Endpoint Protection

symantec.com/connect/blogs/new-reconnaissance-threat-trojanlaziok-targets-energy-sector

Mar 31, 2015 12:45 AM

Migration User

Between January and February, we observed a multi-staged, targeted attack campaign against energy companies around the world, with a focus on the Middle East. This attack campaign used a new information stealer, detected by Symantec as Trojan.Laziok. Laziok acts as a reconnaissance tool allowing the attackers to gather data about the compromised computers.

The detailed information enables the attacker to make crucial decisions about how to proceed further with the attack, or to halt the attack. During the course of our research, we found that the majority of the targets were linked to the petroleum, gas and helium industries, suggesting that whoever is behind these attacks may have a strategic interest in the affairs of the companies affected.

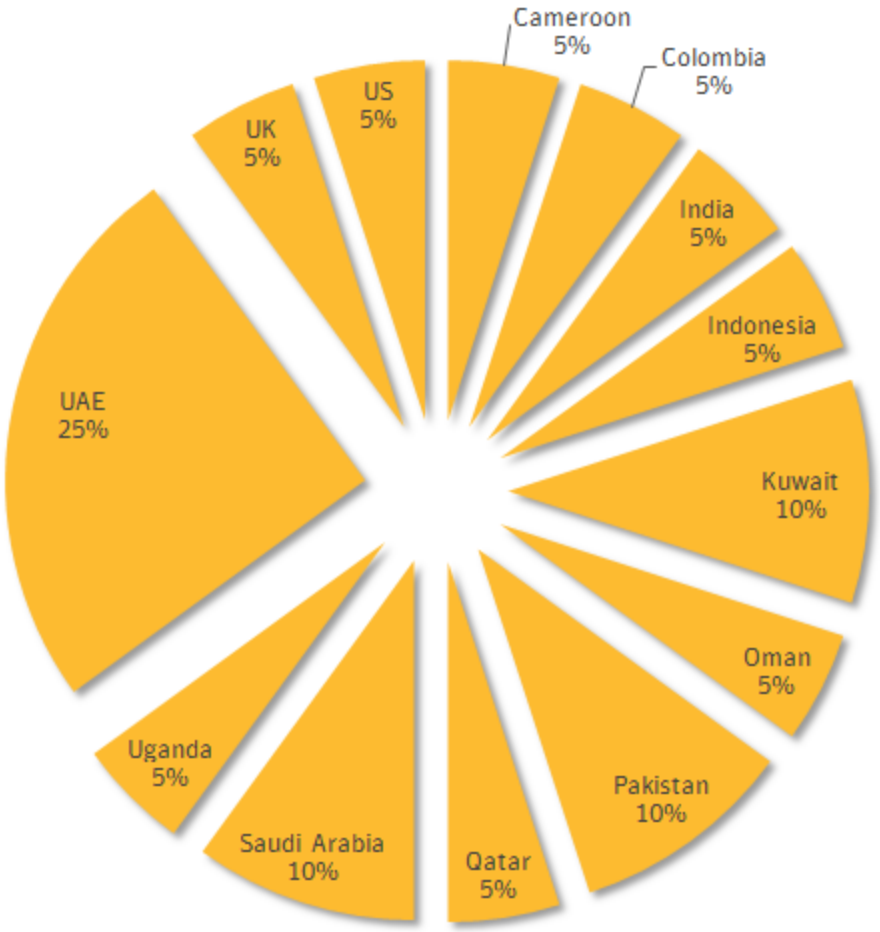

Figure 1. Regions targeted by Trojan.Laziok

How it begins

The initial infection vector involves the use of spam emails coming from the moneytrans[.]eu domain, which acts as an open relay Simple Mail Transfer Protocol (SMTP) server. These emails include a malicious attachment packed with an exploit for the Microsoft Windows Common Controls ActiveX Control Remote Code Execution Vulnerability (CVE-2012-0158). This vulnerability has been exploited in many different attack campaigns in the past, such as Red October. Symantec and Norton products had protection in place against these exploits at the time of the targeted attack as Bloodhound.Exploit.457 and Web Attack: Microsoft Common Controls CVE-2012-0158.

If the user opens the email attachment, which is typically an Excel file, then the exploit code is executed. If the exploit succeeds, it drops Trojan.Laziok, kicking off the infection process.

Infection

The Trojan hides itself in the %SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle directory, making new folders and renaming itself with well-known file names such as:

- %SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle\azioklmpx\search.exe
- %SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle\azioklmpx\ati.exe
- %SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle\azioklmpx\lsass.exe
- %SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle\azioklmpx\smss.exe
- %SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle\azioklmpx\admin.exe
- %SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle\azioklmpx\key.exe
- %SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle\azioklmpx\taskmgr.exe
- %SystemDrive%\Documents and Settings\All Users\Application Data\System\Oracle\azioklmpx\chrome.exe

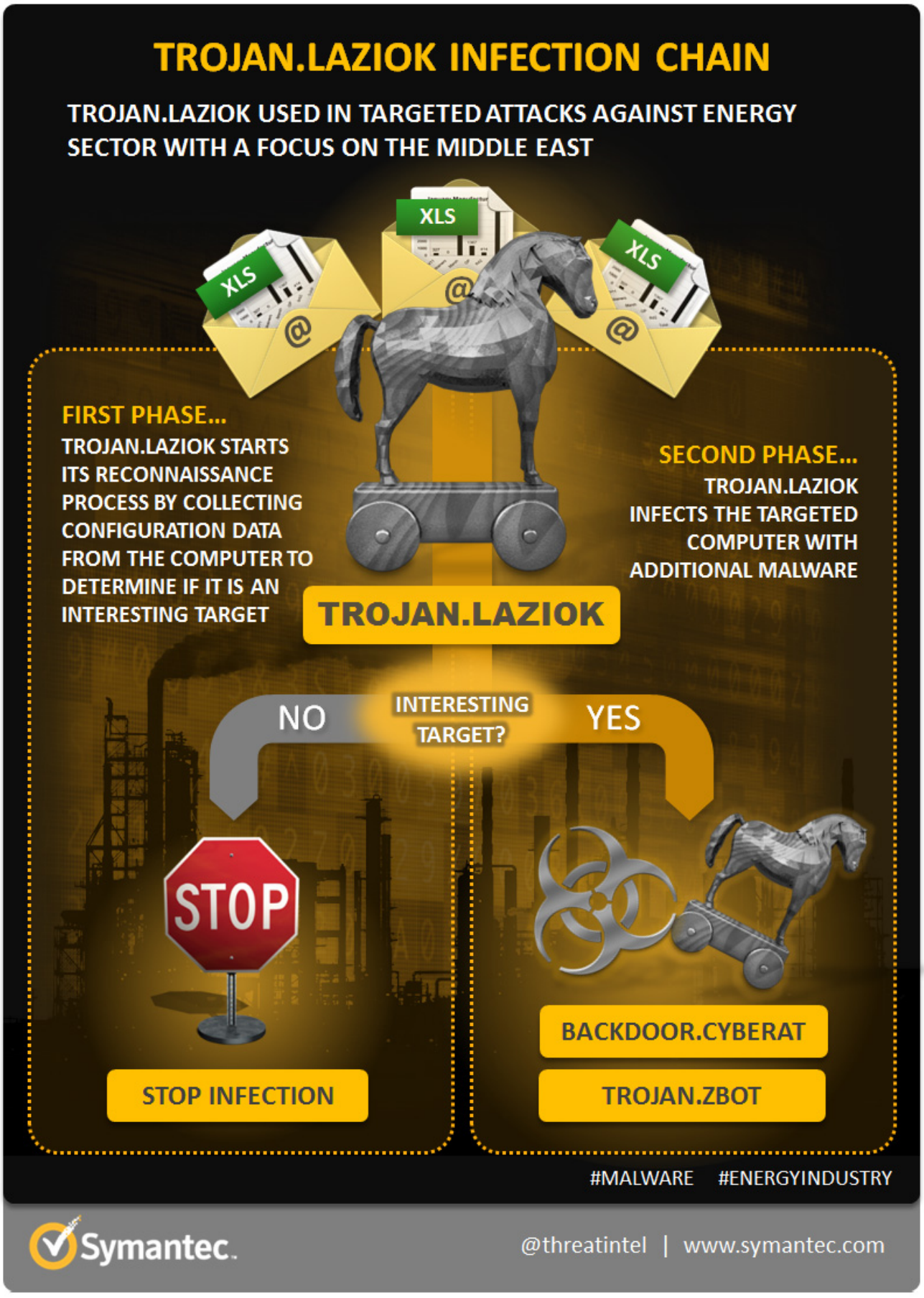

Figure 2. Overview of the Trojan.Laziok attack

Trojan.Laziok then begins its reconnaissance process by collecting system configuration data such as:

- Computer name
- Installed software
- RAM size
- Hard disk size
- GPU details
- CPU details
- Antivirus software

The collected information is then sent to the attackers. Once the attackers received the system configuration data, including details of any installed antivirus software, they then infect the computer with additional malware. In this campaign, the attackers distributed customized copies of Backdoor.Cyberat and Trojan.Zbot which are specifically tailored for the compromised computer's profile. We observed that the threats were downloaded from a few servers operating in the US, UK, and Bulgaria.

The group behind the attack does not seem to be particularly advanced, as they exploited an old vulnerability and used their attack to distribute well-known threats that are available in the underground market. However, many people still fail to apply patches for vulnerabilities that are several years old, leaving themselves open to attacks of this kind. From the attacker's perspective, they don't always need to have the latest tools at their disposal to succeed. All they need is a bit of help from the user and a lapse in security operations through the failure to patch.

Protection and prevention
Symantec and Norton products have the following protections against this campaign:

Antivirus

Intrusion prevention system

Gateway protection

- Trojan.Mdropper
- Our antispam technology detects the emails through generic Brightmail Rules.

Best practices
Users should also adhere to the following best practices to avoid malware infections through spam campaigns:

- Avoid clicking on links in unsolicited, unexpected, or suspicious emails.
- Avoid opening attachments in unsolicited, unexpected, or suspicious emails.

- Use comprehensive security software, such as Symantec Endpoint Protection or Norton Security, to protect yourself from attacks of this kind.
- Take a security layered approach for better protection.
- Keep your security software up to date.
- Apply patches for installed software on a timely basis.