CYBER
THREAT
ANALYSIS

CHINA

Recorded Future®

By Insikt Group®

July 29, 2021

“Beijing One Pass” Employee Benefits Software Exhibits Spyware Characteristics

Executive Summary

A Recorded Future client provided information to Insikt Group relating to a potential security incident triggered by a software application called “Beijing One Pass”. This Chinese government-backed application enables access to state benefits information and was downloaded by employees of the Recorded Future client after they were informed that paper copies of the information would no longer be available.

Insikt Group independently verified that the installed application exhibits characteristics consistent with potentially unwanted applications (PUA) and spyware. The software is associated with the Beijing Certificate Authority (北京数字认证股份有限公司), which is a Chinese state-owned enterprise (BJCA, www.bjca[.]cn).

Some notable suspicious behaviors relate to several dropped files and subsequent processes initiated from the primary application. These behaviors include a persistence mechanism, the collection of user data such as screenshots and keystrokes, a backdoor functionality, and other behaviors commonly associated with malicious tools, such as disabling security and backup-related services.

We cannot confirm the intent behind Beijing One Pass’s containing spyware-like capabilities; however, the presence of software with similar spyware-like functionality, developed by at least one other Chinese region, the Shaanxi CA, is notable. These capabilities could be evidence of a deliberate attempt to gain access to devices (such as in support of China’s Cybersecurity Law that allows security organizations to inspect corporate networks remotely), the result of lax security practices by the certificate authorities (CA) and developers, or features designed to comply with Chinese laws and regulations.

Whatever the motive, installing such software on devices that have access to sensitive data is not advised. Recorded Future recommends that companies with China-based employees who need access to state benefit information using “One Pass” software not use it on devices with access to sensitive corporate data.

Analysis

During preliminary analysis, Insikt Group found that the “Beijing One Pass” PC client exhibits behaviors similar to spyware applications. The software contains built-in functionality that, taken in aggregation, raise considerable suspicions about the implication of its data collection capabilities:

- Ability to autorun at Windows startup to ensure persistence
- Checking periodically for human interaction with the operating system as the file is run
- Attempting to read, create, or modify system registry ROOT certificates
- Disabling security and backup services on the host device
- Allowlisting domains for ActiveX use, which potentially allows it to connect to additional internet resources
- Reading data from the clipboard
- Recording screenshots
- Capturing and retrieving keystrokes

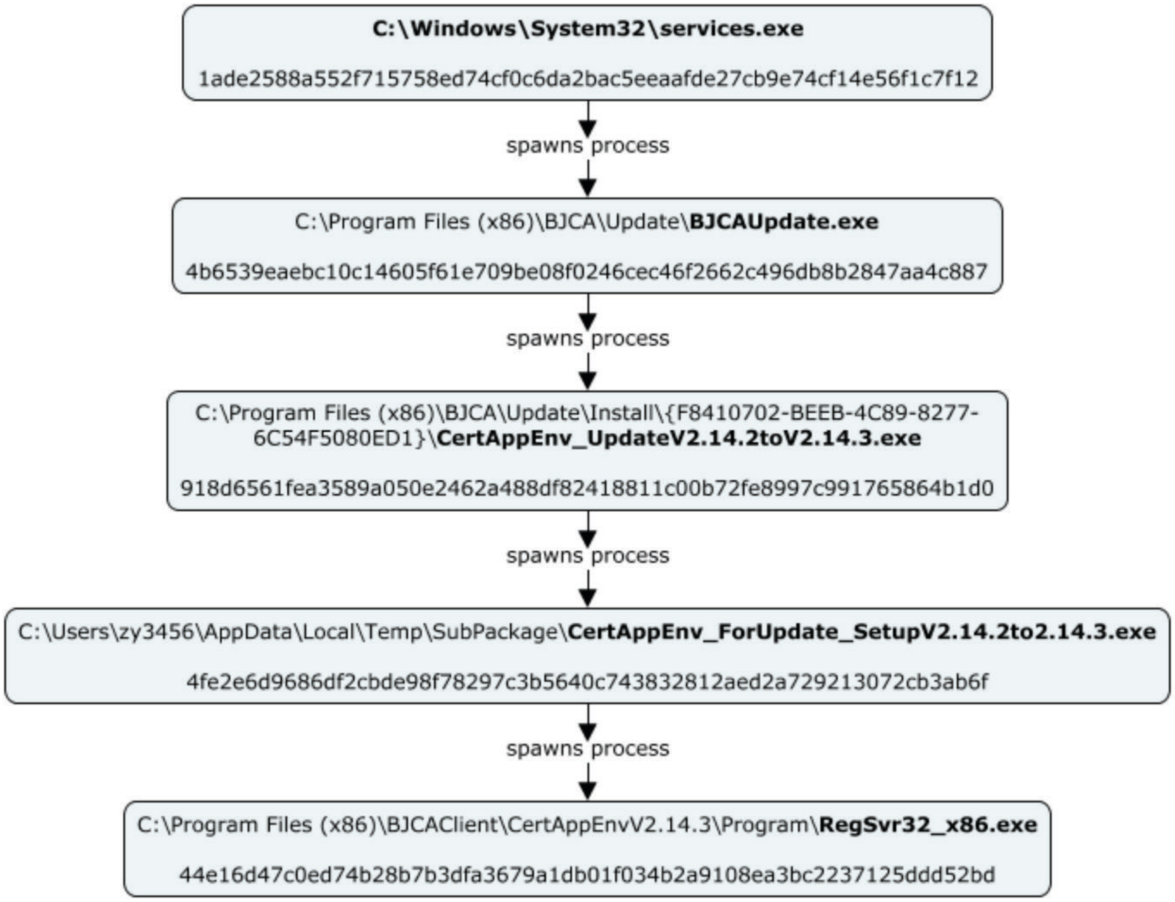
There is also some indication that the file contains backdoor functionality to open a port and listen for incoming connections. This functionality is present in a driver that accompanies the CertAppEnv installation called “wmControl.exe”. We also observed anti-analysis capability within the application, which is typically associated with malware.

Based on data provided by the Recorded Future client, the “Beijing One Pass” application requires the installation of the “Certificate Application Environment” software. This software appears to be developed by the Chinese state-owned enterprise Beijing Certificate Authority (北京数字认证股份有限公司). Upon installation of the One Pass PC client, the subsequent process tree that is spawned is detailed in Figure 1 and was investigated further by Insikt Group analysts.

Stage 1 — Services.exe

The parent process, services.exe, is a benign executable found on Windows machines that launches the Services Control Manager, responsible for starting, interacting with, and ending services. Common processes such as svchost.exe and taskhost.exe are often spawned by services.exe. This particular version of services.exe was first released by Microsoft on April 13, 2021, in a Windows 10 security update (KB5001337), indicating that the One Pass process infection chain may have been adapted since then to include this file as the initial loader.

“Beijing One Pass” Process Tree



C:\Windows\System32\services.exe
1ade2588a552f715758ed74cf0c6da2bac5eeaafde27cb9e74cf14e56f1c7f12
spawns process
C:\Program Files (x86)\BJCA\Update\BJCAUpdate.exe
4b6539eaebc10c14605f61e709be08f0246cec46f2662c496db8b2847aa4c887
spawns process
C:\Program Files (x86)\BJCA\Update\Install\{F8410702-BEEB-4C89-8277-6C54F5080ED1}\CertAppEnv_UpdateV2.14.2toV2.14.3.exe
918d6561fea3589a050e2462a488df82418811c00b72fe8997c991765864b1d0
spawns process
C:\Users\zy3456\AppData\Local\Temp\SubPackage\CertAppEnv_ForUpdate_SetupV2.14.2to2.14.3.exe
4fe2e6d9686df2cbde98f78297c3b5640c743832812aed2a729213072cb3ab6f
spawns process
C:\Program Files (x86)\BJCAClient\CertAppEnvV2.14.3\Program\RegSvr32_x86.exe
44e16d47c0ed74b28b7b3dfa3679a1db01f034b2a9108ea3bc2237125ddd52bd

Figure 1: Investigated process tree for Beijing One Pass application (Source: Recorded Future client)

Stage 2 — BJCAUpdate.exe

BJCAUpdate.exe was spawned from the parent services.exe process, which led to the execution of the subsequent CertAppEnv_UpdateV2.14.2toV2.14.3.exe file that contained PUA-like functionality. BJCAUpdate.exe is detected by several AV engines in a malware multiscanner repository as suspected Boxore adware. The file was first seen in the wild in February 2017 and has been observed with several different file names:

- bjcaupdate.exe
- BJCAUpdate.exe
- lWiOzQzFiNaJbRvUvVtR
- BJCA Update
- BJCACrashHandler.exe
- bjcacrashhandler.exe
- gKARRFUVz.xlsx

The file is signed with a code-signing certificate issued by the Beijing Certificate Authority (BJCA, www.bjca[.]cn). BJCA is a leading provider of information security solutions in China, and one of its key business lines is digital certification services.

Three separate files, all tagged as malicious by AV engine vendors, had also dropped the same BJCAUpdate.exe file previously:

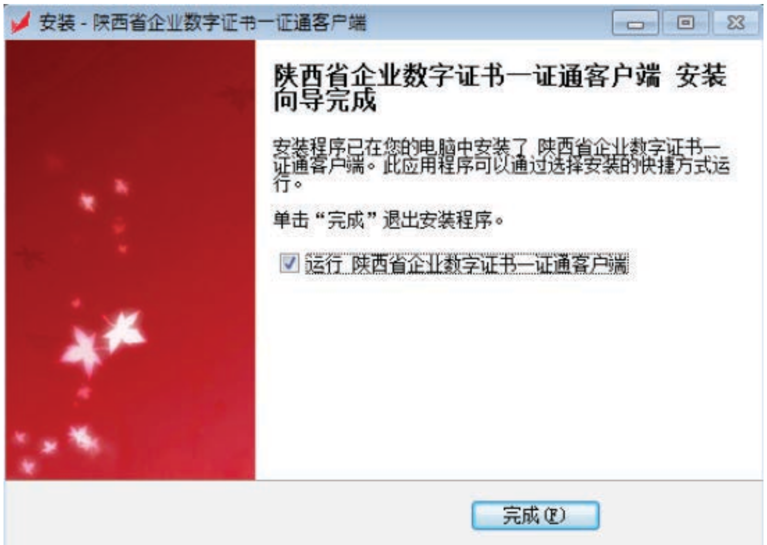
- BJCAUpdateSetup.exe
- Certappenv_setupv3.3.01.19082.exe
- BJCAV2.14.exe

BJCAUpdateSetup.exe, flagged as adware by AV engines, drops several additional temporary files that attempt to call out to update.bjca.org[.]cn, tied to the BJCA certificate authority. Several subdomains associated with bjca.org[.]cn have been flagged in public sandboxing services and open source material as being affiliated with malicious potentially unwanted application (PUA) activity, including in an application called BjTax analyzed by Sophos.

File BJCAV2.14.exe is picked up by Microsoft as a PUA, labeling the file as PUA:Win32/ZfkeyMonitoring. This "ZfkeyMonitoring" signature is likely linked to the "zfkeymonitor.exe" file, which open source information indicates could be a signed loader used to deploy malware onto networks.

Additionally, a file on public malware sandboxing service HybridAnalysis entitled "一证通客户端" ("One Pass Client"), also tagged as "ZFKeyMonitor", has a significant functional overlap with BJCAV2.14.exe. The sandbox report lists 2 hostnames contacted by the application when executed: old.snca[.]com[.]cn and cayzt.snyzt[.]org. A spawned child process file path containing the string "snca.reg" was also observed. These hostnames relate to the Shaanxi Provincial Digital Certificate Certification Center (Shaanxi CA or SNCA for short), an electronic certification service organization established per the "Electronic Signature Law of the People's Republic of China" (《中华人民共和国电子签名法》). The sample calls out to the domain uniplatform[.]snyzt[.]org, which is also linked to the same Shaanxi CA organization, specifically the Shaanxi Enterprise Digital Certificate "One-Pass Client" (陕西省企业数字证书一证通客户端).

The file can read RDP-related keys and open the clipboard and retrieve keystrokes, as well as POST files to a webserver. The filename, "一证通客户端", translates to "One Pass Client", similar to the colloquially named "Beijing One Pass" application that the employees of the Recorded Future client have been asked to install. A child process spawned from "一证通客户端" initiates a further installation — this time, an application called UniClient.exe:


安装 - 陕西省企业数字证书一证通客户端

陕西省企业数字证书一证通客户端 安装向导完成

安装程序已在您的电脑中安装了 陕西省企业数字证书一证通客户端。此应用程序可以通过选择安装的快捷方式运行。

单击"完成"退出安装程序。

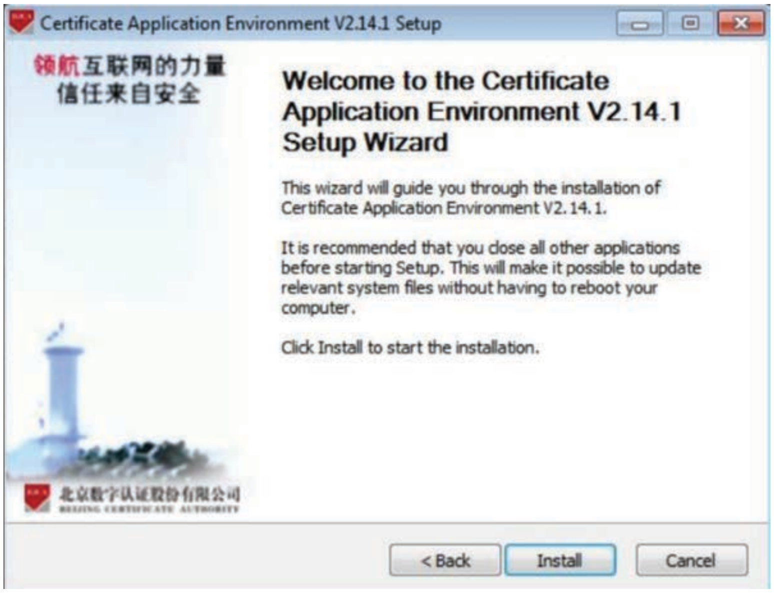
☑ 运行 陕西省企业数字证书一证通客户端

Figure 2: Setup window for UniClient.exe (Source: Hybrid Analysis)

Stage 3 — CertAppEnv_UpdateV2.14.2toV2.14.3.exe

Per client-provided data, "CertAppEnv_UpdateV2.14.2toV2.14.3.exe" was spawned from "BJCAUpdate.exe" and is almost certainly an installer for the "Certificate Application Environment" software developed by BJCA based on a comparison of the filename, functionality, and shared artifacts such as the file import hash (imphash: 7fa974366048f9c551ef45714595665e). AV engines tag this file as malicious in malware multiscanner repositories, specifically as "PUA.ZfkeyMonitoring!8.F694", further indicating "zfkeymonitor.exe" involvement.

Other suspicious characteristics of the process include installing itself to autorun at Windows startup to ensure persistence and checking for human interaction with the operating system as the file is run. The process also attempts to connect to domain time.bjca[.]org[.]cn due to the presence of the BJCA code signing certificate in the file.



Certificate Application Environment V2.14.1 Setup

Welcome to the Certificate Application Environment V2.14.1 Setup Wizard

This wizard will guide you through the installation of Certificate Application Environment V2.14.1.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Install to start the installation.

Figure 3: Setup window for the "Certificate Application Environment V2.14.1" installer (Source: AlienVault OTX)

Pivoting through malware multiscanner repositories, it is clear that there are dozens if not more versions of both "BJCAUpdate.exe" and "CertAppEnv_Update" in circulation. While some appear to be benign based on clean verdicts from AV engines, a significant proportion trigger AV for PUA or spyware applications based on behavioral malware analysis of the files. The varying AV detections for different versions could be due to inconsistent overly restrictive signaturing methods or could indicate that certain functionality was introduced into updated software versions that forced the AV engine detections.

For example, file CertAppEnv_SetupV2.14.1.exe (see Figure 3) is a previous version of the same "Certificate Application Environment" installer that attempted to read, create, or modify system registry ROOT certificates as shown in Table 1, which contributed towards a malicious verdict by malware sandboxing service

Windows Registry Status	Windows Registry Key
Read	HKEY_CURRENT_USER\Local Settings\MuiCache\23\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
Read	HKEY_CURRENT_USER\Local Settings\MuiCache\24\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
Read	HKEY_CURRENT_USER\Local Settings\MuiCache\23\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
Read	HKEY_CURRENT_USER\Local Settings\MuiCache\24\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
Write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\0e7559ecd1a8793fc2f78628328a60bb8b728150\Blob
Write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\81C240D9A20887F3FBE596BB314882E7EE76691A\Blob
Write	HKEY_CURRENT_USER\Local Settings\MuiCache\24\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
Write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\DC3D7D38C1C26CCF6AAA1BA52FB448F5ED3B4431\Blob
Write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\B1BC968BD4F49D622AA89A81F2150152A41D829C\Blob
Write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\DE28F4A4FFE5B92FA3C503D1A349A7F9962A8212\Blob
Write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\A71052B091253A90CA3D423C8A1C0D56E75939AF\Blob
Write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\5070a0e2fa1db04c2ed63461ece36307ab3a863b\Blob
Write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\B4ED58F24E2D40B68DA3BB6D5FD2453BDCF3CAF4\Blob
Write	HKEY_CURRENT_USER\Local Settings\MuiCache\24\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
Write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\EC98F4A5096282FB192FFB168A574236C5A7DC6C\Blob

Table 1: Read and write actions conducted on Windows Registry ROOT certificates upon installation of "Certificate Application Environment V2.14.1 (Source: Alienvault OTX)

Stage 4 — CertAppEnv_ForUpdate_SetupV2.14.2toV2.14.3.exe

The child process "CertAppEnv_ForUpdate_SetupV2.14.2toV2.14.3.exe" is spawned by CertAppEnv_UpdateV2.14.2toV2.14.3.exe and exhibits malicious properties such as backdoor functionality and keystroke capture.

First, the file attempts to disable security and backup-related services on the host device. It then allowlists domains for ActiveX use, which potentially allows it to connect to additional internet resources. Despite the vast reduction in support for ActiveX controls due to a proliferation of related application abuse, it is still an optional extension available for Google Chrome, and Microsoft continues to include it within Internet Explorer 11 while promoting Microsoft Edge as its primary browser.

Second, the file contains functionality to open a port and listen to incoming connections, typically associated with backdoor capabilities. This is present in a driver that accompanies the CertAppEnv installation called "wmControl.exe".

The application can also read data from the clipboard, record screenshots, and capture and retrieve keystrokes. This behavior is considered suspicious for a benefits software application. Finally, the application has some anti-analysis capabilities, which are typically associated with malware. The dropped executable file also contains functionality to detect sandboxes, such as checking for mouse cursor movement or introducing arbitrary sleep commands to hinder dynamic analysis.

Stage 5 — RegSvr32_x86.exe

Both RegSvr32_x86.exe and RegSvr32_x64.exe are dropped by the "CertAppEnv_ForUpdate_SetupV2.14.2to2.14.3.exe" process. The 2 files were created within 8 seconds of each other, shared the same contained resource hashes, and were configured with identical code signing certificates named "北京数字认证股份有限公司" (serial number: 11 21 8E A9 71 3D BB AE 32 7B 49 15 AA 3D 7F CD 15 81), which strongly points to them being closely-linked, renamed versions of the Windows command-line utility RegSvr32. RegSvr32 is typically used to register and unregister DLLs and ActiveX controls in the Windows Registry. Renaming this utility is a red flag in most instances, as this technique can be employed to bypass application controls on a host operating system or hide the utility. The locations of the 2 renamed RegSvr32 instances are as follows:

- C:\Program Files (x86)\BJCAClient\CertAppEnvV2.14.3\BjcaCertAide\RegSvr32_x86.exe
- C:\Program Files (x86)\BJCAClient\CertAppEnvV2.14.3\Program\RegSvr32_x64.exe

Outlook

It remains to be seen if this new policy change is corroborated by other international companies based in China, but the potential ramifications of having employees install state-backed software that exhibits spyware-type characteristics raise concern.

Given the exceptional circumstances brought about by the COVID-19 pandemic and the need for governments to devise new policy and benefit programs to support their citizens during lockdowns, introducing digital platforms to manage state benefits is a reasonable step to reduce inefficiencies. However, Recorded Future's analysis of "Beijing One Pass" and associated software intrinsically tied to Provincial/Municipality certificate authorities in China highlights suspicious spyware-like functionalities that include a persistence mechanism, collection of user data such as screenshots and keystrokes, backdoor functionality, and other behaviors commonly associated with malicious tools, such as disabling security and backup-related services.

While we cannot confirm the intent behind Beijing One Pass containing spyware-like capabilities, installing such software on devices that have access to sensitive data is not advised. Recorded Future recommends that companies with China-based employees who need access to state benefit information using "One Pass" software not use it on devices with access to sensitive corporate data.

Appendix A — Indicators

Host Indicators

```
SHA256: 1ade2588a552f715758ed74cf0c6da2bac5eeaafde27cb9e74cf14e56f1c7f12 - services.exe
SHA256: 4b6539eaebc10c14605f61e709be08f0246cec46f2662c496db8b2847aa4c887 - BJCAUpdate.exe
SHA256: 918d6561fea3589a050e2462a488df82418811c00b72fe8997c991765864b1d0 - CertAppEnv_UpdateV2.14.2toV2.14.3.exe

SHA256: 4fe2e6d9686df2cbde98f78297c3b5640c743832812aed2a729213072cb3ab6f - CertAppEnv_ForUpdate_SetupV2.14.2to2.14.3.exe

SHA256: 44e16d47c0ed74b28b7b3dfa3679a1db01f034b2a9108ea3bc2237125ddd52bd - RegSvr32_x86.exe

SHA256: D9c3f00e4351fff1aba9e72b320dbecdbcb001f553ba3ce3401e7c6f1a471469 - CertAppEnv_SetupV2.14.1.exe

SHA256: 6DC9413628655092E93EBE970C8A9E4D2CBD07B69B5B18BBD483508BB96AA7B3 - RegSvr32_x64.exe

SHA256: 1c03f092ea658270e295806ec1c07c84e12e4520b4344eb60aeeb6ae227fe8c4 - BJCAUpdateSetup.exe

SHA256: edfad91d7587e6206459db71205c23869ac028c429b24d359ee75c85cfd7f713 - BJCAV2.14.exe

SHA256: bed0d1139adcec9292841b7315289bb43960f2c7a4ff1bbab536528b1317b075 - Certappenv_setupv3.3.01.19082.exe

SHA256: a94d56067aa15f28f66a139eecc90e49b008bfa1f0faf7d65721ecfb68a6a6a2 - “一证通客户端” - ZFKeyMonitor

HKEY_CURRENT_USER\Local Settings\MuiCache\23\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
HKEY_CURRENT_USER\Local Settings\MuiCache\24\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
HKEY_CURRENT_USER\Local Settings\MuiCache\23\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
HKEY_CURRENT_USER\Local Settings\MuiCache\24\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\0e7559ecd1a8793fc2f78628328a60bb8b728150\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\81C240D9A20887F3FBE596BB314882E7EE76691A\Blob
HKEY_CURRENT_USER\Local Settings\MuiCache\24\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\DC3D7D38C1C26CCF6AAA1BA52FB448F5ED3B4431\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\B1BC968BD4F49D622AA89A81F2150152A41D829C\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\DE28F4A4FFE5B92FA3C503D1A349A7F9962A8212\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\A71052B091253A90CA3D423C8A1C0D56E75939AF\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\5070a0e2fa1db04c2ed63461ece36307ab3a863b\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\B4ED58F24E2D40B68DA3BB6D5FD2453BDCF3CAF4\Blob
HKEY_CURRENT_USER\Local Settings\MuiCache\24\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\EC98F4A5096282FB192FFB168A574236C5A7DC6C\Blob
```

Network Indicators

```
update[.]bjca[.]org[.]cn
bjca[.]org[.]cn
time[.]bjca[.]org[.]cn
old[.]snca[.]com[.]cn
cayzt[.]snyzt[.]org
```

Recorded Future Threat Activity Group and Malware Taxonomy

Recorded Future's research group, Insikt, tracks threat actors and their activity, focusing on state actors from China, Iran, Russia, and North Korea, as well as cybercriminals — individuals and groups — from Russia, CIS states, China, Iran, and Brazil. We emphasize tracking activity groups and where possible, attributing them to nation state government, organizations, or affiliate institutions.

Our coverage includes:

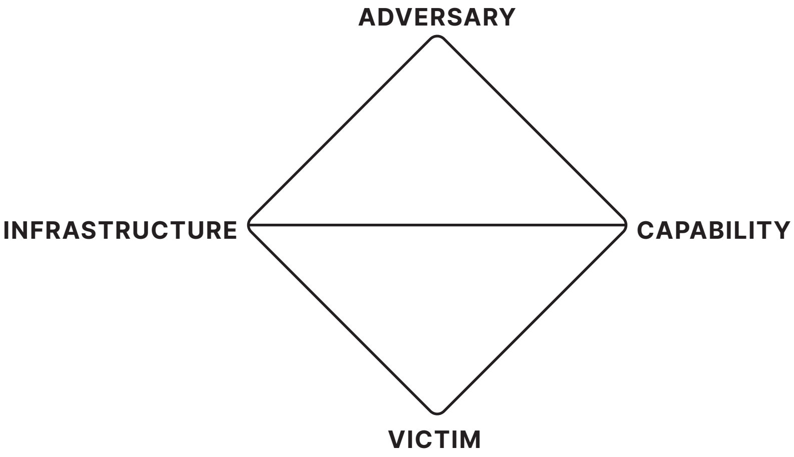
- Government organizations and intelligence agencies, their associated laboratories, partners, industry collaborators, proxy entities, and individual threat actors
- Recorded Future-identified, suspected nation-state activity groups, such as RedAlpha, RedBravo, Red Delta, and BlueAlpha and many other industry established groups
- Cybercriminal individuals and groups established and named by Recorded Future
- Newly emerging malware, as well as prolific, persistent commodity malware

Insikt Group publicly names a new threat activity group or campaign, such as RedFoxtrot, when analysts typically have data corresponding to at least three points on the Diamond Model of Intrusion Analysis with at least medium confidence. We will occasionally report on significant activity using a temporary activity clustering name such as TAG-21 where the activity is new and significant but doesn't map to existing groupings and hasn't yet graduated or merged into an established activity group. We tie this to a threat actor only when we can point to a handle, persona, person, or organization responsible. We will write about the activity as a campaign in the absence of this level of adversary data. We use the most widely used or recognized name for a particular group when the public body of empirical evidence is clear the activity corresponds to a known group.

Insikt Group uses a simple color and phonetic alphabet naming convention for new nation-state threat actor groups or campaigns. The color generally corresponds to that nation's flag colors, with more color/nation pairings to be added as we identify and attribute new threat actor groups associated with new nations.

For newly identified cybercriminal groups, Insikt Group uses a naming convention corresponding to the Greek alphabet. Where we have identified a criminal entity connected to a particular country, we will use the appropriate country color, and where that group may be tied to a specific government organization, tie it to that entity specifically.

Insikt Group uses mathematical terms when naming newly identified malware.



Cn
CHINA
Ir
IRAN
Nk
NORTH KOREA
Ru
RUSSIA

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.