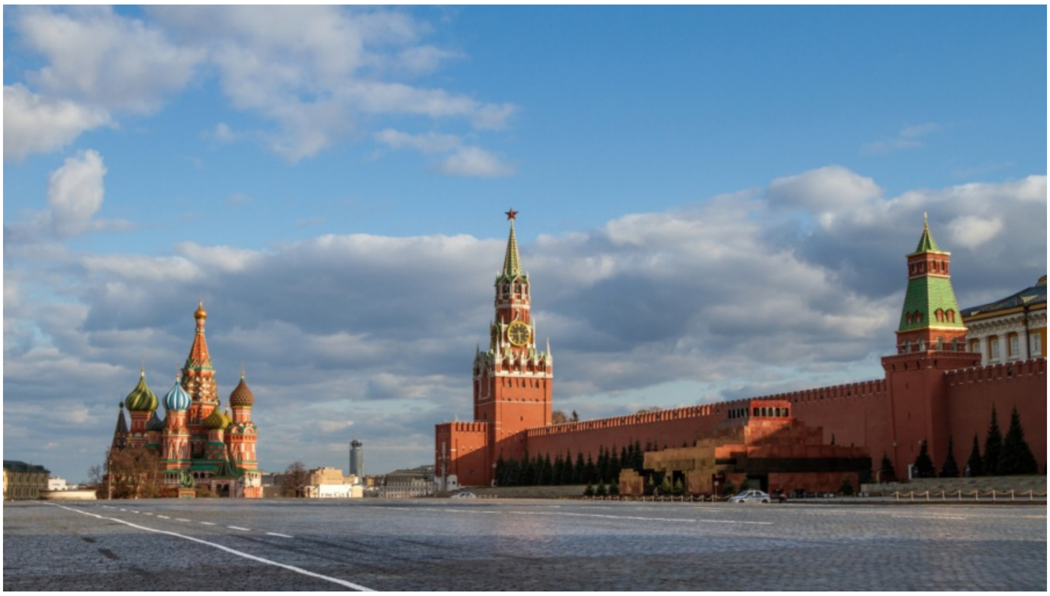

MSHTML attack targets Russian state rocket centre and interior ministry

Posted: September 22, 2021 by Malwarebytes Labs

Malwarebytes has reason to believe that the MSHTML vulnerability listed under CVE-2021-40444 is being used to target Russian entities. The Malwarebytes Intelligence team has intercepted email attachments that are specifically targeting Russian organizations.

The first template we found is designed to look like an internal communication within JSC GREC Makeyev. The Joint Stock Company State Rocket Center named after Academician V.P. Makeyev is a strategic holding of the country's defense and industrial complex for both the rocket and space industry. It is also the lead developer of liquid and solid-fuel strategic missile systems with ballistic missiles, making it one of Russia's largest research and development centers for developing rocket and space technology.

The email claims to come from the Human Resources (HR) department of the organization.

A phishing email targeted at the Makeyev State Rocket Center, posing at its own HR department

It says that HR is performing a check of the personal data provided by employees. The email asks employees to please fill out the form and send it to HR, or reply to the mail. When the receiver wants to fill out the form they will have to enable editing. And that action is enough to trigger the exploit.

The attack depends on MSHTML loading a specially crafted ActiveX control when the target opens a malicious Office document. The loaded ActiveX control can then run arbitrary code to infect the system with more malware.

The second attachment we found claims to originate from the Ministry of the Interior in Moscow. This type of attachment can be used to target several interesting targets.

A phishing email posing as the Russian Ministry of the Interior

The title of the documents translates to “Notification of illegal activity.” It asks the receiver to please fill out the form and return it to the Ministry of Internal affairs or reply to this email. It also urges the intended victim to do so within 7 days.

Russian targets

It is rare that we find evidence of cybercrimes against Russian targets. Given the targets, especially the first one, we suspect that there may be a state-sponsored actor behind these attacks, and we are trying to find out the origin of the attacks. We will keep you informed if we make any progress in that regard.

Patched vulnerability

The CVE-2021-40444 vulnerability may be old-school in nature (it involves ActiveX, remember that?) but it was only recently discovered. It wasn't long before threat actors were sharing PoCs, tutorials and exploits on hacking forums, so that everyone was able to follow step-by-step instructions in order to launch their own attacks.

Microsoft quickly published mitigation instructions that disabled the installation of new ActiveX controls, and managed to squeeze a patch into its recent Patch Tuesday output, just a few weeks after the bug became public knowledge. However, the time it takes to create a patch is often dwarfed by the time it takes people to apply it. Organizations, especially large ones, are often found trailing far behind with applying patches, so we expect to see more attacks like this.

Будьте в безопасности, все!

Related

[updated] Windows MSHTML zero-day actively exploited, mitigations required
September 8, 2021
In "Exploits and vulnerabilities"

[updated] Patch now! PrintNightmare over, MSHTML fixed, a new horror appears … OMIGOD
September 15, 2021
In "Exploits and vulnerabilities"

500,000 Fortinet VPN credentials exposed: Turn off, patch, reset passwords
September 9, 2021
In "Exploits and vulnerabilities"

SHARE THIS ARTICLE

COMMENTS

RELATED ARTICLES

[updated] Patch now! PrintNightmare over, MSHTML fixed, a new horror appears … OMIGOD

September 15, 2021 - Septermber 2021's Patch Tuesday could be remembered for ending the PrintNightnare, or for the bug that made us go OMIGOD.

CONTINUE READING

1 Comment

ABOUT THE AUTHOR

Malwarebytes Labs

Contributors

Threat Center

Glossary

Scams

Write for Labs

Email address

Imagine a world without malware. We do.

FOR PERSONAL (//www.malwarebytes.com/for-home/)

FOR BUSINESS (//www.malwarebytes.com/business/)

COMPANY

ABOUT US (//www.malwarebytes.com/company/)

CAREERS (https://jobs.malwarebytes.com/)

NEWS AND PRESS (https://press.malwarebytes.com/)

MY ACCOUNT

SIGN IN (https://my.malwarebytes.com/en/login)

CONTACT US

GET SUPPORT (https://support.malwarebytes.com/hc/en-us)

CONTACT SALES (https://www.malwarebytes.com/contact/)

3979 Freedom Circle, 12th Floor
Santa Clara, CA 95054