Jurnal Sains Riset (JSR)
ISSN 2088-0952

CELAH KEAMANAN KREDENSIAL WINDOWS PADA GOOGLE CHROME

Sayed Achmady[1], Maryanti[2]

[1,2]Fakultas Teknik, Universitas Jabal Ghafur Sigli, Aceh
[1]sayedachmady@unigha.ac.id, [2]maryanti@unigha.ac.id

ABSTRACT

An attack that can leak authentication credentials on a Windows operating system by using the SMB file sharing protocol on a Windows operating system is an ever-present problem. It's been exploited in many ways, but the only solution found is limited to local area networks. Jonathan Brossard and Hormazd Billimoria recently presented one study involving internet attacks at the Black Hat security conference in 2015. However, no SMB-related attacks were published. In this paper, we will explain how an attack can cause Windows credential theft, which may affect the default configuration in Google Chrome browser.
Keywords: *Kredensial Windows, Google Chrome, Vulnerabilit*

ABSTRAK

Pada system operasi windows adalah sebuah masalah yang selalu muncul, Sudah dieksploitasi dengan berbagaicara, Namun solusi yang di temukan hanya terbatas pada jaringan area lokal. Salah satu penelitian yang melibatkan serangan melalui internet baru-baru ini dipresentasikan oleh Jonathan Brossard dan Hormazd Billimoria dikonferensi keamanan Black Hat pada tahun 2015.Namun, tidak ada serangan yang terkait dengan SMB yang dipublikasikan. Pada paper ini kami akan menjelaskan bagaimana sebuah serangan yang dapat menyebabkan pencurian kredensial Windows, yang dapat mempengaruhi konfigurasi default pada browser Google Chrome.
Kata Kunci:Serangan yang dapat membocorkan kredensial otentikasi pada system operasi windows dengan menggunakan protocol berbagi file SMB

Pendahuluan

Dengan konfigurasi defaultnya, Google Chrome akan secara otomatis mendownload file yang dianggap aman tanpa mendorong pengguna untuk menentukan lokasi penyimpanan file, namun menggunakan yang sudah ada sebelumnya. Dari sudut pandang keamanan, fitur ini bukanlah perilaku yang baik namun setiap konten berbahaya yang masuk masih memerlukan aksi dari pengguna untuk membuka atau menjalankan file untuk melakukan kerusakan. Namun, bagaimana jika file yang sudah diunduh namun tidak memerlukan interaksi pengguna untuk melakukan tindakan merusak? Apakah ada tipe file yang bias melakukan itu?

Windows Explorer Shell Command File atau SCF (.scf) adalah tipe file yang tidak dikenal, Sebagian besar pengguna Windows menemukannya pada Windows 98 / ME / NT / 2000 / XP dimana ia digunakan sebagai Shortcut desktop. Ini pada dasarnya adalah file teks dengan bagian yang menentukan perintah yang akan dijalankan dan lokasi file ikon. Untuk Source code isi dari file View Desktop SCF dapat dilihat dibawahini:

```
[Shell] Command=2
IconFile=explorer.exe,3
[Taskbar] Command=ToggleDesktop
```

Seperti file shortcut Windows LNK, lokasi ikon secara otomatis terselesaikan pada saat file ditampilkan di Explorer. Menentukan lokasi ikon ke server SMB jarak jauh adalah vektor serangan yang diketahui dapat menyalahgunakan fitur otentikasi otomatis pada Windows pada saat

mengakses layanan seperti file file jarak jauh. Tetapi apa perbedaan antara LNK dan SCF dari sudut pandang serangan? Google Chrome dapat membersihkan file LNK dengan memaksa ekstensi download Stuxnet, Namun tidak memberikan aksi yang sama pada file SCF. File SCF yang bisa digunakan untuk memanipulasi Windows menjadi upaya otentikasi ke server SMB remote hanya dengan dua baris perintah saja, Source codenya adalah sebagai berikut:

```
[Shell]
IconFile=\\170.170.170.170\icon
```

Setelah didownload, permintaan akan berjalan pada saat direktori download dibuka pada Windows File Explorer untuk melihat file tersebut, menghapusnya atau bekerja dengan file yang lain dan aksi ini tidak dapat dihindari. Tidak perlu mengklik atau membuka file yang didownload Windows File Explorer secara otomatis akan mencoba untuk mengambil "icon".

Server SMB jarak jauh yang telah disiapkan oleh penyerang untuk menangkap nama pengguna korban dan hash kata sandi NTLMv2 untuk pembengkakan offline atau meneruskan koneksi ke layanan eksternal yang menerima jenis otentikasi yang sama seperti Microsoft Exchange untuk meniru korban tanpa mengetahui kata sandinya yang sudah diambil. Untuk lebih jelasnya anda dapat melihat pada Gambar 1 dibawah ini:

Hal ini dapat melakukan serangan yang tidak diketahui oleh korban dengan menggunakan file SCF.

Dampak

Dari uraian singkat pada pendahuluan diatas dapat di temukan beberapa dampak dari celah kemanan kredensial window tersebut, Antara lain:

Pembobolan Password

Bagi pengguna pada domain Direktori Aktif baik pada perusahaan, pemerintah, dan instansi lainnya, pembobolan kata sandi dapat memiliki berbagai dampak mulai dari meningkatnya pelanggaran jaringan internal hingga mengakses layanan secara eksternal berdasarkan penggunaan ulang kata sandi. Untuk pengguna Windows 8 dan Windows 10 yang menggunakan Akun Microsoft (MSA) dan bukan akun lokal, pembobolan kata sandi akan mempengaruhi pada semua layanan Microsoft yang terintegrasi seperti OneDrive, Outlook, Office 365, Office Online, Skype, Xbox Live dan lainnya.

Mengenai kelayakan cracking password, ini meningkat pesat dalam beberapa tahun terakhir dengan berbasis GPU cracking. Tuntutan hashcat NetNTLMv2 untuk kartu Nvidia GTX 1080 tunggal adalah sekitar 1600 MH/s atau 1,6 miliar hash per detik. Untuk password 8 karakter, GPU rigs dari 4 kartu tersebut dapat melalui seluruh ruang kunci dari huruf besar, huruf kecil, alfa numeric dan karakter khusus yang paling umum digunakan seperti (! @ # $% &) Hanya dalam waktu kurang dari satu hari. Dengan ratusan juta bocoran kata sandi yang diakibatkan oleh beberapa pelanggaran dalam beberapa tahun terakhir (LinkedIn, Myspace), cracking berbasis kata daftar yang dapat menghasilkan hasil yang mengejutkan terhadap kata kunci kompleks dengan lebih banyak entropi.

Situasi ini bahkan lebih buruk lagi pada system dan jaringan di Windows XP di mana kompatibilitas mundur dengan NTLMv1 telah diaktifkan secara eksplisit. Dalam kasus tersebut, serangan downgrade dapat dilakukan dengan memaksa klien untuk melakukan otentikasi dengan hash atau protokol yang lebih lemah (seperti NTLMv1 atau bahkan LM). Hal ini akan memungkinkan penyerang untuk

menangkap hash yang lebih cepat dari NTLMv2 hanya dalam hitungan detik dengan menggunakan tabel precomputed untuk membalikkan fungsi hash kriptografi.

Serangan Relay SNB

Organisasi yang mengizinkan akses jarak jauh ke layanan seperti *Microsoft Exchange (Outlook Anywhere)* dan menggunakan metode otentikasi *NTLM*, Mungkin lebih rentan terhadap serangan relay *SMB*, yang memungkinkan Defense Code penyerang untuk meniru korban, mengakses data dan sistem tanpa harus memecahkan password. Hal ini berhasil ditunjukkan oleh Jonathan Brossard pada konferensi keamanan Black Hat di amerika serikat pada tahun 2015 lalu. Dalam kondisi tertentu penyerang bahkan mungkin bisa menyampaikan kredensial ke kontroler domain pada jaringan korban dan pada dasarnya mendapatkan akses internal ke jaringan.

Tidak Dapat Terdeteksi Oleh Anti Virus

Ketika browser gagal memberi peringatan atau membersihkan jenis file download yang berpotensi berbahaya. Kami menguji beberapa solusi antivirus terkemuka oleh vendor yang berbeda untuk menentukan apakah ada solusi untuk menandai file yang diunduh tersebut berbahaya atau tidak. Semua solusi yang teruji gagal menunjukkan bahwa file download tersebut sebagai sesuatu virus yang mencurigakan.

Refleksi File Download

Seperti yang dijelaskan oleh Oren Hafif pada Konferensi Black Hat Eropa tahun 2014, kerentanan Refleksi File Download terjadi ketika masukan pengguna yang dibuat secara khusus dalam respons situs web dan diunduh oleh browser pengguna pada saat kondisi tertentu. Pada awalnya digunakan sebagai vektor serangan untuk mengelabui pengguna agar menjalankan kode berbahaya, berdasarkan kepercayaan pengguna terhadap domain yang berbahaya. Karena format SCF lebih sederhana dan hanya membutuhkan dua garis untuk mengubah kondisi sempurna yang digunakan dengan RFD.

RFD biasanya ditujukan pada endpoint API karena mereka sering menggunakan pemetaan URL permisif, yang memungkinkan pengaturan ekstensi file di jalur URL. Google Chrome tidak akan mendownload jenis konten respons API secara langsung, Sehingga harus dipaksa melalui atribut unduhan di tag tautan **<a href=… link tags**. Google Chrome menggunakan sniffing MIME dengan jenis teks atau konten biasa dan jika respon tersebut berisi karakter yang tidak dapat dicetak maka file tersebut akan didownload sebagai file secara langsung. Hal ini dapat ditunjukkan pada API Bank Dunia, Seperti terlihan pada link API Word bank berikut ini.

http://api.worldbank.org/v2/country/indicator/iwantyourhash.scf?prefix= %0A[Shell]%0AIconFile=\\170.170.170.170\test%0Alol=%0B&format=jsonp

Karena karakter **%0B** yang tidak dapat dicetak, Maka Google Chrome akan mendownloadnya sebagai file iwantyourhash.scf. Dan pada saat direktori download yang berisi file tersebut dibuka, Maka Windows akan mencoba melakukan otentikasi ke server SMB remote, yang dapat menemukan hash otentikasi korban.

Pencegahan

Untuk pencegahannya dapat menonaktifkan unduhan otomatis pada Google Chrome, Caranya adalah sebagai berikut:

A. Pilih "Settings" pada google chrome
B. Kemudian Klik "Show advanced settings"
C. Periksa di mana penyimpan setiap file download dan rubah download otomatis menjadi manual.

Pemberitahuan secara manual pada saat mendownload file pada google chrome secara signifikan dapat mengurangi risiko serangan pencurian kredensial NTLMv2 dengan menggunakan file SCF. Karena file

SCF dapat menimbulkan ancaman, tindakan yang perlu dilakukan tergantung pada lingkungan jaringan pengguna yang terkena dampak dan mengkonfigurasi peraturan parameter firewall untuk menerapkan tindakan pengamanan tambahan seperti SMB packet signing and Extended Protection. Dengan tujuan mencegah lalu lintas traffic dengan memblokir port yang dapat digunakan untuk memulai koneksi dengan server SMB berbasis Internet yang berpotensi berbahaya. Bila memungkinkan, lalu lintas SMB harus selalu dibatasi dengan private networks.

Kesimpulan

Penyerang hanya perlu menarik perhatian korban dengan menggunakan Google Chrome dan Windows yang telah diperbarui untuk mengunjungi situs webnya agar dapat melanjutkan dan menggunakan kembali kredensial otentikasi korban. Kerentanan semacam itu dapat menimbulkan ancaman yang signifikan terhadap instansi pemerintahan ataus wasta di Indonesia, Karena memungkinkan penyerang untuk meniru sebagai administrator system pada sebuah instansi. Penyerang semacam itu dapat dimanfaatkan sebagai hak istimewa untuk meningkatkan akses lebih lanjut dan melakukan serangan terhadap pengguna lain atau mendapatkan akses dan control sumber daya TI pada instansi tersebut.

Kami berharap semoga browser Google Chrome akan diperbarui untuk mengatasi celah keemanan ini dalam waktu dekat.

REFERENSI

[1] Microsoft Security Bulletin MS10-046, https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2010/ms10-046 (diakses 5 Januari 2018).
[2] Oren Hafif. (2017). Reflected File Download - A New Web Attack Vector. Jonathan Brossard dan Hormazd Billimoria. (2015). Black Hat USA Conference