To Russia With Love: Assessing a KONNI-Backdoored Suspected Russian Consular Software Installer

medium.com/@DCSO_CyTec/to-russia-with-love-assessing-a-konni-backdoored-suspected-russian-consular-software-installer-ce618ea4b8f3

DCSO CyTec Blog February 21, 2024

DCSO CyTec Blog

--

Earlier this year, DCSO observed an intriguing malware sample first uploaded to VirusTotal in mid-January 2024 that we believe to be part of North Korea-linked activity targeting the Russian Ministry of Foreign Affairs.

The malware itself appears to be KONNI, a North Korea (DPRK) nexus tool believed to have been used since as early as 2014. The use of KONNI in highly similar activity targeting the Russian Ministry of Foreign Affairs was previously observed by various researchers in a 2021 campaign. We have noted that additional researchers have independently uncovered the same upload that we assess in this blogpost and identified it as a KONNI sample.

Perhaps more interestingly, however, the sample was bundled into a backdoored Russian language software installer. This is a KONNI delivery technique that we have previously observed, with a sample from 2023 delivered via a backdoored installer for the publicly available Russian state-mandated tax filing software “Spravki BK” (Справки БК).

In this instance, the backdoored installer appears to be for a tool named “Statistika KZU” (Статистика КЗУ). While we were unable to find any public references to the tool, we suspect on the basis of install paths, file metadata, and user manuals bundled into the installer that the software is intended for internal use within the Russian Ministry of Foreign Affairs (MID), specifically for the relaying of annual report files from overseas consular posts (КЗУ — консульские загранучреждения) to the Consular Department of the MID via a secure channel.

In this blogpost we will assess the backdoored Russian installer and the possible implications thereof, document the functionality of the KONNI variant observed, and fit this finding into the bigger picture of historical DPRK-linked espionage activity and KONNI usage targeting Russian entities.

Blog post authored by , Olivia Hayward, , and

Picture by

The Backdoored Installer

As noted above, the KONNI sample we discovered appears to have been distributed via a backdoored installer for a Russian-language tool named “Statistika KZU” (Статистика КЗУ). In spite of a lack of public references to the tool, a number of data points lead us to believe that Statistika KZU is a tool intended for use within the Russian Ministry of Foreign Affairs (MID), specifically for the relaying of consular statistics to the MID from consulates worldwide. In the section below, we will detail the various data points and findings that led us to reach this conclusion.

The main window of the Statistika KZU GUI

User Manual

Two user manual files were discovered bundled into the backdoored installer detailing the installation and usage of the software. The first one (“Инструкция по установке программы StatRKZU”) explains how to install the “Statistika KZU” program on an administrative account and begin running the software. It includes the minimum software requirements and screenshots detailing the process. The software installer installs the program to its default filepath (C:\ConsulSoft\StatRKZU). On the first login, the manual instructs administrators to use the username “ADMIN” and an empty password, as shown in the image below.

Detailing how to log in to the program for the first time

From there, a window pops up and users select the country they are located in and the consulate that they are working for. The KZU code is provided by the program automatically based on the entered information. The user then provides the name of the head as well as their position.

Filling out information about the user's consulate location when configuring Statistika KZU

In order to begin sending the automatic reports to the MID, users must set up ViPNet, which is a secure, encrypted Russian VPN client and one of the stated software requirements for Statistika KZU. In ViPNet, users set up the automated report sending process, which is already listed as an option within the program. In the image below, the option "Statistical report for KD" is selected within the ViPNet program, with the user in the process of creating a new automatic processing rule.

Setting up the automated reports through ViPNet

The second manual ("StatRKZU_Руководство") is a 22-page user manual for both administrators and operators explaining how to use the software. It also clarifies the purpose of the software, which is to generate annual report files on the consular activities of the KZU and automatically send these via a secure internet channel to the consular department of the MID on the KZU Statistics server as well as print the reports.

It begins the same way as the other document, stating the minimum software requirements and how to log in and set up the program for the first time. From there, it walks through the main window of the software and the purpose of each tab. The screenshot below explains the main window of the program and where information should be tracked and entered.

The manual then details the program functions available to administrators, including: registering users, setting up modules in ViPNet, and saving and restoring databases.

The final section explains how to formulate and print annual reports. In the example below, we can see two of the templates. The first is a template for a table containing the number of registered Russian citizens in the KZU at the beginning of the year and at the end, and the second is the number of Russian citizens detained, arrested, or imprisoned in the territory of the consular district at the beginning of the year and the number at the end.

Structure for a printed statistical report template

Installed Software

We were able to successfully run the installer and use the instructions provided in the manual to access the installed software offline. The UI of the installed program also appeared to correspond fully to the details provided in the manual. We were, however,

unable to test the functionality of the installed software, preventing us from conclusively assessing whether the software is legitimate.

Install Path

The default install path created by the installer lends additional credibility to the notion that the software is intended for use in a consular context:

> \ConsulSoft\StatRKZU\

References to “GosNIIAS” (ГосНИИАС) in MSI File Metadata

Additionally, we noted that an entity named “GosNIIAS” (ГосНИИАС) is listed in the “authors” field of the MSI file’s metadata.

The reference to ГосНИИАС in file metadata

GosNIIAS is an acronym for the State Scientific Research Institute of Aviation Systems (Государственный научно-исследовательский институт авиационных систем), a Russian federal research institute primarily involved in aerospace research and associated projects.

We were unable to find any direct correlations between GosNIIAS and Statistika KZU due to a lack of public references to the software. However, we were able to uncover references to contracts fulfilled by GosNIIAS to provide the MID with various automated consular information services solutions.

Specifically, we were able to uncover a series of public procurement records that list the Russian Ministry of Foreign Affairs (Министерство иностранных дел Российской Федерации) as the customer for single-source contracts fulfilled by GosNIIAS in this area.

Two of the potentially relevant contracts discovered include a procurement order (#0173100002211000012) for software maintenance for the operation of automated systems in the consular department of the MID and a procurement order (#0173100002213000006) for the maintenance of comprehensive system software for protecting personal data during processing on consular systems for the MID. In both of the contracts, the Ministry of Foreign Affairs was listed as the customer and GosNIIAS as the supplier.

The following images were taken from the contracts, the first detailing the services procured from GoSNIIAS by the MID as well as information on the amount in rubles that would be paid for the services.

Information on the services procured from contract #0173100002211000012

The second screenshot shows GosNIIAS as the supplier of the services, as well as the organization’s address, fax phone number, and tax IDs.

Information on the supplier (GosNIIAS) of contract #0173100002213000006

Despite the lack of a specific reference to Statistika KZU, the various contracts reflect the work done by GosNIIAS for the Russian MID in the field of consular department data handling, with the two specific contracts pinpointed above detailing work scoping that could plausibly encompass a software solution such as Statistika KZU.

Other public indications of GosNIIAS involvement in Russian Ministry of Foreign Affairs consular service provision can be found; for example, a public portal for consular service reservation credits GosNIIAS for the development of the site.

GosNIIAS credited for work on a public portal for consular service reservation

The KONNI Malware

Believed to have been used since as early as 2014, KONNI was initially known to only serve as an infostealer. Later versions steadily increased its feature-set up to its apparent peak in 2016 where it offered a variety of stealer functionality (browser data, clipboard, keylogging) in addition to common remote administration capabilities as reported by Talos Intelligence, followed by a sharp reduction of functionality in 2017, and only minimal adjustments since.

Current samples, such as the one observed in this instance, only come with a minimal set of capabilities for file transfers, command execution and configuration of check-in intervals. The tool is tracked under other names, including “UpDog” by Proofpoint.

The malware has generally been associated with use by DPRK nexus actors. The threat actor typically referred to as Konni Group due to its prolific use of the tool, also tracked as TA406, is generally understood to fall under the Kimsuky cluster of DPRK Reconnaissance General Bureau-linked actors. The KONNI malware has also been linked to other actors within the DPRK nexus, including APT37.

Installation

Both installers came in the form of an MSI file with the malware integrated into the benign installation process. When a user runs the backdoored installer, a CustomAction triggers execution of the first stage, which detects the environment (32/64 bit) and selects the appropriate payload. The exact implementation differs for both inspected samples — we have observed a VBScript and a small executable performing the same tasks.

In both cases, another batch file is eventually executed, which is responsible for copying the files and setting up the Windows service for persistence and execution simultaneously, as well as copying the included configuration alongside the payload file.

Final .bat file for both samples

The service name is chosen to be inconspicuous, with “Windows image Acquisition Service” being very similar to an existing, legitimate Windows service.

Configuration

The configuration file copied during the malware installation process contains the C2 servers and is encrypted using AES-CTR, with the service name used as key.

You can grab a script to decrypt such configuration files from our GitHub.

We have extracted the C2s from the present samples — you can find them in the IoC section at the end of the blogpost.

Interestingly, one of the C2 domains we identified was “victory-2024[.]mywebcommunity[.]org.” The consistent use of the word “victory” in various aspects of Konni Group/TA406 activity has been highlighted previously by Proofpoint researchers, who identified it as the HTTP title of the version of the PHP e-mail sending tool Star used by the group as well as in an executable deployed in a campaign suspected to have been undertaken by the group. Researchers noted that the word had also been employed in various passwords by a Kimsuky cluster actor tracked as TA408, an observation corroborated in earlier research published by ESTsecurity.

Particularly interestingly from our standpoint, a late 2021 campaign suspected to have leveraged the KONNI malware to target the Russian MID was identified in public reporting by Lumen researchers in early 2022. While this campaign will be explored in more detail later in this blogpost, we note that a C2 domain identified in this campaign was “”victory-2020.atwebpages[.]com.” This may be indicative of a consistent domain name pattern (victory-yyyy) being employed in campaigns seeking to deploy KONNI against Russian MID targets, though we cannot preclude the use of this domain name pattern in C2 for other campaigns.

Capabilities

KONNI’s recent command set has remained largely unchanged and only permits operators to execute commands and receive their output, upload and download files and specify sleep intervals (connectivity check interval, check in interval). Communication is done via HTTP.

For a check-in, KONNI runs the following commands and sends the output to the C2:

```
systeminfotasklist
```

For file transfers, KONNI checks the extensions against a list of file types it transfers as is. Other file extensions are compressed into a .CAB archive and then sent.

The list of extensions transferred unchanged:

```
.7z.zip.rar.cab.docx.xlsx
```

The Bigger Picture

DPRK nexus cyberespionage targeting sensitive Russian sectors is a long-standing phenomenon. In 2019, for example, Check Point Research stated that they had observed a "coordinated North Korean attack against Russian entities" leveraging known DPRK tooling. In 2020, meanwhile, Russian press reported on Kimsuky cluster activity purportedly impacting targets such as defense conglomerate Rostec.

The discovery, however, comes amidst a broader context of increasing geopolitical proximity between Russia and the DPRK in the aftermath of the former's renewed invasion of Ukraine in 2022, reflected in a high-profile summit between the two countries' leaders in 2023 as well as consistent reports that large-scale transfers of artillery ammunition from the DPRK to Russia had taken place in order to support the latter's ongoing invasion effort, likely in exchange for boons such as technical support in areas of key interest to the DPRK such as its ballistic missile program or natural resource provision.

In spite of this evolving strategic relationship, however, DPRK nexus cyberespionage efforts against Russian targets of interest in sensitive sectors such as government or defense appear to be ongoing. Notably, in late 2023, SentinelLabs published findings from a "leaked email collection" that indicated that Russian missile and rocket engineering bureau NPO Mashinostroyeniya had identified a breach in mid-May 2022 that, according to SentinelLabs researchers, featured several overlaps with known DPRK activity.

Microsoft, meanwhile, has disclosed several additional alleged DPRK-linked incidents that impacted Russian victims in 2023. According to the firm, threat actor Ruby Sleet (CERIUM) purportedly compromised an unnamed Russian aerospace research institute in March 2023. Onyx Sleet (PLUTONIUM), another DPRK-linked group, compromised an unspecified device at a Russian university in the same month. Finally, Opal Sleet (OSMIUM/Konni Group) purportedly targeted Russian diplomatic entities via phishing, also in March 2023.

KONNI deployment against Russian foreign policy targets

Within the context of DPRK nexus cyberespionage targeting Russia, a few data points in recent years have specifically involved KONNI or related tooling in activity that appeared to target Russian foreign policy-relevant targets.

In 2018, Palo Alto Networks researchers detailed a campaign leveraging a KONNI variant that they dubbed NOKKI targeting "politically-motivated victims in Eurasia and possibly Southeast Asia." As part of this campaign, the researchers uncovered a series of samples with Cyrillic contents relevant to Russian political matters. While it remains unclear whether

the Russian MID was the ultimate end-target of this activity, it can plausibly be assessed as representing an early instance of KONNI(-adjacent) deployment against targets in the broader sphere of Russian foreign policy interests.

In a similar vein, Malwarebytes researchers uncovered a campaign in mid-2021 involving the use of KONNI leveraging Russian language lures concerning Russian-Korean trade and economic issues, and a meeting of a Russian-Mongolian intergovernmental commission. While the specific targeting of the campaign remains unclear, the discovery nonetheless constitutes another instance of KONNI deployment being facilitated via Russian-language lures with content relevant to Russian foreign policy interests.

The publicly available data point with perhaps the most explicit relevance to our finding is the late 2021 campaign uncovered by Lumen researchers and Cluster 25 researchers already mentioned earlier in this blogpost, involving very similar TTPs and targeting to our finding. The campaign occurred in multiple stages, leveraging tools such as spoofed MID login portals for credential harvesting, a fake malicious installer for a Russian state-mandated vaccination registration tool, and trojanized screensaver attachments to target MID personnel in a “highly targeted” manner.

Finally, as noted above, Microsoft disclosed a March 2023 case in which an account linked to Konni Group targeted Russian “diplomatic government entities” with phishing e-mails. Further details were not provided concerning this activity.

The sample we uncovered, therefore, appears to fit into an established pattern of KONNI deployment against Russian foreign policy targets, with the 2021 campaign uncovered by Lumen and Cluster25 researchers appearing to be particularly similar in its execution and targeting.

Caveats and Open Questions

A number of caveats and open questions remain concerning this finding.

Is this a legitimate software installer?

We cannot conclusively assess whether the software installer itself is legitimate as we were unable to find corroborating references to the existence of Statistika KZU in the public domain. Additionally, we were unable to test the proper functionality of the tool itself.

It should be noted nonetheless that there are strong indicators in favour of Statistika KZU being a legitimate tool. These include the GosNIIAS contracts for technical consular service provision and the inclusion of complete user manuals in the installer discovered.

Furthermore, as noted previously, we were able to use the instructions provided in the user manual to access the tool offline, and the UI layout post-authentication corresponded to the contents of the user manual, lending further credibility to the notion that the backdoored software installer itself may be legitimate.

If the software or installer are not legitimate, considerable effort would appear to have been invested into giving them the veneer of legitimacy.

If it is a legitimate installer, is it publicly obtainable?

If the software installer is indeed legitimate, the natural follow-on question is whether it is publicly obtainable in any way. Investigation on our part, as noted previously, found no public records concerning Statistika KZU or its installer.

It remains possible, however, that a legitimate Statistika KZU installer may have been acquired by the actors via an unidentified public channel.

If the installer is legitimate but not publicly obtainable, how was it acquired by the attackers for backdooring?

If the software installer is legitimate and was not obtained publicly, the question of how the attackers were able to obtain a sample for backdooring emerges.

We are unable to offer any concrete conclusions in this regard. As noted above, however, KONNI and KONNI-linked activity targeting Russian foreign policy end-targets including the MID has been observed for many years, potentially providing many opportunities for internal tool identification and subsequent acquisition or exfiltration for backdooring purposes.

Final Thoughts

As noted by experts, the public discovery and discussion of so-called “red on red” activity between the DPRK and Russia remains necessarily limited due to fundamental visibility constraints. Given the VirusTotal upload date, this finding would appear to indicate that as of early 2024 such activity remains, at the very least, alive and well.

The attempted use of a backdoored software installer that either is or is masquerading as a tool intended specifically for internal use within the Russian Ministry of Foreign Affairs is likely the most interesting aspect of this finding. Whether legitimate or otherwise, the backdoored installer is indicative in itself of highly specific targeting against the MID by virtue of the stated use-case for Statistika KZU. Such activity is in line with but also an evolution from historical KONNI deployment that also appeared to specifically target the MID and its personnel.

It also indicates that this highly specific targeting of the MID by the DPRK appears to have continued in spite of the increasing recent strategic alignment of the DPRK and Russia, in line with other DPRK threat activity targeting strategically sensitive Russian government and economic sectors. To some extent, this should not come as a surprise; increasing strategic proximity would not be expected to fully overwrite extant DPRK collection needs, with an ongoing need on the part of the DPRK to be able to assess and verify Russian foreign policy planning and objectives.

Some accounts of the origins of the DPRK's cyber program detail the role purportedly played by Russian instructors in the early years of foundational institutions in the program such as the then-Mirim College. Though details remain murky, the possibility remains that this may represent a classic case of the chickens coming home to roost.

Indicators of compromise can be found below; as noted earlier in the blogpost, a script to decrypt KONNI configuration files can be found in our GitHub repository.

IoCs

Samples

```
58bcd90f6f04c005c892267a3dfe91d1154d064482b07715ad5802f57c1ea32d    StatRKZU.msi
9339eaf1d77bb0324e393a08a6180fe0658761fc0cd20ba25081963286dfb9c7    wiasvc32.dll
b60dc12833110098f5eec9a51749d227db7a12d4e91a100a4fd8815695f1093f    wiasvc64.dll
```

```
victory-
2024.mywebcommunity[.]org3cym4ims.medianewsonline[.]comj1p75639.medianewsonline[.]com9
```