Re: Pencerobohan Pada Laman Web Malaysia Productivity Corporation

Mohd Suzlezan Supu to: Imran bin Mohd Nor 07/12/2020 05:32 PM

Cc: "Computer Emergency Response Team", "Mohd Nadzri Yusof", "Wan Mohd Nadzir Hadzril Wan Ismail", MIT, Mohd Yazid Abdul Majid

Assalamualaikum Tuan,

Berikut adalah tindakan yang dilaksanakan oleh pihak MPC setakat ini, namun belum dapat menghilangkan kesan pencerobohan.

1. Replaced root with backup files
2. Deleted unrecognised new files
3. Deleted old user
    a. 1 old superadmin
    b. 9 user admin
4. Deleted old sites (blog Wilayah)
    a. www.mpc.gov.my/northern
    b. www.mpc.gov.my/southern
    c. www.mpc.gov.my/sarawak
    d. www.mpc.gov.my/sabah
    e. www.mpc.gov.my/eastcoast
    f. www.mpc.gov.my/terengganu
    g. www.mpc.gov.my/kelantan
    h. www.mpc.gov.my/triz
5. Updated latest version of Wordpress 5.5.3
6. Updated 7 themes

Pihak kami juga masiih mengenalpasti punca pencerobohan ini. Kami akan memaklumkan kepada pihak tuan dari masa ke semasa. Mohon maaf diatas kelewatan membalas emel ini.

Sekian, Terima Kasih.

MOHD SUZLEZAN SUPU
Unit Pengurusan Maklumat (MIT)
Bahagian Pengurusan dan Kewangan (MSF)
Perbadanan Produktiviti Malaysia (MPC)
Tel : 03-79557266 Ext 358

"HELP US, TO HELP YOU"

"Imran bin Mohd Nor" Assalamualaikum dan Salam Sejahtera. Tuan, 07/12/2020 05:09:30 PM

From: "Imran bin Mohd Nor" <imran@nc4.gov.my>
To: "Mohd Nadzri Yusof" <nadzri@miti.gov.my>, "ENCIK MOHD. SUZLEZAN SUPU" <suzlezan@mpc.gov.my>
Cc: "Wan Mohd Nadzir Hadzril Wan Ismail" <wmnadzir@miti.gov.my>, "Computer Emergency Response Team" <cert@nc4.gov.my>
Date: 07/12/2020 05:09 PM
Subject: Re: Pencerobohan Pada Laman Web Malaysia Productivity Corporation

Assalamualaikum dan Salam Sejahtera.

Tuan,

Dengan hormatnya saya diarah merujuk kepada perkara di atas.

Terima kasih di atas maklum balas daripada pihak MITI. Kami mengambil maklum.

Mohon tindakan segera daripada pihak MPC jua.

Perhatian serta kerjasama pihak tuan di dalam perkara ini amat dihargai dan didahului dengan ucapan terima kasih.

Sekian.

Imran bin Mohd Nor
National Cyber Coordination & Command Centre (NC4)
Agensi Keselamatan Siber Negara (NACSA)
Majlis Keselamatan Negara
Jabatan Perdana Menteri
Tel: 03-8064 4828
Fax: 03-8064 4848

From: Mohd Nadzri Yusof <nadzri@miti.gov.my>
Date: Monday, 7 December 2020 at 5:00 PM
To: Imran bin Mohd Nor <imran@nc4.gov.my>
Cc: "ENCIK MOHD. SUZLEZAN SUPU" <suzlezan@mpc.gov.my>, Wan Mohd Nadzir Hadzril Wan Ismail <wmnadzir@miti.gov.my>
Subject: RE: Pencerobohan Pada Laman Web Malaysia Productivity Corporation

En. Imran Portal MPC adalah dibawah penyeliaan sepenuhnya Agensi MPC.

En. Suzlezan mohon maklumbalas kepada En. Imran dan cc kepada saya.

Terima kasih.

From: Imran bin Mohd Nor
Sent: Friday, 4 December, 2020 3:03 PM
To: mtcert <mtcert@miti.gov.my>
Cc: Computer Emergency Response Team <cert@nc4.gov.my>
Subject: Pencerobohan Pada Laman Web Malaysia Productivity Corporation
Importance: High

Assalamualaikum dan Salam Sejahtera.

Tuan,

Dengan hormatnya saya diarah merujuk kepada perkara di atas.

Berdasarkan kepada pemantauan yang dibuat oleh NC4, didapati laman web Malaysia Productivity Corporation (MPC) mengalami pencerobohan yang menyebabkan redirection ke laman web lain apabila dibuka dari hasil carian seperti Google Jepun. Kesan pencerobohan boleh dilihat dengan melaksanakan carian dari www.google.co.jp<http://www.google.co.jp> seperti https://www.google.co.jp/search?q=%E6%BF%80%E5%AE%89+-site%3A.jp+inurl%3Ampc.gov.my. Hasil carian adalah seperti di lampiran.

Sehubungan dengan itu, mohon kerjasama pihak tuan jua untuk melaksanakan tindakan sewajarnya seperti berikut:

* mengesahkan kejadian pencerobohan;
* mengasingkan server yang terlibat dari rangkaian;
* mengenal pasti dan menghapuskan fail, kandungan atau source code yang ditambah oleh penyerang;
* melaksanakan restore dari fail backup sekiranya perlu;
* menyemak source code atau content management system yang digunakan untuk mengenal pasti kelemahan yang membolehkan serangan;
* menyemak akaun pengguna/admin sekiranya telah diceroboh dan menukar kata laluan sekiranya perlu;
* menyemak format katalaluan yang digunakan supaya ianya tidak mudah diteka;
* membuat virus scanning;
* mengemas kini perisian-perisian yang digunakan kepada versi yang terkini; dan
* menyemak log untuk mengenal pasti punca serangan.

Pihak tuan juga diminta untuk mengenal pasti punca serangan serta memaklumkan hasil analisis dan tindakan yang telah dilaksanakan kepada NC4 untuk memastikan serangan seperti ini tidak berulang.

Perhatian serta kerjasama pihak tuan di dalam perkara ini amat dihargai dan didahulukan dengan ucapan terima kasih.

Sekian.

Imran bin Mohd Nor
National Cyber Coordination & Command Centre (NC4)
Agensi Keselamatan Siber Negara (NACSA)
Majlis Keselamatan Negara
Jabatan Perdana Menteri
Tel: 03-8064 4828
Fax: 03-8064 4845

[Image removed by sender.]