Kerangka Kerja untuk Perburuan Ancaman Siber Bagian 1: Piramida Rasa Sakit

23 Juli 2015 oleh
Tim Sqrrl

Kerangka Kerja untuk Perburuan Ancaman Siber Bagian 1: Piramida Penderitaan

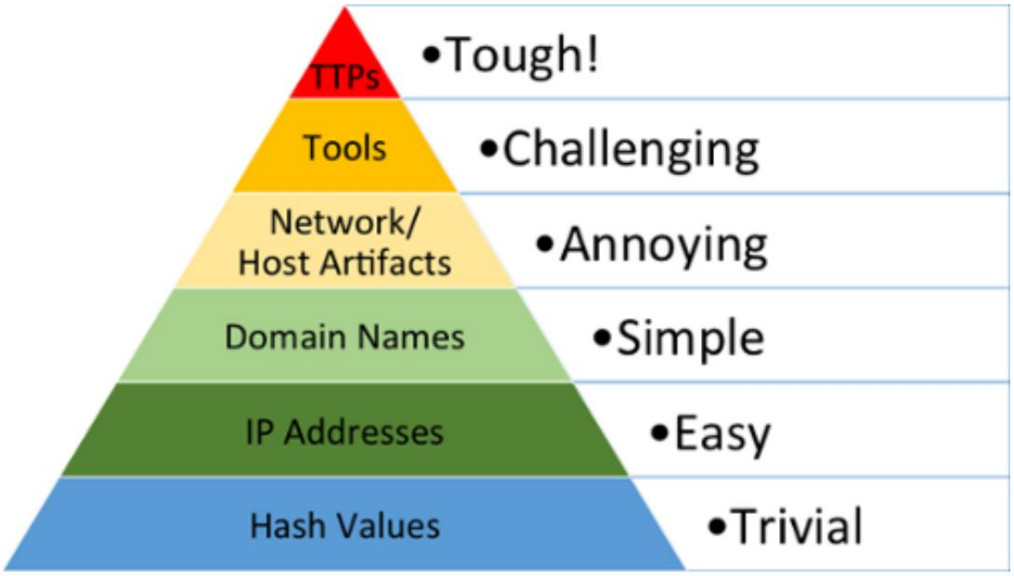
Meskipun mesin deteksi berbasis aturan merupakan fondasi yang kuat bagi organisasi keamanan mana pun, perburuan ancaman dunia maya merupakan kemampuan penting yang harus dimiliki organisasi keamanan untuk mendeteksi ancaman canggih yang tidak diketahui. Perburuan melampaui pendekatan deteksi berbasis aturan dan berfokus pada pendeteksian dan penyelidikan ancaman secara proaktif.

"Perjalanan" perburuan siber didorong oleh hipotesis, memanfaatkan pertanyaan atau hipotesis awal (misalnya, sekelompok eksekutif bepergian ke Tiongkok untuk melakukan negosiasi bisnis; mereka berisiko tinggi mengalami kompromi) untuk terlibat dalam pencarian eksploratif dan berulang melalui kumpulan data keamanan siber. Perjalanan perburuan difokuskan pada pengumpulan Indikator Kompromi (IoC) untuk menemukan musuh, dan dapat memberikan dasar yang kuat tentang cara membentuk hipotesis. Perburuan apa pun dapat dan harus memanfaatkan teknik statistik dan pembelajaran mesin tingkat lanjut untuk membantu analis memprediksi di mana harus memulai dan bagaimana melanjutkannya. Dalam blog ini, kami akan membahas berbagai jenis IoC yang dapat digunakan sebagai titik awal.

Tulisan ini berfokus pada cara berpikir tentang IoC. Ada berbagai macam IoC mulai dari hash file dasar hingga Taktik, Teknik, dan Prosedur peretasan (TTP). Arsitek Keamanan Sqrrl, David Bianco, menggunakan konsep yang disebut Pyramid of Pain untuk mengkategorikan IoC. Piramida tersebut mengorganisasikan IoC dalam dua cara:

1. Seberapa sulit (menyakitkan) mengumpulkan dan menerapkan IoC pada pertahanan siber? Nilai hash berbahaya dan IP alamat IP relatif mudah diperoleh dan diintegrasikan ke dalam alat keamanan. TTP lebih sulit diidentifikasi dan diterapkan, karena sebagian besar alat keamanan tidak cocok untuk memanfaatkannya.
2. Seberapa besar kerugian yang dapat ditimbulkan IoC terhadap musuh siber? Relatif mudah bagi musuh untuk mengaburkan kode malware dan mengubah nilai hash. Alamat IP dapat diubah secara dinamis dengan biaya rendah. TTP bersifat lengket dan mahal bagi musuh untuk diubah. Akibatnya, alat keamanan yang memanfaatkan TTP dapat menimbulkan kerugian yang lebih besar pada musuh.

Rincian mengenai berbagai tingkatan dalam Piramida Rasa Sakit disediakan di bawah ini.



Piramida Rasa Sakit, awalnya dikembangkan oleh David Bianco: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Mari kita mulai dengan mendefinisikan jenis indikator yang membentuk piramida:

1. Nilai Hash: SHA1, MD5 atau hash serupa lainnya yang sesuai dengan file mencurigakan atau berbahaya tertentu. Sering digunakan untuk memberikan referensi unik ke sampel malware tertentu atau ke file yang terlibat dalam intrusi. Nilai hash sangat mudah berubah, dan jumlahnya sangat banyak, sehingga dalam banyak kasus bahkan tidak ada gunanya untuk melacaknya.

2. Alamat IP: Alamat IP secara harfiah merupakan indikator paling mendasar, tetapi jika mereka menggunakan layanan proxy anonim seperti Tor atau yang serupa, mereka dapat mengubah IP cukup sering dan tidak pernah menyadari atau peduli.

3. Nama Domain: Ini bisa berupa nama domain itu sendiri (misalnya, “evil.net”) atau bahkan sub- atau sub-sub-domain (misalnya, “this.is.soooo.evil.net”). Nama-nama tersebut harus didaftarkan, dibayar (bahkan jika dengan dana curian) dan dihosting di suatu tempat. Meskipun demikian, ada banyak penyedia DNS di luar sana dengan standar pendaftaran yang longgar.

4. Artefak Jaringan: Dalam praktiknya, ini adalah bagian dari aktivitas yang mungkin cenderung membedakan malware aktivitas dari pengguna yang sah. Contoh tipikal mungkin pola URI, informasi C2 yang tertanam dalam protokol jaringan, dll.

5. Artefak Host: Observasi yang disebabkan oleh aktivitas musuh pada satu atau beberapa host Anda yang akan membedakan aktivitas jahat dari aktivitas sah. Ini bisa berupa pengenal khusus seperti kunci registri atau nilai yang diketahui dibuat oleh malware tertentu, file atau direktori yang diletakkan di tempat tertentu, dll.

6. Alat: Perangkat lunak yang digunakan oleh penyerang untuk menyelesaikan misinya. Sebagian besar berupa barang yang mereka bawa, bukan perangkat lunak atau perintah yang mungkin sudah terpasang di komputer. Ini mencakup utilitas yang dirancang untuk membuat dokumen berbahaya untuk spearphishing, backdoor yang digunakan untuk membuat C2 atau cracker kata sandi, atau utilitas berbasis host lain yang mungkin ingin mereka gunakan setelah peretasan.

7. Taktik, Teknik dan Prosedur (TTP): Di puncak piramida adalah bagaimana musuh bertindak menyelesaikan misi mereka, mulai dari pengintaian hingga penyusupan data dan di setiap langkah di antaranya. Saat Anda mendeteksi dan merespons pada level ini, Anda beroperasi langsung pada perilaku musuh, bukan melawan alat mereka. “Spearphishing” adalah TTP umum untuk membangun kehadiran di jaringan.

> “Spearphishing dengan file PDF Trojan” atau “… dengan tautan ke file .SCR berbahaya yang disamarkan sebagai ZIP” akan menjadi versi yang lebih spesifik.

Poin penting dari Pyramid of Pain karya Bianco adalah bahwa TTP merupakan indikator yang paling berharga. TTP mencerminkan perilaku penyerang, dan perilaku tersebut memerlukan waktu dan investasi uang yang signifikan untuk dimodifikasi. Namun, TTP juga sulit untuk dimodelkan dan dideteksi menggunakan alat tradisional. Tidak seperti banyak indikator lainnya, TTP hanya dapat dikenali setelah Anda mampu menyusun narasi serangan. Dalam blog mendatang, kami akan menunjukkan cara cyber hunting dan Linked Data Analysis milik Sqrrl pendekatan ini secara unik dilengkapi untuk memodelkan dan mendeteksi TTP. Di bagian 2 dari seri blog ini kami akan fokus secara khusus pada bagaimana organisasi keamanan dapat membangun lingkaran perburuan berbasis intelijen untuk mendukung deteksi TTP.