Targeted attack on industrial enterprises and public institutions

By Kaspersky ICS CERT

Published: 2022-08-08 · Archived: 2026-04-05 13:43:18 UTC

In January 2022, Kaspersky ICS CERT experts detected a wave of targeted attacks on military industrial complex enterprises and public institutions in several countries. In the course of our research, we were able to identify over a dozen of attacked organizations. The attack targeted industrial plants, design bureaus and research institutes, government agencies, ministries and departments in several East European countries (Belarus, Russia, and Ukraine), as well as Afghanistan.

The attackers were able to penetrate dozens of enterprises and even hijack the IT infrastructure of some, taking control of systems used to manage security solutions.

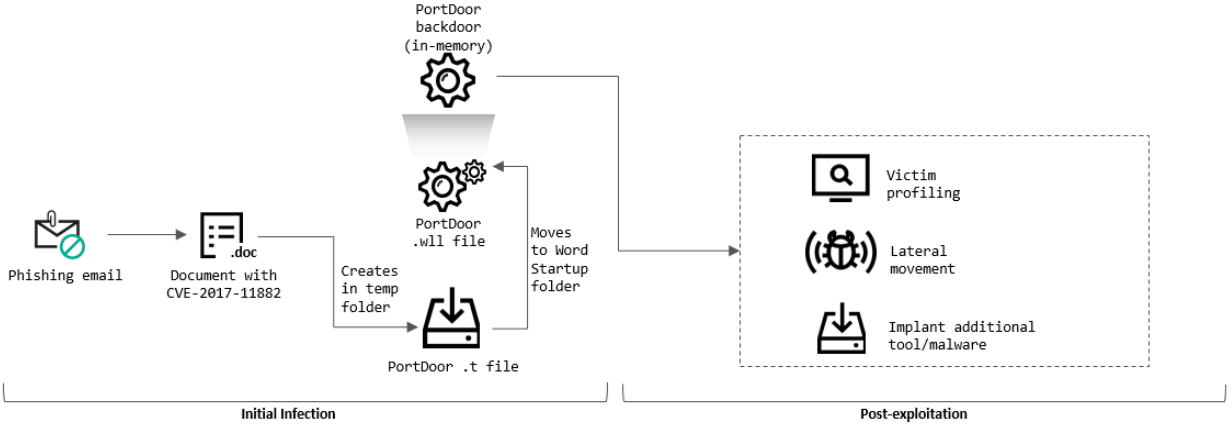
An analysis of information obtained while investigating the incidents indicates that cyberespionage was the goal of this series of attacks.

Initial infection

The attackers penetrated the enterprise network using carefully crafted phishing emails, some of which use information that is specific to the organization under attack and is not publicly available. This could indicate that the attackers did preparatory work in advance (they may have obtained the information in earlier attacks on the same organization or its employees, or on other organizations or individuals associated with the victim organization).

Microsoft Word documents attached to the phishing emails contained malicious code that exploits the CVE-2017-11882 vulnerability. The vulnerability enables an attacker to execute arbitrary code (in the attacks analyzed, the main module of the PortDoor malware) without any additional user activity.

An earlier series of attacks in which the PortDoor malware was also used was described by Cybereason experts. A new version of PortDoor was identified in the course of our research.



Initial infection of a system

After being launched, PortDoor collects general information on the infected system and sends it to the malware command-and-control (CnC) server. In cases where an infected system is of interest to the attackers, they use the PortDoor functionality to control the system remotely and install additional malware.

Additional malware

The attackers used five different backdoors at the same time – probably to set up redundant communication channels with infected systems in case one of the malicious programs was detected and removed by a security solution. The backdoors used provide extensive functionality for controlling infected systems and collecting confidential data.

Of the six backdoors identified on infected systems, five (PortDoor, nccTrojan, Logtu, Cotx, and DNSep) have been used earlier in attacks attributed by other researchers to APT TA428. The sixth backdoor is new and has not been observed in other attacks.

Lateral movement

After gaining a foothold on the initial system, the attackers attempt to spread the malware to other computers on the enterprise network. To gain access to those computers, the attackers use network scanning results, as well as user credentials stolen earlier.

The Ladon hacking utility (which is popular in China) is used as the main lateral movement tool. It combines network scanning, vulnerability search and exploitation, password attack, and other functionality. The attackers also extensively use standard utilities that are part of the Microsoft Windows operating system.

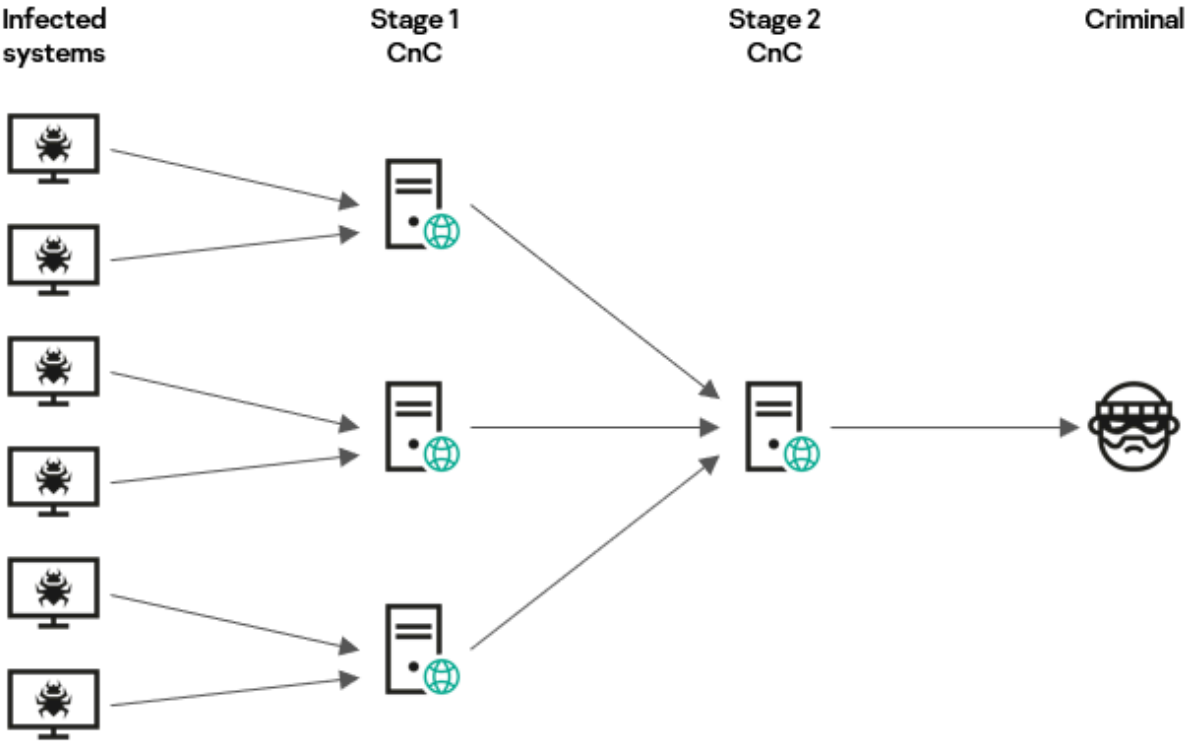
The attack's final stage involves hijacking the domain controller and gaining full control of all of the organization's workstations and servers.

The attackers used DLL hijacking and process hollowing techniques extensively in the attack to prevent security software from detecting the malware.

Data theft

After gaining domain administrator privileges, the attackers searched for and exfiltrated documents and other files that contained the attacked organization's sensitive data to their servers hosted in different countries. These servers were also used as stage one CnC servers.

The attackers compressed stolen files into encrypted and password-protected ZIP archives. After receiving the data collected, the stage one CnC servers forwarded the archives received to a stage two server located in China.



Transfer of stolen data from infected systems

Who is behind the attack?

Significant overlaps in tactics, techniques, and procedures (TTPs) have been observed with APT TA428 activity.

The research identified malware and CnC servers previously used in attacks attributed by other researchers to TA428 APT group.

Some indirect evidence also supports our conclusion.

We believe that the series of attacks that we have identified is highly likely to be an extension of a known campaign that has been described in Cybereason, DrWeb, and NTTSecurity research and has been attributed with a high degree of confidence to APT TA428 activity.

Conclusion

The findings of our research show that spear phishing remains one of the most relevant threats to industrial enterprises and public institutions. In the course of the attack, the attackers used mostly known backdoor malware, as well as standard lateral movement techniques and methods designed to evade detection by security solutions.

The attack series that we have identified is not the first in the campaign. Given that the attackers have had some success, we believe it is highly likely that similar attacks will occur again in the future. Industrial enterprises and public institutions should do a great deal of work to successfully thwart such attacks.

Technical details of the attacks, as well as recommendations and indicators of compromise, can be found in the full public version of the article on the Kaspersky ICS CERT website.

A private version of the article has been published on Kaspersky Threat Intelligence.

We are not wrapping up our investigation as yet and will release information on new findings as they appear. For more information, you can contact ics-cert@kaspersky.com.
