Nama : Ahmad Ridwan

NIM : 09011281419042

MK : Keamanan Jaringan Komputer

SERANGAN CYBER PADA JARINGAN LISTRIK DI UKRAINA

Serangan dunia maya (bahasa Inggris: *cyberattack*) adalah jenis manuver ofensif yang digunakan oleh negara-negara, individu, kelompok, atau organisasi yang menargetkan sistem informasi komputer, infrastruktur, jaringan komputer, dan/atau perangkat komputer pribadi dengan berbagai cara tindakan berbahaya yang biasanya berasal dari sumber anonim yang mencuri, mengubah, atau menghancurkan target yang ditentukan dengan cara meretas sistem yang rentan. Serangan ini dapat diberi label sebagai kampanye dunia maya, perang dunia maya atau terorisme dunia maya dalam konteks yang berbeda. Serangan dunia maya dapat terjadi dari menginstal perangkat pengintai di komputer pribadi untuk mencoba menghancurkan infrastruktur seluruh negara. Serangan dunia maya telah menjadi semakin canggih dan berbahaya.

TENTANG SERANGAN JARINGAN LISTRIK DI UKRAINA

Serangan pada jaringan listrik tidak lagi menjadi perhatian teoritis. Pada tahun 2015, penyerang menurunkan sebagian jaringan listrik di Ukraina. Meskipun atribusi tidak pasti, keadaan geopolitik dan bukti forensik menunjukkan keterlibatan Rusia. Setahun kemudian, peretas Rusia menargetkan gardu tingkat transmisi, menghentikan bagian Kiev. Pada tahun 2014, Admiral Michael Rogers, direktur National Security Agency, memberi kesaksian di depan Kongres AS bahwa China dan beberapa negara lain kemungkinan memiliki kemampuan untuk menutup jaringan listrik AS. Iran, sebagai pelaku cyber yang baru muncul, bisa mendapatkan kemampuan seperti itu. Digitasi cepat dikombinasikan dengan tingkat investasi yang rendah dalam keamanan dunia maya dan rezim peraturan yang lemah menunjukkan bahwa sistem tenaga AS rentan - jika tidak lebih rentan - terhadap serangan cyber sebagai sistem di bagian lain dunia.

Serangan ini dilaksanakan pada 23 Desember 2015, ini direncanakan dengan hati-hati. Jaringan dan sistem dikompromikan sejak delapan bulan sebelumnya. Dengan mengingat kerangka waktu ini penting untuk pemahaman yang benar tentang cara dan sarana yang

seharusnya digunakan untuk mendeteksi, dan pada akhirnya mencegah serangan serupa. Analisis tentang cyberattack ini meliputi beberapa poin:

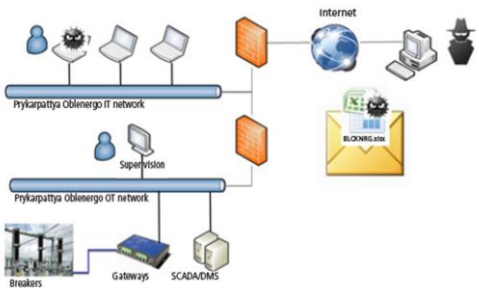
- Intrusi awal jaringan teknologi informasi (IT) menggunakan phishing tombak.
- Intelijen mengumpulkan jaringan dan sistem TI dan OT menggunakan perangkat lunak BlackEnergy yang fleksibel: pemindaian jaringan, melompat dari satu sistem ke sistem lainnya, identifikasi kerentanan perangkat, perancangan serangan, dan pemasangan malware dan backdoor di masa depan.
- Serangan berlangsung 10 menit pada 23 Desember.

TAHAPAN SERANGAN

1. Malware di Email

Pada musim semi 2015, varian malware BlackEnergy dipicu sebagai karyawan Prykarpattya Oblenergo membuka lampiran Excel dari sebuah email. BlackEnergy adalah "suite" malware yang pertama kali menayangkan berita pada tahun 2014, saat digunakan secara luas untuk menyusup ke utilitas energi. Tujuannya adalah mengumpulkan intelijen tentang infrastruktur dan jaringan dan untuk membantu mempersiapkan serangan cyber masa depan.

Diagram pada gambar 1 adalah tampilan disederhanakan dari arsitektur jaringan (yaitu Internet, IT, OT) dan akan membantu menggambarkan setiap langkah serangan cyber. Peretas ditampilkan sebagai "orang topi hitam" di sisi kanan atas. Peretas menggunakan koneksi IT utilitas ke Internet sebagai saluran untuk mempersiapkan dan pada akhirnya memicu serangan cyber.



Gambar 1. Arsitektur Sistem Kontrol

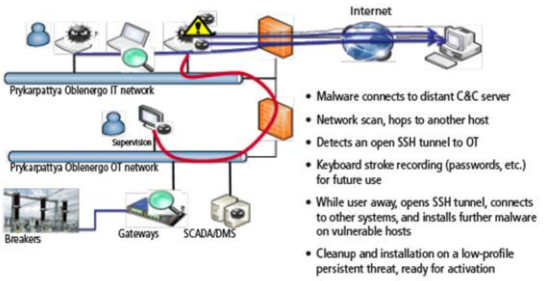
Kita dapat melihat bahwa perusahaan memasang firewall yang tepat, satu di antara jaringan TI dan Internet dan yang kedua antara jaringan TI dan OT (industri). Jaringan PL mencakup kontrol pengawasan sistem distribusi dan akuisisi data dengan server dan workstation dan satu set gateway yang digunakan untuk mengirim pesanan dari DMS ke unit terminal jarak jauh yang mengendalikan pemutus dan peralatan lainnya di gardu listrik. Perangkat tambahan juga terhubung ke jaringan (misalnya, workstation teknik dan server sejarawan) namun tidak relevan untuk kinematika serangan.

Pada langkah ini, hacker berhasil mengkompromikan satu laptop kantor berkat attachment email BlackEnergy. Hal ini sulit dicegah selama orang membuka lampiran email yang tampak sah.

2. Persiapan Serangan, Pemindaian Jaringan dan Ancaman Terus Menerus

Selama beberapa bulan di musim panas 2015, malware BlackEnergy dikendalikan dari jarak jauh untuk mengumpulkan data, melompat dari satu host ke host yang lain, mendeteksi kerentanan, dan bahkan berhasil masuk ke jaringan OT dan melakukan aktivitas "pengintaian" serupa.

Analisis data forensik tentang fase ini tidak lengkap, karena si hacker melakukan beberapa pembersihan dan menghapus beberapa disk selama serangan yang sebenarnya. Namun demikian, analisis BlackEnergy sebelumnya, serta pertimbangan yang masuk akal mengenai proses standar yang digunakan untuk serangan balik cyber, membuat kemungkinan pemulihan berikut dengan keyakinan yang masuk akal.



Gambar 2. Tahap Kedua

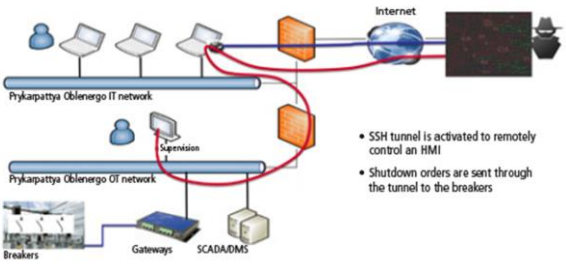
Seperti yang ditunjukkan pada gambar 2, pada tahap kedua, sejumlah besar aktivitas jaringan berlangsung. Perangkat lunak yang dikendalikan remote tersebut memindai jaringan TI, mendeteksi adanya koneksi terbuka dari sistem TI ke platform pengawasan PL, melakukan pemindaian jaringan OT, mengumpulkan informasi komponen PL, dan akhirnya menginstal komponen malware yang siap dipicu pada IT dan PL sistem.

Fase ini berlangsung berminggu-minggu, mungkin berbulan-bulan, dan diizinkan melakukan pengembangan eksploitasi khusus. *Eksploitasi* adalah sedikit perangkat lunak yang dirancang dan dikembangkan untuk memanfaatkan kerentanan tertentu. Ini disematkan sebagai muatan pada perangkat lunak perusak yang dikonfigurasi untuk mengirimkan muatan untuk eksekusi pada target. Sebenarnya usaha ini agak terbatas. Satu-satunya kode asli malware yang dikembangkan adalah yang diperlukan untuk membatalkan gateway sebagai bagian dari langkah ketiga. Dan ini benar-benar bukan "usaha" yang signifikan, karena gerbang sudah lama dikenal sebagai perangkat yang rentan.

3. Pelaksanaan Serangan

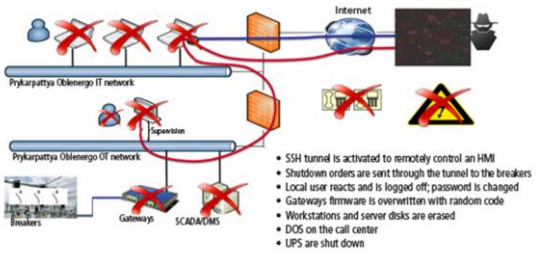
Sore hari dua hari sebelum Natal, seperti yang dinyatakan oleh operator, mouse bergerak pada antarmuka manusia-mesin (HMI) dan mulai mematikan pemutus jarak jauh. Ketika operator lokal berusaha untuk mendapatkan kembali kendali atas antarmuka pengawasan, dia log off dan tidak dapat login lagi, karena kata sandinya telah diubah (gambar 3).

Seluruh serangan hanya berlangsung selama beberapa menit. Peretas menggunakan malware yang sudah terinstal untuk mengendalikan HMI dari jarak jauh dan mematikan sebagian besar gardu induk dari grid. Malware tambahan, khususnya eksploitasi yang dikembangkan khusus, digunakan untuk mencegah operator mendapatkan kembali kendali jaringan dengan menghapus banyak disk (menggunakan KillDisk) dan menimpa firmware gateway Ethernet-to-serial dengan kode acak, sehingga mengubah perangkat menjadi potongan potongan yang tidak terpulihkan.



Gambar 3. Serangan (1)

Aktivitas "bonus" tambahan termasuk melakukan serangan denial-of-service terdistribusi di call center, mencegah pelanggan menghubungi distributor, dan mematikan catu daya tak terputus untuk mematikan daya di pusat kendali itu sendiri (gambar 4).



Gambar 4. Serangan (2)

Langkah ini jelas ditujukan untuk mematikan kekuatan bagi ratusan ribu pelanggan Ukraina barat yang terhubung ke jaringan. Namun, sebagian besar usaha dihabiskan untuk memastikan bahwa daya tidak akan dinyalakan lagi: semua malwares spesifik dikembangkan dengan tujuan itu. Begitu dipicu, satu-satunya cara bagi operator untuk mencegah masalah itu adalah menghentikan serangan seperti yang dilakukan.

Tapi serangannya terlalu cepat untuk memungkinkan reaksi apapun; Memang, di lingkungan infrastruktur yang kritis, tindakan operator dapat menyebabkan masalah keamanan. Oleh karena itu, hanya tindakan yang telah ditentukan yang diizinkan, dan operator harus mengikuti panduan untuk melakukan tindakan apa pun. Jika terjadi situasi operasional yang tidak terduga, mereka tidak dilatih untuk membuat keputusan di tempat. Ini persis situasi dalam kasus Ukraina. Tindakan "Jelas" bisa menghentikan serangan tersebut (seperti menarik kabel yang menghubungkan PL ke jaringan TI), namun operator yang tidak terlatih tidak dapat diharapkan untuk mengambil langkah-langkah mengganggu pada inisiatif mereka sendiri dalam situasi yang penuh tekanan dimana kesalahan sangat mungkin dilakukan.

Sumber : https://www.isa.org/intech/20170406/