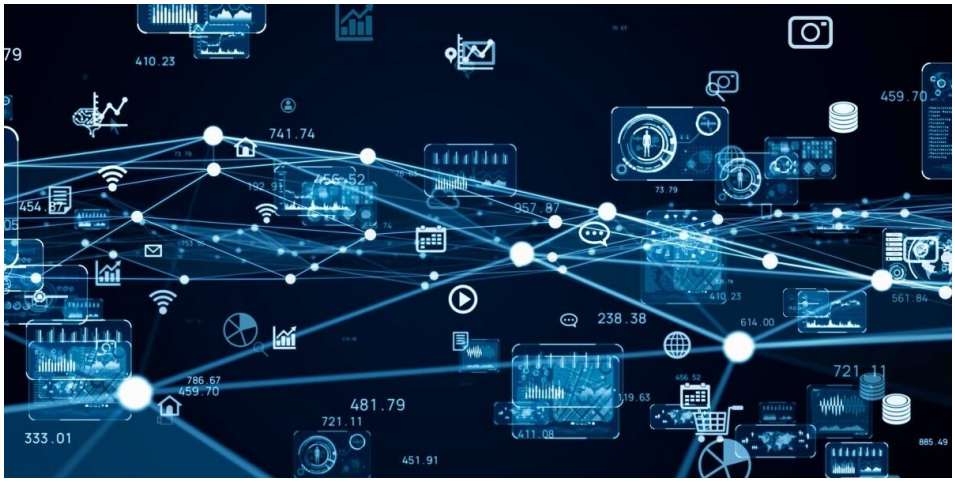
Updated MATA attacks industrial companies in Eastern Europe



Authors

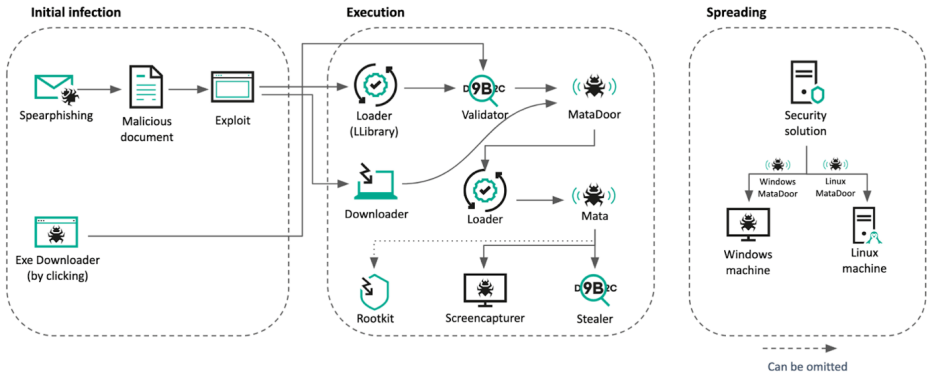
- Expert GReAT
- Expert Kaspersky ICS CERT

In early September 2022, we discovered several new malware samples belonging to the MATA cluster. As we were collecting and analyzing the relevant telemetry data, we realized the campaign had been launched in mid-August 2022 and targeted over a dozen corporations in Eastern Europe from the oil and gas sector and defense industry.

The actors behind the attack used spear-phishing mails to target several victims, some were infected with Windows executable malware by downloading files through an internet browser. Each phishing document contains an external link to fetch a remote page containing a CVE-2021-26411 exploit. The attackers continued to send malicious documents via email until the end of September 2022. Overall, the campaign remained active over 6 months, until May 2023.

The infection chain

After analyzing the timeline and functionality of each malware, we have determined the infection chain of the campaign, although some parts remain unknown due to limited visibility. The attacker employed a combination of loader, main trojan, and stealer infection chains similar to those used by the previous MATA cluster and updated each malware's capabilities. Moreover, they introduced a process to validate compromised victims to ensure careful malware delivery.



The new MATA infection chain

Incident investigation

A turning point in the investigation was the discovery of two MATA samples that had internal IP addresses set as C&C server addresses. Attackers often create a chain of proxy servers within a corporate network to communicate

between the malware and C&C, for example, if the infected system does not have direct access to the internet. Of course, we have seen this before, but in this case the malware configuration included IP addresses from a subnet we were unfamiliar with at the time, and it caught our attention. We immediately notified the affected organization of the likely compromise of systems with these IP addresses and received a swift response.

Starting to investigate this case we realized that the compromised systems were financial software servers and that these servers were having network access to several dozen subsidiaries of the targeted organization. At that point, we realized the compromise of one plant's domain controller was just the tip of the iceberg. As we continued our investigation, we found that the attackers started the attack from the factory, using a phishing email, and progressed through the network until they discovered the shortcut of an RDP connection to the parent company's terminal server. Then they acquired the user's credentials and connected to the terminal server. After that, attackers repeated everything they had done at the attacked plant, but this time on the scale of the entire parent company. Using a vulnerability in a legitimate driver and a rootkit, they interfered with the antivirus, intercepted user credentials (many of which were cached on the terminal server, including accounts with administrator privileges on many systems), and began actively moving around the network.

Naturally, this led to the parent company's domain controller being compromised and control being gained over even more workstations and servers. But the attackers did not stop there. Next, they were able to access the control panels of two security solutions simultaneously. First, they got control over a solution for checking the compliance of systems with information security requirements by exploiting one of its vulnerabilities. Second, with the help of this security solution, they managed to get access to the control panel of the endpoint protection solution that had not been securely configured.
In both cases, security solutions were used by attackers to gather information about the targeted organization's infrastructure and to distribute malware, as both systems have the capability to deploy and execute files remotely. As a result, taking over centralized systems for managing security solutions allowed the attackers to spread the malware to multiple subsidiaries at once, as well as infect servers running Unix-like systems (that they couldn't access even after gaining full control of the organization's domain) with Linux-variant MATA.

Interesting findings

- **Three new generations of the MATA malware**
  The first of the new generations is an evolution of previous MATA generation 2. Second, we dubbed "MataDoor", has been rewritten from scratch and may be considered as generation 4. The last one we named MATA gen.5 and it has been rewritten from the scratch as well. Like previous generations, it has extensive remote control capabilities over the infected system, has a modular architecture, and provides attackers with the ability to connect to control servers using various protocols, as well as supporting flexible proxy server chains.
- **Linux MATA generation 3**
  As said above, we observed that the actor spread the MATA Linux version through security solutions to several Linux servers. We've seen identical ELF malware on several paths including anti-malware solution control server and Linux hosts. Therefore, we strongly believe that this malware was delivered by security solutions remote installation functionality. The Linux version has very similar capability to the 3rd generation MATA Windows version, and seems to have been built from the same sources.
- **USB propagation module capable of bridging the air-gapped networks.**
  It is a special malware module designed to send commands to the infected system via removable media. The same module is also responsible for transporting data collected by the malware on the infected system, which is also done via USB. In our opinion, this component is used by attackers to infiltrate systems that are air-gapped from subnets that have access to the internet, since such systems usually store the most sensitive information.
- **Stealers**
  In previous MATA activity targeting the defense industry, a stealer malware was delivered to the victim. Likewise in this attack, the actor delivered the malware responsible for stealing sensitive information through the complicated infection procedure. The actor employed a variety of stealers based on the circumstances. In some instances, they used malware that was only capable of capturing screenshots from the user's device. In other cases, there were stealers aimed to exfiltrate stored credentials and cookies from the victim.
- **EDR/Security bypass tools**
  In some cases, we observed the actor took advantage of a public exploit called CallbackHell to escalate privilege and bypass endpoint security products. The exploit, which we discovered and reported in 2021, triggers CVE-2021-40449 vulnerability, a use-after-free vulnerability, in Win32k's NtGdiResetDC API. This added layer of complexity allowed them to operate undetected and achieve their objectives more effectively. Similarly, they used the BYOD (Bring Your Own Vulnerable Driver) technique when attacking systems that had the CVE-2021-40449 vulnerability patch installed.

For technical details of the new MATA malware, a description of the malicious infrastructure used by the actor, attribution and victimology read the full "Updated MATA attacks industrial companies in Eastern Europe" report.