alto Networks GlobalProtect, Sophos SSL VPN, and Fortinet FortiGate instances, as well as Outlook Web Access (OWA) instances and Ivanti Connect Secure (ICS) VPN appliances.

RedNovember's activity exemplifies the ability to combine weaponized proof-of-concept (PoC) exploits with open-source post-exploitation frameworks such as Pantegana, lowering the entry barrier for less-capable threat actors. It also allows higher-tier groups to refrain from using customized tools during operations in which they are less concerned with being detected or in which heightened attribution obfuscation is desirable.

Insikt Group followed responsible disclosure procedures in advance of this publication per Recorded Future's notification policy.

Key Findings

- RedNovember continues to rely on command-and-control (C2) frameworks (Pantegana and Cobalt Strike) and open-source backdoors (SparkRAT) for its operations.
- The threat group has significantly broadened its targeting, including by conducting spearphishing and vulnerability exploitation attempts against entities in the US defense industrial base (DIB) and space organizations in Europe.
- At least some of the RedNovember activity that Insikt Group observed, including in Taiwan and Panama, took place in close proximity to geopolitical and military events of key strategic interest to China.
- RedNovember has also increasingly focused its initial access efforts on targeting edge devices, including security solutions such as VPNs, firewalls, load balancers, virtualization infrastructure, and email servers.
- In April 2025, the threat group conducted a campaign focused on the reconnaissance and targeting of Ivanti Connect Secure (ICS) VPN devices across multiple countries. Specific targets included a major US newspaper and a specialized US engineering and military contractor.

Table of Contents

Background

RedNovember (previously tracked as TAG-100 and overlapping with Storm-2077) is a Chinese state-sponsored cyber-espionage group that leverages open-source tools and exploits internet-facing devices to target government, intergovernmental, and private sector organizations globally. Insikt Group has previously publicly reported on RedNovember's use of the multi-platform Go-based backdoor Pantegana and other offensive security tools, including Cobalt Strike and SparkRAT, coupled with exploitation of perimeter appliances, to conduct reconnaissance, initial access, and probable compromise activities.

RedNovember's strategic use of open-source capabilities allows the threat group to lower operational costs and obfuscate attribution, a tactic that aligns with broader state-sponsored cyber-espionage trends that Insikt Group has observed. Combining weaponized proof-of-concept (PoC) exploits and open-source tools enables RedNovember to operate at scale. RedNovember's activity highlights the persistent vulnerabilities of perimeter devices, which remain a significant risk vector due to limited visibility and logging capabilities.

RedNovember is one of multiple other Chinese state-sponsored threat groups that are increasingly achieving initial access to targets by targeting vulnerabilities in internet-facing devices, including security products. Targeting internet-facing devices has proven to be an effective way for Chinese state-sponsored threat groups to scale initial access and achieve initial footholds in large numbers of organizations ahead of more targeted follow-on activity.

Technical Analysis

Since our initial public report on its activity, RedNovember has continued to use the Pantegana C2 framework and Cobalt Strike as part of its intrusion activity. From our visibility and collection, RedNovember also highly likely continues to use ExpressVPN to administer its servers and may, with realistic probability, have started using other VPNs such as Warp VPN to remotely connect to its infrastructure.

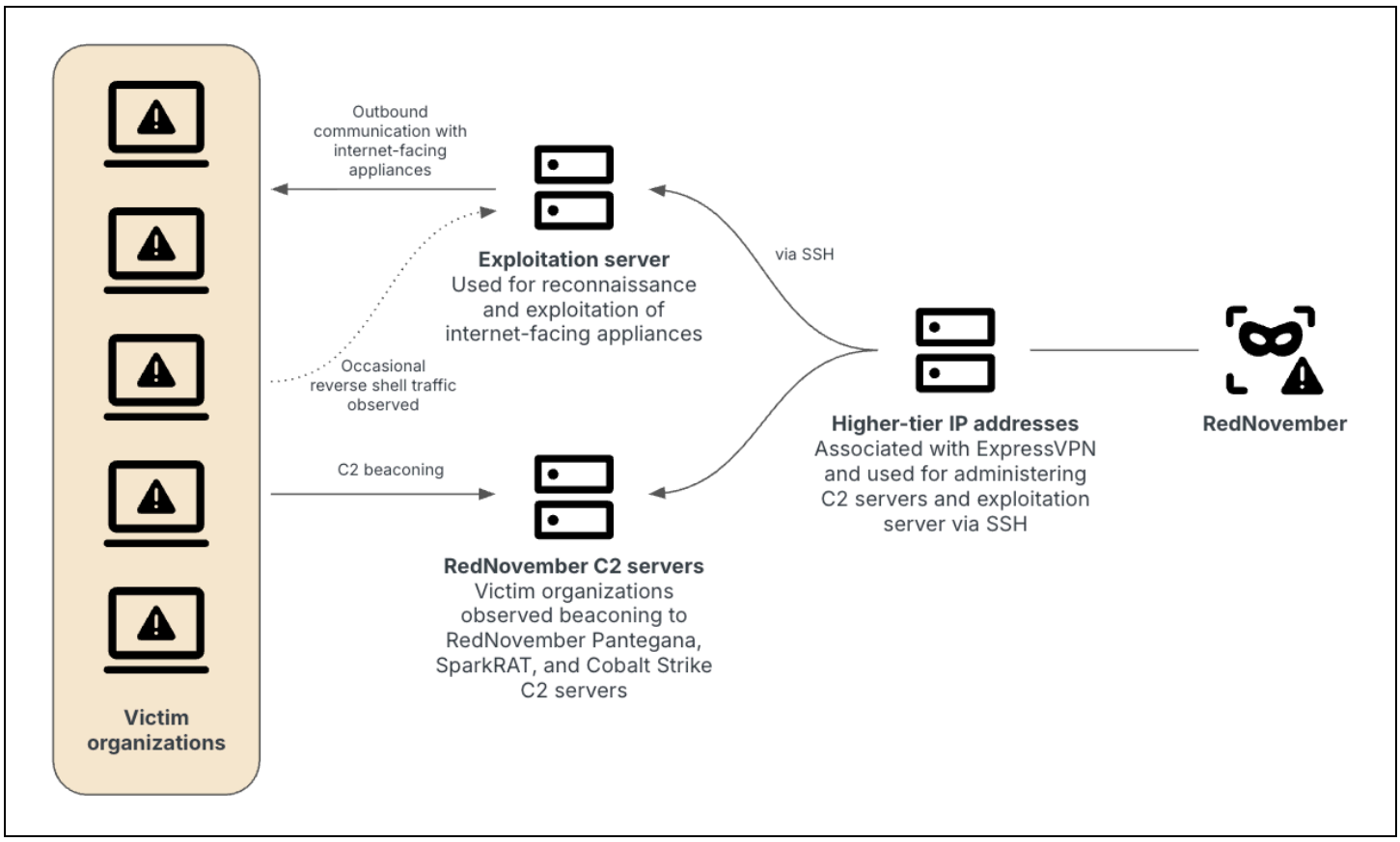


Figure 1: *Overview of RedNovember operations (Source: Recorded Future)*

While monitoring RedNovember's active C2 servers, Insikt Group observed a number of victims on a global scale across the public and private sectors, but concentrated in the following verticals: aerospace and defense, government, and professional services.

In addition to suspected compromise activity by RedNovember, we observed other network communications between multiple organizations and C2 servers associated with RedNovember, likely reflecting, at a minimum, general browsing activity and potentially reconnaissance efforts by the threat group. While the activity could be indicative of an intent to compromise, in these cases, there is currently insufficient evidence to reach such a conclusion.

The terms "compromise," "targeting," "reconnaissance," and "browsing" are used specifically throughout this report to clarify the kind of activity observed. For example, where we assess that RedNovember compromised an entity, we will use terms such as "compromise" and "victim."

Victimology, Targeting, and Reconnaissance

Between H2 2024 and H2 2025, RedNovember compromised, targeted, and reconnoitered organizations on a global scale. In particular, RedNovember heavily targeted organizations in the US, Taiwan, and South Korea, and, in April 2025, it focused its reconnaissance on over 30 Panamanian government organizations.

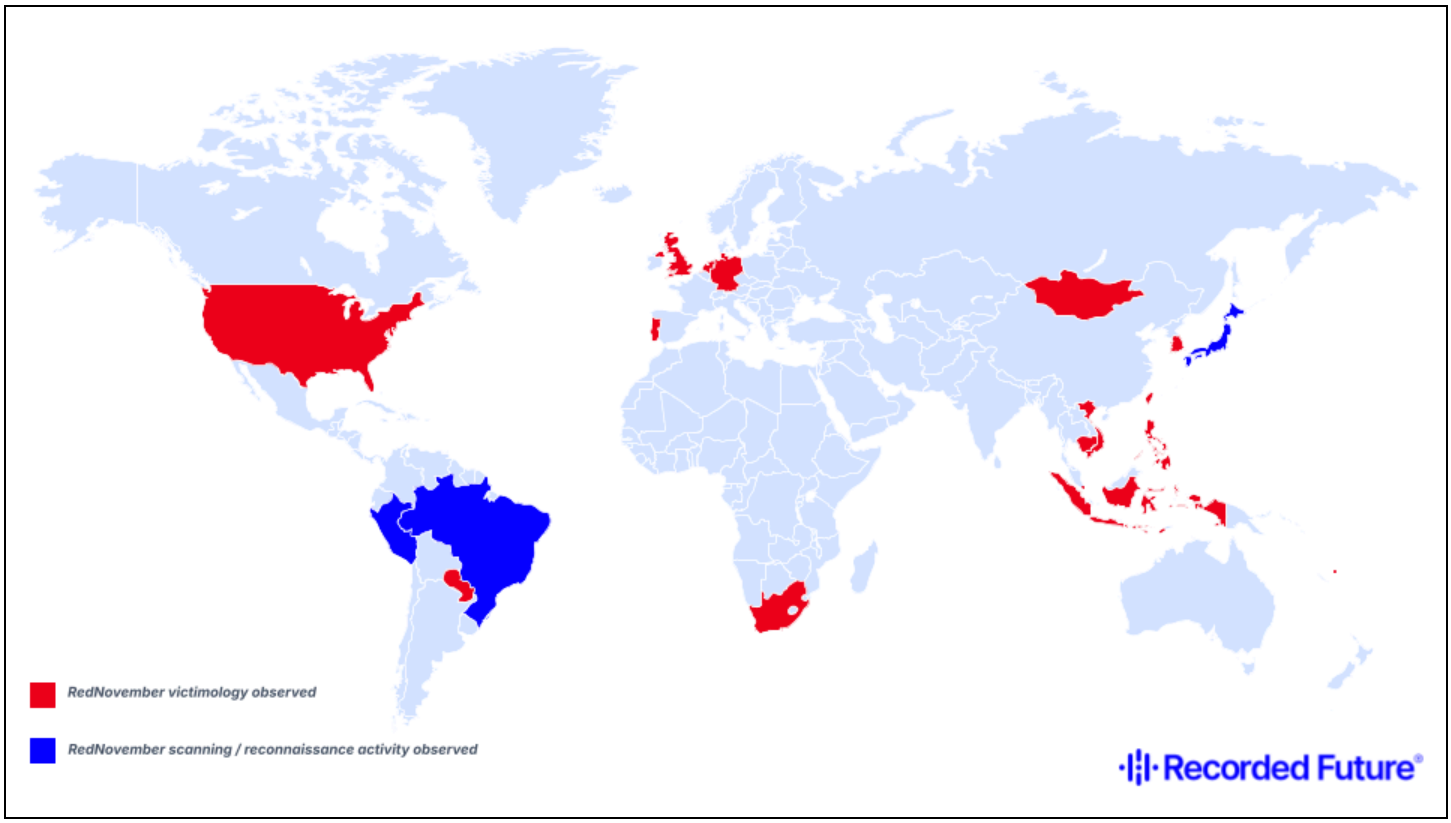


Figure 2: *Mapping of countries with organizations compromised or targeted by RedNovember (Source: Recorded Future)*

Targeting of Government, Intergovernmental, and Diplomatic Entities

RedNovember has targeted government and diplomatic organizations across many countries, as well as intergovernmental organizations. Insikt Group has identified the likely targeting of Outlook Web Access (OWA) portals belonging to a South American country prior to that country's state visit to China. Similar RedNovember activity has been observed targeting OWA portals belonging to ministries of foreign affairs in Southeast Asia and South America.

Since at least mid-2024, RedNovember has highly likely compromised the following targets:

- A 3CX web client instance associated with the ministry responsible for museums in a western European country
- A Zimbra Collaboration Suite server associated with the office of the president of a Southeast Asian country
- A Fortinet FortiGate appliance likely associated with the foreign affairs ministry of an East Asian country
- A Huawei router likely associated with a Southeast Asian government
- An African government's Cisco ASA appliance

Insikt Group also observed communications suggesting a long-running compromise of an intergovernmental organization based in Southeast Asia at least up until March 2025. Other Chinese state-sponsored threat actors, including RedDelta, have previously targeted official intergovernmental organizations in Southeast Asia, likely for the purposes of espionage. Additionally, in March and April 2025, Insikt Group observed evidence suggesting the likely compromise of an additional intergovernmental organization based in Southeast Asia.

Taiwan

Between December 9, 2024, and December 16, 2024, Insikt Group observed browsing and reconnaissance activity from a RedNovember malicious server, *198[.]98[.]50[.]218*, to a location in Taiwan that is home to a Taiwan Air Force military airbase and is also a primary location for semiconductor research and development. On December 9, 2024, China conducted a surprise military exercise around Taiwan, which involved around 90 warships and coast guard vessels and included simulating attacks on foreign ships and practicing the blockading of sea routes. The same server, 198[.]98[.]50[.]218, was also observed hosting a Pantegana C2.

In April 2025, RedNovember also conducted reconnaissance against infrastructure associated with two national scientific research organizations in Taiwan, including one focusing on research and development work related to semiconductors.

South Korea

Insikt Group first observed RedNovember targeting South Korea in late August 2024. Between late August 2024 and March 2025, RedNovember likely compromised a Korean nonprofit organization in the financial services sector. The organization was observed communicating with several of the threat group's Pantegana C2 servers.

Korean organizations were also targeted as part of RedNovember's April 2025 exploitation wave against Ivanti Connect Secure (ICS) VPN devices, such as when Insikt Group observed targeting of a nuclear safety-related organization in South Korea funded by the Korean government. RedNovember also conducted reconnaissance against ICS VPN appliances on a Korean telecommunications company, a Korean marine vessel classification organization, and a Korean national research university.

Broad Targeting of Panamanian Government Entities

Between April 22 and April 24, 2025, Insikt Group observed a significant effort by RedNovember to scan and likely reconnoiter over 30 Panamanian organizations, the majority of which are related to the Panamanian government. Targeted organizations included Panamanian government bodies focused on finance, international relations, and transportation. The targeting also included several other government ministries, including ones focused on land and economic development and emergency services organizations. Targeted devices included F5 BIG-IP instances, a Zimbra Collaboration Web App, and Fortinet FortiWeb and FortiMail servers.

The timing of the observed reconnaissance closely followed US Defense Secretary Pete Hegseth's visit to Panama in early April 2025, and may have been triggered at least in part by several remarks made by US President Donald Trump during January and February 2025 that suggested US interest in asserting control over the Panama Canal. On April 9, 2025, Secretary Hegseth announced an "expanded partnership" with Panama to counter Chinese influence in the canal. Additionally, in February 2025, following a visit by US Secretary of State Marco Rubio, Panama President José Raúl Mulino announced that the country would formally leave China's flagship foreign development project Belt and Road Initiative (BRI), by not renewing the current Memorandum of Understanding, and that Panama would also review its contracts with Hong Kong firm Hutchison PPC, which currently manages Panama's ports of Balboa and Cristóbal. An agreement on the sale involving the two ports to a consortium led by US investment firm BlackRock and MSC (Mediterranean Shipping Company), set to be signed during the first week of April 2025, had reportedly been delayed under pressure from China.

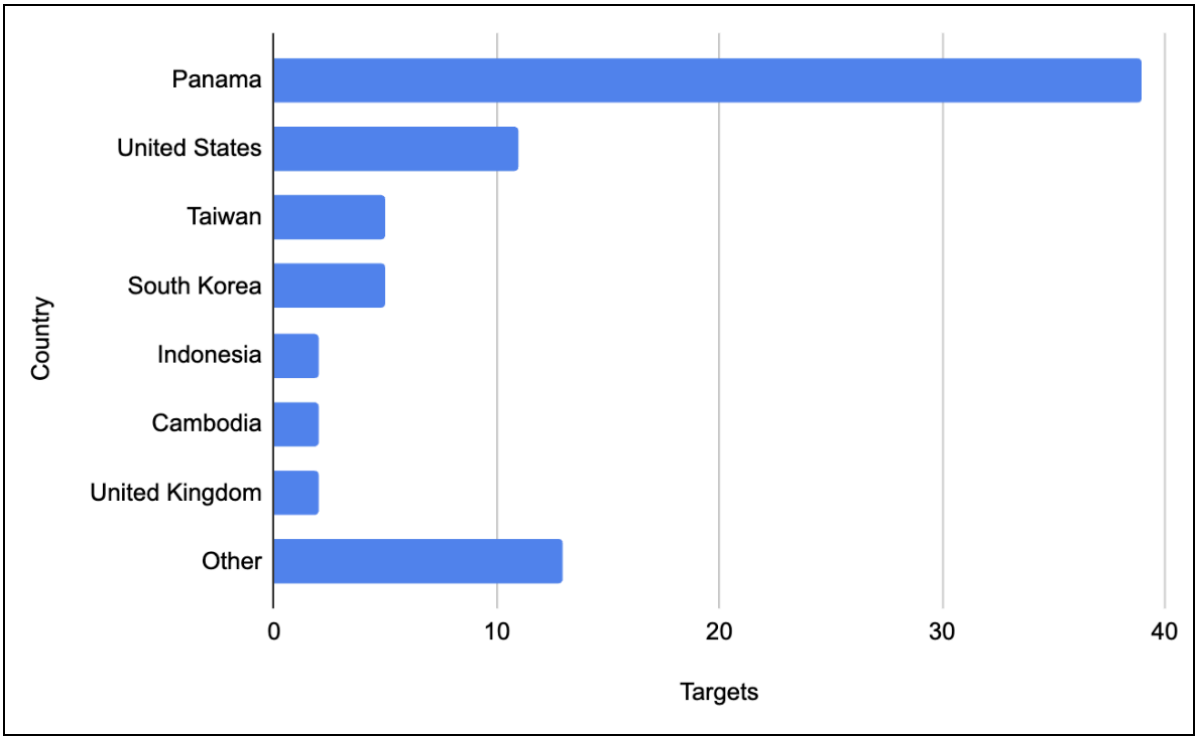


Figure 3: *Breakdown of RedNovember reconnaissance and compromise activity by country between June 2024 and May 2025 (Source: Recorded Future)*

Targeting of US and European Defense and Aerospace Organizations

In July 2024, Insikt Group observed RedNovember conduct a broad reconnaissance campaign exclusively targeting prominent aerospace and defense organizations, with a particular focus on the US. This activity involved suspected port scanning from the RedNovember IP address 209[.]141[.]46[.]57 against these networks. There was no evidence to suggest a successful compromise or exploitation took place against these entities. However, this activity demonstrated that RedNovember was expanding its targeting to include the US DIB and other global defense organizations. In the first half of 2025, Insikt Group has observed further RedNovember reconnaissance activity and compromises targeting this sector.

In April 2025, communications were observed between a RedNovember reconnaissance and vulnerability exploitation server and infrastructure associated with a European space-focused research center.

Moreover, as part of its April 2025 targeting of Ivanti Connect Secure (ICS) VPN devices, RedNovember targeted a specialized US engineering and military contractor. Insikt Group observed direct connections between the same RedNovember reconnaissance and exploitation server and two of the organization's ICS VPN internet-facing endpoints over a period of two days; however, there is currently not sufficient evidence to conclude that RedNovember succeeded in compromising the target.

Also in April 2025, RedNovember conducted extensive reconnaissance against an IP address space associated with a higher education institution associated with the US Navy. Insikt Group did not observe evidence of the organization being compromised.

Targeting of the Private Sector

European Manufacturing Companies

In March 2025, Insikt Group observed a RedNovember reconnaissance and exploitation server being used to target a European engine manufacturer. The same server also hosted a Cobalt Strike C2. The threat group targeted a SonicWall VPN device and login pages for the company's F5 BIG-IP devices and VDI environment.

Additionally, also in March 2025, Insikt Group observed RedNovember-controlled IP address *209[.]141[.]46[.]24* browsing to a SonicWall SonicOS and SonicWall SSL-VPN instance of a United Kingdom (UK)-based company focusing on bespoke cable harnessing, including for aerospace, military and defense, and medical applications.

Law Firms (Globally)

The threat group likely compromised a SonicWall SonicOS and SSL VPN device belonging to an American law firm in April 2025. In March 2025, RedNovember had also targeted IP addresses, including a Palo Alto GlobalProtect Gateway Httpd server, associated with a global law firm that has been involved in a debt restructuring project with a Chinese company.

Taiwanese Technology Companies

Between at least July 2024 and March 2025, RedNovember compromised a Taiwanese IT company, which was observed communicating with the Pantegana C2 IP addresses *209[.]141[.]57[.]116* and *205[.]185[.]126[.]208*. RedNovember has shown particular interest in Taiwanese companies, particularly those related to semiconductors and technology, as well as Taiwanese government bodies related to science.

US Oil and Gas Companies

In April 2025, RedNovember conducted reconnaissance of two American oil and gas companies. Insikt Group had previously publicly reported on RedNovember targeting American utilities organizations in 2024, in the context of a campaign targeting Palo Alto GlobalProtect devices.

Broad Targeting of Fijian Government, Financial, Transportation, and Media Entities

In July 2024, Insikt Group identified a surge in RedNovember activity targeting over 50 Fijian organizations via the actor-controlled IP addresses *209[.]141[.]46[.]57* and *209[.]141[.]47[.]6*. This activity exclusively targeted OWA and Sophos UTM login portals of these organizations. Notable targets included multiple Fijian financial institutions, transportation authorities, media, and government organizations. In particular, the identified targeting of multiple land, sea, and air transportation authorities aligns with ongoing Belt and Road Initiative (BRI) interests within Fiji (1, 2), exemplifying RedNovember activity correlating with Chinese state interests.

Surge Targeting of Edge Devices and Vulnerability Exploitation

RedNovember has repeatedly conducted surge targeting of specific edge devices following the disclosure of vulnerabilities and the publication of PoC exploit code for those same devices. Insikt Group has also observed evidence that the group has targeted the Follina vulnerability (CVE-2022-30190) and a Microsoft Exchange server.

RedNovember has a history of targeting vulnerabilities in edge devices. In April 2024, following the release of a PoC exploit for the Palo Alto Networks GlobalProtect firewall remote code execution (RCE) vulnerability CVE-2024-3400, the group likely conducted reconnaissance and exploitation activity against Palo Alto Networks GlobalProtect appliances associated with American education, finance, legal, local government, and utilities organizations.

Targeting of Ivanti Connect Secure VPN in April 2025

In April 2025, RedNovember conducted a campaign focused on the reconnaissance and targeting of Ivanti Connect Secure (ICS) VPN devices across multiple countries. Specific targets included a major American newspaper, a specialized US engineering and military contractor, and two prominent Korean institutes associated with scientific research and nuclear regulation.

Likely Targeting of Check Point VPN Gateways Following CVE-2024-24919 PoC Publication

From June 3 to June 6, 2024, Insikt Group observed RedNovember IP address *209[.]141[.]47[.]6* communicating with Check Point VPN gateways linked to at least 60 organizations, mainly in Brazil, Germany, Japan, Portugal, the UK, and the US (see **Figure 4**). This activity appeared relatively opportunistic, with minimal themes identified across targeted organizations.

On May 30, 2024, a PoC exploit was published for the arbitrary file read vulnerability CVE-2024-24919 affecting multiple Check Point VPN gateway products, which led to widespread exploitation in the wild by multiple threat actors. While unconfirmed, the timing of the RedNovember activity suggests that the group may have attempted to exploit this vulnerability following the publication of this PoC. Similar behavior by RedNovember was previously noted concerning the targeting of Palo Alto Networks GlobalProtect devices, which closely aligned with the release of a public PoC for the arbitrary file creation vulnerability CVE-2024-3400.

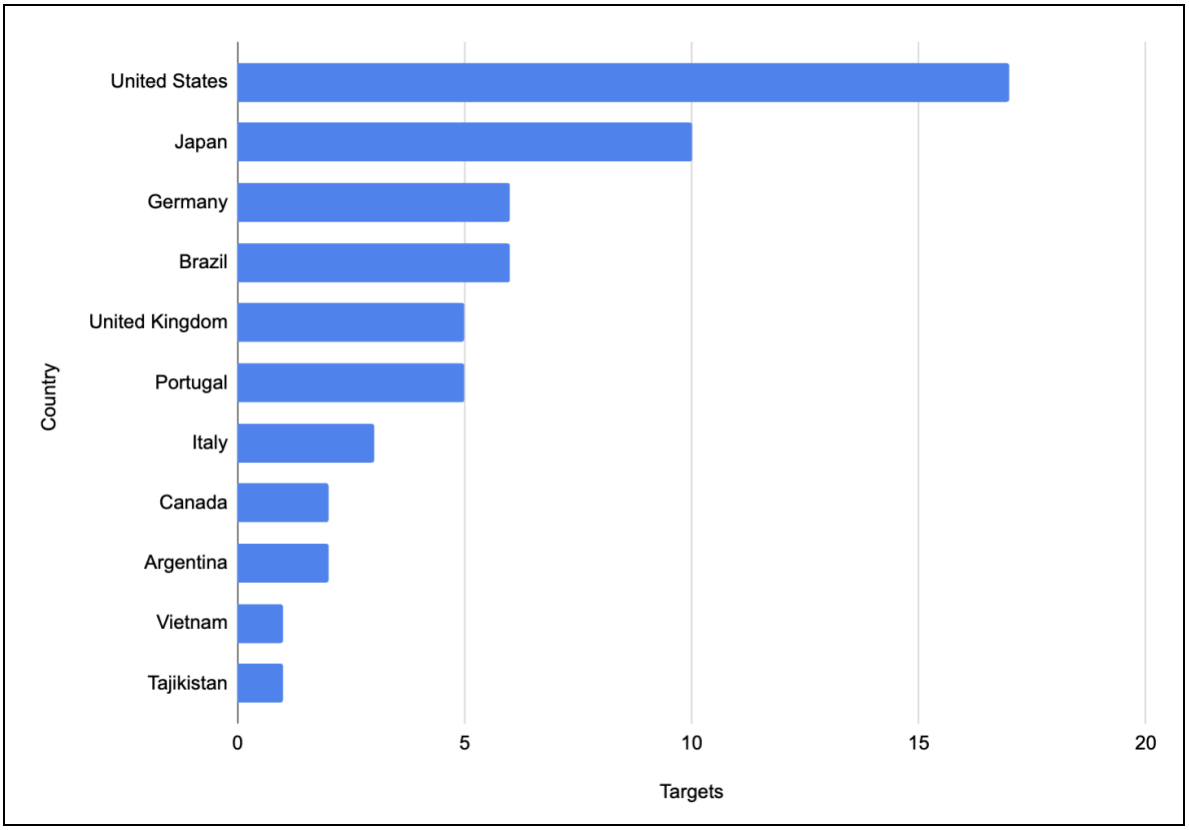


Figure 4: *Breakdown of RedNovember Check Point VPN targeting by country in early June 2024 (Source: Recorded Future)*

Tools Used by RedNovember

LESLIELOADER and SparkRAT

Insikt Group identified two LESLIELOADER samples used by RedNovember to load SparkRAT. The group has previously used a variant of the publicly available Go-based loader LESLIELOADER to load SparkRAT, including in a chain documented by Kroll research in March 2024.

SHA256 Hash	SparkRAT C2 IP Address
8679a25c78e104c6e74996b75882e378f420614fe1379ee9c1e266a11ffa096d	209[.]141[.]46[.]57
06e87a03507213322d876b459194021f876ba90f85c5faa401820954045cd1d2	107[.]189[.]8[.]240

Table 1: *RedNovember LESLIELOADER samples used to load SparkRAT (Source: Recorded Future)*

The 06e87a03507213322d876b459194021f876ba90f85c5faa401820954045cd1d2 sample was first uploaded to a public malware repository within a ZIP file (SHA256: 675874ac8fbe66e76244759ae398a4d30da84ef2435a1384c4be549ca9eba18b), which also contained a PDF lure document (SHA256: 1e37efcd3cd647e6ce5414ae8e353ca690c2d3f7a701a1cc2ec29a4813f5c90b). The PDF lure, which was highly likely delivered via email-based spearphishing, purported to come from the IT department of a US Navy contractor company, and directed targets receiving the file to download and install the LESLIELOADER sample from the threat actor-controlled malicious domain *download[.]offiec[.]us[.]kg*. The LESLIELOADER executable masqueraded as a security patch for VMware software, and its filename included the specific name of the US contractor company being targeted.

LESLIELOADER and Cobalt Strike

In May 2025, Insikt Group identified two additional samples of LESLIELOADER used to load Cobalt Strike Beacon in memory.

SHA256 Hash	Cobalt Strike C2 IP Address
134ed0407956ff1ac59f38e89742e357cc3be565cbaff18b424ed1bcfd130978	47[.]103[.]218[.]35
2bee2cc42322e928bfa0650c5416b14bc0200f2d1156304179d63982baa835dc	

Table 2: *RedNovember LESLIELOADER samples used to load Cobalt Strike (Source: Recorded Future)*

Notably, in this case, the server was hosted in China, specifically on ALIBABA-CN-NET (AS37963), and the Cobalt Strike service was run on TCP port 80.

Additional Malicious Documents

Insikt Group also identified a malicious Word document directing victims to the RedNovember-controlled domain *login[.]offiec[.]us[.]kg* (SHA256: 9a1077f57bac5610d44ac46a8958dd5469522a3db466f164f4dfeada73847b79), specifically to the URL: *hxxps://login[.]offiec[.]us[.]kg/ms-help.html.* The subdomain name "offiec" could be a typosquat reference to the Microsoft Office suite. The file was last modified on August 14, 2024, and was first submitted to a public malware scanner on August 15, 2024. The `ms-help.html` file (SHA256: dba860617762bc713771de351026eb683546b37489fa0359064948f263438030) downloaded by the Word document appears to have been an exploit for the Follina vulnerability (CVE-2022-3019).

Other Potential Tools

Insikt Group has observed RedNovember using multiple file-sharing websites and tools to scan for vulnerabilities.

pan[.]xj[.]hk

In October 2024, Insikt Group observed connections between a RedNovember server and the website *pan[.]xj[.]hk*, an anonymous file-sharing website. This website has been previously highlighted by Mandiant as being used by a suspected China-based threat actor, UNC5266, as part of an exploitation campaign targeting Ivanti devices in 2024. UNC5266 allegedly used the file-sharing website to stage malware payloads and attempted to retrieve them through `curl` and `wget` requests to specific URL paths on the website. Insikt Group does not currently have evidence to substantiate any links between UNC5266 and RedNovember.

Since at least January 23, 2025, and as of July 22, 2025, the domain's landing page displays a Chinese-language message which in translation reads as: "Statement on the abuse of 'pan[.]xj[.]hk' by cyber attackers." The statement acknowledges that recent public reporting has highlighted suspect misuse of the platform by cyber threat actors, stating that it has no connection to such incidents and that it abides by applicable laws and regulations. According to the statement, the platform is temporarily unavailable while work is being conducted to "optimize the download logic and add authentication verification."

Figure 5: *Statement on the pan[.]xj[.]hk main page (Source: urlscan.io)*

PortSwigger

RedNovember browsed to the PortSwigger website on multiple occasions. PortSwigger provides tools for web application security testing and scanning. Its main product, Burp Suite, is widely used by security researchers — and, occasionally, by threat actors — to test and scan web applications for vulnerabilities.

Filemail

RedNovember connected to a dedicated Filemail instance with a domain of *3008[.]filemail[.]com*. Filemail is a cloud-based file transfer service solution that allows users to upload, send, and share large files via email or shareable links.

Acunetix

In at least one instance, a RedNovember Cobalt Strike C2 server ran the vulnerability scanner tool Acunetix, suggesting that the threat group may also be using this tool as part of its reconnaissance activity.

Hacker Target

RedNovember used one of its servers to browse to the *hackertarget[.]com* website in April 2025. Hacker Target provides a free online vulnerability scanner platform with multiple features, including Nmap and ZMap scans and domain and server profiling.

Wayback Machine

In April 2025, RedNovember used at least two of its servers to navigate to the Internet Archive's Wayback Machine. Insikt Group did not have visibility into what the threat group queried in the archive.

Crt[.]sh

Also in April 2025, RedNovember browsed to *crt[.]sh*, a free online TLS certificate transparency service that allows users to look up TLS certificate logs by domain or certificate hash.

Gofile[.]io

Additionally, in April 2025, RedNovember connected to the free cloud storage service *gofile[.]io*, suggesting that the threat actor might have uploaded or browsed files from an account it held on the platform. As highlighted above, RedNovember has previously used similar services, such as the aforementioned *pan[.]xj[.]hk*.

Mitigations

Organizations should take the following measures to detect and mitigate observed TTPs associated with RedNovember activity:

- Detect and block malicious infrastructure such as Pantegana, SparkRAT, and Cobalt Strike C2 servers in real time via the Recorded Future® Threat Intelligence module.
- Recorded Future® Third-Party Intelligence module users can monitor real-time output to identify suspected targeted intrusion activity involving key vendors and partners within physical, network, and software supply chains.
- By monitoring Infrastructure Analysis events, Recorded Future customers can alert on and monitor RedNovember C2 IP addresses.
- By monitoring Malicious Traffic Analysis (MTA), Recorded Future customers can alert on and proactively monitor infrastructure involved in notable communication to known RedNovember C2 IP addresses.
- Ensure a risk-based approach for patching vulnerabilities, prioritizing high-risk vulnerabilities and those exploited in the wild as determined through the Recorded Future® Vulnerability Intelligence module. The public availability of exploit code can substantially increase the likelihood of mass exploitation (1, 2, 3). To specifically protect against some Chinese state-sponsored groups, pay particular attention to remote code execution (RCE) vulnerabilities in external-facing appliances within your environment.
- Configure intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking connection attempts to and from — the external IP addresses and domains linked in **Appendix A**.
- Ensure security monitoring and detection capabilities are in place for all external-facing services and devices. Monitor for follow-on activity likely to occur following exploitation of these external-facing services, such as the deployment of web shells, backdoors, or reverse shells, as well as subsequent lateral movement to internal networks.
- Regularly audit internet-facing and perimeter appliances, and reduce attack surfaces by disabling both internet-facing and internal interfaces or portals where no longer required, and by reducing appliances exposed to the internet to only those that are strictly required.
- Consider logging capabilities and security product support when initially procuring network appliances, in order to be appropriately positioned to detect and respond to threats.
- Practice network segmentation and ensure special protections exist for sensitive information; consider implementing multi-factor authentication and extremely restricted access and storage on systems only accessible via an internal network.
- Focus on defense-in-depth strategies, such as detecting post-exploitation persistence, discovery, and lateral movement activities, as well as unusual network communications. Such strategies can aid detection and response to intrusions arising from the exploitation of both known and zero-day vulnerabilities.

Outlook

RedNovember has historically targeted a diverse range of countries and sectors, suggesting broad and changing intelligence requirements. Some of its activity appears to align with a military affiliation or military-adjacent interests, such as the targeting of specific entities in the US DIB, or the targeting of Taiwan around the time of China's military exercises in Taiwan. However, there are different sets of targeting that do not closely match this pattern: for example, the targeting of law firms, newspaper organizations, and a Christian denomination in the US. Other clusters of RedNovember activity signal a clear interest in foreign governments and foreign policy, such as the targeting of international multilateral organizations based in Southeast Asia and government ministries in several Southeast Asian countries and South American countries, as well as the reconnaissance against dozens of Panamanian government departments in April 2025.

Based on its visibility and collection, Insikt Group has observed that RedNovember's activity to date has primarily focused on several key geographies, including the US, Southeast Asia, the Pacific region, and South America. While targets and victims have also been identified in Europe and at least one in Africa, the overall volume of activity directed toward these areas has been notably lower than that observed in the primary regions of focus.

From a sector perspective, RedNovember continued targeting government organizations in the Pacific Islands, Southeast Asia, and South America, intergovernmental organizations in Southeast Asia, and religious organizations. However, since our first public report on the group, we have also observed RedNovember expand its targeting to defense and aerospace organizations, the private sector, and at least two news outlets.

Insikt Group anticipates that RedNovember, along with other Chinese state-sponsored threat activity groups, will almost certainly continue to target edge devices and exploit vulnerabilities soon after their release.

Appendix A: Indicators of Compromise

Domains:
aeifile[.]offiec[.]us[.]kg
citrix[.]offiec[.]us[.]kg
cna[.]offiec[.]us[.]kg
download[.]offiec[.]us[.]kg
gp[.]offiec[.]us[.]kg
login[.]offiec[.]us[.]kg
test[.]offiec[.]us[.]kg
vpn[.]offiec[.]us[.]kg
vpn1[.]offiec[.]us[.]kg

RedNovember Pantegana C2 IP Addresses:
45[.]61[.]187[.]124
198[.]98[.]50[.]218
198[.]98[.]53[.]163
198[.]98[.]61[.]155
209[.]141[.]37[.]254
205[.]185[.]126[.]208
205[.]185[.]124[.]24
209[.]141[.]42[.]131
209[.]141[.]46[.]83
209[.]141[.]57[.]116

RedNovember Cobalt Strike C2 IP Address:
47[.]103[.]218[.]35

RedNovember Cobalt Strike C2 URLs:
hxxp://47[.]103[.]218[.]35/pixel
hxxp://47[.]103[.]218[.]35/GSjY

LESLIELOADER SHA256 hashes:
06e87a03507213322d876b459194021f876ba90f85c5faa401820954045cd1d2
134ed0407956ff1ac59f38e89742e357cc3be565cbaff18b424ed1bcfd130978
2bee2cc42322e928bfa0650c5416b14bc0200f2d1156304179d63982baa835dc
8679a25c78e104c6e74996b75882e378f420614fe1379ee9c1e266a11ffa096d

ZIP file SHA256 hash:
675874ac8fbe66e76244759ae398a4d30da84ef2435a1384c4be549ca9eba18b

PDF lure SHA256 hash:
1e37efcd3cd647e6ce5414ae8e353ca690c2d3f7a701a1cc2ec29a4813f5c90b

Malicious Follina Word document SHA256 hashes:
9a1077f57bac5610d44ac46a8958dd5469522a3db466f164f4dfeada73847b79
dba860617762bc713771de351026eb683546b37489fa0359064948f263438030

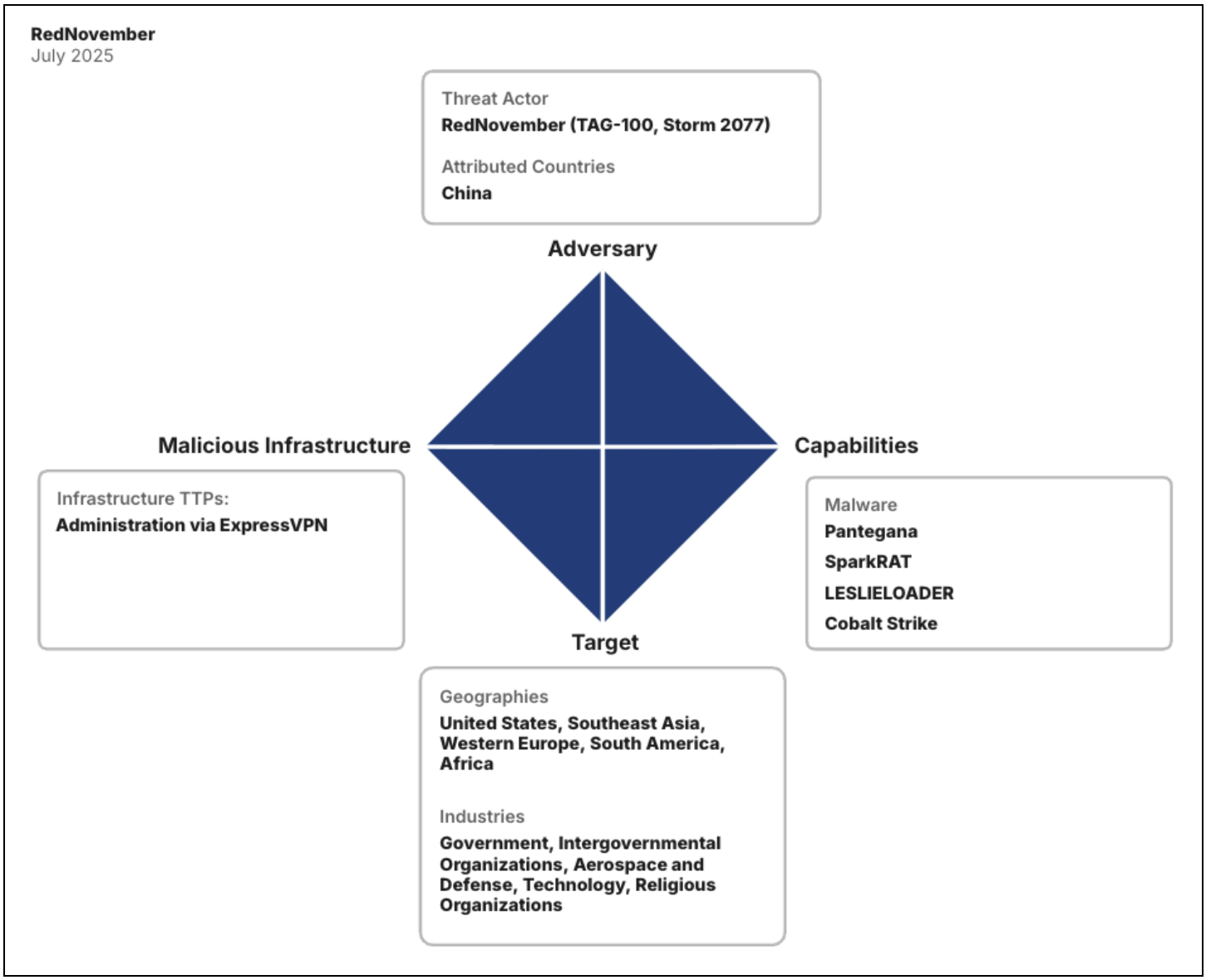
Appendix B: MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Resource Development: Acquire Infrastructure: Virtual Private Server	T1583.003
Reconnaissance: Gather Victim Network Information: Network Security Appliances	T1590.006
Initial Access: Exploit Public-Facing Application	T1190
Initial Access: Spearphishing Attachment	T1566.001
Execution: User Execution: Malicious Link	T1204.001
Execution: User Execution: Malicious File	T1204.002
Command and Control: Application Layer Protocol: Web Protocols	T1071.001
Command and Control: Non-Standard Port	T1571

Appendix C: LESLIELOADER YARA Rule

```
rule MAL_LESLIELOADER {
    meta:
        author = "Insikt Group, Recorded Future"
        date = "2024-11-14"
        description = "Detects LESLIELOADER Malware used by RedNovember"
        version = "1.0"
        hash = "8679a25c78e104c6e74996b75882e378f420614fe1379ee9c1e266a11ffa096d"
        hash = "06e87a03507213322d876b459194021f876ba90f85c5faa401820954045cd1d2"
        malware = "LESLIELOADER"
        malware_id = "u-6JwI"
        category = "MALWARE"
    strings:
        $s1 = ".DecrptogAES"
        $s2 = ".UnPaddingText1"
        // AES key 1
        $k1a = "LeslieCh"
        $k1b = "eungKwok"
        // AES key 2
        $k2a = { 33 44 37 35 45 34 43 39 }
        $k2b = { 42 33 32 41 42 45 31 37 }
    condition:
        uint16be(0) == 0x4d5a
        and all of ($s*)
        and 2 of ($k*)
}
```

Appendix D: RedNovember Diamond Model of Intrusion Analysis



Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com