BRONZE PRESIDENT Targets Russian Speakers with Updated PlugX

secureworks.com/blog/bronze-president-targets-russian-speakers-with-updated-plugx

Counter Threat Unit Research Team

The threat group's targeting shift could reflect a change in China's intelligence collection requirements due to the war in Ukraine. Wednesday, April 27, 2022 *By: Counter Threat Unit Research Team*

Government-sponsored threat actors collect intelligence to benefit their country, and changes to the political landscape can impact the collection requirements. The war in Ukraine has prompted many countries to deploy their cyber capabilities to gain insight about global events, political machinations, and motivations. This desire for situational awareness often extends to collecting intelligence from allies and "friends," which could explain why Secureworks® Counter Threat Unit™ (CTU) researchers detected what appears to be an attempt by China to deploy advanced malware to computer systems of Russian officials.

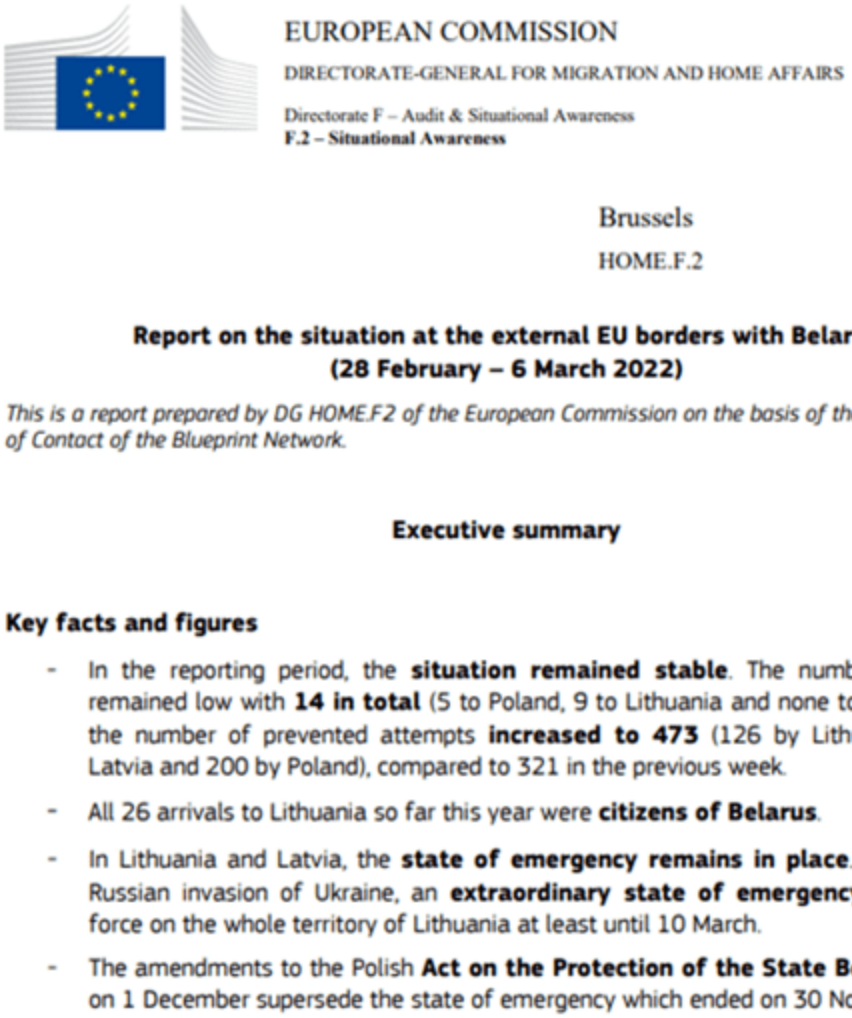
In March 2022, CTU™ researchers analyzed a malicious executable file masquerading as a Russian-language document. The filename is Благовещенск - Благовещенский пограничный отряд.exe ("Blagoveshchensk - Blagoveshchensk Border Detachment.exe"), but the default settings on Windows system do not display the .exe file extension. The file uses a portable document file (PDF) icon for credibility. Blagoveshchensk is a Russian city close to the China border and is home to the 56th Blagoveshchenskiy Red Banner Border Guard Detachment. This connection suggests that the filename was chosen to target officials or military personnel familiar with the region.

The heavily obfuscated executable file downloads additional files from a staging server at 107 . 178 . 71 . 211 (see Table 1).

Target file on staging server	Comment
http: //107 . 178 . 71 . 211/eu/Report.pdf	Decoy document
http: //107 . 178 . 71 . 211/eu/FontEDL.exe	Legitimate signed file
http: //107 . 178 . 71 . 211/eu/DocConvDll.dll	Malicious DLL loader
http: //107 . 178 . 71 . 211/eu/FontLog.dat	Encrypted payload (likely PlugX)

Table 1. Files downloaded from staging server.

The executable file displays the decoy document (see Figure 1) to the victim. This document is written in English and appears to be legitimate, although CTU researchers were unable to locate the original source. It describes the migratory pressure and asylum applications in countries that border Belarus (Lithuania, Latvia, and Poland) and discusses European Union (EU) sanctions against Belarus at the beginning of March 2022. CTU researchers are unclear why a file with a Russian filename downloads an English-language document.



EUROPEAN COMMISSION

DIRECTORATE-GENERAL FOR MIGRATION AND HOME AFFAIRS

Directorate F – Audit & Situational Awareness
F.2 – Situational Awareness

Brussels

HOME.F.2

Report on the situation at the external EU borders with Belarus
(28 February – 6 March 2022)

This is a report prepared by DG HOME.F.2 of the European Commission on the basis of the input of Points of Contact of the Blueprint Network.

Executive summary

Key facts and figures

- In the reporting period, the **situation remained stable**. The number of arrivals remained low with **14 in total** (5 to Poland, 9 to Lithuania and none to Latvia), while the number of prevented attempts **increased to 473** (126 by Lithuania, 147 by Latvia and 200 by Poland), compared to 321 in the previous week.
- All 26 arrivals to Lithuania so far this year were **citizens of Belarus**.
- In Lithuania and Latvia, the **state of emergency remains in place**. Following the Russian invasion of Ukraine, an **extraordinary state of emergency** entered into force on the whole territory of Lithuania at least until 10 March.
- The amendments to the Polish **Act on the Protection of the State Border** adopted on 1 December supersede the state of emergency which ended on 30 November.

Figure 1. Decoy document displayed to victims. (Source: Secureworks)

The other three files downloaded from the staging server are typical of the China-based BRONZE PRESIDENT threat group's use of DLL search order hijacking to execute PlugX malware payloads. The inclusion of the ping command with the "-n 70" option (see Figure 2) adds a significant delay before executing the legitimate signed file. The IP address used for the ping command is Google's public DNS service.

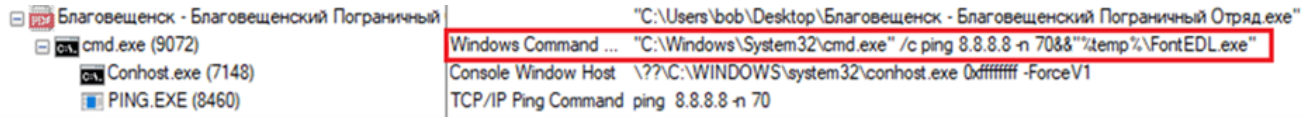


Figure 2. Using ping command to incorporate delay. (Source: Secureworks)

The legitimate signed file originates from UK-based Global Graphics Software Ltd. Because it is vulnerable to DLL search order hijack, it imports the malicious DocConvDll.dll DLL loader. This DLL exports eight functions, several of which use seemingly random names and contain no useful instructions. The only export called by the parent executable is createSystemFontsUsingEDL (see Figure 3).

ordinal	name (8)	location
1	CreatePotPlayerExW	.text:100075B0
2	RunPotPlayer	.text:100075B0
3	akxefyfhxtjnmjbbxpxxtxfxibqcsxwyubssjpatm	.text:100024D7
4	createSystemFontsUsingEDL	.text:100075B1
5	lxwjfnxhbtxreqjqu	.text:100075B0
6	lykidpphnoxostcgyaddu	.text:100075B0
7	nxssxsakvumsxpecxwxlgmcu	.text:100075B0
8	sxpgrjecsoaomwvfusdkrkltidpgpoiypvlacxebip	.text:10002410

Figure 3. Exported functions of DocConvDll.dll. (Source: Secureworks)

The createSystemFontsUsingEDL function loads, decrypts, and executes FontLog.dat. The .dat sample obtained by CTU researchers was corrupt, but based on similar campaigns the file is likely a PlugX payload. However, analysis of the loader suggests that the malware creates a directory structure under C:\ProgramData (C:\ProgramData\Fuji Xerox\Fonts\) and then copies the three files that DLL side-load and execute the payload to this directory. Once PlugX is installed, the malware provides access to the compromised host to extract sensitive system information, upload and download files, and execute a remote command shell.

The staging server (107 . 178 . 71 . 211) hosts the zyber-i . com domain. This domain has been implicated in a broad PlugX campaign targeting European diplomatic entities. The domain was hosted on 103 . 107 . 104 . 19 from March 2-13, when it served a similarly named group of files for DLL search order hijack. A third-party report links the campaign to the locvnpt . com domain. Another report associates the locvnpt . com domain with attacks in 2020 against the Vatican that CTU researchers attribute to BRONZE PRESIDENT. This 2020 campaign also used customized decoy documents and downloaded PlugX .dat files that were loaded by DLL search order hijack. The locvnpt . com domain was hosted on 2EZ Networks (IP address 167 . 88 . 177 . 151) in September 2020. BRONZE PRESIDENT extensively used that company's IP range in a 2020 campaign targeting Hong Kong, Myanmar, and Vietnam (see Figure 4).

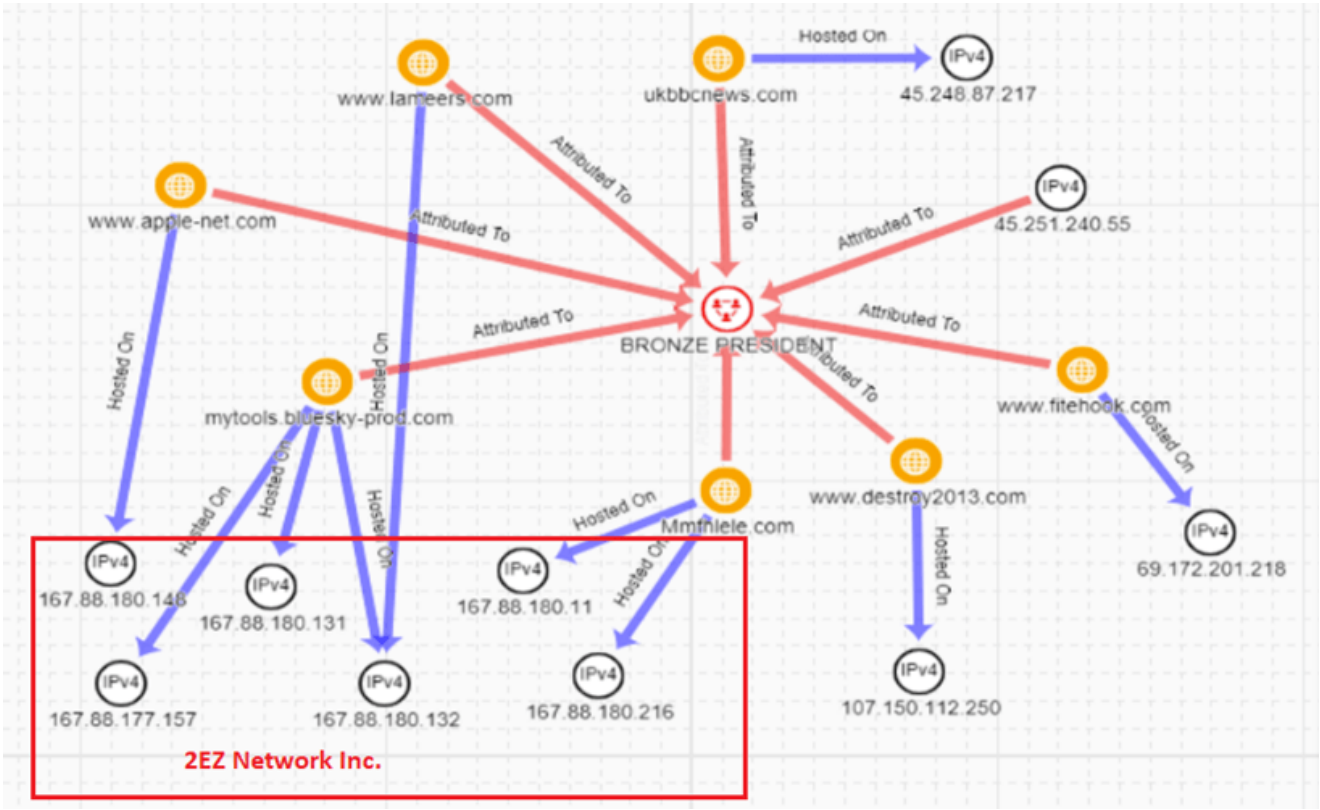


Figure 4. BRONZE PRESIDENT network infrastructure used in 2020 campaign. (Source: Secureworks)

BRONZE PRESIDENT appears to be changing its targeting in response to the political situation in Europe and the war in Ukraine. The threat group has primarily focused on Southeast Asia, gathering political and economic intelligence valuable to the People's Republic of China (PRC). Targeting Russian-speaking users and European entities suggests that the threat actors have received updated tasking that reflects the changing intelligence collection requirements of the PRC.

To mitigate exposure to this malware, CTU researchers recommend that organizations use available controls to review and restrict access using the indicators listed in Table 2. Note that IP addresses can be reallocated. The domains, IP addresses, and URLs may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
b0a7b7a1cb4bf9a1de7f4b1af46ed956	MD5 hash	Malicious Russian-language executable masquerading as PDF, downloads PlugX
937975e3ea50c15476aef050295f4031f5fda2a4	SHA1 hash	Malicious Russian-language executable masquerading as PDF, downloads PlugX

Indicator	Type	Context
dbdbc7ede98fa17c36ea8f0516cc50b138fbe63af 659feb69990cc88bf7df0ad	SHA256 hash	Malicious Russian-language executable masquerading as PDF, downloads PlugX
69ab42012ddce428c73940dcf343910e	MD5 hash	Malicious DLL (DocConvDll.dll) that loads PlugX
698d1ade6defa07fb4e4c12a19ca309957fb9c40	SHA1 hash	Malicious DLL (DocConvDll.dll) that loads PlugX
436d5bf9eba974a6e97f6f5159456c642e53213d7e4 f8c75db5275b66fedd886	SHA256 hash	Malicious DLL (DocConvDll.dll) that loads PlugX
ad3ddb4cbe7ece8cb723f63f3b855b85	MD5 hash	PlugX payload (FontLog.dat)
6856bb506a0858cc5597666d966b5b7499e38542	SHA1 hash	PlugX payload (FontLog.dat)
ca622bdc2b66f0825890d36ec09e6a64e631638f d1792d792cfa02048c27c69f	SHA256 hash	PlugX payload (FontLog.dat)
107.178.71.211	IP address	Staging server that hosted PlugX files
103.107.104.19	IP address	Staging server that hosted PlugX files
zyber-i.com	Domain name	Associated with BRONZE PRESIDENT PlugX activity
locvnpt.com	Doman name	Associated with BRONZE PRESIDENT PlugX activity
http://107.178.71.211/eu/docconvdll.dll	URL	PlugX DLL loader
http://107.178.71.211/eu/fontlog.dat	URL	PlugX payload
92.118.188.78	IP address	PlugX C2 server

Table 2. Indicators for this threat.

Learn more about Secureworks insights regarding the Russia-Ukraine crisis.

If you need urgent assistance with an incident, contact the Secureworks Incident Response team.