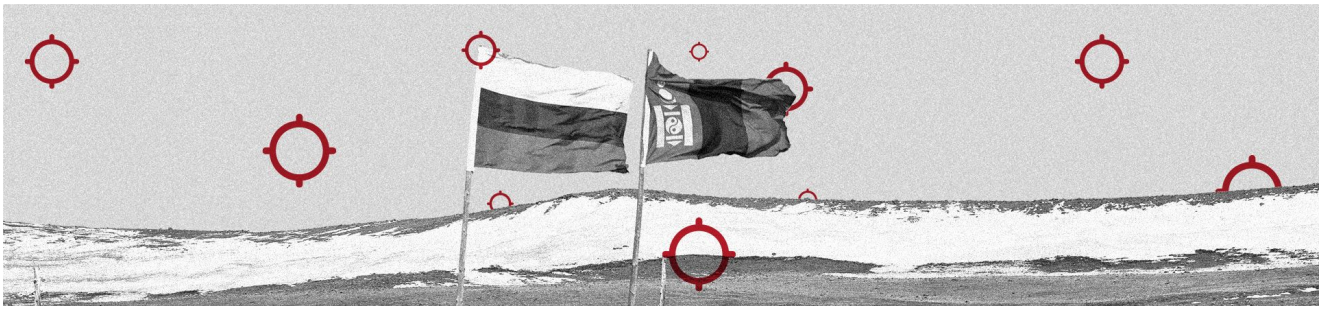
China-linked TA428 Continues to Target Russia and Mongolia IT

recordedfuture.com/china-linked-ta428-threat-group



Insikt Group

Recorded Future's Insikt Group recently identified renewed activity attributed to the suspected Chinese threat activity group TA428. The identified activity overlaps with a TA428 campaign previously reported by Proofpoint as "Operation LagTime IT", which targeted Russian and East Asian government information technology agencies in 2019. Based on the infrastructure, tactics, and victim organization identified, we assess that TA428 likely continues to engage in intrusion activity targeting organizations in Russia and Mongolia.

Infrastructure and Targeting

On January 21, 2021, Insikt Group detected the PlugX C2 server 103.125.219[.]222 (Hosting provider: VPSServer[.]com) hosting multiple domains spoofing various Mongolian news entities. One of the domains, f1news.vzglagtime[.]net, previously appeared in the aforementioned Proofpoint Operation LagTime IT blog. At the time of the Proofpoint blog publication in July 2019, the vzglagtime[.]net domain was hosted on 45.76.211[.]18 through the hosting provider Vultr. According to passive DNS data, this IP address also hosted the Mongolian-themed domains at the same time, further strengthening the overlaps between these unreported suspected TA428 domains and Operation LagTime IT activity. The subdomains appear to spoof familiar news-themed names and words, both in English and in Mongolian languages. Insikt Group also identified two subdomains in this campaign with the term "Bloomberg", a US-based news agency. However, we have no other indication that this campaign targeted US companies. The subdomains in this campaign used familiar terms to lure victims into trusting these sites. These unreported domains include the following:

aircraft.tsagagaar[.]com	Tsag agaar (цаг агаар) is a Mongolian word for "weather"
nubia.tsagagaar[.]com	Likely spoofing New Ulaanbaatar International Airport (NUBIA)
gazar.ecustoms-mn[.]com	Likely spoofing Mongolian e-customs

govi-altai.ecustoms-mn[.]com	References the Govi-Altai region of Mongolia
gogonews.organiccrap[.]com	Likely spoofing Mongolia news agency GoGo News
niigem.olloo-news[.]com	Likely spoofing Mongolian news agency Olloo
oolnewsmongol.ddns[.]info	Likely spoofing Mongolian news-themed domain
bloomberg.mefound[.]com	Additional spoofed news-themed subdomain
bloomberg.ns02[.]biz	Additional spoofed news-themed subdomain

Malware Analysis

Insikt Group identified multiple Royal Road, Poison Ivy, and PlugX samples communicating with the newly identified TA428-linked infrastructure. This closely matches previous reporting by Proofpoint and NTT Security on TA428 activity. In particular, the following PoisonIvy sample was uploaded to a malware multi-scanning source in December 2020: 15ce51dd036231d1ef106cd499c7539e68b195a5b199150a30aa2ba41d3076fb (filename: x64.dll)

1145d39ce42761862eeb7c46500b3fc5cd0dcd9c0fed35623b577b01d0ec3c8e (filename: x86.dll)

The x86.dll is designed for a 32-bit environment and the x64.dll one for a 64-bit environment. Once executed, the DLL file drops two files: PotPlayerMini.exe, a legitimate executable vulnerable to DLL hijacking, and PotPlayer.dll, a PoisonIvy payload. PotPlayerMini.exe is executed to load the malicious PoisonIvy DLL, which in this case is configured to communicate with the C2 domain nubia.tsagagaar[.]com. This PoisonIvy loading sequence directly matches TA428 activity described by NTT Security in October 2020. NTT researchers found that the group used the EternalBlue exploit to move laterally and inject the initial DLL files into the lsass.exe process on the target host.

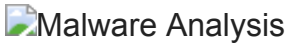


Figure 1: Malware analysis of recent TA428 sample

Insikt Group also identified a malware sandbox upload containing the TA428-linked PoisonIvy sample seen above alongside an EternalBlue exploit tool, the WinEggDrop port scanner, and an MS17-010 scanning tool. The presence of file paths within the upload suggests that the malware was possibly used to target the Russian IT firm ATOL. This victimology also aligns with Operation Lagtime IT activity previously observed, which featured targeting of Russian and East Asian government information technology agencies. Additionally, a blog post by researcher Sebdraven from November 2020 details an additional Royal Road document sample that he attributes to TA428 as a continuation of Operation Lagtime IT. The lure document spoofs the sender as Mongolian authorities and refers to the

conflict between Armenia and Azerbaijan in order to lure the victim to opening the document. According to Sebdraven, the file uses Version 7 of Royal Road RTF weaponizer, which installs a very simple backdoor in memory, rewriting the EQNEDT32.EXE process. After the backdoor gathers initial information on the target machine's disk, running processes, Windows OS version, and user privileges, it attempts to reach out to the command and control (C2) domain custom.songuulcomiss[.]com, which was hosted on the Malaysian IP address 103.106.250[.]239 at the time of discovery.

Attacker Profile

TA428 is a China-linked cyber espionage group identified and named by Proofpoint researchers in 2019, but some overlaps in infrastructure, victimology, and tools indicate that this group may have been active as far back as 2013. TA428 is believed to use custom tool sets and targets organizations of high strategic value to China, including but not limited to IT, scientific research, domestic affairs, foreign affairs, political processes, and financial development. In February 2021, NTT researchers attributed a new campaign to TA428, this time targeting East Asian defense and aviation organizations in Russia and Mongolia with a malware they call nccTrojan, observed between March 2019 and November 2020.

Indicators of Compromise

Indicators of compromise related to this campaign can be found on the Insikt Group GitHub repository here.

C2 IPs

103.125.219[.]222 103.249.87[.]72 45.76.211[.]18

Poison Ivy

1145d39ce42761862eeb7c46500b3fc5cd0dcd9c0fed35623b577b01d0ec3c8e (C2: nubia.tsagagaar[.]com)
15ce51dd036231d1ef106cd499c7539e68b195a5b199150a30aa2ba41d3076fb (C2: nubia.tsagagaar[.]com)
33c0be46fea3a981ae94c1ae0b23c04a763f8318706bd9f7530347f579a2282e (C2: bloomberg.ns02[.]biz)

PlugX

3a5828fe5e55e52f041ad8d67b12a6fc23ec2d2d37a6adde59139d523f1dfc8b (C2: nubia.tsagagaar[.]com)

Royal Road RTF

4f941e1203bf7c1cb3ec93d42792f7f971f8ec923d11017902481ccf42efaf75 (C2: 95.179.131[.]29 - previous hosted multiple vzglagtime[.]net subdomains)

WinEggDrop Port Scanner

13eaf5c0c0a22b09b9dead93c86f085b6c010e3413b0e27c0616896978871048

EternalBlue Exploit Tool

82b0488fd910fe428513813343bf3a9a62c7bf450d509f00f437766cdc0c7aea

MS17-010 Scanner

15585fd878af7d9efd6cac2984cf52371312439797ee2c8f8180ad149e3f8b07

TA428-linked Domains

aircraft.tsagagaar[.]com ecustoms-mn[.]com f1news.vzglagtime[.]net gazar.ecustoms-mn[.]com govi-altai.ecustoms-mn[.]com news.vzglagtime[.]net niigem.olloo-news[.]com nubia.tsagagaar[.]com olloo-news[.]com oolnewsmongol.ddns[.]info bloomberg.mefound[.]com bloomberg.ns02[.]biz nmcustoms.https443[.]org gogonews.organiccrap[.]com tsagagaar[.]com vzglagtime[.]net