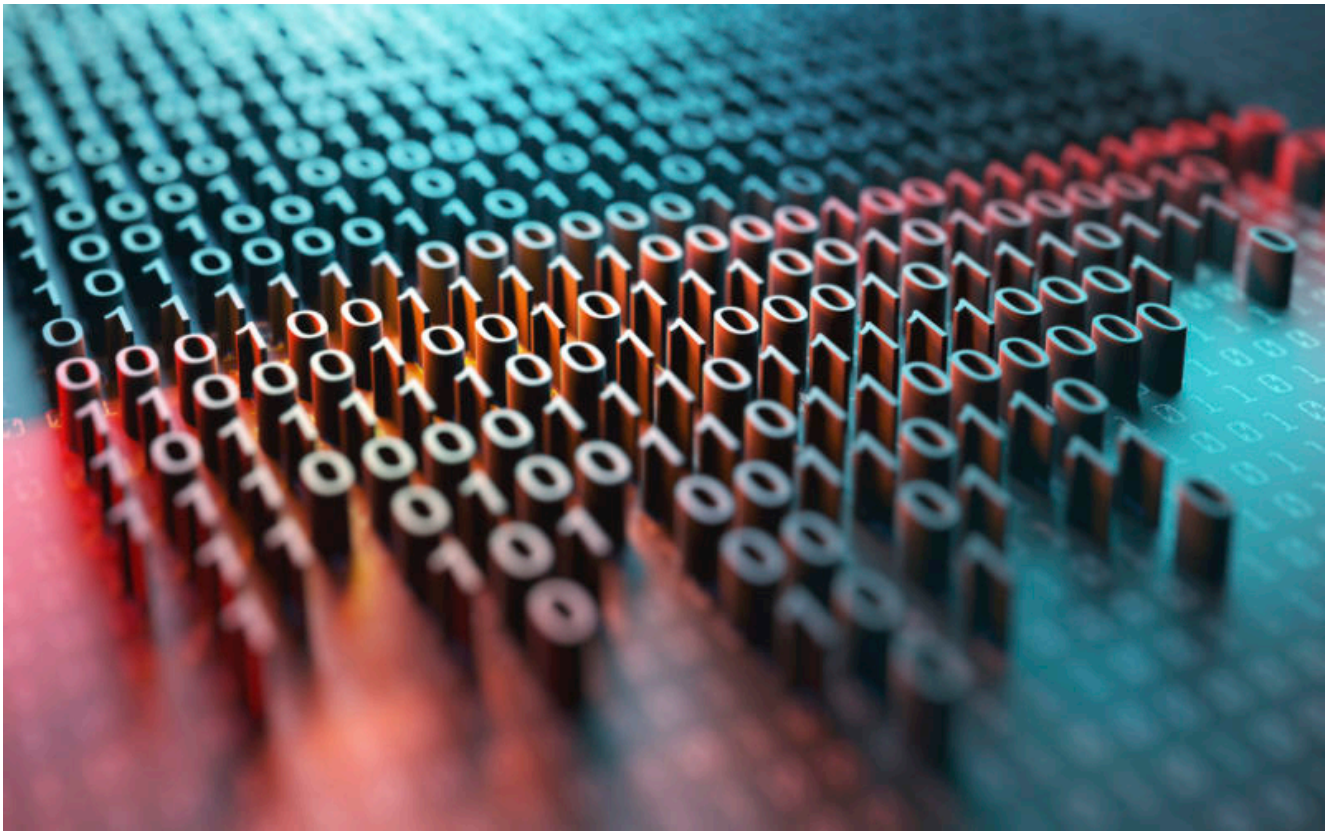
An advanced and unconventional hack is targeting industrial firms



Enlarge / Binary code, illustration.

reader comments

54 with 47 posters participating

Share this story

Attackers are putting considerable skill and effort into penetrating industrial companies in multiple countries, with hacks that use multiple evasion mechanisms, an innovative encryption scheme, and exploits that are customized for each target with pinpoint accuracy.

The attacks begin with emails that are customized for each target, a researcher at security firm Kaspersky Lab reported

this week. For the exploit to trigger, the language in the email must match the localization of the target's operating system. For example, in the case of an attack on a Japanese company, the text of the email and an attached Microsoft Office document containing a malicious macro had to be written in Japanese. Also required: an encrypted malware module could be decrypted only when the OS had a Japanese localization as well.

Recipients who click on a request to urgently enable the document's active content will see no indication anything is amiss. Behind the scenes, however, a macro executes a Powershell script. The reason it stays hidden: the command parameters:

- ExecutionPolicy ByPass—to override organization policies
- WindowStyle Hidden. This hides the PowerShell window
- NoProfile, which executes the script with no end-user configuration.

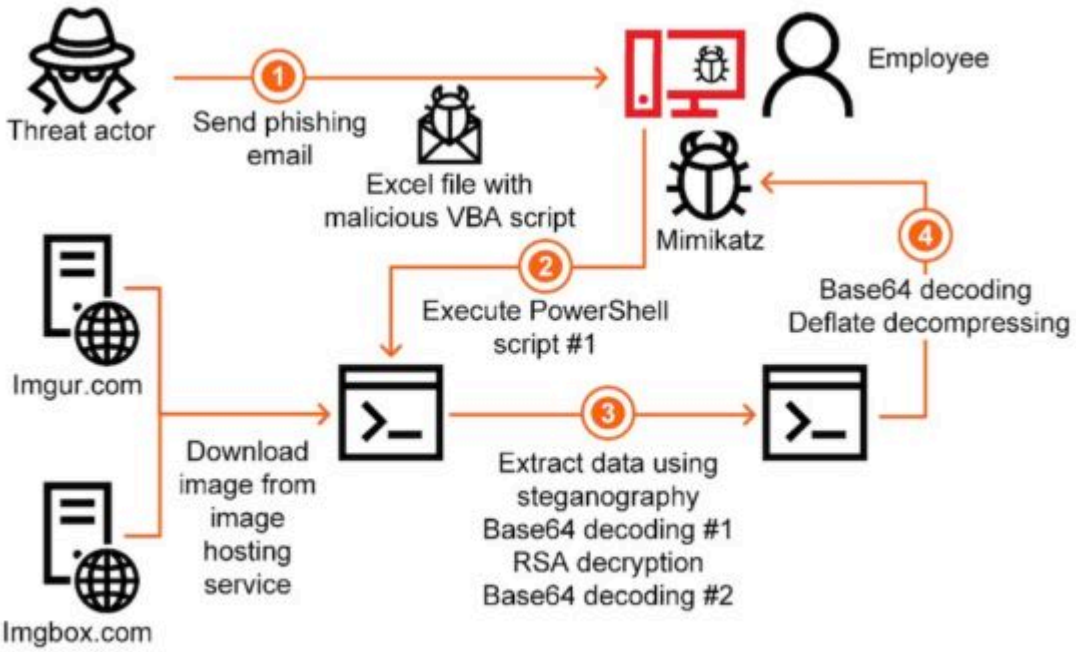
Triple-encoded steganography, anyone?

The PowerShell script reaches out to either imgur.com or imgbox.com and downloads an image that has malicious code hidden inside the pixels through a technique called steganography. The data is encoded by the Base64 algorithm, encrypted with an RSA key, and then Base64-encoded again. In a clever move, the script contains an intentional error in its code. The resulting error message that's returned—which is different for each language pack installed on the OS—is the decryption key.

The decrypted and decoded data is used as a second PowerShell script that, in turn, unpacks and decodes another blob of Base64-encoded data. With that, a third obfuscated PowerShell script executes Mimikatz malware that's designed to steal

Windows account credentials used to access various network resources. In the event stolen credentials include those for the all-powerful Windows Active Directory, attackers have access to virtually every node on the network.

The following diagram summarizes the flow of the attack:



Attack kill chain

Kaspersky Lab

The attacks—which Kaspersky Lab has spotted in Japan, Italy, Germany, and the UK—are notable for their unconventional approaches, as noted in this week's post from Kaspersky Lab. Company researcher Vyacheslav Kopeytsev wrote:

> *First, the malicious module is encoded in an image using steganographic techniques and the image is hosted on legitimate web resources. This makes it virtually impossible to detect such malware using network traffic monitoring and control tools while it is being downloaded. From the standpoint of technical solutions, this activity is indistinguishable from sending ordinary requests to legitimate image hosting services.*
>
> *A second curious feature of the malware is the use of the*

> *exception message as the decryption key for the malicious payload. This technique can help the malware evade detection in automatic analysis systems of the sandbox class and makes analyzing the functionality of the malware significantly more difficult for researchers if they do not know what language pack was used on the victim's computer.*
>
> *The use of the above techniques, combined with the pinpoint nature of the infections, indicates that these were targeted attacks. It is a matter of concern that attack victims include contractors of industrial enterprises. If the attackers are able to harvest the credentials of a contractor organization's employees, this can lead to a range of negative consequences, from the theft of sensitive data to attacks on industrial enterprises via remote administration tools used by the contractor.*

Kaspersky Lab software shut down the attacks before they could get any further. As a result, researchers still don't know what attackers' ultimate goal was. In recent years, control systems for gas refineries, power plants, factories, and other critical infrastructure have come under increasing attack by saboteurs and ransomware alike. It's possible the ultimate target in these attacks were the contractors' industrial enterprise customers.

https://arstechnica.com/?p=1680042