**KEAMANAN JARINGAN KOMPUTER**



**M. NIZAL**

**(09011181419025)**

**FAKULTAS ILMU KOMPUTER**

**JURUSAN SISTEM KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**2018**

**Kelompok hacker Korea Utara yang bernama Lazarus Curi Uang untuk demi tambah devisa negara**

Korea Utara ([Korut](http://global.liputan6.com/read/3038367/tangisan-dan-hujan-deras-warnai-peringatan-hari-kemerdekaan-korut?source=search)) tidak pernah selesai untuk menuai sensasi. Selain terus menerus mendapat gencatan dari dunia internasional akibat uji coba persenjataan nuklirnya, negara ini juga mendapat sorotan akibat serangan hacker-nya yang merugikan banyak pihak.

Meski demikian, serangan hacker Korea Utara dilakukan bukan tanpa alasan. Hasil studi Institut Keamanan Finansial Korea Selatan atau FSI menyebutkan, aksi peretasan ini dilakukan Korea Utara untuk mencuri uang demi menghidupi negaranya yang miskin di tengah belenggu sanksi internasional.

Dilansir dari Thestar.com.my, Sabtu (29/7/2017), awalnya dunia internasional mencurigai motif Korut di balik aksi peretasan untuk mencuri berbagai data rahasia pemerintahan di beberapa negara. Namun FSI mengungkap, hal tersebut tidak lagi dilakukan dalam beberapa tahun belakangan ini.

Banyaknya mata uang asing yang masuk ke Korea Utara membuat kecurigaan tersendiri bagi badan intelijen ini. FSI mengatakan, mata uang asing tersebut justru didapat pemerintah [Korut](http://bisnis.liputan6.com/read/3034833/mau-dongkrak-ekonomi-korut-kirim-ribuan-warga-untuk-jadi-budak?source=search)dari aksi peretasan yang dilakukan pasukan sibernya.

Korea Utara dicurigai berada di balik kelompok peretas internasional bernama Lazarus. Laporan terbaru dari analisa kejahatan cyber pemerintah Korea Selatan dengan sejumlah lembaga komersial pada 2015 hingga 2017 menemukan nama jaringan kerja Lazarus lainnya, yakni Andariel.

"Bluenoroff dan Andariel memiliki kesamaan akar, namun mereka berbeda target dan motif. Andariel fokus untuk menyerang bisnis Korea Selatan dan lembaga pemerintahan dengan menggunakan metode yang dirancang khusus untuk negara itu," ujar laporan tersebut.

Menurut National Intelligence Service, Korea Selatan, ada sekitar 1.000 hingga 3.000 hacker profesional yang dibina Korut. Pemerintah Korut melatih para hacker tersebut di sekolah-sekolah elite dan ditempatkan dalam satu tempat tinggal terpusat sehingga mudah dimanfaatkan untuk melancarkan serangan siber ke berbagai negara.

Dari aksi meretasnya, pasukan siber Korut mampu mendulang untung besar. Seperti dilaporkan Dailybeast, aksi hacker Korut meretas Bangladesh Bank pada 2016 dan mampu mencuri uang hingga US$ 1 miliar. Jumlah uang tersebut dinilai cukup untuk membiayai percobaan nuklir di Korut.

Sebelumnya diberitakan, pasukan hacker Korea Utara juga mampu meretas Banco del Austro di Ekuador. Aksi pencurian ini mampu meraup uang hingga US$ 12 juta pada 2015.

Paling baru, lembaga keamanan siber Korea Selatan menuduh hacker Korea Utara atas pencurian bitcoin senilai US$ 90 ribu. Pencurian ini dilakukan setiap bulan dari Korea Selatan dan beberapa negara di dunia sepanjang 2013-2015.

Laporan yang dikeluarkan perusahaan keamanan Symantec Corp menjelaskan, kelompok hacker Korea Utara sering disebut dengan nama Lazarus. Dalam sebuah pernyataan di blog-nya, Symantec mengatakan kelompok ini bertanggung jawab atas serangan siber di 31 negara.

Kasus hacking terbesar yang ditemukan Symantec adalah di Polandia, diikuti Amerika Serikat (AS), Meksiko, Brasil, dan Chili.

Meski sebagian besar serangan siber itu tak berhasil mendapatkan sejumlah uang, Symantec menyebut sebagian lagi berhasil menghasilkan uang dengan metode yang makin canggih. Misalnya, saat meretas sebuah situs di Polandia, para hacker [Korut](http://bisnis.liputan6.com/read/2945722/berapa-uang-yang-dihasilkan-pasukan-hacker-korea-utara?source=search) menanamkan kode berbahaya ke laman tersebut.



**Gambar 1. Negara yang menjadi Target serangan kelompok Lazarus**

**2.** **SKENARIO MAUPUN TAKTIK DARI KELOMPOK LAZARUS**



**Gambar 2. Teknik yang digunakan kelompok Lazarus untuk melakukan penyerangan**

**TAKTIK YANG DIGUNAKAN KELOMPOK LAZARUS**

1. Taktik awal dari kelompok lazarus yaitu mereka melakukan diskusi atau tahap kompromi untuk memilih server mana yang akan digunakan sebagai pintu masuk ke perusahaan yang ingin diserang .
2. Taktik kedua dari kelompok ini mereka memiliki sebuah backdoor untuk tahap dasar yang digunakan untuk tujuan pengintaian. Kelompok penyerangan ini dengan cepat bemigrasi atau berpindah – pindah ke sistem lain di perusahaan dan mendapatkan pijakan.
3. Taktik ketiga para penyerang ini menganalisa jaringan dan melakukan identifikasi aset penting dalam organisasi tersebut.
4. Taktik terakhir yang dilakukan kelompok lazarus ini mereka menggunakan malware khusus untuk dikerahkan yang digunakan untuk menonaktifkan pemeriksaan keamanan dari internal dari software. Digunakan juga malware penyaringan pesan cepat terintegrasi untuk menyembunyikan pesan nakal yang dibuat oleh penyerang.

**3. DAMPAK YANG DITIMBULKAN DARI KELOMPOK LAZARUS**

Menurut Senior Security Researcher Kaspersky Lab, Juan Guerrero, pihaknya melalui sebuah program bernama operasi Blockbuster tengah mengembangkan penelitian terkait dengan aksi hacking yang dilakukan oleh kelompok Lazarus. Hal ini dirasa sangat penting karena kelompok ini telah mulai menunjukkan ancaman yang serius, tidak hanya di negara tertentu saja namun telah menyebar hingga ke seluruh dunia.

Pengamatan ini sendiri dilakukan dengan data pertama ketika kelompok Lazarus mengadakan penyerangan terhadap perusahaan Sony Pictures beberapa tahun yang lalu. Selepas itu, angka dari tindak hacking yang disinyalir didalangi oleh kelompok Lazarus terus meningkat mulai tahun 2010.

Selain menyerang perusahaan yang bergerak di bidang entertainment, Sony Picture, kelompok Lazarus sebelumnya juga sempat mencuat dengan aksi serangan berjuluk DarkSeoul yang memakan korban perusahaan perbankan serta sistem kemiliteran Korea Selatan. Bisa dibayangkan, kapasitas serta kemampuan dari kelompok ini tentu tidak bisa dianggap remeh. Pasalnya melihat dari pola serangan dan juga target yang diincar, kelompok ini nampak sangat profesional dan rapi dalam menjalankan aksinya.

Kelompok Lazarus sekarang sedang banyak melakukan serangan terhadap bank- bank yang ada didunia ini. bank – bank dunia telah banyak mengalami kerugian yang dilakukan oleh kelompok ini . diduga kuat kelompok ini di perintahkan langsung oleh pemerintahan korea utara untuk memperbaiki keuangan dinegara tersebut serta menaikan devisa negara mereka